Michael G. Solomon, K Rudolph,
Ed Tittel, Neil Broom, and Diane Barrett

Computer Forensics JumpStart

2nd Edition

The Best First Step Toward a Career in Computer Forensics

SYBEX SERIOUS SKILLS.

Computer Forensics JumpStart

Second Edition

Computer Forensics JumpStart

Second Edition

Michael G. Solomon
K Rudolph
Ed Tittel
Neil Broom
Diane Barrett

Wiley Publishing, Inc.

Acquisitions Editor: Agatha Kim
Development Editor: Stef Jones
Technical Editor: Neil Broom
Production Editor: Dassi Zeidel
Copy Editor: Sara E. Wilson
Editorial Manager: Pete Gaughan
Production Manager: Tim Tate
Vice President and Executive Group Publisher: Richard Swadley
Vice President and Publisher: Neil Edde
Book Designer: Judy Fung
Compositor: James D. Kramer, Happenstance Type-O-Rama
Proofreader: Publication Services, Inc.
Indexer: Nancy Guenther
Project Coordinator, Cover: Katherine Crocker
Cover Designer: Ryan Sneed
Cover Image: © Tetra Images / Getty Images

Published simultaneously in Canada

ISBN: 978-0-470-93166-0
ISBN: 978-1-118-06757-4 (ebk.)
ISBN: 978-1-118-06765-9 (ebk.)
ISBN: 978-1-118-06764-2 (ebk.)

10 9 8 7 6 5 4 3 2 1

Dear Reader,

Thank you for choosing *Computer Forensics JumpStart, Second Edition*. This book is part of a family of premium-quality Sybex books, all of which are written by outstanding authors who combine practical experience with a gift for teaching.

Sybex was founded in 1976. More than 30 years later, we're still committed to producing consistently exceptional books. With each of our titles, we're working hard to set a new standard for the industry. From the paper we print on, to the authors we work with, our goal is to bring you the best books available.

I hope you see all that reflected in these pages. I'd be very interested to hear your comments and get your feedback on how we're doing. Feel free to let me know what you think about this or any other Sybex book by sending me an email at `nedde@wiley.com`. If you think you've found a technical error in this book, please visit `http://sybex.custhelp.com`. Customer feedback is critical to our efforts at Sybex.

Best regards,

Neil Edde
Vice President and Publisher
Sybex, an Imprint of Wiley

To begin with, I'd like to welcome Mary Kyle to our merry band, and to thank her for bull-dogging this project in fine fashion. Thanks also to Kim Lindros, Agatha Kim, Jeff Kellum, and the rest of the Sybex/Wiley gang. Dearer to my heart, I'd like to thank my lovely wife, Dina, and my son, Gregory, for once again putting up with the old man when he's in the throes of creating and finishing another book. You two make everything else worthwhile, and I'm really looking forward to a fun, frenetic, and distraction-free holiday season. Best to one and all, and thanks to our readers who provide the justification for all this learning and hard work. May it do much good, and very little harm!

—Ed Tittel

To God, who has richly blessed me in so many ways, and to my wife and best friend, Stacey.

—Michael G. Solomon

To Richard Kane

—K Rudolph

To my mother, you gave me everything. I love you.

—Neil Broom

Acknowledgments

The authors of this book are a sizable and rowdy crowd, including Michael G. Solomon, Diane Barrett, K Rudolph, Neil Broom, and Ed Tittel. We'll start off by thanking each other for hanging together, rather than separately, in compiling this second edition. Next, we'd like to thank our able and capable project managers, Mary Kyle Inks and Kim Lindros, both of whom help herd the rest of us cats across the finish line. To our Waterside agent, Carole Jelen, who help put the deal together and shot trouble whenever and wherever she saw it: Thanks, and keep up the good work! After that, it's time for the folks at Sybex/Wiley to take a bow and accept our thanks, too: Agatha Kim, our intrepid acquisitions editor; Stef Jones, our masterful development editor; Jenni Housh, our editorial assistant and Jill of all processes and procedures; Dassi Zeidel, our amazing production editor; as well as Pete Gaughan, our dazzling editorial manager. We're sure there are plenty of others we would be thanking, if only we knew their names and roles. Please accept this shout out, in lieu of something more personal and informed. Believe it or not, we are quite grateful! And finally, to all the vendors who contributed software, hardware, and even the rights to reproduce screenshots or photographs: Thanks for creating the technologies that helped to make this book possible, and we hope also, its contents useful. We literally could not have done it without you.

