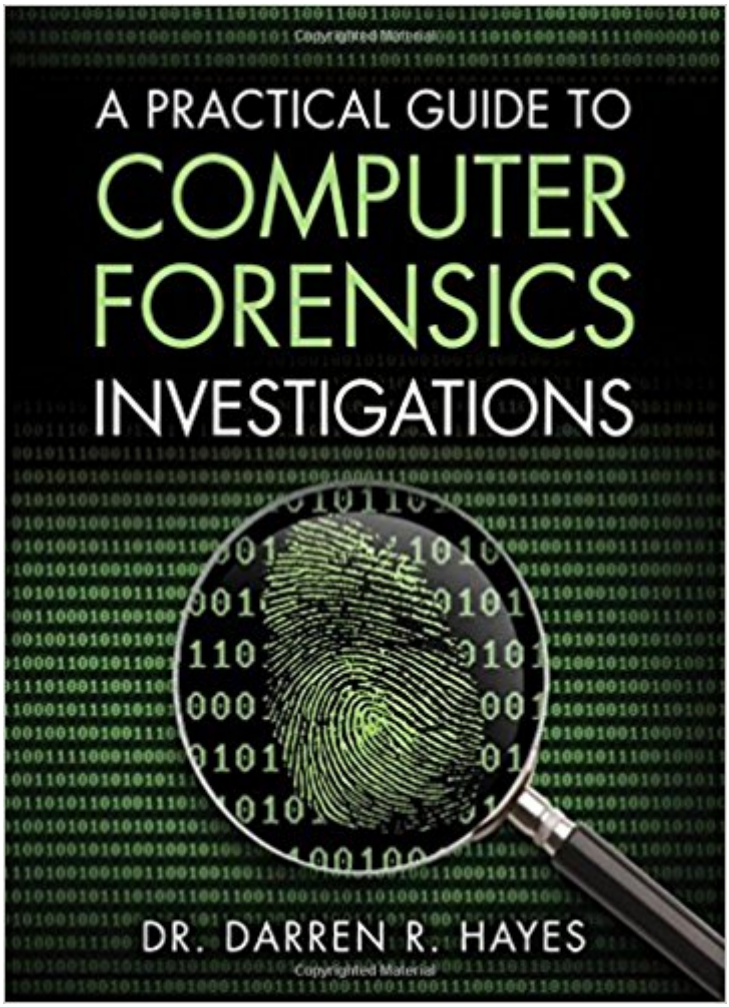
A Practical Guide To Computer Forensics Investigations



Synopsis

All you need to know to succeed in digital forensics: technical and investigative skills, in one book Â Complete, practical, and up-to-date Thoroughly covers digital forensics for Windows, Mac, mobile, hardware, and networks Addresses online and lab investigations, documentation, admissibility, and more By Dr. Darren Hayes, founder of Pace Universityâ ™s Code Detectives forensics labâ “one of Americaâ ™s â œTop 10 Computer Forensics Professorsâ • Perfect for anyone pursuing a digital forensics career or working with examiners Â Criminals go where the money is. Today, trillions of dollars of assets are digital, and digital crime is growing fast. In response, demand for digital forensics experts is soaring. To succeed in this exciting field, you need strong technical and investigative skills. In this guide, one of the worldâ ™s leading computer orensics experts teaches you all the skills youâ ™ll need. Â Writing for students and professionals at all levels, Dr. Darren Hayes presents complete best practices for capturing and analyzing evidence, protecting the chain of custody, documenting investigations, and scrupulously adhering to the law, so your evidence can always be used. Â Hayes introduces todayâ ™s latest technologies and technical challenges, offering detailed coverage of crucial topics such as mobile forensics, Mac forensics, cyberbullying, and child endangerment. Â This guideâ ™s practical activities and case studies give you hands-on mastery of modern digital forensics tools and techniques. Its many realistic examples reflect the authorâ ™s extensive and pioneering work as a forensics examiner in both criminal and civil investigations. Â Understand what computer forensics examiners do, and the types of digital evidence they work with Explore Windows and Mac computers, understand how their features affect evidence gathering, and use free tools to investigate their contents Extract data from diverse storage devices Establish a certified forensics lab and implement good practices for managing and processing evidence Gather data and perform investigations online Capture Internet communications, video, images, and other content Write comprehensive reports that withstand defense objections and enable successful prosecution Follow strict search and surveillance rules to make your evidence admissible Investigate network breaches, including dangerous Advanced Persistent Threats (APTs) Retrieve immense amounts of evidence from smartphones, even without seizing them Successfully investigate financial fraud performed with digital devices Use digital photographic evidence, including metadata and social media images Â

