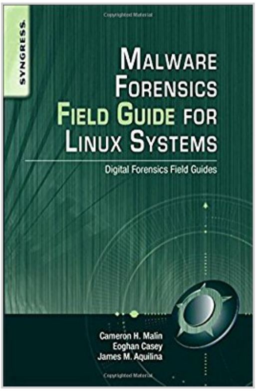


# Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides

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



**Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides** By Cameron H. Malin, Eoghan Casey, James M. Aquilina

*Malware Forensics Field Guide for Linux Systems* is a handy reference that shows students the essential tools needed to do computer forensics analysis at the crime scene. It is part of Syngress *Digital Forensics Field Guides*, a series of companions for any digital and computer forensic student, investigator or analyst. Each Guide is a toolkit, with checklists for specific tasks, case studies of difficult situations, and expert analyst tips that will aid in recovering data from digital media that will be used in criminal prosecution.

This book collects data from all methods of electronic data storage and transfer devices, including computers, laptops, PDAs and the images, spreadsheets and other types of files stored on these devices. It is specific for Linux-based systems, where new malware is developed every day. The authors are world-renowned leaders in investigating and analyzing malicious code. Chapters cover malware incident response - volatile data collection and examination on a live Linux system; analysis of physical and process memory dumps for malware artifacts; post-mortem forensics - discovering and extracting malware and associated artifacts from Linux systems; legal considerations; file identification and profiling initial analysis of a suspect file on a Linux system; and analysis of a suspect program.

This book will appeal to computer forensic investigators, analysts, and specialists.

- A compendium of on-the-job tasks and checklists
- Specific for Linux-based systems in which new malware is developed every day
- Authors are world-renowned leaders in investigating and analyzing malicious code

**Read Online** Malware Forensics Field Guide for Linux Systems: ...pdf

# Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides

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

**Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides** By Cameron H. Malin, Eoghan Casey, James M. Aquilina

*Malware Forensics Field Guide for Linux Systems* is a handy reference that shows students the essential tools needed to do computer forensics analysis at the crime scene. It is part of Syngress *Digital Forensics Field Guides*, a series of companions for any digital and computer forensic student, investigator or analyst. Each Guide is a toolkit, with checklists for specific tasks, case studies of difficult situations, and expert analyst tips that will aid in recovering data from digital media that will be used in criminal prosecution.

This book collects data from all methods of electronic data storage and transfer devices, including computers, laptops, PDAs and the images, spreadsheets and other types of files stored on these devices. It is specific for Linux-based systems, where new malware is developed every day. The authors are world-renowned leaders in investigating and analyzing malicious code. Chapters cover malware incident response - volatile data collection and examination on a live Linux system; analysis of physical and process memory dumps for malware artifacts; post-mortem forensics - discovering and extracting malware and associated artifacts from Linux systems; legal considerations; file identification and profiling initial analysis of a suspect file on a Linux system; and analysis of a suspect program.

This book will appeal to computer forensic investigators, analysts, and specialists.

- A compendium of on-the-job tasks and checklists
- Specific for Linux-based systems in which new malware is developed every day
- Authors are world-renowned leaders in investigating and analyzing malicious code

**Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides By Cameron H. Malin, Eoghan Casey, James M. Aquilina Bibliography**

- Sales Rank: #982652 in Books
- Brand: Syngress Publishing
- Published on: 2014-01-03
- Original language: English
- Number of items: 1
- Dimensions: 9.02" h x 1.24" w x 5.98" l, 1.60 pounds
- Binding: Paperback
- 616 pages

## Editorial Review

Review

"...a useful companion for law enforcement and the forensic community, as it will enhance their capability to deal with cases involving malware on Linux systems." -***Computing Reviews*, Oct 08, 2014**

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:**

**Zachary Kirkland:**

The guide untitled Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides is the reserve that recommended to you to study. You can see the quality of the publication content that will be shown to you. The language that author use to explained their way of doing something is easily to understand. The writer was did a lot of investigation when write the book, hence the information that they share for your requirements is absolutely accurate. You also will get the e-book of Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides from the publisher to make you a lot more enjoy free time.

**John Burns:**

This Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides is great reserve for you because the content which is full of information for you who have always deal with world and also have to make decision every minute. This specific book reveal it data accurately using great coordinate word or we can declare no rambling sentences in it. So if you are read this hurriedly you can have whole details in it. Doesn't mean it only offers you straight forward sentences but tough core information with beautiful delivering sentences. Having Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides in your hand like finding the world in your arm, info in it is not ridiculous just one. We can say that no reserve that offer you world throughout ten or fifteen minute right but this guide already do that. So , this is certainly good reading book. Hey there Mr. and Mrs. stressful do you still doubt that will?

**Lenora Dryer:**

As we know that book is very important thing to add our know-how for everything. By a guide we can know everything we wish. A book is a pair of written, printed, illustrated as well as blank sheet. Every year seemed to be exactly added. This publication Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides was filled with regards to science. Spend your time to add your knowledge about your research competence. Some people has diverse feel when they reading some sort of book. If you know how big benefit of a book, you can feel enjoy to read a reserve. In the modern era like currently, many ways to get book you wanted.

**Julie Slocum:**

A lot of reserve has printed but it takes a different approach. You can get it by internet on social media. You can choose the most beneficial book for you, science, witty, novel, or whatever by simply searching from it. It is named of book Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides. Contain your knowledge by it. Without leaving behind the printed book, it might add your knowledge and make you happier to read. It is most significant that, you must aware about book. It can bring you from one destination for a other place.

# Read Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides By Cameron H. Malin, Eoghan Casey, James M. Aquilina for online ebook

Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides 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 Field Guide for Linux Systems: Digital Forensics Field Guides By Cameron H. Malin, Eoghan Casey, James M. Aquilina books to read online.

## Online Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides By Cameron H. Malin, Eoghan Casey, James M. Aquilina ebook PDF download

### Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides By Cameron H. Malin, Eoghan Casey, James M. Aquilina Doc

#### Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides By Cameron H. Malin, Eoghan Casey, James M. Aquilina Mobipocket

#### Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides By Cameron H. Malin, Eoghan Casey, James M. Aquilina EPub

#### XEIYH2359B7: Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides By Cameron H. Malin, Eoghan Casey, James M. Aquilina