A PRACTICAL GUIDE TO COMPUTER FORENSICS INVESTIGATIONS

DR. DARREN R. HAYES

A Practical Guide to Computer Forensics Investigations

Dr. Darren R. Hayes

PEARSON

800 East 96th Street, Indianapolis, Indiana 46240 USA

A Practical Guide to Computer Forensics Investigations

Copyright © 2015 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-7897-4115-8
ISBN-10: 0-7897-4115-6

Library of Congress Control Number: 2014955541

Printed in the United States of America

Second Printing: August 2015

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact international@pearsoned.com.

Associate Publisher
Dave Dusthimer

Acquisitions Editor
Betsy Brown

Development Editor
Jeff Riley

Managing Editor
Sandra Schroeder

Project Editor
Mandie Frank

Copy Editor
Krista Hansing

Indexer
Larry Sweazy

Proofreader
Megan Wade-Taxter

Technical Editors
Dennis Dragos
Shawn Merdinger

Publishing Coordinator
Vanessa Evans

Designer
Alan Clements

Compositor
Tricia Bronkella

Contents at a Glance

	Introduction	xx
1	The Scope of Computer Forensics	2
2	Windows Operating and File Systems	32
3	Handling Computer Hardware	80
4	Acquiring Evidence in a Computer Forensics Lab	116
5	Online Investigations	162
6	Documenting the Investigation	210
7	Admissibility of Digital Evidence	238
8	Network Forensics	292
9	Mobile Forensics	320
10	Photograph Forensics	372
11	Mac Forensics	390
12	Case Studies	436
	Index	458

Table of Contents

Introduction xx

Chapter 1: The Scope of Computer Forensics 2

Introduction 2

Popular Myths about Computer Forensics 3

Types of Computer Forensics Evidence Recovered 5

Electronic Mail (Email) 5

Images 7

Video 8

Websites Visited and Internet Searches 9

Cellphone Forensics 10

What Skills Must a Computer Forensics Investigator Possess? 10

Computer Science Knowledge 10

Legal Expertise 11

Communication Skills 11

Linguistic Abilities 11

Continuous Learning 11

An Appreciation for Confidentiality 12

The Importance of Computer Forensics 12

Job Opportunities 12

A History of Computer Forensics 14

1980s: The Advent of the Personal Computer 14

1990s: The Impact of the Internet 15

Training and Education 19

Law Enforcement Training 19

Summary 25

Chapter 2: Windows Operating and File Systems **32**

Introduction 32

Physical and Logical Storage 34

File Storage 34

File Conversion and Numbering Formats 37

Conversion of Binary to Decimal 37

Hexadecimal Numbering 37

Conversion of Hexadecimal to Decimal 38

Conversion of Hexadecimal to ASCII (American Standard Code for Information Interchange) 38

Unicode 42

Operating Systems 42

The Boot Process 42

Windows File Systems 44

Windows Registry 50

Registry Data Types 52

FTK Registry Viewer 52

Microsoft Windows Features 53

Windows Vista 53

Windows 7 59

Windows 8.1 70

Summary 73

Chapter 3: Handling Computer Hardware **80**

Introduction 80

Hard Disk Drives 81

Small Computer System Interface (SCSI) 81

Integrated Drive Electronics (IDE) 82

Serial ATA (SATA) 83

Cloning a PATA or SATA Hard Disk 86

Cloning Devices 86

Removable Memory 93
FireWire 94
USB Flash Drives 94
External Hard Drives 95
MultiMedia Cards (MMCs) 96
Summary 109
References 114
Chapter 4: Acquiring Evidence in a Computer Forensics Lab 116
Introduction 116
Lab Requirements 117
American Society of Crime Laboratory Directors 117
American Society of Crime Laboratory Directors/Lab Accreditation Board (ASCLD/LAB) 117
ASCLD/LAB Guidelines for Forensic Laboratory Management Practices 117
Scientific Working Group on Digital Evidence (SWGDE) 119
Private Sector Computer Forensics Laboratories 119
Evidence Acquisition Laboratory 120
Email Preparation Laboratory 120
Inventory Control 120
Web Hosting 121
Computer Forensics Laboratory Requirements 121
Laboratory Layout 121
Laboratory Management 141
Laboratory Access 141
Extracting Evidence from a Device 144
Using the dd Utility 144
Using Global Regular Expressions Print (GREP) 145
Skimmers 152
Summary 156

Chapter 5: Online Investigations **162**

Introduction 162

Working Undercover 163

Generate an Identity 164

Generate an Email Account 165

Mask Your Identity 167

Website Evidence 171

Website Archives 171

Website Statistics 172

Background Searches on a Suspect 173

Personal Information: Mailing Address, Email Address, Telephone Number, and Assets 174

Personal Interests and Membership of User Groups 178

Searching for Stolen Property 179

Online Crime 195

Identity Theft 195

Credit Cards for Sale 195

Electronic Medical Records 196

Cyberbullying 196

Social Networking 196

Capturing Online Communications 197

Using Screen Captures 197

Using Video 199

Viewing Cookies 199

Using Windows Registry 200

Summary 202

Chapter 6: Documenting the Investigation **210**

Introduction 210

Obtaining Evidence from a Service Provider 211

Documenting a Crime Scene 211

Seizing Evidence 213
Crime Scene Examinations 213
Documenting the Evidence 214
Completing a Chain of Custody Form 215
Completing a Computer Worksheet 216
Completing a Hard Disk Drive Worksheet 217
Completing a Server Worksheet 218
Using Tools to Document an Investigation 220
CaseNotes 220
FragView 220
Helpful Mobile Applications (Apps) 221
Network Analyzer 221
System Status 221
The Cop App 221
Lock and Code 221
Digital Forensics Reference 221
Federal Rules of Civil Procedure (FRCP) 222
Federal Rules of Evidence (FREvidence) 222
Writing Reports 222
Time Zones and Daylight Saving Time (DST) 222
Creating a Comprehensive Report 224
Using Expert Witnesses at Trial 227
The Expert Witness 228
The Goals of the Expert Witness 228
Preparing an Expert Witness for Trial 228
Summary 231

Chapter 7: Admissibility of Digital Evidence **238**

Introduction 238

History and Structure of the United States Legal System 239

Origins of the U.S. Legal System 240

Overview of the U.S. Court System 241

In the Courtroom 245

Evidence Admissibility 248

Constitutional Law 248

First Amendment 248

First Amendment and the Internet 249

Fourth Amendment 251

Fifth Amendment 263

Sixth Amendment 264

Congressional Legislation 265

Rules for Evidence Admissibility 271

Criminal Defense 276

When Computer Forensics Goes Wrong 277

Pornography in the Classroom 277

Structure of the Legal System in the European Union (E.U.) 278

Origins of European Law 278

Structure of European Union Law 279

Structure of the Legal System in Asia 282

China 282

India 282

Summary 283

Chapter 8: Network Forensics **292**

Introduction 292

The Tools of the Trade 293

Networking Devices 294
Proxy Servers 295
Web Servers 295
DHCP Servers 298
SMTP Servers 299
DNS Servers 301
Routers 302
IDS 304
Firewalls 304
Ports 305
Understanding the OSI Model 305
The Physical Layer 306
The Data Link Layer 306
The Network Layer 306
The Transport Layer 307
The Session Layer 308
The Presentation Layer 308
The Application Layer 309
Advanced Persistent Threats 310
Cyber Kill Chain 310
Indicators of Compromise (IOC) 312
Investigating a Network Attack 313
Summary 314
Chapter 9: Mobile Forensics **320**
Introduction 320
The Cellular Network 322
Base Transceiver Station 322
Mobile Station 326
Cellular Network Types 331

SIM Card Forensics 334
Types of Evidence 337
Handset Specifications 338
Memory and Processing 338
Battery 338
Other Hardware 338
Mobile Operating Systems 339
Android OS 339
Windows Phone 347
Standard Operating Procedures for Handling Handset Evidence 347
National Institute of Standards and Technology 348
Preparation and Containment 349
Wireless Capabilities 352
Documenting the Investigation 354
Handset Forensics 354
Cellphone Forensic Software 354
Cellphone Forensics Hardware 357
Logical versus Physical Examination 358
Manual Cellphone Examinations 358
Flasher Box 359
Global Satellite Service Providers 360
Satellite Communication Services 360
Legal Considerations 360
Carrier Records 361
Other Mobile Devices 361
Tablets 361
GPS Devices 362
Summary 364

Chapter 10: Photograph Forensics **372**

Introduction 372

Understanding Digital Photography 375

File Systems 375

Digital Photography Applications and Services 376

Examining Picture Files 377

Exchangeable Image File Format (EXIF) 377

Evidence Admissibility 380

Federal Rules of Evidence (FRE) 380

Analog vs. Digital Photographs 381

Case Studies 382

Worldwide Manhunt 382

NYPD Facial Recognition Unit 383

Summary 384

Chapter 11: Mac Forensics **390**

Introduction 390

A Brief History 391

Macintosh 391

Mac Mini with OS X Server 391

iPod 393

iPhone 394

iPad 394

Apple Wi-Fi Devices 395

Macintosh File Systems 397

Forensic Examinations of a Mac 398

IOReg Info 398

PMAP Info 399

Epoch Time 399

Recovering Deleted Files 401

Journaling 401
DMG File System 401
PList Files 401
SQLite Databases 404
Macintosh Operating Systems 404
Mac OS X 405
Target Disk Mode 408
Apple Mobile Devices 409
iOS 410
iOS 7 410
iOS 8 410
Security and Encryption 411
iPod 412
iPhone 413
Enterprise Deployment of iPhone and iOS Devices 426
Case Studies 426
Find My iPhone 427
Wanted Hactevist 427
Michael Jackson 427
Stolen iPhone 427
Drug Bust 427
Summary 428
Chapter 12: Case Studies **436**
Introduction 436
Zacharias Moussaoui 437
Background 437
Digital Evidence 438
Standby Counsel Objections 439
Prosecution Affidavit 440

Exhibits 440
Email Evidence 440
BTK (Bind Torture Kill) Killer 441
Profile of a Killer 441
Evidence 442
Cyberbullying 443
Federal Anti-harassment Legislation 443
State Anti-harassment Legislation 443
Warning Signs of Cyberbullying 443
What Is Cyberbullying? 444
Phoebe Prince 444
Ryan Halligan 445
Megan Meier 445
Tyler Clementi 445
Sports 447
Summary 449

Index **458**

About the Author

Dr. Darren R. Hayes is a leading expert in the field of digital forensics and computer security. He is the director of cybersecurity and an assistant professor at Pace University, and he has been named one of the Top 10 Computer Forensics Professors by Forensics Colleges.

Hayes has served on the board of the High Technology Crime Investigation Association (HTCIA), Northeast Chapter, and is the former president of that chapter. He also established a student chapter of the HTCIA at Pace University.

