



Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry

By Harlan Carvey

Download now

Read Online ➔

Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry By Harlan Carvey

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 tools
- Deep explanation and understanding of the Windows Registry - the most difficult part of Windows to analyze forensically
- Includes a CD containing code and author-created tools discussed in the book

 [Download Windows Registry Forensics: Advanced Digital Foren ...pdf](#)

 [Read Online Windows Registry Forensics: Advanced Digital For ...pdf](#)

Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry

By Harlan Carvey

Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry By Harlan Carvey

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 tools
- Deep explanation and understanding of the Windows Registry - the most difficult part of Windows to analyze forensically
- Includes a CD containing code and author-created tools discussed in the book

Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry By Harlan Carvey **Bibliography**

- Sales Rank: #1064386 in Books
- Brand: Brand: Syngress
- Published on: 2011-02-07
- Released on: 2011-01-24
- Original language: English
- Number of items: 1
- Dimensions: 9.25" h x .51" w x 7.50" l, 1.05 pounds
- Binding: Paperback
- 248 pages

 [Download Windows Registry Forensics: Advanced Digital Foren ...pdf](#)

 [Read Online Windows Registry Forensics: Advanced Digital For ...pdf](#)

Download and Read Free Online Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry By Harlan Carvey

Editorial Review

Amazon.com Review

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 tools
 - Deep explanation and understanding of the Windows Registry--the most difficult part of Windows to analyze forensically
 - Includes a CD containing code and author-created tools discussed in the book
-

An Interview with Harlan Carvey, Author of *Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry*

Why do you feel a book on the Windows Registry is needed?

The Windows Registry is perhaps one of the least understood sources of digital evidence on a Windows system. Unfortunately, bad guys have used specific locations in the Registry to remain persistent on systems a lot longer than many analysts actually realize. I think that what most analysts don't realize is that the Registry is an excellent source of both direct and indirect artifacts.

Don Weber, a friend and fellow IBM alum who's now with InGuardians, was on an engagement where he found that the bad guys were actually storing executable files in binary Registry values. His find makes me wonder how many times this has occurred but not been "seen" because no one was looking.

Intrusions aside, I've also dug into the Registry to perform malware detection. As sometimes happens, malware files will change and avoid detection, but as with malware such as Conficker, some Registry artifacts remained relatively stable across the family. The same has been true for the examinations I've performed that involved Zeus, or Z-bot. Understanding this has allowed me and others to determine that malware was on a system, when multiple AV scans were negative.

Finally, the Registry contains a wealth of time stamped data, that when taken in context, can be extremely valuable to an analyst.

Why do you think so many analysts overlook the Windows Registry as a source of data?

For the most part, I think that most analysts really aren't familiar with the Windows Registry as a source of data. From a purely binary perspective, all the way up to an application-level perspective, I think that most analysts simply aren't familiar with what is and isn't in the Registry, and how the Registry can be used to further a wide range of analysis.

Many times, however, when some analysts have become familiar with the Registry as a source of evidence,

the pendulum swings too far in the other direction. I've seen and received questions along the lines of "where are file copy operations recorded in the Registry?"

As the Windows operating systems become even more sophisticated, analysts who are not actively investigating the Registry now will become completely overwhelmed in very short order.

What is your most memorable experience working in digital forensics?

There've been several, and all of them have been like turning a corner and suddenly being face-to-face with someone really famous. Sometimes it's finding that one artifact that ties everything together, while other times it's been discovering a whole series of artifacts that are essentially a storyboard or script for what the intruder did while on the system. Sometimes you get lucky and find a log file of what the bad guy did . . . sort of a ".bash-history" file, but on Windows. Other times, you end up constructing a timeline of systems activity from multiple data sources both on and off a system, and when you look at your results, you have what amounts to that storyboard.

Across the board, however, I think that most memorable experiences have come from taking a step back, developing a "new" analysis methodology, and then having that methodology succeed in some pretty amazing and spectacular ways.

Review

*"As an experienced security architect?I've been reasonably familiar with the "windows registry" for many years and have frequently used regedit to look at various keys and values (and have sometimes even taken the dangerous steps of changing values!). In my vast library I also have a number of books describing the registry, although I have to say they are somewhat ancient. However, it was not until I read this book I really appreciated the vast amount of information contained in the various registry files. Indeed I was not aware of forensic importance of these files."***--Best Digital Forensics Book in InfoSecReviews Book Awards**

*"It is no exaggeration to say that nearly everything that happens on a Windows system involves the registry?which makes effective examination of the registry absolutely fundamental to good Windows forensics. By devoting a whole book to this critical Windows artifact, Harlan has delivered a much needed resource to everyone doing forensics investigations of Windows systems. What I appreciate about this book, however, is that it is much more than a mere compilation of registry keys important to forensics investigation. This is a book about how to examine the registry, and it is a good one."***--Troy Larson, Principal Forensic Program Manager, Network Security Investigations, Microsoft**

