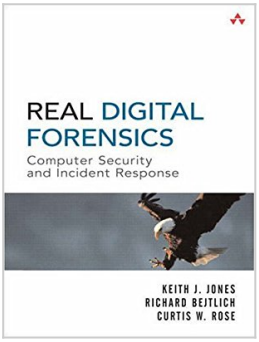


# Real Digital Forensics: Computer Security and Incident Response

*By Keith J. Jones, Richard Bejtlich, Curtis W. Rose*



**Real Digital Forensics: Computer Security and Incident Response** By Keith J. Jones, Richard Bejtlich, Curtis W. Rose

This is a book and DVD set providing an interactive experience that helps readers master the tools and techniques of forensic analysis by investigating real cases. Offers practical hands-on approach to solving problems encountered when performing computer-related investigations. It's authors are well known and well respected in the industry, speak widely, and teach forensics classes. The motto of this book and DVD set is learn by doing. Many people understand the basics of computer forensics and incident response, but lack the necessary skills and direct experience to tackle a case on their own. Organized around case studies, this book offers a comprehensive introduction to the methods, techniques, and tools of forensic investigations through direct contact with real cases. All of the material is introduced within the context of a complete forensic investigation, and the book's companion DVD allows readers to immediately test their skills by working with real data.

# Real Digital Forensics: Computer Security and Incident Response

*By Keith J. Jones, Richard Bejtlich, Curtis W. Rose*

**Real Digital Forensics: Computer Security and Incident Response** By Keith J. Jones, Richard Bejtlich, Curtis W. Rose

This is a book and DVD set providing an interactive experience that helps readers master the tools and techniques of forensic analysis by investigating real cases. Offers practical hands-on approach to solving problems encountered when performing computer-related investigations. It's authors are well known and well respected in the industry, speak widely, and teach forensics classes. The motto of this book and DVD set is learn by doing. Many people understand the basics of computer forensics and incident response, but lack the necessary skills and direct experience to tackle a case on their own. Organized around case studies, this book offers a comprehensive introduction to the methods, techniques, and tools of forensic investigations through direct contact with real cases. All of the material is introduced within the context of a complete forensic investigation, and the book's companion DVD allows readers to immediately test their skills by working with real data.

**Real Digital Forensics: Computer Security and Incident Response By Keith J. Jones, Richard Bejtlich, Curtis W. Rose Bibliography**

- Sales Rank: #292505 in Books
- Published on: 2005-10-03
- Original language: English
- Number of items: 1
- Dimensions: 9.20" h x 1.70" w x 7.00" l, 2.44 pounds
- Binding: Paperback
- 688 pages

# Preface

# Our Purpose and Approach

Welcome to the book named *Real Digital Forensics*. When we conceived this book, we wanted to give forensic investigators more than words to learn new skills. Many people express to us in our classes and speaking engagements a simple sentence we have heard hundreds of times: "How do I get into the field of computer forensics?" In our opinion, you cannot learn forensics unless you have hands-on practical experience. This brings up a more important question we usually hear next: "How do I get my hands on data to gain that experience?" This question is much more difficult to answer because the only data most people have to practice with comes from real cases—and we all know that our clients do not want their data disseminated for learning tools! Therefore, it is difficult for most people to find data to practice with in order to sharpen their computer forensic skills. To answer this second question, we decided to publish this book with a DVD containing realistic evidence collected from several fictitious scenarios for the sole purpose of teaching the computer forensic tradecraft.

Most of the scenarios you will find throughout this book are very similar to types of cases that we investigate every day. We used the same tools attackers use when establishing a foothold in your network, the same methods rogue employees make use of to steal your trade secrets, and the same media we typically collect when we created the evidence files found on the DVD. Although we attempted to thoroughly investigate each company name we used for our scenarios, we want to state that *none of this data was collected from computers within companies with coincidentally similar names or IP addresses*.

The book begins by presenting methodologies used for the collection and analysis of computer forensic data. Then the book presents methods for compiling tool kits you can take with you to the scene of a computer-related crime. The book concludes by providing methodologies for deeper forensic analysis and solutions for when you run into other types of computer media such as USB memory and Palm devices.

Although computer forensic software tends to be commercially dominated, which means you would have to pay a hefty licensing fee just to get your feet wet, we wholeheartedly believe in open source because of the documented methodologies and availability of the source code. Reproducibility and documentation of methodologies is the cornerstone of any forensic science. Therefore, you will find that most techniques we recommend utilize a freely available and publicly documented toolset. This will enable you to examine the evidence found on the DVD without having to purchase additional software. When we do talk about commercial software to help round out your knowledge base, we will point it out in the text so that you are fully aware.

