

SECTION I COMPUTER FORENSIC INVESTIGATION BASICS

1	Computer Forensic Investigation Basics	3
	Chapter Objectives	3
	Introduction	3
A.	Forensics Defined	4
1.	Computer Forensic Science	5
B.	The Four-Step Process.....	5
1.	Acquisition	6
2.	Identification.....	6
3.	Evaluation	7
4.	Presentation.....	7
C.	What Is Electronic Evidence?	7
1.	Circumstantial	8
2.	Physical	8
3.	Hearsay	9
4.	Repeatability and Reproducibility	9
D.	Who Is at Risk?	10
1.	Incidents and Threats	10
a.	Incidents.....	11
b.	Threats	11
E.	Criminal versus Business Policy Investigations	12
1.	Criminal Activities.....	12
2.	Network and Computer Center Threats.....	13
3.	Infrastructure Threat Targets	14
F.	Proactive versus Reactive Policies.....	15
1.	White-Collar and Blue-Collar Crimes	16
2.	Legal Activity.....	16
	Chapter Summary	16
	Terms.....	17
	Review Questions	18

2	Policies, Standards, Laws, and Legal Processes	19
	Chapter Objectives	19
	Introduction	19
A.	Laws and Legal Issues	20
1.	Wiretaps.....	21
2.	Stored Electronic Communications.....	21
3.	Privacy Protection Act.....	23
4.	Cable Communications Privacy Act.....	23
5.	USA Patriot Act	23
6.	The Fourth Amendment.....	24
B.	Witnesses.....	24
C.	Evidence	25
D.	Search Warrants	27
1.	Discovery	27
2.	Interrogatories and Requests for Production.....	28
3.	Electronic Discovery	30
E.	Laws Relating to Computer Crimes.....	30
1.	Health Insurance Portability and Accountability Act.....	31
2.	Sarbanes-Oxley Act.....	31
a.	Title VIII: Corporate and Criminal Fraud Accountability Act of 2002	32
b.	Title IX: White-Collar Crime Penalty Enhancements.....	32
3.	Children's Online Privacy Protection Act of 1998	32
4.	California Database Security Breach Act of 2003	33
5.	The Computer Security Act	33
6.	The Privacy Act of 1974	34
7.	Uniform Electronic Transactions Act.....	34
8.	Electronic Signatures in Global and National Commerce Act	35
9.	Uniform Computer Information Transactions Act	35
F.	E-Mail Laws	35
1.	Title 18 USC Section 2511—Interception of Communication (Interception in Transit)	35
2.	Title 18 USC Section 2701–2711—Electronic Communications Privacy Act (ECPA)	36
	(Unlawful Access to Stored Communications)	36
G.	Computer Crime and Intellectual Property Section (CCIPS)	36
H.	Policies and Standards	36
1.	Generally Accepted Accounting Principles (GAAP)	37
2.	ISO 17799 Code of Practice for Security Management.....	37
3.	Information Technology Evidence Standards	37

I.	Policies.....	38
1.	Computer Resource Policies	38
2.	Computer-Use Requirements and Restrictions.....	39
3.	Organizational Security Policies.....	39
J.	Internal Investigations	40
1.	Civil and Criminal Computer Incidents.....	41
2.	Security Departments	41
3.	Civil Litigation.....	42
4.	Criminal Prosecution	43
5.	Law Enforcement Involvement.....	44
K.	Expert Witnesses and Computer Forensic Experts.....	45
1.	National Institute of Justice Methods.....	47
	Chapter Summary	47
	Terms.....	48
	Review Questions	51

3 Computer Forensic Examination Categories53

	Chapter Objectives	53
	Introduction	53
A.	Common Law Overview	54
B.	Financial Crime Categories	55
1.	Auction Fraud	55
2.	Economic Fraud and Property Theft	55
3.	Identity Theft	56
C.	Computer Crime Categories.....	57
1.	Software and Video Piracy	57
2.	Computer Threats and Intrusions	58
D.	Telecommunications Fraud.....	58
1.	E-Mail Issues	59
E.	Personal Crime Categories.....	59
1.	Domestic Violence	59
2.	Extortion.....	60
3.	Gambling.....	60
4.	Controlled Substances.....	60
5.	Prostitution	61
6.	Death and Assault Investigation.....	61
7.	Child Exploitation.....	61
F.	Cyber-Terrorism and Information Warfare	62
1.	Cyber-Terrorism	62
2.	Information Warfare	63
G.	Forensic Accounting	63
1.	Forensic Accountant.....	64
H.	Corporate Security and Computer-Use Policies	64

