Windows Forensics

Dr. Philip Polstra

Windows Forensics

Dr. Philip Polstra

Windows Forensics Dr. Philip Polstra

Windows Forensics is the most comprehensive and up-to-date resource for those wishing to leverage the power of Linux and free software in order to quickly and efficiently perform forensics on Windows systems. It is also a great asset for anyone that would like to better understand Windows internals.

Windows Forensics will guide you step by step through the process of investigating a computer running Windows. Whatever the reason for performing forensics on a Windows system, be it incident response, a criminal investigation, suspected data ex-filtration, or data recovery, this book will tell you what you need to know in order to perform the vast majority of investigations. All of the tools discussed in this book are free and most are also open source.

Dr. Philip Polstra shows how to leverage numerous tools such as Python, shell scripting, and MySQL to quickly, easily, and accurately analyze Windows systems. While readers will have a strong grasp of Python and shell scripting by the time they complete this book, no prior knowledge of either of these scripting languages is assumed. **Windows Forensics** begins by showing you how to determine if there was an incident with minimally invasive techniques. Once it appears likely that an incident has occurred, Dr. Polstra shows you how to collect data from a live system before shutting it down for the creation of filesystem images.

Windows Forensics contains extensive coverage of Windows FAT and NTFS filesystems. A large collection of Python and shell scripts for creating, mounting, and analyzing filesystem images are presented in this book. The treasure trove of data found in the Windows Registry and other artifacts are discussed in detail. Dr. Polstra introduces readers to the exciting new field of memory analysis using the Volatility framework. Discussion of malware analysis rounds out the book.

Book Highlights

- 554 pages in large, easy-to-read 8.5 x 11 inch format
- Over 11,000 lines of Python scripts with explanations
- Over 500 lines of shell and command scripts with explanations
- A 96 page chapter covering the FAT filesystem in detail
- A 164 page chapter on NTFS filesystems
- Multiple scenarios described in detail with images available from the book website
- All scripts and other support files are available from the book website

---

From reader reviews:

Marilyn Daniels:

Do you have favorite book? In case you have, what is your favorite's book? Guide is very important thing for us to be aware of everything in the world. Each book has different aim or perhaps goal; it means that publication has different type. Some people really feel enjoy to spend their the perfect time to read a book. They are reading whatever they get because their hobby will be reading a book. Consider the person who don't like looking at a book? Sometime, person feel need book when they found difficult problem or maybe exercise. Well, probably you should have this Windows Forensics.

Victor Elam:

Book is definitely written, printed, or descriptive for everything. You can recognize everything you want by a guide. Book has a different type. As it is known to us that book is important thing to bring us around the world. Adjacent to that you can your reading ability was fluently. A guide Windows Forensics will make you to be smarter. You can feel far more confidence if you can know about every thing. But some of you think that will open or reading any book make you bored. It is far from make you fun. Why they may be thought like that? Have you in search of best book or appropriate book with you?

Anna Wright:

What do you consider book? It is just for students because they are still students or the idea for all people in the world, exactly what the best subject for that? Only you can be answered for that concern above. Every person has diverse personality and hobby for every other. Don't to be pushed someone or something that they don't want do that. You must know how great and also important the book Windows Forensics. All type of book is it possible to see on many sources. You can look for the internet solutions or other social media.

Danny Jarosz:

In this 21st hundred years, people become competitive in each and every way. By being competitive now, people have do something to make these individuals survives, being in the middle of the crowded place and notice by means of surrounding. One thing that occasionally many people have underestimated it for a while is reading. Yep, by reading a publication your ability to survive boost then having chance to remain than other is high. For you personally who want to start reading a new book, we give you this kind of Windows Forensics book as nice and daily reading reserve. Why, because this book is usually more than just a book.

#KQSENL3DACT

Read Windows Forensics by Dr. Philip Polstra for online ebook

Windows Forensics by Dr. Philip Polstra 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 Forensics by Dr. Philip Polstra books to read online.

Online Windows Forensics by Dr. Philip Polstra ebook PDF download

Windows Forensics by Dr. Philip Polstra Doc

Windows Forensics by Dr. Philip Polstra Mobipocket

Windows Forensics by Dr. Philip Polstra EPub