

Digital Forensics, Investigation, and Response

FOURTH EDITION

Chuck Easttom



JONES & BARTLETT
LEARNING



World Headquarters

Jones & Bartlett Learning
25 Mall Road, 6th Floor
Burlington, MA 01803
978-443-5000
info@jblearning.com
www.jblearning.com

Jones & Bartlett Learning books and products are available through most bookstores and online booksellers. To contact Jones & Bartlett Learning directly, call 800-832-0034, fax 978-443-8000, or visit our website, www.jblearning.com.

Substantial discounts on bulk quantities of Jones & Bartlett Learning publications are available to corporations, professional associations, and other qualified organizations. For details and specific discount information, contact the special sales department at Jones & Bartlett Learning via the above contact information or send an email to specialsales@jblearning.com.

Copyright © 2022 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the copyright owner.

The content, statements, views, and opinions herein are the sole expression of the respective authors and not that of Jones & Bartlett Learning, LLC. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement or recommendation by Jones & Bartlett Learning, LLC and such reference shall not be used for advertising or product endorsement purposes. All trademarks displayed are the trademarks of the parties noted herein. *Digital Forensics, Investigation, and Response, Fourth Edition* is an independent publication and has not been authorized, sponsored, or otherwise approved by the owners of the trademarks or service marks referenced in this product.

There may be images in this book that feature models; these models do not necessarily endorse, represent, or participate in the activities represented in the images. Any screenshots in this product are for educational and instructive purposes only. Any individuals and scenarios featured in the case studies throughout this product may be real or fictitious but are used for instructional purposes only.

24449-6

Production Credits

VP, Product Management: Christine Emerton
Director of Product Management: Laura Pagluica
Product Manager: Ned Hinman
Tech Editor: Jeffrey Parker
Content Strategist: Melissa Duffy
Content Strategist: Paula Gregory
Project Manager: Kristen Rogers
Senior Project Specialist: Dan Stone
Digital Project Specialist: Rachel DiMaggio
Marketing Manager: Suzy Balk
Product Fulfillment Manager: Wendy Kilborn

Composition: Straive
Cover Design: Briana Yates
Text Design: Kristin E. Parker
Content Services Manager: Colleen Lamy
Media Development Editor: Faith Brosnan
Rights & Permissions Manager: John Rusk
Rights Specialist: Benjamin Roy
Cover Image (Title Page, Part Opener, Chapter Opener):
© phyZick/Shutterstock
Printing and Binding: McNaughton & Gunn

Library of Congress Cataloging-in-Publication Data

Names: Easttom, Chuck, author.

Title: Digital forensics, investigation, and response / Chuck Easttom.

Other titles: System forensics, investigation, and response

Description: Fourth edition. | Burlington, Massachusetts : Jones & Bartlett Learning, [2022] | Includes index.

Identifiers: LCCN 2021003216 | ISBN 9781284226065 (paperback)

Subjects: LCSH: Computer crimes—Investigation—Textbooks.

Classification: LCC HV8079.C65 E37 2022 | DDC 363.25/968--dc23

LC record available at <https://lccn.loc.gov/20210032166048>

Printed in the United States of America

25 24 23 22 21 10 9 8 7 6 5 4 3 2 1

Contents

Preface	xv
Dedication	xvii
About the Author	xix

PART I **Introduction to Forensics** **1**

CHAPTER 1

Introduction to Forensics **3**

What Is Computer Forensics? **4**

Using Scientific Knowledge	5
Collecting	6
Analyzing	6
Presenting	6

Understanding the Field of Digital Forensics **10**

What Is Digital Evidence?	11
Scope-Related Challenges to System Forensics	12
Types of Digital System Forensics Analysis	15
General Guidelines	16

Knowledge Needed for Computer Forensics Analysis **17**

Hardware	17
Software	20
Networks	22
Addresses	23
Obscured Information and Anti-Forensics	26

The Daubert Standard **28**

U.S. Laws Affecting Digital Forensics **29**

The Federal Privacy Act of 1974	29
The Privacy Protection Act of 1980	29
The Communications Assistance to Law Enforcement Act of 1994	29
Unlawful Access to Stored Communications: 18 U.S.C. § 2701	29
The Electronic Communications Privacy Act of 1986	30
The Computer Security Act of 1987	30
The Foreign Intelligence Surveillance Act of 1978	30
The Child Protection and Sexual Predator Punishment Act of 1998	30
The Children's Online Privacy Protection Act of 1998	30
The Communications Decency Act of 1996	31
The Telecommunications Act of 1996	31
The Wireless Communications and Public Safety Act of 1999	31