During his time at Pace University, Hayes developed a computer forensics track for the school's bachelor of science in information technology degree. He also created a computer forensics research laboratory, where he devotes most of his time to working with a team of students in computer forensics and, most recently, the burgeoning field of mobile forensics. As part of his research and promotion of this scientific field of study, he has fostered relationships with the NYPD, N.Y. State Police, and other law enforcement agencies. He also organized a successful internship program at the cybercrime division of the New York County D.A. Office and the Westchester County D.A. Office.

Hayes is not only an academic, however—he is also a practitioner. He has been an investigator on both civil and criminal investigations and has been called upon as an expert for a number of law firms. In New York City, Hayes has been working with six to eight public high schools to develop a curriculum in computer forensics. He collaborates on computer forensics projects internationally and has served as an extern examiner for the MSc in Forensic Computing and Cybercrime Investigation degree program at University College Dublin for four years.

Hayes has appeared on Bloomberg Television and Fox 5 News and been quoted by *Associated Press, CNN, Compliance Week, E-Commerce Times, The Guardian (UK), Investor's Business Daily, MarketWatch, Newsweek, Network World, Silicon Valley Business Journal, USA Today, Washington Post*, and *Wired News*. His op-eds have been published by American Banker's BankThink and The Hill's Congress Blog. In addition, he has authored a number of peer-reviewed articles in computer forensics, most of which have been published by the Institute of Electrical and Electronics Engineers (IEEE). Hayes has been both an author and reviewer for Pearson Prentice Hall since 2007.

About the Technical Reviewer

Dennis Dragos, President of DDragos Information Security and Investigation Corp. (DDIS) served 20 years in the New York City Police Department. For 11 years, he was assigned to the NYPD Computer Crimes Squad, Special Investigations Division, Detective Bureau, reaching the rank of 2nd grade detective. He is currently an adjunct assistant professor of the Cyber Security Systems Program within the College of Professional Studies at St. John's University, Queens, N.Y.

Shawn Merdinger is the CISO for Valdosta State University in Georgia. He has worked with Cisco Systems, 3Com/TippingPoint at University of Florida Health Science Center, and as an independent consultant. His current research focuses on medical device security, and he is the founder of the MedSec group on LinkedIn. Shawn has presented original research at security conferences such as DEFCON, Educause, ISSA, InfraGard, Ph-Neutral, ShmooCon, CONfidence, NoConName, O'Reilly, CSI, IT Underground, CarolinaCon, and SecurityOpus. He holds a bachelor's degree from University of Connecticut and a master's from the University of Texas at Austin.

Dedication

This book is dedicated to my loving wife, Nalini, and my children, Nicolai, Aine, Fiona, and Shay.

Acknowledgments

I should begin by acknowledging my supportive and patient wife, Nalini, who is my best friend. Long hours working on a book mean sacrifices for everyone in the family, and my children, Nicolai, Aine, Fiona, and Shay, have been brilliant. My parents, Annette and Ted, have been mentors throughout my life, and I will always be in their debt.

Professionally, I should acknowledge the former deans of the Seidenberg School at Pace University, Dr. Susan Merritt and Dr. Constance Knapp, who have always believed in me and supported me. My current dean, Dr. Amar Gupta, continues to support my passion for computer forensics and security. Others who deserve honorable mention are my colleagues at Pace, Dean Jonathan Hill, Dr. Catherine Dwyer, Dr. Nancy Hale, Dr. John Molluzzo, Dean Bernice Houle, Dr. Susan Maxam, Dr. Richard Kline, Professor Andreea Cotoranu, Dr. Li-Chiou Chen, Dr. Lixin Tao, Dr. Fred Grossman, Ms. Susan Downey, Ms. Bernice Tracey, Ms. Fran O'Gara, Dr. Narayan Murthy, Dr. James Gabberty, Professor Robert Benjes, Ms. Stephanie Elson, Ms. Kimberly Brazaitis, and many others.

The students at Pace University inspire me more than they realize and work many hours in the computer forensics lab. I appreciate all the hard work and dedication by Pace students Mr. Roman Perez, Ms. Renee Pollack, Mr. Mario Camilla, Mr. James Ossipov, Mr. Shariq Qureshi, Ms. Eileen Mulhall, Mr. Matthew Chao, Mr. Jakub Redziniak, and Ms. Fitore Balidemaj, to name but a few.

I wish to acknowledge my good friends from the Computer Crimes Squad, New York Police Department. We have enjoyed a marvelous relationship with the NYPD for many years, and I have attended many certification classes with them. My friends and colleagues include Det. Dennis Dragos, Det. Richard Macnamara, Det. Robert DiBattista, Det. Jorge Ortiz, Det. Joseph Garcia, Lt. Dennis Lane, Lt. Felix Rivera, Det. Owen Soba, Det. Waldo Gonzalez, Det. John Crosas, and a number of other wonderful detectives. I have also gained invaluable practical experience by working with former Lt. John Otero, former Det. Domingo Gonzalez, and former Det. Yalkin Demirkaya.

I would also like to mention other law enforcement and government agencies that have been marvelous friends and collaborators. They include the New York State Police, Federal Bureau of Investigation, United States Secret Service, Central Intelligence Agency, Bundeskriminalamt, U.K. law enforcement, and Europol.

My thanks to Mr. David Szuchman, Mr. Richard Brittson, and Mr. Steven Moran of the New York County D.A. Office. Thanks also to Mr. Michael Delohery, Bureau Chief, High Technology Crime Bureau, Westchester County D.A., and his colleagues.

Special thanks to Mr. Ryan Kubasiak, an expert in Mac forensics and my good friend; Mr. Thomas Ryan, Bristol Global; and Mr. Kenneth Citarella, one of the founding fathers of HTCIA Northeast. Thanks also to Dr. John Collins, Chairperson; and Mr. Bill Soo Hoo, College of Professional Studies, New Jersey City University. Ms. Bernadette Gleason, Citi, Ms. Dora Gomez, and Alex Allphin have been tremendous supporters as well. I appreciate the professional support and guidance from my good friend Francis X. Schroeder.

My sincere thanks to Mr. Warner Johnston and Ms. Ruth Fasoldt from the Association of Chartered Certified Accountants USA. Their tremendous support for our work at Pace has been well noted. I also wish to thank my friends at my alma mater, University College Dublin, Ireland. Dr. Pavel Gladyshev and Dr. Fergus Toolan have been terrific collaborators, and it was an honor to serve as extern examiner for their master of science in forensic computing and cybercrime investigation.

Ms. Debra Lesser, Executive Director, Justice Resource Center, has been very kind to me over the years and has allowed me to work with many magnificent high school teachers, including Mr. Stephen Bland, from Lehman High School. My thanks also to Ms. Gladys Aviles, Executive Assistant, and Carolyn Morway, Civic Education Coordinator, at the Justice Resource Center.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonitcertification.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

Introduction

The field of digital forensics is relatively new, and more books are being published on this subject matter in recent times. The problem is that many of books are very technical but are lacking in terms of the investigative skills. To be an exemplary computer forensics examiner, you need to have both technical and investigative skills. For example, simply finding the evidence on a computer is not good enough—you must be able to place the suspect behind the keyboard. Moreover, a good investigator must be able to think well beyond the scope of the computer. Chapter 11, "Mobile Forensics," is a good example of this: an investigator can retrieve an extraordinary amount of evidence about a user's activity on a smartphone without actually seizing the device. This book also clearly outlines the many different skills that are beneficial in the field of computer forensics, including knowledge of hardware, programming, and the law, as well as the ability to speak a second language and possession of solid writing skills.

This book assumes no prior knowledge of the subject matter, and I have written it for both high school and university students and professional forensics investigators. Additionally, other professions can clearly benefit from reading this book—it is useful for lawyers, forensic accountants, security professionals, and others who have a need to understand how digital evidence is gathered, handled, and admitted to court. The book places a significant emphasis on process and adherence to the law, which are equally important to the evidence that can ultimately be retrieved.

The reader of this book should also realize that a comprehensive knowledge of computer forensics can lead to a variety of careers. Digital forensics examiners and experts work for accounting firms, software companies, banks, law enforcement, intelligence agencies, and consulting firms. Some are experts in mobile forensics, some excel in network forensics, and others focus on personal computers. Other experts specialize in Mac forensics or reverse engineering malware. The good news for graduates with computer forensics experience is that they have a variety of directions to choose from: the job market for them will remain robust, with more positions than graduates for the foreseeable future.

This book is a practical guide, not only because of the hands-on activities it offers, but also because of the numerous case studies and practical applications of computer forensics techniques. Case studies are a highly effective way to demonstrate how particular types of digital evidence have been successfully used in different investigations.

Finally, this book often refers to professional computer forensics tools that can be expensive. You should realize that academic institutions can take advantage of significant discounts when purchasing these products. I also included many free or low-cost forensics tools in the book, and these can be just as effective as some of the expensive tools. You can definitely develop your own program or laboratory in a budget-conscious way.

Register this Book to unlock the data files that are needed to complete the end-of-chapter projects.

Follow the steps below:

1. Go to www.pearsonITcertification.com/register and log in or create a new account.
2. Enter the ISBN: 9780789741158
3. Click on the "Access Bonus Content" link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

Chapter 1

The Scope of Computer Forensics

Learning Outcomes

After reading this chapter, you will be able to understand the following:

- The definition and importance of computer forensics;
- Different types of digital evidence and how they are used;
- The skills, training, and education required to become a computer forensics investigator;
- Job opportunities in the field of computer forensics;
- The history of computer forensics; and
- Agencies in the U.S. and internationally involved in computer forensics investigations.

Introduction

Computer forensics is the retrieval, analysis, and use of digital evidence in a civil or criminal investigation. Ironically, computer forensics is not limited to computers as the source of evidence. Any medium that can store digital files is a potential source of evidence for a computer forensics investigator. Therefore, computer forensics involves the examination of digital files.

Computer forensics is a science because of the accepted practices used for acquiring and examining the evidence and its admissibility in court. Additionally, the tools used to retrieve and analyze digital evidence have been subjected to scientific testing over many years. In fact, the word **forensics** means "to bring to court." This definition infers that digital evidence used in an investigation needs to be retrieved, handled, and analyzed in a forensically sound manner. *Forensically sound* means that, during the acquisition of digital evidence and throughout the investigative process, the evidence must remain in its original state. Moreover, everyone who has been in contact with the evidence must be accounted for and documented in the **Chain of Custody** form.

The use of computer forensics is sometimes used as incriminating evidence in criminal cases and is often referred to as **inculpatory evidence**. However, digital evidence can be used as **exculpatory evidence,** or evidence used to prove the innocence of a defendant.

Popular Myths about Computer Forensics

Many people think that computer security and computer forensics are the same, but they are not. This is one of several misconceptions about computer forensics.

