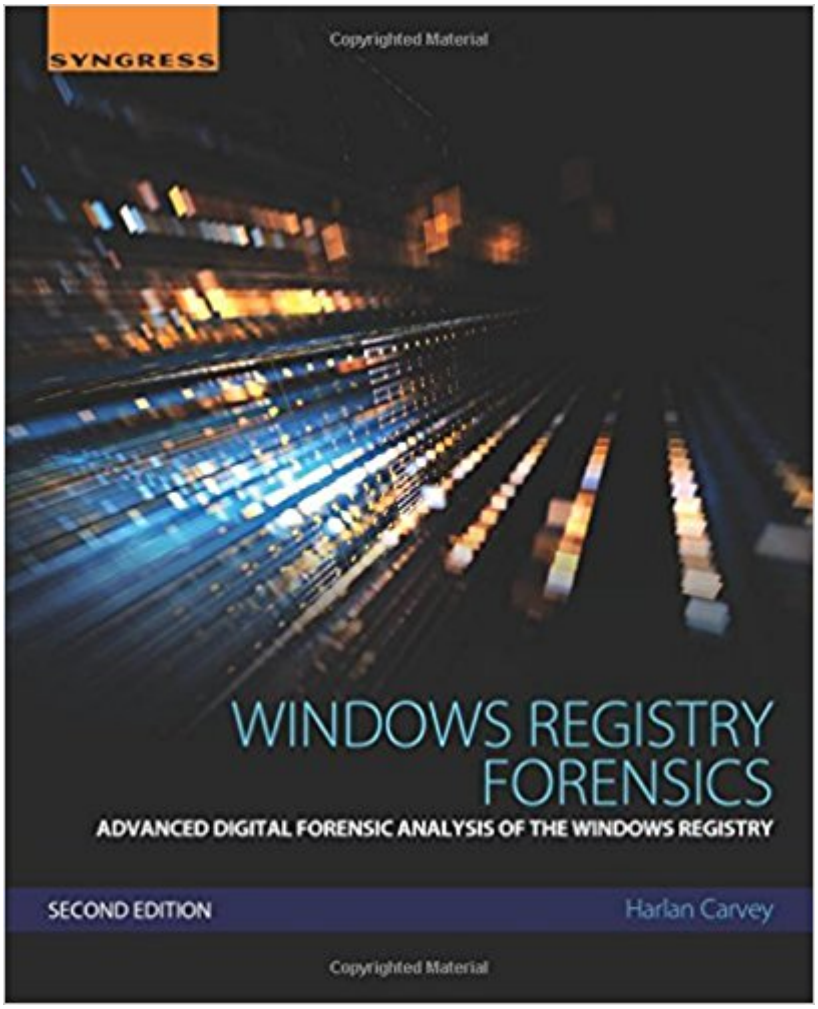
Windows Registry Forensics, Second Edition: Advanced Digital Forensic Analysis Of The Windows Registry



Synopsis

Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry, Second Edition, provides the most in-depth guide to forensic investigations involving Windows Registry. This book is one-of-a-kind, giving the background of the Registry to help users develop an understanding of the structure of registry hive files, as well as information stored within keys and values that can have a significant impact on forensic investigations. Tools and techniques for post mortem analysis are discussed at length to take users beyond the current use of viewers and into real analysis of data contained in the Registry. This second edition continues a ground-up approach to understanding so that the treasure trove of the Registry can be mined on a regular and continuing basis.Named a Best Digital Forensics Book by InfoSec ReviewsPacked with real-world examples using freely available open source toolsProvides a deep explanation and understanding of the Windows RegistryÃ¢â ¬â ¢perhaps the least understood and employed source of information within Windows systemsIncludes a companion website that contains the code and author-created tools discussed in the bookFeatures updated, current tools and techniquesContains completely updated content throughout, with all new coverage of the latest versions of Windows

Book Information

Paperback: 216 pages
Publisher: Syngress; 2 edition (April 8, 2016)
Language: English
ISBN-10: 012803291X
ISBN-13: 978-0128032916
Product Dimensions: 7.5 x 0.5 x 9.2 inches
Shipping Weight: 1.2 pounds (View shipping rates and policies)
Average Customer Review: 4.2 out of 5 stars 27 customer reviews
Best Sellers Rank: #100,657 in Books (See Top 100 in Books) #1 inÃ Â Books > Computers & Technology > Programming > APIs & Operating Environments > Microsoft Windows Registry #84 inÃ Â Books > Law > Criminal Law > Forensic Science #112 inÃ Â Books > Textbooks > Computer Science > Operating Systems

Customer Reviews

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.

The book provides a detailed discussion on the structure of the registry, its keys and relevancy to digital forensics & incident response(DFIR). The author also focuses on presenting examples and use cases on how the reader can leverage information in the registry as part of an analysis. Discussion of tools is given and the tools presented are free and some are open source which you can modify if you understand the programming language they are written to fit your needs. The author dedicates a chapter on regripper a tool that he wrote to parse registry hives and serves as a mini manual. After reading the previous chapters, hopefully the reader will understand the flexibility of the tool and how one can expand functionality. Overall the author does a great job in presenting the information, although short (191 pages) the content is targeted at what can bring value to the reader/analyst. I recommend to all who work in the DFIR field or are starting to. A longer review will be posted on my blog and i will update this review in the future.