1.	Corporate Security Investigations.....	65
2.	Computer-Abuse Investigations.....	66
I.	Compliance Analysis Investigations.....	67
	Chapter Summary	68
	Terms.....	68
	Review Questions	70
4	Computer, Internet, and Electronic Crimes	71
	Chapter Objectives	71
	Introduction	71
A.	Scams and Scam Artists.....	72
1.	Free Credit Reports	73
2.	Free Prizes	73
3.	Pyramid Schemes and Chain Letters.....	73
4.	Questionnaires	73
5.	Job Advertisements.....	74
6.	Work-at-Home	74
7.	Charities.....	74
8.	Credit Information Requests	75
9.	Check Cashing.....	75
10.	Scam Baiting.....	76
11.	Resources	76
B.	Activities That Initiate Personal Asset Crimes.....	76
C.	Identity Theft.....	78
1.	Avoid Becoming a Victim of Identity Theft.....	80
D.	Victims of Identity Theft	82
1.	Contacts.....	82
2.	Credit Reporting Agencies	83
3.	Federal Deposit Insurance Corporation (FDIC).....	83
4.	Check-Verification Companies	84
E.	Internet Fraud.....	84
1.	Internet Fraud Tips	85
2.	New Solutions	86
3.	Internet Fraud Statistics	87
F.	Combating Identity Theft and Fraud.....	87
1.	Government Contacts	88
2.	Nongovernment Contacts	88
3.	Awareness and Education	88
4.	Using the Internet for Investigations	89
G.	Exploiting Children on the Web.....	89
1.	Child Predators	89
2.	Child Predators on the Internet.....	90

3.	Child Predator and Privacy Laws	91
4.	Child Predator Investigations	92
	Chapter Summary	93
	Terms.....	93
	Review Questions	94
5	Computers, Electronics, and Networking Environment	97
	Chapter Objectives	97
	Introduction	97
A.	E-Commerce and E-Business Issues	98
B.	Computers and Computer Devices.....	99
1.	Computer Systems.....	101
a.	Mainframes.....	101
b.	Client Servers/PCs/Laptops.....	103
2.	Personal Computing and Wireless Devices.....	104
a.	Personal Digital Assistants (PDAs) and Organizers.....	104
b.	Pagers.....	106
3.	Telephone Systems and Communication Devices.....	106
a.	Telephones and Cell Phones	108
b.	Answering Machines	109
4.	Network Devices.....	109
5.	Imaging Devices.....	110
a.	Printers.....	110
b.	Scanners	111
c.	Fax Machines	111
6.	Storage Devices	112
7.	Miscellaneous Electronic Devices.....	113
a.	Cameras	114
C.	The Next Steps.....	114
	Chapter Summary	114
	Terms.....	115
	Review Questions	116
6	Investigative Tools, Technical Training, and Forensic Equipment ...	117
	Chapter Objectives	117
	Introduction	117
A.	Forensic Investigation Requirements	118
1.	Tool Kits	119
2.	Forensic Workstations	121
B.	Forensic Software	122
1.	Computer Forensic Products	122
2.	Computer and Electronic Forensic Utilities and Programs.....	123

C.	Computer Media Recovery	123
1.	MD5 Algorithm.....	124
2.	SHA Algorithm.....	124
3.	CRC Algorithm	124
D.	Forensic Hardware Devices.....	125
1.	Imaging.....	125
E.	Surveillance Equipment.....	125
1.	Snooping.....	126
2.	Sniffing	126
3.	Probing	127
F.	Network Security Management.....	127
G.	Network Management Tools	128
1.	NetView	128
2.	OpenView	128
3.	SunNet Manager.....	129
4.	RMON	129
H.	Network Forensics	129
I.	Computer Forensic Training	130
1.	Training Requirements.....	131
2.	Training Providers.....	132
3.	Specialized Training.....	133
4.	Forensic Investigations Training.....	134
J.	Support Organizations.....	135
	Chapter Summary	136
	Terms.....	136
	Review Questions	137

SECTION II EVIDENCE COLLECTION AND MANAGEMENT

7	Managing the Crime/Incident Scene	141
	Chapter Objectives	141
	Introduction	141
A.	Scope of the Problem	142
1.	The Incident Scene	143
2.	The Initial Response.....	143
B.	Crime Scene Investigation	144
C.	Electronic and Computer Investigations.....	145
D.	Physical Evidence at a Crime Scene	146
E.	Types of Evidence	146
F.	Processing the Crime Scene	147
1.	Evidence Recognition and Identification	147
2.	Scene Documentation	147

