MAGNET FORENSICS TRAINING

Magnet AXIOM macOS Examinations (AX350)

AX350 is an expert-level four-day training course, designed for participants who are somewhat familiar with the principles of digital forensics and who are seeking to expand their knowledge base on macOS and the forensic analysis of devices using the APFS file system and Magnet AXIOM.

Examiners will investigate a scenario dealing with a misconfigured webserver that allowed hackers to exploit vulnerabilities and gain access to the network to perform nefarious activity and steal intellectual property and potentially customer data as well.

magnetforensics.com/training-overview

MAGNET AXIOM macOS EXAMINATIONS (AX350) MODULES

Each module of instruction employs instructor-led and student practical exercises to reinforce the learning objectives and provide the participants with the knowledge and skills necessary to successfully utilize Magnet AXIOM in their investigative workflow.

MODULE 1:

INTRODUCTION AND COURSE OVERVIEW

An introduction as to what to expect throughout the course for students as well as the scenario that will be followed over the four-day training.

MODULE 2:

macOS OVERVIEW

Learn about the macOS operating system and APFS file system, including changes to the security of macOS devices including the T2 chips, SIP, and other security protocols being used by Apple, and discuss proper handling techniques for macOS devices. Several key operating system artifacts for macOS will be covered including Finder, File System Events, Sidebar items, Trash Items, Installed Applications, and more.

MODULE 3:

STARTING OUR EXAMINATION

Discuss encryption issues such as FileVault2 and methods that can be taken to brute force this technology using Passware.

MODULE 4:

LOG FILES

Several macOS log files will be investigated, such as the unified logs, configuration files, file/folder permissions, daily logs, USB connection history, and other key logging artifacts to track user access of information.

MODULE 5:

KnowledgeC

The KnowledgeC database stores a wealth of information about the macOS usage as well as user activity. Learn how to glean information from the KnowledgeC.db, including Application Usage, Application Activities, Safari Browser History, and Device Power Status.

MODULE 6:

INTERNET ARTIFACTS

Several browser history artifacts from Safari, Chrome, and Firefox will be examined to assist in the investigation and collection of evidence in furtherance of the investigation being carried out by the students.

MODULE 7:

USER ACCOUNTS

Understanding the data specific to a user account can be key in an investigation. This module will cover artifacts dealing with contacts, address books, saved apple accounts, keychain information, installed applications, and logon/logoff times.

MODULE 8:

EMAIL

The default mail application (Mail.App) stores both email and calendar data inside macOS. This module will discuss how to recover artifacts and attachments from these stored files.

MODULE 9:

MAC DESKTOP

The macOS Desktop stores several valuable artifacts around what a user has been accessing including the Menu Bar applications, recently used items, and the quick-look thumbnails.

MODULE 10:

TIME MACHINE AND SNAPSHOTS

Time Machine is a built-in backup methodology for macOS. In this module, students will cover the Time Machine and Snapshot functionalities of macOS and the APFS file system. This information will be valuable in trying to recover files that may no longer be active on the macOS system.

MODULE 11:

CLOUD SERVICES

MacOS users typically have an Apple ID and with it, free iCloud storage. This cloud storage can prove important in an investigation as well as other cloud sources of data such as OneDrive and Google Drive. Understanding how macOS uses these services and what databases control the flow of data between the cloud service and the host computer is imperative to solving these types of investigations.

MODULE 12:

CUMULATIVE REVIEW

A final practical will walk students through practicing the techniques and analyzing the artifacts discussed throughout this course.

For more information on Magnet Forensics Training and Certification programs, visit magnetforensics.com/training-overview

Any completed instructor-led Magnet Forensics training course (in-person or virtual) can be counted for 32 CPE credits through NASBA.

MAGNET FORENSICS®