

Table of Contents

Cyber Forensics—A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes.....	1
Disclaimer.....	6
Introduction.....	7
Background.....	8
Dimensions of the Problem.....	9
Computer Forensics.....	10
Works Cited.....	11
Section I: Cyber Forensics.....	13
Chapter List.....	13
.....	13
Chapter 1: The Goal of the Forensic Investigation.....	14
Overview.....	14
Why Investigate.....	14
Internet Exceeds Norm.....	14
Inappropriate E-mail.....	16
Non-Work-Related Usage of Company Resources.....	17
Theft of Information.....	18
Violation of Security Parameters.....	18
Intellectual Property Infraction.....	19
Electronic Tampering.....	20
Establishing a Basis or Justification to Investigate.....	21
Determine the Impact of Incident.....	22
Who to Call/Contact.....	24
If You Are the Auditor/Investigator.....	24
Resources.....	25
Authority.....	25
Obligations/Goals.....	25
Reporting Hierarchy.....	25
Escalation Procedures.....	25
Time Frame.....	26
Procedures.....	26
Precedence.....	26
Independence.....	26
Chapter 2: How to Begin a Non-Liturgical Forensic Examination.....	27
Overview.....	27
Isolation of Equipment.....	27
Cookies.....	29
Bookmarks.....	31
History Buffer.....	32
Cache.....	34
Temporary Internet Files.....	35
Tracking of Logon Duration and Times.....	35
Recent Documents List.....	36
Tracking of Illicit Software Installation and Use.....	37

Table of Contents

Chapter 2: How to Begin a Non-Liturgical Forensic Examination

The System Review.....	38
The Manual Review.....	41
Hidden Files.....	42
How to Correlate the Evidence.....	43
Works Cited.....	44

Chapter 3: The Liturgical Forensic Examination: Tracing Activity on a Windows-Based

Desktop.....	45
Gathering Evidence For Prosecution Purposes.....	45
Gathering Evidence Without Intent to Prosecute.....	45
The Microsoft Windows-Based Computer.....	46
General Guidelines To Follow.....	48
Cookies.....	50
Bookmarks/Favorites.....	53
Internet Explorer's History Buffer.....	54
Temporary Storage on the Hard Drive.....	55
Temporary Internet Files.....	56
System Registry.....	57
Enabling and Using Auditing via the Windows Operating System.....	61
Confiscation of Computer Equipment.....	65
Other Methods of Covert Monitoring.....	66

Chapter 4: Basics of Internet Abuse: What is Possible and Where to Look Under the

Hood.....	68
Terms.....	68
Types of Users.....	69
E-Mail Tracking.....	69
IP Address Construction.....	69
Browser Tattoos.....	69
How an Internet Search works.....	70
Swap Files.....	74
ISPs.....	75
Servers.....	75
Works Cited.....	75

Chapter 5: Tools of the Trade: Automated Tools Used to Secure a System Throughout the Stages of a Forensic Investigation.....

Overview.....	77
Detection Tools.....	77
Protection Tools.....	84
Analysis Tools.....	87

Chapter 6: Network Intrusion Management and Profiling.....

Overview.....	91
Common Intrusion Scenarios.....	91
Intrusion Profiling.....	95
Creating the Profile.....	96
Conclusion.....	103

Table of Contents

Chapter 7: Cyber Forensics and the Legal System.....	105
Overview.....	105
How the System Works.....	105
Issues of Evidence.....	106
Hacker, Cracker, or Saboteur.....	108
Best Practices.....	115
Notes.....	115
Acknowledgments.....	116
Section II: Federal and International Guidelines.....	117
Chapter List.....	117
.....	117
References.....	118
Chapter 8: Searching and Seizing Computers and Obtaining Electronic Evidence.....	118
Recognizing and Meeting Title III Concerns in Computer Investigations.....	123
Computer Records and the Federal Rules of Evidence.....	131
Proposed Standards for the Exchange of Digital Evidence.....	134
Recovering and Examining Computer Forensic Evidence.....	140
International Principles for Computer Evidence.....	141
Chapter 9: Computer Crime Policy and Programs.....	143
The National Infrastructure Protection Center Advisory 01–003.....	143
The National Information Infrastructure Protection Act of 1996.....	146
Distributed Denial of Service Attacks.....	157
The Melissa Virus.....	163
Cybercrime Summit: A Law Enforcement/Information Technology Industry Dialogue.....	163
Chapter 10: International Aspects of Computer Crime.....	165
Council of Europe Convention on Cybercrime.....	165
Council of Europe Convention on Cybercrime Frequently Asked Questions.....	168
Internet as the Scene of Crime.....	168
Challenges Presented to Law Enforcement by High–Tech and Computer Criminals.....	169
Problems of Criminal Procedural Law Connected with Information Technology.....	169
Combating High–Tech and Computer–Related Crime.....	169
Vienna International Child Pornography Conference.....	171
OECD Guidelines for Cryptography Policy.....	171
Fighting Cybercrime: What are the Challenges Facing Europe?.....	171
Chapter 11: Privacy Issues in the High–Tech Context.....	172
Law Enforcement Concerns Related to Computerized Databases.....	172
Enforcing the Criminal Wiretap Statute.....	174
Referring Potential Privacy Violations to the Department of Justice for Investigation and Prosecution.....	174
Testimony on Digital Privacy.....	175
Chapter 12: Critical Infrastructure Protection.....	176
Attorney General Janet Reno's Speech on Critical Infrastructure Protection.....	176
Protecting the Nation's Critical Infrastructures: Presidential Decision Directive 63.....	176
The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential	

