

Computer Forensics: Incident Response Essentials

By Warren G. Kruse II, Jay G. Heiser

Donwload Read Online

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

Download Computer Forensics: Incident Response Essentials ...pdf

Read Online Computer Forensics: Incident Response Essentials ...pdf

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

Download Computer Forensics: Incident Response Essentials ...pdf

Read Online Computer Forensics: Incident Response Essentials ...pdf

Download and Read Free Online Computer Forensics: Incident Response Essentials By Warren G. Kruse II, Jay G. Heiser

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:

Eldon Hall:

Book is written, printed, or created for everything. You can learn everything you want by a reserve. Book has a different type. As we know that book is important issue to bring us around the world. Beside that you can your reading proficiency was fluently. A publication Computer Forensics: Incident Response Essentials will make you to become smarter. You can feel a lot more confidence if you can know about anything. But some of you think that will open or reading a new book make you bored. It is not necessarily make you fun. Why they may be thought like that? Have you searching for best book or suitable book with you?

Albert Hartley:

Reading a reserve can be one of a lot of pastime that everyone in the world enjoys. Do you like reading book consequently. There are a lot of reasons why people enjoy it. First reading a publication will give you a lot of new info. When you read a reserve you will get new information mainly because book is one of a number of ways to share the information or even their idea. Second, examining a book will make you more imaginative. When you reading a book especially fictional book the author will bring you to definitely imagine the story how the character types do it anything. Third, you can share your knowledge to other folks. When you read this Computer Forensics: Incident Response Essentials, it is possible to tells your family, friends in addition

to soon about yours e-book. Your knowledge can inspire the others, make them reading a guide.

Jon Watson:

This Computer Forensics: Incident Response Essentials is brand new way for you who has attention to look for some information given it relief your hunger associated with. Getting deeper you upon it getting knowledge more you know or perhaps you who still having bit of digest in reading this Computer Forensics: Incident Response Essentials can be the light food to suit your needs because the information inside this specific book is easy to get by anyone. These books create itself in the form which is reachable by anyone, sure I mean in the e-book form. People who think that in book form make them feel drowsy even dizzy this e-book is the answer. So there is absolutely no in reading a e-book especially this one. You can find what you are looking for. It should be here for anyone. So , don't miss this! Just read this e-book kind for your better life in addition to knowledge.

Irma Lovern:

A lot of book has printed but it differs. You can get it by web on social media. You can choose the most effective book for you, science, comic, novel, or whatever by simply searching from it. It is called of book Computer Forensics: Incident Response Essentials. Contain your knowledge by it. Without causing the printed book, it may add your knowledge and make an individual happier to read. It is most significant that, you must aware about e-book. It can bring you from one location to other place.

Download and Read Online Computer Forensics: Incident Response Essentials By Warren G. Kruse II, Jay G. Heiser #8NVHX4PCJYS

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