



The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory

[Paperback]

Andrew Case, Jamie Levy, Aaron Walters by Michael Hale Ligh

Download now

[Click here](#) if your download doesn't start automatically

The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback]

Andrew Case, Jamie Levy, Aaron Walters by Michael Hale Ligh

The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback] Andrew Case, Jamie Levy, Aaron Walters by Michael Hale Ligh

Printed in Asia. Table of Contents: Introduction An Introduction to Memory Forensics • Systems Overview • Data Structures • The Volatility Framework • Memory Acquisition Windows Memory Forensics • Windows Objects and Pool Allocations • Processes, Handles and Tokens • Process Memory Internals • Hunting Malware in Process Memory • Event Logs • Registry in Memory • Networking • Windows Services • Kernel Forensics and Rootkits • Windows GUI Subsystem, Part I • Windows GUI Subsystem, Part II • Disk Artifacts in Memory • Event Reconstruction • Timelining Linux Memory Forensics • Linux Memory Acquisition • Linux Operating System • Processes and Process Memory • Networking Artifacts • Kernel Memory Artifacts • File Systems in Memory • User land Rootkits • Kernel Mode Rootkits • Case Study: Phalanx Mac Memory Forensics • Mac Acquisition and Internals • Mac Memory Overview • Malicious Code and Rootkits • Tracking User Activity Index

 [Download The Art of Memory Forensics: Detecting Malware and ...pdf](#)

 [Read Online The Art of Memory Forensics: Detecting Malware a ...pdf](#)

Download and Read Free Online The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback] Andrew Case, Jamie Levy, Aaron Walters by Michael Hale Ligh

From reader reviews:

Mary Edick:

The book The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback] can give more knowledge and also the precise product information about everything you want. Why must we leave the good thing like a book The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback]? Some of you have a different opinion about publication. But one aim that book can give many information for us. It is absolutely appropriate. Right now, try to closer using your book. Knowledge or data that you take for that, you can give for each other; you may share all of these. Book The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback] has simple shape but you know: it has great and large function for you. You can search the enormous world by open and read a publication. So it is very wonderful.

Mary McKay:

This The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback] tend to be reliable for you who want to become a successful person, why. The reason why of this The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback] can be one of the great books you must have is actually giving you more than just simple studying food but feed you with information that possibly will shock your earlier knowledge. This book is handy, you can bring it just about everywhere and whenever your conditions throughout the e-book and printed people. Beside that this The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback] giving you an enormous of experience for instance rich vocabulary, giving you tryout of critical thinking that could it useful in your day activity. So , let's have it and luxuriate in reading.

Melody Grissom:

The reason why? Because this The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback] is an unordinary book that the inside of the publication waiting for you to snap the idea but latter it will zap you with the secret the item inside. Reading this book close to it was fantastic author who write the book in such wonderful way makes the content inside easier to understand, entertaining approach but still convey the meaning entirely. So , it is good for you for not hesitating having this nowadays or you going to regret it. This excellent book will give you a lot of gains than the other book have such as help improving your expertise and your critical thinking technique. So , still want to hesitate having that book? If I were being you I will go to the guide store hurriedly.

Bruce Herrera:

The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory

[Paperback] can be one of your nice books that are good idea. Many of us recommend that straight away because this e-book has good vocabulary which could increase your knowledge in words, easy to understand, bit entertaining but nonetheless delivering the information. The article writer giving his/her effort to get every word into delight arrangement in writing The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback] although doesn't forget the main level, giving the reader the hottest and also based confirm resource facts that maybe you can be certainly one of it. This great information could drawn you into new stage of crucial pondering.

**Download and Read Online The Art of Memory Forensics:
Detecting Malware and Threats in Windows, Linux, and Mac
Memory [Paperback] Andrew Case, Jamie Levy, Aaron Walters by
Michael Hale Ligh #41QUGESCMRT**

Read The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback] by Andrew Case, Jamie Levy, Aaron Walters by Michael Hale Ligh for online ebook

The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback] by Andrew Case, Jamie Levy, Aaron Walters by Michael Hale Ligh 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 The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback] by Andrew Case, Jamie Levy, Aaron Walters by Michael Hale Ligh books to read online.

Online The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback] by Andrew Case, Jamie Levy, Aaron Walters by Michael Hale Ligh ebook PDF download

The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback] by Andrew Case, Jamie Levy, Aaron Walters by Michael Hale Ligh Doc

The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback] by Andrew Case, Jamie Levy, Aaron Walters by Michael Hale Ligh Mobipocket

The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory [Paperback] by Andrew Case, Jamie Levy, Aaron Walters by Michael Hale Ligh EPub