Mastering Windows Network Forensics and Investigation

By Steven Anson, Steve Bunting

Mastering Windows Network Forensics and Investigation By Steven Anson, Steve Bunting

This comprehensive guide provides you with the training you need to arm yourself against phishing, bank fraud, unlawful hacking, and other computer crimes. Two seasoned law enforcement professionals discuss everything from recognizing high-tech criminal activity and collecting evidence to presenting it in a way that judges and juries can understand. They cover the range of skills, standards, and step-by-step procedures you'll need to conduct a criminal investigation in a Windows environment and make your evidence stand up in court.

Mastering Windows Network Forensics and Investigation

By Steven Anson, Steve Bunting

Mastering Windows Network Forensics and Investigation By Steven Anson, Steve Bunting

This comprehensive guide provides you with the training you need to arm yourself against phishing, bank fraud, unlawful hacking, and other computer crimes. Two seasoned law enforcement professionals discuss everything from recognizing high-tech criminal activity and collecting evidence to presenting it in a way that judges and juries can understand. They cover the range of skills, standards, and step-by-step procedures you'll need to conduct a criminal investigation in a Windows environment and make your evidence stand up in court.

Mastering Windows Network Forensics and Investigation By Steven Anson, Steve Bunting Bibliography

- Sales Rank: #1196407 in Books
- Published on: 2007-04-02
- Released on: 2012-10-15
- Original language: English
- Number of items: 1
- Dimensions: 9.30" h x 1.10" w x 7.30" l, 1.77 pounds
- Binding: Paperback
- 552 pages

[Download](#) Mastering Windows Network Forensics and Investigat ...pdf

[Read Online](#) Mastering Windows Network Forensics and Investig ...pdf

Editorial Review

From the Back Cover
Conduct Cutting-Edge Forensic Investigations of Computer Crimes.

Whether it's phishing, bank fraud, or unlawful hacking, computer crimes are on the rise, and law enforcement personnel who investigate these crimes must learn how to properly gather forensic evidence in the computer age.

Now you can get the training you need in this comprehensive guide from two seasoned law enforcement professionals. From recognizing high-tech criminal activity and collecting evidence to presenting it in a way that judges and juries can understand, this book covers the range of skills, standards, and step-by-step procedures you'll need to conduct a criminal investigation in a Windows environment and make your evidence stand up in court.

The book also covers the emerging field of "live forensics," where investigators examine a system to obtain evidence while it is still running, thus preserving live data that may be lost if the system is shut down.

COVERAGE INCLUDES:

- Responding to a reported computer intrusion
- Conducting the initial interview with the victims
- Understanding how attackers exploit Windows networks
- Deciphering Windows file systems, registries, and more
- Analyzing data rapidly using live analysis techniques
- Examining suspects' computers
- Using EnCase® for Windows event log analysis
- Presenting technically complicated material to juries

About the Author
Steve Anson , CISSP, MCSE, is a special agent with the Pentagon's Defense Criminal Investigative Service. He has a master's degree in computer science as well as numerous industry certifications. As a former contract instructor for the FBI, he has taught hundreds of veteran federal agents, state and local police officers, and intelligence agency employees techniques for conducting computerintrusion investigations. He also founded and supervised a local police department computer crime and information services unit and served as a task force agent for the FBI. He has conducted investigations involving large-scale computer intrusions, counterterrorism, crimes against children, and many other offenses involving the substantive use of computers.

Steve Bunting is a captain with the University of Delaware Police Department, where he is responsible for computer forensics, video forensics, and investigations involving computers. He has more than thirty years experience in law enforcement, and his background in computer forensics is extensive. He is a Certified Computer Forensics Technician (CCFT) and an EnCase Certified Examiner (EnCE). He was the recipient of the 2002 Guidance Software Certified Examiner Award of Excellence. He has a bachelor's degree in applied professions/business management from Wilmington College and a computer applications certificate in network environments from the University of Delaware. He has conducted computer forensic examinations

for numerous local, state, and federal agencies on a variety of cases, including extortion, homicide, embezzlement, child exploitation, intellectual property theft, and unlawful intrusions into computer systems. He has testified in court on numerous occasions as a computer forensics expert. He has taught computer forensics for Guidance Software, makers of EnCase, and taught as a lead instructor at all course levels. He has been a presenter at several seminars and workshops, is the author of numerous white papers, and is the primary author of the book *EnCase Computer Forensics: The Official EnCE: EnCase Certified Examiner Study Guide* , which was published by Sybex in early 2006. You can reach him at sbunting@udel.edu.

Users Review

From reader reviews:

Mora Miller:

Do you have favorite book? In case you have, what is your favorite's book? Publication is very important thing for us to learn everything in the world. Each e-book has different aim as well as goal; it means that reserve has different type. Some people feel enjoy to spend their a chance to read a book. They are really reading whatever they have because their hobby is usually reading a book. Consider the person who don't like examining a book? Sometime, individual feel need book when they found difficult problem or exercise. Well, probably you'll have this Mastering Windows Network Forensics and Investigation.

James Walton:

Inside other case, little men and women like to read book Mastering Windows Network Forensics and Investigation. You can choose the best book if you'd prefer reading a book. Provided that we know about how is important the book Mastering Windows Network Forensics and Investigation. You can add expertise and of course you can around the world by the book. Absolutely right, since from book you can recognize everything! From your country until finally foreign or abroad you can be known. About simple factor until wonderful thing you could know that. In this era, we can open a book or even searching by internet gadget. It is called e-book. You need to use it when you feel bored to go to the library. Let's examine.

Walter Dion:

Book is definitely written, printed, or illustrated for everything. You can realize everything you want by a reserve. Book has a different type. As it is known to us that book is important matter to bring us around the world. Next to that you can your reading expertise was fluently. A e-book Mastering Windows Network Forensics and Investigation will make you to possibly be smarter. You can feel more confidence if you can know about everything. But some of you think that will open or reading a book make you bored. It is far from make you fun. Why they could be thought like that? Have you searching for best book or suited book with you?

Manuel Frazier:

Do you like reading a book? Confuse to looking for your preferred book? Or your book ended up being rare? Why so many query for the book? But any kind of people feel that they enjoy for reading. Some people likes

looking at, not only science book but in addition novel and Mastering Windows Network Forensics and Investigation or even others sources were given information for you. After you know how the great a book, you feel need to read more and more. Science guide was created for teacher or even students especially. Those textbooks are helping them to bring their knowledge. In some other case, beside science guide, any other book likes Mastering Windows Network Forensics and Investigation to make your spare time more colorful. Many types of book like this one.

Download and Read Online Mastering Windows Network Forensics and Investigation By Steven Anson, Steve Bunting #14BUAKO7FI9

Read Mastering Windows Network Forensics and Investigation By Steven Anson, Steve Bunting for online ebook

Mastering Windows Network Forensics and Investigation By Steven Anson, Steve Bunting 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 Mastering Windows Network Forensics and Investigation By Steven Anson, Steve Bunting books to read online.

Online Mastering Windows Network Forensics and Investigation By Steven Anson, Steve Bunting ebook PDF download

Mastering Windows Network Forensics and Investigation By Steven Anson, Steve Bunting Doc

Mastering Windows Network Forensics and Investigation By Steven Anson, Steve Bunting Mobipocket

Mastering Windows Network Forensics and Investigation By Steven Anson, Steve Bunting EPub