—Ed Tittel

Thanks to the wonderful team that made this a fun and productive project. Mary did an outstanding job of managing the flow of tons of content and materials, as well as managing the authors and editors. Our technical editor, Neil, made all of our work better through his insightful comments and suggestions. And finally, Ed and K are both outstanding authors who make it all look easy. I'd love to work with this team again.

—Michael G. Solomon

This book would not have been possible without the support of Mary Kyle, Michael G. Solomon, Ed Tittel, Neil Broom, John B. Ippolito, Sam Carter, and Richard Kane. I am deeply grateful for their fantastic suggestions and unbelievable patience. I am fortunate and happy to be surrounded by such great people.

—K Rudolph

Thank you to my aunt, Jeanne Starnes, for your great advice, help, and love throughout the years. Special thanks to Gary Harbin for showing me how to build my first computer—look what you started. Bryan Bain, Lee Ann Bain, David Klukowski, Kenny Wilkins, and Doug Moore, you all made my first IT job great. Thank you for helping me get started in the field. Thanks to Brad Reninger and Will Dean for working so hard every day to make TRC successful. Your professionalism, dedication, and friendship are what make the company great. It is always a pleasure to work with legal professionals as dedicated as Jennifer Georges, Brian Saulnier, Hank Fellows, and Christine Tenley. Shauna Waters, thank you for always being upbeat and for teaching me how to sell. Thanks to the wonderful people at Intelligent Computer Solutions, especially Ezra Kohavi, Gonen Ravid, San Casas, Karen Benzakein, and Viviana Meneses, who help me stay on the cutting edge of new technology in this ever-changing field. Thank you, Amber Schroader and Shannon Honea at Paraben, for all the support. And finally, thank you to Ted Augustine and Chris Brown at Technology Pathways. Chris, you have been a great friend and a wonderful mentor.

—Neil Broom

About the Authors

Ed Tittel is a 28-year veteran of the IT industry. After spending his first seven years writing code (mostly for database engines and applications), he switched to a networking focus. After working for Excelan/Novell from 1987 to 1994, he became a full-time freelance writer, consultant, and trainer. He has contributed to more than 100 books on a variety of subjects, including the Sybex *CISSP Study Guide, Fifth Edition*, and many *For Dummies* titles. He also blogs regularly for TechTarget.com, and writes for a variety of IT certification-oriented Web sites.

Michael G. Solomon, CISSP, PMP, CISM, GSEC, is a full-time security speaker, consultant, and author specializing in achieving and maintaining secure IT environments. An IT professional and consultant since 1987, he has worked on projects for more than 100 major organizations and authored and contributed to numerous books and training courses. From 1998 to 2001, he was an instructor in the Kennesaw State University's Computer Science and Information Sciences (CSIS) department, where he taught courses on software project management, C++ programming, computer organization and architecture, and data communications. Michael holds an M.S. in Mathematics and Computer Science from Emory University (1998), a B.S. in Computer Science from Kennesaw State University (1987), and is currently pursuing a Ph.D. in Computer Science and Informatics at Emory University. He has also contributed to various security certification books for LANWrights, including *TICSA Training Guide* (Que, 2002) and an accompanying Instructor Resource Kit (Que, 2002), *CISSP Study Guide* (Sybex, 2003), as well as *Security+ Training Guide* (Que, 2003). Michael coauthored *Information Security Illuminated* (Jones & Bartlett, 2005), *Security+ Lab Guide* (Sybex, 2005), *Computer Forensics JumpStart* (Sybex, 2005), *PMP ExamCram2* (Que, 2005) and authored and provided the on-camera delivery of LearnKey's CISSP Prep and PMP Prep e-Learning course.

