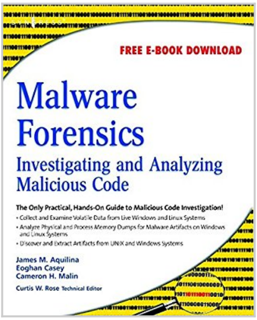
FREE E-BOOK DOWNLOAD
Malware Forensics
Investigating and Analyzing Malicious Code
The Only Practical, Hands-On Guide to Malicious Code Investigation!
• Collect and Examine Volatile Data from Live Windows and Linux Systems
• Analyze Physical and Process Memory Dumps for Malware Artifacts on Windows and Linux Systems
• Discover and Extract Artifacts from UNIX and Windows Systems
James M. Aquilina
Eoghan Casey
Cameron H. Malin
Curtis W. Rose Technical Editor

Malware Forensics: Investigating and Analyzing Malicious Code

By Cameron H. Malin, Eoghan Casey, James M. Aquilina

Malware Forensics: Investigating and Analyzing Malicious Code By Cameron H. Malin, Eoghan Casey, James M. Aquilina

Malware Forensics: Investigating and Analyzing Malicious Code covers the complete process of responding to a malicious code incident. Written by authors who have investigated and prosecuted federal malware cases, this book deals with the emerging and evolving field of live forensics, where investigators examine a computer system to collect and preserve critical live data that may be lost if the system is shut down. Unlike other forensic texts that discuss live forensics on a particular operating system, or in a generic context, this book emphasizes a live forensics and evidence collection methodology on both Windows and Linux operating systems in the context of identifying and capturing malicious code and evidence of its effect on the compromised system. It is the first book detailing how to perform live forensic techniques on malicious code.

The book gives deep coverage on the tools and techniques of conducting runtime behavioral malware analysis (such as file, registry, network and port monitoring) and static code analysis (such as file identification and profiling, strings discovery, armoring/packing detection, disassembling, debugging), and more. It explores over 150 different tools for malware incident response and analysis, including forensic tools for preserving and analyzing computer memory. Readers from all educational and technical backgrounds will benefit from the clear and concise explanations of the applicable legal case law and statutes covered in every chapter. In addition to the technical topics discussed, this book also offers critical legal considerations addressing the legal ramifications and requirements governing the subject matter.

This book is intended for system administrators, information security professionals, network personnel, forensic examiners, attorneys, and law enforcement working with the inner-workings of computer memory and malicious code.

* **Winner of Best Book Bejtlich read in 2008!**

* http://taosecurity.blogspot.com/2008/12/best-book-bejtlich-read-in-2008.html
* Authors have investigated and prosecuted federal malware cases, which allows them to provide unparalleled insight to the reader.
* First book to detail how to perform "live forensic" techniques on malicous code.
* In addition to the technical topics discussed, this book also offers critical legal considerations addressing the legal ramifications and requirements governing the subject matter

Download Malware Forensics: Investigating and Analyzing Mal ...pdf

Read Online Malware Forensics: Investigating and Analyzing M ...pdf

Malware Forensics: Investigating and Analyzing Malicious Code

By Cameron H. Malin, Eoghan Casey, James M. Aquilina

Malware Forensics: Investigating and Analyzing Malicious Code By Cameron H. Malin, Eoghan Casey, James M. Aquilina

Malware Forensics: Investigating and Analyzing Malicious Code covers the complete process of responding to a malicious code incident. Written by authors who have investigated and prosecuted federal malware cases, this book deals with the emerging and evolving field of live forensics, where investigators examine a computer system to collect and preserve critical live data that may be lost if the system is shut down. Unlike other forensic texts that discuss live forensics on a particular operating system, or in a generic context, this book emphasizes a live forensics and evidence collection methodology on both Windows and Linux operating systems in the context of identifying and capturing malicious code and evidence of its effect on the compromised system. It is the first book detailing how to perform live forensic techniques on malicious code.

The book gives deep coverage on the tools and techniques of conducting runtime behavioral malware analysis (such as file, registry, network and port monitoring) and static code analysis (such as file identification and profiling, strings discovery, armoring/packing detection, disassembling, debugging), and more. It explores over 150 different tools for malware incident response and analysis, including forensic tools for preserving and analyzing computer memory. Readers from all educational and technical backgrounds will benefit from the clear and concise explanations of the applicable legal case law and statutes covered in every chapter. In addition to the technical topics discussed, this book also offers critical legal considerations addressing the legal ramifications and requirements governing the subject matter.

This book is intended for system administrators, information security professionals, network personnel, forensic examiners, attorneys, and law enforcement working with the inner-workings of computer memory and malicious code.