The USA PATRIOT Act	31
The Sarbanes-Oxley Act of 2002	31
18 USC 1030 Fraud and Related Activity in Connection with Computers	31
18 USC 1020 Fraud and Related Activity in Connection with Access Devices	31
The Digital Millennium Copyright Act (DMCA)	31
18 USC § 1028A Identity Theft and Aggravated Identity Theft	32
18 USC § 2251 Sexual Exploitation of Children	32
Warrants	32

Federal Guidelines 33

The FBI	33
The Secret Service	34
The Regional Computer Forensics Laboratory Program	35

CHAPTER SUMMARY 35

KEY CONCEPTS AND TERMS 35

CHAPTER 1 ASSESSMENT 36

REFERENCES 36

CHAPTER 2

Overview of Computer Crime 39

How Computer Crime Affects Forensics 40

Identity Theft 41

Phishing	42
Spyware	43
Discarded Information	44
How Does This Crime Affect Forensics?	45

Hacking 45

Structured Query Language Injection	45
Cross-Site Scripting	47
Ophcrack	48
Tricking Tech Support	50
Hacking in General	50

Cyberstalking and Harassment 51

Real Cyberstalking Cases	52
--------------------------	----

Fraud 54

Investment Offers	54
Data Piracy	55

Non-Access Computer Crimes 55

Denial of Service	56
Viruses	58
Logic Bombs	60

Cyberterrorism 61

How Does This Crime Affect Forensics?	62
---------------------------------------	----

CHAPTER SUMMARY 62

KEY CONCEPTS AND TERMS 63**CHAPTER 2 ASSESSMENT 63****CHAPTER 3****Forensic Methods and Labs 65****Forensic Methodologies 66**

Handle Original Data as Little as Possible	66
Comply with the Rules of Evidence	66
Avoid Exceeding Your Knowledge	68
Create an Analysis Plan	69
Technical Information Collection Considerations	70

Formal Forensic Approaches 71

DoD Forensic Standards	71
The DFRWS Framework	71
The SWGDE Framework	72
An Event-Based Digital Forensics Investigation Framework	72

Documentation of Methodologies and Findings 72

Disk Structure	73
File Slack Searching	73

Evidence-Handling Tasks 73

Evidence-Gathering Measures	74
Expert Reports	74

How to Set Up a Forensics Lab 75

Equipment	75
Security	75
American Society of Crime Laboratory Directors	76

Common Forensic Software Programs 77

EnCase	77
Forensic Toolkit	80
OSForensics	81
Helix	81
Kali Linux	81
AnaDisk Disk Analysis Tool	82
CopyQM Plus Disk Duplication Software	82
The Sleuth Kit	82
Disk Investigator	83

Forensic Certifications 83

EnCase Certified Examiner Certification	85
AccessData Certified Examiner	85
OSForensics	85
EC Council Certified Hacking Forensic Investigator	85
GIAC Certifications	85

CHAPTER SUMMARY 86

KEY CONCEPTS AND TERMS	86
CHAPTER 3 ASSESSMENT	86
REFERENCES	87

PART II **Forensics Tools, Techniques, and Methods** **89**

CHAPTER 4

Collecting, Seizing, and Protecting Evidence **91**

Proper Procedure **92**

Shutting Down the Computer	92
Transporting the Computer System to a Secure Location	95
Preparing the System	95
Documenting the Hardware Configuration of the System	98
Mathematically Authenticating Data on All Storage Devices	98

Handling Evidence **99**

Collecting Data	99
Documenting Filenames, Dates, and Times	100
Identifying File, Program, and Storage Anomalies	100
Evidence-Gathering Measures	101
What to Examine	102

Storage Formats **105**

Magnetic Media	105
Solid-State Drives	106
Digital Audio Tape Drives	107
Digital Linear Tape and Super DLT	107
Optical Media	107
Using USB Drives	108
File Formats	108

Forensic Imaging **109**

Imaging with EnCase	110
Imaging with the Forensic Toolkit	112
Imaging with OSForensics	115

