

(Download pdf ebook) Cyber Crime Investigator's Field Guide

Cyber Crime Investigator's Field Guide

Bruce Middleton

*audiobook / *ebooks / Download PDF / ePub / DOC*



Cyber Crime Investigator's Field Guide



BRUCE MIDDLETON

 [Download](#)

 [Read Online](#)

#3918076 in eBooks 2001-11-28 2001-11-28 File Name: B00W4YSEKI | File size: 38.Mb

Bruce Middleton : Cyber Crime Investigator's Field Guide before purchasing it in order to gage whether or not it would be worth my time, and all praised Cyber Crime Investigator's Field Guide:

0 of 0 people found the following review helpful. Good info. Very informativeBy JaegerGood info. Very informative.4 of 4 people found the following review helpful. A few good chaptersBy Ben RothkeI was disappointed with the Cyber Crime Investigator's Field Guide. Half of the book (Appendix G) is simply a printout of the US Department of Justice Search and Seizure Guidelines. Although the guidelines are required reading, one should not have to pay for information that is available for free on the Department of Justice Web site. Chapter 6 of the book is a series of questions and answers on various subjects. The questions and answers are valuable, but the overly brief

answers do not provide readers with the rationale behind the answers. The book is not without merit, though; Chapter 9, "Case Study," describes the general course of action a forensic examiner should take when involved in a computer investigation. The author details what he does in the course of a general forensic investigation -- from the time he gets the call, to his ride from the airport to the client site, to the on-site pre-briefing, and beyond. 15 of 16 people found the following review helpful. Cyber Crime Investigator's Field Guide By Robert Mozia I found this book to be fantastic. Whether you are an experienced investigator of computer network security incidents (as I am for government/military/commercial organizations) or a neophyte just getting into the field of computer forensics, this book takes you through everything you need to know. The chapter on how the author handles an investigation in detail from start to finish is great. I'm applying what I learned there already. The coverage of forensic tools such as EnCase and tools from NTI is great. He gives me step by step information on how to use these tools, which I really need because you can't remember everything to do with all the tools I am involved with. The various reference sections on web sites, tool sites, attack signatures, etc. has been extremely useful for me and various organizations I work with. It's great to have the DOJ Search Seizure Guidelines in the book. Sure, I can go out to the DOJ website and after some searching find them, but it is difficult to work through all the various links, I can't take notes there, make underlines, etc. It's really nice to have these and other guidelines in a handy written reference. This is one book that goes with me and my team members whenever we leave for a client site. It has just about everything we need for reference purposes. The author calls it a field guide and that is just what it is. I highly recommend this book. Very practical. I just hope the author is going to write another book...no doubt we will pick it up.

Long gone are the days when a computer took up an entire room. Now we have computers at home, laptops that travel just about anywhere, and data networks that allow us to transmit information from virtually any location in a timely and efficient manner. What have these advancements brought us? Another arena for criminal activity. If someone wants to focus and target something, more than likely they will obtain what they want. We shouldn't expect it to be any different in cyberspace. Cyber Crime Field Handbook provides the details of investigating computer crime from soup to nuts. It covers everything from what to do upon arrival at the scene until the investigation is complete, including chain of evidence. You get easy access to information such as: Questions to ask the client Steps to follow when you arrive at the client's site Procedures for collecting evidence Details on how to use various evidence collection and analysis tools How to recover lost passwords or documents that are password protected Commonly asked questions with appropriate answers Recommended reference materials A case study to see the computer forensic tools in action Commonly used UNIX/Linux commands Port number references for various services and applications Computer forensic software tools commands synopsis Attack signatures Cisco PIX firewall commands We now have software and hardware to protect our data communication systems. We have laws that provide law enforcement more teeth to take a bite out of cyber crime. Now we need to combine understanding investigative techniques and technical knowledge of cyberspace. That's what this book does. Cyber Crime Field Handbook provides the investigative framework, a knowledge of how cyberspace really works, and the tools to investigate cyber crime; tools that tell you the who, where, what, when, why, and how.