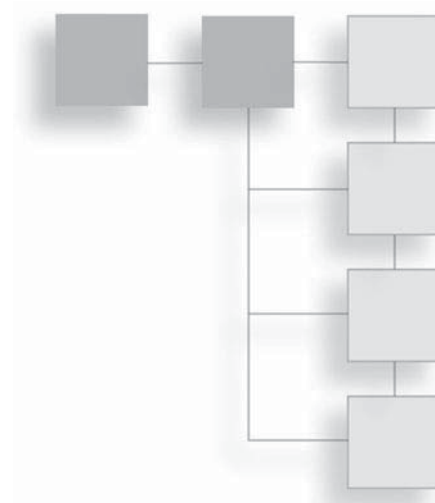


CONTENTS



Introduction	xvi
--------------------	-----

Part 1	Computer Crime	1
---------------	-----------------------------	----------

Chapter 1	Introduction to Computer Crime	3
------------------	---	----------

Introduction	3
Identity Theft	5
Phishing	7
Hacking or Spyware	10
Hacking	10
Spyware	11
Unauthorized Access of Data	12
Discarded Information	14
Cyber Stalking/Harassment	15
Real Cyber-Stalking Cases	18
Unauthorized Access to Computer Systems or Data	19
Fraud	19
Investment Offers	20
Auction Fraud	22
Check/Money-Order Fraud	23
Data Piracy	23
Non-Access Computer Crimes	24
Cybercrime Meets the Real World	25

	Hate Groups, Gangs, and the Internet	26
	Conclusion	29
Chapter 2	A History of Computer Crime in America	31
	Introduction	31
	The "Prehistory" of Computer Crime	33
	The Early Days	38
	The 1990s	43
	The 21 st Century	50
	Modern Attacks	54
	Privilege Escalation	55
	Malware	56
	Viruses	57
	Worms	58
	Spyware	58
	The Trojan Horse	59
	Logic Bomb	59
	Rootkit	61
	Phishing	61
	Social Engineering	63
	Session Hijacking	63
	Password Cracking	64
	Denial of Service	65
	Issues	69
	Conclusion	69
Chapter 3	United States Computer Laws Part I	71
	Introduction	71
	The Ribicoff Bill	72
	The Computer Fraud and Abuse Act of 1986	72
	Amendments to the Legislation	77
	Related Cases	77
	The Actual Law	78
	The Electronic Communications Privacy Act of 1986	82
	Related Cases	83
	The Actual Law	84

The Communications Decency Act of 1996	87
Related Cases.	88
The Actual Law	89
No Electronic Theft Act of 1997	93
Related Cases.	93
The Actual Law	94
Digital Millennium Copyright Act.	97
Related Cases.	97
Children’s Internet Protection Act	98
The Actual Law	99
CAN-SPAM Act of 2003.	104
Related Cases.	105
The Actual Law	106
Identity Theft Enforcement and Restitution Act of 2008	122
The Actual Law	123
Conclusion	127
 Chapter 4 United States Computer Laws Part II.	 131
Introduction	131
Cyber-Stalking Laws	131
California Cyber-Stalking Law.	132
Texas Cyber-Stalking Law	132
Utah Cyber-Stalking Laws	133
Louisiana Cyber-Stalking Laws	133
Miscellaneous States.	136
Identity-Theft Laws.	138
Alabama Consumer Identity Protection Act	138
Florida Criminal Use of Personal Identification Information	139
Idaho Identity-Theft Laws	141
New York Identity-Theft Laws.	142
Maryland Identity-Theft Laws.	143
Child-Pornography Laws	149
Arkansas Legislation.	149
Illinois Laws	150
California Laws	151
Connecticut Laws	152
Delaware Laws	153
Oregon Laws	154
Sexting	156

Hacking Laws	159
Maine Laws	159
Montana Laws	160
North Carolina Laws	161
Rhode Island Laws	163
State Spyware Laws	166
Arizona Laws	166
Texas Laws	167
Conclusion	168
 Chapter 5 Techniques and Resources for Computer Crime	171
Introduction	171
Identity-Theft Techniques	171
Non-Specific Identity Theft	173
Phishing	174
Spyware	176
Delivering Spyware to the Target	176
Legal Uses of Spyware	177
Obtaining Spyware Software	178
Non-Computer	179
Specific Target Identity Theft	180
Fraud Techniques	184
Auction Frauds	184
Shill Bidding	186
Bid Shielding	186
Bid Siphoning	187
Investment Offers	187
Common Investment Fraud Schemes	188
Investment Advice	189
Hacking Techniques	190
Footprinting	190
Password Cracking	195
Brute-Force Attack	196
Dictionary Attack	196
Web-Site Hacking	198
SQL Injection	198
Cross-Site Scripting	199
Session Hijacking	199

	Man-in-the-Middle Attack.	200
	Tools of the Trade.	200
	Sniffers	200
	Password Crackers.	200
	Conclusion	201
Chapter 6	Organized Crime and Cyber Terrorism	203
	Introduction	203
	Organized Crime on the Internet	204
	Traditional Crime Augmented with Computer Systems	204
	Computer Crimes Executed by Organized Groups	207
	Cyber Terrorism.	210
	Economic Attacks	210
	Information Warfare	217
	Cyber Espionage	219
	Conclusion	223
Part 2	Computer Forensics	225
Chapter 7	Observing, Collecting, Documenting, and Storing Electronic Evidence	227
	Introduction	227
	Federal Guidelines	229
	FBI Forensics Guidelines	229
	Seizing Without a Warrant	231
	Basic Forensics	233
	Securing the Scene	234
	Remove Individuals Involved.	235
	Document Everything.	236
	Conclusion	245
Chapter 8	Collecting Evidence from Hardware	247
	Introduction	247
	Forensic Tools	247
	AccessData Forensic Toolkit.	248
	E-fense Helix	248
	ILook.	249

