



Practical Windows Forensics

By Ayman Shaaban, Konstantin Sapronov



Download



Read Online

Practical Windows Forensics By Ayman Shaaban, Konstantin Sapronov

Leverage the power of digital forensics for Windows systems

About This Book

- Build 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 For

This 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 Learn

- Perform live analysis on victim or suspect Windows systems locally or remotely
- Understand 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 Detail

Over 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 approach

This 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.

 [Download Practical Windows Forensics ...pdf](#)

 [Read Online Practical Windows Forensics ...pdf](#)

Practical Windows Forensics

By Ayman Shaaban, Konstantin Sapronov

Practical Windows Forensics By Ayman Shaaban, Konstantin Sapronov

Leverage the power of digital forensics for Windows systems

About This Book

- Build 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 For

This 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 Learn

- Perform live analysis on victim or suspect Windows systems locally or remotely
- Understand 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 Detail

Over 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 approach

This 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.

Practical Windows Forensics By Ayman Shaaban, Konstantin Sapronov Bibliography

- Rank: #289984 in Books
- Published on: 2016-07-06
- Released on: 2016-06-29
- Original language: English
- Dimensions: 9.25" h x .76" w x 7.50" l, 1.22 pounds
- Binding: Paperback
- 322 pages

 [Download Practical Windows Forensics ...pdf](#)

 [Read Online Practical Windows Forensics ...pdf](#)

Download and Read Free Online Practical Windows Forensics By Ayman Shaaban, Konstantin Sapronov

Editorial Review

About the Author

Ayman Shaaban Ayman Shaaban (@aymanshaaban) has been working as a security researcher for Kaspersky Lab since May 2014. He worked in the Egyptian national CERT as a digital forensics engineer for 5 years. During his career, Ayman has participated in building digital forensics labs, provided analysis for cases with national and international scopes, and delivered training courses on digital forensics analysis for different high-profile entities. Ayman is a certified GSEC, GCIH, GCFA, and CFCE. He also has a BSc in communication and electronics, an information security diploma from ITI, and is working on his master's degree in information security. Ayman can be found on LinkedIn at <http://eg.linkedin.com/in/aymanshaaban>.

Konstantin Sapronov Konstantin Sapronov works as the deputy head of the Global Emergency Response Team at Kaspersky Lab. He joined Kaspersky Lab in 2000 and has been in his current position since August 2011. His previous position was group manager of the virus lab in China since 2007, and he has been responsible for establishing and developing the virus lab at Kaspersky Lab's office in China. Prior to this, he worked as a virus analyst and head of the Non-Intel Platform Group in the virus lab at Kaspersky Lab's HQ in Moscow, specializing in reverse engineering and the analysis of malware, exploits, and vulnerabilities. Konstantin is the author of several analytical articles on malware for Unix and other information security topics. Konstantin holds degrees from the Moscow Power Engineering Institute (a technical university) and the Moscow State University of Economics, Statistics and Information Technology.

Users Review

From reader reviews:

Coleman Jones:

Have you spare time for any day? What do you do when you have more or little spare time? Yeah, you can choose the suitable activity with regard to spend your time. Any person spent all their spare time to take a wander, shopping, or went to the actual Mall. How about open or even read a book titled Practical Windows Forensics? Maybe it is for being best activity for you. You recognize beside you can spend your time with your favorite's book, you can wiser than before. Do you agree with it has the opinion or you have other opinion?

Katrina Scofield:

Do you considered one of people who can't read pleasant if the sentence chained within the straightway, hold on guys this specific aren't like that. This Practical Windows Forensics book is readable simply by you who hate the perfect word style. You will find the info here are arrange for enjoyable reading through experience without leaving actually decrease the knowledge that want to deliver to you. The writer involving Practical Windows Forensics content conveys prospect easily to understand by lots of people. The printed and e-book are not different in the information but it just different by means of it. So , do you still thinking Practical Windows Forensics is not loveable to be your top listing reading book?

David Mathews:

This Practical Windows Forensics is fresh way for you who has fascination to look for some information given it relief your hunger associated with. Getting deeper you in it getting knowledge more you know or else you who still having tiny amount of digest in reading this Practical Windows Forensics can be the light food for you personally because the information inside this kind of book is easy to get by anyone. These books acquire itself in the form and that is reachable by anyone, that's why I mean in the e-book contact form. People who think that in guide form make them feel tired even dizzy this e-book is the answer. So there is not any in reading a publication especially this one. You can find what you are looking for. It should be here for you actually. So , don't miss it! Just read this e-book type for your better life in addition to knowledge.

John Moreno:

With this era which is the greater man or who has ability to do something more are more treasured than other. Do you want to become among it? It is just simple way to have that. What you have to do is just spending your time almost no but quite enough to get a look at some books. One of several books in the top listing in your reading list is definitely Practical Windows Forensics. This book which is qualified as The Hungry Hillside can get you closer in becoming precious person. By looking upwards and review this e-book you can get many advantages.

**Download and Read Online Practical Windows Forensics By
Ayman Shaaban, Konstantin Sapronov #J9SUWGQBKEI**

Read Practical Windows Forensics By Ayman Shaaban, Konstantin Sapronov for online ebook

Practical Windows Forensics By Ayman Shaaban, Konstantin Sapronov 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 Practical Windows Forensics By Ayman Shaaban, Konstantin Sapronov books to read online.

Online Practical Windows Forensics By Ayman Shaaban, Konstantin Sapronov ebook PDF download

Practical Windows Forensics By Ayman Shaaban, Konstantin Sapronov Doc

Practical Windows Forensics By Ayman Shaaban, Konstantin Sapronov Mobipocket

Practical Windows Forensics By Ayman Shaaban, Konstantin Sapronov EPub