K Rudolph is the founder and CIO (Chief Inspiration Officer) of Native Intelligence, Inc. She is a Certified Information Systems Security Professional (CISSP) with a degree from Johns Hopkins University. K creates entertaining educational materials that have been presented to more than 400,000 learners and translated into five languages. She has contributed to eight books on security topics including the *Handbook of Information Security*, *Computer Security Handbook*, *System Forensics, Investigation, and Response*, and NIST Special Publication 800–16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. K has presented at numerous conferences, including the Computer Security Institute Security Exchange (CSI SX) Conference, CSI Annual Security Conferences, New York Cyber Security Conferences, and Information Assurance and Security Conferences held by the FISSEA, FIAC, and eGOV. She has been a speaker for Security Awareness Day events held by the Army, Census Bureau, DLA, IHS, IRS, NOAA, NRC, and the government of Johnson County, Kansas. K volunteers with $(ISC)^2$'s Safe and Secure Online program, which brings awareness presentations for 11- to 14-year-olds to local schools. In March 2006, the Federal Information Systems Security Educators' Association (FISSEA) honored K as the Security Educator of the Year. K is interested in just about everything, including contact juggling, mind mapping, storytelling, core work, aviation, teaching analogies, and photography.

Neil Broom is the President and Laboratory Director of Technical Resource Center, Inc. (`www.trcglobal.com`) in Atlanta, Georgia. TRC is the only private lab east of the Mississippi that earned the prestigious ASCLD/LAB accreditation in the field of Digital Evidence (Computer Forensics) from the American Society of Crime Laboratory Directors/Laboratory Accreditation Board as an expert witness, investigator, speaker, trainer, course director, and consultant in the fields of computer forensics, network and computer security, information assurance, and professional security testing. Neil has more than 15 years of experience providing investigative, technical, educational, and security services to the military, attorneys, law enforcement, the health care industry, financial institutions, and government agencies. Neil is a Certified Computer Examiner (CCE), Certified Information Systems Security Professional (CISSP), and Certified Fraud Examiner (CFE). He is a licensed Georgia private detective and private detective instructor. TRC is a licensed Georgia private detective agency. Neil has presented testimony as an expert witness many times. He has also provided training in the fields of computer forensics and information security to more than 3,000 students in the U.S. government, U.S. military, U.S. intelligence agencies, and Fortune 500 companies in the United States and abroad. Neil was the Chairman of the Digital Evidence Subcommittee for the International Association for Identification (IAI) and is a current member of the ASCLD/LAB Delegate Assembly. His past employment includes the U.S. Navy as a submariner, a law enforcement officer for the Gainesville Police Department, system administrator for the S1 Corporation, and a security trainer for Internet Security Systems (now a division of IBM).

Diane Barrett has been involved in the IT industry for about 20 years and has been active in education, security, and forensics for the past 10 years. She holds an M.S. degree in Technology with a specialization in Information Security and will be starting Ph.D. dissertation work shortly. Diane is currently a forensic trainer for Paraben and has been doing contract forensic work for the past several years in the Phoenix area. In addition to developing forensic curriculum for American Military University, she was the program champion for the Technology Forensics program at the University of Advancing Technology. She holds many industry certifications including CISSP, ISSMP, and DCFP. Diane has either coauthored or been the lead author on several computer forensics and security books. She is also a regular committee member for the Conference on Digital Forensics, Security and Law and presenter at Paraben's Forensic Innovations Conference.

Contents

Introduction

Want to know what computer forensic examiners really do? This book covers the essentials of computer forensics, and it's especially designed for those new to the field or who simply wish to learn more about undertaking this type of work. Many news stories and television shows highlight the role of forensic investigators in solving cases. It all seems so exciting, doesn't it? Computer forensics is really not that different from what you see on TV. Although it's quite a bit less glamorous, you'll find similarities in the real world.

After a crime or incident that involves a computer occurs, a specialist trained in computer forensics examines the computer to find clues about what happened. That is the role of the computer forensic examiner. This specialist may work with law enforcement or with a corporate incident response team. Although the rules governing each activity can be dramatically different depending on who your client is, the approach to the investigation remains roughly the same.

This book covers the basic elements, concepts, tools, and common activities to equip you with a solid understanding of the field of computer forensics. Although this book is not a definitive training guide for specific forensic tools, you will learn about the most common tasks that you'll encounter during any investigation. After reading this book, you will be able to participate in investigations and understand the process of finding, collecting, and analyzing the evidence gathered.

A heightened awareness of security in the wake of the attacks on September 11, 2001, has also provided many nontechnical people with an awareness of security issues previously known only in security specialist circles. Computers play a central role in all activities, both legal and illegal. The material in this book can be applied to both criminal investigations and corporate incident response. You don't have to be a member of law enforcement to benefit from the material presented here. Nontechnical people can also benefit from this book because it covers the basic approach computer examiners take in an investigation.

