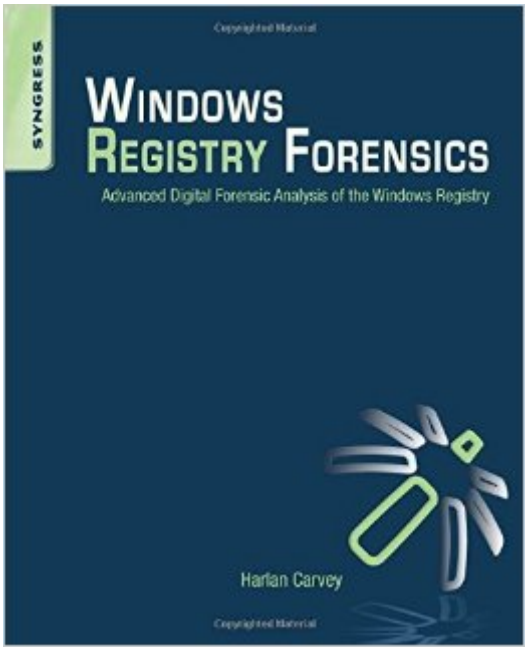
Windows Registry Forensics: Advanced Digital Forensic Analysis Of The Windows Registry



Synopsis

Harlan Carvey brings readers an advanced book on Windows Registry. The first book of its kind EVER -- Windows Registry Forensics provides the background of the Registry to help develop an understanding of the binary structure of Registry hive files. Approaches to live response and analysis are included, and tools and techniques for postmortem analysis are discussed at length. Tools and techniques will be presented that take the analyst beyond the current use of viewers and into real analysis of data contained in the Registry.Packed with real-world examples using freely available open source toolsDeep explanation and understanding of the Windows Registry - the most difficult part of Windows to analyze forensicallyIncludes a CD containing code and author-created tools discussed in the book

Book Information

Paperback: 248 pages

Publisher: Syngress; 1 edition (February 7, 2011)

Language: English

ISBN-10: 1597495808

ISBN-13: 978-1597495806

Product Dimensions: 7.5 x 0.5 x 9.2 inches

Shipping Weight: 1.2 pounds (View shipping rates and policies)

Average Customer Review: 4.4 out of 5 starsÂ Â See all reviewsÂ (18 customer reviews)

Best Sellers Rank: #866,639 in Books (See Top 100 in Books) #5 inÂ Books > Computers & Technology > Programming > APIs & Operating Environments > Microsoft Windows Registry #192 inÂ Books > Computers & Technology > Security & Encryption > Encryption #202 inÂ Books > Computers & Technology > Security & Encryption > Cryptography

Customer Reviews

Windows Registry Forensics is another excellent installment of Harlan’s continuing research and education efforts relating to Windows forensics. In his previous work, 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.

After having read the subtitle -- Advanced Digital Forensic Analysis of the Windows Registry' -- I was a bit surprised to find that this book seems to have its roots in 'the number of analysts ... [who] have no apparent idea of the forensic value of the Windows Registry' as the Preface mentions. This suggests the book is not so much for the advanced analyst, but more of an introduction to the area for those who are not yet proficient in analysing Registry information.Other areas of the book, such as the description of some of the internal structures of the registry, tend to support this. An advanced book would probably not have omitted a description of the security descriptors on registry keys, for example.This is probably not obvious to the buyer -- who is likely to go by the subtitle. I bought the book largely on the strength of the title, myself, and while I'm not disappointed, it's not quite the book I hoped for.To the presumed reader, then, the main value is probably to be found in the two chapters of Case Studies. Here is where the value of the registry in a forensic analysis is most clearly described. These chapters are what beginning registry analysts want to read.The focus of these chapters, though, is on the information in the registry, not where it is located, or to what extent it can be relied on. This is a deliberate decision of the author, and may be sound enugh. It means, though, that the reader is more drawn into using the author's tools, and less into being able to locate the actual keys and values himself with regedit or other tools. In a text for more advanced users, it would have been been a serious error to omit full key/value descriptions; in this type of book, it may lead to more complexity than is strictly warranted.

Four chapters. You might think that with only four chapters the author could in no way write a book that covers Windows registry forensics. I was a bit skeptical at first too but was quickly proven wrong. I've known Harlan for a few years now and I know that his knowledge of the Windows registry is in the 99th percentile when compared to his peers. Do not think of this as a four-chapter book. Think of this as a continuation of the concepts that Harlan presented in Chapter 4 of his

Windows Forensic Analysis DVD Toolkit, Second Edition. With only roughly 100 pages in which to describe the valuable artifacts that reside in the Windows registry, Harlan obviously felt that he needed more room to spread his wing - hence the new book.Chapter 1 provides a very detailed overview of registry analysis. Harlan really wants analysts to first consider the types of information they need prior to starting a forensic exercise. The `what' and `where' of the registry is detailed at great length in addition to its structure. Though this book shows you where to find the registry and some important keys, the author is careful to not present this as the bible of registry information - knowing full well that the minutiae will change from Windows release to Windows release. What this chapter does provide, however, is a good sense of what types of information can be found within the Windows registry. Chapter 2 provides in-depth coverage of several tools to not only conduct forensic investigations on the Windows registry but also how to interact with the registry (both on the target systems and remotely). The author describes tools that he has crated (and that are freely available) in addition to tools and applications from others.

Scientific & Investigative Techniques) Practical Homicide Investigation: Tactics, Procedures, and Forensic Techniques, Fifth Edition (Practical Aspects of Criminal and Forensic Investigations) Advanced Windows: The Developer's Guide to the WIN32 API for Windows NT 3.5 and Windows 95 Real Digital Forensics: Computer Security and Incident Response Handbook of Digital Forensics of Multimedia Data and Devices, Enhanced E-Book (Wiley - IEEE) Wedding Planning - 25 Essentials: The Ultimate Guide for Selecting Dresses, Cakes and Decorations on a Budget (Wedding Planning, Wedding Registry, Wedding ... Rings, Wedding Reception, Getting Married) 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)