Preface
Who this book is for
What this book covers
Get in touch
Types of Computer-Based Investigations
Introduction to computer-based investigations
Criminal investigations
First responders
Investigators
Crime scene technician
Illicit images
The crime of stalking
Criminal conspiracy
Corporate investigations
Employee misconduct
Corporate espionage
Security
Threat Actors
Social engineering
Real-world experience
Insider threat
Case studies
Dennis Rader
Silk Road
San Bernardino terror attack
Theft of intellectual property
Summary
Questions
Further reading
The Forensic Analysis Process
Pre-investigation considerations
The forensic workstation
The response kit
Forensic software
Forensic investigator training
Understanding case information and legal issues
Understanding data acquisition
Chain of custody
Understanding the analysis process
Dates and time zones
Hash analysis
File signature analysis
Antivirus
Reporting your findings
Details to include in your report
Document facts and circumstances
The report conclusion
Summary

Questions
Further reading
Acquisition of Evidence
Exploring evidence
Understanding the forensic examination environment
Tool validation
Creating sterile media
Understanding write blocking
Hardware write blocker
Software write blocker
Defining forensic imaging
DD image
EnCase evidence file
SSD device
Imaging tools
FTK Imager
PALADIN
Summary
Questions
Further reading
Computer Systems
Understanding the boot process
Forensic boot media
Creating a bootable forensic device
Hard drives
Drive geometry
MBR (Master Boot Record) partitions
Extended partitions
GPT partitions
Host Protected Area (HPA) and Device Configuration Overlay (DCO)
Understanding filesystems
The FAT filesystem
Boot record
File allocation table
Data area
Long filenames
Recovering deleted files
Slack space
Understanding the NTFS filesystem
Summary
Questions
Further reading
Computer Investigation Process
Timeline analysis
X-Ways
Plaso (Plaso Langar AÃ° Safna Ã– Ilu)
Media analysis
String search

Recovering deleted data
Summary
Questions
Further reading
Exercise
Data set
Software needed
Email exercise
Data carving exercise
Windows Artifact Analysis
Understanding user profiles
Understanding Windows Registry
Determining account usage
Last login/last password change
Determining file knowledge
Exploring the thumbcache
Exploring Microsoft browsers
Determining most recently used/recently used
Looking into the Recycle Bin
Understanding shortcut (LNK) files
Deciphering JumpLists
Opening shellbags
Understanding prefetch
Identifying physical locations
Determining time zones
Exploring network history
Understanding the WLAN event log
Exploring program execution
Determining UserAssist
Exploring the Shimcache
Understanding USB/attached devices
Summary
Questions
Further reading
Exercise
Data set
Software needed
Scenario
RAM Memory Forensic Analysis
Fundamentals of memory
Random access memory?
Identifying sources of memory
Capturing RAM
Preparing the capturing device
Exploring RAM capture tools
Using DumpIt
Using FTK Imager
Exploring RAM analyzing tools

Using Bulk Extractor
Using VOLIX II
Summary
Questions
Further reading
Email Forensics â€“ Investigation Techniques
Understanding email protocols
Understanding SMTP â€“ Simple Mail Transfer Protocol
Understanding the Post Office Protocol
IMAP â€“ Internet Message Access Protocol
Understanding web-based email
Decoding email
Understanding the email message format
Email attachments
Understanding client-based email analysis
Exploring Microsoft Outlook/Outlook Express
Exploring Microsoft Windows Live Mail
Mozilla Thunderbird
Understanding WebMail analysis
Summary
Questions
Further reading
Exercise
Data set
Software needed
Scenario
Interviews
Email accounts
Question to answer
Internet Artifacts
Understanding browsers
Exploring Google Chrome
Understanding bookmarks
Understanding the Chrome history file
Cookies
Cache
Passwords
Exploring Internet Explorer/Microsoft Edge (Old Version)
Bookmarks
IE history
Typed URL
Cache
Cookies
Exploring Firefox
Profiles
Cache
Cookies
History

Passwords
Bookmarks
Social media
Facebook
Twitter
Service provider
P2P file sharing
Ares
eMule
Shareaza
Cloud computing
Summary
Questions
Further reading
Online Investigations
Undercover investigations
Undercover platform
Online persona
Background searches
Preserving online communications
Summary
Questions
Further reading
Networking Basics
The Open Source Interconnection (OSI) model
Physical (Layer 1)
Data link (Layer 2)
Network (Layer 3)
Transport (Layer 4)
Session (Layer 5)
Presentation (Layer 6)
Application (Layer 7)
Encapsulation
TCP/IP
IPv4
Port numbers
IPv6
Application layer protocols
Transport layer protocols
Internet layer protocols
Summary
Questions
Further reading
Report Writing
Effective note taking
Writing the report
Evidence analyzed
Acquisition details

Analysis details
Exhibits/technical details
Summary
Questions
Further reading
Expert Witness Ethics
Understanding the types of proceedings
Beginning the preparation phase
Understanding the curriculum vitae
Understanding testimony and evidence
Understanding the importance of ethical behavior
Summary
Questions
Further reading
Assessments
Chapter 01
Chapter 02
Chapter 03
Chapter 04
Chapter 05
Chapter 06
Chapter 07
Chapter 08
Chapter 09
Chapter 10
Chapter 11
Chapter 12
Chapter 13
Other Books You May Enjoy
Index