* **Winner of Best Book Bejtlich read in 2008!**
* http://taosecurity.blogspot.com/2008/12/best-book-bejtlich-read-in-2008.html
* Authors have investigated and prosecuted federal malware cases, which allows them to provide unparalleled insight to the reader.
* First book to detail how to perform "live forensic" techniques on malicous code.
* In addition to the technical topics discussed, this book also offers critical legal considerations addressing the legal ramifications and requirements governing the subject matter

Malware Forensics: Investigating and Analyzing Malicious Code By Cameron H. Malin, Eoghan Casey, James M. Aquilina Bibliography

- Rank: #1629777 in eBooks
- Published on: 2008-08-08

- Released on: 2008-08-08
- Format: Kindle eBook

Download Malware Forensics: Investigating and Analyzing Mal ...pdf

Read Online Malware Forensics: Investigating and Analyzing M ...pdf

Editorial Review

About the Author

Cameron H. Malin is a Certified Ethical Hacker (C|EH) and Certified Network Defense Architect (C|NDA) as designated by the International Council of Electronic Commerce Consultants (EC-Council); a GIAC Certified Intrusion Analyst (GCIA), GIAC Certified Forensic Analysis (GCFA), a GIAC Certified Incident Handler (GCIH), GIAC Certified Reverse Engineering Malware professional (GREM), GIAC Penetration Tester (GPEN), and GIAC Certified Unix Security Administrator (GCUX) as designated by the SANS Institute; and a Certified Information Systems Security Professional (CISSP), as designated by the International Information Systems Security Certification Consortium ((ISC)2®).

From 1998 through 2002, Mr. Malin was an Assistant State Attorney (ASA) and Special Assistant United States Attorney in Miami, Florida, where he specialized in computer crime prosecutions. During his tenure as an ASA, he was also an Assistant Professorial Lecturer in the Computer Fraud Investigations Masters Program at George Washington University.

Mr. Malin is currently a Supervisory Special Agent with the Federal Bureau of Investigation assigned to the Behavioral Analysis Unit, Cyber Behavioral Analysis Center. He is also a Subject Matter Expert for the Department of Defense (DoD) Cyber Security & Information Systems Information Analysis Center and Defense Systems Information Analysis Center.

Mr. Malin is co-author of the Malware Forensics book series, Malware Forensics: Investigating and Analyzing Malicious Code, the Malware Forensics Field Guide for Windows Systems, and the Malware Forensics Field Guide for Linux Systems published by Syngress, an imprint of Elsevier, Inc.

The techniques, tools, methods, views, and opinions explained by Cameron Malin are personal to him, and do not represent those of the United States Department of Justice, the Federal Bureau of Investigation, or the government of the United States of America. Neither the Federal government nor any Federal agency endorses this book or its contents in any way.

Eoghan Casey is an internationally recognized expert in data breach investigations and information security forensics. He is founding partner of CASEITE.com, and co-manages the Risk Prevention and Response business unit at DFLabs. Over the past decade, he has consulted with many attorneys, agencies, and police departments in the United States, South America, and Europe on a wide range of digital investigations, including fraud, violent crimes, identity theft, and on-line criminal activity. Eoghan has helped organizations investigate and manage security breaches, including network intrusions with international scope. He has delivered expert testimony in civil and criminal cases, and has submitted expert reports and prepared trial exhibits for computer forensic and cyber-crime cases.

In addition to his casework and writing the foundational book Digital Evidence and Computer Crime, Eoghan has worked as R&D Team Lead in the Defense Cyber Crime Institute (DCCI) at the Department of Defense Cyber Crime Center (DC3) helping enhance their operational capabilities and develop new techniques and tools. He also teaches graduate students at Johns Hopkins University Information Security

Institute and created the Mobile Device Forensics course taught worldwide through the SANS Institute. He has delivered keynotes and taught workshops around the globe on various topics related to data breach investigation, digital forensics and cyber security.

Eoghan has performed thousands of forensic acquisitions and examinations, including Windows and UNIX systems, Enterprise servers, smart phones, cell phones, network logs, backup tapes, and database systems. He also has information security experience, as an Information Security Officer at Yale University and in subsequent consulting work. He has performed vulnerability assessments, deployed and maintained intrusion detection systems, firewalls and public key infrastructures, and developed policies, procedures, and educational programs for a variety of organizations. Eoghan has authored advanced technical books in his areas of expertise that are used by practitioners and universities around the world, and he is Editor-in-Chief of Elsevier's International Journal of Digital Investigation.

