

COURSE TECHNOLOGY
CENGAGE Learning
Professional • Technical • Reference



Computer Evidence

Collection and Preservation
Second Edition

Christopher L. T. Brown

COMPUTER EVIDENCE: COLLECTION AND PRESERVATION, SECOND EDITION

CHRISTOPHER L. T. BROWN

Charles River Media

A part of Course Technology, Cengage Learning



COURSE TECHNOLOGY
CENGAGE Learning™

Australia, Brazil, Japan, Korea, Mexico, Singapore, Spain, United Kingdom, United States

Computer Evidence: Collection and Preservation, Second Edition

Christopher L. T. Brown

Publisher and General Manager,
Course Technology PTR:
Stacy L. HiquetAssociate Director of Marketing:
Sarah PanellaContent Project Manager:
Jessica McNavich

Marketing Manager: Mark Hughes

Acquisitions Editor: Heather Hurley

Project/Copy Editor: Karen A. Gill

Technical Reviewer: Gary Kessler

Editorial Services Coordinator: Jen Blaney

Interior Layout: Jill Flores

Cover Designer: Mike Tanamachi

CD-ROM Producer: Brandon Penticuff

Indexer: Valerie Haynes Perry

Proofreader: Sue Boshers

© 2010 Course Technology, a part of Cengage Learning.

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced, transmitted, stored, or used in any form or by any means graphic, electronic, or mechanical, including but not limited to photocopying, recording, scanning, digitizing, taping, Web distribution, information networks, or information storage and retrieval systems, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the publisher.

For product information and technology assistance, contact us at
Cengage Learning Customer & Sales Support, 1-800-354-9706.

For permission to use material from this text or product,
submit all requests online at **cengage.com/permissions.**

Further permissions questions can be e-mailed to
permissionrequest@cengage.com.

ProDiscover Basic is copyright Technology Pathways. Maresware is copyright Mares and Company, LLC. WinHex is copyright X-Ways Software Technology AG. LANSurveyor is copyright Neon Software. CryptCat is copyright Farm9.

All other trademarks are the property of their respective owners.

Library of Congress Control Number: 2009928938

ISBN-13: 978-1-58450-699-7

ISBN-10: 1-58450-699-7

eISBN-10: 1-58450-708-X

Course Technology, a part of Cengage Learning

20 Channel Center Street
Boston, MA 02210
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at: **international.cengage.com/region.**

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

For your lifelong learning solutions, visit **courseptr.com.**

Visit our corporate Web site at **cengage.com.**

To Bobbie, Rudy, and Annie, who keep me on course
and constantly remind me why life is such a joy.



Acknowledgments

In life we hardly ever go it alone. The same holds true when taking on writing projects such as *Computer Evidence: Collection and Preservation, Second Edition*. Many people, such as the technical and copy editors including Adam Speer, Leo Manning, Erin Kenneally, Gary Kessler, Karen Gill, and the Cengage Learning staff, have contributed significantly to the creation of this book. I would like to specifically call attention to and thank members of the High Technology Crime Investigation Association (HTCIA) and High Tech Crime Consortium (HTCC), List Servers for their support and mentoring over the years. This book could not have been created without their vast cumulative knowledge. I would also like to thank Alex Augustin for his years of support, and Steven Richardson and Ted Augustine for taking up the slack at Technology Pathways.



About the Author

Christopher L. T. Brown, CISSP, is the founder and CTO of Technology Pathways. He is the chief architect of the Technology Pathways ProDiscover family of security products. Prior to his position with Technology Pathways, Mr. Brown served in key technology positions at several companies including GlobalApp, Inc., CompuVision, Inc., and StoragePoint, Inc. He is retired from a career with the U.S. Navy, where he managed a large team of technicians working in the area of information warfare and network security operations.

In addition to his demanding duties as ProDiscover's chief architect, Mr. Brown teaches network security and computer forensics at the University of California at San Diego and has written numerous books on Windows, Security, the Internet, and forensics.