Book Information

Paperback: 600 pages
Publisher: Pearson IT Certification; 1 edition (December 27, 2014)

Language: English
ISBN-10: 0789741156
ISBN-13: 978-0789741158
Product Dimensions: 7 x 1.2 x 9.1 inches
Shipping Weight: 1.8 pounds (View shipping rates and policies)
Average Customer Review: 4.1 out of 5 stars 7 customer reviews
Best Sellers Rank: #289,787 in Books (See Top 100 in Books) #169 inÂ Books > Computers & Technology > Security & Encryption > Privacy & Online Safety #236 inÂ Books > Law > Criminal Law > Forensic Science #431 inÂ Books > Textbooks > Computer Science > Networking

Customer Reviews

Dr. Darren R. Hayes is a leading expert in the field of digital forensics and computer security. He is the director of cybersecurity and an assistant professor at Pace University, and he has been named one of the Top 10 Computer Forensics Professors by Forensics Colleges. Â Hayes has served on the board of the High Technology Crime Investigation Association (HTCIA), Northeast Chapter, and is the former president of that chapter. He also established a student chapter of the HTCIA at Pace University. Â During his time at Pace University, Hayes developed a computer forensics track for the schoolâ ™s bachelor of science in information technology degree. He also created a computer forensics research laboratory, where he devotes most of his time to working with a team of students in computer forensics and, most recently, the burgeoning field of mobile forensics. As part of his research and promotion of this scientific field of study, he has fostered relationships with the NYPD, N.Y. State Police, and other law enforcement agencies. He also organized a successful internship program at the cybercrime division of the New York County D.A. Office and the Westchester County D.A. Office. Â Hayes is not only an academic, howeverâ ”he is also a practitioner. He has been an investigator on both civil and criminal investigations and has been called upon as an expert for a number of law firms. In New York City, Hayes has been working with six to eight public high schools to develop a curriculum in computer forensics. He collaborates on computer forensics projects internationally and has served as an extern examiner for the MSc in Forensic Computing and Cybercrime Investigation degree program at University College Dublin for four years. Â Hayes has appeared on Bloomberg Television and Fox 5 News and been quoted by Associated Press, CNN, Compliance Week, E-Commerce Times, The Guardian (UK), Investorâ ™s Business Daily, MarketWatch, Newsweek, Network World, Silicon Valley Business Journal, USA Today, Washington Post, and Wired News. His op-eds have been published by American Bankerâ ™s BankThink and

The Hillâ ™s Congress Blog. In addition, he has authored a number of peer-reviewed articles in computer forensics, most of which have been published by the Institute of Electrical and Electronics Engineers (IEEE). Hayes has been both an author and reviewer for Pearson Prentice Hall since 2007.

This book is written with extreme eloquence. I find that with many technical books, I find myself having to keep going back and rereading things. However, with this book everything was extremely clear and easy to read and learn. Dr. Hayes goes into great detail and all the information in this book is up to date and current. I highly recommend this book to anybody with an interest in digital forensics.

