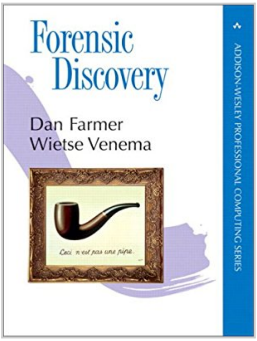

Forensic Discovery

By Dan Farmer, Wietse Venema

Forensic Discovery By 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.

Forensic Discovery

By Dan Farmer, Wietse Venema

Forensic Discovery By 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.

Forensic Discovery By Dan Farmer, Wietse Venema Bibliography

- Rank: #792196 in Books
- Published on: 2005-01-09
- Original language: English
- Number of items: 1
- Dimensions: 9.58" h x .78" w x 7.20" l, 1.43 pounds
- Binding: Hardcover
- 240 pages

Editorial Review

From the Back Cover

"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.

About the Author

Dan Farmer is author of a variety of security programs and papers. He is currently chief technical officer of Elemental Security, a computer security software company. Together he and Wietse Venema, have written many of the world's leading information security and forensics packages, including the SATAN network security scanner and the Coroner's Toolkit.
Wietse Venema has written some of the world's most widely used software, including TCP Wrapper and the Postfix mail system. He is currently a research staff member at IBM Research. Together, he and Dan Farmer have written many of the world's leading information security and forensics packages, including the SATAN network security scanner and the Coroner's Toolkit.

Today, only minutes pass between plugging in to the Internet and being attacked by some other machine--and that's only the background noise level of nontargeted attacks. There was a time when a computer could tick away year after year without coming under attack. For examples of Internet background radiation studies, see CAIDA 2003, Cymru 2004, or IMS 2004.

With this book, we summarize experiences in post-mortem intrusion analysis that we accumulated over a decade. During this period, the Internet grew explosively, from less than a hundred thousand connected hosts to more than a hundred million (ISC 2004). This increase in the number of connected hosts led to an even more dramatic--if less surprising--increase in the frequency of computer and network intrusions. As the network changed character and scope, so did the character and scope of the intrusions that we faced. We're pleased to share some of these learning opportunities with our readers.

In that same decade, however, little changed in the way that computer systems handle information. In fact, we feel that it is safe to claim that computer systems haven't changed fundamentally in the last 35 years--the entire lifetime of the Internet and of many operating systems that are in use today, including Linux, Windows, and many others. Although our observations are derived from today's systems, we optimistically expect that at least some of our insights will remain valid for another decade.

What You Can Expect to Learn from This Book

The premise of the book is that forensic information can be found everywhere you look. With this guiding principle in mind, we develop tools to collect information from obvious and not-so-obvious sources, we walk through analyses of real intrusions in detail, and we discuss the limitations of our approach.

Although we illustrate our approach with particular forensic tools in specific system environments, we do not provide cookbooks for how to use those tools, nor do we offer checklists for step-by-step investigation. Instead, we present a background on how information persists, how information about past events may be recovered, and how the trustworthiness of that information may be affected by deliberate or accidental processes.

In our case studies and examples, we deviate from traditional computer forensics and head toward the study of system dynamics. Volatility and the persistence of file systems and memory are pervasive topics in our book. And while the majority of our examples are from Solaris, FreeBSD, and Linux systems, Microsoft's Windows shows up on occasion as well. Our emphasis is on the underlying principles that these systems have in common: we look for inherent properties of computer systems, rather than accidental differences or superficial features.

Our global themes are problem solving, analysis, and discovery, with a focus on reconstruction of past events. This approach may help you to discover why events transpired, but that is generally outside the scope of this work. Knowing what happened will leave you better prepared the next time something bad is about to occur, even when that knowledge is not sufficient to prevent future problems. We should note up front, however, that we do not cover the detection or prevention of intrusions. We do show that traces from one intrusion can lead to the discovery of other intrusions, and we point out how forensic information may be affected by system-protection mechanisms, and by the failures of those mechanisms.

Our Intended Audience

We wrote this book for readers who want to deepen their understanding of how computer systems work, as well as for those who are likely to become involved with the technical aspects of computer intrusion or system analysis. System administrators, incident responders, other computer security professionals, and forensic analysts will benefit from reading this book, but so will anyone who is concerned about the impact of computer forensics on privacy.

Although we have worked hard to make the material accessible to nonexpert readers, we definitely do not target the novice computer user. As a minimal requirement, we assume strong familiarity with the basic concepts of UNIX or Windows file systems, networking, and processes.

Organization of This Book

The book has three parts: we present foundations first, proceed with analysis of processes, systems, and files, and end the book with discovery. We do not expect you to read everything in the order presented. Nevertheless, we suggest that you start with the first chapter, as it introduces all the major themes that return throughout the book.

In Part I, "Basic Concepts," we introduce general high-level ideas, as well as basic techniques that we rely on in later chapters.

- Chapter 1, "The Spirit of Forensic Discovery," shows how general properties of computer architecture can impact post-mortem analysis. Many of the limitations and surprises that we encounter later in the book can already be anticipated by reading this chapter.
- Chapter 2, "Time Machines," introduces the concept of timelining, using examples of host-based and network-based information, including information from the domain name system. We look at an intrusion that stretches out over an entire year, and we show examples of finding time information in non-obvious places.

