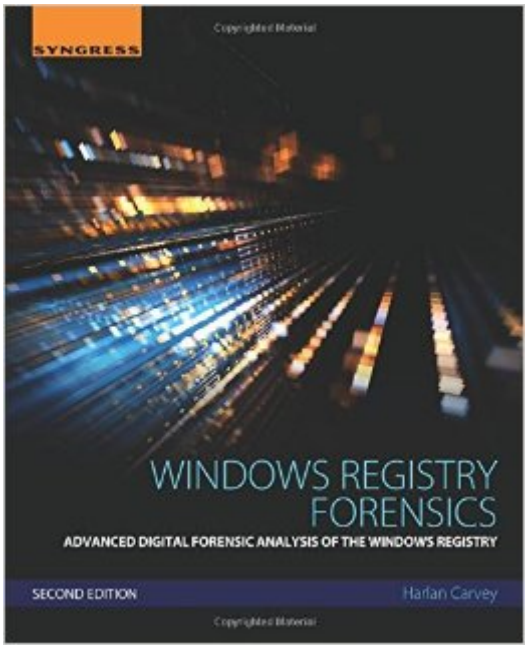
Windows Registry Forensics, Second Edition: Advanced Digital Forensic Analysis Of The Windows Registry



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 Registryâ •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: 4.0 out of 5 starsÂ Â See all reviewsÂ (6 customer reviews)
Best Sellers Rank: #56,027 in Books (See Top 100 in Books) #1 inÂ Books > Computers & Technology > Programming > APIs & Operating Environments > Microsoft Windows Registry #23 inÂ Books > Law > Criminal Law > Forensic Science #169 inÂ Books > Computers & Technology > Security & Encryption

Customer Reviews

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.

There are few DF practitioners I know of (some I know personally) that when a book is written, I buy it without even considering if it will be a good read simply because I know it will be. Harlan's books are in that group of books I know will be worth the money to buy and time to read. Windows Registry Forensics/2E is no different.If for no other reason but to learn to use RegRipper, buy this book. In the DFIR field, books are expensive and by the time you have read a few dozen books and worked dozens (hundreds...) of cases, you have pretty seen most of what you will ever see. So when you find one chapter in a book that makes a difference in the way you work, that makes the book worth it. The RegRipper chapter is one of those chapters for those who 'use' RegRipper but could actually exploit RegRipper to more potential with a few key points laid out in the book.As for me, any book that helps me do something faster, easier, and with more accuracy is worth it. And if any book has just one golden nugget to help me to that, it's a keeper. Just as Harlan's previous books are a keeper, so is this one. I recommend it for any practitioner. Actually, I would not expect that it not be on every practitioner's shelf. When you can get into the mind and theory of someone like Harlan through a book, do it. You won't regret it.

It's an ok book for some. But, I want to see much more detail on making changes and maybe a whole book of nothing but explainations ofeach part of the Binary. And, tons of examples of what changes when the data is altered and what each change makes. Real time effects for actual changes in Windows 7, 8, & 10. XP is over with. A lot of actual examples would be helpful and very useful. This would make for a book Icould really use on a regular basis.

Debugging Courses) Practical Windows Forensics Sorting the Beef from the Bull: The Science of Food Fraud Forensics (Bloomsbury Sigma) Sexual Abuse and the Sexual Offender: Common Man or Monster? (Forensic Psychotherapy Monograph Series) The Spyglass File (The Forensic Genealogist Book 4) Body of the Crime: A Chip Palmer Forensic Mystery Windows 10: Windows10 Mastery. The Ultimate Windows 10 Mastery Guide (Windows Operating System, Windows 10 User Guide, User Manual, Windows 10 For Beginners, Windows 10 For Dummies, Microsoft Office) Windows 10: The Ultimate User Guide for Advanced Users to Operate Microsoft Windows 10 (tips and tricks, user manual, user guide, updated and edited, Windows ... (windows,guide,general.guide,all Book 4) Windows 10: The Ultimate Guide For Beginners (Windows 10 for dummies, Windows 10 Manual, Windows 10 Complete User Guide, Learn the tips and tricks of Windows 10 Operating System) Pix Magazine - Playboy Germany Special Digital Edition - 2016 (German Edition) Echo: The Ultimate Guide to Learn Echo In No Time (Echo, Alexa Skills Kit, smart devices, digital services, digital media) (Prime, internet device, guide) (Volume 6) Echo: 2016 - The Ultimate Guide to Learn Echo In No Time (Echo, Alexa Skills Kit, smart devices, digital services, digital media) (Prime, internet device, guide) Windows 10 Troubleshooting: Windows 10 Manuals, Display Problems, Sound Problems, Drivers and Software: Windows 10 Troubleshooting: How to Fix Common Problems ... Tips and Tricks, Optimize Windows 10) Windows 10: The Ultimate Beginner's Guide How to Operate Microsoft Windows 10 (tips and tricks, user manual, user guide, updated and edited, Windows ... (windows,guide,general,guide,all) (Volume 3) Advanced Oncology Nursing Certification Review and Resource Manual (Second Edition) Large Print SPANISH Word Search Puzzles (Revised Edition No.1) (Large Print SPANISH Word Search Puzzles (Revised Edition Vol 1)) (Volume 1) (Spanish Edition) IntroducciÃ n al procesamiento digital de seÃ ales con dsPIC y C30. Volumen 2 (Spanish Edition) Creatividad y diseÃ o digital. Tercera ediciÃ n (Spanish Edition) IniciaciÃ n a la Quena: GuÃ- a PrÃ¡ctica Para el Principiante Incluye Audios en Formato Digital (Spanish Edition)