RAID Acquisitions **116**

CHAPTER SUMMARY **117**

KEY CONCEPTS AND TERMS **117**

CHAPTER 4 ASSESSMENT **118**

CHAPTER LAB **118**

CHAPTER 5

Understanding Techniques for Hiding and Scrambling Information **119**

Steganography **120**

Historical Steganography	122
Steganophony	122

Video Steganography	122
More Advanced Steganography	122
Steganalysis	123
Invisible Secrets	124
MP3Stego	127
Deep Sound	127
Additional Resources	127
Encryption	128
The History of Encryption	128
Modern Cryptography	135
Breaking Encryption	143
Quantum Computing and Cryptography	146
CHAPTER SUMMARY	147
KEY CONCEPTS AND TERMS	147
CHAPTER 5 ASSESSMENT	148
REFERENCES	149

CHAPTER 6**Recovering Data 151****Undeleting Data 151**

File Systems and Hard Drives	152
Windows	152
Forensically Scrubbing a File or Folder	155
Linux	162
Mac OS	165

Recovering Information from Damaged Media 166

Physical Damage Recovery Techniques	167
Recovering Data After Logical Damage	167

File Carving 169**CHAPTER SUMMARY 170****KEY CONCEPTS AND TERMS 170****CHAPTER 6 ASSESSMENT 170****REFERENCES 171****CHAPTER 7****Incident Response 173****Disaster Recovery 174**

ISO 27001	175
NIST 800-34	175
NFPA 1600	176

Business Impact Analysis 176**Describing the Incident 178**

Common Vulnerability Scoring System	178
DREAD	180

RMON	180
Mean Squared Deviation	181
Mean Percentage Error	181
Ishikawa Diagram	181
The Recovery Plan	182
The Post Recovery Follow-Up	183
Incident Response	183
Detection	184
Containment	184
Eradication	184
Recovery	185
Follow-Up	185
Preserving Evidence	186
Adding Forensics to Incident Response	187
Forensic Resources	187
Forensics and Policy	188
CHAPTER SUMMARY	188
KEY CONCEPTS AND TERMS	188
CHAPTER 7 ASSESSMENT	189
REFERENCE	189

PART III**Branches of Digital Forensics 191****CHAPTER 8****Windows Forensics 193****Windows Details 194**

Windows History	194
64-Bit Processing	196
The Boot Process	196
Important Files	197

Volatile Data 199

Tools	200
-------	-----

Windows Swap File 204**Volume Shadow Copy 204****Windows Logs 204****Windows Directories 206**

UserAssist	206
Unallocated/Slack Space	206
Alternate Data Streams	207

Index.dat 208

Windows Files and Permissions 209

MAC 209

The Registry 210

USB Information 212

Wireless Networks 212

Tracking Word Documents in the Registry 213

Malware in the Registry 213

Uninstalled Software 213

Passwords 214

ShellBag 214

Shimcache 215

Amcache 215

Prefetch 216

SRUM 217

BAM and DAM 217

Recycle Bin 217**The \$I30 Attribute 218****PowerShell Forensics 219****CHAPTER SUMMARY 221****KEY CONCEPTS AND TERMS 221****CHAPTER 8 ASSESSMENT 221****REFERENCES 222****CHAPTER 9****Linux Forensics 223****Linux and Forensics 224****Linux Basics 224**

Linux History 224

Linux Shells 225

Graphical User Interface 228

Linux Boot Process 229

Logical Volume Management 231

Linux Distributions 232

Linux File Systems 232

Ext 232

The Reiser File System 233

The Berkeley Fast File System 233

Linux Logs 233

The /var/log/faillog Log 233

The /var/log/kern.log Log 233

The /var/log/lpr.log Log 233

The /var/log/mail.* Log 234

The /var/log/mysql.* Log 234

The /var/log/apache2/* Log	234
The /var/log/lighttpd/* Log	234
The /var/log/appport.log Log	234
Other Logs	235
Viewing Logs	235

Linux Directories 235

The /root Directory	235
The /bin Directory	235
The /sbin Directory	236
The /etc Folder	236
The /etc/inittab File	236
The /dev Directory	237
The /mnt Directory	237
The /boot Directory	237
The /usr Directory	237
The /tmp Directory	237
The /var Directory	237
The /proc Directory	238
The /run Directory	238

Tmpfs 239

Shell Commands for Forensics 239

The dmesg Command	239
The fsck Command	239
The grep Command	240
The history Command	241
The mount Command	241
The ps Command	241
The pstree Command	242
The pgrep Command	242
The top Command	242
The kill Command	243
The file Command	243
The su Command	243
The who Command	243
The finger Command	244
The dd Command	244
The ls Command	244
Find Executables	244
Checking Scheduled Tasks	244
Finding Oddities	245

