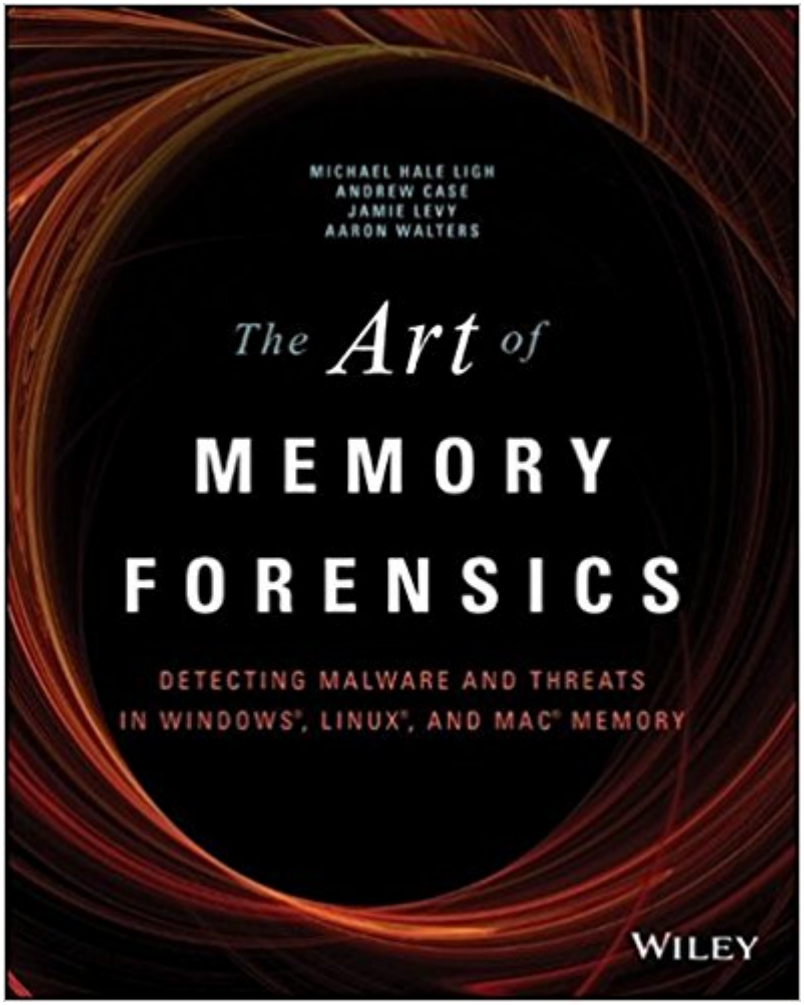
The Art Of Memory Forensics: Detecting Malware And Threats In Windows, Linux, And Mac Memory



Synopsis

Memory forensics provides cutting edge technology to help investigate digital attacks Memory forensics is the art of analyzing computer memory (RAM) to solve digital crimes. As a follow-up to the best seller Malware Analyst's Cookbook, experts in the fields of malware, security, and digital forensics bring you a step-by-step guide to memory forensicsâ ”now the most sought after skill in the digital forensics and incident response fields. Beginning with introductory concepts and moving toward the advanced, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory is based on a five day training course that the authors have presented to hundreds of students. It is the only book on the market that focuses exclusively on memory forensics and how to deploy such techniques properly. Discover memory forensics techniques: How volatile memory analysis improves digital investigations Proper investigative steps for detecting stealth malware and advanced threats How to use free, open source tools for conducting thorough memory forensics Ways to acquire memory from suspect systems in a forensically sound manner The next era of malware and security breaches are more sophisticated and targeted, and the volatile memory of a computer is often overlooked or destroyed as part of the incident response process. The Art of Memory Forensics explains the latest technological innovations in digital forensics to help bridge this gap. It covers the most popular and recently released versions of Windows, Linux, and Mac, including both the 32 and 64-bit editions.

