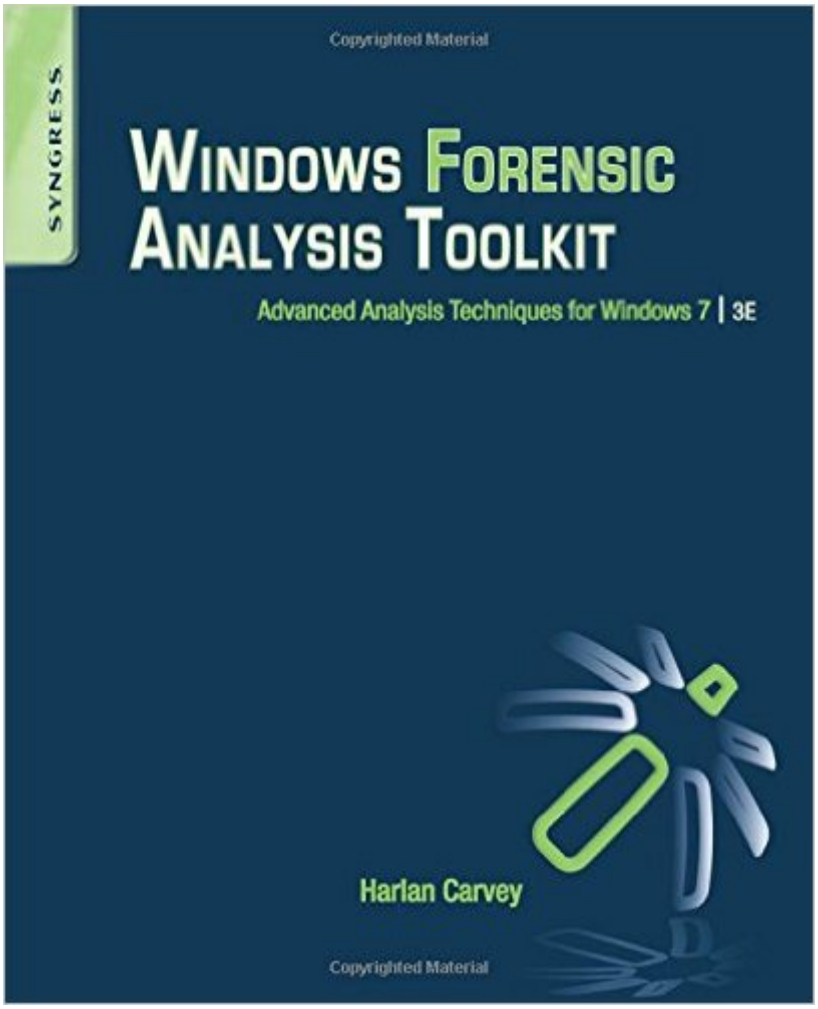
Windows Forensic Analysis Toolkit, Third Edition: Advanced Analysis Techniques For Windows 7



Synopsis

Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 7 provides an overview of live and postmortem response collection and analysis methodologies for Windows 7. It considers the core investigative and analysis concepts that are critical to the work of professionals within the digital forensic analysis community, as well as the need for immediate response once an incident has been identified. Organized into eight chapters, the book discusses Volume Shadow Copies (VSCs) in the context of digital forensics and explains how analysts can access the wealth of information available in VSCs without interacting with the live system or purchasing expensive solutions. It also describes files and data structures that are new to Windows 7 (or Vista), Windows Registry Forensics, how the presence of malware within an image acquired from a Windows system can be detected, the idea of timeline analysis as applied to digital forensic analysis, and concepts and techniques that are often associated with dynamic malware analysis. Also included are several tools written in the Perl scripting language, accompanied by Windows executables. This book will prove useful to digital forensic analysts, incident responders, law enforcement officers, students, researchers, system administrators, hobbyists, or anyone with an interest in digital forensic analysis of Windows 7 systems.Timely 3e of a Syngress digital forensic bestsellerUpdated to cover Windows 7 systems, the newest Windows versionNew online companion website houses checklists, cheat sheets, free tools, and demos

Book Information

Paperback: 296 pages

Publisher: Syngress; 3 edition (February 10, 2012)

Language: English

ISBN-10: 1597497274

ISBN-13: 978-1597497275

Product Dimensions: 7.5 x 0.7 x 9.2 inches

Shipping Weight: 1.3 pounds (View shipping rates and policies)

Average Customer Review: 4.8 out of 5 starsÂ Â See all reviewsÂ (14 customer reviews)

Best Sellers Rank: #398,738 in Books (See Top 100 in Books) #25 inÂ Books > Computers & Technology > Operating Systems > Windows > Windows Desktop > Windows 7 #446 inÂ Books > Textbooks > Computer Science > Operating Systems #1033 inÂ Books > Computers & Technology > Software > Microsoft

Customer Reviews

If you've worked with Windows for any length of time, you know that each subsequent version of Microsoft's operating system tends to be almost the same...and yet entirely different. Windows 7 is no exception, giving us many familiar logs, structures, and artifacts that we know from Windows XP or 2003...only revised and expanded, or in different locations, or in different formats, or all of the above. Not to mention the brand new stuff.Harlan has once again found the sweet spot - instead of fully revising the Second Edition of his book (which would be premature, as most environments still have extensive XP / 2003 infrastructure in place, and likely will for some time), he provides a companion book that builds on his previous volumes and outlines the new technologies and key differences between Windows 7 and earlier versions of the OS.Now that many corporations are finally rolling out Windows 7 in force, forensic examiners are also making the transition to analyzing "new" Windows systems. This book provides the essential reference for Windows 7 analysis. While many of the technologies and techniques in Harlan's book have been discussed on blogs, mailing lists, and at conferences, he has been kind enough to collect the information in one place. In addition, he has been thorough enough to verify and expand upon the information through his own research and analysis, providing real world examples, tips, and cautions along the way.Finally, as always Harlan writes with a keen awareness - both first-hand and through his extensive industry contacts - of what is current "in the field". This encompasses not only the specific questions and challenges faced by real analysts in real cases, but the tools and techniques in use or under development to address those issues.

Pineal Gland, Third Eye Chakra, Open Third Eye) 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) 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) Windows 10: The Ultimate Guide For Beginners (Windows 10 for dummies, Windows 10 Manual, Windows 10 Complete User Guide, Learn the tips and tricks of Windows 10 Operating System) Windows 8.1: Learn Windows 8.1 in Two Hours: The Smart and Efficient Way to Learn Windows 8.1 (Windows 8.1, Windows 8.1 For Beginners) Forensic Psychotherapy: Crime, Psychodynamics & the Offender Patient (Forensic Focus) Advanced Windows: The Developer's Guide to the WIN32 API for Windows NT 3.5 and Windows 95 Windows 8 Tips for Beginners 2nd Edition: A Simple, Easy, and Efficient Guide to a Complex System of Windows 8! (Windows 8, Operating Systems, Windows ... Networking, Computers, Technology) Microsoft Windows Internals (4th Edition): Microsoft Windows Server 2003, Windows XP, and Windows 2000 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)