Dear Reader,

Thank you for choosing *Mastering Windows® Network Forensics and Investigation, 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 my parents, with thanks for the countless times you have helped me along the way.
—Steve Anson

To Donna, my loving wife and partner for life, for your unwavering love, encouragement, and support.
—Steve Bunting

To my wife Stacy and my sons Finn and Declan, for your loving support, understanding, and most of all your patience. I wouldn’t be where I am without you all.
—Ryan Johnson

To my mother, Geneva Tucker, for introducing me to this digital world and for instilling in me the passion to work hard, while smiling in the face of adversity.
—Scott Pearson
Acknowledgments

Any work of this magnitude requires the hard work of many dedicated people, all doing what they enjoy and what they do best. In addition, many others have contributed indirectly, and without their efforts and support, this book would not have come to fruition. That having been said, there are many people deserving of our gratitude.

Our appreciation goes to our development editor, Mary Ellen Schutz, Gentle Editing LLC, our technical editors Lance Mueller and Rob Lee, and the entire team at Wiley for helping keep us on track and focused on the task at hand. Without them, this book would never have been completed. Finally, we would like to thank Aleksandar Palauzov for helping us test, document, and verify many of the facts and updates in this version of the book.

—The authors

The field of computer crime investigation is constantly evolving to try to address the challenges that come with each new technology, and no individual can keep up with this ever-changing landscape. Just as each case and each new incident require a group effort to address it, so did this project. I would like to thank all of my coworkers, students, teachers, and friends who have worked with me over the years and have shared their knowledge, trust, and insight. The team at Forward Discovery deserves special recognition for their daily contribution to my personal knowledge pool and for the countless times I reached out to them for advice while updating this version of the book. My thanks go to all of my previous coworkers at the former Sytex training group who worked with me to develop my initial understanding of many of the topics presented in this book, as well as to the hundreds of students who taught me as much as I ever taught them. Thanks also to everyone at the P.D. for the opportunities and friendships that you provided. To the agents of the FBI Task Force, the Defense Criminal Investigative Service, and the crew at the U.S. Department of State, Bureau of Diplomatic Security, Office of Antiterrorism Assistance - Cyber Division, I extend my heartfelt appreciation for the mentoring, knowledge, and friendship that you have shown to me. A special thanks goes to my coauthors, for their tireless and exceptional contribution to this project. Finally, I thank Juliet for being my rock in a sea of shifting sands.

—Steve Anson

The study of computer forensics can’t exist within a vacuum. To that extent, any individual examiner is a reflection and product of his instructors, mentors, and colleagues. Through them we learn, share ideas, troubleshoot, conduct research, grow, and develop. Over my career, I’ve had the good fortune of interacting with many computer forensics professionals and have learned much through those relationships. In no particular order, I would like to thank the following for sharing their knowledge over the years: Keith Lockhart, Ben Lewis, Chris Stippich, Grant Wade, Ed Van Every, Raemarie Schmidt, Mark Johnson, Bob Weitershausen, John Colbert, Bruce Pixley, Lance Mueller, Howie Williamson, Lisa Highsmith, Dan Purcell, Ben Cotton, Patrick Paige, John D’Andrea, Mike Feldman, Mike Nelson, Joel Horne, Mark Stringer, Fred Cotton, Ross Mayfield, Bill Spernow, Arnie “A.J.” Jackson, Ed Novreske, Bob Moses, Kevin Perna, Dan Willey, Scott Garland, Erik Miyake, Art Ehuan, Ryan Johnson, Shawn Fleury, Steve Williams, and Scott Pearson.

A special thanks also goes to Steve Anson, who is my fellow author on this project. Steve is a long-standing friend and mentor. He was a super partner in this endeavor, and his contribution to this work is immeasurable.
Last, but by no means least, I would like to acknowledge the contributions by my family. My parents instilled in me, at a very young age, an insatiable quest for knowledge that has persisted throughout my life, and I thank them for it along with a lifetime of love and support. My best friend and loving wife, Donna, encouraged and motivated me long ago to pursue computer forensics. While the pursuit of computer forensics never ends, without her support, sacrifices, motivation, sense of humor, and love, this book would never have been completed.

Thank you everyone.

—Steve Bunting

I hadn’t intended to get into a career in computers. When I was a kid, I wanted to be many things, but never once did I say that I wanted to investigate computer intrusions for a living. I got my first computer in the early ’80s and it was downhill from there.

