Table of contents provided by Syndetics

- **List of Figures** (p. xi)
- **About the Author** (p. xiii)
- **Foreword** (p. xv)
- **Acknowledgments** (p. xvii)
- **Chapter 1 Introduction** (p. 1)
- **Chapter 2 Cybercrime Offenses** (p. 9)
- **Potential Cybercrime Offenses** (p. 11)
- **Cybercrime Case Study** (p. 26)
- **Notes** (p. 26)
- **Chapter 3 Motivations of the Attacker** (p. 29)
- **Common Motivators** (p. 30)
- **Cybercrime Case Study I** (p. 33)
- **Cybercrime Case Study II** (p. 34)
- **Note** (p. 35)
- **Chapter 4 Determining That a Cybercrime Is Being Committed** (p. 37)
- **Cyber Incident Alerts** (p. 38)
- **Attack Methodologies** (p. 41)
- **Cybercrime Case Study I** (p. 44)
- **Cybercrime Case Study II** (p. 44)
- **Notes** (p. 45)
- **Chapter 5 Commencing a Cybercrime Investigation** (p. 47)
- **Why Investigate a Cybercrime?** (p. 47)
- **The Cyber Investigator** (p. 48)
- **Management Support** (p. 48)
- **Is There a Responsibility to Try to Get the Data Back?** (p. 50)
- **Cybercrime Case Study** (p. 51)
- **Notes** (p. 52)
- **Chapter 6 Legal Considerations When Planning an Investigation** (p. 53)
- **Role of the Law in a Digital Crimes Investigation** (p. 54)
- **Protecting Digital Evidence** (p. 55)
- **Preservation of the Chain of Custody** (p. 56)
- **Protection of Evidence** (p. 59)
- **Legal Implications of Digital Evidence Collection** (p. 60)
- **Cybercrime Case Study** (p. 63)
- **Note** (p. 63)
- **Chapter 7 Initial Meeting with the Complainant** (p. 65)
- **Initial Discussion** (p. 65)
- **Complainant Details** (p. 68)
- **Event Details** (p. 68)
- **Cyber Security History** (p. 69)
- **Scene Details** (p. 70)
- **Identifying Offenses** (p. 71)
- **Identifying Witnesses** (p. 71)
- **Identifying Suspects** (p. 71)

- **Identifying the Modus Operandi of Attack** (p. 72)
- **Evidence: Technical** (p. 73)
- **Evidence: Other** (p. 74)
- **Cybercrime Case Study** (p. 74)
- **Chapter 8 Containing and Remediating the Cyber Security Incident** (p. 77)
- **Containing the Cyber Security Incident** (p. 77)
- **Eradicating the Cyber Security Incident** (p. 80)
- **Note** (p. 82)
- **Chapter 9 Challenges in Cyber Security incident Investigations** (p. 83)
- **Unique Challenges** (p. 84)
- **Cybercrime Case Study** (p. 91)
- **Chapter 10 Investigating the Cybercrime Scene** (p. 93)
- **The Investigation Team** (p. 96)
- **Resources Required** (p. 101)
- **Availability and Management of Evidence** (p. 104)
- **Technical Items** (p. 105)
- **Scene Investigation** (p. 123)
- **What Could Possibly Go Wrong?** (p. 152)
- **Cybercrime Case Study I** (p. 155)
- **Cybercrime Case Study II** (p. 156)
- **Notes** (p. 158)
- **Chapter 11 Log File Identification, Preservation, Collection, and Acquisition** (p. 159)
- **Log Challenges** (p. 160)
- **Logs as Evidence** (p. 161)
- **Types of Logs** (p. 162)
- **Cybercrime Case Study** (p. 164)
- **Notes** (p. 165)
- **Chapter 12 Identifying, Seizing, and Preserving Evidence from Cloud-Computing Platforms** (p. 167)
- **What Is Cloud Computing?** (p. 167)
- **What Is the Relevance to the Investigator?** (p. 172)
- **The Attraction of Cloud Computing for the Cybercriminal** (p. 173)
- **Where Is Your Digital Evidence Located?** (p. 174)
- **Lawful Seizure of Cloud Digital Evidence** (p. 175)
- **Preservation of Cloud Digital Evidence** (p. 177)
- **Forensic Investigations of Cloud-Computing Servers** (p. 178)
- **Remote Forensic Examinations** (p. 182)
- **Cloud Barriers to a Successful Investigation** (p. 196)
- **Suggested Tips to Assist Your Cloud-Based Investigation** (p. 203)
- **Cloud-Computing Investigation Framework** (p. 206)
- **Cybercrime Case Study** (p. 219)
- **Notes** (p. 221)
- **Chapter 13 Identifying, Seizing, and Preserving Evidence from Internet of Things Devices** (p. 225)
- **What Is the Internet of Things?** (p. 225)

- **What Is the Relevance to Your Investigation?** (p. 226)
- **Where Is Your Internet of Things Digital Evidence Located?** (p. 228)
- **Lawful Seizure of Internet of Things Evidence** (p. 228)
- **Notes** (p. 229)
- **Chapter 14 Open Source Evidence** (p. 231)
- **The Value of Open Source Evidence** (p. 231)
- **Examples of Open Source Evidence** (p. 233)
- **Note** (p. 236)
- **Chapter 15 The Dark Web** (p. 237)
- **Crime and the Dark Web** (p. 238)
- **Notes** (p. 242)
- **Chapter 16 Interviewing Witnesses and Suspects** (p. 243)
- **Suspect Interviews** (p. 245)
- **Witness Interviews** (p. 246)
- **Preparing for an Interview** (p. 247)
- **The Interview Process** (p. 250)
- **Closing the Interview** (p. 254)
- **Review of the Interview** (p. 254)
- **Preparation of Brief for Referral to Police** (p. 255)
- **Chapter 17 Review of Evidence** (p. 257)
- **Chapter 18 Producing Evidence for Court** (p. 265)
- **Digital Evidence and Its Admissibility** (p. 267)
- **Preparing for Court** (p. 268)
- **Chapter 19 Conclusion** (p. 273)
- **Glossary** (p. 277)
- **Index** (p. 283)