Can You Undelete in Linux? 245

Manual Method	245
---------------	-----

Kali Linux Forensics 246

Forensics Tools for Linux 250

More Linux Forensics	250
Documenting	251
Advanced Commands	251
CHAPTER SUMMARY	251
KEY CONCEPTS AND TERMS	252
CHAPTER 9 ASSESSMENT	252
REFERENCE	252

CHAPTER 10**Mac OS Forensics 253****Mac Basics 254**

Apple History	254
Mac File Systems	257
Partition Types	259
Boot Camp Assistant	259

Mac OS Logs 260

The /var/log Log	260
The /var/spool/cups Folder	260
The /private/var/audit Logs	260
The /private/var/VM Folder	260
The /Library/Receipts Folder	260
/Library/Mobile Documents	261
The /Users/<user>/bash_history Log	261
The var/vm Folder	261
The /Users/ Directory	261
The /Users/<user>/Library/Preferences Folder	261

Directories 261

The /Volumes Directory	261
The /Users Directory	262
The /Applications Directory	262
The /Network Directory	262
The /etc Directory	262
The /Library/Preferences/SystemConfiguration/dom.apple.preferences.plist File	262

Mac OS Forensic Techniques 262

Target Disk Mode	262
Searching Virtual Memory	263
Shell Commands	263

How to Examine an Apple Device 264**MacQuisition 264**

Reading Apple Drives	265
----------------------	-----

Can You Undelete in Mac OS? 266**Mac OS Password Recovery 268**

CHAPTER SUMMARY	270
KEY CONCEPTS AND TERMS	270
CHAPTER 10 ASSESSMENT	270

CHAPTER 11**Email Forensics 271****How Email Works 272**

Email Protocols 273

Faking Email 274

Email Headers 275

Getting Headers in Outlook 2019 276

Getting Headers from Yahoo! Email 277

Getting Headers from Gmail 279

Other Email Clients 280

Email Files 281

Paraben's Email Examiner 282

ReadPST 283

Tracing Email 284**Email Server Forensics 284****Email and the Law 285**

The Fourth Amendment to the U.S. Constitution 285

The Electronic Communications Privacy Act 285

The CAN-SPAM Act 286

18 U.S.C. 2252B 287

The Communication Assistance to Law Enforcement Act 287

The Foreign Intelligence Surveillance Act 287

The USA PATRIOT Act 288

CHAPTER SUMMARY 288**KEY CONCEPTS AND TERMS 288****CHAPTER 11 ASSESSMENT 289****CHAPTER 12****Mobile Forensics 291****Cellular Device Concepts 292**

Terms 292

Networks 293

Operating Systems 294

Evidence You Can Get from a Cell Phone 304

SWGDE Guidelines 305

Types of Investigations 306

Types of Information 306

Seizing Evidence from a Mobile Device 306

SQLite 308

The iPhone 309

CHAPTER SUMMARY	311
KEY CONCEPTS AND TERMS	311
CHAPTER 12 ASSESSMENT	312
REFERENCES	312

CHAPTER 13**Network Forensics 313****Network Basics 313**

IP Addresses and MAC Addresses	314
Open Systems Interconnection Model	318

Network Packet Analysis 321

Network Packets	321
Packet Headers	321
Network Attacks	325

Network Traffic Analysis Tools 328

Wireshark	328
Nmap	331
Tcpdump	331
Snort	332
NetWitness	332

Network Traffic Analysis 332

Using Log Files as Evidence	332
-----------------------------	-----

Wireless 333

Wi-Fi Security	334
Other Wireless Protocols	335

Router Forensics 336

Router Basics	336
Types of Router Attacks	338
Getting Evidence from the Router	338

Firewall Forensics 340

Firewall Basics	340
Packet Filter	340
Stateful Packet Inspection	340
Collecting Data	340

CHAPTER SUMMARY 341**KEY CONCEPTS AND TERMS 341****CHAPTER 13 ASSESSMENT 342****CHAPTER 14****Memory Forensics 343****How Computer Memory Works 344**

Stack Versus Heap	344
Paging	345

	Capturing Memory	345
	Analyzing Memory with Volatility	347
	Analyzing Memory with OSForensics	352
	Understanding the Output	352
	Putting It All Together	354
	Malware Techniques	355
	Viruses	355
	Worms	356
	Spyware	356
	Logic Bomb	356
	Trojan Horse	356
	Malware Hiding Techniques	357
	Density Scout	358
	CHAPTER SUMMARY	360
	KEY CONCEPTS AND TERMS	360
	CHAPTER 14 ASSESSMENT	360
CHAPTER 15	Trends and Future Directions	361
	Technical Trends	362
	What Impact Does This Have on Forensics?	363
	Software as a Service	363
	The Cloud	364
	New Devices	367
	Legal and Procedural Trends	371
	Changes in the Law	372
	Private Labs	372
	International Issues	373
	Techniques	373
	CHAPTER SUMMARY	373
	KEY CONCEPTS AND TERMS	373
	CHAPTER 15 ASSESSMENT	374
	REFERENCES	374
APPENDIX A	Answer Key	375
APPENDIX B	Standard Acronyms	377
	Glossary of Key Terms	381
	Index	387

