Google Drive

Forensic Discovery

Dan Farmer, Wietse Venema

Download now

Click here if your download doesn"t start automatically

Forensic Discovery

Dan Farmer, Wietse Venema

Forensic Discovery Dan Farmer, Wietse Venema

"Don't look now, but your fingerprints are all over the cover of this book. Simply picking it up off the shelf to read the cover has left a trail of evidence that you were here.

"If you think book covers are bad, computers are worse. Every time you use a computer, you leave elephant-sized tracks all over it. As Dan and Wietse show, even people trying to be sneaky leave evidence all over, sometimes in surprising places.

"This book is about computer archeology. It's about finding out what might have been based on what is left behind. So pick up a tool and dig in. There's plenty to learn from these masters of computer security."
--Gary McGraw, Ph.D., CTO, Cigital, coauthor of *Exploiting Software* and *Building Secure Software*

"A wonderful book. Beyond its obvious uses, it also teaches a great deal about operating system internals."
--Steve Bellovin, coauthor of *Firewalls and Internet Security, Second Edition,* and Columbia University professor

"A must-have reference book for anyone doing computer forensics. Dan and Wietse have done an excellent job of taking the guesswork out of a difficult topic."
--Brad Powell, chief security architect, Sun Microsystems, Inc.

"Farmer and Venema provide the essential guide to 'fossil' data. Not only do they clearly describe what you can find during a forensic investigation, they also provide research found nowhere else about how long data remains on disk and in memory. If you ever expect to look at an exploited system, I highly recommend reading this book."
--Rik Farrow, Consultant, author of *Internet Security for Home and Office*

"Farmer and Venema do for digital archaeology what Indiana Jones did for historical archaeology. *Forensic Discovery* unearths hidden treasures in enlightening and entertaining ways, showing how a time-centric approach to computer forensics reveals even the cleverest intruder."
--Richard Bejtlich, technical director, ManTech CFIA, and author of *The Tao of Network Security Monitoring*

"Farmer and Venema are 'hackers' of the old school: They delight in understanding computers at every level and finding new ways to apply existing information and tools to the solution of complex problems."
--Muffy Barkocy, Senior Web Developer, Shopping.com

"This book presents digital forensics from a unique perspective because it examines the systems that create digital evidence in addition to the techniques used to find it. I would recommend this book to anyone interested in learning more about digital evidence from UNIX systems."
--Brian Carrier, digital forensics researcher, and author of *File System Forensic Analysis*

The Definitive Guide to Computer Forensics: Theory and Hands-On Practice

Computer forensics--the art and science of gathering and analyzing digital evidence, reconstructing data and

attacks, and tracking perpetrators--is becoming ever more important as IT and law enforcement professionals face an epidemic in computer crime. In Forensic Discovery, two internationally recognized experts present a thorough and realistic guide to the subject.

Dan Farmer and Wietse Venema cover both theory and hands-on practice, introducing a powerful approach that can often recover evidence considered lost forever.

The authors draw on their extensive firsthand experience to cover everything from file systems, to memory and kernel hacks, to malware. They expose a wide variety of computer forensics myths that often stand in the way of success. Readers will find extensive examples from Solaris, FreeBSD, Linux, and Microsoft Windows, as well as practical guidance for writing one's own forensic tools. The authors are singularly well-qualified to write this book: They personally created some of the most popular security tools ever written, from the legendary SATAN network scanner to the powerful Coroner's Toolkit for analyzing UNIX break-ins.

After reading this book you will be able to

- Understand essential forensics concepts: volatility, layering, and trust
- Gather the maximum amount of reliable evidence from a running system
- Recover partially destroyed information--and make sense of it
- Timeline your system: understand what really happened when
- Uncover secret changes to everything from system utilities to kernel modules
- Avoid cover-ups and evidence traps set by intruders
- Identify the digital footprints associated with suspicious activity
- Understand file systems from a forensic analyst's point of view
- Analyze malware--without giving it a chance to escape
- Capture and examine the contents of main memory on running systems
- Walk through the unraveling of an intrusion, one step at a time

The book's companion Web site contains complete source and binary code for open source software discussed in the book, plus additional computer forensics case studies and resource links.

Download Forensic Discovery ...pdf

Read Online Forensic Discovery ...pdf

Download and Read Free Online Forensic Discovery Dan Farmer, Wietse Venema

---

From reader reviews:

Edward Vogler:

Reading a reserve can be one of a lot of activity that everyone in the world loves. Do you like reading book so. There are a lot of reasons why people enjoy it. First reading a guide will give you a lot of new data. When you read a publication you will get new information because book is one of several ways to share the information or their idea. Second, reading a book will make you actually more imaginative. When you studying a book especially fictional works book the author will bring someone to imagine the story how the characters do it anything. Third, you could share your knowledge to other people. When you read this Forensic Discovery, it is possible to tells your family, friends along with soon about yours e-book. Your knowledge can inspire different ones, make them reading a e-book.

William Hughes:

In this era which is the greater man or woman or who has ability in doing something more are more special than other. Do you want to become certainly one of it? It is just simple method to have that. What you are related is just spending your time very little but quite enough to experience a look at some books. Among the books in the top checklist in your reading list is definitely Forensic Discovery. This book and that is qualified as The Hungry Mountains can get you closer in becoming precious person. By looking up and review this reserve you can get many advantages.

Zandra Woods:

As a student exactly feel bored to reading. If their teacher inquired them to go to the library or to make summary for some book, they are complained. Just minor students that has reading's heart or real their interest. They just do what the instructor want, like asked to the library. They go to at this time there but nothing reading critically. Any students feel that examining is not important, boring and also can't see colorful pics on there. Yeah, it is for being complicated. Book is very important for you. As we know that on this period of time, many ways to get whatever you want. Likewise word says, many ways to reach Chinese's country. Therefore , this Forensic Discovery can make you sense more interested to read.

John Moreno:

What is your hobby? Have you heard this question when you got college students? We believe that that question was given by teacher to the students. Many kinds of hobby, All people has different hobby. And you also know that little person similar to reading or as looking at become their hobby. You need to know that reading is very important along with book as to be the thing. Book is important thing to incorporate you knowledge, except your own teacher or lecturer. You find good news or update with regards to something by book. A substantial number of sorts of books that can you go onto be your object. One of them are these claims Forensic Discovery.

Download and Read Online Forensic Discovery Dan Farmer, Wietse Venema #Q3IF0ULXBWN

Read Forensic Discovery by Dan Farmer, Wietse Venema for online ebook

Forensic Discovery by Dan Farmer, Wietse Venema 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 Forensic Discovery by Dan Farmer, Wietse Venema books to read online.

Online Forensic Discovery by Dan Farmer, Wietse Venema ebook PDF download

Forensic Discovery by Dan Farmer, Wietse Venema Doc

Forensic Discovery by Dan Farmer, Wietse Venema Mobipocket

Forensic Discovery by Dan Farmer, Wietse Venema EPub