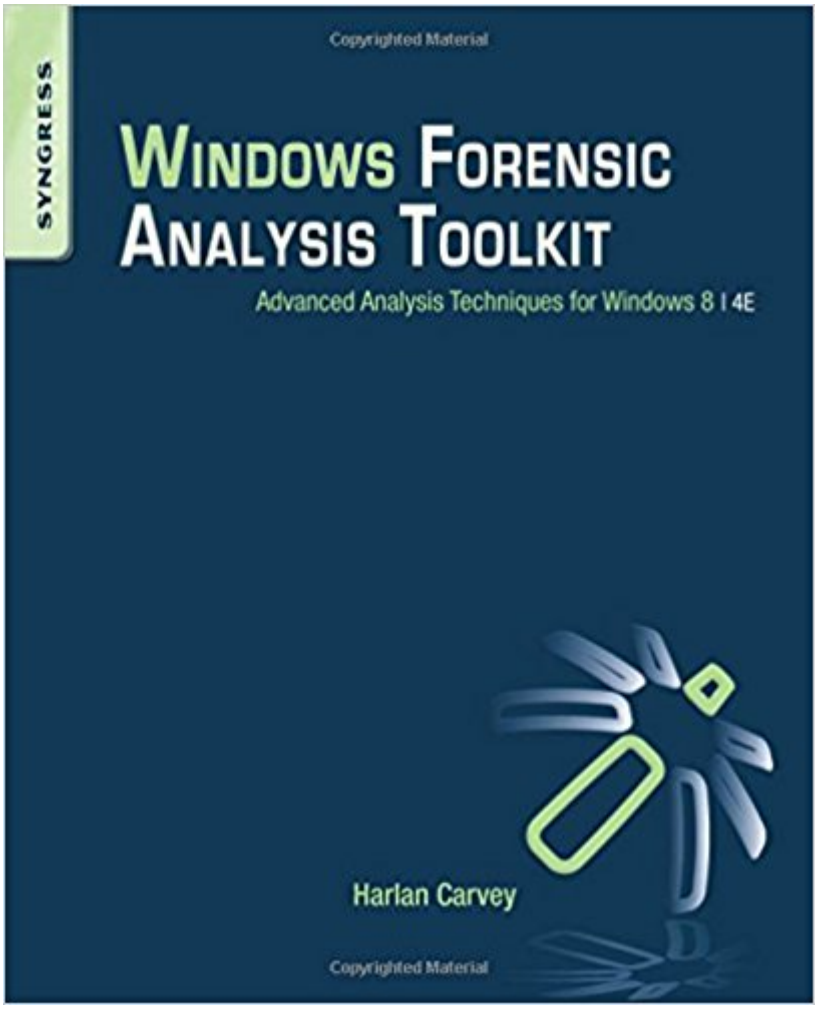
Windows Forensic Analysis Toolkit, Fourth Edition: Advanced Analysis Techniques For Windows 8



Synopsis

Harlan Carvey has updated Windows Forensic Analysis Toolkit, now in its fourth edition, to cover Windows 8 systems. The primary focus of this edition is on analyzing Windows 8 systems and processes using free and open-source tools. The book covers live response, file analysis, malware detection, timeline, and much more. Harlan Carvey presents real-life experiences from the trenches, making the material realistic and showing the why behind the how. The companion and toolkit materials are hosted online. This material consists of electronic printable checklists, cheat sheets, free custom tools, and walk-through demos. This edition complements Windows Forensic Analysis Toolkit, Second Edition, which focuses primarily on XP, and Windows Forensic Analysis Toolkit, Third Edition, which focuses primarily on Windows 7. This new fourth edition provides expanded coverage of many topics beyond Windows 8 as well, including new cradle-to-grave case examples, USB device analysis, hacking and intrusion cases, and "how would I do this" from Harlan's personal case files and questions he has received from readers. The fourth edition also includes an all-new chapter on reporting. Complete coverage and examples of Windows 8 systems Contains lessons from the field, case studies, and war stories Companion online toolkit material, including electronic printable checklists, cheat sheets, custom tools, and walk-throughs

