Table of Contents

About the Author xiii

About the Technical Reviewer xv

Acknowledgments xvii

Introduction xix

Chapter 1: Introduction: Understanding Digital Forensics 1

What Is Digital Forensics? 2

Digital Forensics Goals 3

Cybercrime 4

Cybercrime Attack Mode 4

How Are Computers Used in Cybercrimes? 5

Example of Cybercrime 5

Digital Forensics Categories 9

Computer Forensics 9

Mobile Forensics 10

Network Forensics 10

Database Forensics 10

Forensics Data Analysis 10

Digital Forensics Users 11

Law Enforcement 11

Civil Ligation 11

Intelligence and Counterintelligence 12

Digital Forensics Investigation Types 13

Forensics Readiness 14

The Importance of Forensic Readiness for Organizations 14

Digital Evidence 16

Digital Evidence Types 17

Locations of Electronic Evidence 20

Challenge of Acquiring Digital Evidence 21

Who Should Collect Digital Evidence? 23

Chain of Custody 24

Digital Forensics Examination Process 26

Seizure 26

Acquisition 27

Analysis 28

Reporting 29

Digital Forensics Process Official Guides 29

Digital Forensics Certifications 30

Digital Forensics vs. Other Computing Domain 32

Chapter Summary 33

Chapter 2: Essential Technical Concepts 35

Data Representation 35

Decimal (Base-10) 35

Binary 36

Hexadecimal (Base-16) 37

Computer Character Encoding Schema 40

File Structure 41

Digital File Metadata 43

Timestamps Decoder (Tool) 46

Hash Analysis 47

How to Calculate File Hash 47

Memory Types 48

Volatile Memory 48

Nonvolatile Memory 48

Types of Computer Storage 48
Primary Storage 49
Secondary Storage 51
HPA and DCO 55
Data Recovery Considerations 58
File Systems 58
NTFS 58
FAT 59
Computing Environment 59
Personal Computing Environment 60
Client Server Computing Environment 60
Distributed Computing Environment 60
Cloud Computing 60
Windows Version Variations 62
IP Address 63
What Is an IP Address? 63
Digital Forensics Resources and Study Materials 65
Chapter Summary 66
Chapter 3: Computer Forensics Lab Requirements 69
Lab Physical Facility Requirements 71
Environment Controls 73
Hardware Equipment 74
Furniture and Consumable Materials 76
Evidence Container 76
Forensic Workstation 77
Commercial Ready-Made Digital Forensic Workstation 79
Forensic Software 79
Commercial Forensics Tools 79
Free and Open Source Forensic Tools 80

Linux Distribution for Digital Forensics ... 81

Virtualization Technology ... 81

Laboratory Information Management System (LIMS) ... 81

Other Software ... 82

Validation and Verification of Forensics Hardware and Software ... 82

Lab Manager ... 83

Secrecy Requirements ... 84

Lab Data Backup ... 84

Training Requirements ... 85

Lab Policies and Procedures ... 86

Documentation ... 87

Lab Accreditation Requirements ... 87

Step 1: Self-Assessment ... 88

Step 2: Identifying the Current Level of Conformance to the Target Accreditation Standards ... 89