3.	Evidence Collection	148
G.	Issues and Warnings when Seizing Evidence	149
H.	Steps for a Crime/Incident Scene Search.....	150
1.	Secure and Protect Scene	152
2.	Initiate Preliminary Survey	152
3.	Evaluate Physical Evidence Possibilities	153
4.	Prepare Narrative Description	153
5.	Take Photographs of Scene	154
a.	Photographs	154
6.	Prepare Diagram/Sketch of Scene	155
7.	Conduct Detailed Search, Record, and Collect Physical Evidence	156
8.	Conduct Final Survey	157
9.	Release Incident/Crime Scene	157
I.	Documentation Procedures	157
J.	Administrative Audit Worksheet	158
1.	Narrative Description.....	159
2.	Photographic Log.....	159
3.	Diagram/Sketch	159
4.	Evidence Recovery Log	159
5.	Latent Print-Lift Log.....	160
K.	Personnel Duties and Responsibilities.....	160
1.	Team Leader	160
2.	Photographer and Photographic Log Recorder	162
3.	Sketch Developer	162
4.	Evidence Recorder/Custodian	162
5.	Forensic Scientist or Evidence Recovery Technician.....	163
6.	Specialists and Consultants	163
	Chapter Summary	163
	Terms.....	164
	Review Questions	165

8	Investigating Computer Center Incidents	167
	Chapter Objectives	167
	Introduction	167
A.	Corporate Criminal Activities	169
B.	Preparation	170
C.	Case Categories	170
D.	Preliminary Investigation and Fact Finding.....	171
E.	Documenting the Corporate Incident Scene.....	172
F.	Conducting Interviews	174
G.	Identifying and Collecting Evidence.....	174
H.	Stand-Alone and Networked Computers	176

I.	Miscellaneous Devices	178
J.	Disclaimers That Aid Investigators	179
K.	E-Mail Investigations	180
L.	Types of Evidence	181
M.	Evidence Handling	181
1.	Forms and Documentation	182
2.	Labeling and Tagging.....	182
3.	Protecting and Packaging	182
4.	Transportation	184
5.	Storage	184
N.	Forensic Investigation Documents.....	185
O.	Law Enforcement Involvement	186
	Chapter Summary	186
	Terms.....	187
	Review Questions	188

9 Computer Systems Disk and File Structures189

	Chapter Objectives	189
	Introduction	189
A.	Disk Drive Overview.....	190
B.	Computer Hard Drive Interfaces	192
C.	Microsoft File System Overview	196
1.	Partitions.....	197
2.	Master Boot Record.....	197
3.	Registry Data	198
4.	Windows Forensic Tools.....	198
D.	Macintosh Computer Systems	198
1.	Forensic Tools for Mac Systems.....	199
E.	UNIX/Linux Systems.....	199
1.	Examining a UNIX or Linux System	200
2.	UNIX and Linux Forensic Tools.....	201
	Chapter Summary	201
	Terms.....	201
	Review Questions	204

10 The Computer and Electronic Forensic Lab205

	Chapter Objectives	205
	Introduction	205
A.	Computer Forensic Issues	206
B.	Forensic Laboratories	207
C.	Examining Computer Evidence.....	208
1.	Procedures and Practices	209
2.	Documentation and Reporting	210

D.	Data Recovery versus Forensic Recovery.....	210
E.	Forensic Analysis	212
F.	Collecting Evidence Relating to Electronic Systems	214
1.	Log Evidence.....	215
G.	Forensic Lab Functions.....	215
1.	Cyber-Intelligence	216
H.	Lab Design and Components	217
1.	Environmental	217
2.	Lighting	217
3.	Electrical and Cabling.....	218
4.	Communications.....	218
5.	Fire Suppression	219
6.	Security and Safety.....	219
7.	Storage	219
8.	Work Areas	220
I.	Devices, Tools, and Supplies.....	221
1.	Forensic Workstations	221
2.	Turnkey Forensic Workstation	221
3.	Supplies.....	224
4.	Toolbox and Tools.....	224
J.	Training Forensic Lab Examiners	225
1.	Certification and Training	226
2.	International Association of Computer Investigative Specialists (IACIS)	226
3.	High Technology Crime Investigation Association (HTCIA)	226
4.	SANS	227
5.	Computer Technology Investigators Network (CTIN)	227
6.	New Technologies, Inc. (NTI)	227
7.	National White Collar Crime Center (NW3C)	227
8.	Certified Electronic Evidence Collection Specialist (CEECS)	228
9.	Certified Forensics Computer Examiners (CFCE)	228
10.	Certified Computer Forensic Technician (CCFT)— Basic and Advanced.....	228
11.	Certified Computer Crime Investigator (CCCI)—Basic and Advanced	229
12.	EnCase Certified Examiner (EnCE).....	229
K.	Commercial Forensic Labs.....	229
L.	Forensic Lab Tools	231
1.	Software Tools.....	231
2.	CRCMd5 Data Validation Tool	232
3.	Forensic Tool Testing	233

