Table of Contents

Preface

Section 1: Acquiring Evidence

1

Types of Computer-Based Investigations

Differences in computer-based investigations 4
Criminal investigations 6
First responders 6
Corporate investigations 18
Employee misconduct 19
Corporate espionage 22
Insider threat 27
Summary 29
Questions 30
Further reading 31

2

The Forensic Analysis Process

Pre-investigation considerations 34
The forensic workstation 35
The response kit 36
Forensic software 40
Forensic investigator training 43
Understanding case information and legal issues 44
Understanding data acquisition 47
Chain of custody 49
Understanding the analysis process 53
Dates and time zones 54
Hash analysis 54
File signature analysis 57
Antivirus 59
Reporting your findings 63
Details to include in your report 63
Document facts and circumstances 65
The report conclusion 66

Summary 67
Questions 68
Further reading 69

3

Acquisition of Evidence

Exploring evidence 72
Understanding the forensic examination environment 75
Tool validation 76
Creating sterile media 81
Understanding write blocking 86
Defining forensic imaging 89
DD image 90
EnCase evidence file 91
SSD device 92
Imaging tools 93
Summary 106
Questions 107
Further reading 108

4

Computer Systems

Understanding the boot process 110
Forensic boot media 112
Hard drives 115
MBR (Master Boot Record) partitions 117
GPT partitions 121
Host Protected Area (HPA) and Device Configuration Overlays (DCO) 125
Understanding filesystems 126
The FAT filesystem 126
Data area 131
Long filenames 134
Recovering deleted files 134
Slack space 137
Understanding the NTFS filesystem 137
Summary 149
Questions 149
Further reading 150

Section 2: Investigation

5

Computer Investigation Process

Timeline analysis 154
X-Ways 156
Media analysis 172
String search 174

Recovering deleted data 176
Summary 179
Questions 179
Further reading 181

6
Windows Artifact Analysis

Understanding user profiles 184
Understanding Windows Registry 186
Determining account usage 189
Last login/last password change 189
Determining file knowledge 195
Exploring the thumbcache 195
Exploring Microsoft browsers 198
Determining most recently used/ recently used 199
Looking into the Recycle Bin 202
Understanding shortcut (LNK) files 203
Deciphering JumpLists 204
Opening shellbags 206
Understanding prefetch 207
Identifying physical locations 209
Determining time zones 209
Exploring network history 210
Understanding the WLAN event log 211
Exploring program execution 213
Determining UserAssist 213
Exploring Shimcache 214
Understanding USB/attached devices 215
Summary 218
Questions 218
Further reading 219

7
RAM Memory Forensic Analysis

Fundamentals of memory 222
Random access memory? 223
Identifying sources of memory 225
Capturing RAM 227
Preparing the capturing device 227
Exploring RAM capture tools 228
Exploring RAM analyzing tools 232
Using Bulk Extractor 232
Summary 240
Questions 240
Further reading 241

8
Email Forensics – Investigation Techniques

Understanding email protocols 244
Understanding SMTP – Simple Mail Transfer Protocol 244
Understanding the Post Office Protocol 245
IMAP – Internet Message Access Protocol 246
Understanding web-based email 247
Decoding email 247
Understanding the email message format 248
Email attachments 252
Understanding client-based email analysis 252
Exploring Microsoft Outlook/Outlook Express 253
Exploring Microsoft Windows Live Mail 253
Mozilla Thunderbird 254
Understanding WebMail analysis 256
Summary 259
Questions 260
Further reading 261

9
Internet Artifacts

Understanding browsers 264
Exploring Google Chrome 264
Exploring Internet Explorer/Microsoft Edge 271
Exploring Firefox 279
Social media 286
Facebook 288
Twitter 290
Service provider 291
Peer-to-Peer file sharing 291
Ares 292
eMule 293
Shareaza 296
Cloud computing 297
Summary 300
Questions 301
Further reading 302

Section 3: Reporting

10
Report Writing

Effective note taking 305
Writing the report 307
Evidence analyzed 310
Acquisition details 311
Analysis details 312

Exhibits/technical details 313
Summary 315
Questions 315
Further reading 316

11
Expert Witness Ethics

Understanding the types of proceedings 318
Beginning the preparation phase 320
Understanding the curriculum vitae 321
Understanding testimony and evidence 324
Understanding the importance of ethical behavior 326
Summary 329
Questions 330
Further reading 331

Assessments

Chapter 01 333
Chapter 02 333
Chapter 03 334
Chapter 04 334
Chapter 05 334
Chapter 06 335
Chapter 07 335
Chapter 08 335
Chapter 09 336
Chapter 10 336
Chapter 11 336

Other Books You May Enjoy

Index