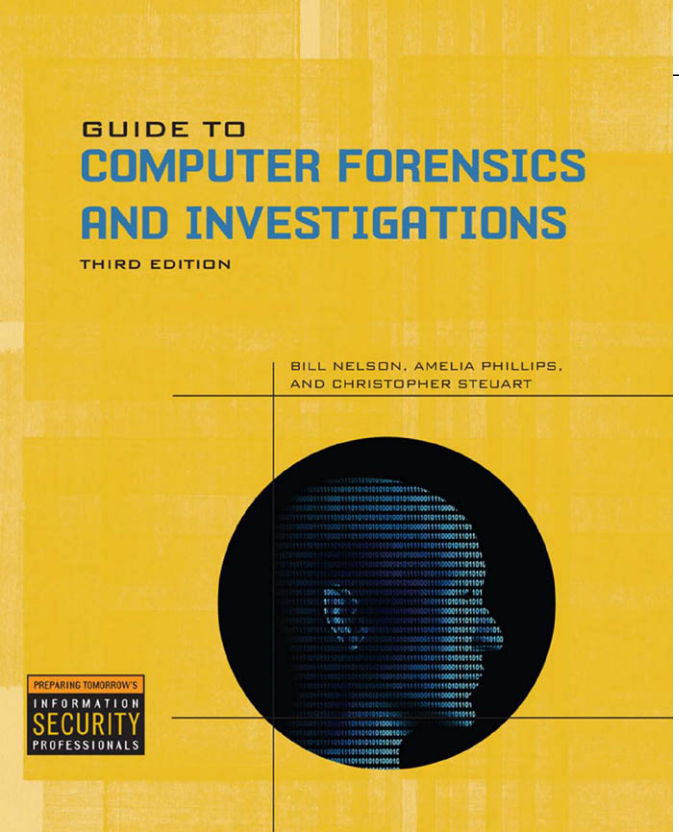
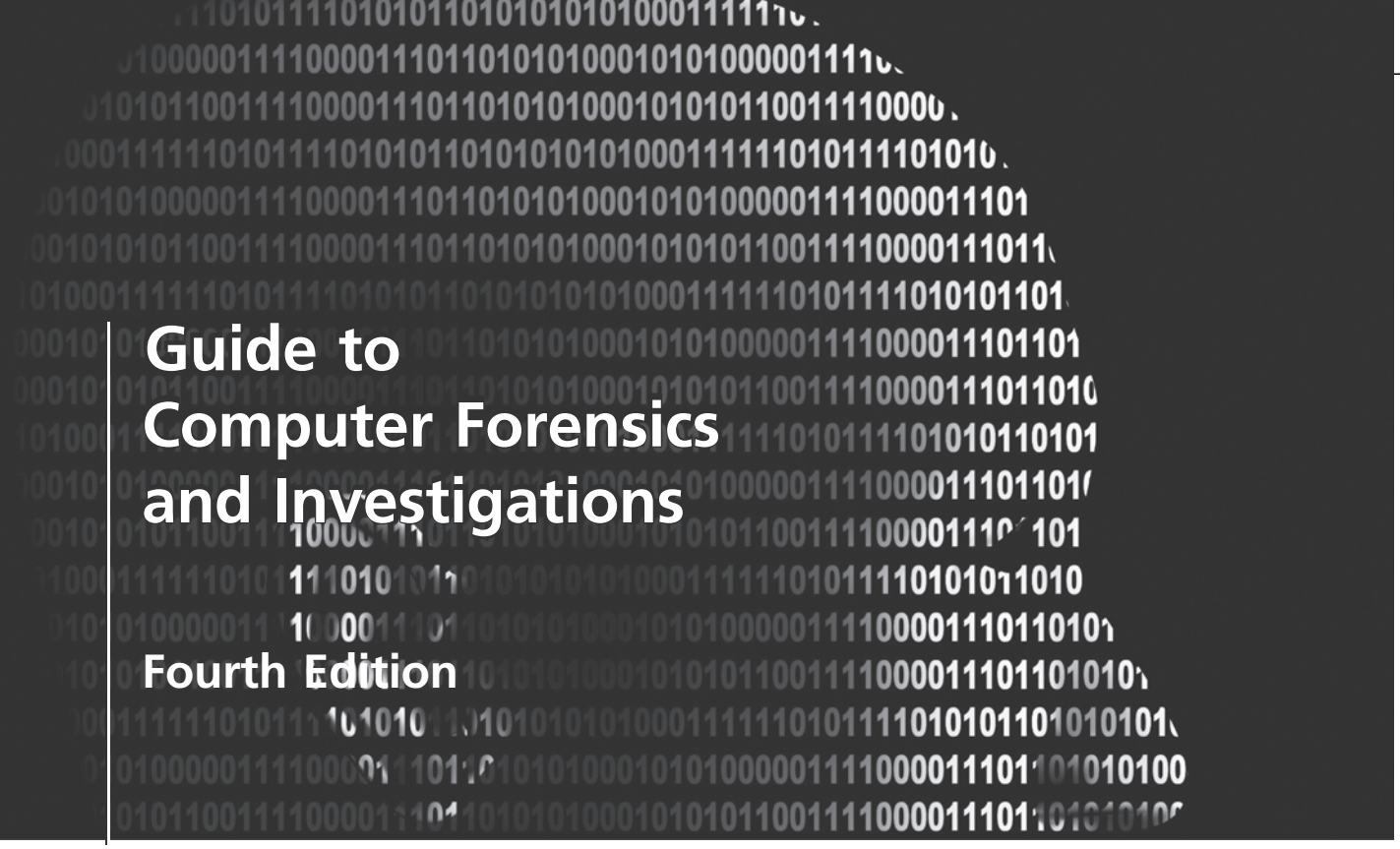

