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:

Benny Joiner:

Have you spare time for the day? What do you do when you have much more or little spare time? Yep, you can choose the suitable activity with regard to spend your time. Any person spent their very own spare time to take a go walking, shopping, or went to the Mall. How about open or perhaps read a book entitled Mastering Python Forensics? Maybe it is to get best activity for you. You understand beside you can spend your time along with your favorite's book, you can cleverer than before. Do you agree with the opinion or you have additional opinion?

Diane Worrell:

The actual book Mastering Python Forensics has a lot info on it. So when you read this book you can get a lot of advantage. The book was published by the very famous author. Tom makes some research previous to write this book. This specific book very easy to read you can get the point easily after scanning this book.

Lisa Bentley:

Exactly why? Because this Mastering Python Forensics is an unordinary book that the inside of the publication waiting for you to snap the item but latter it will distress you with the secret the idea inside. Reading this book next to it was fantastic author who have write the book in such wonderful way makes the content within easier to understand, entertaining technique but still convey the meaning fully. So , it is good for you because of not hesitating having this any longer or you going to regret it. This amazing book will give you a lot of gains than the other book have such as help improving your expertise and your critical thinking means. So , still want to hesitate having that book? If I were being you I will go to the publication store hurriedly.

Sherry Fitzgerald:

Mastering Python Forensics can be one of your nice books that are good idea. We all recommend that straight away because this e-book has good vocabulary that may increase your knowledge in terminology, easy to understand, bit entertaining but delivering the information. The article writer giving his/her effort to get every word into satisfaction arrangement in writing Mastering Python Forensics but doesn't forget the main point, giving the reader the hottest in addition to based confirm resource data that maybe you can be among it. This great information may drawn you into new stage of crucial thinking.

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