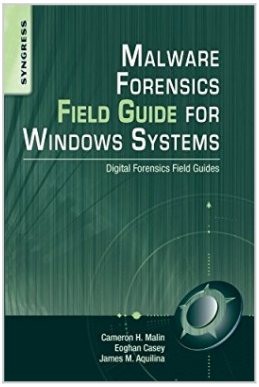


# Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides

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



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

*Malware Forensics Field Guide for Windows 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 Windows-based systems, the largest running OS in the world. 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 Windows system; analysis of physical and process memory dumps for malware artifacts; post-mortem forensics - discovering and extracting malware and associated artifacts from Windows systems; legal considerations; file identification and profiling initial analysis of a suspect file on a Windows system; and analysis of a suspect program.

This field guide is intended for computer forensic investigators, analysts, and specialists.

- A condensed hand-held guide complete with on-the-job tasks and checklists
- Specific for Windows-based systems, the largest running OS in the world
- Authors are world-renowned leaders in investigating and analyzing malicious code

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

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

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

*Malware Forensics Field Guide for Windows 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 Windows-based systems, the largest running OS in the world. 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 Windows system; analysis of physical and process memory dumps for malware artifacts; post-mortem forensics - discovering and extracting malware and associated artifacts from Windows systems; legal considerations; file identification and profiling initial analysis of a suspect file on a Windows system; and analysis of a suspect program.

This field guide is intended for computer forensic investigators, analysts, and specialists.

- A condensed hand-held guide complete with on-the-job tasks and checklists
- Specific for Windows-based systems, the largest running OS in the world
- Authors are world-renowned leaders in investigating and analyzing malicious code

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

- Sales Rank: #605656 in Books
- Published on: 2012-06-27
- Released on: 2012-06-13
- Original language: English
- Number of items: 1
- Dimensions: 9.00" h x 1.27" w x 6.00" l, 1.95 pounds
- Binding: Paperback
- 560 pages

## Editorial Review

Review

"For anyone working in this field, this is an invaluable book that deserves a permanent place in your toolkit. For those entering into this line of work, it’s worth reading so that you know what you’re in for." **--Network Security, December 2013**

From the Back Cover

*Malware Forensics Field Guide for Windows Systems* is a companion for computer forensic investigators, incident responders and malware analysts that distills the formalized methods introduced in the authors’ previous work and presents the new forensic concepts of digital impression and trace evidence, along with advanced profiling techniques based in malware taxonomy and phylogeny.

Presented in succinct outline format with cross-references to supplemental appendices, this tactical and practical resource is designed to provide the digital investigator clear and concise guidance in an easily accessible format while responding to an incident or conducting analysis in a lab.

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:**

**Donna Antonucci:**

Often the book Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides will bring you to definitely the new experience of reading any book. The author style to describe the idea is very unique. If you try to find new book you just read, this book very ideal to you. The book Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides is much recommended to you to read. You can also get the e-book from the official web site, so you can more easily to read the book.

**Effie Phillips:**

Spent a free a chance to be fun activity to do! A lot of people spent their free time with their family, or all their friends. Usually they doing activity like watching television, gonna beach, or picnic from the park. They actually doing same task every week. Do you feel it? Would you like to something different to fill your current free time/ holiday? May be reading a book can be option to fill your free time/ holiday. The first thing that you'll ask may be what kinds of publication that you should read. If you want to try out look for book, may be the publication untitled Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides can be excellent book to read. May be it might be best activity to you.

**Lorraine Wheat:**

A lot of e-book has printed but it is different. You can get it by world wide web on social media. You can choose the most effective book for you, science, witty, novel, or whatever through searching from it. It is referred to as of book Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides. You can contribute your knowledge by it. Without causing the printed book, it might add your knowledge and make you actually happier to read. It is most significant that, you must aware about reserve. It can bring you from one spot to other place.

**Cheryl Saldana:**

Guide is one of source of understanding. We can add our information from it. Not only for students but in addition native or citizen require book to know the revise information of year to be able to year. As we know those books have many advantages. Beside all of us add our knowledge, can also bring us to around the world. By book Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides we can acquire more advantage. Don't someone to be creative people? Being creative person must love to read a book. Only choose the best book that acceptable with your aim. Don't end up being doubt to change your life with that book Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides. You can more desirable than now.

**Malin, Eoghan Casey, James M. Aquilina #P82YNFE79UJ**

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

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

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

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

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

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