GUIDE TO
COMPUTER FORENSICS
AND INVESTIGATIONS
THIRD EDITION
BILL NELSON, AMELIA PHILLIPS,
AND CHRISTOPHER STEUART
PREPARING TOMORROW'S
INFORMATION
SECURITY
PROFESSIONALS

Information Security Web Site Resources

www.cert.org - Computer Emergency Response Team Coordination Center (CERT/CC)
www.ists.dartmouth.edu - Research and education for cyber security
www.first.org - Organization of 170 incident response teams
www.sans.org - SysAdmin, Audit, Network, Security (SANS) Institute
www.infragard.net - Information sharing between private industry and the U.S. government
www.issa.org - Information Systems Security Association (ISSA)
nsi.org - Information about security vulnerabilities and threats
csrc.nist.gov/index.html - Computer Security Resource Center (CSRC)
cve.mitre.org - Dictionary of reported information security vulnerabilities
www.mcafee.com/us/threat_center - McAfee Threat Center
www.microsoft.com/security/portal/default.aspx - Microsoft Malware Protection Center
secureitalliance.org - Industry partners to promote software that interoperates with Microsoft platform
www.securityfocus.com/archive/1 - Detailed information about the latest computer security vulnerabilities and fixes
atlas.arbor.net - Global threat analysis network
secunia.com - Information regarding security vulnerabilities, advisories, viruses, and online vulnerability tests
www.ieee.org - Institute of Electrical and Electronics Engineers (IEEE)
www.wi-fi.org - Wi-Fi Alliance
www.fcc.gov - Federal Communications Commission
www.hhs.gov/ocr/hipaa - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
www.sec.gov/spotlight/sarbanes-oxley.htm - Sarbanes-Oxley Act of 2002 (Sarbox)
www.ftc.gov/privacy/glbact/glbsub1.htm - Gramm-Leach-Bliley Act (GLBA)
www.fincen.gov/statutes_regs/patriot/index.html - USA Patriot Act (2001)
info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html - California Database Security Breach Act (2003)
www.ftc.gov/bcp/conline/pubs/buspubs/coppa.shtm - Children's Online Privacy Protection Act of 1998 (COPPA)
secunia.com/software_inspector - Secunia Software Inspector software
www.microsoft.com/security/malwareremove/default.mspx - Microsoft Windows Malicious Software Removal Tool
www.microsoft.com/technet/sysinternals/Security/RootkitRevealer.mspx - Microsoft RootkitRevealer software
www.softdd.com/keystrokerecorder/index.html - Keyboard Collector software
irongeek.com/i.php?page=security/thumbscrew-software-usb-write-blocker - Thumbscrew software
www.microsoft.com/windows/products/winfamily/virtualpc/default.mspx - Microsoft Virtual PC 2007
www.vmware.com - Vmware Workstation
www.grc.com/securable - Data Execution Prevention
www.eicar.org/anti_virus_test_file.htm - EICAR Anti
www.microsoft.com/downloads/details.aspx?FamilyID
4e72-bfb5-b84a526c1565&displaylang=en - Micros templates
www.microsoft.com/technet/security/tools/mbsahome Baseline Security Analyzer (MBSA)
www.wireshark.org - Wireshark protocol analyzer
www.netstumbler.com - Netstumbler software
www.klcconsulting.net/smac - MAC spoofing softwar
ophcrack.sourceforge.net - Open-source password c that uses rainbow tables
keepass.info - KeePass password storage software
www.nessus.org/download - Nessus vulnerability sca
www.gfi.com/lannetscan - GFI LANguard vulnerabilit
www.threatfire.com/download - ThreatFire behavior- monitoring tool
md5deep.sourceforge.net - Hash generator software
www.truecrypt.org - TrueCrypt encryption software
www.briggsoft.com - Directory Snoop software
www.heidi.ie/node/6 - File wipe software