Windows Registry Forensics is another excellent installment of Harlan’s continuing research and education efforts relating to Windows forensics. In his previous work,Ã Â Windows Forensic Analysis DVD Toolkit, Second Edition, Harlan covered the broader topic of Windows forensics. While he did cover registry forensics issues in his previous work, this book drills down even deeper into the subject and provides the reader with a comprehensive view of the inner workings of the Windows Registry. If you couple this book with his previous book, you essentially get Windows Forensic Analysis, Second Edition: The Director’s Cut. I recommend this book to anyone who is interested in digital forensics and will be adding it to my "So you’d like to... Learn Digital Forensics" guide.Previous reviewers such as David Nardoni have provided excellent detailed overviews of the individual chapters so I won’t repeat that level of depth for this review. Harlan takes a "teach them to fish" approach in teaching the reader about the Windows Registry. If the reader is expecting a book with a laundry list of interesting Registry keys, they will walk away disappointed. This isn’t to say that there isn’t a tremendous amount revealed about individual keys, but it’s done in the larger context of

Harlan’s efforts to teach the reader about the Registry in a comprehensive manner.The first chapter is where Harlan teaches the reader about fish (the Registry). This chapter explains what the registry is and how to think about it in the context of an examination. The second chapter teachers the reader about the various fishing poles available to them such as Harlan’s own RegRipper tool. The third and fourth chapters is where Harlan takes the reader fishing as he walks the reader through Registry examination using a case study approach.Harlan is an excellent technical writer so the book flows well and the concepts are presented clearly to the reader. The pictures are large enough to show up clearly in the Kindle version of the book which I was grateful for since this is not always the case with Kindle books. My primary complaint with the book is the price especially for the Kindle edition. I don’t expect technical books written for a small audience to be as inexpensive as mass market fiction, but a retail price of $69.95 is pretty steep. As I write this, the price is $62.95 for the physical version and $55.96 for the Kindle version. The price of the Kindle version is especially irritating considering it doesn’t come with the DVD and doesn’t require a physical distribution channel to provide it to me. In most cases (pay attention Syngress), I simply won’t pay that much for a technical book unless it’s something that I know is well written and will provide good value. This is one of those exceptional circumstances. Harlan is one of the few authors who I trust enough to spend that amount of money on for a book.

Helped for some of the reports I was writing at the time, but found more up to date info on the web after some more extensive searches.

Needed a deeper technical reference for server performance and troubleshooting use.

I love this book and I found the information within it very valuable.However the kindle edition of it is lazily programmed. The index and table of contents are very poor, lacking detail, and it is difficult to find sections that you wish to reference.There are no page numbers either, just section numbers.This wouldn’t be such a problem with a print edition which is easy to browse through, but it is not sufficient for an ebook.If this kindle book was easy to navigate it would be indispensible.The content is worth five stars but the poor design of the kindle edition is worth about two. Therefore I will give this edition four stars.

Drills down into depths of Registry.

So far so good. I have 25 years in IT and 6 years as a municipal police officer. It was the forensics direction this book goes that piqued my interest. I may consider a second profession after I retire from IT. I'm fairly versed in courtroom procedures and attorney questioning techniques from my many times on the stand. The early part of the book is a little boring or me since I've been there and done that. I peeked to some of the later pages and saw good stuff coming after the basics. It's nice to read what someone else has experienced.

Windows Registry Forensics, Second Edition: Advanced Digital Forensic Analysis of the Windows Registry Windows Forensic Analysis Toolkit, Fourth Edition: Advanced Analysis Techniques for Windows 8 Windows 10: The Ultimate 2 in 1 User Guide to Microsoft Windows 10 User Guide to Microsoft Windows 10 for Beginners and Advanced Users (tips and tricks, ... Windows, softwares, guide Book 7) The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics 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 Computer Forensics: Investigating File and Operating Systems, Wireless Networks, and Storage (CHFI), 2nd Edition (Computer Hacking Forensic Investigator) Forensic Analysis and DNA in Criminal Investigations and Cold Cases Solved: Forensic Science Forensic Pathology, Second Edition (Practical Aspects of Criminal and Forensic Investigations) The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory Odysseys in Crime Scene Science : Digital Forensics Digital Forensics Practical Homicide Investigation: Tactics, Procedures, and Forensic Techniques, Fifth Edition (Practical Aspects of Criminal and Forensic Investigations) An Introduction to Forensic DNA Analysis, Second Edition Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations Forensic Psychological Assessment in Practice: Case Studies (International Perspectives on Forensic Mental Health) Forensic Science: Fundamentals and Investigations (Forensic Science, Fundamentals and Investigations)

Privacy

FAQ & Help