Table of Contents

Chapter 12: Critical Infrastructure Protection	
Decision Directive 63.....	177
Foreign Ownership Interests in the American Communications Infrastructure.....	187
Carnivore and the Fourth Amendment.....	188
Chapter 13: Electronic Commerce: Legal Issues.....	195
Overview.....	195
Guide for Federal Agencies on Implementing Electronic Processes.....	195
Consumer Protection in the Global Electronic Marketplace.....	196
The Government Paperwork Elimination Act.....	196
Internet Gambling.....	197
Sale of Prescription Drugs Over the Internet.....	197
Guidance on Implementing the Electronic Signatures in Global And National Commerce Act (E-SIGN).....	198
Part I: General Overview of the E-SIGN Act.....	198
The Electronic Frontier: the Challenge of Unlawful Conduct Involving the Use of the Internet.....	215
Internet Health Care Fraud.....	217
Jurisdiction in Law Suits.....	218
Electronic Case Filing at the Federal Courts.....	225
Notes.....	226
Chapter 14: Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies.....	229
Executive Summary.....	229
Introduction.....	237
I. Why Agencies Should Consider Legal Risks.....	238
II. Legal Issues to Consider in "Going Paperless".....	242
III. Reducing The Legal Risks in "Going Paperless".....	255
Conclusion.....	266
Notes.....	267
Chapter 15: Encryption.....	273
Department of Justice FAQ on Encryption Policy (April 24, 1998).....	273
Interagency and State and Federal Law Enforcement Cooperation.....	273
Law Enforcement's Concerns Related to Encryption.....	273
Privacy in a Digital Age: Encryption and Mandatory Access.....	274
Modification of H.R. 695.....	280
Security and Freedom Through Encryption Act.....	281
OECD Guidelines for Cryptography Policy.....	285
Recommended Reading.....	285
Chapter 16: Intellectual Property.....	286
Prosecuting Intellectual Property Crimes Guidance.....	286
Deciding Whether to Prosecute an Intellectual Property Case.....	286
Government Reproduction of Copyrighted Materials.....	286
Federal Statutes Protecting Intellectual Property Rights.....	286
IP Sentencing Guidelines.....	289
Intellectual Property Policy and Programs.....	292
Copyrights, Trademarks and Trade Secrets.....	294

Table of Contents

Section III: Forensics Tools.....	296
Chapter List.....	296
.....	296
Chapter 17: Forensic and Security Assessment Tools.....	297
Detection, Protection, and Analysis.....	297
Detection and Prevention Tools for the PC Desktop.....	297
Analysis Tools.....	299
Applications.....	301
Additional Free Forensics Software Tools.....	307
Chapter 18: How to Report Internet–Related Crime.....	308
Overview.....	308
The Internet Fraud Complaint Center (IFCC).....	309
Chapter 19: Internet Security: An Auditor's Basic Checklist.....	310
Firewalls.....	310
Supported Protocols.....	311
Anti–Virus Updates.....	311
Software Management Systems.....	312
Backup Processes and Procedures.....	312
Intra–Network Security.....	312
Section IV: Appendices.....	314
Appendix List.....	314
.....	314
Appendix A: Glossary of Terms.....	314
A–C.....	314
D.....	317
E–G.....	319
H–I.....	322
K–Q.....	323
R–S.....	324
T–W.....	326
Appendix B: Recommended Reading List.....	329
Books.....	329
Articles.....	332
Web Sites.....	333
List of Exhibits.....	337
Chapter 2: How to Begin a Non–Liturgical Forensic Examination.....	337
Chapter 3: The Liturgical Forensic Examination: Tracing Activity on a Windows–Based Desktop.....	337
Chapter 4: Basics of Internet Abuse: What is Possible and Where to Look Under the Hood.....	337
Chapter 5: Tools of the Trade: Automated Tools Used to Secure a System Throughout the Stages of a Forensic Investigation.....	338
Chapter 6: Network Intrusion Management and Profiling.....	338
Chapter 8: Searching and Seizing Computers and Obtaining Electronic Evidence.....	338

Table of Contents

List of Exhibits

Chapter 9: Computer Crime Policy and Programs.....	338
Chapter 11: Privacy Issues in the High–Tech Context.....	338
Chapter 12: Critical Infrastructure Protection.....	339
Chapter 13: Electronic Commerce: Legal Issues.....	339
Chapter 14: Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies.....	339
Chapter 18: How to Report Internet–Related Crime.....	339