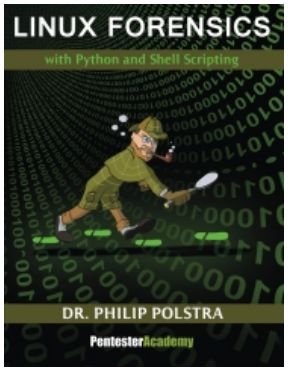

List Price: $49.00

Add to Cart

Linux Forensics

Authored by Dr. Philip Polstra
Edition: 1

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

About the author:
Dr. Philip Polstra (known to his friends as Dr. Phil) is an internationally recognized hardware hacker. His work has been presented at numerous conferences around the globe including repeat performances at DEFCON (six presentations in four years), BlackHat, 44CON, GrrCON, MakerFaire, ForenSecure, and other top conferences. Dr. Polstra is a well-known expert on USB forensics and has published several articles on this topic. He has developed a number of video courses including ones on Linux forensics, USB forensics, and reverse engineering.

Dr. Polstra has developed degree programs in digital forensics and ethical hacking while serving as a professor and Hacker in Residence at a private university in the Midwestern United States. He currently teaches in one of the top Digital Forensics degree programs in the United States at Bloomsburg University of Pennsylvania. In addition to teaching, he provides training and performs penetration tests on a consulting basis. When not working, he has been known to fly, build aircraft, and tinker with electronics. He is an accomplished aviator with thousands of hours of flight time and a dozen ratings as a pilot, flight instructor, mechanic, aircraft inspector, and avionics specialist. His latest happenings can be found on his website http://philpolstra.com. You can also follow him at @ppolstra on Twitter.

Dr. Polstra authored **Hacking and Penetration Testing with Low Power Devices** (Syngress, 2014) in which he showed the world how to easily build drop boxes, hacking consoles, and remote hacking drones with the BeagleBone Black and similar devices. In the course of creating these devices he developed his own Linux, *Deck Linux*, which is optimized for security testing with ARM-based devices. Techniques described in this book permit security penetration tests to be performed with multiple, possibly battery powered, devices which are controlled by a user up to two miles away from the target organization.

His latest book, **Linux Forensics** (Pentester Academy, 2015), is the most comprehensive and up-to-date resource available to anyone wishing to perform forensics on Linux systems. The first printing of this book sold out in under twenty five hours. This book is

- All scripts and other support files are available from the book website

considered a must have by a number of forensic investigators around the world.

Chapter Contents

1. First Steps
   - General Principles
   - Phases of Investigation
   - High-level Process
   - Building a Toolkit
2. Determining If There Was an Incident
   - Opening a Case
   - Talking to Users
   - Documenation
   - Mounting Known-good Binaries
   - Minimizing Disturbance to the Subject
   - 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

Publication Date:	七月 13 2015
ISBN/EAN13:	1515037630 / 9781515037637
Page Count:	370
Binding Type:	US Trade Paper
Trim Size:	8.5" x 11"
Language:	English
Color:	Black and White
Related Categories:	Computers / Security / General