James M. Aquilina, Esq. is the Managing Director and Deputy General Counsel of Stroz Friedberg, LLC, a consulting and technical services firm specializing in computer forensics; cyber-crime response; private investigations; and the preservation, analysis and production of electronic data from single hard drives to complex corporate networks. As the head of the Los Angeles Office, Mr. Aquilina supervises and conducts digital forensics and cyber-crime investigations and oversees large digital evidence projects. Mr. Aquilina also consults on the technical and strategic aspects of anti-piracy, antispyware, and digital rights management (DRM) initiatives for the media and entertainment industries, providing strategic thinking, software assurance, testing of beta products, investigative assistance, and advice on whether the technical components of the initiatives implicate the Computer Fraud and Abuse Act and anti-spyware and consumer fraud legislation. His deep knowledge of botnets, distributed denial of service attacks, and other automated cyber-intrusions enables him to provide companies with advice to bolster their infrastructure protection.

Users Review

From reader reviews:

Brian Andres:

Now a day folks who Living in the era where everything reachable by match the internet and the resources inside can be true or not involve people to be aware of each information they get. How a lot more to be smart in receiving any information nowadays? Of course the reply is reading a book. Reading a book can help persons out of this uncertainty Information especially this Malware Forensics: Investigating and Analyzing Malicious Code book as this book offers you rich info and knowledge. Of course the details in this book hundred percent guarantees there is no doubt in it as you know.

Deanna Ratliff:

Reading a book tends to be new life style in this era globalization. With examining you can get a lot of information that could give you benefit in your life. Having book everyone in this world could share their idea. Publications can also inspire a lot of people. Lots of author can inspire their own reader with their story or perhaps their experience. Not only the storyline that share in the guides. But also they write about the knowledge about something that you need example of this. How to get the good score toefl, or how to teach your kids, there are many kinds of book which exist now. The authors in this world always try to improve their proficiency in writing, they also doing some study before they write to the book. One of them is this

Malware Forensics: Investigating and Analyzing Malicious Code.

Tracie Berry:

Do you have something that you enjoy such as book? The e-book lovers usually prefer to opt for book like comic, small story and the biggest some may be novel. Now, why not trying Malware Forensics: Investigating and Analyzing Malicious Code that give your enjoyment preference will be satisfied simply by reading this book. Reading addiction all over the world can be said as the opportinity for people to know world far better then how they react toward the world. It can't be said constantly that reading behavior only for the geeky individual but for all of you who wants to possibly be success person. So , for all you who want to start reading through as your good habit, you can pick Malware Forensics: Investigating and Analyzing Malicious Code become your own personal starter.

Casey Reeves:

In this era globalization it is important to someone to acquire information. The information will make you to definitely understand the condition of the world. The healthiness of the world makes the information much easier to share. You can find a lot of recommendations to get information example: internet, classifieds, book, and soon. You will observe that now, a lot of publisher which print many kinds of book. Typically the book that recommended for you is Malware Forensics: Investigating and Analyzing Malicious Code this publication consist a lot of the information in the condition of this world now. This kind of book was represented how do the world has grown up. The language styles that writer use for explain it is easy to understand. The writer made some study when he makes this book. Honestly, that is why this book appropriate all of you.

Download and Read Online Malware Forensics: Investigating and Analyzing Malicious Code By Cameron H. Malin, Eoghan Casey, James M. Aquilina #SRFLX5O4EUN

Read Malware Forensics: Investigating and Analyzing Malicious Code By Cameron H. Malin, Eoghan Casey, James M. Aquilina for online ebook

Malware Forensics: Investigating and Analyzing Malicious Code By Cameron H. Malin, Eoghan Casey, James M. Aquilina 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 Malware Forensics: Investigating and Analyzing Malicious Code By Cameron H. Malin, Eoghan Casey, James M. Aquilina books to read online.

Online Malware Forensics: Investigating and Analyzing Malicious Code By Cameron H. Malin, Eoghan Casey, James M. Aquilina ebook PDF download

Malware Forensics: Investigating and Analyzing Malicious Code By Cameron H. Malin, Eoghan Casey, James M. Aquilina Doc

Malware Forensics: Investigating and Analyzing Malicious Code By Cameron H. Malin, Eoghan Casey, James M. Aquilina Mobipocket

Malware Forensics: Investigating and Analyzing Malicious Code By Cameron H. Malin, Eoghan Casey, James M. Aquilina EPub

SRFLX5O4EUN: Malware Forensics: Investigating and Analyzing Malicious Code By Cameron H. Malin, Eoghan Casey, James M. Aquilina