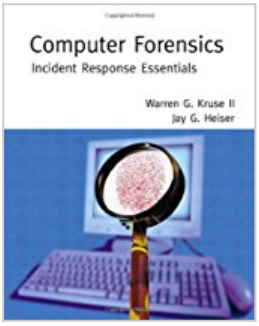

Computer Forensics: Incident Response Essentials

By Warren G. Kruse II, Jay G. Heiser

Computer Forensics: Incident Response Essentials By Warren G. Kruse II, Jay G. Heiser

Every computer crime leaves tracks—you just have to know where to find them. This book shows you how to collect and analyze the digital evidence left behind in a digital crime scene.

Computers have always been susceptible to unwanted intrusions, but as the sophistication of computer technology increases so does the need to anticipate, and safeguard against, a corresponding rise in computer-related criminal activity.

Computer forensics, the newest branch of computer security, focuses on the aftermath of a computer security incident. The goal of computer forensics is to conduct a structured investigation to determine exactly what happened, who was responsible, and to perform the investigation in such a way that the results are useful in a criminal proceeding.

Written by two experts in digital investigation, ***Computer Forensics*** provides extensive information on how to handle the computer as evidence. **Kruse** and **Heiser** walk the reader through the complete forensics process—from the initial collection of evidence through the final report. Topics include an overview of the forensic relevance of encryption, the examination of digital evidence for clues, and the most effective way to present your evidence and conclusions in court. Unique forensic issues associated with both the Unix and the Windows NT/2000 operating systems are thoroughly covered.

This book provides a detailed methodology for collecting, preserving, and effectively using evidence by addressing the three A's of computer forensics:

- **Acquire** the evidence without altering or damaging the original data.
- **Authenticate** that your recorded evidence is the same as the original seized data.
- **Analyze** the data without modifying the recovered data.

Computer Forensics is written for everyone who is responsible for investigating digital criminal incidents or who may be interested in the techniques that such investigators use. It is equally helpful to those investigating hacked web servers, and those who are investigating the source of illegal pornography.

0201707195B09052001

Computer Forensics: Incident Response Essentials

By Warren G. Kruse II, Jay G. Heiser

Computer Forensics: Incident Response Essentials By Warren G. Kruse II, Jay G. Heiser

Every computer crime leaves tracks—you just have to know where to find them. This book shows you how to collect and analyze the digital evidence left behind in a digital crime scene.

Computers have always been susceptible to unwanted intrusions, but as the sophistication of computer technology increases so does the need to anticipate, and safeguard against, a corresponding rise in computer-related criminal activity.

Computer forensics, the newest branch of computer security, focuses on the aftermath of a computer security incident. The goal of computer forensics is to conduct a structured investigation to determine exactly what happened, who was responsible, and to perform the investigation in such a way that the results are useful in a criminal proceeding.

Written by two experts in digital investigation, ***Computer Forensics*** provides extensive information on how to handle the computer as evidence. **Kruse** and **Heiser** walk the reader through the complete forensics process—from the initial collection of evidence through the final report. Topics include an overview of the forensic relevance of encryption, the examination of digital evidence for clues, and the most effective way to present your evidence and conclusions in court. Unique forensic issues associated with both the Unix and the Windows NT/2000 operating systems are thoroughly covered.

This book provides a detailed methodology for collecting, preserving, and effectively using evidence by addressing the three A's of computer forensics:

- **Acquire** the evidence without altering or damaging the original data.
- **Authenticate** that your recorded evidence is the same as the original seized data.
- **Analyze** the data without modifying the recovered data.

Computer Forensics is written for everyone who is responsible for investigating digital criminal incidents or who may be interested in the techniques that such investigators use. It is equally helpful to those investigating hacked web servers, and those who are investigating the source of illegal pornography.

0201707195B09052001

Computer Forensics: Incident Response Essentials By Warren G. Kruse II, Jay G. Heiser Bibliography

- Sales Rank: #929953 in Books
- Published on: 2001-10-06
- Original language: English
- Number of items: 1

- Dimensions: 9.10" h x .88" w x 7.40" l, 1.36 pounds
- Binding: Paperback
- 416 pages

Editorial Review

Amazon.com Review
Computer security is a crucial aspect of modern information management, and one of the latest buzzwords is *incident response*--detecting and reacting to security breaches. *Computer Forensics* offers information professionals a disciplined approach to implementing a comprehensive incident-response plan, with a focus on being able to detect intruders, discover what damage they did, and hopefully find out who they are.

There is little doubt that the authors are serious about cyberinvestigation. They advise companies to "treat every case like it will end up in court," and although this sounds extreme, it is good advice. Upon detecting a malicious attack on a system, many system administrators react instinctively. This often involves fixing the problem with minimal downtime, then providing the necessary incremental security to protect against an identical attack. The authors warn that this approach often contaminates evidence and makes it difficult to track the perpetrator. This book describes how to maximize system uptime while protecting the integrity of the "crime scene."