I wish I could thank all the people in my life who helped to get me where I am now; however, I’m told that I’m not allowed to blow my page count by doing so. So for once in this book, I will be brief.

Thank you to my wonderful, loving, patient, and supportive wife, Stacy, for encouraging me to undertake this project and almost every other worthwhile endeavor I’ve embarked on. Your encouragement, sacrifice, and (sometimes forceful) prodding were instrumental to my being able to complete this process.

Thank you to my son, Finn, for letting me experience the sheer joy with which you engage your surroundings and for teaching me that it’s a lot more fun to eat spaghetti with your hands—and to the BT folks who taught me that that should really be considered more of a metaphor than anything else. Thank you to my son Declan, whose interaction with the world is a sight to behold and a source of constant enjoyment and wonder.

Thank you to Toby Terrill for being the person responsible for my stepping out of the safety of my lab and doing some very gratifying work with the U.S. military in Iraq. Thank you to Chris Chappell for always being there to laugh about the silliness all around us.

Thank you to Ray “NMN” Reyes, Scott Pearson, Lance Mueller, Steve Bunting, Jason Fry, Charles Giglia, Rob Lee, and Jansen Cohoon for never ceasing to entertain my questions and crazy concepts, even in the dead of night and from one side of the world to the other.

—Ryan Johnson

Digital forensics is an exciting field that attempts to satisfy the insatiable addiction for knowledge (and the latest technology) that exists in a very special group of people. I have had the great fortune of being introduced to some really great minds and shockingly interesting personalities who have collectively taught me how to research, but more important, how to think outside of the box—for this is where the bad guys we chase live and operate. Lance Mueller, Steve Bunting, Steve Anson, and Ryan Johnson—it has been a pleasure working with you on this project, and I am humbled that you would allow me into your circle to collaborate on your vision. Thank you for taking that chance when you really didn’t have to.

To my colleagues at the U.S. Department of State, Bureau of Diplomatic Security, Office of Antiterrorism Assistance - Cyber Division—I can’t thank you enough for investing the time and patience to show me the ropes and how to be a true professional in this field. It is because of your efforts that I have the confidence and credibility to even attempt a project such as this.

To my best friend and staunchest critic, Liezel Pearson—thank you for sacrificing your time and patience (and sanity) so that I could be a part of this book. You are the “glue” and I appreciate your countless words of encouragement when I needed them and the swift kicks to the backside when I needed them more.

—Scott Pearson
About the Authors

Steve Anson is currently the managing director of Forward Discovery Middle East (www.forwarddiscovery.com) providing digital forensics, incident investigation, and IT security solutions to clients in the Middle East, Africa, and Asia markets. He is an active instructor for the U.S. Department of State, Bureau of Diplomatic Security, Office of Antiterrorism Assistance - Cyber Division, providing training to law enforcement agencies, prosecutors, and judges around the world. Steve is a former special agent with the Pentagon’s Defense Criminal Investigative Service, where he conducted network investigations involving U.S. military systems. He holds a master’s degree in computer science, as well as numerous industry certifications. As a former contract instructor for the FBI, he taught hundreds of veteran federal agents, state and local police officers, and intelligence agency employees techniques for conducting computer-intrusion investigations. He also founded and supervised a local police department computer crime and information services unit and served as a cyber task force agent for the FBI. He has conducted investigations involving large-scale computer intrusions, counterterrorism, crimes against children, and many other offenses involving the substantive use of computers. Steve can be reached at steveanson@gmail.com.

Steve Bunting is a retired captain with the University of Delaware Police Department, where he was responsible for computer forensics, video forensics, and investigations involving computers. He has more than 35 years of experience in law enforcement, and his background in computer forensics is extensive. Currently, he is a senior forensic consultant with Forward Discovery, Inc., where he is responsible for conducting forensic examinations, electronic discovery planning and processing, investigative consultation, and course development and instruction. He develops courses and instructs for the U.S. Department of State, Bureau of Diplomatic Security, Office of Antiterrorism Assistance - Cyber Division. He is a Certified Computer Forensics Technician (CCFT), EnCase Certified Examiner (EnCE), and an Access Data Certified Examiner (ACE). He was the recipient of the 2002 Guidance Software Certified Examiner Award of Excellence. He holds a bachelor’s degree in applied professions/business management from Wilmington College and a computer applications certificate in network environments from the University of Delaware. He has conducted computer forensic examinations for numerous local, state, and federal agencies on a variety of cases, including extortion, homicide, embezzlement, child exploitation, intellectual property theft, and unlawful intrusions into computer systems. He has testified in court on numerous occasions as a computer forensics expert. He has taught computer forensics for Guidance Software, makers of EnCase, and taught as a lead instructor at all course levels. He has been a presenter at several seminars and workshops, is the author of numerous white papers, and is the primary author of the book EnCase Computer Forensics: The Official EnCE: EnCase Certified Examiner Study Guide, First Edition, Second Edition, and Third Edition. You can reach him at bunting.steve@gmail.com.