Book Information

Paperback: 350 pages
Publisher: Syngress; 4 edition (April 10, 2014)
Language: English
ISBN-10: 0124171575
ISBN-13: 978-0124171572
Product Dimensions: 7.5 x 0.8 x 9.2 inches
Shipping Weight: 1.5 pounds (View shipping rates and policies)
Average Customer Review: 4.3 out of 5 stars 15 customer reviews
Best Sellers Rank: #158,881 in Books (See Top 100 in Books) #143 inÃ Â Books > Law > Criminal Law > Forensic Science #185 inÃ Â Books > Textbooks > Computer Science > Operating Systems #323 inÃ Â Books > Computers & Technology > Operating Systems

Customer Reviews

"... this book is well written and easy to readÃ¢â ¬Â¦has some material of interest to expertsÃ¢â ¬Â"--Computing Reviews, Windows Forensic Analysis Toolkit, 4th Edition "...technical detail is extensive here and those realworld examples mentioned earlier are worked through in

intricate detail. You will definitely want to try this at homeÃ¢â ¬Â¦" -Network Security, Nov 2014

Harlan Carvey is a senior information security researcher with the Dell SecureWorks Counter Threat Unit - Special Ops (CTU-SO) team, where his efforts are focused on targeted threat hunting, response, and research. He continues to maintain a passion and focus in analyzing Windows systems, and in particular, the Windows Registry.Harlan is an accomplished author, public speaker, and open source tool author. He dabbles in other activities, including home brewing and horseback riding. As a result, he has become quite adept at backing up and parking a horse trailer. Harlan earned a bachelorÃ¢â ¬â„¢s degree in electrical engineering from the Virginia Military Institute, and a masterÃ¢â ¬â„¢s degree in the same discipline from the Naval Postgraduate School. He served in the United States Marine Corps, achieving the rank of captain before departing the service. He resides in Northern Virginia with his family.

I must state at the onset - This is a great digital forensics book.This book as both an knowledge-builder and go-to desk-reference is a formidable and useful work. It is very well written and well attributed. If i had to take one book about Windows 8 with me to Bezerkistan in order to complete an WIN 8 digital forensics mission. This Windows Forensics Analysis Tool Kit - is it.I admire Harlan’s technical forensics skills, understanding about limitations the forensics practice and his excellence in writing. This is a "must have" for digital forensics professionals. If you are in the digital forensics - business - get this book - read it - use it.

I am a fan of Harlan’s books and we even carry them in the SANS bookstore at conference events as recommended reading by SANS instructors. His last book "Windows Forensic Analysis: Advanced Analysis Techniques for Windows 7" was a wonderful rewrite and included many new artifacts found on Windows 7 including jumplists, volume shadow copy, and many new registry keys.This new book, is basically a reprint of his previous book based on Windows 7 with some brief mentions of Windows 8 artifacts. Harlan does mention this fact even in the book, but I feel the title is a bit misleading especially if you have a copy of his previous book.If you have already purchased his 3rd edition book, I would pass on this book until more Windows 8 artifacts are detailed in full. Having read the book in full including the last two new chapters, it does include some brief new artifacts for Windows 8, but not enough to warrant spending the money to update your library at this point.The book is great if the majority of your analysis is on Windows 7 systems. If you don’t have a copy of the 3rd edition, then this book is a great addition to your forensics library. However, due the

the misleading title "Advanced Analysis Techniques for Windows 8," I cannot rate the version of the book any higher.

Needed a technical reference to assist with server performance, troubleshooting and cyber security use.

Decent foundation for Windows Forensics, but there isn’t any information about new artifacts in Windows 8.1. It’s mostly just updated paths from Windows 7. So if you want a good foundation, this is a good book, but you won’t really learn much about Windows 8+.

Purchased for college course.

Great book.

I had to buy this book for a third/fourth-year forensics course, the one where we perfect the collection of evidence and the writing digital forensics reports. I would like to give this book four-and-a-half stars for information, but I deducted over a star for the editing errors. I do not know what it is about computer manuals, but of all the books I have had to read during the last seven years of school--including books on accounting, criminal justice, psychology, math, English literature, creative writing, and humanities--the computer manuals sit at the very bottom regarding grammar and punctuation. The glaring errors make it very hard for me to concentrate.One might think this is a trivial concern, but in fact grammar is exceedingly important to a computer forensic major. We have to match pronouns to antecedents. We have to know about the possessive gerund. We must understand where commas go and understand the difference between colons and semicolons. We have to avoid certain tenses of being, staying mostly in direct past tense. We cannot use first-person speech. We must avoid contractions, and so on. While some of these directives can be ignored in the writing of textbooks and manuals, such as using contractions and even using the first person, a computer forensic professional must adhere to the basics of good grammar. The author and line editors of this book did not match pronouns to antecedents, and they did not use possessive nouns in front of gerunds. They used semicolons where colons would have gone. And I cannot even go into the misuse of comma placement. For one example of the grammar usage in this book, I have written verbatim a sentence on page 37 of the text:"The two primary concerns during an incident with respect to logs are, where they are located and what’s in