	EnCase	249
	Preliminary Activities	251
	Working with EnCase	253
	Computer Acquisitions	259
	Conclusions	273
Chapter 9	Collecting Evidence from the Operating System.....	275
	Introduction	275
	Finding Evidence in Browsers, Chat Logs, and Other Applications	276
	Finding Evidence in the Browser	276
	Finding Evidence in Chat Logs	279
	Finding Evidence in System Logs	279
	Windows Logs	279
	Linux Logs	283
	Recovering Deleted Files	285
	Recovering Files from Windows	286
	UndeletePlus	287
	DiskDigger	287
	Recovering Files from Unix/Linux	290
	Other Forensic Tools	292
	The Sleuth Kit	292
	Disk Investigator	293
	Computer Online Forensic Evidence Extractor	294
	Important Locations to Check	295
	Checking in Windows	295
	Checking in Linux	296
	Operating-System Utilities	297
	Conclusion	300
Chapter 10	Collecting Evidence from Other Sources	301
	Introduction	301
	Tracing IP Addresses	301
	Gathering E-mail Evidence	307
	Gathering Evidence from Routers	311
	Gathering Evidence from a Cell Phone	313
	Gathering Evidence from Firewalls	315
	Gathering Evidence from Intrusion-Detection Systems	315
	Conclusion	315

Part 3	Litigation	317
Chapter 11	Experts and Expert Reports	319
	Introduction	319
	Selecting an Expert	319
	Clean Background Check	320
	Well Trained	321
	Academic Training and Programs	321
	Academic Credibility	322
	Certifications	323
	Security+	323
	CIW Security Analyst	324
	MCSE Security Specialization	325
	CISSP	326
	Certified Ethical Hacker	327
	Forensic Certifications	327
	Experience	328
	No Conflicts of Interest	328
	Personality Issues in an Expert	329
	Hiring and Paying Experts	331
	Volunteer Experts	332
	Expert Reports	333
	Conclusion	335
Chapter 12	Depositions and Trials	337
	Introduction	337
	Depositions	337
	What Is a Deposition?	338
	Rule 30	339
	Rule 31	345
	What to Do, What Not to Do	346
	Trials	350
	The Daubert Decision and Trials	351
	Use of Depositions at Trials	352
	Case Studies	356
	Expert Performs Well	356
	Expert Makes Major Mistake	357
	Expert Not Fully Qualified	358
	Conclusion	359

Chapter 13	Civil Matters Relating to Computer Crime	361
	Introduction	361
	Civil Law Related to Computer Crime	362
	The Main Categories of Civil Law	363
	Contract Law	363
	Tort Law	363
	Property Law	364
	What Court?	364
	The Process	365
	Pretrial	365
	Motions	367
	Trial	368
	Post Trial	370
	Real Cases	370
	U.S. v. AOL	371
	eBay v. Bidder's Edge, Inc.	372
	International Airport Centers, L.L.C. v. Citrin	373
	Conclusion	374
Part 4	Computer Crime and Individuals	377
Chapter 14	Protecting Children on the Internet	379
	Introduction	379
	The Problem	379
	How Online Predators Operate	380
	Solutions for Parents	382
	How to Know if Your Child Is Already in Danger	387
	Solutions for Law Enforcement	389
	Conclusion	390
Chapter 15	How to Protect Your Identity on the Internet	393
	Introduction	393
	What You Can Do	394
	Phishing	394
	Phishing E-mails	394
	Phishing Web Sites	396
	Spyware	398
	Gathering Personal Data	400

	General Countermeasures	401
	What to Do If You Become a Victim	402
	Law Enforcement and Identity Theft	404
	Conclusion	405
Chapter 16	Harassment and Stalking Via the Computer	407
	Introduction	407
	What Is Cyber Stalking and Harassment?	407
	Why Cyber Stalkers Do It	410
	Real-World Cases	411
	England's Most Obsessive Stalker	411
	70-Year-Old Man Stalks 16-Year-Old Girl Online	412
	Protecting Yourself	412
	Guidelines for Law Enforcement	414
	Conclusion	417
Part 5	Techniques	419
Chapter 17	Hacker Techniques	421
	Introduction	421
	The Pre-Attack Phase	422
	The Passive Search	422
	The Active Scan	425
	Angry IP	427
	NSAuditor	427
	Microsoft Baseline Security Analyzer	430
	Enumeration	433
	Manual Scanning	436
	The Attack Phase	437
	Physical Access Attacks	438
	OphCrack	438
	Cain and Abel	440
	Retrieve Login Accounts	440
	Get Other Passwords	441
	Get a Wireless Key	441
	Remote Access Attacks	443
	Countermeasures	445
	Conclusion	447

Chapter 18	How Cyber Criminals Communicate	449
	Introduction	449
	Encryption	449
	History of Encryption	449
	Caesar Cipher	450
	Multi-Alphabet Substitution	451
	Binary Operations	451
	Modern Encryption Methods	453
	Data Encryption Standard	454
	RSA	454
	Others	455
	How Criminals Use Encryption	455
	Steganography	457
	Leet	461
	Meeting	464
	Online Discussions	464
	Conclusion	465
Appendix A	Introduction to Computer Networks	467
	Introduction	467
	Network Basics	467
	The Physical Connection	467
	The Hub	469
	The Switch	469
	The Router	469
	The Data Packets	469
	IP Addresses	471
	Basic Network Utilities	471
	IPConfig	472
	ping and tracert	473
	Network Security Measures	475
Appendix B	Glossary	477
	Index	483