Mastering Python Forensics

Dr. Michael Spreitzenbarth, Dr. Johann Uhrmann

Mastering Python Forensics

Dr. Michael Spreitzenbarth, Dr. Johann Uhrmann

Mastering Python Forensics Dr. Michael Spreitzenbarth, Dr. Johann Uhrmann

Master the art of digital forensics and analysis with Python

About This Book

- Learn to perform forensic analysis and investigations with the help of Python, and gain an advanced understanding of the various Python libraries and frameworks
- Analyze Python scripts to extract metadata and investigate forensic artifacts
- The writers, Dr. Michael Spreitzenbarth and Dr. Johann Uhrmann, have used their experience to craft this hands-on guide to using Python for forensic analysis and investigations

Who This Book Is For

If you are a network security professional or forensics analyst who wants to gain a deeper understanding of performing forensic analysis with Python, then this book is for you. Some Python experience would be helpful.

What You Will Learn

- Explore the forensic analysis of different platforms such as Windows, Android, and vSphere
- Semi-automatically reconstruct major parts of the system activity and time-line
- Leverage Python ctypes for protocol decoding
- Examine artifacts from mobile, Skype, and browsers
- Discover how to utilize Python to improve the focus of your analysis
- Investigate in volatile memory with the help of volatility on the Android and Linux platforms

In Detail

Digital forensic analysis is the process of examining and extracting data digitally and examining it. Python has the combination of power, expressiveness, and ease of use that makes it an essential complementary tool to the traditional, off-the-shelf digital forensic tools.

This book will teach you how to perform forensic analysis and investigations by exploring the capabilities of various Python libraries.

The book starts by explaining the building blocks of the Python programming language, especially ctypes in-depth, along with how to automate typical tasks in file system analysis, common correlation tasks to discover anomalies, as well as templates for investigations. Next, we'll show you cryptographic algorithms that can be used during forensic investigations to check for known files or to compare suspicious files with online services such as VirusTotal or Mobile-Sandbox.

Moving on, you'll learn how to sniff on the network, generate and analyze network flows, and perform log correlation with the help of Python scripts and tools. You'll get to know about the concepts of virtualization

and how virtualization influences IT forensics, and you'll discover how to perform forensic analysis of a jailbroken/rooted mobile device that is based on iOS or Android.

Finally, the book teaches you how to analyze volatile memory and search for known malware samples based on YARA rules.

Style and approach

This easy-to-follow guide will demonstrate forensic analysis techniques by showing you how to solve real-word-scenarios step by step.

Download and Read Free Online Mastering Python Forensics Dr. Michael Spreitzenbarth, Dr. Johann Uhrmann

---

From reader reviews:

Caroline Petrie:

The book Mastering Python Forensics can give more knowledge and also the precise product information about everything you want. So why must we leave the good thing like a book Mastering Python Forensics? Wide variety you have a different opinion about book. But one aim that will book can give many details for us. It is absolutely suitable. Right now, try to closer along with your book. Knowledge or info that you take for that, you are able to give for each other; you may share all of these. Book Mastering Python Forensics has simple shape however you know: it has great and big function for you. You can seem the enormous world by open and read a book. So it is very wonderful.

Edward Phillips:

Reading a book to be new life style in this year; every people loves to examine a book. When you learn a book you can get a lot of benefit. When you read books, you can improve your knowledge, because book has a lot of information onto it. The information that you will get depend on what types of book that you have read. If you need to get information about your analysis, you can read education books, but if you act like you want to entertain yourself read a fiction books, this sort of us novel, comics, and soon. The Mastering Python Forensics will give you a new experience in examining a book.

William Farley:

Beside this specific Mastering Python Forensics in your phone, it could give you a way to get more close to the new knowledge or info. The information and the knowledge you can got here is fresh from oven so don't end up being worry if you feel like an outdated people live in narrow small town. It is good thing to have Mastering Python Forensics because this book offers to you personally readable information. Do you oftentimes have book but you seldom get what it's exactly about. Oh come on, that will not happen if you have this within your hand. The Enjoyable set up here cannot be questionable, similar to treasuring beautiful island. Use you still want to miss the idea? Find this book and read it from today!

Brianna Bell:

What is your hobby? Have you heard in which question when you got pupils? We believe that that issue was given by teacher to the students. Many kinds of hobby, Everybody has different hobby. And you also know that little person just like reading or as looking at become their hobby. You need to understand that reading is very important as well as book as to be the issue. Book is important thing to increase you knowledge, except your teacher or lecturer. You find good news or update concerning something by book. Many kinds of books that can you choose to use be your object. One of them are these claims Mastering Python Forensics.

Read Mastering Python Forensics by Dr. Michael Spreitzenbarth, Dr. Johann Uhrmann for online ebook

Mastering Python Forensics by Dr. Michael Spreitzenbarth, Dr. Johann Uhrmann 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 Mastering Python Forensics by Dr. Michael Spreitzenbarth, Dr. Johann Uhrmann books to read online.

Online Mastering Python Forensics by Dr. Michael Spreitzenbarth, Dr. Johann Uhrmann ebook PDF download

Mastering Python Forensics by Dr. Michael Spreitzenbarth, Dr. Johann Uhrmann Doc

Mastering Python Forensics by Dr. Michael Spreitzenbarth, Dr. Johann Uhrmann Mobipocket

Mastering Python Forensics by Dr. Michael Spreitzenbarth, Dr. Johann Uhrmann EPub