Linux Forensics

Philip Polstra

Linux Forensics

Philip Polstra

Linux Forensics Philip Polstra

Linux Forensics is the most comprehensive and up-to-date resource for those wishing to quickly and efficiently perform forensics on Linux systems. It is also a great asset for anyone that would like to better understand Linux internals.

Linux Forensics will guide you step by step through the process of investigating a computer running Linux. Everything you need to know from the moment you receive the call from someone who thinks they have been attacked until the final report is written is covered in this book. All of the tools discussed in this book are free and most are also open source.

Dr. Philip Polstra shows how to leverage numerous tools such as Python, shell scripting, and MySQL to quickly, easily, and accurately analyze Linux systems. While readers will have a strong grasp of Python and shell scripting by the time they complete this book, no prior knowledge of either of these scripting languages is assumed. **Linux Forensics** begins by showing you how to determine if there was an incident with minimally invasive techniques. Once it appears likely that an incident has occurred, Dr. Polstra shows you how to collect data from a live system before shutting it down for the creation of filesystem images.

Linux Forensics contains extensive coverage of Linux ext2, ext3, and ext4 filesystems. A large collection of Python and shell scripts for creating, mounting, and analyzing filesystem images are presented in this book. Dr. Polstra introduces readers to the exciting new field of memory analysis using the Volatility framework. Discussions of advanced attacks and malware analysis round out the book.

Book Highlights

- 370 pages in large, easy-to-read 8.5 x 11 inch format
- Over 9000 lines of Python scripts with explanations
- Over 800 lines of shell scripts with explanations
- A 102 page chapter containing up-to-date information on the ext4 filesystem
- Two scenarios described in detail with images available from the book website
- All scripts and other support files are available from the book website

Chapter Contents

- Automation With Scripting

3. Live Analysis
   - Getting Metadata
   - Using Spreadsheets
   - Getting Command Histories
   - Getting Logs
   - Using Hashes
   - Dumping RAM
4. Creating Images
   - Shutting Down the System
   - Image Formats
   - DD
   - DCFLDD
   - Write Blocking
   - Imaging Virtual Machines
   - Imaging Physical Drives
5. Mounting Images
   - Master Boot Record Based Partions
   - GUID Partition Tables
   - Mounting Partitions In Linux
   - Automating With Python
6. Analyzing Mounted Images
   - Getting Timestamps
   - Using LibreOffice
   - Using MySQL
   - Creating Timelines
7. Extended Filesystems
   - Basics
   - Superblocks
   - Features
   - Using Python
   - Finding Things That Are Out Of Place
   - Inodes
   - Journaling
8. Memory Analysis
   - Volatility
   - Creating Profiles
   - Linux Commands
9. Dealing With More Advanced Attackers
10. Malware
    - Is It Malware?
    - Malware Analysis Tools
    - Static Analysis
    - Dynamic Analysis
    - Obfuscation
11. The Road Ahead
    - Learning More
    - Communities
    - Conferences

- Certifications

Download and Read Free Online Linux Forensics Philip Polstra

From reader reviews:

Hannelore Evans:

Do you have favorite book? For those who have, what is your favorite's book? Guide is very important thing for us to find out everything in the world. Each reserve has different aim or even goal; it means that reserve has different type. Some people really feel enjoy to spend their time and energy to read a book. They are reading whatever they acquire because their hobby is reading a book. Think about the person who don't like reading through a book? Sometime, man or woman feel need book once they found difficult problem or exercise. Well, probably you will need this Linux Forensics.

Gordon Woods:

The book Linux Forensics give you a sense of feeling enjoy for your spare time. You can utilize to make your capable much more increase. Book can for being your best friend when you getting strain or having big problem along with your subject. If you can make looking at a book Linux Forensics for being your habit, you can get a lot more advantages, like add your personal capable, increase your knowledge about several or all subjects. You could know everything if you like wide open and read a publication Linux Forensics. Kinds of book are several. It means that, science reserve or encyclopedia or other folks. So , how do you think about this publication?

Robert Banks:

The guide with title Linux Forensics contains a lot of information that you can find out it. You can get a lot of gain after read this book. That book exist new information the information that exist in this guide represented the condition of the world right now. That is important to yo7u to learn how the improvement of the world. That book will bring you with new era of the globalization. You can read the e-book on your smart phone, so you can read this anywhere you want.

Gary Lewis:

Don't be worry for anyone who is afraid that this book will filled the space in your house, you could have it in e-book way, more simple and reachable. That Linux Forensics can give you a lot of friends because by you checking out this one book you have thing that they don't and make a person more like an interesting person. This particular book can be one of one step for you to get success. This book offer you information that possibly your friend doesn't learn, by knowing more than different make you to be great folks. So , why hesitate? We should have Linux Forensics.

Read Linux Forensics by Philip Polstra for online ebook

Linux Forensics by Philip Polstra 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 Linux Forensics by Philip Polstra books to read online.

Online Linux Forensics by Philip Polstra ebook PDF download

Linux Forensics by Philip Polstra Doc

Linux Forensics by Philip Polstra Mobipocket

Linux Forensics by Philip Polstra EPub

Linux Forensics by Philip Polstra Ebook online

Linux Forensics by Philip Polstra Ebook PDF