He served as president of the San Diego HTCIA chapter in 2006, first vice president in 2005, second vice president in 2003, and was the 2007 HTCIA International conference chair. He attended UCSD and holds numerous career certifications from (ISC)², Microsoft, Cisco, CompTIA, and CITRIX.



Contents

Introductionxxii

Part I Computer Forensics and Evidence Dynamics 1

1 Computer Forensics Essentials 3

What Is Computer Forensics?4

Crime Scene Investigation5

Phases of Computer Forensics7

 Collection8

 Preservation8

 Filtering9

 Presentation9

Formalized Computer Forensics from the Start10

Who Performs Computer Forensics?12

Seizing Computer Evidence17

Challenges to Computer Evidence20

Summary21

References22

Resources23

2 Rules of Evidence, Case Law, and Regulation 25

 Understanding Rules of Evidence26

 2007 Amendments to the *FRCP*29

 Expert Witness (Scientific) Acceptance30

Testifying Tips: You Are the Expert	33
Computer-Related Case Law	34
Regulation	38
Securities and Exchange Commission (SEC)	
Rule 17a-4 (1947)	38
National Association of Securities Dealers (NASD)	
Rules 3010 and 3110 (1997)	38
Sarbanes-Oxley Act (2002)	39
Gramm-Leach-Bliley Act (1999)	39
California Privacy Law: SB 1386 (2003)	39
Health Insurance Portability and Accountability Act (HIPAA) (First Rule in Effect in 2002)	40
International Organization for Standardization (ISO)	
17799 (2000)	41
U.S.A. PATRIOT Act (2001)	42
Personal Information Protection and Electronic Documents Act (PIPED) C-6 (2001)	42
Summary	45
References	46
Resources	47
3 Evidence Dynamics	49
Forces of Evidence Dynamics	50
Human Forces	51
Emergency Personnel	52
Forensics Investigators	52
Law Enforcement Personnel	56
Victim	59
Suspect	60
Bystanders	61
Natural Forces	61

Equipment Forces	64
Proper Tools and Procedures	66
Summary	68
References	68
Resources	69
Part II Information Systems	71
4 Interview, Policy, and Audit	73
Supporting and Corroborating Evidence	74
Subject Interviews	74
Policy Review	79
Audit	81
Executive Summary	86
Recommendations	86
Scope	87
Host-Specific Findings	88
War Dialing Results	90
Conclusion	90
Summary	92
References	92
Resources	93
5 Network Topology and Architecture	95
Networking Concepts	96
Types of Networks	97
Physical Network Topology	99
Network Cabling	104
Wireless Networks	106
Open Systems Interconnection (OSI) Model	107
TCP/IP Addressing	112

Diagramming Networks	114
Summary	117
References	118
Resources	118
6 Volatile Data	121
Types and Nature of Volatile Data	122
Operating Systems	125
Volatile Data in Routers and Appliances	128
Volatile Data in Personal Devices	130
Traditional Incident Response of Live Systems	130
Understanding Windows Rootkits in Memory	132
Accessing Volatile Data	139
Summary	142
References	142
Part III Data Storage Systems and Media	145
7 Physical Disk Technologies	147
Physical Disk Characteristics	148
Physical Disk Interfaces and Access Methods	152
Logical Disk Addressing and Access	162
Disk Features	164
Summary	167
References	167
Resources	168
8 SAN, NAS, and RAID	169
Disk Storage Expanded	170
Redundant Array of Independent Disks	173
Level 0	173

- Level 1173
- Level 2174
- Level 3174
- Level 4174
- Level 5174
- Level 6175
- Level 0+1175
- Level 10175
- Level 7175
- RAID 5175
- JBOD176
- Storage Area Networks177
- Network-Attached Storage180
- Storage Service Providers184
- Summary187
- References188
- Resources188

