UNIX and Linux Forensic Analysis DVD Toolkit

Chris Pogue, Cory Altheide, Todd Haverkos

UNIX and Linux Forensic Analysis DVD Toolkit

Chris Pogue, Cory Altheide, Todd Haverkos

UNIX and Linux Forensic Analysis DVD Toolkit Chris Pogue, Cory Altheide, Todd Haverkos
This book addresses topics in the area of forensic analysis of systems running on variants of the UNIX operating system, which is the choice of hackers for their attack platforms. According to a 2007 IDC report, UNIX servers account for the second-largest segment of spending (behind Windows) in the worldwide server market with $4.2 billion in 2Q07, representing 31.7% of corporate server spending. UNIX systems have not been analyzed to any significant depth largely due to a lack of understanding on the part of the investigator, an understanding and knowledge base that has been achieved by the attacker. The companion DVD provides a simulated or "live" UNIX environment where readers can test the skills they've learned in the book and use custom tools developed by the authors.

The book begins with a chapter to describe why and how the book was written, and for whom, and then immediately begins addressing the issues of live response (volatile) data collection and analysis. The book continues by addressing issues of collecting and analyzing the contents of physical memory (i.e., RAM). The following chapters address /proc analysis, revealing the wealth of significant evidence, and analysis of files created by or on UNIX systems. Then the book addresses the underground world of UNIX hacking and reveals methods and techniques used by hackers, malware coders, and anti-forensic developers. The book then illustrates to the investigator how to analyze these files and extract the information they need to perform a comprehensive forensic analysis. The final chapter includes a detailed discussion of Loadable Kernel Modules and Malware. The companion DVD provides a simulated or "live" UNIX environment where readers can test the skills they've learned in the book and use custom tools developed by the authors.

Throughout the book the author provides a wealth of unique information, providing tools, techniques and information that won't be found anywhere else. Not only are the tools provided, but the author also provides sample files so that after completing a detailed walk-through, the reader can immediately practice the new-found skills.

* The companion DVD for the book contains significant, unique materials (movies, spreadsheet, code, etc.) not available any place else.
* This book contains information about UNIX forensic analysis that is not available anywhere else. Much of the information is a result of the author's own unique research and work.
* The authors have the combined experience of Law Enforcement, Military, and Corporate forensics. This unique perspective makes this book attractive to ALL forensic investigators.

Note: The Kindle edition of this book does not include any CDs or DVDs.

Download and Read Free Online UNIX and Linux Forensic Analysis DVD Toolkit Chris Pogue, Cory Altheide, Todd Haverkos

---

From reader reviews:

Ann Fout:

Why don't make it to be your habit? Right now, try to ready your time to do the important behave, like looking for your favorite reserve and reading a e-book. Beside you can solve your problem; you can add your knowledge by the e-book entitled UNIX and Linux Forensic Analysis DVD Toolkit. Try to face the book UNIX and Linux Forensic Analysis DVD Toolkit as your pal. It means that it can for being your friend when you experience alone and beside regarding course make you smarter than in the past. Yeah, it is very fortuned for you. The book makes you much more confidence because you can know anything by the book. So , we need to make new experience along with knowledge with this book.

Donald Farrell:

Do you among people who can't read pleasant if the sentence chained within the straightway, hold on guys this aren't like that. This UNIX and Linux Forensic Analysis DVD Toolkit book is readable simply by you who hate those straight word style. You will find the information here are arrange for enjoyable looking at experience without leaving also decrease the knowledge that want to provide to you. The writer regarding UNIX and Linux Forensic Analysis DVD Toolkit content conveys the thought easily to understand by many individuals. The printed and e-book are not different in the articles but it just different in the form of it. So , do you nonetheless thinking UNIX and Linux Forensic Analysis DVD Toolkit is not loveable to be your top checklist reading book?

Aaron Eldred:

Playing with family within a park, coming to see the water world or hanging out with friends is thing that usually you may have done when you have spare time, in that case why you don't try thing that really opposite from that. A single activity that make you not experience tired but still relaxing, trilling like on roller coaster you have been ride on and with addition of information. Even you love UNIX and Linux Forensic Analysis DVD Toolkit, it is possible to enjoy both. It is excellent combination right, you still wish to miss it? What kind of hang-out type is it? Oh occur its mind hangout men. What? Still don't obtain it, oh come on its referred to as reading friends.

Amy Christensen:

Do you like reading a publication? Confuse to looking for your best book? Or your book ended up being rare? Why so many problem for the book? But any people feel that they enjoy for reading. Some people likes looking at, not only science book and also novel and UNIX and Linux Forensic Analysis DVD Toolkit or others sources were given know-how for you. After you know how the good a book, you feel wish to read more and more. Science publication was created for teacher or perhaps students especially. Those ebooks are helping them to bring their knowledge. In other case, beside science e-book, any other book likes UNIX and Linux Forensic Analysis DVD Toolkit to make your spare time far more colorful. Many types of book like

this.

Read UNIX and Linux Forensic Analysis DVD Toolkit by Chris Pogue, Cory Altheide, Todd Haverkos for online ebook

UNIX and Linux Forensic Analysis DVD Toolkit by Chris Pogue, Cory Altheide, Todd Haverkos 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 UNIX and Linux Forensic Analysis DVD Toolkit by Chris Pogue, Cory Altheide, Todd Haverkos books to read online.

Online UNIX and Linux Forensic Analysis DVD Toolkit by Chris Pogue, Cory Altheide, Todd Haverkos ebook PDF download

UNIX and Linux Forensic Analysis DVD Toolkit by Chris Pogue, Cory Altheide, Todd Haverkos Doc

UNIX and Linux Forensic Analysis DVD Toolkit by Chris Pogue, Cory Altheide, Todd Haverkos Mobipocket

UNIX and Linux Forensic Analysis DVD Toolkit by Chris Pogue, Cory Altheide, Todd Haverkos EPub