You will find that this book takes a practical, hands-on approach to solving problems that we frequently encounter when performing computer-related investigations. This book will not contain pages and pages about the theory of computer forensics. What it will contain are techniques you can employ immediately to solve your problems when performing an analysis. We hope you enjoy the *Real Digital Forensics* experience.

# The Prerequisites and Target Audiences

Some of the techniques we discuss in this book are considered more advanced than common forensic knowledge. If you are just starting out in the computer forensic field, we suggest a basic understanding of computer forensics to more fully enjoy the content within this book. For an understanding of computer forensics that will help you work through the investigations throughout this book, we recommend you review

the following publications:

- *The Tao of Network Security Monitoring: Beyond Intrusion Detection* by Richard Bejtlich
- *Extrusion Detection: Security Monitoring for Internal Intrusions* by Richard Bejtlich
- *Incident Response: Investigating Computer Crime* by Kevin Mandia, Chris Prosise, and Matt Pepe
- *File System Forensic Analysis* by Brian Carrier
- *Computer Forensics* by Kruse, Warren and Jay Heiser

# About the Art

Due to the complex nature of the data we discuss, some of our screenshots may appear small in this book and may be difficult to read. We have made all the artwork available at http://www.realdigitalforensics.com.

# How To Use the DVD

All the evidence collected for each of the scenarios presented throughout the book is loaded on the DVD. If you insert the DVD into a Windows machine, a new drive such as D: or E: will appear. If you insert the DVD into a Unix machine, you will need to mount the file system using the mount command, such as:

```
?mount /dev/cdrom /mnt/realdigitalforensics
```

Off of the DVD root directory, you will find another directory named after the scenario. Typically this directory has the same name as the victim company's name. For example, to find the "JBR Bank's Intrusion" scenario, you would navigate to the jbr_bank directory on the DVD. Within the scenario directory, you will find more subdirectories. Each subdirectory contains a particular type of evidence that the investigator collected. If the investigator acquired a forensic duplication, you can find the corresponding data in the forensic_duplication directory. If the responder performed a live response, the live_response directory will contain the relevant data, and so on.

Most of the data on the DVD is stored in native format. The live response data is plain text, memory dumps are binary files, and so on. When you want to examine a forensic duplication, you will notice that the files are compressed. This was done because the duplications can be up to 4 GB in size when they are uncompressed, which would not fit on a single DVD. *Therefore, be warned—you may want to have 10 to 20 GB of working room on your hard drive when you analyze this evidence.* To analyze a forensic duplication, you must first copy the evidence from the DVD to your local hard drive and uncompress the duplication. The forensic duplications can be uncompressed with Winzip (http://www.winzip.com) in Windows or unzip/gzip in Unix.

The data on the DVD represents our best efforts to mirror the real world scenarios we encounter every day. We were forced, unfortunately, to perform some post processing so that we did not distribute copies of commercial software. Therefore, some system-related files on the victim machines containing the Windows operating system had zeros written over it. The original size of the file and directory structure we kept "as is" to simulate a real machine.

With that in mind, please load up your DVD and follow along with our many examples. We invite you to visit our Web site, http://www.realdigitalforensics.com, for updates to the text, links to forensics tools, and other information to make your incident response and forensics duties more pleasurable.

# Read Real Digital Forensics: Computer Security and Incident Response By Keith J. Jones, Richard Bejtlich, Curtis W. Rose for online ebook

Real Digital Forensics: Computer Security and Incident Response By Keith J. Jones, Richard Bejtlich, Curtis W. Rose 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 Real Digital Forensics: Computer Security and Incident Response By Keith J. Jones, Richard Bejtlich, Curtis W. Rose books to read online.

## Online Real Digital Forensics: Computer Security and Incident Response By Keith J. Jones, Richard Bejtlich, Curtis W. Rose ebook PDF download

### Real Digital Forensics: Computer Security and Incident Response By Keith J. Jones, Richard Bejtlich, Curtis W. Rose Doc

**Real Digital Forensics: Computer Security and Incident Response By Keith J. Jones, Richard Bejtlich, Curtis W. Rose Mobipocket**

**Real Digital Forensics: Computer Security and Incident Response By Keith J. Jones, Richard Bejtlich, Curtis W. Rose EPub**