them--both of which can have a significant impact on the outcome of your incident response activities."The comma after "are" makes no sense unless the editor inserted a comma after "incident." The m-dash is oddly used, almost as if the first comma put the author and editors at odds at what punctuation to use for the afterthought to the sentence. The usage of the pronoun "your" is overtly colloquial for a textbook. I could even let the usage of "your" go, as this author enjoys the colloquial speech, but the punctuation errors throughout the book reduce the tone's effectiveness. Just because someone is using a friendly tone does not mean that awkward punctuation is any easier to take. This sentence is one of many, many sentences in the book that is clumsily written.I think the author is a brilliant person, and I certainly will be using his techniques. I just wish that he and the other computer professionals in the field of manual writing would dare the expense of hiring professional textbook editors.This being said, I would recommend this book for personal information. I would not recommend the book as it is written now for class usage and hope future editions are edited more stringently.

While this book is an updated version of 3e (author mentions this) with some artifacts for win 8 it is still a great read. The last two chapters which focus on how to's and writing reports has been of great help and i plan to use the template to better organize my reporting format. Speaking of structures, i like that the book focuses on explaining the artifact structures, relevance and when you could use the tool applicable to parse the artifact. This also applies to the process methodology laid out in the book, i like the example of "why scan the machine twice with the same AV if it didn't find anything in the first place?" i have seen too many cases like this in real life. Also defining analysis goals before starting analysis is something i have been stressing on my self and my teammates and Harlan does a good job laying that out.The concept of using micro timelines is great and i have found success applying this technique for finding pivot points rather than taking a kitchen sink approach and creating a supertimeline, not to say the supertimeline doesnt have its place :) it does but not all scenarios require one.In closing, if you haven't picked up the 3e pick this one up, if you are new to digital forensics and incident response, pick this one up. having the textbook version helps as you can reference the material quicker and its easier on the eyes when it comes to screenshots and quoted text for ch.7 (timelines), i had a hard time reading these with the 3e ebook.

7) Windows Registry Forensics, Second Edition: Advanced Digital Forensic Analysis of the Windows Registry Windows 10: The Best Guide How to Operate New Microsoft Windows 10 (tips and tricks, 2017 user manual, user guide, updated and edited, Windows for beginners) Windows 10: The Best Guide How to Operate New Microsoft Windows 10 (tips and tricks, user manual, user guide, updated and edited, Windows for beginners) Windows 10: The Ultimate 2017 Updated User Guide to Microsoft Windows 10 (2017 updated user guide, tips and tricks, user manual, user guide, Windows 10) Windows 10 Manual and Windows 10 User Guide (Windows 10 Guide for Beginners) Windows 10: User Guide and Manual: Microsoft Windows 10 for Windows Users The Production Manager's Toolkit: Successful Production Management in Theatre and Performing Arts (The Focal Press Toolkit Series) The Technical Director's Toolkit: Process, Forms, and Philosophies for Successful Technical Direction (The Focal Press Toolkit Series) The Assistant Lighting Designer's Toolkit (The Focal Press Toolkit Series) The Don't Get Me Started! Toolkit - Workbook and Teacher Answer Key: Strategies for a Culturally-Challenged World (The Don't Get Me Started! Toolkit - Workbook and Teacher Key) (Volume 1) Practical Homicide Investigation: Tactics, Procedures, and Forensic Techniques, Fifth Edition (Practical Aspects of Criminal and Forensic Investigations) Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations Forensic Analysis and DNA in Criminal Investigations and Cold Cases Solved: Forensic Science Forensic Science: An Introduction to Scientific and Investigative Techniques, Fourth Edition Forensic Pathology, Second Edition (Practical Aspects of Criminal and Forensic Investigations) The Sponsorship Seeker's Toolkit, Fourth Edition (Business Books) Forensic Psychological Assessment in Practice: Case Studies (International Perspectives on Forensic Mental Health) Forensic Science: Fundamentals and Investigations (Forensic Science, Fundamentals and Investigations)