Step 3: Closing the Gap ... 89

Step 4: Implementation ... 89

Step 5: Conformance to Standards Documentation ... 90

Chapter Summary ... 90

Chapter 4: Initial Response and First Responder Tasks ... 93

Search and Seizure ... 94

Consent to Search ... 95

Subpoena ... 97

Search Warrant ... 97

First Responder Toolkit ... 98

First Responder Tasks ... 99

Order of Volatility ... 104

Documenting the Digital Crime Scene ... 105

Packaging and Transporting Electronic Devices ... 106

Conducting Interview 107
First Responder Questions When Contacted by a Client 107
Witness Interview Questions 108
Witness Signature 109
Chapter Summary 109
Chapter 5: Acquiring Digital Evidence 111
Forensic Image File Format 112
Raw Format 112
AFF 112
Expert Witness (EnCase) 113
Other File Formats 113
Forensics Image File Validation 113
Acquiring Volatile Memory (Live Acquisition) 114
Virtual Memory (Swap Space) 115
The Challenges of Acquiring RAM Memory 116
Capturing RAM Using the DumpIt Tool 118
Belkasoft Live RAM Capturer 120
Capture RAM with Magnet 121
Capture RAM with FTK Imager 121
Acquiring Nonvolatile Memory (Static Acquisition) 124
Hard Drive Acquisition Methods 125
Using FTK Imager to Capture Hard Drive 128
Hard Drive Imaging Risks and Challenges 135
NAS 136
Encrypted Hard Drive 136
Corrupted or Physically Damaged Hard Drive 136
Cloud Data Acquisition 137
Network Acquisition 137
Forensic Tool Limitations 138
Other Challenges 138
Chapter Summary 139

Chapter 6: Analyzing Digital Evidence..141

Analyzing Hard Drive Forensic Images..141

Arsenal Image Mounter..142

OSFMount..143

Autopsy..145

Analyzing RAM Forensic Image..162

Redline..162

Volatility Framework..173

Chapter Summary..177

Chapter 7: Windows Forensics Analysis..179

Timeline Analysis..181

Creating a Timeline Using Autopsy..181

Generate a Timeline Report Using Autopsy..183

File Recovery..186

Undeleting Files Using Autopsy..187

Windows Recycle Bin Forensics..187

Data Carving..193

Attributing an Action to Its Associated User Account..194

Windows Registry Analysis..194

Architecture of Windows Registry..194

Acquiring Windows Registry..197

Registry Examination..198

Deleted Registry Key Recovery..212

File Format Identification..214

Windows Features Forensics Analysis..217

Windows Prefetch Analysis..217

Windows Thumbnail Forensics..219

Jump Lists Forensics..220

LNK File Forensics..223

Event Log Analysis... 226

Hidden Hard Drive Partition Analysis.. 230

Windows Minidump File Forensics.. 232

Pagefile.sys, Hiberfil.sys, and Swapfile.sys.. 234

Windows Volume Shadow Copies Forensics.. 236

Windows 10 Forensics.. 239

Windows 10 Features Forensics... 240

Chapter Summary... 245

Chapter 8: Web Browser and E-mail Forensics 247

Web Browser Forensics... 248

IE... 248

Microsoft Edge Web Browser.. 251

Firefox.. 253

Google Chrome.. 257

History.. 259

Cookies.. 262

Top Sites.. 262

Shortcuts.. 262

Login Data... 262

Web Data... 263

Bookmarks.. 263

Bookmarks.bak.. 264

Cache Folder... 264

Other Web Browser Investigation Tools.. 265

E-mail Forensics... 267

Steps in E-mail Communications... 268

List of E-mail Protocols... 269

E-mail Header Examination.. 270

Chapter Summary.. 289

Chapter 9: Antiforensics Techniques....................................291
Users of Antiforensics Techniques....................................292
Classification of Antiforensics Techniques....................................292
Digital Steganography....................................293
Data Destruction and Antirecovery Techniques....................................299
Encryption Techniques....................................303
Cryptographic Anonymity Techniques....................................308
Direct Attacks Against Computer Forensics Tools....................................309
Chapter Summary....................................310
Chapter 10: Gathering Evidence from OSINT Sources....................................311
Goals of OSINT Collection....................................312
OSINF Categories....................................313
OSINT Benefits....................................315
Challenges of OSINT....................................316
The OSINT Cycle....................................317
OSINT Gathering and the Need for Privacy....................................318
OSINT and the Darknet....................................319
Internet Layers....................................319
Online Resources....................................321
Chapter Summary....................................322
Chapter 11: Digital Forensics Report....................................323
Report Main Elements....................................323
Autogenerated Report....................................324
Chapter Summary....................................326
Index....................................327