4.	Hardware Tools.....	233
5.	Photography	234
M.	Computer Forensic Lab Issues and Concerns.....	234
1.	Portable Flyaway Kit	236
2.	Lab Work Flow	237
3.	Examinations	237
4.	Chain-of-Custody Checklist	237
5.	Evidence Receipt	238
6.	Hard Drive Examination	239
7.	Imaging Checklist.....	239
8.	Windows Examination Checklist.....	239
9.	Linux Examination Checklist	240
10.	Macintosh Examination Checklist	240
N.	Auditing the Forensic Lab	241
	Chapter Summary	241
	Terms.....	242
	Review Questions	243

11 Extracting Computer and Electronic Evidence245

	Chapter Objectives	245
	Introduction	245
A.	Forensic Laboratory Functions.....	246
B.	IACIS Guide for Forensic Examinations.....	247
C.	Managing the Imaging Process.....	249
D.	Evidence Collection and Archiving.....	250
1.	Order of Volatility	251
2.	Things to Avoid	251
3.	Privacy Considerations	252
4.	Legal Considerations	252
E.	Residual Data	252
F.	Examining the Digital Images.....	253
G.	Qualifying a Computer for Forensic Recovery.....	254
H.	Forensic Tools	256
I.	Disk Drive Examinations	258
1.	IDE-to-IDE Imaging	259
2.	Software Acquisition	260
J.	Review and Quality Assurance	260
1.	Proficiency Testing and Validation	262
K.	Legal Issues with Hard Drive Examinations.....	262
1.	Redaction	264
	Chapter Summary	266
	Terms.....	266

Review Questions	267
12 E-Mail and Internet Investigations	269
Chapter Objectives	269
Introduction	269
A. Internet Basics	270
B. E-Mail Basics.....	271
C. E-Mail Systems.....	272
D. Specialized Tools	273
E. Internet Search Tools	274
F. Crimes and Incidents Involving the Internet and E-Mail.....	276
G. E-Mail Investigations	276
H. Examining E-Mail Images.....	277
I. E-Mail Headers	278
1. SMTP Servers	278
J. E-Mail and Web Evidence	282
K. SPAM Investigations	285
L. Documenting Evidence	292
Chapter Summary	292
Terms.....	293
Review Questions	294
13 Mobile Phone and PDA Investigations	297
Chapter Objectives	297
Introduction	297
A. Wireless Protocols and Components.....	298
B. Mobile Telephone Service and Handset Providers	300
1. Mobile Phone Features	301
C. Subscriber Identity Module (SIM)	301
1. SIM Implementations	303
2. SIM Security	303
D. Memory Cards.....	304
E. Mobile Phone Investigations.....	304
1. SIM Forensics	305
2. SIM Data Acquisition	305
3. SIM Card Text Encoding	306
F. Wireless Device Forensics	306
1. Acquisitions and Device Seizures	307
2. To Prevent a Phone from Becoming PIN-Locked.....	308
G. Forensic Tools.....	309
H. Forensic Software Tools	311
I. Forensic Card Reader (FCR)	312
J. The International Mobile Station Identity (IMSI)	312

K.	PDA Investigations	313
1.	PDA Devices	313
2.	Hardware Characteristics	314
L.	PDA OS.....	315
M.	PDA Forensics	316
1.	A Caution when Using Forensic Tools.....	317
2.	Data Retrieval	318
N.	Forensic Examination Protocol	319
	Chapter Summary	321
	Terms.....	322
	Review Questions	324

14 Court Preparation, Presentations, and Testimony..... 325

	Chapter Objectives	325
	Introduction	325
A.	Computer and Electronic Evidence	326
1.	When Is Forensic Evidence Relevant?.....	327
B.	Technical and Expert Testimony	328
C.	The Financial Forensic Expert.....	328
D.	Forensic Accounting Testimony.....	329
E.	Court Appearances	331
1.	Preparing for Testimony.....	332
F.	Testifying in Court.....	334
G.	Presenting Evidence	334
H.	Direct Examination Testifying	335
I.	Cross-Examination Testifying	336
J.	The Deposition	337
	Chapter Summary	338
	Terms.....	338
	Review Questions	339

Glossary 341

Appendix A 359

	Investigation Forms	359
	Examination Forms	359

Appendix B 377

	Forensic Cases and Exercises	377
	Case 1	377
	Action	377
	Exercises	378
	Case 2	378

Action	378
Exercises	378

Appendix C 383

Answers to Review Questions	383
-----------------------------------	-----

Appendix D 391

Binary and Hexadecimal Number Systems	391
---	-----

Overview	391
----------------	-----

Decimal to Binary Conversion	392
------------------------------------	-----

Binary to Hexadecimal Conversion	393
--	-----

Binary Complement (Logical AND)	395
---------------------------------------	-----

ASCII	395
-------------	-----

Bibliography 397

Index 299