Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring

Harlan Carvey, Jeremy Faircloth

Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring

Harlan Carvey, Jeremy Faircloth

Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring Harlan Carvey, Jeremy Faircloth

I decided to write this book for a couple of reasons. One was that I've now written a couple of books that have to do with incident response and forensic analysis on Windows systems, and I used a lot of Perl in both books. Okay…I'll come clean…I used nothing but Perl in both books! What I've seen as a result of this is that many readers want to use the tools, but don't know how…they simply aren't familiar with Perl, with interpreted (or scripting) languages in general, and may not be entirely comfortable with running tools at the command line. This book is intended for anyone who has an interest in useful Perl scripting, in particular on the Windows platform, for the purpose of incident response, and forensic analysis, and application monitoring. While a thorough grounding in scripting languages (or in Perl specifically) is not required, it helpful in fully and more completely understanding the material and code presented in this book. This book contains information that is useful to consultants who perform incident response and computer forensics, specifically as those activities pertain to MS Windows systems (Windows 2000, XP, 2003, and some Vista). My hope is that not only will consultants (such as myself) find this material valuable, but so will system administrators, law enforcement officers, and students in undergraduate and graduate programs focusing on computer forensics.

Code can be found at: http://www.elsevierdirect.com/companion.jsp?ISBN=9781597491730

*Perl Scripting for Live Response

Using Perl, there's a great deal of information you can retrieve from systems, locally or remotely, as part of troubleshooting or investigating an issue. Perl scripts can be run from a central management point, reaching out to remote systems in order to collect information, or they can be "compiled" into standalone executables using PAR, PerlApp, or Perl2Exe so that they can be run on systems that do not have ActiveState's Perl distribution (or any other Perl distribution) installed.

*Perl Scripting for Computer Forensic Analysis

Perl is an extremely useful and powerful tool for performing computer forensic analysis. While there are applications available that let an examiner access acquired images and perform some modicum of visualization, there are relatively few tools that meet the specific needs of a specific examiner working on a specific case. This is where the use of Perl really shines through and becomes apparent.

*Perl Scripting for Application Monitoring

Working with enterprise-level Windows applications requires a great deal of analysis and constant monitoring. Automating the monitoring portion of this effort can save a great deal of time, reduce system downtimes, and improve the reliability of your overall application. By utilizing Perl scripts and integrating them with the application technology, you can easily build a simple monitoring framework that can alert you

to current or future application issues.

Download and Read Free Online Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring Harlan Carvey, Jeremy Faircloth

---

From reader reviews:

Earl Goodman:

The experience that you get from Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring will be the more deep you excavating the information that hide within the words the more you get considering reading it. It doesn't mean that this book is hard to recognise but Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring giving you thrill feeling of reading. The copy writer conveys their point in particular way that can be understood by anyone who read that because the author of this book is well-known enough. This specific book also makes your personal vocabulary increase well. So it is easy to understand then can go along with you, both in printed or e-book style are available. We highly recommend you for having this kind of Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring instantly.

Antoinette Hogg:

Information is provisions for individuals to get better life, information these days can get by anyone from everywhere. The information can be a information or any news even restricted. What people must be consider if those information which is within the former life are hard to be find than now is taking seriously which one works to believe or which one the actual resource are convinced. If you get the unstable resource then you get it as your main information you will have huge disadvantage for you. All of those possibilities will not happen inside you if you take Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring as the daily resource information.

Gerri Pettit:

Reading a book being new life style in this yr; every people loves to study a book. When you study a book you can get a lot of benefit. When you read textbooks, you can improve your knowledge, simply because book has a lot of information on it. The information that you will get depend on what sorts of book that you have read. If you would like get information about your review, you can read education books, but if you want to entertain yourself you can read a fiction books, this kind of us novel, comics, and also soon. The Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring offer you a new experience in reading through a book.

Gloria Lentz:

As we know that book is vital thing to add our knowledge for everything. By a reserve we can know everything we would like. A book is a pair of written, printed, illustrated or blank sheet. Every year seemed to be exactly added. This publication Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring was filled in relation to science. Spend your extra time to add your knowledge about your technology competence. Some people has different feel when they reading a book. If you know how big benefit of a book, you can feel enjoy to read a reserve. In the modern era like now, many ways to

get book that you simply wanted.

Read Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring by Harlan Carvey, Jeremy Faircloth for online ebook

Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring by Harlan Carvey, Jeremy Faircloth 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 Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring by Harlan Carvey, Jeremy Faircloth books to read online.

Online Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring by Harlan Carvey, Jeremy Faircloth ebook PDF download

Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring by Harlan Carvey, Jeremy Faircloth Doc

Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring by Harlan Carvey, Jeremy Faircloth Mobipocket

Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring by Harlan Carvey, Jeremy Faircloth EPub