- 9 Removable Media189**
 - Removable, Portable Storage Devices190
 - Tape Systems191
 - Full Backup194
 - Incremental Backup194
 - Differential Backup194
 - Optical Discs195
 - Removable Disks—Floppy and Rigid200
 - Flash Media201
 - Summary205
 - References206
 - Resources206

Part IV Artifact Collection207

10 Tools, Preparation, and Documentation209

- Planning210
- Boilerplates210
- Hardware Tools212
 - Imagers and Write-Blocking212
- Software Tools222
 - Forensics Application Suites (Tier I)223
 - Utilities and Other Applications
(Tier II and Tier II–Repurposed)231
- Tool Testing233
- Documentation235
- Summary238
- References239
- Resources241

11 Collecting Volatile Data243

- Benefits of Volatile-Data Collection244
- A Blending of Incident Response and Forensics246
- Building a Live Collection Disk249
 - Scenario 1: Using Utilities249
 - Scenario 2: Using Windows Tools257
- Live Boot CD-ROMs262
- Summary264
- References265
- Resources266

- 12 Imaging Methodologies267**
 - Approaches to Collection268
 - Bit-Stream Images270
 - Local Dead System Collection275
 - Verification, Testing, and Hashing281
 - Live and Remote Collection284
 - Summary290
 - References291
 - Resources293

- 13 Large System Collection295**
 - Defining a Large Collection296
 - Large System Imaging Methodologies296
 - Tying Together Dispersed Systems303
 - Risk-Sensitive Evidence Collection309
 - Summary311
 - References312

- 14 Personal Portable Device Collection315**
 - Seemingly Endless Device List316
 - Device Architectures316
 - Special Collection Considerations322
 - Mobile Phones330
 - Special-Purpose Personal Devices336
 - Summary339
 - References339
 - Resources341

Part V Archiving and Maintaining Evidence	343
15 The Forensics Workstation	345
The Basics	346
Lab Workstations	349
Portable Field Workstations	356
Configuration Management	360
Summary	363
References	364
Resources	365
16 The Forensics Lab	367
Lab and Network Design	368
Logical Design, Topology, and Operations	373
Storage	378
Lab Certifications	381
Summary	384
References	386
17 What's Next	387
Areas of Interest	388
Collection	388
Analysis	388
Discovery	388
Criminal	389
Corporate	389
Training, Knowledge, and Experience	390
Computer Forensic Investigators Digest Listserv (CFID)	390
Computer Forensics Tool Testing (CFTT)	390
High Tech Crime Consortium (HTCC)	391

Security Focus Forensics	391
CCE	392
CISSP	393
SSCP	393
GIAC	393
CISA	394
MCSE	394
MCSD	394
RHCE	394
CCNA	394
CCDA	395
CompTIA	395
Analysis and Reporting	395
Methodologies	397
Professional Advancement	399
Summary	403
References	404
Resources	405
Part IV Computer Evidence Collection and Preservation Appendixes . . .	407
A Sample Chain of Custody Form	409
B Evidence Collection Worksheet	413
C Evidence Access Worksheet	417
D Forensics Field Kit	421
E Hexadecimal Flags for Partition Types	425

F Forensics Tools for Digital Evidence Collection431

- Software432
 - AccuBurn432
 - Autopsy Forensic Browser432
 - BitPim432
 - BlackBag MacQuisition CF432
 - Byte Back432
 - Device Seizure by Paraben433
 - dtSearch Desktop433
 - EnCase433
 - FIRE (Originally Named Biatchux)433
 - Forensics Tool Kit (FTK)—System Analysis Tool433
 - Foundstone434
 - Frank Heyne Software434
 - Helix434
 - ILook434
 - MaresWare Suite434
 - pdd435
 - ProDiscover Forensics, Investigator, and Incident Response . . .435
 - SafeBack435
 - The Coroners Toolkit (TCT)435
 - Trinix436
 - Various Must-Have Utilities from Microsoft Sysinternals436
 - WinHex and X-Ways Forensics436
- Hardware437
 - ACARD SCSI-to-IDE Write-Blocking Bridge (AEC7720WP) . . .437
 - CellDek437
 - CS Electronics437
 - DD 300/500437
 - DIBS, Inc.437