Myth 1: Computer Forensics Is the Same As Computer Security

Computer security is proactive—protecting computers and their data from being stolen or being misused. Conversely, computer forensics is reactive—a crime has been committed, and digital evidence may be the key to solving a crime and convicting a criminal. Nevertheless, computer forensics can complement computer security, particularly in the area of incident handling.

Note, however, that the National Academy of Sciences has identified digital forensics as a subset of cybersecurity.

Myth 2: Computer Forensics Is about Investigating Computers

Future chapters of this book will demonstrate how any device that stores files can be a medium for computer forensics investigators to examine. For example, a compact disc (CD) is not a computer but may contain important digital evidence.

Myth 3: Computer Forensics Is about Investigating Computer Crime

A popular misconception is that computer forensics is used only for solving computer crime or cybercrime. While this may be true, computer forensics is often equally important in murder, embezzlement, and corporate espionage investigations. On April 16, 2007, Seung-Hui Cho killed 32 people and wounded many more on the campus of Virginia Polytechnic. He subsequently committed suicide. Computer forensics investigators examined Cho's computer to reconstruct the events that led up to the murder investigation. They investigated his email account, Blazers5505@hotmail.com, and his user activity on eBay, with the username blazers5505. Computer forensics investigators were able to assess who Cho was communicating with and what he was searching for and purchasing online. Examiners also investigated his cellular telephone. One of the reasons for the rapid response by computer forensics examiners was to quickly ascertain whether Cho had an accomplice in this sordid act.

When federal agents searched Enron offices in late 2001, they found that employees had been shredding a large number of documents. Computer forensic examiners were needed to retrieve evidence from computer hard drives. The amount of digital data recovered was estimated to be equivalent to 10 times the size of the Library of Congress.

Myth 4: Computer Forensics Is Really Used to Resurrect Deleted Files

The primary purpose of computer forensics is to retrieve and analyze files with computer forensics hardware and software, utilizing a scientific methodology that is acceptable in a court of law. Computer forensics goes well beyond the ability to resurrect deleted files; numerous other files that are not easily accessible can be retrieved using computer forensics tools. Additionally, computer forensic analysis tools have highly effective search and filtering capabilities. Moreover, many professional tools provide password-cracking and decryption tools. AccessData's FTK and its Password Recovery Toolkit (PRTK) provide these capabilities.

In Practice

Locard's Exchange Principle

Dr. Edmond Locard, a forensic scientist at the University of Lyon, developed a theory known as *Transfer of Evidence* whose premise was that whenever a criminal comes into contact with his environment, a cross-transference of evidence occurs:

"Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study, and understand it can diminish its value."

This theory also applies to computer forensics, where the investigator must be conscious of the entire environment that the criminal has been in contact with. In other words, it is important for the investigator to not just focus on a laptop found inside an apartment, but to also think about connections from the laptop, including router connections and also external hard drives. Thumb drives or CDs in the dwelling might also contain important evidence. Login names and passwords could be written on pieces of paper in the apartment and might be critical to accessing a suspect's system, files, or Internet service such as email. A TiVo box, which is used to record television shows, is a storage medium that may also store important evidence. Guidance Software's most recent version of EnCase software supports the imaging and analysis of files stored on a TiVo box. EnCase is a bit-stream imaging tool. A **bit-stream imaging tool** will produce a bit-for-bit copy of original media, which includes files marked for deletion.

Naturally, the investigator must ensure that evidentiary files are maintained in their original state as when they were first acquired. In later chapters it will become clear how computer forensics investigators use processes, hardware, and software to ensure that evidence remains unchanged.

Types of Computer Forensics Evidence Recovered

Practically every type of file can be recovered using computer forensics—from system files to user-created files such as spreadsheets. The following is a list of some of the most important files to be recovered and used in criminal investigations. Of course, many of the files mentioned can often be recovered regardless of whether the user has tried to delete them.

Electronic Mail (Email)

Email is arguably the most important type of digital evidence. It is very important for a number of reasons, including the following:

- Control, ownership, and intent
- Chain of events
- Prevalence
- Endurance (tampering with evidence)
- Admissibility
- Accessibility

Control, Ownership, and Intent

In computer forensics, establishing control, ownership, and intent is critical in making the evidence incriminating. Sometimes nothing is more personal than email. Email can show the intentions of the suspect and victim. In the case of Sharon Lopatka, who was murdered by Robert Glass, email was the most important evidence in the murder trial. Glass and Lopatka exchanged numerous emails prior to their rendezvous in North Carolina, where Glass tortured and strangled Lopatka. The emails supported the disturbing claims that the torture and murder were consensual.

In cases involving possession of child pornography, the defendant commonly claims that he was unaware that the images were stored on his computer. The prosecution must prove that the defendant knew of their existence and that the pictures were of minors. Email often shows that images were shared, by the suspect, with other pedophiles. Ultimately, this helps prove the suspect's guilt and enables prosecution for the possession of child pornography using a computer to commit a child sex crime and distribute illegal images. A process known as MD5 hashing can be used to verify that an image from one computer is the same as that on another computer.

Chain of Events

Reconstructing the events that led to a crime being committed is an important aspect of presenting a case. Often one email file can contain a chain of conversations over a number of days and include the times, dates, email sender, and recipient. This can aid in establishing a chain of events.

Prevalence

Electronic mail is so important because we use it so much to communicate. Therefore, it is pervasive in society in personal and business communications. In the Enron investigation, tens of thousands of emails were acquired and investigated. In some cases accounting firms with a computer forensics unit will have a separate laboratory with a group of analysts who spend every day just working on email evidence.

Endurance: Tampering with Evidence

Endurance is defined as the concealment, destruction, alteration, or falsification of evidence. It is a serious crime that carries a felony charge in many states. In the case of *Mattel vs. MGA Entertainment, Inc.,* U.S. District Judge Stephen Larson ruled that the jury could hear testimony by Mattel that its former employee, Carter Bryant, used an application called Evidence Eliminator to tamper with evidence before releasing his computer to lawyers in 2004.

Email is very valuable to investigators because even if the defendant tries to tamper with email on his or her computer, it is still accessible from other sources. For example, email files can potentially be found on the suspect's computer or the recipient's computer. The email service can also be served a subpoena or search warrant to turn over email files stored on its email servers. Email files can also often be acquired from smartphones, like BlackBerries and iPhones, and other devices, like an iTouch or iPad.

Admissibility

Judges and courts have accepted electronic mail as admissible evidence for a number of years. Interestingly, in one case, *Rombom, et al. v. Weberman et al.*, the judge accepted email printouts as evidence; the plaintiff testified that he had received emails from the defendant and printed them.

Accessibility

Unlike many other sources of evidence, access to an individual's email is not necessarily subject to a search warrant. The Department of Justice has argued that after email has been opened, it is no longer protected by the Stored Communications Act (SCA). Although a judge has already rejected the government's petition for a warrantless search, the government has continued to argue that email resides in the Cloud and that it has the right to freely access email. Under the SCA, stored communications such as email that are less than 180 days old require law enforcement to obtain a warrant. Companies such as Yahoo!, Google, and Microsoft have combined as a group, called the Electronic Frontier Foundation, to vigorously oppose the government's efforts. However, some analysts believe that the law could change in favor of the government.

Nevertheless, what is clear is that an employee's email is the property of an individual's employer. Therefore, a company can search an employee's email without the consent of the individual. In 2009, in the case of *Stengart vs. Loving Care Agency, Inc.*, the New Jersey Superior Court, Appellate Division, reiterated that an employer may access and read an employee's email without the employee's consent

when the employee uses the company's technology to access email. Therefore, gaining access to email communications is often easier than gaining access to other methods of communication.

Images

There are numerous image file types in existence. The most widely used formats are BMP (Windows bitmap), JPEG (Joint Photographic Experts Group), TIFF (Tagged Image File Format), and PNG (Portable Network Graphics). Images have increased importance in child exploitation cases. Photographs have even greater importance today than they did 20 years ago. This is because digital photographs will provide details about the type of camera used to take a picture (proving ownership) and often contain **GPS (Global Positioning System)** data identifying the location of the cellular telephone and when the photograph was taken. The latter occurs more frequently with photographs taken with a smartphone. Generally, the file metadata of a digital photograph can identify the make and model of the camera used to take the photograph, which is valuable information for investigators. **File metadata** (see Figure 1.1) is information about a file and can include the creation, modified and last access dates, and sometimes the user who created the file.

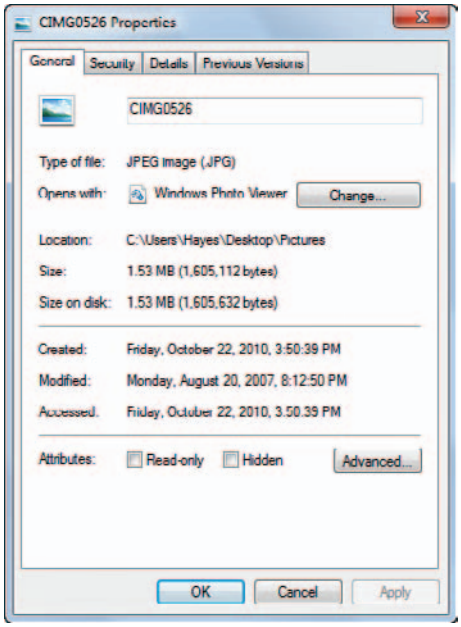

FIGURE 1.1 File metadata

Most professional computer forensics imaging and analysis software, including AccessData's FTK application, contains a user interface that can filter by file type and separate images. These image files are grouped together and include image files that the software carved away from other files. For

example, if an email or a Microsoft Word document contained an image, the application would remove it and group it with other image files that it found.

X-Ways Forensics analysis software and other forensic tools allow the investigator to filter all images with a skin tone ratio. The result is that, for the most part, only images of people are displayed after the search is run. Photographs have been used for many years in the courtroom, but digital images today provide more information than traditional film photography.

Video

Video evidence can be found on many different types of devices, including computers, digital cameras, and cellular telephones. Surveillance video today is mostly stored on computers and therefore falls under the domain of computer forensics. Surveillance video is often associated with the burglary of banks and convenience stores, but it is also being used for a much wider array of criminal activity.

The use of skimmers at automated teller machines (ATMs) has resulted in the theft of millions of dollars worldwide. A **skimmer** (see Figure 1.2) is a device used to capture the data stored on the magnetic stripe of an ATM card, credit card, or debit card. Surveillance video can be critical to the successful capture of these criminals.

