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:

Carmen Russell:

Here thing why this specific Mastering Python Forensics are different and dependable to be yours. First of all examining a book is good nonetheless it depends in the content from it which is the content is as scrumptious as food or not. Mastering Python Forensics giving you information deeper since different ways, you can find any publication out there but there is no reserve that similar with Mastering Python Forensics. It gives you thrill studying journey, its open up your personal eyes about the thing that will happened in the world which is might be can be happened around you. You can bring everywhere like in recreation area, café, or even in your method home by train. When you are having difficulties in bringing the imprinted book maybe the form of Mastering Python Forensics in e-book can be your choice.

Donald Diaz:

Is it you actually who having spare time then spend it whole day by means of watching television programs or just telling lies on the bed? Do you need something totally new? This Mastering Python Forensics can be the solution, oh how comes? A book you know. You are consequently out of date, spending your spare time by reading in this brand-new era is common not a geek activity. So what these ebooks have than the others?

Kelli Valverde:

In this particular era which is the greater man or woman or who has ability to do something more are more special than other. Do you want to become certainly one of it? It is just simple way to have that. What you should do is just spending your time very little but quite enough to have a look at some books. On the list of books in the top checklist in your reading list is definitely Mastering Python Forensics. This book and that is qualified as The Hungry Hills can get you closer in getting precious person. By looking upwards and review this publication you can get many advantages.

Teresa Thomas:

As we know that book is very important thing to add our information for everything. By a reserve we can know everything we want. A book is a range of written, printed, illustrated or even blank sheet. Every year has been exactly added. This book Mastering Python Forensics was filled concerning science. Spend your extra time to add your knowledge about your scientific research competence. Some people has different feel when they reading a new book. If you know how big good thing about a book, you can truly feel enjoy to read a reserve. In the modern era like currently, many ways to get book that you just wanted.

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