If you like the introduction to computer forensics we present in this book, you can pursue the topic further in several ways. Most major forensic tools vendors offer training on their own products and teach how to use them in investigations. See Chapter 8, "Common Forensic Tools," and Appendix D, "Forensic Tools," for more information. Appendix B, "Forensic Resources," contains many references to resources where you can obtain more information. If you decide to pursue computer forensic certification, Appendix C, "Forensic Certifications and More," provides a list of common certifications and contact information for each. If your job involves computer investigations, this book can help you expand your knowledge and abilities. Keep it handy as a resource as you acquire more experience and knowledge. And good luck with your pursuit!

Who Should Read This Book

Anyone fulfilling, or aspiring to fulfill, the responsibilities of a computer forensic examiner can benefit from this book. Also, if you just want to know more about what computer forensic examiners do, this book will fill you in on the details. The material is organized to provide a high-level view of the process and methods used in an investigation. Both law enforcement personnel and non-law enforcement can benefit from the topics presented here.

Because you are reading this introduction, you must have some interest in computer forensics. Why are you interested? Are you just curious, do you want to start working in computer forensics, or have you just been given the responsibility of conducting or managing an investigation? This book addresses readers in all of these categories.

Although we recommend that you read the book from start to finish for a complete overview of the topics, you can jump right to an area of interest. If you bought this book for a concise list of forensic tools, go right to Chapter 8. But don't forget the other chapters! You'll find a wealth of information in all chapters that will expand your understanding of computer forensics.

What This Book Covers

Chapter 1: "The Need for Computer Forensics" This chapter lays the foundation for the rest of the book. It discusses the need for computer forensics and how the examiners' activities meet the need.

Chapter 2: "Preparation—What to Do Before You Start" This chapter addresses the necessary knowledge you must have before you start. When you finish this chapter, you will know how to prepare for an investigation.

Chapter 3: "Computer Evidence" This chapter discusses computer evidence and focuses on identifying, collecting, preserving, and analyzing evidence.

Chapter 4: "Common Tasks" Most investigations include similar common tasks. This chapter outlines those tasks you are likely to see again and again. It sets the stage for the action items you will use in your activities.

Chapter 5: "Capturing the Data Image" This chapter covers the first functional step in many investigations. You will learn the reason for and the process of creating media images for analysis.

Chapter 6: "Extracting Information from Data" After you have an exact media image, you can start analyzing it for evidence. This chapter covers the basics of data analysis. You will learn what to look for and how to find it.

Chapter 7: "Passwords and Encryption" Sooner or later, you will run into password-protected resources and encrypted files. This chapter covers basic encryption and password issues and discusses how to deal with them.

Chapter 8: "Common Forensic Tools" Every computer forensic examiner needs a toolbox. This chapter covers many popular hardware and software forensic tools.

Chapter 9: "Pulling It All Together" When the analysis is done, you need to present the results. This chapter covers the elements and flow of an investigation report.

Chapter 10: "How to Testify in Court" If your evidence ends up in court, you need to know how to effectively present it. This chapter covers many ins and outs of being an expert witness and presenting evidence in court.

Appendix A: "Answers to Review Questions" Answers to the Review Questions

Appendix B: "Forensic Resources" A list of forensic resources you can use for further research

Appendix C: "Forensic Certifications and More" A list of computer forensic certifications and contact information

Appendix D: "Forensic Tools" A summary list of forensic tools, several of which are discussed in the text, with contact information

Glossary A list of terms used throughout the book

Making the Most of This Book

At the beginning of each chapter you'll find a list of topics that the chapter covers. You'll find new terms (specific terminology) defined in the margins of the pages to help you quickly get up to speed on computer forensics. In addition, several special elements highlight important information:

Notes provide extra information and references to related information.

NOTE

Tips are insights to help you perform tasks more easily and effectively.

TIP

Warnings let you know about things you should—or shouldn't—do as you perform computer investigations.

WARNING

You'll find Review Questions at the end of each chapter to test your knowledge of the material covered. The answers to the Review Questions may be found in

Appendix A. You'll also find a list of Terms to Know at the end of each chapter to help you review key terms introduced in that chapter. These terms are also included in the Glossary at the end of this book.