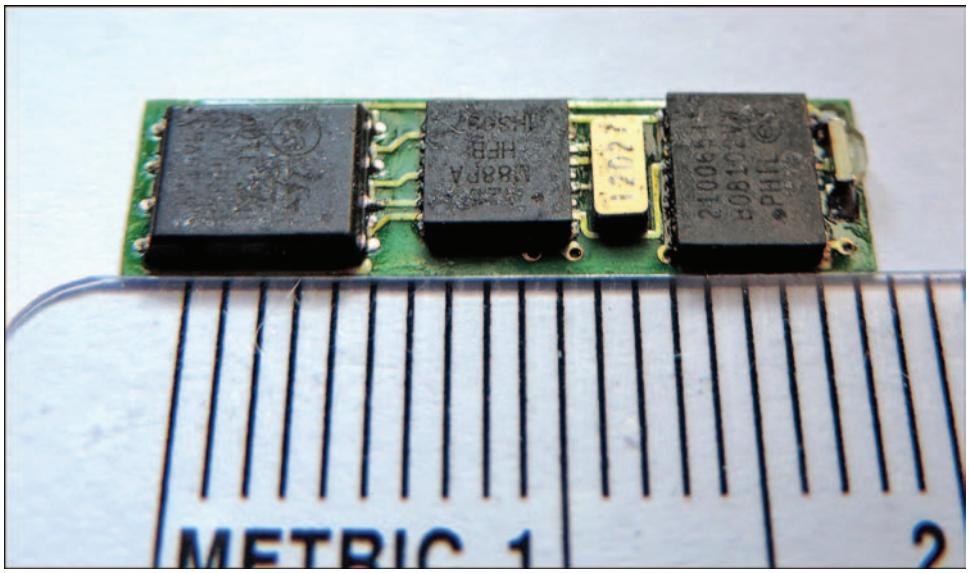

FIGURE 1.2 Skimming device

Closed-circuit television (CCTV) is the use of video transmitted to a particular location. In the city of London, there are an estimated 500,000 CCTV cameras. These cameras have been used to investigate tourists who have been robbed of their possessions or the high-profile cases like the poisoning of former Russian spy Alexander Litvenko in 2006.

Computer forensics investigators have a variety of forensic tools to choose from, including some that enhance the quality of video being analyzed. Other tools provide customizable stills at predetermined points in a video. These image stills are valuable because they can be included in an investigator's report. More importantly, these tools provide the investigator with an efficient method of identifying when in the video the important incriminating evidence exists without having to watch the video from start to finish. Moreover, if the video content is disturbing, the investigator does not have to be subjected to watching the entire distressing video.

Ultimately, in the courtroom, video evidence can be the most compelling type of evidence for a jury to convict a criminal.

Websites Visited and Internet Searches

The debate continues in law enforcement about whether the plug on a computer should be pulled to maintain the evidence in its original state or whether a live computer should stay switched on when found. With advancements in encryption and the nature of the evidence that is lost if the plug is pulled, most investigators agree that a live system should be forensically examined while it is turned on. **Encryption** is the process of scrambling plain text into an unreadable format using a mathematical formula known as an algorithm. Evidentiary files and data relating to Internet searches and websites visited are more readily available while the computer is turned on. The reason is that much of a user's current activity, including Internet activity, is stored in random access memory (RAM). RAM is often referred to as short-term memory or volatile memory because its contents largely disappear when the computer is powered down. It is important to understand that when a website is visited, a client computer makes a request to a web server. The client computer actually downloads an HTML document and related resources from the web page, like images, to the memory on the computer.

As Figure 1.3 shows, the **client computer** is a computer that requests a resource from a server computer. The primary purpose of a **web server** is to deliver HTML documents and related resources (like images) in response to client computer requests. The easiest way to remember what a client and a server do is to think of a client as a customer and a server as providing a service. Most professional computer forensics tools can image the contents of RAM effectively while the computer is powered on. A number of open source RAM analysis tools also are available.

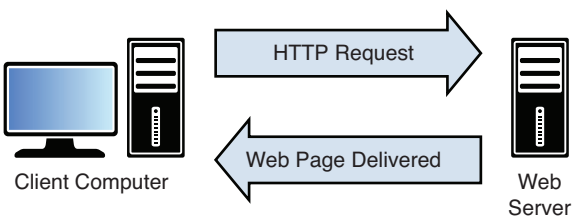

FIGURE 1.3 Communication between a client and a web server

Cellphone Forensics

The field of cellular telephone forensics is growing exponentially because the capabilities of these mobile devices continue to expand. A cellphone can tell you who the suspect knows (contacts), appointments (scheduler), who the suspect has been speaking to (call logs), and what the person has been saying (text messages). Other mobile telephones can provide image and video evidence (phone camera), places visited (GPS), online purchases, and websites visited (Internet-enabled telephones).

Cellular telephones are often used to track down suspects. In the recent murder investigation of Fred Jablin, Detective Coby Kelley obtained a warrant for suspect Piper Rountree's cellular telephone records. Because cellular telephone towers keep track of your cellular telephone as you move from one cell zone to another, the detective was able to locate the suspect in Richmond, Virginia, as she was heading east on I-64 toward the Norfolk airport. Later the cellular telephone was found transmitting from Baltimore, Maryland. After further investigation, it was discovered that Rountree had booked a flight from Baltimore to Texas in her sister's name. Piper Rountree maintained that she had never left Houston, Texas, but the cellphone forensics proved otherwise and was critical to establishing Rountree's guilt.

More information about the use of cellular telephones, in computer forensics investigations, will be discussed in Chapter 9 – Mobile Forensics.

What Skills Must a Computer Forensics Investigator Possess?

It is important to understand that computer forensics is a multidiscipline field that draws upon skills from the fields of computer science, criminal justice, law, mathematics, writing, forensic science, and linguistics.

Computer Science Knowledge

In terms of computer science, it is important to develop a strong knowledge of both operating systems and their associated file systems. A strong foundation in this subject matter will allow the investigator to know where files are stored and determine their value to prosecutors in a criminal case. Knowledge of operating systems provides an understanding of how hardware and software interact with one another. This information is vital to reconstructing the actions of a user on a computer. For example, **BitLocker**, an encryption tool that was introduced with the Ultimate and Enterprise editions of Microsoft Windows Vista, allows for encryption at the file, folder, or drive level. Therefore, a knowledgeable computer forensics investigator who encounters this operating system on a live computer will clearly understand the potential hazards of shutting down the computer. In other words, turning off the computer activates the BitLocker encryption tool if the tool has been enabled.

Simply locating and retrieving the evidentiary files is not enough. An expert computer forensics examiner must have extensive investigative abilities, which will allow him to associate that evidence

with an individual; the examiner should be able to use digital evidence to demonstrate control, ownership, and intent. For example, an investigator must be able to prove that a suspect was in control of a computer when the files were stored in memory. An example of control in this scenario is if the user used a login and password to access the computer. Ownership is another important factor when trying to prove guilt. This can be proved when the investigator can demonstrate that the suspect created a file, modified a file, or emailed the file to someone. Finally, intent is generally vital to the successful prosecution of a criminal. In computer forensics, defendants might argue that they did not intend to visit a particular website or that they inadvertently downloaded images but never viewed them. Therefore, the computer forensics investigator is also obligated to prove that a website was accessed multiple times or perhaps that an image was viewed on a number of occasions and subsequently distributed to others, to prove intent.

Legal Expertise

Knowledge of the law is extremely important, especially when it comes to computer forensics. Gaining access to a suspect's computer may be the first challenge to an investigator. If the suspect's computer is located at the person's residence, then knowledge of the Fourth Amendment, which deals with search and seizure, is imperative. Investigators must convince a judge that a crime has been committed and that there is a reasonable expectation that key evidence is present at a particular location; law enforcement must show "probable cause" or "reasonable cause to believe" that a crime has been committed.

Communication Skills

The importance of writing skills must never be underestimated in the field of computer forensics. Ultimately, the investigator must document the investigative process and findings. Moreover, the report must be written in such a way that those involved in the case who do not possess the technical expertise of the computer forensics examiner can comprehend the report's findings. If a criminal case goes to trial, the computer forensics investigator could be asked to testify as an expert witness. The investigator will then have to effectively communicate findings to a judge and jury who have a limited knowledge of computers or computer forensics.

Linguistic Abilities

Crime today has a greater international presence, facilitated by the proliferation of the Internet. With the growth of cybercrime and the adoption of technology by international terrorists, the need for bilingual investigators has grown. Therefore, a bilingual computer forensics investigator has the ability to contribute more to certain investigations.

Continuous Learning

An effective computer forensics investigator will continually learn new skills. However, there will always be skills that are critical but difficult to measure. Abstraction, or the ability to think outside

the box, is imperative because every crime is different and the evidence varies. Therefore, computer forensics investigators need to continually develop new tactics and new solutions. This ability to be flexible and continuously learn new skills is particularly important, given how rapidly technology changes. Rapid changes in technology mean changes in the nature of crime. Another intangible is related to psychology. Being able to understand the criminal provides a better understanding of that person's actions and can provide faster answers in an investigation. For this reason, we need experts who can profile serial killers and other criminals.

An Appreciation for Confidentiality

Finally, the ability to keep information confidential is imperative. Only those who need to know about an investigation should know—the fewer, the better. This is because you want to minimize the risk of the suspect finding out about an investigation. If the suspect finds out, then you risk the suspect fleeing and also risk **spoliation of evidence,** or the hiding, altering, or destroying of evidence related to an investigation. Leaks to the media are also a concern, and the jury pool can be contaminated in high-profile cases.

The Importance of Computer Forensics

Computer forensics has grown in importance because more of our lives are being captured by technology. Information about our lives is being recorded on our computers, on our cellular telephones, and across the World Wide Web, especially through social networking websites. Facebook, for example, has more than half a billion members and provides a wealth of information for investigators—from photographs, to clues about a user's password, to gaining knowledge about a suspect's networks of friends or accomplices.

Criminal investigators are typically required to reconstruct the events of a crime. Technology has facilitated this reconstruction process. A suspect can be tracked through his use of an MTA MetroCard, linked to a credit card, in the New York City Subway or through an E-Z Pass tollbooth payment. In early 2014, Queens County (NY) prosecutors charged a taxi driver, Rodolfo Sanchez, with grand larceny, theft of service, and possession of stolen property for a scheme after an E-Z Pass transmitter and its records showed that the driver had evaded paying numerous MTA (Metropolitan Transportation Authority) bridge and tunnel tolls. A suspect can also be potentially tracked by cellular telephone usage.

Job Opportunities

The Bureau of Labor Statistics has recognized the importance of computer forensics and security. It estimates that, between 2008 and 2018, job opportunities will increase by 22 percent. The increase in employment opportunities will result from an increase in criminal activity on the Internet, such as identity theft, spamming, email harassment, and illegal downloading of copyrighted materials. During

the same time period, approximately 800,000 computer and mathematical science jobs will be created, according to the bureau.

