Mastering Python Forensics

Dr. Michael Spreitzenbarth, Dr. Johann Uhrmann

Download now

Read Online

Click here if your download doesn"t start automatically

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 Mastering Python Forensics ...pdf

Read Online Mastering Python Forensics ...pdf

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

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

---

From reader reviews:

Wilma Baca:

Do you among people who can't read pleasant if the sentence chained in the straightway, hold on guys this particular aren't like that. This Mastering Python Forensics book is readable simply by you who hate the perfect word style. You will find the info here are arrange for enjoyable studying experience without leaving also decrease the knowledge that want to deliver to you. The writer connected with Mastering Python Forensics content conveys prospect easily to understand by a lot of people. The printed and e-book are not different in the information but it just different in the form of it. So , do you continue to thinking Mastering Python Forensics is not loveable to be your top checklist reading book?

Renee Oneal:

Nowadays reading books become more than want or need but also become a life style. This reading routine give you lot of advantages. The advantages you got of course the knowledge the particular information inside the book this improve your knowledge and information. The knowledge you get based on what kind of e-book you read, if you want attract knowledge just go with knowledge books but if you want truly feel happy read one along with theme for entertaining including comic or novel. Typically the Mastering Python Forensics is kind of reserve which is giving the reader erratic experience.

Damon Smith:

The reserve untitled Mastering Python Forensics is the reserve that recommended to you to see. You can see the quality of the reserve content that will be shown to you actually. The language that writer use to explained their way of doing something is easily to understand. The article writer was did a lot of exploration when write the book, therefore the information that they share to your account is absolutely accurate. You also could get the e-book of Mastering Python Forensics from the publisher to make you much more enjoy free time.

Maryann Warren:

A lot of people always spent their free time to vacation or maybe go to the outside with them friends and family or their friend. Do you know? Many a lot of people spent these people free time just watching TV, or even playing video games all day long. If you wish to try to find a new activity that is look different you can read any book. It is really fun to suit your needs. If you enjoy the book that you simply read you can spent all day every day to reading a publication. The book Mastering Python Forensics it is quite good to read. There are a lot of individuals who recommended this book. These were enjoying reading this book. If you did not have enough space to deliver this book you can buy the e-book. You can m0ore effortlessly to read this book through your smart phone. The price is not too expensive but this book possesses high quality.

Download and Read Online Mastering Python Forensics Dr. Michael Spreitzenbarth, Dr. Johann Uhrmann #VHZLPNMA8WS

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