You'll also find special sidebars in each chapter titled "Tales from the Trenches," written by Neil Broom. These are war stories Neil has acquired throughout his career as a computer forensic examiner. They are written in first person, so you'll really get a sense of what it's like to go "on scene" and get your hands dirty. Enjoy!

How to Contact the Authors

The authors welcome feedback from you about this book or about books you'd like to see in the future. You can reach the authors by writing to them at the addresses below. For more information about their work, please visit their respective Web sites.

Ed Tittel: ed@edtittel.com; learn more about Ed at http://www.edtittel.com.

Michael G. Solomon: michael@solomonconsulting.com; learn more about Michael at http://www.solomonconsulting.com/.

K Rudolph: Kaie@NativeIntelligence.com; learn more about K at www.NativeIntelligence.com.

Neil Broom: nbroom@trcglobal.com; learn more about Neil at www.trcglobal.com.

Sybex strives to keep you supplied with the latest tools and information you need for your work. Please check their Web site at www.sybex.com, where we'll post additional content and updates that supplement this book if the need arises. Enter Computer Forensics in the Search box (or type the book's ISBN—**9780470931660**), and click Go to get to the book's update page.

Chapter 1

The Need for Computer Forensics

In this chapter, you'll learn more about:

- Defining computer forensics
- Understanding corporate forensic needs
- Understanding law enforcement forensic
- Training forensic practitioners
- Training end users
- Assessing your organization's needs

Computer forensics is a fascinating field. As enterprises become more complex and exchange more information online, high-tech crimes are increasing at a rapid rate. The computer forensic industry has taken off in recent years, and it's no surprise that a profession once regarded as a vague counterpart of network security has grown into a science all its own. In addition, numerous companies and professionals now offer computer forensic services as a main line of business.

A computer forensic technician is a combination of a private eye and a computer scientist. Although the ideal background for this field includes legal, technical, and law enforcement experience, many industries as well as government and military organizations use professionals with investigative intelligence and technology proficiency. A computer forensic professional can fill a variety of roles such as private investigator, corporate compliance professional, or law enforcement official.

This chapter introduces you to the concept of computer forensics, while addressing computer forensic needs from two views—corporate policy and law enforcement. It will present some real-life examples of computer crime. It will help you assess your organization's needs and discuss various training methods used for practitioners and end users.

Defining Computer Forensics

computer forensics
Computer investigation and analysis techniques that involve the identification, preservation, extraction, documentation, and interpretation of computer data to determine potential legal evidence.

The digital age has produced many new professions, but one of the most unusual is computer forensics. Computer forensics deals with the application of law to a science. The New Shorter Oxford English Dictionary defines *computer forensics* as "the application of forensic science techniques to computer-based material." In other words, forensic computing is the process of identifying, preserving, analyzing, and presenting digital evidence in a manner that is acceptable in a legal proceeding. At times, it is more science than art; other times, it is more art than science.

Although it is similar to other forms of legal forensics, the computer forensics process requires a vast knowledge of computer hardware, software, and proper techniques to avoid compromising or destroying evidence. Computer forensic review involves the application of investigative and analytical techniques to acquire and protect potential legal evidence; therefore, a professional within this field needs to have a detailed understanding of the local, regional, national, and sometimes even international laws affecting the process of evidence collection and retention. This is especially true in cases involving attacks that may be waged from widely distributed systems located in many separate regions.

intrusion
Any unauthorized access to a computer, including the use, alteration, or disclosure of programs or data residing on the computer.

Computer forensics can also be described as the critical analysis of a computer hard disk drive after an *intrusion* or crime. This is mainly because specialized software tools and procedures are required to analyze, after the fact, the various areas where computer data is stored. Often this involves retrieving deleted data from hard drives and servers that have been subpoenaed to appear in court or seized by law enforcement.

electronic discovery or e-discovery
The process whereby electronic documents are collected, prepared, reviewed, and distributed in association with legal and government proceedings.

During the course of forensic work, you will run into a practice that is called *electronic discovery*, or *e-discovery*. Electronic discovery produces electronic documents for litigation. Data that is created or stored on a computer, computer network, or other storage media are included in e-discovery. Examples of such are e-mail, word-processing documents, plaintext files, database files, spreadsheets, digital art, photos, and presentations. Electronic discovery using computer forensic techniques requires in-depth computer knowledge and the ability to logically dissect a computer system or network to locate the desired evidence. It may also require expert witness testimony to explain to the court the exact method or methods by which the evidence was obtained.