Computer forensic investigation occupations exist in law enforcement at the local, county, state, federal, and international levels. However, the private sector also has extensive opportunities for computer forensics examiners. Most accounting firms have a computer forensics laboratory, and the major firms have multiple laboratories nationwide. Corporations often procure the services of an accounting firm's computer forensics division in their investigations. Much of their business is derived from **eDiscovery** (electronic discovery), which refers to the recovery of digitally stored data. The need for this recovery could be necessitated by litigation with another corporation or could be in response to a request for information from the Securities and Exchange Commission (SEC). eDiscovery services are generally associated with civil litigation.

Skilled computer forensics examiners also have job opportunities within private investigation firms. These firms will be retained by individuals who are involved in litigation. Other times, they are retained by individuals going through divorce proceedings that involve a contested settlement or accusations of infidelity. This is especially true when a contentious custody battle ensues. It could be argued that the growth of cellular telephone forensics was prompted by some people investigating their spouse's calls to identify infidelity.

As computer forensics grows in importance, and as we embrace new technologies, continuing needs arise for new software and hardware solutions. Software and hardware companies, like AccessData, Guidance Software, BlackBag, and Paraben, employ and need individuals skilled in both computer science and investigations. Some of the larger law firms around the world also have employed computer forensics investigators or contracted the services of computer forensics consultants as the need for this type of expertise increases. Moreover, in many cases, computer forensics examiners have been called to the stand at trials to testify as expert witnesses.

Financial systems across the world also rely heavily on electronic communications and the digital storage of customer account information. Credit card fraud, wire fraud, and other instances of financial fraud have quickly pushed financial institutions to develop and invest in the field of computer forensics to capture and convict criminals. This capability provides financial institutions with a greater knowledge of criminal activity and strategies and tactics for improving computer security.

Other types of organizations training or engaging the services of computer forensics investigators are Department of Defense agencies, including the United States Air Force, Army, and Navy. The Internal Revenue Service (IRS) is one of the oldest government agencies involved in computer forensics. Federal agencies such as the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), Immigration Customs Enforcement (ICE), Drug Enforcement Agency (DEA), and U.S. Secret Service have computer forensics laboratories as well. For the FBI, this knowledge is critical, whether it's for a white-collar crime involving money laundering or perhaps the electronic communications of Al-Qaida terrorist operatives. The Secret Service also increasingly utilizes computer forensics in its investigations, including counterfeiting investigations.

In October 2001, President Bush signed the USA PATRIOT Act into law (H.R. 3162). One of the provisions of the act was to establish a nationwide network of Electronic Crimes Task Forces. The network consists of federal, state, and local law enforcement, in addition to prosecutors, academia, and private industry. This force is charged with protection of the United States's critical infrastructures. Moreover, the expertise of computer forensics examiners is imperative to the successful investigation of attacks on infrastructures, including the financial system and the power grid.

Clearly, jobs for computer forensics investigators are available in many sectors of the economy, propelled by the digitization of our personal information. Theft of our personal information and attacks on our critical infrastructures will only increase, so there will continue to be a need for expertise in the field of computer forensics. The scope of the discipline has expanded so much that specialized positions have emerged. Some examiners are trained to seize digital devices and then create images of files on those devices. These images of stored files are then transferred to another area of the laboratory, where the image is searched for files that are specifically linked to the investigation. Later, another team might be responsible for writing the report and making the evidence available through a secure website. The latter is a procedure known as discovery, whereby both defense and prosecution lawyers can view the evidence.

Specialization within the field of computer forensics is also apparent when it comes to different types of devices. Mobile forensics investigators focus on cellular telephone evidence, and now Mac forensics specialists focus on Apple computers and devices such as an iPad or an iPod.

A History of Computer Forensics

Although crimes involving computers have existed for many years, crime began to really grow with the advent of the personal computer (PC) in the 1980s. IBM was at the forefront of PC development initially, and in 1981, the company introduced the 5150 PC. IBM competed in the 1980s with other PC manufacturers, including Atari, Commodore, Tandy, and Apple. Apple was extremely successful in the personal computer market in the 1980s. In 1984, the Macintosh 128K machine was introduced, with a built-in black-and-white display. Apple soon followed with the Macintosh 512K Personal Computer that same year. This computer supported productivity software, including Microsoft Excel. The Macintosh SE became one of the most popular personal computers when it launched in 1987.

1980s: The Advent of the Personal Computer

Interestingly, around this time, the first electronic bulletin boards emerged and facilitated communication between hackers. Subsequently, hacking groups, like the Legion of Doom in the United States, emerged. The 1983 film *War Games* introduced the public to the concept of hacking with a personal computer in order to gain access to government computers. In 1984, Eric Corley (with the handle Emmanuel Goldstein) published *2600: The Hacker Quarterly*, which facilitated the exchange of hacking ideas. Kevin Mitnick, one of the earliest hackers, was convicted in 1989 of stealing firmware (software) from DEC and access codes from MCI. In the wake of numerous high-profile system

break-ins, Congress passed the Computer Fraud and Abuse Act in 1986. The act has subsequently been amended several times.

Federal Bureau of Investigation (FBI)

In 1984, the FBI established the Magnetic Media Program, which subsequently became known as the **Computer Analysis and Response Team** (CART). The group was responsible for computer forensics examinations. Special Agent Michael Anderson, in the criminal investigation division of the IRS, has sometimes been referred to as the Father of Computer Forensics.

National Center for Missing and Exploited Children (NCMEC)

In local and county law enforcement, computer forensics investigators generally spend a large proportion of their time on child endangerment cases, especially those involving the possession and distribution of child pornography. In 1984, the U.S. Congress established the National Center for Missing and Exploited Children (NCMEC). **NCMEC** is mandated to help locate missing children and combat the (sexual) exploitation of children. It acts as a central repository for documenting crimes against missing children, including victims of child endangerment.

1990s: The Impact of the Internet

With the advent of web browsers, like Netscape in the 1990s, access to the Internet became much easier. No longer did Internet users have to use a command-line interface to reach Internet resources because there was a user-friendly, aesthetically pleasing interface. Web browsers prompted a massive migration of computers to the Internet. Equally important was the fact that computers that could not communicate with one another, such as a PC and a Mac, could now with relative ease thanks to the establishment of a common communication Internet protocol known as HyperText Transport Protocol (HTTP). Electronic mail (email) was also created around this time, although initially it was used as a method of communicating within organizations. Multinational companies could dramatically reduce their telephone costs by establishing an email network. New uses of technology for communication meant that there was new value put on digital evidence. In 1993, the first International Conference on Computer Evidence took place.

Department of Defense (DoD)

In 1998, the Defense Reform Initiative Directive #27 directed the U.S. Air Force to establish the joint Department of Defense Computer Forensics Laboratory, which would be responsible for counterintelligence, criminal, and fraud computer evidence investigations. Simultaneously, a computer forensics training program was created, known as the Defense Computer Investigations Training Program. The training program became an academy that is accredited by the American Council of Education. The Department of Defense Cyber Crime Center, or DC3, was comprised of the academy and laboratory and was later joined by the Department of Defense Cyber Crime Institute (DCCI) in 2002. DC3 has partnered with Oklahoma State University's Center for Telecommunications and Network Security

(CTANS) to develop and operate the National Repository for Digital Forensic Intelligence (NRDFI), which has developed a number of forensic tools.

U.S. Internal Revenue Service

The IRS dates back to the American Civil War, when President Lincoln created the position of Commissioner of Internal Revenue. Today the IRS is a division of the Department of the Treasury. As computer usage has increased over the years, so has the need for use of computer forensics in IRS investigations. The IRS Criminal Investigation Division Electronic Crimes Program funded Elliott Spencer to develop a computer forensics tool known as ILook. The IRS Criminal Investigation Division (IRS-CID) has been using ILook since 2000 to facilitate financial investigations. The ILook Suite was historically available to local and state law enforcement free of charge.

United States Secret Service (USSS)

We often think of the United States Secret Service (USSS) as solely providing protection for the commander in chief—the president of the United States. However, this federal agency has a relatively long and distinguished history in the field of computer forensics. This is because the USSS has field agents across the United States working on criminal investigations, including crimes involving money laundering and currency counterfeiting. In the 1994 Crime Bill, Congress mandated that the USSS apply its forensic and technical knowledge to criminal investigations connected to missing and exploited children. Thus, the Secret Service works closely with NCMEC. In 1996, the USSS established the New York **Electronic Crimes Task Force (ECTF),** a center used to collaboratively investigate cybercrimes.

In 2001, the USA PATRIOT Act mandated that the United States Secret Service expand its successful New York Electronic Crimes Task Force and establish ECTFs nationwide. The following year, in response to a lack of coordination of law enforcement agencies prior to the events of September 11, 2001, the Department of Homeland Security (DHS) was formed. Its primary responsibility was to protect the United States from terrorist attacks and also to effectively respond to natural disasters. The Secret Service then became an agency within the DHS. In April 2003, the PROTECT Act (also known as the Amber Alert Bill) gave full authorization to the USSS to manage investigations involving child abuse and provided greater funding and resources to these efforts. In 2007, the agency established the National Computer Forensics Institute (NCFI) as a partnership between the USSS and the DHS, the Alabama District Attorneys Association, the State of Alabama, and the city of Hoover, AL. NCFI provides computer forensics training to law enforcement, prosecutors, and judges. The NCFI facility is comprised of high-technology classrooms, a computer forensics laboratory, and a mock courtroom. In reality, the USSS is typically less involved with child exploitation cases, given its focus on financial crimes. The FBI, the DHS-ICE, and the Postal Inspector's Service are more involved in child abuse cases.

The need for international collaboration, especially cooperation with law enforcement in Europe, has become more important since the events of September 11, 2001. Therefore, in 2009 the USSS established the first European Electronic Crimes Task Force, based in Rome, Italy. The following year, the USSS established the United Kingdom Electronic Crimes Task Force.

International Collaboration

International collaboration on investigations is extremely important because, generally, the larger the crime, the larger the scope geographically. Criminals tend to use the Internet to effectively communicate both on an intrastate level and internationally. In 1995, the International Organization on Computer Evidence (IOCE) was formed. The organization facilitates the exchange of information for law enforcement internationally. In 1998, G8 appointed IICE to create standards for digital evidence handling.

INTERPOL

In terms of international efforts and collaboration, INTERPOL has taken a central role in applying digital evidence to criminal investigations. **INTERPOL** is the world's largest international police organization, representing 188 member countries. In 1989, the General Secretariat was moved to Lyon, France. In 2004, an INTERPOL liaison office was established at the United Nations, and in 2008, a special representative was appointed to the European Union in Brussels.

INTERPOL's Incident Response Team (IRT) has provided computer forensics expertise on a number of high-profile international investigations. In a 2008 report, computer forensics examiners from law enforcement in Australia and Singapore examined 609GB of data on eight laptops, two external hard drives, and three USB thumb drives at the request of the Columbian authorities. The hardware and software belonged to the *Fuerzas Armadas Revolucionarias de Colombia* (FARC). FARC is an anti-government terrorist organization in Columbia, which is largely funded through its control of illegal drug trafficking, primarily the trafficking of cocaine. Columbian investigators contacted INTERPOL to examine the seized laptops in an effort to have unbiased investigators view the digital evidence to corroborate assertions that the digital evidence had been handled in a forensically sound manner.

