

Contents

<i>Introduction</i>	xvii
Chapter 1	The Need for Computer Forensics
	1
Defining Computer Forensics	2
Real-Life Examples of Computer Crime	4
Hacker Pleads Guilty to Illegally Accessing New York Times Computer Network	4
Man Pleads Guilty to Hacking Intrusion and Theft of Data Costing Company \$5.8 Million	5
Three Men Indicted for Hacking into Lowe's Companies' Computers with Intent to Steal Credit Card Information	6
Former Chief Computer Network Program Designer Arrested for Alleged \$10 Million Computer Software Bomb	7
Juvenile Computer Hacker Sentenced to Six Months in Detention Facility	8
Corporate versus Law Enforcement Concerns	9
Corporate Concerns Focus on Detection and Prevention	9
Law Enforcement Focuses on Prosecution	11
Russian Computer Hacker Indicted in California for Breaking into Computer Systems and Extorting Victim Companies	11
Training	13
Practitioners	13
End Users	15
What Are Your Organization's Needs?	18
Terms to Know	19
Review Questions	20
Chapter 2	Preparation—What to Do Before You Start
	21
Know Your Hardware	22
What I/O Devices Are Used?	22
Check Computers for Unauthorized Hardware	28
Keep Up to Date with New I/O Trends	32

- Know Your Operating System 35
 - Different Operating Systems 35
 - Know What Filesystems Are in Use 38
 - Maintain Tools and Procedures for
 - Each Operating System and Filesystem 40
 - Preinstalled Tools Make Forensics Easier 41
- Know Your Limits 42
 - Legal Organizational Rights and Limits 43
 - Search and Seizure Guidelines 44
 - Will This End Up in Court? 45
- Develop Your Incident Response Team 45
 - Organize the Team 46
 - State Clear Processes 46
 - Coordinate with Local Law Enforcement 47
- Terms to Know 48
- Review Questions 49

Chapter 3 Computer Evidence 51

- What Is Computer Evidence? 52
 - Incidents and Computer Evidence 52
 - Types of Evidence 52
- Search and Seizure 58
 - Voluntary Surrender 58
 - Subpoena 59
 - Search Warrant 59
- Chain of Custody 60
 - Definition 60
 - Controls 61
 - Documentation 64
- Evidence Admissibility in a Court of Law 66
 - Relevance and Admissibility 66
 - Techniques to Ensure Admissibility 67
- Leave No Trace 68
 - Read-Only Image 68
 - Software Write Blocker 69
 - Hardware Write Blocker 69
- Terms to Know 70
- Review Questions 71

Chapter 4 Common Tasks 73

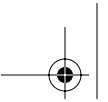
- Evidence Identification 74
 - Physical Hardware 75
 - Removable Storage 78
 - Documents 79

Evidence Preservation	80
Pull the Plug or Shut It Down?	81
Supply Power As Needed	82
Provide Evidence of Initial State	83
Evidence Analysis	85
Knowing Where to Look	85
Wading through the Sea of Data	87
Sampling Data	88
Evidence Presentation	88
Know Your Audience	89
Organization of Presentation	91
Keep It Simple	92
Terms to Know	93
Review Questions	94
Chapter 5 Capturing the Data Image	95
Full Volume Images	96
Evidence Collection Order	96
Preparing Media and Tools	97
Collecting the Volatile Data	100
Creating a Duplicate of the Hard Disk	103
Extracting Data from PDAs	107
Image and Tool Documentation	108
Partial Volume Image	109
Imaging/Capture Tools	111
Utilities	112
Commercial Software	113
PDA Tools	115
Terms to Know	115
Review Questions	116
Chapter 6 Extracting Information from Data	117
What Are You Looking For?	118
Internet Files	118
E-mail Headers	122
Deleted Files	126
Passwords	127
How People Think	129
Picking the Low-Hanging Fruit	130
Hidden Evidence	131
Trace Evidence	135
Terms to Know	137
Review Questions	138

