Malware Forensics: Investigating and Analyzing Malicious Code

Cameron H. Malin, Eoghan Casey, James M. Aquilina

Malware Forensics: Investigating and Analyzing Malicious Code

Cameron H. Malin, Eoghan Casey, James M. Aquilina

Malware Forensics: Investigating and Analyzing Malicious Code Cameron H. Malin, Eoghan Casey, James M. Aquilina
Malware Forensics: Investigating and Analyzing Malicious Code covers the emerging and evolving field of "live forensics," where investigators examine a computer system to collect and preserve critical live data that may be lost if the system is shut down. Unlike other forensic texts that discuss "live forensics" on a particular operating system, or in a generic context, this book emphasizes a live forensics and evidence collection methodology on both Windows and Linux operating systems in the context of identifying and capturing malicious code and evidence of its effect on the compromised system.
Malware Forensics: Investigating and Analyzing Malicious Code also devotes extensive coverage of the burgeoning forensic field of physical and process memory analysis on both Windows and Linux platforms. This book provides clear and concise guidance as to how to forensically capture and examine physical and process memory as a key investigative step in malicious code forensics.
Prior to this book, competing texts have described malicious code, accounted for its evolutionary history, and in some instances, dedicated a mere chapter or two to analyzing malicious code. Conversely, *Malware Forensics: Investigating and Analyzing Malicious Code* emphasizes the practical "how-to" aspect of malicious code investigation, giving deep coverage on the tools and techniques of conducting runtime behavioral malware analysis (such as file, registry, network and port monitoring) and static code analysis (such as file identification and profiling, strings discovery, armoring/packing detection, disassembling, debugging), and more.

* **Winner of Best Book Bejtlich read in 2008!**
* http://taosecurity.blogspot.com/2008/12/best-book-bejtlich-read-in-2008.html
* Authors have investigated and prosecuted federal malware cases, which allows them to provide unparalleled insight to the reader.
* First book to detail how to perform "live forensic" techniques on malicous code.
* In addition to the technical topics discussed, this book also offers critical legal considerations addressing the legal ramifications and requirements governing the subject matter

Download and Read Free Online Malware Forensics: Investigating and Analyzing Malicious Code Cameron H. Malin, Eoghan Casey, James M. Aquilina

---

From reader reviews:

Irving Gaston:

Often the book Malware Forensics: Investigating and Analyzing Malicious Code has a lot of information on it. So when you check out this book you can get a lot of benefit. The book was compiled by the very famous author. This articles author makes some research before write this book. This kind of book very easy to read you will get the point easily after reading this article book.

Randy Garrison:

The book untitled Malware Forensics: Investigating and Analyzing Malicious Code contain a lot of information on it. The writer explains the woman idea with easy way. The language is very clear and understandable all the people, so do not really worry, you can easy to read that. The book was authored by famous author. The author provides you in the new time of literary works. You can read this book because you can read on your smart phone, or program, so you can read the book with anywhere and anytime. If you want to buy the e-book, you can available their official web-site and also order it. Have a nice learn.

Garnet Veach:

Is it you actually who having spare time subsequently spend it whole day by watching television programs or just lying down on the bed? Do you need something new? This Malware Forensics: Investigating and Analyzing Malicious Code can be the solution, oh how comes? The new book you know. You are so out of date, spending your spare time by reading in this brand new era is common not a nerd activity. So what these textbooks have than the others?

Gary Collis:

Do you like reading a publication? Confuse to looking for your selected book? Or your book ended up being rare? Why so many issue for the book? But almost any people feel that they enjoy to get reading. Some people likes looking at, not only science book but additionally novel and Malware Forensics: Investigating and Analyzing Malicious Code as well as others sources were given expertise for you. After you know how the good a book, you feel need to read more and more. Science publication was created for teacher or even students especially. Those publications are helping them to put their knowledge. In some other case, beside science guide, any other book likes Malware Forensics: Investigating and Analyzing Malicious Code to make your spare time much more colorful. Many types of book like this.

Read Malware Forensics: Investigating and Analyzing Malicious Code by Cameron H. Malin, Eoghan Casey, James M. Aquilina for online ebook

Malware Forensics: Investigating and Analyzing Malicious Code by Cameron H. Malin, Eoghan Casey, James M. Aquilina 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 Malware Forensics: Investigating and Analyzing Malicious Code by Cameron H. Malin, Eoghan Casey, James M. Aquilina books to read online.

Online Malware Forensics: Investigating and Analyzing Malicious Code by Cameron H. Malin, Eoghan Casey, James M. Aquilina ebook PDF download

Malware Forensics: Investigating and Analyzing Malicious Code by Cameron H. Malin, Eoghan Casey, James M. Aquilina Doc

Malware Forensics: Investigating and Analyzing Malicious Code by Cameron H. Malin, Eoghan Casey, James M. Aquilina Mobipocket

Malware Forensics: Investigating and Analyzing Malicious Code by Cameron H. Malin, Eoghan Casey, James M. Aquilina EPub