Ryan Johnson is a senior forensic consultant with Forward Discovery. He is a former digital forensics examiner for the Durham Police Department in Durham, North Carolina, where he helped develop, equip, and implement their initial digital forensics capability. He left the Durham Police Department in January 2007 to deploy with the U.S. Army to Iraq, where he served as a media exploitation analyst working with the brave men and women of the 25th ID, 1st CAV, and 4th ID. After leaving Iraq, he started with Forward Discovery, where he performs
a variety of tasks including digital forensic examinations, electronic discovery, intrusion
response, security consultations, and course development and instruction. He is an instructor
and course developer with the U.S. Department of State, Bureau of Diplomatic Security, Office of
Antiterrorism Assistance - Cyber Division. He is a Digital Forensics Certified Practitioner (DFCP),
Certified Forensic Computer Examiner (CFCE), EnCase Certified Examiner (EnCE), and Seized
Computer Evidence Recovery Specialist (SCERS). He holds two bachelor’s degrees from Queen’s
University in Kingston, Ontario, Canada, and a master’s degree from Dalhousie University in
Halifax, Nova Scotia, Canada. He has conducted investigations into some of the largest com-
puter network breaches in the United States and abroad and specializes in theft of intellectual
property cases. He can be reached at johnson.ryan67@gmail.com.

Since 2004, Scott Pearson has provided technical training and investigative consultations over-
seas to foreign law enforcement entities, military personnel, and network/system administra-
tors in Antigua and Barbuda, Bahrain, Bangladesh, Colombia, Egypt, Ethiopia, Greece, India,
Indonesia, Jordan, Kazakhstan, Kenya, Malaysia, Morocco, Pakistan, Philippines, Singapore,
Thailand, Trinidad and Tobago, and Turkey. On behalf of the U.S. Department of State, Bureau
of Diplomatic Security, Office of Antiterrorism Assistance - Cyber Division, he has advised and
trained on topics pertaining to computer and mobile device forensics, network forensics, inci-
dent response, network security, Internet-based investigations, and various advanced consul-
tations with emerging technologies. Pearson has helped design and build numerous digital
forensics labs around the world for law enforcement entities in nations that have requested
assistance from the United States government. Scott is also a certifying instructor on the
Cellebrite UFED Logical and Physical Analyzer Mobile Device Forensics tool. From 2006 to 2007,
Scott was also an instructor for the Department of Defense Computer Investigations Training
Academy in Linthicum, Maryland, where he was a member of the Network Intrusions track
and taught courses in advanced network log analysis to analysts from the United States Marine
Corps, Navy, Air Force, and FBI. You can reach him at spearson47@gmail.com.
Contents at a Glance

Introduction .................................................................................................................. xvii

Part 1 • Understanding and Exploiting Windows Networks  .................. 1

Chapter 1 • Network Investigation Overview ......................................................... 3
Chapter 2 • The Microsoft Network Structure ....................................................... 25
Chapter 3 • Beyond the Windows GUI ................................................................. 63
Chapter 4 • Windows Password Issues ............................................................... 85
Chapter 5 • Windows Ports and Services ............................................................ 137

Part 2 • Analyzing the Computer ................................................................. 157

Chapter 6 • Live-Analysis Techniques ............................................................... 159
Chapter 7 • Windows Filesystems ................................................................. 179
Chapter 8 • The Registry Structure ............................................................... 215
Chapter 9 • Registry Evidence ................................................................. 257
Chapter 10 • Introduction to Malware .......................................................... 325

Part 3 • Analyzing the Logs ............................................................... 349