At the 2008 ICPO-INTERPOL General Assembly in St. Petersburg, Russian approval was made for the creation of an INTERPOL Computer Forensics Analysis Unit. This unit provides training and assistance on computer forensics investigations and has been charged with the development of international standards for the search, seizure, and investigation of electronic evidence.

INTERPOL has worked for many years on fighting crimes against children. Similar to NCMEC, since 2001, INTERPOL has maintained a database of exploited children, referred to as the INTERPOL Child Abuse Image Database (ICAID). Subsequently, in 2009, ICAID was replaced by the International Child Sexual Exploitation image database (ICSE DB). The database is accessible to law enforcement in real time around the world. This powerful database incorporates image comparison software to link victims with places. INTERPOL also works with other agencies worldwide to fight child abuse, including COSPOL Internet Related Child Abuse Material Project (CIRCAMP) and the Virtual Global Taskforce. CIRCAMP is a European law enforcement network, that monitors the Internet to detect child pornography and child abuse. The Virtual Global Taskforce has the same purpose and mission but is a global network of law enforcement agencies fighting online child abuse.

INTERPOL has been successful in coordinating international efforts to apprehend suspected pedophiles. Following a 2006 police raid on Internet predators in Norway, investigators discovered a laptop containing nearly 800 horrifying images of young boys. Nearly 100 of the images depicted a

middle-aged, white male watching these boys being abused. The authorities requested the assistance of INTERPOL to track down the unknown predator. INTERPOL initiated a massive manhunt and solicited help from the public through the media. Within 48 hours of the appeal for help, INTERPOL and Immigration and Customs Enforcement (ICE) arrested 60-year-old Wayne Nelson Corliss of Union, New Jersey.

Regional Computer Forensics Laboratory

In 1999, the first Regional Computer Forensics Laboratory (RCFL) was established in San Diego California. In 2000, the second RCFL in the United States was opened in Dallas, Texas. An **RCFL** is an FBI-sponsored laboratory used to train law enforcement in the use of computer forensics tools. The laboratories are also used for law enforcement personnel from different agencies to collaborate on criminal investigations. Smaller law enforcement agencies often do not have the budget and resources for an effective computer forensics laboratory. RCFLs provide smaller police departments the opportunity to send one or two officers to a laboratory where they can be trained and work on their investigations. The types of crimes investigated include terrorism, child pornography, theft or destruction of intellectual property, Internet crimes, property fraud, and financial fraud. Today there are 14 RCFLs in the United States and 2 in Europe.

Fusion Centers

Established in 2003, fusion centers are central repositories for collecting intelligence at the state and local levels, with the goal of preventing terrorist attacks. The project is a joint initiative between the Department of Homeland Security (DHS) and the Department of Justice (DOJ). More than 70 fusion centers operate around the country. The locations of these centers are classified (however, a group known as Public Intelligence has disclosed the physical locations of most of these centers). The buildings have no signs and no geographical addresses, and are only associated with a P.O. Box. For example, the fusion center located in West Trenton, New Jersey, has P.O. Box 7068 instead of a street address.

Reports after the events of 9/11 cited the lack of information sharing between government agencies, like the NSA, CIA, and FBI, as being a major impediment to preventing the terrorist attacks. For example, Ziad Jarrah, who hijacked the United Airlines Flight 93 on September 11, 2001, which crashed in Pennsylvania, was stopped by local police for speeding on September 9. The state trooper had no intelligence to detain Jarrah and did not know that he was being tracked by the FBI.

Local law enforcement collects information and then adds this information to fusion centers. The type of information collected includes surveillance camera footage, license plate numbers, and suspicious activity reports. The suspicious activity reports can include reports about individuals taking photographs of government buildings, making maps, or holding unusual group meetings.

The fusion centers reportedly maintain databases of information for just about every American—information that includes unlisted cellular telephones numbers, drivers' license information, and insurance claims. The fusion centers also collect information from relatively unknown data mining companies such as Entersect. Entersect provides information to human resources about potential

hires and their criminal records, litigation and bankruptcy histories, education, and employment references. It also provides a service to law enforcement known as Entersect Police Online. According to its website (entersect.net) they can provide law enforcement with access to 12 billion online records covering 98 percent of the U.S. population. Fusion centers also utilize other commercial database vendors, like Lexis-Nexis.

As a result of their secrecy and the amount of personal information collected, fusion centers have been shrouded in controversy. Civil liberties organizations, like the American Civil Liberties Union (ACLU), have frowned upon their zeal for collecting personal information and their lack of oversight. These fusion centers are a combination of both law enforcement and corporate personnel. Some have questioned the role of local law enforcement in monitoring suspicious activity. For example, in 2008, Duane Kerzic was arrested by Amtrak Police at Penn Station in New York after he was spotted on a train platform taking a photo of a train. He was handcuffed in a holding cell. It transpired that Kerzic was actually trying to win Amtrak's annual photo contest.

Although the role of fusion centers can be categorized as counterterrorism, they may well play an active role in future computer forensics investigations. Fusion centers provide a clear indication of the type of digital information being collected and stored.

Training and Education

There are a number of ways to become a computer forensics investigator. An indirect way into the profession for many has been through law enforcement. Many of these professionals began their careers as police officers and later became successful investigators. Subsequently, their aptitude for computing, in addition to the needs of their department in investigating digital evidence, provided them with the opportunity to become skilled computer forensics examiners. Formal training in computer forensics is a relatively new concept.

Law Enforcement Training

As noted earlier, Regional Computer Forensic Laboratories (RCFL) are used by law enforcement to share resources, collaborate on criminal investigations, and improve their skills as computer forensics investigators. RCFLs also provide formal training classes to RCFL and FBI CART examiners. Training includes seizing and handling evidence, as well as operating systems and their associated file systems.

Carnegie Mellon's Computer Emergency Response Team (CERT) has developed a number of computer forensics tools exclusively for law enforcement. Training on these tools has been available through CERT's Virtual Training Environment (VTE).

Headquartered in Glynco, Georgia, the **Federal Law Enforcement Training Center (FLETC)** is an interagency law enforcement training organization for more than 80 federal agencies nationwide. One of the programs it provides is the Seized Computer Evidence Recovery Specialist (SCERS). FLETC also provides training in topics such as Mac forensics and network forensics.

The **National White Collar Crime Center (NW3C)** is an agency that delivers training and investigative support to law enforcement and those who prosecute criminal cases. NW3C hosts classes in various aspects of computer forensics, including cellphone forensics, online investigations, operating systems, file systems, and acquisition and handling of digital evidence. The Secure Techniques for Onsite Preview (STOP) class is one of its well-recognized courses. The class is for probation/parole officers, detectives, and officers who perform spot checks or home visits and need to quickly check a computer in a forensically sound manner. For example, a parole officer might need to check for images on the home computer of a convicted sex offender.

INTERPOL has provided computer forensics investigative support globally for law enforcement. In April 2009, University College Dublin (UCD) and INTERPOL launched an e-crime investigation training initiative. Not only did this initiative provide training, but it also facilitated academic exchanges in the field of computer forensics to further the skills of computer forensics examiners. UCD has a prestigious Master of Science in Forensic Computing and Cybercrime investigation degree program that is exclusively available to law enforcement worldwide.

The **High Tech Crime Investigation Association (HTCIA)** is an organization that was established to facilitate the exchange of information for computer forensics professionals in law enforcement and prosecution. However, it is not a formal training organization. Membership is available to security professionals and computer forensics researchers, as well as teachers in academia. Professionals associated with criminal defense are prohibited from joining the organization. The HTCIA has local chapters around the United States that have monthly meetings featuring guest speakers from the private and public sectors. The HTCIA also provides training in the latest computer forensics tools and investigative techniques.

Another organization committed to the exchange of ideas and practices in computer forensics is the **Computer Technology Investigators Network (CTIN)**. CTIN membership is open to law enforcement, corporate security professionals, and members of the academic community. Finally, **InfraGard** is a public-private agency of the FBI, which promotes the exchange of information between the private and public sectors on issues related to terrorism, intelligence, and security matters. InfraGard has established local chapters nationally, and membership is open to all U.S. citizens, who are subject to an FBI background check.

High Schools

A number of high schools around the United States have adopted a computer forensics curriculum for both law and technology track students. One example is the New York City Department of Education, which worked with Pace University to create the first computer forensics curriculum for high school students in 1997. A computer forensics curriculum is a marvelous way to teach high school students about the intricacies of investigations involving digital evidence.

Universities

More recently, many universities have created classes for both undergraduate and graduate degree programs in computer forensics. Three of the earliest and prestigious third-level institutions to develop

degree programs are Champlain College, Purdue University, and Carnegie Mellon University. Carnegie Mellon and Purdue University work with local law enforcement in the field of computer forensics. Another notable computer forensics degree programs is offered at Bloomsberg University. Tracks in computer forensics are offered at other academic institutions, like Pace University, which also works closely with law enforcement.

Professional Certifications

Achieving a degree in computer forensics, information technology, or even information systems can provide a strong foundation in computer forensics. A degree supplemented by certifications provides greater competencies in the field and makes a candidate even more marketable to a potential employer. This is because many certification classes are taught by industry professionals and include hands-on training with professional tools.

The following is a list of computer forensics certifications available that are beneficial to legitimizing the credentials of a computer forensics examiner. However, the list is not an exhaustive one.

Professional Certifications Available to the General Public

The International Association of Computer Investigative Specialists (IACIS) is a nonprofit organization dedicated to educating law enforcement in the field of computer forensics. One of the most recognized industry certifications is the Certified Forensic Computer Examiner (CFCE), which is offered by IACIS.

John Mellon was an active member of IACIS before he founded the International Society of Forensic Computer Examiners (ISFCE). He developed a certificate known as the Certified Computer Examiner (CCE), which was first awarded in 2003. The ISFCE has four testing centers and provides a proficiency test for the American Society of Crime Laboratories Directors/Laboratory Accreditation Board (ASCLD/LAB), which is recognized as the pinnacle of certifications for forensic laboratories. ASCLD is a nonprofit, professional society of crime laboratory directors and forensic science managers who seek to promote excellence in the field of forensic science, including computer forensics. The United States Secret Service and many other law enforcement computer forensics laboratories are accredited by ASCLD/LAB, which is a testament to the prestige that this certification carries.