Guide to Computer Forensics and Investigations

Fourth Edition

Bill Nelson
Amelia Phillips
Christopher Steuart

COURSE TECHNOLOGY
CENGAGE Learning™

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

COURSE TECHNOLOGY
CENGAGE Learning™

Guide to Computer Forensics and Investigations, Fourth Edition

Bill Nelson, Amelia Phillips, Christopher Steuart

Vice President, Career and Professional Editorial: Dave Garza
Executive Editor: Stephen Helba
Managing Editor: Marah Bellegarde
Senior Product Manager: Michelle Ruelos Cannistraci
Developmental Editor: Lisa M. Lord
Editorial Assistant: Sarah Pickering
Vice President, Career and Professional Marketing: Jennifer McAvey
Marketing Director: Deborah S. Yarnell
Senior Marketing Manager: Erin Coffin
Marketing Coordinator: Shanna Gibbs
Production Director: Carolyn Miller
Production Manager: Andrew Crouth
Content Project Manager: Jessica McNavich
Art Director: Jack Pendleton
Cover photo or illustration: Shutterstock
Production Technology Analyst: Tom Stover
Manufacturing Coordinator: Julio Esperas
Copyeditor: Ruth Bloom
Proofreader: Michele Callaghan
Compositor: Cadmus Communications

Library of Congress Control Number: 2009929885

ISBN-13: 978-1-435-49883-9
ISBN-10: 1-435-49883-6

Course Technology
20 Channel Center Street
Boston, MA 02210

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

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

For your lifelong learning solutions, visit **course.cengage.com**

Visit our corporate website at **cengage.com**.

Printed in the United States of America
1 2 3 4 5 6 7 12 11 10 09

Brief Table of Contents

Table of Contents

Preface

The rapid advance of technology has changed and influenced how we think about gathering digital evidence. Soon after the attacks on the World Trade Center in New York City on September 11, 2001, many young men and women volunteered to serve their country in different ways. For those who did not choose the military, options included positions with law enforcement and corporate security organizations. Ultimately, the combination of a renewed emphasis on homeland security along with the popularity of mainstream television shows, such as *CSI*, *Forensic Files*, and *NCIS*, has created a huge demand for highly educated specialists in the discipline of computer forensics. This demand is now being met by the advent of specialized forensics courses in colleges, universities, and even high schools throughout the United States.

Computer forensics, however, is by no means a new field of endeavor. During the early 1990s, while serving as a Special Agent with the Naval Criminal Investigative Service (NCIS), I realized that personal computers and, more specifically, unsecured personal computers posed a potential threat to national security. I became involved in conducting forensic investigations involving white collar crime, network intrusions, and telecommunications fraud. Recently, the U.S. government has taken significant steps to improve the quality and sophistication of the country's computer forensic capabilities, including the formation of the U.S. Cyber Command (CYBERCOM) in the Department of Defense. Today, most new computer forensics specialists can expect to be involved in a wide variety of investigations, including terrorism counterintelligence, financial fraud issues, intellectual property theft, data security breaches, and electronic data discovery.

The skill sets computer forensics specialists must have are varied. At a minimum, they must have an in-depth knowledge of the criminal justice system, computer hardware and software systems, and

investigative and evidence-gathering protocols. The next generation of "digital detectives" will have to possess the knowledge, skills, and experience to conduct complex, data-intensive forensic examinations involving various operating systems, platforms, and file types with data sets in the multiple-terabyte range.

As time passes, the "hybrid discipline" of computer forensics is slowly evolving into a "hybrid science"—the science of digital forensics. Many colleges and universities in the United States and the United Kingdom have created multidiscipline curriculums that will offer undergraduate and graduate degrees in digital forensics. *Guide to Computer Forensics and Investigations*, now in its fourth edition, has emerged as a significant authoritative text for the computer and digital forensics communities. It's my belief that this book, designed to be used primarily in an academic setting with an enthusiastic and knowledgeable facilitator, will make for a fascinating course of instruction.

