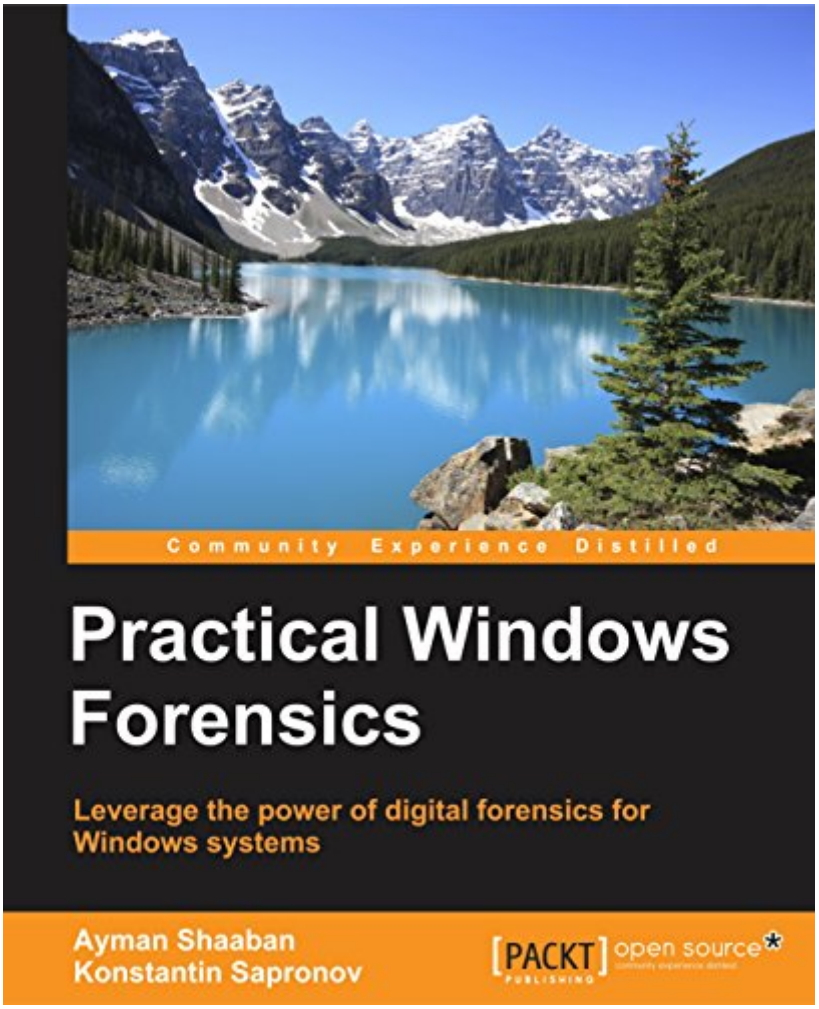
Practical Windows Forensics



Synopsis

Leverage the power of digital forensics for Windows systemsAbout This BookBuild your own lab environment to analyze forensic data and practice techniques.This book offers meticulous coverage with an example-driven approach and helps you build the key skills of performing forensics on Windows-based systems using digital artifacts.It uses specific open source and Linux-based tools so you can become proficient at analyzing forensic data and upgrade your existing knowledge.Who This Book Is ForThis book targets forensic analysts and professionals who would like to develop skills in digital forensic analysis for the Windows platform. You will acquire proficiency, knowledge, and core skills to undertake forensic analysis of digital data.Prior experience of information security and forensic analysis would be helpful. You will gain knowledge and an understanding of performing forensic analysis with tools especially built for the Windows platform.What You Will LearnPerform live analysis on victim or suspect Windows systems locally or remotelyUnderstand the different natures and acquisition techniques of volatile and non-volatile data.Create a timeline of all the system actions to restore the history of an incident.Recover and analyze data from FAT and NTFS file systems.Make use of various tools to perform registry analysis.Track a system user’s browser and e-mail activities to prove or refute some hypotheses.Get to know how to dump and analyze computer memory.In DetailOver the last few years, the wave of the cybercrime has risen rapidly. We have witnessed many major attacks on the governmental, military, financial, and media sectors. Tracking all these attacks and crimes requires a deep understanding of operating system operations, how to extract evident data from digital evidence, and the best usage of the digital forensic tools and techniques. Regardless of your level of experience in the field of information security in general, this book will fully introduce you to digital forensics. It will provide you with the knowledge needed to assemble different types of evidence effectively, and walk you through the various stages of the analysis process.We start by discussing the principles of the digital forensics process and move on to show you the approaches that are used to conduct analysis. We will then study various tools to perform live analysis, and go through different techniques to analyze volatile and non-volatile data.Style and approachThis is a step-by-step guide that delivers knowledge about different Windows artifacts. Each topic is explained sequentially, including artifact analysis using different tools and techniques. These techniques make use of the evidence extracted from infected machines, and are accompanied by real-life examples.

Book Information

File Size: 59808 KB

Print Length: 322 pages

Publisher: Packt Publishing (June 29, 2016)

Publication Date: June 29, 2016

Sold by:Â Digital Services LLC

Language: English

ASIN: B012B1H8GY

Text-to-Speech: Enabled

X-Ray: Not Enabled

Word Wise: Not Enabled

Lending: Not Enabled

Enhanced Typesetting: Not Enabled

Best Sellers Rank: #857,610 Paid in Kindle Store (See Top 100 Paid in Kindle Store) #160 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Administration > Email Administration #463 inÂ Kindle Store > Kindle eBooks > Computers & Technology > Microsoft > Windows - General #1430 inÂ Books > Computers & Technology > Operating Systems > Windows > Windows Desktop

Customer Reviews

i am reading in chapter 2 now, it is very interesting and useful book, contain a lot of information and explain in easy way

Great book that provides practical steps when dealing with windows incidents. I highly recommend it.

Windows 10: Windows10 Mastery. The Ultimate Windows 10 Mastery Guide (Windows Operating System, Windows 10 User Guide, User Manual, Windows 10 For Beginners, Windows 10 For Dummies, Microsoft Office) 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) 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 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) 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) WindowsÃ Â® Group Policy Resource Kit: Windows ServerÃ Â® 2008 and Windows VistaÃ Â®: Windows ServerÃ Â® 2008 and Windows VistaÃ Â® Microsoft Windows Internals (4th Edition): Microsoft Windows Server 2003, Windows XP, and Windows 2000 Windows 10: The Ultimate Beginner's Guide - Learn How To Start Using Windows 10, Easy User Manual, Plus The Best Hidden Features, Tips And Tricks! (Windows ... Windows 10 Software, Operating System) 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 Beginner's Guide How to Operate Microsoft Windows 10 (tips and tricks, user manual, user guide, updated and edited, Windows ... (windows,guide,general,guide,all) (Volume 3) Practical Windows Forensics The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory Hands-on Study Guide for Exam 70-411: Administering Windows Server 2012 R2 (Exam 70-411, 70-411, Exam Ref 70-411, MCSA Windows Server 2012 R2, MCSE Windows Server 2012 R2) Windows 10: From Beginner To Expert: A Complete User Guide to Microsoft's Intelligent New Operating System (Now With Bonus Chapter) (Windows - General ... General Guide, Windows - General Mastery,) Windows 10 New Users Guide: Learn How To Master Windows 10 Step By Step! (Windows 10 For Beginners) Windows 8.1 :: Migrating to Windows 8.1.: For computer users without a touch screen, coming from XP, Vista or Windows 7