Many other vendor-neutral certifications are available to the public. The Certified Computer Forensics Examiner (CCFE) certification is offered by the Information Assurance Certification Review Board (IACRB). To attain the CCFE, the candidate must successfully demonstrate a mastery of the following domains:

- Law, ethics, and legal issues
- The investigation process
- Computer forensic tools
- Hard disk evidence recovery and integrity
- Digital device recovery and integrity

- File system forensics
- Evidence analysis and correlation
- Evidence recovery of Windows-based systems
- Network and volatile memory forensics
- Report writing

The Certified Forensic Consultant (CFC) certification, awarded by the American College of Forensics Examiners International (ACFEI), focuses on the legal aspects of computer forensics within the United States. The program educates students in the following areas:

- The litigation process
- Federal rules of evidence
- The discovery process
- Note taking
- Site inspection
- The written report
- The retainer letter
- Types of witness
- The expert witness report
- Preparing for deposition
- What to expect at deposition
- Preparing for trial
- Testifying at trial
- What to bring to court
- The business of forensic consulting

The ACFEI also provides training and assessment for the Certified Forensic Accountant (Cr.FA) certification. A **forensic accountant** is an individual who has an accounting background and is involved with financial investigations.

Since its formation in 1989, the SANS (SysAdmin, Audit, Network, Security) Institute has provided training to security professionals in both the public and private sectors. SANS also provides training in computer forensics and hosts a class called Computer Forensic Investigations and Incident Response. This course provides the training required to achieve the certification of GIAC Certified Forensic

Analyst (GCFA). Founded in 1999, the Global Information Assurance Certification (GIAC) provides skills assessments for security professionals.

Professional Certifications Offered to Security Professionals

Although computer security and computer forensics are two different disciplines, they are two disciplines that complement each other. Therefore, many professional computer forensics examiners have computer security certifications. Both security professionals and computer forensics experts can be involved in handling incidents, also known as security breaches. Security professionals can provide information about the type of security breach that occurred and the scope of the attack, whereas the computer forensics examiner can often determine the trail of evidence left by the perpetrator of the attack.

The Certified Security Incident Handler (CSIH) program is an excellent course for a computer forensics investigator to take. The certificate program is offered by CERT (Computer Emergency Response Team) and is a division of the Software Engineering Institute (SEI) at Carnegie Mellon University. SEI is a federally funded research and development center sponsored by the Department of Defense (DoD). CERT provides training to network administrators and other technical support staff. The training includes the identification of existing and potential threats to networks. Moreover, CERT trains security professionals on how to handle security breaches. CERT has a renowned forensics team that works closely with law enforcement on research projects for gap areas not addressed by commercial tools for computer forensics investigators.

It is quite common for a computer forensics investigator, particularly in the private sector, to be a Certified Information Systems Security Professional (CISSP). The certification is offered by the International Information Systems Security Certification Consortium $(ISC)^2$. The certification has been formally approved by the DoD in its Information Assurance Technical and Managerial categories. This important well-regarded certification is achieved after successful completion of an examination of the Common Body of Knowledge (CBK). The CBK covers the following domains of security:

- Access control
- Application development security
- Business continuity and disaster recovery planning
- Cryptography
- Information security governance and risk management
- Legal, regulations, investigations, and compliance
- Operations security
- Physical security
- Security architecture and design
- Telecommunications and network security

To pass the CISSP examination, the examinee must score at least 700 out of 1,000 points from 250 multiple-choice questions. A CISSP applicant must prove that he has a minimum of five years' experience in 2 or more of the 10 domains. The applicant is also subject to a criminal background check and must abide by the CISSP Code of Ethics. Once approved for the certification, a CISSP must attain Continuing Professional Credits (CPE) to maintain his certification.

Another recognized security certification often held by computer forensics examiners is the Certified Information Security Manager (CISM). Like the CISSP certification, the CISM certification is for security professionals. It differs from the CISSP, however, because the CISM is a certification for information security managers with experience in the following areas:

- Information security governance
- Information risk management
- Information security program development
- Information security program management
- Incident management and response

As with the CISSP certification, anyone with CISM certification has a continuing professional education requirement so that they stay up-to-date with the latest knowledge in information security management.

Professional Certifications Offered by Computer Forensics Software Companies

Most computer forensics software vendors offer certification classes. Arguably, the three most prominent computer forensics imaging software vendors are AccessData, Guidance Software, and X-Ways Forensics:

- AccessData provides an AccessData Bootcamp and classes in Windows Forensics, Mac Forensics, Internet Forensics, and Mobile Forensics. Its best-known certification is the AccessData Certified Examiner (ACE). The exam tests the user's competencies with the FTK Imager, Registry Viewer, and PRTK tools.
- Guidance Software also provides training and assessment for computer forensics examiners. A student who can demonstrate proficiency with EnCase can become an EnCase Certified Examiner (EnCE).
- X-Ways Forensics provides regular training and assessment with the X-Ways Forensics bitstream imaging tool and also the WinHex product. Typically, an X-Ways instructor conducts a 5-day class, beginning with a 2-day session on file systems. The remaining days focus on the forensic tools.

The ACE and EnCE certifications, as well as X-Ways Forensics training, are open to professionals from both the private and public sectors.

Summary

Computer forensics is the use of digital data to solve a crime. It is a scientific discipline, and as with any area of forensics, close adherence to the law is important. Computer forensics has been used in many different types of criminal investigations but can also be used in civil litigation or as part of incident response to a network intrusion. A computer forensics investigator uses many different types of hardware and software to extract and analyze files, including a bit-stream imaging tool that produces a bit-for-bit copy of the suspect's device. Finding the evidence is not always enough: It is important to establish control, ownership, and intent by the suspect. Digital evidence can include emails, images, videos, websites visited, and Internet searches.

An effective computer forensics investigator should possess skills in a number of areas, including computer science, criminal justice, law, mathematics, writing, forensic science, and linguistics. These skills can be gained through various avenues, such as on-the-job training (common in law enforcement), degree programs at colleges, or certification courses. Those who want to pursue a career in computer forensics have many opportunities in both the private and public sectors.

The advent of the personal computer in the 1980s increased computer usage in the home and prompted an increase in computer-related crime. Subsequently, government agencies began to devote resources to computer forensics, evidenced by the establishment of the Computer Analysis and Response Team (CART) at the FBI. The introduction of web browsers in the 1990s stimulated a huge migration of personal computer users to the Internet and ultimately made the Internet a valuable resource for finding information about suspects and also a source of incriminating evidence. Many agencies within the Department of Homeland Security (DHS) use computer forensics. For example, the Internet has facilitated international criminal networks, so INTERPOL has greatly enhanced its computer forensics capabilities. The need for international collaboration between DHS and other countries already exists but will continue to grow, especially in the field of computer forensics.

Table 1.1 provides a brief historical perspective of computer forensics.

TABLE 1.1 A Brief History of Computer Forensics

Year	Event
1981	IBM introduced the 5150 PC.
1984	The FBI established the Magnetic Media Program, later known as CART.
1984	The National Center for Missing and Exploited Children (NCMEC) was founded.
1985	HTCIA was founded in CA.
1986	The USSS established the Electronic Crimes Task Force (ECTF).
1986	Congress passed the Computer Fraud and Abuse Act.
1993	The first International Conference on Computer Evidence took place.
1994	Congress passed the Crime Bill, and the USSS began working on crimes against children.
1994	Mosaic Netscape, the first graphical web browser, was released.
1995	The International Organization on Computer Evidence (IOCE) was formed.

Year	Event
1996	USSS founded the New York Electronic Crimes Task Force (ECTF).
1999	The First Regional Computer Forensics Laboratory (RCFL) was established in San Diego.
2000	The IRS Criminal Investigation Division (IRS-CID) began using ILook.
2001	The USA PATRIOT Act and USSS were directed to establish ECTFs nationwide.
2001	INTERPOL developed a database of exploited children (ICAID).
2002	The Department of Homeland Security (DHS) was formed.
2003	The PROTECT Act was passed to fight against child exploitation.
2003	Fusion centers were established.
2007	The National Computer Forensics Institute (NCFI) was established.
2008	The formation of an INTERPOL Computer Forensics Analysis Unit was approved.
2009	The first European ECTF was formed (Italy).
2010	The second European ECTF was formed (United Kingdom).

KEY TERMS

algorithm: A set of steps used to solve a problem.

BitLocker: An encryption tool that was introduced with the Ultimate and Enterprise editions of Microsoft Windows Vista, which allows for encryption at the file, folder, or drive level.

bit-stream imaging tool: A tool that produces a bit-for-bit copy of original media, including files marked for deletion.

Chain of Custody: Documentation of each person who has been in contact with evidence, from its seizure, to its investigation, to its submission to court.

client computer: A computer that requests a resource from a server computer.

closed-circuit television (CCTV): Use of video that is transmitted to a particular location.

Computer Analysis and Response Team (CART): A unit within the FBI that is responsible for providing support for investigations that require skilled computer forensics examinations.

computer forensics: The retrieval, analysis, and use of digital evidence in a civil or criminal investigation.

computer security: Prevention of unauthorized access to computers and their associated resources.

Computer Technology Investigators Network (CTIN): An organization committed to the exchange of ideas and practices in computer forensics.

eDiscovery: The recovery of digitally stored data.

Electronic Crimes Task Force (ECTF): Nationwide centers used to collaboratively investigate cybercrimes.

encryption: The process of scrambling plain text into an unreadable format using a mathematical formula.

exculpatory evidence: Evidence used to prove the innocence of a defendant.

Federal Law Enforcement Training Center (FLETC): An interagency law enforcement training organization for more than 80 federal agencies nationwide.

file metadata: Information about a file that can include the creation, modified and last access dates, and also the user who created the file.

forensic accountant: An individual who has an accounting background and is involved with financial investigations.

forensics: To bring to court.

GPS (Global Positioning System): Is a device that receives communications from orbiting satellites to determine geographic location.

High Tech Crime Investigation Association (HTCIA): An organization that was established to facilitate the exchange of information between computer forensics in law enforcement and prosecution.

inculpatory evidence: Incriminating evidence often used to convict a criminal.

InfraGard: A public-private agency of the FBI that promotes the exchange of information between the private and public sectors on issues related to terrorism, intelligence, and security matters.

INTERPOL: The world's largest international police organization, representing 188 member countries.

National Center for Missing and Exploited Children (NCMEC): An agency mandated to help locate missing children and combat the (sexual) exploitation of children.

National White Collar Crime Center (NW3C): An agency that delivers training and investigative support to law enforcement and those who prosecute criminal cases.

random access memory (RAM): Often referred to as short-term memory or volatile memory because its contents largely disappear when the computer is powered down. A user's current activity and processes, including Internet activity, are stored in RAM.

Regional Computer Forensics Laboratory (RCFL): An FBI-sponsored laboratory that trains law enforcement in the use of computer forensics tools and collaboratively works on criminal investigations.

skimmer: A device used to capture the information stored in the magnetic strip of an ATM card, credit card, or debit card.

spoliation of evidence: Hiding, altering, or destroying evidence related to an investigation.

tampering with evidence: The concealment, destruction, alteration, or falsification of evidence.

web server: Delivers HTML documents and related resources in response to client computer requests.

