INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

ISSA

Digital Forensics, Investigation, and Response

FOURTH EDITION

Chuck Easttom

JONES & BARTLETT
LEARNING

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

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

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

24449-6

Production Credits
VP, Product Management: Christine Emerton
Director of Product Management: Laura Pagluica
Product Manager: Ned Hinman
Tech Editor: Jeffrey Parker
Content Strategist: Melissa Duffy
Content Strategist: Paula Gregory
Project Manager: Kristen Rogers
Senior Project Specialist: Dan Stone
Digital Project Specialist: Rachel DiMaggio
Marketing Manager: Suzy Balk
Product Fulfillment Manager: Wendy Kilborn
Composition: Straive
Cover Design: Briana Yates
Text Design: Kristin E. Parker
Content Services Manager: Colleen Lamy
Media Development Editor: Faith Brosnan
Rights & Permissions Manager: John Rusk
Rights Specialist: Benjamin Roy
Cover Image (Title Page, Part Opener, Chapter Opener): © phyZick/Shutterstock
Printing and Binding: McNaughton & Gunn

Library of Congress Cataloging-in-Publication Data
Names: Easttom, Chuck, author.
Title: Digital forensics, investigation, and response / Chuck Easttom.
Other titles: System forensics, investigation, and response
Description: Fourth edition. | Burlington, Massachusetts : Jones & Bartlett Learning, [2022] | Includes index.
Identifiers: LCCN 2021003216 | ISBN 9781284226065 (paperback)
Subjects: LCSH: Computer crimes—Investigation—Textbooks.
Classification: LCC HV8079.C65 E37 2022 | DDC 363.25/968--dc23
LC record available at https://lccn.loc.gov/20210032166048

Printed in the United States of America
25 24 23 22 21 10 9 8 7 6 5 4 3 2 1

Contents

Preface

Purpose of This Book

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

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

New to This Edition

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

Cloud Labs

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

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

Learning Features

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

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

Audience

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

Dedication

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

About the Author

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

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