Forensic Discovery

Dan Farmer, Wietse Venema

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 and Read Free Online Forensic Discovery Dan Farmer, Wietse Venema

---

From reader reviews:

Kelly Brooks:

Book is written, printed, or highlighted for everything. You can know everything you want by a publication. Book has a different type. As you may know that book is important thing to bring us around the world. Beside that you can your reading proficiency was fluently. A book Forensic Discovery will make you to be smarter. You can feel considerably more confidence if you can know about everything. But some of you think that will open or reading the book make you bored. It is not make you fun. Why they could be thought like that? Have you searching for best book or ideal book with you?

Pamela Eckert:

Reading can called thoughts hangout, why? Because if you are reading a book mainly book entitled Forensic Discovery the mind will drift away trough every dimension, wandering in every single aspect that maybe unknown for but surely can become your mind friends. Imaging each word written in a book then become one type conclusion and explanation that will maybe you never get previous to. The Forensic Discovery giving you one more experience more than blown away your thoughts but also giving you useful details for your better life within this era. So now let us teach you the relaxing pattern at this point is your body and mind will likely be pleased when you are finished reading through it, like winning a. Do you want to try this extraordinary spending spare time activity?

Danny Solberg:

Does one one of the book lovers? If yes, do you ever feeling doubt if you are in the book store? Try and pick one book that you never know the inside because don't ascertain book by its include may doesn't work here is difficult job because you are frightened that the inside maybe not because fantastic as in the outside seem likes. Maybe you answer can be Forensic Discovery why because the amazing cover that make you consider with regards to the content will not disappoint you actually. The inside or content is usually fantastic as the outside or even cover. Your reading 6th sense will directly guide you to pick up this book.

Randi Adams:

Is it you who having spare time subsequently spend it whole day by simply watching television programs or just telling lies on the bed? Do you need something totally new? This Forensic Discovery can be the reply, oh how comes? A fresh book you know. You are consequently out of date, spending your time by reading in this fresh era is common not a nerd activity. So what these books have than the others?

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