Today, it's not just computers that harbor the binary code of 1s and 0s, but an infinite array of personal digital devices. If one of these devices retains evidence of a crime, it will be up to newly trained and educated digital detectives to find the digital evidence in a forensically sound manner. This book will assist both students and practitioners in accomplishing this goal.

Respectfully,

John A. Sgromolo

As a Senior Special Agent, John was one of the founding members of the NCIS Computer Crime Investigations Group. John left government service to run his own company, Digital Forensics, Inc., and has taught hundreds of law enforcement and corporate students nationwide the art and science of computer forensics investigations. Currently, John serves as the senior forensics examiner for digital forensic investigations at Verizon.

Introduction

Computer forensics has been a professional field for many years, but most well-established experts in the field have been self-taught. The growth of the Internet and the worldwide proliferation of computers have increased the need for computing investigations. Computers can be used to commit crimes, and crimes can be recorded on computers, including company policy violations, embezzlement, e-mail harassment, murder, leaks of proprietary information, and even terrorism. Law enforcement, network administrators, attorneys, and private investigators now rely on the skills of professional computer forensics experts to investigate criminal and civil cases.

This book is not intended to provide comprehensive training in computer forensics. It does, however, give you a solid foundation by introducing computer forensics to those who are new to the field. Other books on computer forensics are targeted to experts; this book is intended for novices who have a thorough grounding in computer and networking basics.

The new generation of computer forensics experts needs more initial training because operating systems, computer hardware, and forensics software tools are changing more quickly. This book covers current and past operating systems and a range of computer hardware, from basic workstations to high-end network servers. Although this book focuses on a few forensics software tools, it also reviews and discusses other currently available tools.

The purpose of this book is to guide you toward becoming a skilled computer forensics investigator. A secondary goal is to help you pass the appropriate certification exams. As the field of computer forensics and investigations matures, keep in mind that certifications will change. You can find more information on certifications in Chapter 3 and Appendix A.

Intended Audience

Although this book can be used by people with a wide range of backgrounds, it's intended for those with an A+ and Network+ certification or equivalent. A networking background is necessary so that you understand how PCs operate in a networked environment and can work with a network administrator when needed. In addition, you must know how to use a computer from the command line and how to use popular operating systems, including Windows, Linux, and Mac OS, and their related hardware.

This book can be used at any educational level, from technical high schools and community colleges to graduate students. Current professionals in the public and private sectors can also use this book. Each group will approach investigative problems from a different perspective, but all will benefit from the coverage.

What's New in This Edition

The chapter flow of this book has been revised so that you're first exposed to what happens in a computer forensics lab and how to set one up before you get into the nuts and bolts. Coverage of several GUI tools has been added to give you a familiarity with some widely used software. In addition, Chapter 6 includes new information on interpreting the Windows NTFS Master File Table. The book's DVD includes video tutorials for each chapter that show how to perform the steps in in-chapter activities and explain how to use most of the forensics tools on the DVD. Corrections have been made to this edition based on feedback from users, and all software packages and Web sites have been updated to reflect what's current at the time of publication. A new lab manual is now offered to go with the new fourth edition textbook (ISBN: 1-4354-9885-2).

Chapter Descriptions

Here is a summary of the topics covered in each chapter of this book:

Chapter 1, "Computer Forensics and Investigations as a Profession," introduces you to the history of computer forensics and explains how the use of electronic evidence developed. It also introduces legal issues and compares public and private sector cases.

Chapter 2, "Understanding Computer Investigations," introduces you to tools used throughout the book and shows you how to apply scientific techniques to an investigative case. In addition, it covers procedures for corporate investigations, such as industrial espionage and employee termination cases.

Chapter 3, "The Investigator's Office and Laboratory," outlines physical requirements and equipment for computer forensics labs, from small private investigators' labs to the regional FBI lab. It also covers certifications for computing investigators and building a business case for a forensics lab.

Chapter 4, "Data Acquisition," explains how to prepare to acquire data from a suspect's drive and discusses available command-line and GUI acquisition tools. This chapter also discusses acquiring data from RAID systems and gives you an overview of tools for remote acquisitions.

Chapter 5, "Processing Crime and Incident Scenes," explains search warrants and the nature of a typical computer forensics case. It discusses when to use outside professionals, how to assemble a team, and how to evaluate a case and explains proper procedures for searching and seizing evidence. This chapter also introduces you to calculating hashes to verify data you collect.