Chapter 11 • Text-Based Logs ................................................................. 351
Chapter 12 • Windows Event Logs ............................................................... 381
Chapter 13 • Logon and Account Logon Events ........................................... 419
Chapter 14 • Other Audit Events ............................................................... 463
Chapter 15 • Forensic Analysis of Event Logs ............................................. 505
## Contents at a Glance

**Part 4 • Results, the Cloud, and Virtualization** ........................................... 537

Chapter 16 • Presenting the Results .................................................. 539
Chapter 17 • The Challenges of Cloud Computing and Virtualization ........ 565

**Part 5 • Appendices** ........................................................................... 597

Appendix A • The Bottom Line............................................................. 599
Appendix B • Test Environments ......................................................... 633

*Index* .................................................................................................... 647
# Contents

*Introduction* ................................................................. xvi

## Part 1 • Understanding and Exploiting Windows Networks .......................... 1

### Chapter 1 • Network Investigation Overview ........................................... 3
- Performing the Initial Vetting ......................................................... 3
- Meeting with the Victim Organization .............................................. 5
- Understanding the Victim Network Information .................................. 6
- Understanding the Incident ............................................................ 8
- Identifying and Preserving Evidence ............................................... 9
- Establishing Expectations and Responsibilities ................................... 11
- Collecting the Evidence ................................................................... 12
- Analyzing the Evidence .................................................................. 15
- Analyzing the Suspect’s Computers ............................................... 18
- Recognizing the Investigative Challenges of Microsoft Networks ......... 21
- The Bottom Line ............................................................................ 22

### Chapter 2 • The Microsoft Network Structure .......................................... 25
- Connecting Computers .................................................................... 25
- Windows Domains .......................................................................... 27
  - Interconnecting Domains ............................................................. 29
  - Organizational Units .................................................................... 34
- Users and Groups ........................................................................... 35
- Types of Accounts .......................................................................... 36
- Groups .......................................................................................... 40
- Permissions ..................................................................................... 44
- File Permissions ............................................................................. 45
- Share Permissions .......................................................................... 48
  - Reconciling Share and File Permissions ....................................... 50
- Example Hack .................................................................................. 52
- The Bottom Line ............................................................................ 61

### Chapter 3 • Beyond the Windows GUI ....................................................... 63
- Understanding Programs, Processes, and Threads ............................. 64
- Redirecting Process Flow .................................................................. 67
  - DLL Injection ............................................................................. 70
  - Hooking ...................................................................................... 74
- Maintaining Order Using Privilege Modes ....................................... 78
- Using Rootkits .............................................................................. 80
- The Bottom Line ............................................................................ 83
## Chapter 4 • Windows Password Issues ................................. 85
- Understanding Windows Password Storage ....................... 85
- Cracking Windows Passwords Stored on Running Systems .... 88
- Exploring Windows Authentication Mechanisms ................ 98
  - LanMan Authentication ........................................... 99
  - NTLM Authentication ............................................. 103
  - Kerberos Authentication ........................................... 108
- Sniffing and Cracking Windows Authentication Exchanges ........ 111
  - Using ScoopLM and BeatLM to Crack Passwords ............ 114
- Cracking Offline Passwords ........................................... 121
  - Using Cain & Abel to Extract Windows Password Hashes ... 122
  - Accessing Passwords through the Windows Password Verifier 126
  - Extracting Password Hashes from RAM ........................ 127
  - Stealing Credentials from a Running System .................... 128
- The Bottom Line ...................................................... 134

## Chapter 5 • Windows Ports and Services............................. 137
- Understanding Ports ................................................... 137
- Using Ports as Evidence .............................................. 142
- Understanding Windows Services .................................... 149
- The Bottom Line ...................................................... 155

## Part 2 • Analyzing the Computer .................................... 157

## Chapter 6 • Live-Analysis Techniques ............................... 159
- Finding Evidence in Memory ......................................... 159
- Creating a Windows Live-Analysis Toolkit ......................... 161
  - Using DumpIt to Acquire RAM from a 64-Bit Windows 7 System 164
  - Using WinEn to Acquire RAM from a Windows 7 Environment 166
  - Using FTK Imager Lite to Acquire RAM from Windows Server 2008 167
  - Using Volatility 2.0 to Analyze a Windows 7 32-Bit RAM Image 169
- Monitoring Communication with the Victim Box ................ 173
- Scanning the Victim System ......................................... 176
- The Bottom Line ...................................................... 178

