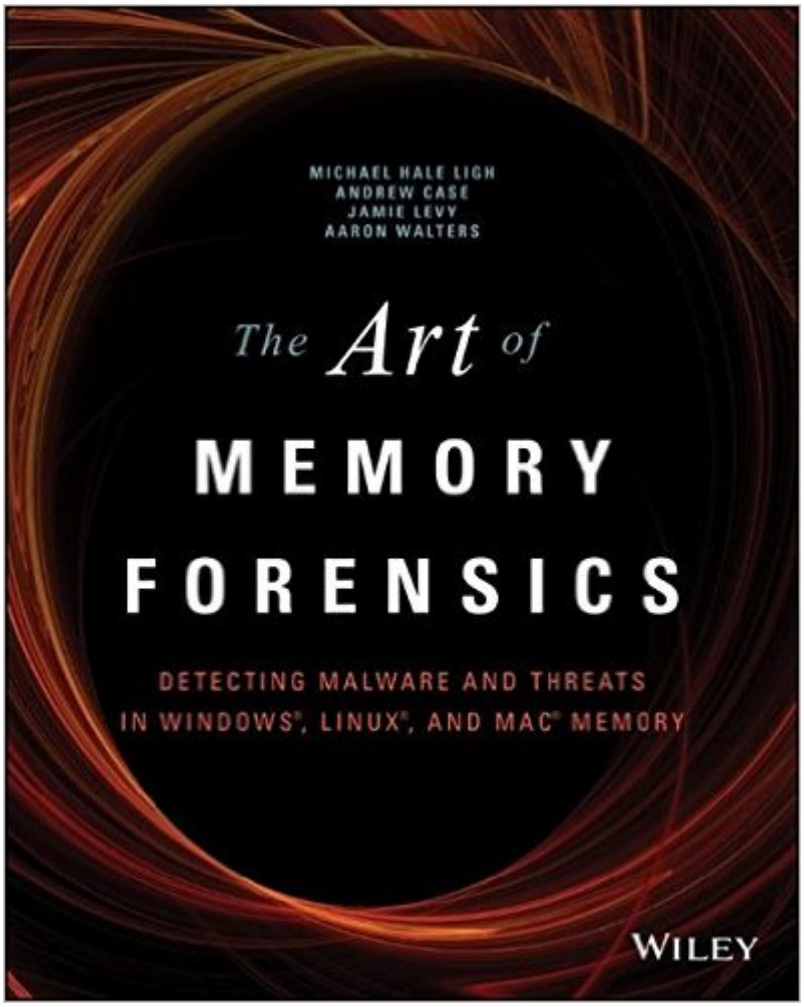
The Art Of Memory Forensics: Detecting Malware And Threats In Windows, Linux, And Mac Memory



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: 7.4 x 1.6 x 9.3 inches

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

Average Customer Review: 4.9 out of 5 starsÂ Â See all reviewsÂ (32 customer reviews)

Best Sellers Rank: #91,522 in Books (See Top 100 in Books) #32 inÂ Books > Computers & Technology > Operating Systems > Linux > Programming #33 inÂ Books > Computers & Technology > Security & Encryption > Encryption #35 inÂ Books > Computers & Technology > Security & Encryption > Cryptography

Customer Reviews

At this writing (Fall 2014) the Wiley instructor companion website is not up to Wiley standards (yet). I wanted to test the code for this review, but the code section on the site only defaults to the creative commons license (both the code and license links). Same with all the chapters, they only display commons, a strawman syllabus and an intro letter. They only resource that is already up is the Powerpoint presentation, and at over 100 pages it is simply OUTSTANDING, which whets the appetite even more for the rest of the outlines, solutions, code, and much more.So, Wiley, get with it! If you are considering buying this, add your vote in comments and Wiley might listen. I'll update this once we get the code, both with quality of the code and where it can be used. Going over the license so far, it is quite generous, much like GNU with an attribution link, although of course more robust beyond teaching (eg commercial) if you do get permission. The text itself has wonderful, up to date sploit and software info, patches, etc. but the site, for a book this costly, needs to be completed. I'm not recommending you pass on this because of it, but we won't be getting the full value for our purchase, nor will our students, until the site is completed.REVIEW UPDATE: SEE MICHAEL'S COMMENT ATTACHED TO THIS REVIEW. Although 's automated system generally removes links, the comment gives complete and up to date online resources for this book, as the publisher's link is incomplete, and will not be updated. The publisher promotion of online evidence samples, code, etc. is not wrong or deceptive, it is just on github rather than the publisher's site as indicated.

Two Hours: The Smart and Efficient Way to Learn Windows 8.1 (Windows 8.1, Windows 8.1 For Beginners) The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry Windows Registry Forensics, Second Edition: Advanced Digital Forensic Analysis of the Windows Registry Cross-Platform Development in C++: Building Mac OS X, Linux, and Windows Applications Modern Tkinter for Busy Python Developers: Quickly learn to create great looking user interfaces for Windows, Mac and Linux using Python's standard GUI toolkit Cross-Platform Development in C++: Building Mac OS X, Linux, and Windows Applications (Adobe Reader) 100 Command Line Tools For Windows, Linux and Mac OS/X: How to do things fast, with the same commands, on every computer Windows 10 Troubleshooting: Windows 10 Manuals, Display Problems, Sound Problems, Drivers and Software: Windows 10 Troubleshooting: How to Fix Common Problems ... Tips and Tricks, Optimize Windows 10) Windows 10: The Ultimate User Guide for Advanced Users to Operate Microsoft Windows 10 (tips and tricks, user manual, user guide, updated and edited, Windows ... (windows,guide,general.guide,all Book 4) WindowsÃ Â® Group Policy Resource Kit: Windows ServerÃ Â® 2008 and Windows VistaÃ Â®: Windows ServerÃ Â® 2008 and Windows VistaÃ Â® A Beginner's Guide to AutoHotkey, Absolutely the Best Free Windows Utility Software Ever! (Third Edition): Create Power Tools for Windows XP, Windows Vista, ... and Windows 10 (AutoHotkey Tips and Tricks)