# Contents

ACKNOWLEDGMENTS.......... xiii
AUTHOR BIOGRAPHIES.......... xv
INTRODUCTION.......... xxi

**PART 1 Digital Forensics**

**CHAPTER 1** Foundations of Digital Forensics.......... 3
*Eoghan Casey*

1.1 Digital Evidence.......... 7
1.2 Increasing Awareness of Digital Evidence.......... 9
1.3 Digital Forensics: Past, Present, and Future.......... 10
1.4 Principles of Digital Forensics.......... 14
1.5 Challenging Aspects of Digital Evidence.......... 25
1.6 Following the Cybertrail.......... 28
1.7 Digital Forensics Research.......... 32
1.8 Summary.......... 32

**CHAPTER 2** Language of Computer Crime Investigation.......... 35
*Eoghan Casey*

2.1 Language of Computer Crime Investigation.......... 36
2.2 The Role of Computers in Crime.......... 39
2.3 Summary.......... 47

**CHAPTER 3** Digital Evidence in the Courtroom.......... 49
*Eoghan Casey*

3.1 Duty of Experts.......... 51
3.2 Admissibility.......... 56
3.3 Levels of Certainty in Digital Forensics.......... 68
3.4 Direct versus Circumstantial Evidence.......... 72
3.5 Scientific Evidence.......... 73

3.6 Presenting Digital Evidence ........ 75
3.7 Summary ........ 81

CHAPTER 4 Cybercrime Law: A United States Perspective ........ 85
*Susan W. Brenner*

4.1 Federal Cybercrime Law ........ 85
4.2 State Cybercrime Law ........ 103
4.3 Constitutional Law ........ 107
4.4 Fourth Amendment ........ 107
4.5 Fifth Amendment and Encryption ........ 115

CHAPTER 5 Cybercrime Law: A European Perspective ........ 123
*Bert-Jaap Koops and Tessa Robinson*

5.1 The European and National Legal Frameworks ........ 123
5.2 Progression of Cybercrime Legislation in Europe ........ 126
5.3 Specific Cybercrime Offenses ........ 129
5.4 Computer-Integrity Crimes ........ 133
5.5 Computer-Assisted Crimes ........ 149
5.6 Content-Related Cybercrimes ........ 155
5.7 Other Offenses ........ 173
5.8 Jurisdiction ........ 178
5.9 Summary ........ 182

PART 2 Digital Investigations

CHAPTER 6 Conducting Digital Investigations ........ 187
*Eoghan Casey and Bradley Schatz*

6.1 Digital Investigation Process Models ........ 187
6.2 Scaffolding for Digital Investigations ........ 197
6.3 Applying the Scientific Method in Digital Investigations ........ 201
6.4 Investigative Scenario: Security Breach ........ 220
6.5 Summary ........ 224

CHAPTER 7 Handling a Digital Crime Scene ........ 227
*Eoghan Casey*

7.1 Published Guidelines for Handling Digital Crime Scenes ........ 230
7.2 Fundamental Principles ........ 232
7.3 Authorization ........ 234

7.4 Preparing to Handle Digital Crime Scenes....238
7.5 Surveying the Digital Crime Scene....240
7.6 Preserving the Digital Crime Scene....245
7.7 Summary....253

**CHAPTER 8** Investigative Reconstruction with Digital Evidence....255
*Eoghan Casey and Brent E. Turvey*

8.1 Equivocal Forensic Analysis....259
8.2 Victimology....266
8.3 Crime Scene Characteristics....268
8.4 Threshold Assessments....273
8.5 Summary....282

**CHAPTER 9** *Modus Operandi*, Motive, and Technology....285
*Brent E. Turvey*

9.1 Axes to Pathological Criminals and Other Unintended Consequences....285
9.2 *Modus Operandi*....287
9.3 Technology and *Modus Operandi*....288
9.4 Motive and Technology....297
9.5 Current Technologies....303
9.6 Summary....304

**PART 3 Apprehending Offenders**

**CHAPTER 10** Violent Crime and Digital Evidence....307
*Eoghan Casey and Terrance Maguire*

10.1 The Role of Computers in Violent Crime....308
10.2 Processing the Digital Crime Scene....312
10.3 Investigative Reconstruction....316
10.4 Conclusions....321

**CHAPTER 11** Digital Evidence as Alibi....323
*Eoghan Casey*

11.1 Investigating an Alibi....324
11.2 Time as Alibi....326
11.3 Location as Alibi....327
11.4 Summary....328

**CHAPTER 12** Sex Offenders on the Internet ..................................... 329
*Eoghan Casey, Monique M. Ferraro, and Michael McGrath*

12.1 Old Behaviors, New Medium ....................................... 332
12.2 Legal Considerations .................................................... 335
12.3 Identifying and Processing Digital Evidence ............... 338
12.4 Investigating Online Sexual Offenders ........................ 341
12.5 Investigative Reconstruction ....................................... 349
12.6 Case Example: Scott Tyree .......................................... 357
12.7 Case Example: Peter Chapman ................................... 360
12.8 Summary ...................................................................... 362

**CHAPTER 13** Computer Intrusions..................................................... 369
*Eoghan Casey and Christopher Daywalt*