Book Information

Paperback: 912 pages

Publisher: Wiley; 1 edition (July 28, 2014)

Language: English

ISBN-10: 1118825098

ISBN-13: 978-1118825099

Product Dimensions: 7.3 x 1.7 x 9.2 inches

Shipping Weight: 3.2 pounds (View shipping rates and policies)

Average Customer Review: 4.8 out of 5 stars 38 customer reviews

Best Sellers Rank: #71,245 in Books (See Top 100 in Books) #21 inÂ Books > Computers & Technology > Operating Systems > Linux > Programming #22 inÂ Books > Computers & Technology > Security & Encryption > Viruses #28 inÂ Books > Computers & Technology > Security & Encryption > Encryption

Customer Reviews

SOPHISTICATED DISCOVERY AND ANALYSIS FOR THE NEXT WAVE OF DIGITAL ATTACKS

The Art of Memory Forensics, a follow-up to the bestselling Malware Analystâ ™s Cookbook, is a practical guide to the rapidly emerging investigative technique for digital forensics, incident response, and law enforcement. Memory forensics has become a must-have skill for combating the next era of advanced malware, targeted attacks, security breaches, and online crime. As breaches and attacks become more sophisticated, analyzing volatile memory becomes ever more critical to the investigative process. This book provides a comprehensive guide to performing memory forensics for Windows, Linux, and Mac systems, including x64 architectures. Based on the authorsâ ™ popular training course, coverage includes memory acquisition, rootkits, tracking user activity, and more, plus case studies that illustrate the real-world application of the techniques presented. Bonus materials include industry-applicable exercises, sample memory dumps, and cutting-edge memory forensics software. Memory forensics is the art of analyzing RAM to solve digital crimes. Conventional incident response often overlooks volatile memory, which contains crucial information that can prove or disprove the systemâ ™s involvement in a crime, and can even destroy it completely. By implementing memory forensics techniques, analysts are able to preserve memory resident artifacts which often provides a more efficient strategy for investigating modern threats. In The Art of Memory Forensics, the Volatility Projectâ ™s team of experts provides functional guidance and practical advice that helps readers to: Acquire memory from suspect systems in a forensically sound manner Learn best practices for Windows, Linux, and Mac memory forensics Discover how volatile memory analysis improves digital investigations Delineate the proper investigative steps for detecting stealth malware and advanced threats Use free, open source tools to conduct thorough memory forensics investigations Generate timelines, track user activity, find hidden artifacts, and more The companion website provides exercises for each chapter, plus data that can be used to test the various memory analysis techniques in the book. Visit our website at www.wiley.com/go/memoryforensics.

Michael Hale-Ligh is author of Malware Analyst’s Cookbook, Secretary/Treasurer of Volatility Foundation, and a world-class reverse engineer. Andrew Case is a Digital Forensics Researcher specializing in memory, disk, and network forensics. Jamie Levy is a Senior Researcher and Developer, targeting memory, network, and malware forensics analysis. AAron Walters is founder and lead developer of the Volatility Project, President of the Volatility Foundation, and Chair of Open Memory Forensics Workshop.

I wish I had purchased this a lot sooner than I did. Although the SANS FOR 508 course was a great course, this book goes even further in detail regarding not just how to use Volatility and its plugins, but more importantly WHY you use certain plugins and HOW the plugins work based on how malware works. Very thorough explanations, it makes thing a lot more clearer now. Its like a lightbulb went off and I'm only half-way through the book. Well worth the price. A must for any serious forensics analyst who wants to stand out amongst his/her peers.

The Art of Memory Forensics (AOMF) is a ground-breaking technical resource (800+ pages) that is critical to everyone who currently works in Information Security or aspires to. I leverage this book almost daily as a digital forensics and incident response practitioner. It allows analysts better understand multiple OS (Windows/OSX/Linux) data and memory structures and how forensic tools can used and be written to parse them. AOMF also starts at a lower level than memory, defining Intel (IA) and related hardware architecture before building up to data types and structures found in memory.AOMF has over 450 pages dedicated to Windows forensic analysis. While there is a primary focus memory, the authors do a fantastic job of explaining technical analysis concepts around critical areas including the Windows Registry, Event logs, Services, Networking, timelining, kernel level artifacts and much more.AOMF also covers Linux and OSX, which are two OSÃ¢Â Â™s that are utilized more frequently and require deep-dive analysis today. The memory analysis chapters in these sections provide a solid resource for those interested in understanding more about investigating the bowels of what goes on behind the scenes with regards to unique Linux and OSX files, filesystems, processes, networking and unique userland/kernel artifacts for starters.Finally, AOMF serves as a verbose educational resource for both professors and students. This is the primary/sole resource I will be leveraging, using labs from and referencing as a graduate level memory forensics professor starting next month.

