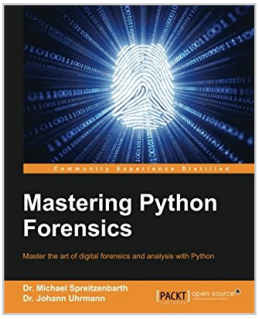

Mastering Python Forensics

By Dr. Michael Spreitzenbarth, Dr. Johann Uhrmann

Mastering Python Forensics By 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.

Mastering Python Forensics

By Dr. Michael Spreitzenbarth, Dr. Johann Uhrmann

Mastering Python Forensics By 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.

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

- Sales Rank: #1493353 in Books
- Published on: 2015-10-30
- Released on: 2015-10-30
- Original language: English
- Number of items: 1
- Dimensions: 9.25" h x .44" w x 7.50" l, .75 pounds
- Binding: Paperback
- 192 pages

Editorial Review

About the Author

Dr. Michael Spreitzenbarth

Dr. Michael Spreitzenbarth holds a degree of doctor of engineering in IT security from the University of Erlangen-Nuremberg and is a CISSP as well as a GMOB. He has been an IT security consultant at a worldwide operating CERT for more than three years and has worked as a freelancer in the field of mobile phone forensics, malware analysis, and IT security consultancy for more than six years. Since the last four years, he has been giving talks and lectures in the fields of forensics and mobile security at various universities and in the private sector.

Dr. Johann Uhrmann

Dr. Johann Uhrmann holds a degree in computer science from the University of Applied Sciences Landshut and a doctor of engineering from the University of the German Federal Armed Forces. He has more than ten years of experience in software development, which includes working for start-ups, institutional research, and corporate environment. Johann has several years of experience in incident handling and IT governance, focusing on Linux and Cloud environments.

Users Review

From reader reviews:

Jetta Butler:

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

Barbara Tucker:

Book is actually written, printed, or illustrated for everything. You can realize everything you want by a guide. Book has a different type. As it is known to us that book is important point to bring us around the world. Beside that you can your reading ability was fluently. A e-book Mastering Python Forensics will make you to become smarter. You can feel much more confidence if you can know about every thing. But some of you think that will open or reading some sort of book make you bored. It is not necessarily make you fun. Why they could be thought like that? Have you trying to find best book or suited book with you?

Robert Marshall:

As people who live in the particular modest era should be up-date about what going on or facts even knowledge to make these people keep up with the era which can be always change and move forward. Some of you maybe can update themselves by reading books. It is a good choice for yourself but the problems coming to a person is you don't know what one you should start with. This Mastering Python Forensics is our recommendation to cause you to keep up with the world. Why, as this book serves what you want and wish in this era.

Warren Bowers:

The book Mastering Python Forensics will bring someone to the new experience of reading the book. The author style to elucidate the idea is very unique. Should you try to find new book you just read, this book very ideal to you. The book Mastering Python Forensics is much recommended to you to read. You can also get the e-book from the official web site, so you can quicker to read the book.

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

HGN50VSD9O3: Mastering Python Forensics By Dr. Michael Spreitzenbarth, Dr. Johann Uhrmann