Chapter 6, "Working with Windows and DOS Systems," discusses the most common operating systems. You learn what happens and what files are altered during computer startup and how each

system deals with deleted and slack space. In addition, a new section on working with virtual machines has been added.

Chapter 7, "Current Computer Forensics Tools," explores current computer forensics software and hardware tools, including those that might not be readily available, and evaluates their strengths and weaknesses.

Chapter 8, "Macintosh and Linux Boot Processes and File Systems," continues the operating system discussion from Chapter 6 by examining Macintosh and Linux operating systems. It also covers CDs, DVDs, and SCSI, IDE/EIDE, and SATA drives.

Chapter 9, "Computer Forensics Analysis and Validation," covers determining what data to collect and analyze and refining investigation plans. It also explains validation with hex editors and forensics software, data-hiding techniques, and techniques for remote acquisitions.

Chapter 10, "Recovering Graphics Files," explains how to recover graphics files and examines data compression, carving data, reconstructing file fragments, and steganography and copyright issues.

Chapter 11, "Virtual Machines, Network Forensics, and Live Acquisitions" covers tools and methods for acquiring virtual machines, conducting network investigations, performing live acquisitions, and reviewing network logs for evidence. It also examines using UNIX/Linux tools and the Honeynet Project's resources.

Chapter 12, "E-mail Investigations," covers e-mail and Internet fundamentals and examines e-mail crimes and violations. It also reviews some specialized e-mail forensics tools.

Chapter 13, "Cell Phone and Mobile Device Forensics," covers investigation techniques and acquisition procedures for recovering data from cell phones and mobile devices. It also provides guidance on dealing with these constantly changing technologies.

Chapter 14, "Report Writing for High-Tech Investigations," discusses the importance of report writing in computer forensics examinations; offers guidelines on report content, structure, and presentation; and explains how to generate report findings with forensics software tools.

Chapter 15, "Expert Testimony in High-Tech Investigations," explores the role of an expert or technical/scientific witness, including developing a curriculum vitae, understanding the trial process, and preparing forensics evidence for testimony. It also offers guidelines for testifying in court and at depositions and hearings.

Chapter 16, "Ethics for the Expert Witness," provides guidance in the principles and practice of ethics for computer forensics investigators and examines other professional organizations' codes of ethics.

Appendix A, "Certification Test References," provides information on the National Institute of Standards and Technology (NIST) testing processes for validating computer forensics tools and covers computer forensics certifications and training programs.

Appendix B, "Computer Forensics References," lists recommended books, journals, e-mail lists, and Web sites for additional information and further study.

Appendix C, "Computer Forensics Lab Considerations," provides more information on considerations for forensics labs, including certifications, ergonomics, structural design, and communication and fire-suppression systems.

Appendix D, "DOS File System and Forensics Tools," reviews FAT file system basics and explains using DOS computer forensics tools, creating forensic boot media, and using scripts. It also reviews DriveSpy commands and X-Ways Replica.

Features

To help you fully understand computer forensics, this book includes many features designed to enhance your learning experience:

- *Chapter objectives*—Each chapter begins with a detailed list of the concepts to be mastered in that chapter. This list gives you a quick reference to the chapter's contents and is a useful study aid.
- *Figures and tables*—Screenshots are used as guidelines for stepping through commands and forensics tools. For tools not included with the book or that aren't offered in free demo versions, figures have been added to illustrate the tool's interface. Tables are used throughout the book to present information in an organized, easy-to-grasp manner.
- *Chapter summaries*—Each chapter's material is followed by a summary of the concepts introduced in that chapter. These summaries are a helpful way to review the ideas covered in each chapter.
- *Key terms*—Following the chapter summary, a list of all new terms introduced in the chapter with boldfaced text are gathered together in the Key Terms list, with full definitions for each term. This list encourages a more thorough understanding of the chapter's key concepts and is a useful reference.
- *Review questions*—The end-of-chapter assessment begins with a set of review questions that reinforce the main concepts in each chapter. These questions help you evaluate and apply the material you have learned.
- *Hands-on projects*—Although understanding the theory behind computer technology is important, nothing can improve on real-world experience. To this end, each chapter offers several hands-on projects with software supplied with this book or free downloads. You can explore a variety of ways to acquire and even hide evidence. For the conceptual chapters, research projects are provided.
- *Case projects*—At the end of each chapter are several case projects, including a running case example used throughout the book. To complete these projects, you must draw on real-world common sense as well as your knowledge of the technical topics covered to that point in the book. Your goal for each project is to come up with answers to problems similar to those you'll face as a working computer forensics investigator.
- *Video tutorials*—The book's DVD includes audio-video instructions to help with learning the tools needed to perform in-chapter activities. Each tutorial is a .wmv file that can be played in most OSs. The skills learned from these tutorials can be applied to hands-on projects at the end of each chapter.
- *Software and student data files*—This book includes a DVD containing student data files and free software demo packages for use with activities and projects in the chapters. (Additional software demos or freeware can be downloaded to use in some projects.) Four software companies have graciously agreed to allow including their products with this book: Technology Pathways (ProDiscover Basic), AccessData (Forensic Toolkit, Registry Viewer, and FTK Imager), X-Ways (WinHex Demo), and Runtime Software (DiskExplorer for FAT,