Whenever I look at buying a book I look at the price of the book after I have flipped through a few pages. I want to know if the object IÃ¢Â Â™m interested in is worth the cost associated with it. Money doesnÃ¢Â Â™t grow on trees but books are made of trees so the riddle goes around and around in my head. I need to know if that $65.00 book is going to bring a me return on investment somehow. Will buying that book make me a better professional or will it bring me enough enjoyment to warrant spending that amount of money? In the case of A practical Guide to Computer Forensic Investigations written by Dr. Darren R. Hayes, the answer is at the end of my review.When I get a technical book I usually read a few pages throughout, bouncing around from chapter to chapter to get a feel for the book and how it was designed before I settle in to read the entire manual. Dr. Hayes didnÃ¢Â Â™t give me that opportunity because the first pages drew me in almost like a mystery novel. I couldnÃ¢Â Â™t put the darn thing down. The only reason I noticed this was because I coughed and saw the time on the clock. I was on page 139 and my highlighter was worn out.Somehow the author managed to entice me with page after page of incredible information that I failed to adhere to my normal reading ritual of bouncing around. And I didnÃ¢Â Â™t even notice until I was on page 139. In that space of time, I switched out highlighters because my orange one dried up with over usage and I lost four hours of sleep. For example, during the Enron Oil scandal of 2001 the employees there shredded thousands of pages of documents but FBI forensic investigators were able to retrieve the equivalent to 10 times the size of the U.S. Library of Congress from hard drives. ThatÃ¢Â Â™s a whole lot of data recovery.HereÃ¢Â Â™s another tidbit: MicrosoftÃ¢Â Â™s COFEE program only works properly if the system is captured live and hasnÃ¢Â Â™t been powered down. This book goes into a large segment of live resident memory data recovery, all written in vivid detail by Dr. Hayes. Did you know that Bitlocker only activates

when the device is shut down or the Bitlocker USB drive is removed? ThatÃ¢Â Â™s how the FBI was able to capture all that data from the recent Silk Road operator. The suspect was at a restaurant with his back to the door when federal agents swept in from behind and grabbed him and his laptop before he knew what happened. His computer was fully logged on and his encryption unlocked.A Practical Guide to Computer Forensic Investigations goes into some of the basics of forensic investigation, as you might expect, but then dives into registry analysis, hard drive composition, file indexing, email event archives and pages after page of incredible information. Dr. Hayes writes long and in-depth about the differences between each version of Windows. He covers how each File Allocation Table (FAT) is different and what the examiner needs to consider based on the OS and update. While this topic alone could easily take up an entire book, Dr. Hayes manages to blanket Linux, and iOS too.This is just the tip of the iceberg. Practical Guide to Computer Forensic Investigations also discusses the differences between media formats and how you need to consider your connections for evidence gathering. Many other forensic books cover this same topic but none do as good of a job as this author does. Wait until you see Dr. Hayes idea of a computer tool kit, besides including a soldering iron and wrenches, I could almost swear I saw a blow torch and a surgical knife. He doesnÃ¢Â Â™t mess around. What kind of doctor is this guy?Most of the software tools mentioned in the book are your typical commercial deep-lined pocket tools. For those of us without fat wallets, the good doctor adds plenty of free or open source tools that do the same thing as the expensive ones. In fact, many of the free tools work better. Dr. Hayes is very serious when he points out that you need to have you own set of tools and know those tools well. You need to know how your tools work before you have to use them in real cases. This may sound like common sense but you donÃ¢Â Â™t want to be called out by a legal team as a sworn expert witness only to have them make you look like an idiot because you didnÃ¢Â Â™t add the Ã¢Â Â“d switch when you ran your acquisition tool.Be aware that some of the information is a bit disturbing because the author made sure to include plenty of real life examples of crimes. Child exploitation, murder and physical harm are cases that have the reader reminded that this isnÃ¢Â Â™t a hobby. The guilt or innocence of someone may rest on your shoulders as an investigator. Dr. Hayes brings up the team concept of working alongside other professionals who are building that case with you. It is your responsibility to conduct your portion of the investigation with as much knowledge as you can offer. This book is a huge part of your knowledge base.Many new devices are part of the evidence collection process. This guide doesnÃ¢Â Â™t linger on just desktop or laptop machines. There is 501 pages of content that ranges from cellular signal interception, SIM card reading, different tablet operating systems, Android forensics, iPhone data analysis, RIM data acquisition,