In Part II, "Exploring System Abstractions," we delve into the abstractions of file systems, processes, and operating systems. The focus of these chapters is on analysis: making sense of information found on a computer system and judging the trustworthiness of our findings.

- Chapter 3, "File System Basics," introduces fundamental file system concepts, as well as forensic tools and techniques that we will use in subsequent chapters.
- Chapter 4, "File System Analysis," unravels an intrusion by examining the file system of a compromised machine in detail. We look at both existing files and deleted information. As in Chapter 2, we use correlation to connect different observations, and to determine their consistency.
- Chapter 5, "Systems and Subversion," is about the environment in which user processes and operating systems execute. We look at subversion of observations, ranging from straightforward changes to system utilities to almost undetectable malicious kernel modules, and detection of such subversion.
- Chapter 6, "Malware Analysis Basics," presents techniques to discover the purpose of a process or a program file that was left behind after an intrusion. We also discuss safeguards to prevent malware from escaping, and their limitations.

In Part III, "Beyond the Abstractions," we look beyond the constraints of the file, process, and operating system abstractions. The focus of this part is on discovery, as we study the effects of system architecture on the decay of information.

- Chapter 7, "The Persistence of Deleted File Information," shows that large amounts of deleted file information can survive intact for extended periods. We find half-lives on the order of two to four weeks on actively used file systems.
- Chapter 8, "Beyond Processes," shows examples of persistence of information in main memory, including the decrypted contents of encrypted files. We find large variations in persistence, and we correlate these variations to operating system architecture properties.

The appendices present background material: Appendix A is an introduction to the Coroner's Toolkit and related software. Appendix B presents our current insights with respect to the order of volatility and its ramifications when capturing forensic information from a computer system.

Conventions Used in This Book

In the examples, we use `constant-width font` for program code, command names, and command input/output. User input is shown in **`bold constant-width font`. We use $ as the shell command prompt for unprivileged users, and we reserve # for super-user shells. Capitalized names, such as Argus, are used when we write about a system instead of individual commands.**

Whenever we write "UNIX," we implicitly refer to Solaris, FreeBSD, and Linux. In some examples we include the operating system name in the command prompt. For example, we use `solaris$` to indicate that an example is specific to Solaris systems.

As hinted at earlier, many examples in this book are taken from real-life intrusions. To protect privacy, we anonymize information about systems that are not our own. For example, we replace real network addresses with private network addresses such as 10.0.0.1 or 192.168.0.1, and we replace host names or user names. Where appropriate, we even replace the time and time zone.

Web Sites

The examples in this book feature several small programs that were written for the purpose of discovery and analysis. Often we were unable to include the entire code listing because the additional detail would only detract from the purpose of the book. The complete source code for these and other programs is made available online at these Web sites:

http://www.fish.com/forensics/
http://www.porcupine.org/forensics/

On the same Web sites, you will also find bonus material, such as case studies that were not included in the book and pointers to other resources.

Users Review

From reader reviews:

Carissa Ware:

In this 21st one hundred year, people become competitive in each and every way. By being competitive right now, people have do something to make them survives, being in the middle of the actual crowded place and notice by surrounding. One thing that oftentimes many people have underestimated the item for a while is reading. Yeah, by reading a e-book your ability to survive increase then having chance to stand than other is high. For yourself who want to start reading a new book, we give you this specific Forensic Discovery book as beginning and daily reading publication. Why, because this book is more than just a book.

Victor Elam:

Nowadays reading books be than want or need but also get a life style. This reading routine give you lot of advantages. The benefits you got of course the knowledge the actual information inside the book that will improve your knowledge and information. The data you get based on what kind of book you read, if you want drive more knowledge just go with schooling books but if you want really feel happy read one together with theme for entertaining such as comic or novel. Often the Forensic Discovery is kind of publication which is giving the reader unforeseen experience.

Yolanda Ocasio:

People live in this new day time of lifestyle always aim to and must have the free time or they will get lot of stress from both lifestyle and work. So , once we ask do people have time, we will say absolutely indeed. People is human not only a robot. Then we consult again, what kind of activity are you experiencing when the spare time coming to you actually of course your answer will unlimited right. Then ever try this one, reading textbooks. It can be your alternative in spending your spare time, the particular book you have read is usually Forensic Discovery.

Miles Towles:

Playing with family within a park, coming to see the ocean world or hanging out with close friends is thing that usually you have done when you have spare time, after that why you don't try issue that really opposite from that. Just one activity that make you not experience tired but still relaxing, trilling like on roller coaster you are ride on and with addition of information. Even you love Forensic Discovery, you are able to enjoy both. It is good combination right, you still need to miss it? What kind of hang-out type is it? Oh occur its mind hangout fellas. What? Still don't get it, oh come on its named reading friends.

Download and Read Online Forensic Discovery By Dan Farmer, Wietse Venema #GKNFUX2RJOZ

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

GKNFUX2RJOZ: Forensic Discovery By Dan Farmer, Wietse Venema