e.s.i.Discover	438
Fernico ZRT	438
Forensic Recovery Evidence Device (FRED)	438
Intelligent Computer Solutions, Inc.	438
Kazeon	438
MOBILedit	439
NoWrite IDE Write-Blocker	439
Portable Drive Service/Test/Dup by Corporate Systems	439
Project-a-Phone	439
Secure Kit for Forensics	439
Solitaire Forensics by Logicube	440
Stored IQ	440
Tableau Imagers and Write-Blockers	440
UFED (Universal Forensic Extraction Device) System	440
WiebiTech	440
ZERT by Netherlands Forensic Institute	441
General Supplies	441
CGM Security Solutions	441
Chief Supply	441
G Agencies, Contacts, and Resources	443
Agencies	444
FBI Computer Analysis Response Team (CART)	444
Internal Revenue Service	444
National Aeronautics and Space Administration	444
National Railroad Passenger Corporation (NRPC) (AMTRAK)	445
Social Security Administration Office of Inspector General	445
U.S. Customs Service's Cyber Smuggling Center	445
U.S. Department of Defense, Computer Forensics Laboratory	445

U.S. Department of Defense, Office of Inspector General445

U.S. Department of Energy446

U.S. Department of Justice, Computer Crime Intellectual
 Property Section (CCIPS)446

U.S. Department of Justice Drug Enforcement
 Administration446

U.S. Department of Transportation446

U.S. Department of the Treasury447

U.S. Postal Inspection Service447

U.S. Secret Service447

Veterans Affairs447

Training Resources447

 Canadian Police College447

 Champlain College448

 DoD Computer Investigations Training Program448

 FBI Academy at Quantico448

 Federal Law Enforcement Training Center448

 Florida Association of Computer Crime Investigators, Inc. . . .449

 Forensic Association of Computer Technologists449

 High Technology Crime Investigation Association
 (International)449

 Institute of Police Technology and Management449

 International Association for Computer
 Information Systems (IACIS)449

 International Organization on Computer Evidence (IOCE) . . .450

 International System Security Association (ISSA)450

 Getronics450

 National Center for Forensic Science450

 National Colloquium for Information Systems
 Security Education (NCISSE)450

National Criminal Justice Computer Laboratory and Training Center	450
National White Collar Crime Center (NW3C)	450
New Technologies, Inc.	451
Purdue University—CERIAS (Center for Education and Research in Information and Assurance Security)	451
Redlands Community College	451
University of New Haven	451
University of New Haven—California Campus	451
Utica College—Economic Crime Institute	452
Wisconsin Association of Computer Crime Investigators ...	452
Associations	452
High Technology Crime Investigation Association (International)	452
International Association for Computer Information Systems (IACIS)	452
International Information Systems Forensics Association (IISFA)	453
International Systems Security Association (ISSA)	453
High Tech Crime Consortium	453
Florida Association of Computer Crime Investigators, Inc. ...	453
Forensic Association of Computer Technologists	453
State Agencies	454
Alabama	454
Alaska	454
Arizona	455
Arkansas	455
California	455
Colorado	457
Connecticut	458

Delaware 458

District of Columbia 459

Florida 459

Georgia 460

Hawaii 460

Idaho 460

Illinois 461

Indiana 461

Iowa 462

Kansas 462

Kentucky 463

Louisiana 463

Maine 463

Maryland 463

Massachusetts 464

Michigan 464

Minnesota 465

Mississippi 465

Missouri 465

Montana 465

Nebraska 466

Nevada 466

New Hampshire 466

New Jersey 467

New Mexico 467

New York 467

North Carolina 469

North Dakota 469

Ohio 469

Oklahoma 470