Computer forensics has become a hot topic in computer security circles and in the legal community. It's a fascinating field with far more information available than can be analyzed in a single book, although this book will provide you with an understanding of the basic skills you'll need as a forensic investigator. Key skills in computer forensics are knowing the best places to look for evidence, and knowing when to stop looking. These skills come with time and experience.

In looking at the major concepts behind computer forensics, the main emphasis is on data recovery. To do that you must:

- Identify meaningful evidence
- Determine how to preserve the evidence
- Extract, process, and interpret the evidence
- Ensure that the evidence is acceptable in a court of law

All of these concepts are discussed in great detail throughout this book. Because computer-based information is fragile and can be easily fabricated, the simple presence of incriminating material is not always evidence of guilt. Electronic information is easy to create and store, yet computer forensics is a science that requires specialized training, experience, and equipment.

Real World Scenario

Tales from the Trenches: Why Computer Forensics Matters

A computer forensic examiner might be called upon to perform any of a number of different types of computer forensic investigations.

We have all heard of or read about the use of computer forensics by law enforcement agencies to help catch criminals. The criminal might be a thief who was found with evidence of his crime when his home or office computer was searched, or a state employee who was found to have stolen funds from public accounts by manipulating accounting software to hide funds transfers.

Most of us know that computer forensics is used every day in the corporate business world to help protect the assets and reputation of large companies. Forensic examiners are called upon to monitor the activities of employees, assist in locating evidence of industrial espionage, and provide support in defending allegations of misconduct by senior management.

Government agencies hire computer forensic specialists to help protect the data the agencies maintain. Sometimes, it's as simple as making sure IRS employees don't misuse the access they have been granted to view your tax information by periodically reviewing their activities. Many times, it's as serious as helping to defend the United States to protect the most vital top secret information by working within a counterintelligence group.

Every day, divorce attorneys ask examiners to assist in the review of personal computers belonging to spouses involved in divorce proceedings. The focus of such investigations usually is to find information about assets that the spouse may be hiding and to which the other spouse is entitled.

Continues

More recently, defense attorneys have asked forensic examiners to reexamine computers belonging to criminal defendants. Computer forensic experts have even been asked to reexamine evidence used in a capital murder case that resulted in the defendant's receiving a death sentence. Such reexaminations are conducted to refute the findings of the law enforcement investigations.

Although each of these areas seems entirely unique, the computer forensic examiner who learns the basics, obtains appropriate equipment, follows proper procedures, and continues to educate himself or herself will be able to handle each of these investigations and many other types not yet discussed. The need for proper computer forensic investigations is growing every day as new methods, technologies, and reasons for investigations are discovered.

Computer Crime in Real Life

An endless number of computer crime cases is available for you to read. Most of the crimes presented in the following sections come from the Department of Justice Web site, online at `www.cybercrime.gov`. In these cases, we'll look at several types of computer crime and how computer forensic techniques were used to capture criminals. The cases presented here illustrate some of the techniques that you will learn as you advance through this book. As a forensic investigator, you never know what you may come across when you begin an investigation. As the cases in this section show, sometimes you find more than you could have ever imagined.

Hacker Sentenced for Identity Thefts from Payment Processor and Retail Networks

Alberto Gonzalez, 28, led a hacking and identity theft ring that compromised record-breaking numbers of credit cards. For his part in the crimes, Gonzalez received the longest sentence imposed for criminal hacking to date. In March 2010, in separate cases, U.S. District Court judges sentenced Gonzalez to two 20-year prison terms for hacking into several retail networks and a major payment processor.

Gonzalez committed access device fraud, aggravated identity theft, computer fraud, conspiracy, and wire fraud. He and his associates hacked into major U.S. retailers, including the TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, and Sports Authority. He also led the group that breached the Dave and Buster's restaurant chain electronic payment systems. The second prison sentence, 20 years and one day, was for two counts of conspiracy for assisting others in breaching the networks of card processor Heartland Payment Systems,

supermarket chain, Hannaford Brothers Co. Inc., and nationwide convenience store chain, 7-Eleven.