Assessment

CLASSROOM DISCUSSIONS

1. How do you become a computer forensics investigator?
2. What is computer forensics, and how is it used in investigations?

MULTIPLE-CHOICE QUESTIONS

1. Which of the following statements best defines computer forensics?
   - **A.** Computer forensics is the use of evidence to solve computer crimes.
   - **B.** Computer forensics is the use of digital evidence to solve a crime.
   - **C.** Computer forensics is used only to find deleted files on a computer.
   - **D.** Computer forensics is used only to examine desktop and laptop computers.
2. A Chain of Custody form is used to document which of the following?
   - **A.** Law enforcement officers who arrest and imprison a criminal suspect
   - **B.** A chain of letters or emails used in an investigation
   - **C.** Anyone who has been in contact with evidence in a case
   - **D.** None of the above
3. Which of the following can be of evidentiary value to a computer forensics examiner?
   - **A.** A compact disc
   - **B.** An Xbox
   - **C.** A digital camera
   - **D.** All of the above
4. Which of the following statements best describes a bit-stream imaging tool?
   - **A.** A bit-stream imaging tool produces a bit-for-bit copy of the original media.
   - **B.** A bit-stream imaging tool often provides the examiner with deleted files.
   - **C.** Neither A or B is correct.
   - **D.** Both A and B are correct.

5. Which of the following are benefits of email evidence?

   A. Email evidence generally exists in multiple areas.
   B. It can often be found easier than other types of evidence.
   C. It has been accepted as admissible evidence in a number of cases.
   D. All of the above.

6. Which of the following statements is not true about photo images?

   A. Images can possess evidence of where the suspect has been.
   B. Images cannot be easily found using bit-stream imaging tools such as FTK.
   C. An image can identify the make and model of the digital camera.
   D. Basically just one type of digital image is used today.

7. Which of the following terms best describes the hiding, altering, or destroying of evidence related to an investigation?

   A. Spoliation of evidence
   B. Manipulation of evidence
   C. Inculpatory evidence
   D. Exculpatory evidence

8. The Computer Analysis and Response Team (CART) is a unit of which government agency?

   A. USSS
   B. FBI
   C. CIA
   D. ICE

9. Which of the following acts established the Department of Homeland Security and mandated that the United States Secret Service establish Electronic Crime Task Forces nationwide?

   A. Health Insurance Portability and Accountability Act
   B. Children's Online Privacy Protection Act
   C. The PROTECT Act
   D. The USA PATRIOT Act

10. Which of the following statements is not true about Regional Computer Forensics Laboratories (RCFLs)?

    A. RCFLs can be used by criminal defense lawyers.
    B. The establishment of RCFLs has been sponsored by the FBI.
    C. RCFLs not only are used for investigations, but also provide computer forensics training.
    D. RCFLs exist in both the United States and Europe.

FILL IN THE BLANKS

1. A(n) _____ is a set of steps used to solve a problem.
2. Computer _____ is the use of digital evidence in a criminal investigation.
3. Computer _____ is the prevention of unauthorized access to computers and their associated resources.
4. A defendant can prove his innocence with the use of _____ evidence.
5. The process of scrambling plain text into an unreadable format using a mathematical formula is called _____.
6. The world's largest international police organization is called _____.
7. Short-term, volatile memory, the contents of which disappear when a computer is powered down, is called _____ access memory.
8. A(n) _____ is a device used to capture the information stored in the magnetic strip of an ATM, credit, or debit card.
9. A(n) _____ server delivers HTML documents and related resources in response to client computer requests.
10. _____ is a public-private agency of the FBI, which promotes the exchange of information between the private and public sectors on issues related to terrorism, intelligence, and security matters.

PROJECTS

Investigate a Crime

You are a computer forensics investigator in local law enforcement and have been assigned to a criminal investigation. The suspect, Michael Murphy, worked as the director of product development for a computer software company. He was questioned about a number of expensive international telephone calls. Further inspection of his telephone records revealed that he had been calling a software development competitor based in China with offices here in the United States. When confronted, he stated that he would need to consult with his lawyer and had no further comment. He did not show up for work the next day. The local authorities were contacted the following day. Murphy was caught trying to board a one-way flight to Beijing two days after being questioned about his contact with a competitor. At the airport, TSA officials discovered a bag filled with CDs, three SATA hard drives, and five USB thumb drives.

Detail the types of digital evidence you will need for this investigation.

Research Employment Prospects for Computer Forensics Investigators

Describe why the need for computer forensics examiners will be in demand over the coming years. Include in your answer statistics detailing the growth of certain crimes.

Research Federal Agencies

Create an organizational chart detailing all of the federal agencies involved in computer forensics. Begin with the Department of Homeland Security at the top, and then provide the name of each agency and include its computer forensics unit name where appropriate.

Chapter 2

Windows Operating and File Systems

Learning Outcomes

After reading this chapter, you will be able to understand the following:

- What an operating system is;
- What binary, decimal, and hexadecimal are and how to convert from each notation;
- The physical structure of a hard drive and how files are stored and retrieved;
- The booting process;
- The Windows file systems; and
- The different features of each Windows operating system and their implications on investigations.

Introduction

A strong foundation in operating systems is an important building block in becoming a highly effective computer forensics investigator. The evidence that computer forensics investigators work with are files. The organization of these files, the data they contain, and their locations will vary according to the operating system and associated file system that exists on the suspect's computer or digital device. Moreover, the type of operating system and file system will determine the way that digital evidence is acquired and analyzed in terms of both software and hardware. A **file system** is a hierarchy of files and their respective directories.

This chapter begins by outlining the important concept of logical versus physical storage, which is important when discussing how we all view files on our computers through File Explorer on a PC versus how files are actually physically stored on a hard drive. A file on a computer is merely a physical impression on a metal platter, as you will learn later in this chapter. Therefore, computer scientists represent the underlying data on the hard drive in a number of ways—sometimes in binary format or hexadecimal or decimal. This chapter explains these various numbering systems in detail and shows you how to translate from one numbering system to another. This is important because most computer

forensics analysis tools give you a "natural" view of the file but also enable the investigator to view a hexadecimal view of the file, to reveal far more information about the file (the file header, metadata, and other helpful information).

An understanding of operating systems is also important because different types and versions of operating systems have different features, and knowing these features will assist the investigator in understanding where on the computer the most valuable evidence resides and what tools to use. Moreover, most computer forensics imaging tools give the investigator access to a variety of operating system files; the examiner must be familiar with them and be able to explain them.

When analyzing evidence from a hard disk drive, the computer forensics software displays files associated with the booting up process (when the computer is powered on). Therefore, the investigator should be familiar with these files. In fact, an investigator should be familiar with both system and user files and should be able to account for changes to these files. This is the case for all computing devices. For example, a defense attorney may state that some file changes occurred from when the suspect last used a computer, and the investigator must account for these changes.

The chapter continues by outlining all of the file systems that are supported by Windows operating systems. This is key because the type of file system impacts the value of the evidence and the investigator's ability to view that evidence. For example, FAT12 files are not encrypted, whereas NTFS files can possess strong encryption and be unreadable. Nevertheless, a FAT12 file has a lot less valuable metadata than an NTFS file, and file backups are generally more probable than with FAT12. Therefore, understanding the characteristics of each file system is important for the investigator.

A recurring theme throughout this book is the importance of placing the suspect behind the keyboard and re-creating the events leading up to a crime. File Registry in Windows records any kind of configuration change to a system, which opens a tremendous wealth of information related to a user's wireless connections and Internet activity. Therefore, we delve into Windows' File Registry to see what information we can ascertain about a suspect or victim.

The chapter then discusses the file systems supported by Microsoft. The type of file system determines the way files are stored and retrieved in memory. Moreover, the file system defines the limits on file size. The evidentiary value of a file will differ from file system to file system. There are a multitude of reasons for this. For example, the longevity of a file can vary; deleting a file on a Macintosh computer is a different process than deleting a file on a Windows personal computer running NTFS. Metadata, or the attributes of a file, is often critical to associating a criminal with evidence, but the nature of this evidence differs from one file system to another. Encryption is yet another variable, and it generally becomes a more difficult proposition for forensic examiners to contend with as vendors continue to improve the quality of their file systems' security.

A file system is also responsible for determining allocated and unallocated storage space. **Allocated storage space** is the area on a volume where a file or files are stored. When a file on a personal computer is deleted, it is not physically erased from the volume (disk) but now becomes available space. When a file is deleted, it is still physically stored on a volume. However, that space is now available to be overwritten. This available file storage space is referred to as **unallocated storage space**. Users can look

to certain tools to securely delete a file. There are, however, search methods that a forensic examiner can use to check to see if a secure delete tool has been used. Unallocated storage space can generally be used to create a primary partition on a volume. A **partition** is a logical storage unit on a disk. In computer forensics, we often hear this notion of physical versus logical when it comes to file storage or files retrieved from a computer or media storage. Therefore, it is critical for an investigator to know the difference and be able to explain that difference to nontechnical people.

Physical and Logical Storage

Understanding the physical and logical storage aspects of file systems is important because computer forensics imaging software provides a very different view of the data stored on a computer. Forensic imaging software is also known as bit-stream imaging software because it captures every bit stored on a computer's hard drive. Unlike Microsoft's Windows File Explorer, forensic imaging software displays every file stored in a computer's memory, including files from the operating system.

Physical versus *logical* can also refer to the difference between how the operating system refers to the location of a sector and the physical location of a sector on a disk relative to the storage media. Physical storage is discussed in greater detail later in this chapter.

File Storage

An investigator should understand how files on a computer are stored. With this understanding comes the realization that users cannot determine the physical location of where a file is stored and, therefore, cannot control the deletion of that file evidence from a hard drive. File storage and recording is largely controlled by the operating system.

A **byte** is comprised of 8 bits and is the smallest addressable unit in memory. A **sector** on a magnetic hard disk represents 512 bytes, or 2048 bytes on optical disks. More recently, some hard drives contain 4096 byte sectors. Usually a disk has bad sectors, which computer forensics software can identify. A **bad sector** is an area of the disk that can no longer be used to store data. Bad sectors can be caused by viruses, corrupted boot records, physical disruptions, and a host of other disk errors. A **cluster** is a logical storage unit on a hard disk that contains contiguous sectors. When a disk volume is partitioned, the number of sectors in a cluster is defined. A cluster can contain 1 sector (512K) or even 128 sectors (65,536K). **Tracks** are thin, concentric bands on a disk that consist of sectors where data is stored. Computer forensic tools allow the investigator to easily navigate to specific sectors on a disk image, even if a sector is part of the operating system. Figure 2.1 shows the physical layout of a hard disk.