*"Windows Registry Forensics provides extensive proof that registry examination is critical to every digital forensic case. Harlan Carvey steps the reader through critical analysis techniques recovering key evidence of activity of suspect user accounts or intrusion-based malware. Using his extensive experience and research, Harlan's case studies provide behind-the-scenes details that enable every analyst to utilize these techniques immediately in their own investigations. This book is a must have reference for current forensic knowledge of the Microsoft Registry Windows XP through Windows 7 and should become core knowledge for any serious digital forensic investigator."***--Rob Lee, SANS Institute**

"Useful to beginning and intermediate practitioners, but even advanced examiners may find registry information here that they were not previously aware of. Anyone working in digital forensics or incident response who has not made registry examination integral to their process must read and absorb this book. The information is vital to Windows examinations.... Windows Registry Forensics easily succeeds in its

mission to convey the value of integrating registry examination into the forensic process. It provides valuable information relevant to a wide range of investigations. And Mr. Carvey's conversational writing style makes the book easy to read...."--**Digital Forensics Magazine**

"This guide to digital forensics on computers running the Microsoft Windows operating system provides detailed information on the analysis of the Windows registry to detect intrusion and document user actions. The work is divided into three sections beginning with an overview of the registry structure and following with a discussion of registry analysis tools and concluding with an in depth case study of a registry forensics project. Each section includes answers to frequently asked questions and a selection of references for further reading. Illustrations, code examples, tips and warning notes are provided throughout and an accompanying CD-ROM provides copies of registry analysis tools created by the author. Carvey is a computer forensics consultant."--**Book News, Reference & Research**

"As an experienced security architect I've been reasonably familiar with the 'windows registry' for many years and have frequently used regedit to look at various keys and values (and have sometimes even taken the dangerous steps of changing values!). In my vast library I also have a number of books describing the registry, although I have to say they are somewhat ancient. However it was not until I read this book I really appreciated the vast amount of information contained in the various registry files. Indeed I was not aware of forensics importance of these files..... An extremely useful book to a forensics investigator, even an experienced one. I would not hesitate in recommending this book to anyone..."--**InfoSecReviews.com**

From the Back Cover

Harlan Carvey brings you an advanced book on just the Windows Registry – the most difficult part of Windows to analyze forensically. *Windows Registry Forensics* provides the background of the Registry to developing an understanding of the binary structure of Registry hive files. Approaches to live response and analysis are included and tools and techniques for post-mortem 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, and demonstrate the forensic value of the Registry.

- Packed with real-world examples using freely available tools
- Deep explanation and understanding of the Windows Registry
- Includes a CD containing code and author-created tools discussed in the book

Users Review

From reader reviews:

Bobbi Gonzales:

What do you consider book? It is just for students since they are still students or this for all people in the world, what best subject for that? Merely you can be answered for that concern above. Every person has diverse personality and hobby for every single other. Don't to be compelled someone or something that they don't desire do that. You must know how great and important the book *Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry*. All type of book would you see on many options. You can look for the internet solutions or other social media.

Robert Dunham:

What do you about book? It is not important together with you? Or just adding material when you need something to explain what you problem? How about your free time? Or are you busy man or woman? If you don't have spare time to complete others business, it is make you feel bored faster. And you have free time? What did you do? All people has many questions above. They have to answer that question because just their can do this. It said that about reserve. Book is familiar in each person. Yes, it is proper. Because start from on pre-school until university need that Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry to read.

Cheryl Burnett:

In this era globalization it is important to someone to obtain information. The information will make someone to understand the condition of the world. The fitness of the world makes the information easier to share. You can find a lot of sources to get information example: internet, magazine, book, and soon. You will observe that now, a lot of publisher which print many kinds of book. The particular book that recommended for your requirements is Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry this book consist a lot of the information of the condition of this world now. This particular book was represented how can the world has grown up. The words styles that writer value to explain it is easy to understand. Typically the writer made some analysis when he makes this book. Honestly, that is why this book suited all of you.

Joseph Carter:

Reading a guide make you to get more knowledge as a result. You can take knowledge and information from a book. Book is created or printed or illustrated from each source that will filled update of news. Within this modern era like today, many ways to get information are available for an individual. From media social similar to newspaper, magazines, science guide, encyclopedia, reference book, story and comic. You can add your knowledge by that book. Isn't it time to spend your spare time to open your book? Or just in search of the Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry when you required it?

Download and Read Online Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry By Harlan Carvey #P10M7XB3FDS

Read Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry By Harlan Carvey for online ebook

Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry By Harlan Carvey Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry By Harlan Carvey books to read online.

Online Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry By Harlan Carvey ebook PDF download

Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry By Harlan Carvey Doc

Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry By Harlan Carvey Mobipocket

Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry By Harlan Carvey EPub

P10M7XB3FDS: Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry By Harlan Carvey