## Chapter 7 • Windows Filesystems ................................... 179
- Filesystems vs. Operating Systems .................................. 179
- Understanding FAT Filesystems ..................................... 183
- Understanding NTFS Filesystems .................................... 198
  - Using NTFS Data Structures ...................................... 198
  - Creating, Deleting, and Recovering Data in NTFS ............. 205
- Dealing with Alternate Data Streams ................................ 208
- The exFAT Filesystem ................................................ 212
- The Bottom Line ...................................................... 213
## Chapter 8 • The Registry Structure

<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding Registry Concepts</td>
<td>215</td>
</tr>
<tr>
<td>Registry History</td>
<td>217</td>
</tr>
<tr>
<td>Registry Organization and Terminology</td>
<td>217</td>
</tr>
<tr>
<td>Performing Registry Research</td>
<td>228</td>
</tr>
<tr>
<td>Viewing the Registry with Forensic Tools</td>
<td>232</td>
</tr>
<tr>
<td>Using EnCase to View the Registry</td>
<td>234</td>
</tr>
<tr>
<td>Examining Information Manually</td>
<td>234</td>
</tr>
<tr>
<td>Using EnScripts to Extract Information</td>
<td>236</td>
</tr>
<tr>
<td>Using AccessData's Registry Viewer</td>
<td>246</td>
</tr>
<tr>
<td>Other Tools</td>
<td>251</td>
</tr>
<tr>
<td>The Bottom Line</td>
<td>254</td>
</tr>
</tbody>
</table>

## Chapter 9 • Registry Evidence

<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finding Information in the Software Key</td>
<td>258</td>
</tr>
<tr>
<td>Installed Software</td>
<td>258</td>
</tr>
<tr>
<td>Last Logon</td>
<td>264</td>
</tr>
<tr>
<td>Banners</td>
<td>265</td>
</tr>
<tr>
<td>Exploring Windows Security, Action Center, and Firewall Settings</td>
<td>267</td>
</tr>
<tr>
<td>Analyzing Restore Point Registry Settings</td>
<td>276</td>
</tr>
<tr>
<td>Windows XP Restore Point Content</td>
<td>280</td>
</tr>
<tr>
<td>Analyzing Volume Shadow Copies for Registry Settings</td>
<td>284</td>
</tr>
<tr>
<td>Exploring Security Identifiers</td>
<td>290</td>
</tr>
<tr>
<td>Examining the Recycle Bin</td>
<td>291</td>
</tr>
<tr>
<td>Examining the ProfileList Registry Key</td>
<td>293</td>
</tr>
<tr>
<td>Investigating User Activity</td>
<td>295</td>
</tr>
<tr>
<td>Examining the PSSP and IntelliForms Keys</td>
<td>295</td>
</tr>
<tr>
<td>Examining the MRU Key</td>
<td>296</td>
</tr>
<tr>
<td>Examining the RecentDocs Key</td>
<td>298</td>
</tr>
<tr>
<td>Examining the TypedURLs Key</td>
<td>298</td>
</tr>
<tr>
<td>Examining the UserAssist Key</td>
<td>299</td>
</tr>
<tr>
<td>Extracting LSA Secrets</td>
<td>305</td>
</tr>
<tr>
<td>Using Cain &amp; Abel to Extract LSA Secrets from Your Local Machine</td>
<td>306</td>
</tr>
<tr>
<td>Discovering IP Addresses</td>
<td>307</td>
</tr>
<tr>
<td>Dynamic IP Addresses</td>
<td>307</td>
</tr>
<tr>
<td>Getting More Information from the GUID-Named Interface</td>
<td>309</td>
</tr>
<tr>
<td>Compensating for Time Zone Offsets</td>
<td>312</td>
</tr>
<tr>
<td>Determining the Startup Locations</td>
<td>313</td>
</tr>
<tr>
<td>Exploring the User Profile Areas</td>
<td>316</td>
</tr>
<tr>
<td>Exploring Batch Files</td>
<td>318</td>
</tr>
<tr>
<td>Exploring Scheduled Tasks</td>
<td>318</td>
</tr>
<tr>
<td>Exploring the AppInit_DLL Key</td>
<td>320</td>
</tr>
<tr>
<td>Using EnCase and Registry Viewer</td>
<td>320</td>
</tr>
<tr>
<td>Using Autoruns to Determine Startups</td>
<td>320</td>
</tr>
<tr>
<td>The Bottom Line</td>
<td>322</td>
</tr>
</tbody>
</table>