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:

David Robinson:

Why don't make it to become your habit? Right now, try to ready your time to do the important take action, like looking for your favorite publication and reading a reserve. Beside you can solve your long lasting problem; you can add your knowledge by the reserve entitled Malware Forensics: Investigating and Analyzing Malicious Code. Try to make book Malware Forensics: Investigating and Analyzing Malicious Code as your friend. It means that it can to be your friend when you feel alone and beside that of course make you smarter than ever before. Yeah, it is very fortuned in your case. The book makes you more confidence because you can know every thing by the book. So , let us make new experience and knowledge with this book.

James Bergeron:

This Malware Forensics: Investigating and Analyzing Malicious Code are generally reliable for you who want to be described as a successful person, why. The explanation of this Malware Forensics: Investigating and Analyzing Malicious Code can be one of the great books you must have is definitely giving you more than just simple examining food but feed you with information that perhaps will shock your previous knowledge. This book is definitely handy, you can bring it just about everywhere and whenever your conditions in e-book and printed people. Beside that this Malware Forensics: Investigating and Analyzing Malicious Code giving you an enormous of experience for instance rich vocabulary, giving you test of critical thinking that we understand it useful in your day activity. So , let's have it and luxuriate in reading.

Jacqueline Britt:

Reading a book can be one of a lot of pastime that everyone in the world enjoys. Do you like reading book thus. There are a lot of reasons why people enjoyed. First reading a e-book will give you a lot of new data. When you read a e-book you will get new information because book is one of several ways to share the information or maybe their idea. Second, reading through a book will make you actually more imaginative. When you reading through a book especially fictional book the author will bring that you imagine the story how the people do it anything. Third, you may share your knowledge to other folks. When you read this Malware Forensics: Investigating and Analyzing Malicious Code, you can tells your family, friends and also soon about yours publication. Your knowledge can inspire different ones, make them reading a reserve.

William Kavanaugh:

Reading a guide make you to get more knowledge from this. You can take knowledge and information originating from a book. Book is prepared or printed or created from each source that will filled update of news. With this modern era like right now, many ways to get information are available for you actually. From media social such as newspaper, magazines, science book, encyclopedia, reference book, new and comic. You can add your knowledge by that book. Isn't it time to spend your spare time to spread out your

book? Or just seeking the Malware Forensics: Investigating and Analyzing Malicious Code when you required it?

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