Between July 2005 and his arrest in May 2008, Gonzalez and his group hacked into retail credit card payment systems by installing sniffer programs that captured payment card numbers used at the stores and by wardriving. Wardriving involves driving around in a car with a laptop computer looking for unsecured wireless computer networks. Gonzalez and his co-defendants stole more than 40 million credit and debit card numbers from major retailers. They sold the numbers and also committed ATM fraud by encoding the stolen data onto blank cards and then withdrawing cash from ATMs.

Gonzalez's ring hid and laundered their fraudulent gains by moving the money through bank accounts in Eastern Europe and using anonymous Internet-based currencies in the United States and abroad.

Gonzalez gave malware to other hackers that enabled them to bypass firewalls and anti-virus programs to break into companies' networks. (Malware is discussed in the Security Awareness section below.) Gonzalez admitted that his assistance allowed his co-conspirators to steal tens of millions of card numbers, adversely impacting hundreds of financial institutions.

In the largest investigation to date of its kind, the U.S. Secret Service worked abroad and in the United States using computer forensics to solve these cases. In July 2007, Secret Service in Turkey worked with Turkish agents to obtain Ukrainian suspect Maksym Yastremskiy's laptop while he danced at a nearby nightclub. After downloading data, U.S. agents returned the computer to Yastremskiy's hotel room. Instead of user names, Yastremskiy's accomplices used secure communication networks with numerical IDs.

Detectives noted Yastremskiy's chats with an American who sold millions of stolen credit card numbers to Yastremskiy. The American used the identity "201679996." The detectives worked with Carnegie Mellon University experts to link the numbers to a Russian e-mail address that belonged to Gonzalez. Ironically, Gonzalez had been working with the Secret Service as a consultant since 2003.

Shortly thereafter, the Secret Service arrested an Estonian hacker and found more than 40 million unsold credit card numbers linked to the break-ins at U.S. companies on two Latvian servers.

For months, Gonzalez hid in the National Hotel where he was living off more than $400,000 cash. He had buried another $1.1 million in the back yard of his parents' house. On May 7, 2008, agents raided Gonzalez's hotel room, condo, and parents' home. Gonzalez was then arrested.

Source: Wired.com, August 17, 2009, `http://www.wired.com/threatlevel/2009/08/tjx-hacker-charged-with-heartland`; **U.S. Department of Justice, Office of Public Affairs,** `http://www.justice.gov/opa/pr/2010/March/10-crm-329.html`.

NOTE

Man Charged with Operating Online Scheme to Steal Income Tax Refunds

In June 2010, Mikalai Mardakhayeu was arrested and charged for his alleged role in an online phishing scam. The international scam was designed to steal U.S. taxpayer income tax refunds. Mardakhayeu is a Belarusian national living in Massachusetts. He was charged with conspiracy and wire fraud.

As alleged in the indictment, in 2006 and 2007, Mardakhayeu and his co-conspirators operated Web sites that offered lower-income taxpayers online tax return preparation and electronic tax return filing services at no cost. The fraudulent Web sites claimed to be authorized by the Internal Revenue Service (IRS). Co-conspirators in Belarus allegedly collected the data entered by taxpayers and then changed the returns so that the legitimate tax refund payments would be redirected to U.S. bank accounts that Mardakhayeu controlled. In some cases, his co-conspirators increased the amount of the claimed refund.

Allegedly, his co-conspirators electronically filed the modified returns with the IRS and various state treasury departments. As a result, the U.S. Treasury and state treasury departments deposited stolen refunds of approximately $200,000 into bank accounts that Mardakhayeu controlled. If convicted, he could be sentenced to 20 years in prison.

NOTE

Source: U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), `http://www.justice.gov/criminal/cybercrime/mardakhayeuIndict.htm`.

In this case, the forensic examiner might have found the files used to create the fraudulent Web sites. If the files were deleted, parts or all of them could have been recovered. Other evidence might include the actual data entered by the victims. The server logs and bank deposit records might have recorded who accessed the accounts. The forensic examiner has a wide variety of tools available to extract data and deleted information.

Newell Rubbermaid Network Hacked for Botnet and Adware Scams

In June 2008, a federal judge sentenced 21-year-old Robert Matthew Bentley to 41 months in prison and payment of $65,000 in restitution for conspiracy and computer fraud. Bentley and others (who are still being investigated) infected hundreds of computers in Europe with adware. The cost to detect and neutralize the adware was tens of thousands of dollars. Bentley and his co-conspirators

were paid for installing the adware through a Western European-based operation called "Dollar Revenue."