Preface

Purpose of This Book

This book is part of the *Information Systems Security & Assurance Series* from Jones & Bartlett Learning (www.jblearning.com). Designed for courses and curriculums in IT Security, Cybersecurity, Information Assurance, and Information Systems Security, this series features a comprehensive, consistent treatment of the most current thinking and trends in this critical subject area. These titles deliver fundamental information security principles packed with real-world applications and examples. Authored by Certified Information Systems Security Professionals, they deliver comprehensive information on all aspects of information security. Reviewed word-for-word by leading technical experts in the field, these books are not just current, but forward-thinking—putting you in the position to solve the cybersecurity challenges not just of today, but of tomorrow as well.

Computer crimes call for forensics specialists—people who know how to find and follow the evidence. But even aside from criminal investigations, incident response requires forensic skills. This book begins by examining the fundamentals of system forensics: what forensics is, an overview of computer crime, the challenges of system forensics, and forensic methods and labs. The second part of this book addresses the tools, techniques, and methods used to perform computer forensics and investigation. These include collecting evidence, investigating information hiding, recovering data, and scrutinizing email. It also discusses how to perform forensics in the Windows, Linux, and Macintosh operating systems; on mobile devices; and on networks. Finally, the third part explores incident and intrusion response, emerging technologies and future directions of this field, and additional system forensics resources.

New to This Edition

All aspects of the book have been updated, to include recent changes in Windows, Macintosh, and mobile devices. For example, Chapter 8, “Windows Forensics” has been expanded to include SRUM, BAM, and DAM registry entries. The updates to all chapters include changes to the underlying technology, changes to the law, and newer case studies. There is now a separate chapter regarding memory forensics, Chapter 14. Chapter 15, “New Trends,” introduces a general methodology of smart TV forensics.

Cloud Labs

This text is accompanied by Cybersecurity Cloud Labs. These hands-on virtual labs provide immersive mock IT infrastructures where students can learn and practice foundational

cybersecurity skills as an extension of the lessons in this textbook. For more information or to purchase the labs, visit go.jblearning.com/forensics4e.

Learning Features

The writing style of this book is practical and conversational. Each chapter begins with a statement of learning objectives. Step-by-step examples of information security concepts and procedures are presented throughout the text. Illustrations are used both to clarify the material and to vary the presentation. The text is sprinkled with Notes, Tips, FYIs, Warnings, and sidebars to alert the reader to additional helpful information related to the subject under discussion. Chapter assessments appear at the end of each chapter, with solutions provided at the back of the book.

Chapter summaries are included in the text to provide a rapid review or preview of the material and to help students understand the relative importance of the concepts presented.

Audience

This material is suitable for undergraduate or graduate computer science majors or information science majors, students at a two-year technical college or community college who have a basic technical background, or readers who have a basic understanding of IT security and want to expand their knowledge.

Dedication

This book is dedicated to all the forensic analysts who work diligently to extract the evidence necessary to find the truth in criminal and civil cases.

About the Author

Dr. Chuck Easttom is the author of 32 books, including several on computer security, forensics, and cryptography. He has also authored scientific papers on digital forensics, cyber warfare, machine learning, cryptography, and applied mathematics. He is an inventor with 22 computer science patents. He holds a Doctor of Science (D.Sc.) in cyber security, a Ph.D. in nanotechnology, a Ph.D. in computer science, and three master's degrees (one in applied computer science, one in education, and one in systems engineering). He is a senior member of both the IEEE and the ACM. He is also a Distinguished Speaker of the ACM and a Distinguished Visitor of the IEEE.

He also holds 55 industry certifications, including many cyber security and digital forensics certifications. He has both academic hands-on forensics experience. He has served as an expert witness in U.S. court cases since 2004. He is currently an adjunct lecturer at Georgetown University, where he teaches cyber security, systems engineering and cryptography, and an adjunct professor at University of Dallas, where he teaches a graduate course in digital forensics.

