Computer Forensics
JumpStart
Second Edition
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,

[Signature]

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 bulldogging 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* xvii

**Chapter 1**  
**The Need for Computer Forensics**  
1

- Defining Computer Forensics 2
- Computer Crime in Real Life 4
- Hacker Sentenced for Identity Thefts from Payment Processor and Retail Networks 4
- Man Charged with Operating Online Scheme to Steal Income Tax Refunds 6
- Newell Rubbermaid Network Hacked for Botnet and Adware Scams 6
- Former Intel Employee Indicted for Alleged Heist of $1B in Trade Secrets 7
- Corporate versus Law Enforcement Concerns 9
  - Corporate Concerns: Detection and Prevention 10
  - Law Enforcement Concerns: Prosecution 12
- Training 14
  - Forensic Practitioners 15
  - End Users 18
- What Are Your Organization’s Needs? 21
- Terms to Know 22
- Review Questions 22

**Chapter 2**  
**Preparation—What to Do Before You Start** 23

- Know Your Hardware 24
- What I/O Devices Are Used? 24
- Check for Unauthorized Hardware 31
- Keep Up with I/O Trends 38
- Know Your Operating System 40
  - Commonly Encountered Operating Systems 40
- Know Your Local File Systems 43
- Maintain Tools and Procedures for Each Operating System and File System 46
- Know Your Limits 48
  - Legal Organizational Rights and Limits 48
  - Search and Seizure Guidelines 49
- Will This End Up in Court? 51
- Develop Your Incident Response Team 51
- Organize the Team 51
- State Clear Processes 52
- Coordinate with Local Law Enforcement 53
Terms to Know ................................... 54
Review Questions ................................. 54

Chapter 3

Computer Evidence 55
What Is Computer Evidence? ................. 56
Incidents and Computer Evidence .......... 56
Types of Evidence ................................ 57
Search and Seizure .............................. 63
Voluntary Surrender ............................ 63
Subpoena ........................................ 64
Search Warrant ................................... 64
Chain of Custody ............................... 65
Definition ........................................ 65
Controls .......................................... 65
Documentation ................................... 69
Admissibility of Evidence in a Court of Law 71
Relevance and Admissibility ................. 71
Techniques to Ensure Admissibility .......... 72
Leave No Trace ................................... 73
Read-Only Image ............................... 74
Software Write Blocker ....................... 74
Hardware Write Blocker ....................... 75
Terms to Know ................................... 76
Review Questions ................................. 76

Chapter 4

Common Tasks 77
Evidence Identification .......................... 78
Physical Hardware ................................ 79
Removable Storage .............................. 81
Documents ....................................... 84
Evidence Preservation ......................... 85
Pull the Plug or Shut It Down? ............... 85
Supply Power As Needed ....................... 87
Provide Evidence of Initial State ............. 88
Evidence Analysis ............................... 90
Knowing Where to Look ....................... 90
Wading through a Sea of Data ............... 92
Sampling Data ................................... 93
Evidence Presentation ......................... 94
Know Your Audience ......................... 94
Organization of Presentation ................. 96
Keep It Simple .................................. 97
Terms to Know ................................... 98
Review Questions ................................. 98
Chapter 5  Capturing the Data Image  99
The Imaging Process ................................. 100
Evidence Collection Order ......................... 101
Evidence Collection Methods to Avoid ............ 101
Preparing Media and Tools .......................... 103
Collecting the Volatile Data ......................... 104
Creating a Duplicate Hard Disk .................... 110
Extracting Data from Personal Portable Devices .. 114
Image and Tool Documentation ..................... 115
Partial Volume Images ............................... 116
Working with Virtual Machines ..................... 118
Imaging/Capture Tools .............................. 119
Utilities ........................................... 120
Commercial Software ............................... 121
PDA, Mobile Phone, and Portable Device Tools 123
Terms to Know .................................... 124
Review Questions .................................. 124

Chapter 6  Extracting Information from Data  125
What Are You Looking For? .......................... 126
Discovering Evidence Using Connectors ............. 126
Network Activity Files ............................... 127
Activity Log Files .................................. 133
E-mail Headers ..................................... 133
Deleted Files ....................................... 137
Attempts at Password Cracking ..................... 138
How People Think ................................... 140
Picking the Low-Hanging Fruit ...................... 142
Hidden Evidence .................................... 143
Metadata ........................................... 143
Steganography ....................................... 144
HTML Documents .................................... 145
Hiding Documents by Changing Names, Properties, or Locations ......................... 146
Hidden Disk Partitions ............................... 146
Covert Channels and Other Hiding Places ........... 146
Trace Evidence ..................................... 147
Terms to Know .................................... 149
Review Questions .................................. 149

Chapter 7  Passwords and Encryption  151
Passwords ........................................... 152
Finding Passwords .................................. 153