Forensic Discovery

Dan Farmer, Wietse Venema

Download now

Read Online

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

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

---

From reader reviews:

James Sanchez:

Nowadays reading books are more than want or need but also work as a life style. This reading routine give you lot of advantages. The huge benefits you got of course the knowledge your information inside the book that will improve your knowledge and information. The knowledge you get based on what kind of book you read, if you want get more knowledge just go with knowledge books but if you want sense happy read one with theme for entertaining like comic or novel. The Forensic Discovery is kind of publication which is giving the reader capricious experience.

Caleb Hutto:

Your reading 6th sense will not betray a person, why because this Forensic Discovery book written by well-known writer who really knows well how to make book that could be understand by anyone who else read the book. Written with good manner for you, still dripping wet every ideas and writing skill only for eliminate your own personal hunger then you still hesitation Forensic Discovery as good book not only by the cover but also from the content. This is one publication that can break don't evaluate book by its protect, so do you still needing an additional sixth sense to pick this!? Oh come on your reading sixth sense already said so why you have to listening to another sixth sense.

Margarita Culbertson:

Many people spending their time by playing outside having friends, fun activity having family or just watching TV the whole day. You can have new activity to invest your whole day by reading through a book. Ugh, ya think reading a book will surely hard because you have to take the book everywhere? It alright you can have the e-book, getting everywhere you want in your Mobile phone. Like Forensic Discovery which is finding the e-book version. So , why not try out this book? Let's notice.

Jeffrey Call:

What is your hobby? Have you heard in which question when you got students? We believe that that question was given by teacher to their students. Many kinds of hobby, All people has different hobby. And also you know that little person similar to reading or as studying become their hobby. You must know that reading is very important in addition to book as to be the point. Book is important thing to include you knowledge, except your current teacher or lecturer. You get good news or update about something by book. Numerous books that can you decide to try be your object. One of them is Forensic Discovery.

Download and Read Online Forensic Discovery Dan Farmer, Wietse Venema #DWN62OXG07B

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