AMF is a volume of stuff you just have to know, or at least you have to know where to find it. The book is an essential reference, reasonably complete and well written. It reminds me of the classic Morse and Feshbach "Methods of Mathematical Physics". Like M&F, its contents must be ingested in small chunks when needed. It isn't a textbook entitled the principles of memory forensics.It's not a comprehensive handbook like Morse and Feshbach. But the current empirical field of memory forensics is not amenable to the kind of structural analysis that can be taught to graduate level physics students. My reason for not rating it five stars is the lack of a theoretical backbone. This is not a computer science book. This is a book about the volatility framework with application to the

structure and function of computer memory. It is not a book about data structures or processes. It isn’t really forensics, which is the presentation of scientific data and analysis in a court of law.If you buy the book as a practical handbook of memory forensics, as its authors say, "Art

This book is one of the best book i have read in recent years. This is a book for anyone in the field of Incident Response, Malware Analysis, Reverse Engineering and Digital Forensics. This book is written by the Core Developers of Volatility and pioneers in the field of memory forensics.The book is very well structured it covers the internals of the Operating System and then the authors explain how the structures are used by the plugins, the authors also show how these plugins can be run against the memory images with real case examples to identify forensic artifacts. In many cases the authors show how to access the operating system structures programmatically using the volshell, this can help in writing your own plugins and also the author references various external sources where you can find more information on a specific topic. The book covers many creative techniques that you can apply in the real world and it also covers information on the Anti-Forensics techniques and how to detect them by cross referencing them with different plugins/data sources. The amount of detail explained in the book shows the knowledge and amount of research the authors have done in this field and the effort the authors have put in to write this book and the Volatility plugins. In short After reading this book you will understand how the operating system works, how the Volatility works, how malware works, how memory forensics work, how to identify the malware and forensic artifacts using memory forensics, how to write your own plugin. I have never seen any book covering these many details, this is one book for everything on memory forensics. This definitely should be the Book of the Year. If there was an option of giving this book ten stars, i would give it ten stars.

I took the memory forensics workshop at DefCon this year. That was an amazing introduction to Volatility. But I expected that it would still be difficult to get far into such a complex technical subject. Silly me. This book is so well structured and written. Makes memory forensics fun.

This book is awesome. It starts broad and gets extremely detailed.

Good book. It was a lot of information. Not only did it help with memory forensics but the chapters on windows helped me to understand windows internals even more. I wish there was even more on Linux and Mac, though.

Delivers detailed and accurate information, practical examples, additional information available online: "The book’s supplementary materials are freely available to everyone. You don’t need to buy the book before you access them." (source: AMF website)

The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory Windows 10: The Ultimate 2 in 1 User Guide to Microsoft Windows 10 User Guide to Microsoft Windows 10 for Beginners and Advanced Users (tips and tricks, ... Windows, softwares, guide Book 7) CompTIA Linux+ Powered by Linux Professional Institute Study Guide: Exam LX0-103 and Exam LX0-104 (Comptia Linux + Study Guide) Mac’s Field Guide to Cacti and Common Trees and Shrubs of the Southwest (Mac’s Guides) (Mac’s Guides (Paperback)) Windows Registry Forensics, Second Edition: Advanced Digital Forensic Analysis of the Windows Registry Memory Exercises: Memory Exercises Unleashed: Top 12 Memory Exercises To Remember Work And Life In 24 Hours With The Definitive Memory Exercises Guide! (memory exercises, memory, brain training) Windows 10: The Best Guide How to Operate New Microsoft Windows 10 (tips and tricks, 2017 user manual, user guide, updated and edited, Windows for beginners) Windows 10: The Best Guide How to Operate New Microsoft Windows 10 (tips and tricks, user manual, user guide, updated and edited, Windows for beginners) Windows 10: The Ultimate 2017 Updated User Guide to Microsoft Windows 10 (2017 updated user guide, tips and tricks, user manual, user guide, Windows 10) Windows 10 Manual and Windows 10 User Guide (Windows 10 Guide for Beginners) Windows 10: User Guide and Manual: Microsoft Windows 10 for Windows Users The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics Memory Training: Train your brain to improve your memory (Unlimited Memory, Mental Health, Memory Techniques, Education & Reference, Study Skills, Memory Improvement Book 1) The Linux Programming Interface: A Linux and UNIX System Programming Handbook Easy Linux For Beginners: A Complete Introduction To Linux Operating System & Command Line Fast! CompTIA Linux+ Guide to Linux Certification The Mac + Cheese Cookbook: 50 Simple Recipes from Homeroom, America’s Favorite Mac and Cheese Restaurant Mac’s Pocket Guide: Grand Canyon National Park, Birds & Mammals (Mac’s Pocket Guides) Cuando Mack conocio a Mac (When Mack Met Mac) (Coleccion Leer En Espanol) (Spanish Edition) Computer Viruses and Malware (Advances in Information Security)

Privacy

FAQ & Help