The bulk of *Computer Forensics* details the technical skills required to become an effective electronic sleuth, with an emphasis on providing a well-documented basis for a criminal investigation. The key to success is becoming a "white hat" hacker in order to combat the criminal "black hat" hackers. The message is clear: if you're not smart enough to break into someone else's system, you're probably not smart enough to catch someone breaking into your system. In this vein, the authors use a number of technical examples and encourage the readers to develop expertise in Unix/Linux and Windows NT fundamentals. They also provide an overview of a number of third-party tools, many of which can be used for both tracking hackers and to probe your own systems.

The authors explain their investigative techniques via a number of real-world anecdotes. It is striking that many of the same hacks detailed in Cliff Stoll's classic *The Cuckoo's Egg* are still in use over 10 years later--both on the criminal and investigative fronts. It is up to individual companies whether or not to pursue each attempted security violation as a potential criminal case, but *Computer Forensics* provides a strong argument to consider doing so. --*Pete Ostenson*

Topics covered: Overview of computer crime investigative response, including extensive descriptions of hacking techniques. Frequent examples are used to demonstrate how to extract evidence from a violated computer system. Appendices include sample incident-response forms.

From the Back Cover

Every computer crime leaves tracks--you just have to know where to find them. This book shows you how to collect and analyze the digital evidence left behind in a digital crime scene.

Computers have always been susceptible to unwanted intrusions, but as the sophistication of computer technology increases so does the need to anticipate, and safeguard against, a corresponding rise in computer-related criminal activity.

Computer forensics, the newest branch of computer security, focuses on the aftermath of a computer security incident. The goal of computer forensics is to conduct a structured investigation to determine exactly what happened, who was responsible, and to perform the investigation in such a way that the results are useful in a

criminal proceeding.

Written by two experts in digital investigation, "Computer Forensics" provides extensive information on how to handle the computer as evidence. Kruse and Heiser walk the reader through the complete forensics process--from the initial collection of evidence through the final report. Topics include an overview of the forensic relevance of encryption, the examination of digital evidence for clues, and the most effective way to present your evidence and conclusions in court. Unique forensic issues associated with both the Unix and the Windows NT/2000 operating systems are thoroughly covered.

This book provides a detailed methodology for collecting, preserving, and effectively using evidence by addressing the three A's of computer forensics:

- Acquire the evidence without altering or damaging the original data.
- Authenticate that your recorded evidence is the same as the original seized data.
- Analyze the data without modifying the recovered data.

"Computer Forensics" is written for everyone who is responsible for investigating digital criminal incidents or who may be interested in the techniques that such investigators use. It is equally helpful to those investigating hacked web servers, and those who are investigating the source of illegal pornography. 0201707195B09052001

About the Author

0201707195AB05232001

Users Review

From reader reviews:

Carl White:

Here thing why this particular Computer Forensics: Incident Response Essentials are different and trusted to be yours. First of all studying a book is good nevertheless it depends in the content of the usb ports which is the content is as delightful as food or not. Computer Forensics: Incident Response Essentials giving you information deeper since different ways, you can find any publication out there but there is no book that similar with Computer Forensics: Incident Response Essentials. It gives you thrill reading through journey, its open up your personal eyes about the thing this happened in the world which is might be can be happened around you. You can bring everywhere like in playground, café, or even in your method home by train. Should you be having difficulties in bringing the imprinted book maybe the form of Computer Forensics: Incident Response Essentials in e-book can be your option.

Mary Perez:

Many people spending their time period by playing outside having friends, fun activity having family or just watching TV the whole day. You can have new activity to invest your whole day by studying a book. Ugh, ya think reading a book can really hard because you have to take the book everywhere? It ok you can have the e-book, delivering everywhere you want in your Smart phone. Like Computer Forensics: Incident

Response Essentials which is finding the e-book version. So , try out this book? Let's see.

Rodney Natale:

That guide can make you to feel relax. This particular book Computer Forensics: Incident Response Essentials was bright colored and of course has pictures around. As we know that book Computer Forensics: Incident Response Essentials has many kinds or category. Start from kids until youngsters. For example Naruto or Detective Conan you can read and feel that you are the character on there. Therefore not at all of book are generally make you bored, any it can make you feel happy, fun and loosen up. Try to choose the best book for you and try to like reading in which.

Ashley Johnson:

A lot of reserve has printed but it differs from the others. You can get it by web on social media. You can choose the most effective book for you, science, comedian, novel, or whatever through searching from it. It is called of book Computer Forensics: Incident Response Essentials. You can include your knowledge by it. Without leaving behind the printed book, it might add your knowledge and make you happier to read. It is most essential that, you must aware about e-book. It can bring you from one destination to other place.

Read Computer Forensics: Incident Response Essentials By Warren G. Kruse II, Jay G. Heiser for online ebook

Computer Forensics: Incident Response Essentials By Warren G. Kruse II, Jay G. Heiser 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 Computer Forensics: Incident Response Essentials By Warren G. Kruse II, Jay G. Heiser books to read online.

Online Computer Forensics: Incident Response Essentials By Warren G. Kruse II, Jay G. Heiser ebook PDF download

Computer Forensics: Incident Response Essentials By Warren G. Kruse II, Jay G. Heiser Doc

Computer Forensics: Incident Response Essentials By Warren G. Kruse II, Jay G. Heiser Mobipocket

Computer Forensics: Incident Response Essentials By Warren G. Kruse II, Jay G. Heiser EPub