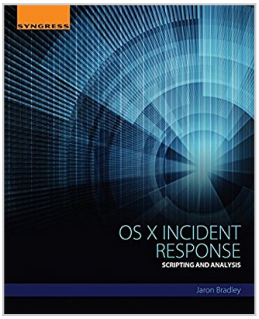


# OS X Incident Response: Scripting and Analysis

*By Jaron Bradley*



**OS X Incident Response: Scripting and Analysis** By Jaron Bradley

OS X Incident Response: Scripting and Analysis is written for analysts who are looking to expand their understanding of a lesser-known operating system. By mastering the forensic artifacts of OS X, analysts will set themselves apart by acquiring an up-and-coming skillset.

Digital forensics is a critical art and science. While forensics is commonly thought of as a function of a legal investigation, the same tactics and techniques used for those investigations are also important in a response to an incident. Digital evidence is not only critical in the course of investigating many crimes but businesses are recognizing the importance of having skilled forensic investigators on staff in the case of policy violations.

Perhaps more importantly, though, businesses are seeing enormous impact from malware outbreaks as well as data breaches. The skills of a forensic investigator are critical to determine the source of the attack as well as the impact. While there is a lot of focus on Windows because it is the predominant desktop operating system, there are currently very few resources available for forensic investigators on how to investigate attacks, gather evidence and respond to incidents involving OS X. The number of Macs on enterprise networks is rapidly increasing, especially with the growing prevalence of BYOD, including iPads and iPhones.

Author Jaron Bradley covers a wide variety of topics, including both the collection and analysis of the forensic pieces found on the OS. Instead of using expensive commercial tools that clone the hard drive, you will learn how to write your own Python and bash-based response scripts. These scripts and methodologies can be used to collect and analyze volatile data immediately.

For online source codes, please visit:

https://github.com/jbradley89/osx_incident_response_scripting_and_analysis

- Focuses exclusively on OS X attacks, incident response, and forensics
- Provides the technical details of OS X so you can find artifacts that might be

missed using automated tools
- Describes how to write your own Python and bash-based response scripts, which can be used to collect and analyze volatile data immediately
- Covers OS X incident response in complete technical detail, including file system, system startup and scheduling, password dumping, memory, volatile data, logs, browser history, and exfiltration

# OS X Incident Response: Scripting and Analysis

*By Jaron Bradley*

**OS X Incident Response: Scripting and Analysis** By Jaron Bradley

OS X Incident Response: Scripting and Analysis is written for analysts who are looking to expand their understanding of a lesser-known operating system. By mastering the forensic artifacts of OS X, analysts will set themselves apart by acquiring an up-and-coming skillset.

Digital forensics is a critical art and science. While forensics is commonly thought of as a function of a legal investigation, the same tactics and techniques used for those investigations are also important in a response to an incident. Digital evidence is not only critical in the course of investigating many crimes but businesses are recognizing the importance of having skilled forensic investigators on staff in the case of policy violations.

Perhaps more importantly, though, businesses are seeing enormous impact from malware outbreaks as well as data breaches. The skills of a forensic investigator are critical to determine the source of the attack as well as the impact. While there is a lot of focus on Windows because it is the predominant desktop operating system, there are currently very few resources available for forensic investigators on how to investigate attacks, gather evidence and respond to incidents involving OS X. The number of Macs on enterprise networks is rapidly increasing, especially with the growing prevalence of BYOD, including iPads and iPhones.

Author Jaron Bradley covers a wide variety of topics, including both the collection and analysis of the forensic pieces found on the OS. Instead of using expensive commercial tools that clone the hard drive, you will learn how to write your own Python and bash-based response scripts. These scripts and methodologies can be used to collect and analyze volatile data immediately.

For online source codes, please visit:

https://github.com/jbradley89/osx_incident_response_scripting_and_analysis

- Focuses exclusively on OS X attacks, incident response, and forensics
- Provides the technical details of OS X so you can find artifacts that might be missed using automated tools
- Describes how to write your own Python and bash-based response scripts, which can be used to collect and analyze volatile data immediately
- Covers OS X incident response in complete technical detail, including file system, system startup and scheduling, password dumping, memory, volatile data, logs, browser history, and exfiltration

**OS X Incident Response: Scripting and Analysis By Jaron Bradley Bibliography**

- Rank: #425294 in eBooks
- Published on: 2016-05-07
- Released on: 2016-05-07
- Format: Kindle eBook

## Editorial Review

About the Author
Jaron Bradley has a background in host-based incident response and forensics. He entered the information security field as an incident responder immediately after graduating from Eastern Michigan University, where he received his degree in Information Assurance. He now works as a Senior Intrusion Analyst, with a focus on OS X and Linux based attacks.

## Users Review

**From reader reviews:**

**Jackson Cabrera:**

Hey guys, do you really wants to finds a new book to learn? May be the book with the headline OS X Incident Response: Scripting and Analysis suitable to you? Often the book was written by popular writer in this era. The particular book untitled OS X Incident Response: Scripting and Analysisis a single of several books in which everyone read now. That book was inspired lots of people in the world. When you read this reserve you will enter the new dimensions that you ever know prior to. The author explained their plan in the simple way, therefore all of people can easily to understand the core of this publication. This book will give you a wide range of information about this world now. To help you to see the represented of the world in this particular book.

**Lena Drew:**

Are you kind of active person, only have 10 or even 15 minute in your day to upgrading your mind talent or thinking skill possibly analytical thinking? Then you are experiencing problem with the book than can satisfy your short time to read it because this time you only find reserve that need more time to be study. OS X Incident Response: Scripting and Analysis can be your answer mainly because it can be read by anyone who have those short free time problems.

**April Miller:**

Do you like reading a reserve? Confuse to looking for your favorite book? Or your book seemed to be rare? Why so many concern for the book? But just about any people feel that they enjoy to get reading. Some people likes examining, not only science book but additionally novel and OS X Incident Response: Scripting and Analysis or perhaps others sources were given expertise for you. After you know how the truly amazing a book, you feel desire to read more and more. Science reserve was created for teacher as well as students especially. Those publications are helping them to bring their knowledge. In other case, beside science guide, any other book likes OS X Incident Response: Scripting and Analysis to make your spare time considerably more colorful. Many types of book like this.

**Minerva Garrison:**

Reading a publication make you to get more knowledge from that. You can take knowledge and information from your book. Book is composed or printed or created from each source which filled update of news. In this particular modern era like currently, many ways to get information are available for a person. From media social like newspaper, magazines, science guide, encyclopedia, reference book, new and comic. You can add your knowledge by that book. Ready to spend your spare time to spread out your book? Or just searching for the OS X Incident Response: Scripting and Analysis when you necessary it?

# Read OS X Incident Response: Scripting and Analysis By Jaron Bradley for online ebook

OS X Incident Response: Scripting and Analysis By Jaron Bradley 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 OS X Incident Response: Scripting and Analysis By Jaron Bradley books to read online.

## Online OS X Incident Response: Scripting and Analysis By Jaron Bradley ebook PDF download

### OS X Incident Response: Scripting and Analysis By Jaron Bradley Doc

#### OS X Incident Response: Scripting and Analysis By Jaron Bradley Mobipocket

#### OS X Incident Response: Scripting and Analysis By Jaron Bradley EPub

#### YITR1N7G0PH: OS X Incident Response: Scripting and Analysis By Jaron Bradley