Chapter 7	Passwords and Encryption	139
	Passwords	140
	Finding Passwords	141
	Deducing Passwords	142
	Cracking Passwords	143
	Encryption Basics	146
	Common Encryption Practices	147
	Private Key Algorithms	148
	Public Key Algorithms	150
	Steganography	151
	Strengths and Weaknesses of Encryption	152
	Key Length	153
	Key Management	153
	Handling Encrypted Data	154
	Identifying Encrypted Files	154
	Decrypting Files	155
	Terms to Know	159
	Review Questions	160
Chapter 8	Common Forensics Tools	161
	Disk Imaging and Validation Tools	162
	ByteBack	163
	<i>dd</i>	164
	DriveSpy	165
	EnCase	165
	Forensic Replicator	166
	FTK Imager	167
	Norton Ghost	168
	ProDiscover	168
	SafeBack	170
	SMART	170
	WinHex	171
	Forensics Tools	172
	Software Suites	172
	Miscellaneous Software Tools	184
	Hardware	187
	Your Forensics Toolkit	190
	Each Organization Is Different	192
	Most Examiners Use Overlapping Tools	192
	Terms to Know	192
	Review Questions	193

Chapter 9	Pulling It All Together	195
	Begin with a Concise Summary	196
	Document Everything, Assume Nothing	197
	Interviews and Diagrams	198
	Videotapes and Photographs	200
	Transporting the Evidence	201
	Documenting Gathered Evidence	201
	Additional Documentation	204
	Formulating the Report	205
	Sample Analysis Reports	206
	Case #234—NextGard Technology Copyright	
	Piracy Summary	207
	Additional Report Subsections	213
	Using Software to Generate Reports	214
	Terms to Know	218
	Review Questions	219
Chapter 10	How to Testify in Court	221
	Preparation Is Everything	222
	Understand the Case	224
	Understand the Strategy	225
	Understand Your Job	225
	Appearance Matters	226
	Clothing	226
	Grooming	226
	Attitude	227
	What Matters Is What They Hear	227
	Listening	228
	Tone	228
	Vocabulary	229
	Know Your Forensics Process and Tools	229
	Best Practices	230
	Your Process and Documentation	230
	Your Forensic Toolkit	231
	Say Only What Is Necessary	231
	Be Complete, But Not Overly Elaborate	231
	Remember Your Audience	232
	Keep It Simple	234
	Explaining Technical Concepts	234
	Use Presentation Aids When Needed	234
	Watch for Feedback	235
	Be Ready to Justify Every Step	235
	Summary	236
	Terms to Know	236
	Review Questions	237

Appendix A	Answers to Review Questions	239
	Chapter 1	239
	Chapter 2	240
	Chapter 3	240
	Chapter 4	241
	Chapter 5	242
	Chapter 6	243
	Chapter 7	244
	Chapter 8	245
	Chapter 9	246
	Chapter 10	247
Appendix B	Forensics Resources	249
	Information	249
	Organizations	249
	Publications	249
	Services	250
	Software	250
	Training	251
Appendix C	Forensics Certifications	253
	Advanced Information Security (AIS)	254
	Certified Computer Examiner (CCE)	254
	Certified Cyber-Crime Expert (C ³ E)	255
	Certified Information Forensics Investigator (CIFI)	255
	Certified Computer Crime Investigator (CCCI)	256
	Certified Computer Forensic Technician (CCFT)	256
	Certified Forensic Computer Examiner (CFCE)	257
	Certified Information Systems Auditor (CISA)	257
	EnCase Certified Examiner Program	258
	GIAC Certified Forensic Analyst (GCFA)	258
	Professional Certified Investigator (PCI)	258
Appendix D	Forensics Tools	261
	Forensics Tool Suites	261
	Ultimate Toolkit	261
	Maresware	261
	X-Ways Forensics	262
	Forensicware	262
	Password-Cracking Utilities	262
	Passware	262
	ElcomSoft	263



CD Analysis Utilities	263
IsoBuster	263
CD/DVD Inspector	264
Metadata Viewer Utility	264
Metadata Assistant	264
Graphic Viewing Utility	265
Quick View Plus	265
Forensics Hardware Devices	265
Intelligent Computer Solutions	265
Computer Forensics Training	266
Intense School Computer Forensics Training Class . .	266

Glossary **267**

Index 274