13.1 How Computer Intruders Operate............................... 371
13.2 Investigating Computer Intrusions .............................. 377
13.3 Forensic Preservation of Volatile Data ........................ 388
13.4 Post-Mortem Investigation of a Compromised System ..................................... 401
13.5 Investigation of Malicious Computer Programs .......... 403
13.6 Investigative Reconstruction ....................................... 406
13.7 Summary ...................................................................... 419

**CHAPTER 14** Cyberstalking................................................................ 421
*Eoghan Casey*

14.1 How Cyberstalkers Operate......................................... 423
14.2 Investigating Cyberstalking......................................... 425
14.3 Cyberstalking Case Example ....................................... 432
14.4 Summary ...................................................................... 433

## PART 4 Computers

**CHAPTER 15** Computer Basics for Digital Investigators.................. 437
*Eoghan Casey*

15.1 A Brief History of Computers....................................... 437
15.2 Basic Operation of Computers ..................................... 439
15.3 Representation of Data ................................................. 442
15.4 Storage Media and Data Hiding................................... 447
15.5 File Systems and Location of Data............................... 450

15.6 Dealing with Password Protection and Encryption ...... 458
15.7 Summary ...... 462

CHAPTER 16 Applying Forensic Science to Computers ...... 465
*Eoghan Casey*

16.1 Preparation ...... 466
16.2 Survey ...... 467
16.3 Documentation ...... 470
16.4 Preservation ...... 474
16.5 Examination and Analysis ...... 485
16.6 Reconstruction ...... 499
16.7 Reporting ...... 508
16.8 Summary ...... 510

CHAPTER 17 Digital Evidence on Windows Systems ...... 513
*Eoghan Casey*

17.1 File Systems ...... 514
17.2 Data Recovery ...... 529
17.3 Log Files ...... 535
17.4 Registry ...... 536
17.5 Internet Traces ...... 538
17.6 Program Analysis ...... 547
17.7 Summary ...... 548

CHAPTER 18 Digital Evidence on UNIX Systems ...... 551
*Eoghan Casey*

18.1 UNIX Evidence Acquisition Boot Disk ...... 552
18.2 File Systems ...... 552
18.3 Overview of Digital Evidence Processing Tools ...... 557
18.4 Data Recovery ...... 565
18.5 Log Files ...... 574
18.6 File System Traces ...... 575
18.7 Internet Traces ...... 579
18.8 Summary ...... 585

CHAPTER 19 Digital Evidence on Macintosh Systems ...... 587
*Eoghan Casey*

19.1 File Systems ...... 587
19.2 Overview of Digital Evidence Processing Tools ...... 590

19.3 Data Recovery ..... 591
19.4 File System Traces ..... 592
19.5 Internet Traces ..... 597
19.6 Summary ..... 602

**CHAPTER 20** Digital Evidence on Mobile Devices
*Eoghan Casey and Benjamin Turnbull*

This chapter appears online at http://www.elsevierdirect.com/companion.jsp?ISBN=9780123742681

## PART 5 Network Forensics

**CHAPTER 21** Network Basics for Digital Investigators ..... 607
*Eoghan Casey and Benjamin Turnbull*

21.1 A Brief History of Computer Networks ..... 608
21.2 Technical Overview of Networks ..... 609
21.3 Network Technologies ..... 613
21.4 Connecting Networks Using Internet Protocols ..... 619
21.5 Summary ..... 631

**CHAPTER 22** Applying Forensic Science to Networks ..... 633
*Eoghan Casey*

22.1 Preparation and Authorization ..... 634
22.2 Identification ..... 640
22.3 Documentation, Collection, and Preservation ..... 646
22.4 Filtering and Data Reduction ..... 651
22.5 Class/Individual Characteristics and Evaluation of Source ..... 653
22.6 Evidence Recovery ..... 657
22.7 Investigative Reconstruction ..... 659
22.8 Reporting Results ..... 667
22.9 Summary ..... 668

**CHAPTER 23** Digital Evidence on the Internet ..... 671
*Eoghan Casey*

23.1 Role of the Internet in Criminal Investigations ..... 671
23.2 Internet Services: Legitimate versus Criminal Uses ..... 672

23.3 Using the Internet as an Investigative Tool....685
23.4 Online Anonymity and Self-Protection....691
23.5 E-mail Forgery and Tracking....699
23.6 Usenet Forgery and Tracking....703
23.7 Searching and Tracking on IRC....706
23.8 Summary....711

**CHAPTER 24** Digital Evidence on Physical and Data-Link Layers....713
*Eoghan Casey*

24.1 Ethernet....714
24.2 Linking the Data-Link and Network Layers: Encapsulation....716
24.3 Ethernet versus ATM Networks....721
24.4 Documentation, Collection, and Preservation....722
24.5 Analysis Tools and Techniques....727
24.6 Summary....736

**CHAPTER 25** Digital Evidence at the Network and Transport Layers....737
*Eoghan Casey*

25.1 TCP/IP....738
25.2 Setting up a Network....750
25.3 TCP/IP-Related Digital Evidence....754
25.4 Summary....769

CASE INDEX....771

NAME INDEX....773

SUBJECT INDEX....775