Learning Network Forensics

Samir Datt

Learning Network Forensics

Samir Datt

Learning Network Forensics Samir Datt

Key Features

- Lay your hands on physical and virtual evidence to understand the sort of crime committed by capturing and analyzing network traffic
- Connect the dots by understanding web proxies, firewalls, and routers to close in on your suspect
- A hands-on guide to help you solve your case with malware forensic methods and network behaviors

Book Description

We live in a highly networked world. Every digital device—phone, tablet, or computer is connected to each other, in one way or another. In this new age of connected networks, there is network crime. Network forensics is the brave new frontier of digital investigation and information security professionals to extend their abilities to catch miscreants on the network.

The book starts with an introduction to the world of network forensics and investigations. You will begin by getting an understanding of how to gather both physical and virtual evidence, intercepting and analyzing network data, wireless data packets, investigating intrusions, and so on. You will further explore the technology, tools, and investigating methods using malware forensics, network tunneling, and behaviors. By the end of the book, you will gain a complete understanding of how to successfully close a case.

What you will learn

- Understand Internetworking, sources of network-based evidence and other basic technical fundamentals, including the tools that will be used throughout the book
- Acquire evidence using traffic acquisition software and know how to manage and handle the evidence
- Perform packet analysis by capturing and collecting data, along with content analysis
- Locate wireless devices, as well as capturing and analyzing wireless traffic data packets
- Implement protocol analysis and content matching; acquire evidence from NIDS/NIPS
- Act upon the data and evidence gathered by being able to connect the dots and draw links between various events
- Apply logging and interfaces, along with analyzing web proxies and understanding encrypted web traffic
- Use IOCs (Indicators of Compromise) and build real-world forensic solutions, dealing with malware

About the Author

Samir Datt has been dabbling with digital investigations since 1988, which was around the time he solved his first case with the help of an old PC and Lotus 123. He is the Founder CEO of Foundation Futuristic Technologies (P) Ltd, better known as ForensicsGuru.com. He is widely credited with evangelizing computer forensics in the Indian subcontinent and has personally trained thousands of law enforcement officers in the area. He has the distinction of starting the computer forensics industry in South Asia and setting up India's first computer forensic lab in the private sector. He is consulted by law enforcement agencies and private sector on various technology-related investigative issues. He has extensive experience in training thousands of investigators as well as examining a large number of digital sources of evidence in both private and government investigations.

Table of Contents

1. Becoming Network 007s
2. Laying Hands on the Evidence
3. Capturing & Analyzing Data Packets
4. Going Wireless
5. Tracking an Intruder on the Network
6. Connecting the Dots – Event Logs
7. Proxies, Firewalls, and Routers
8. Smuggling Forbidden Protocols – Network Tunneling
9. Investigating Malware – Cyber Weapons of the Internet
10. Closing the Deal – Solving the Case

Download and Read Free Online Learning Network Forensics Samir Datt

From reader reviews:

Carissa Taylor:

In this 21st hundred years, people become competitive in every single way. By being competitive right now, people have do something to make these individuals survives, being in the middle of typically the crowded place and notice by surrounding. One thing that at times many people have underestimated it for a while is reading. Yeah, by reading a e-book your ability to survive improve then having chance to stand up than other is high. For you personally who want to start reading a new book, we give you this particular Learning Network Forensics book as beginning and daily reading book. Why, because this book is more than just a book.

Aaron Eldred:

Do you one among people who can't read pleasant if the sentence chained inside straightway, hold on guys this aren't like that. This Learning Network Forensics book is readable simply by you who hate those perfect word style. You will find the facts here are arrange for enjoyable reading through experience without leaving even decrease the knowledge that want to give to you. The writer of Learning Network Forensics content conveys the thought easily to understand by many people. The printed and e-book are not different in the content material but it just different in the form of it. So , do you still thinking Learning Network Forensics is not loveable to be your top checklist reading book?

Willie Quinones:

Spent a free time to be fun activity to perform! A lot of people spent their free time with their family, or their particular friends. Usually they undertaking activity like watching television, likely to beach, or picnic inside park. They actually doing same every week. Do you feel it? Would you like to something different to fill your current free time/ holiday? Can be reading a book may be option to fill your cost-free time/ holiday. The first thing that you will ask may be what kinds of publication that you should read. If you want to try out look for book, may be the publication untitled Learning Network Forensics can be fine book to read. May be it can be best activity to you.

Johnny Grady:

Many people spending their time period by playing outside with friends, fun activity using family or just watching TV the entire day. You can have new activity to invest your whole day by examining a book. Ugh, think reading a book can actually hard because you have to use the book everywhere? It alright you can have the e-book, having everywhere you want in your Cell phone. Like Learning Network Forensics which is having the e-book version. So , try out this book? Let's observe.

Download and Read Online Learning Network Forensics Samir Datt #N8XRPV9DKAB

Read Learning Network Forensics by Samir Datt for online ebook

Learning Network Forensics by Samir Datt 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 Learning Network Forensics by Samir Datt books to read online.

Online Learning Network Forensics by Samir Datt ebook PDF download

Learning Network Forensics by Samir Datt Doc

Learning Network Forensics by Samir Datt Mobipocket

Learning Network Forensics by Samir Datt EPub