DiskExplorer for NTFS, and HDHOST). To check for newer versions or additional information, visit Technology Pathways, LLC at *www.techpathways.com*, AccessData Corporation at *www.accessdata.com*, X-Ways Software Technology AG at *www.x-ways.net*, and Runtime Software at *www.runtime.org*.

Text and Graphic Conventions

When appropriate, additional information and exercises have been added to this book to help you better understand the topic at hand. The following icons used in this book alert you to additional materials:

The Note icon draws your attention to additional helpful material related to the subject being covered.

Tips based on the authors' experience offer extra information about how to attack a problem or what to do in real-world situations.

The Caution icons warn you about potential mistakes or problems and explain how to avoid them.

Each hands-on project in this book is preceded by the Hands-On icon and a description of the exercise that follows.

These icons mark case projects, which are scenario-based assignments. In these extensive case examples, you're asked to apply independently what you have learned.

Instructor's Resources

The following additional materials are available when this book is used in a classroom setting. All the supplements available with this book are provided to instructors on a single CD (ISBN 1435498844). You can also retrieve these supplemental materials from the Cengage Web site, *www.cengage.com*, by going to the page for this book, under "Download Instructor Files & Teaching Tools."

- *Electronic Instructor's Manual*—The Instructor's Manual that accompanies this book includes additional instructional material to assist in class preparation, including suggestions for lecture topics, recommended lab activities, tips on setting up a lab for hands-on projects, and solutions to all end-of-chapter materials.
- *ExamView Test Bank*—This cutting-edge Windows-based testing software helps instructors design and administer tests and pretests. In addition to generating tests that can be printed and administered, this full-featured program has an online testing component that allows students to take tests at the computer and have their exams automatically graded.

- *PowerPoint presentations*—This book comes with a set of Microsoft PowerPoint slides for each chapter. These slides are meant to be used as a teaching aid for classroom presentations, to be made available to students on the network for chapter review, or to be printed for classroom distribution. Instructors are also at liberty to add their own slides for other topics introduced.
- *Figure files*—All the figures in the book are reproduced on the Instructor's Resources CD. Similar to the PowerPoint presentations, they're included as a teaching aid for classroom presentation, to make available to students for review, or to be printed for classroom distribution.

Student Resources

Lab Manual for Guide to Computer Forensics and Investigations (ISBN: 1-4354-9885-2)

- Companion to *Guide to Computer Forensics and Investigations, Fourth Edition*. This lab manual provides students with additional hands-on experience.

Web-Based Labs for Guide to Computer Forensics and Investigations (ISBN: 1-4354-9886-0)

- Using a real lab environment over the Internet, students can log on anywhere, anytime via a Web browser to gain essential hands-on experience in computer forensics using labs from *Guide to Computer Forensics and Investigations, Fourth Edition*.

Lab Requirements

The hands-on projects in this book help you apply what you have learned about computer forensics techniques. The following sections list the minimum requirements for completing all the projects in this book. In addition to the items listed, you must be able to download and install demo versions of software.

Minimum Lab Requirements

- Lab computers that boot to Windows XP
- Computers that dual-boot to Linux or UNIX
- At least one Macintosh computer running Mac OS X (although most projects are done in Windows or Linux/UNIX)
- An external USB, FireWire, or SATA drive larger than a typical 512 MB USB drive

The projects in this book are designed with the following hardware and software requirements in mind. The lab in which most of the work takes place should be a typical network training lab with a variety of operating systems and computers available.

Operating Systems and Hardware

Windows XP or Vista

Use a standard installation of Windows XP Professional or Vista. The computer running Windows XP or Vista should be a fairly current model that meets the following minimum requirements:

- USB ports
- CD-ROM/DVD-ROM drive