The investigation began when the U.S.-based Newell Rubbermaid Corporation and at least one other European-based company reported a computer intrusion against the companies' European networks to the London Metropolitan Police.

This complex, multiyear, international criminal investigation also involved the U.S. Secret Service, the Finland National Bureau of Investigation, London's Metropolitan Police Computer Crime Unit, and the Federal Bureau of Investigation (FBI). Each of these law enforcement organizations detected and responded to botnets of computers secretly controlled by Bentley and his co-conspirators. Evidence was found on computers in Florida that were used in the actual intrusions and to receive payment for placing the adware.

NOTE

See U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), `http://www.justice.gov/criminal/cybercrime/bentleySent.pdf`**. See also "Hacker Pleads Guilty to Computer Fraud" at** `http://pcworld.about.com/od/adware/Hacker-Pleads-Guilty-to-Comput.htm`**.**

This case spanned several countries. National and international law enforcement agencies had to work together to track the illicit computer accesses. By installing the adware and accepting payments, the suspect unwittingly left a trail of forensic evidence. The evidence may have included items such as the parts of the program used to control the botnets.

Former Intel Employee Indicted for Alleged Heist of $1B in Trade Secrets

This case involves employee theft of valuable intellectual property. Stealing and selling proprietary information has become big business. When proprietary information is stolen, a computer forensic investigator may work in tandem with corporate human resources and compliance professionals to help examine not only how the theft occurred, but also provide evidence for prosecution. This case shows that the FBI takes a tough line against stealing data from former employers.

In 2008, Biswamohan Pani, 33, a former Intel employee, was indicted for wire fraud and the theft of more than $1 billion worth of trade secrets from Intel. The stolen information was valued in research and development costs and included mission-critical details about Intel's processes for designing its newest microprocessors. According to the affidavit, Pani told Intel management that he was resigning to work for a hedge fund and that he would use his accrued vacation until his termination date on June 11, 2008.

Pani remained on Intel's payroll through June 11, 2008, but he started work at Intel rival Advanced Micro Devices, Inc. (AMD) on June 2, 2008. From June 8 until June 11, 2008, Pani used his Intel laptop to access Intel's servers and download commercially sensitive data, including more than 100 sensitive documents, 13 of which were classified by Intel as "Top Secret." He also downloaded a document explaining how the encrypted Intel documents could be reviewed from an external hard drive after he left Intel. The indictment also alleged that Pani attempted to access Intel's computer network again two days after his last day at Intel. On July 1, 2008, proprietary Intel documents were located at Pani's home.

During his June 11 exit interview, Pani acknowledged his confidentiality obligations and falsely told Intel that he had returned all of Intel's property, including any documents or computer data.

Per the indictment, AMD personnel neither requested the stolen information nor knew that Pani had taken or would take it. Pani may have planned to use the information to further his career, with or without his employer's knowledge. Both Intel and AMD have assisted the FBI investigation.

If convicted, Pani faces up to 10 years on the trade secret charge, and an additional 20 years on each of the wire fraud counts.

NOTE

See U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), `http://www.justice.gov/usao/ma/Press%20Office%20-%20Press%20Release%20Files/Nov2008/PaniBiswamohanIndictmentPR.html`. **See also *Secure Computing Magazine*, September 18, 2008,** `http://www.securecomputing.net.au/News/123155,amd-worker-charged-with-intel-theft.aspx`.

In this case, computer forensic evidence may include the date and time the files were downloaded as well as access information showing that Pani logged into the Intel servers. Time and date stamps are an important part of the computer forensic process. You will learn about these and other forensic techniques later in the book.

disaster recovery
The ability of an organization to recover from an occurrence inflicting widespread destruction and distress.

best practices
A set of recommended guidelines that outline a set of controls to improve internal and business processes, performance, quality and efficiency.

Figure 1.1 is from the Web site of the Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice (`http://cybercrime.gov`). Here you can find a lot of useful information and additional cases.

The following examples illustrate that computer forensic investigators have no idea where their cases will end up. As a computer sleuth, you may be required to work across state lines and with various agencies. You may end up working with several companies in various countries. You may wind up at a dead end because it takes too long to get the information you need or the employer decides not to prosecute. The computer forensic world is full of surprises.