photo researching, Bluetooth data storage locations and everything in-between. These arenÃ¢Â Â™t merely mentioned as part of a paragraph, they are written about with extensive background information.This guide meets my criteria for a desk top reference book. I donÃ¢Â Â™t have much space on my desk so space is at a premium. I donÃ¢Â Â™t even have room for speakers so I manage (if you want to call it that) my little space based on how often I use a particular object. For books, I only have three books that have made it to a permanent spot on my desk. The other hundreds of books I have are stashed in the book cases above my desk, daring to collapse at any moment. A Practical Guide to Computer Forensic Investigations has earned a coveted spot on my desk. This means I have to get rid of my computer or move another hard drive to the attic. Some people give awards for great books, I give room for great books.So to answer the question of whether the book is worth the price, my answer is no, it is worth twice that amount.

Computer Forensics Investigations covers many different specialty areas including legal, documentation and technical procedures which need to be accurately followed in order to achieve a successful investigation. This book is an excellent source which covers many if not all of these key areas. It should be part of every Computer Forensic student’s book collection as well as in Computer Forensic Labs. The non-working link only reflects one "Let’s Get Practical" exercise which DOES NOT make the book useless. This seems to be a publisher oversight which I’m sure will get corrected soon. Don’t let this stop you from getting this book. Even if that link never work at all, the book is still a must have in my opinion.

Excellent Book! I feel like I learned a lot of secret information from reading this book and hopefully it stays a secret and only Computer forensics professionals find out! This book tells you everything you need to know about Computer Forensics and probably even more than the average person should know about how to investigate mobile devices and computers.If you’re serious about investigating a computer or mobile device this book is for you, just be sure to follow the chain of custody that the book tell you about to preserve evidence from the time its collected to the time it is presented in court otherwise your evidence will be inadmissible in court. Happy Reading!

This is surely a very interesting book but it seems I bought it to early. There is lot of digital content needed for the book, the book tells you to register it and download the content by "Click on the ’Access Bonus Content’ link". However there is no such link. I have other books registered at PearsonITcertification, and some of them have that link, but not Computer Forensics Investigation.

Without being able to download the digital content you are not able to do all the "Let's get Practical!" exercises in the book - making this book useless :(I will update my critics here if there are any news in this matter.

Excellent resource for both new and experienced Computer Forensic Examiners. A very nice blend of different key areas within digital forensics.

Average, but what did you expect?

A Practical Guide to Computer Forensics Investigations Guide to Computer Forensics and Investigations (with DVD) Computer Forensics: Investigating File and Operating Systems, Wireless Networks, and Storage (CHFI), 2nd Edition (Computer Hacking Forensic Investigator) The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics Forensic Science: Fundamentals and Investigations (Forensic Science, Fundamentals and Investigations) 1st Grade Computer Basics : The Computer and Its Parts: Computers for Kids First Grade (Children's Computer Hardware Books) Incident Response & Computer Forensics, Third Edition (Networking & Comm - OMG) Computer Forensics: Investigating Network Intrusions and Cybercrime (CHFI), 2nd Edition Computer Forensics Sex-Related Homicide and Death Investigation: Practical and Clinical Perspectives, Second Edition (Practical Aspects of Criminal and Forensic Investigations) Practical Crime Scene Processing and Investigation, Second Edition (Practical Aspects of Criminal and Forensic Investigations) Practical Homicide Investigation: Tactics, Procedures, and Forensic Techniques, Fifth Edition (Practical Aspects of Criminal and Forensic Investigations) Practical Aspects of Interview and Interrogation, Second Edition (Practical Aspects of Criminal and Forensic Investigations) Forensic Pathology, Second Edition (Practical Aspects of Criminal and Forensic Investigations) Computer Science for the Curious: Why Study Computer Science? (The Stuck Student's Guide to Picking the Best College Major and Career) Forest Forensics: A Field Guide to Reading the Forested Landscape Quick Reference to Adult and Older Adult Forensics: A Guide for Nurses and Other Health Care Professionals Holt McDougal Science: Forensics and Applied Science Experiments Student Guide Comfort at Your Computer: Body Awareness Training for Pain-Free Computer Use Crs Computer-Related Syndrome: The Prevention & Treatment of Computer-Related Injuries