MAGNET FORENSICS TRAINING

Magnet AXIOM Advanced Computer Forensics (AX250)

Magnet AXIOM Advanced Computer Forensics (AX250) is an expert-level four-day training course, designed for participants who are familiar with the principles of digital forensics and who are seeking to leverage Magnet AXIOM, Magnet RAM Capture, and third-party tools to improve their computer investigations.

AX250 will give participants the knowledge and skills they need to track computer access and file usage, utilizing Magnet AXIOM to explore the evidence in greater depth by learning about the newest sign-on technologies — such as pin password, Windows Hello, picture password, fingerprint recognition, and facial recognition.

In this course, a deeper understanding of investigating Windows computers will be provided by searching through artifacts like Windows Notification, Windows System Resource Utilization, Windows Error Reporting (WER) Logs, Event Logs (EVT), Event Tracing Logs (ETL), as well as a breakdown of the taskbar and whether an artifact was system pinned or user pinned to it.

Also, there will be time spent investigating EMDMgmt to dig deep into tracking drives attached to the Windows OS that may leave traces nowhere else. AppCompatFlags and AMCACHE will also be investigated to determine executable files which were previously executed on the system, but no longer exist.

This course will also discuss how to track files and folders based on information in the user profile and information recovered from Shellbags. Maximizing the data from Prefetch files, Jumplists, and Recent Docs to correlate the data recovered from the artifacts previously mentioned above. This course also takes a look at collecting RAM images and parsing those images for actionable intelligence in support of the investigation. Participants of this course will be utilizing Passware and the AXIOM Wordlist Generator to crack iTunes backups and Windows passwords from information in the image of the suspect hard disk drive including the most up to date versions of that software. Finally, participants of this course will investigate Google Drive, Modern Apps (Windows Store Apps), UsnJrnl and an in-depth look at File history and the extensible Database files tracking it.

AXIOM ADVANCED COMPUTER (AX250) 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: Windows 10 Overview

Participants will gain an understanding of why Microsoft stated Windows 10 is the last Windows version they will ever release and the impact that is having and will continue to have on the forensic community. This module will also explore the new Windows sign-in technologies, reporting on the System Resource Utilization database, and tracking current Windows build numbers of systems being examined.

Module 2: EMDMgmt and Volume Serial numbers

This module will focus on utilizing not so well-known registry locations to track serial numbers of volumes being accessed by the Windows Operating System.

Module 3: Finding Missing Executables

Participants will learn how to utilize the Program Compatibility Assistant and AMCache Data to track the use of executables and their hashes on the computer in question.

Module 4: Investigating Shellbags Beyond the Surface

Shellbags will be explored in this module — what they are and how they can be used in an investigation to determine if a file or path was accessed by a specific user.

Module 5: Prefetch Files and Correlating the Data

In this module, participants will examine prefetch files in a much more in-depth view to determine the secrets they may hold, as well as how Windows stores and deletes them to ensure when they testify they are doing so with knowledge and confidence.

Module 6: Jumplists, what are They and what do They Tell Us

Understanding Jumplists is just the beginning. being able to utilize the data provided to correlate information about previously existing drives and the files located on them which are no longer part of the system, is what this lesson is all about.

Module 7: Recent Docs

Making use of the information found in recent docs and reporting on the information is important. What is more important is the ability to correlate that data with the data from the previous lessons to continuously track key pieces of information across the system and see how and possibly when and where that data was accessed is even more important.

Module 8: Collecting RAM and Parsing RAM Images

Collection of RAM in running computers is paramount. Examiners would not leave a 16 GB or 32 GB thumb drive laying at the collection scene and surely, they are not going to leave RAM uncollected. This lesson will discuss the collection of RAM and where and why it is important.

Module 9: Sharing Files and Folders and Settings Across Devices

Microsoft makes is easy to share between devices, using OneDrive for file sharing, and a Microsoft email account for other settings. Determine when the first time and last time data was shared with other devices via Sync technology. Settings of one Windows system can be shared with other Windows systems including Wi-Fi profiles and deleted profiles. In this module, students will use the acquired RAM from the previous module and Passware to gain access to the Truecrypt container and its contents.

Module 10: Using Passware to Break iTunes Backup Passwords

Students will receive a refresher on IOS backups and use the AXIOM Wordlist Generator (AWG) and Passware to gain entry to the IOS backup and obtain the password. The password will then be used to gain access to the keychain data to see passwords utilized by the suspect for WiFi devices joined as well as any iOS Keychain passwords.

Module 11: Cracking Windows 10 Passwords

In this module, participants will use AXIOM, the AXIOM Wordlist Generator and a combination of software to extract the Windows 10 password from the SAM hive using the algorithm stored in the System hive.

Module 12: Investigating Google Drive Back to the Local System

Google Drive uses a program aptly named Backup and Sync and it leaves behind quite a few forensic artifacts which participants will investigate to recover forensic artifacts about the uploading and downloading of files to a specific computer system.

Module 13: Windows File History and What It Could Mean

Not to be confused with Volume Shadow Service, File History is a Windows 10 program which regularly backs up versions of your files in the Documents, Music, Pictures, Videos, and Desktop folders and the OneDrive files available offline on your PC. At the conclusion of this module, participants will be able to determine File History.

Module 14: Investigating Modern Apps (Windows Store Apps) overview

Modern Apps were designed to be immersive. There is a focus on the touchscreen, but they also work on the standard desktop with no problems. By investigating Modern Apps, participants will gain an understanding that internet history and cache for Modern Apps are not stored in the usual locations where an examiner would expect.

Module 15: Maximizing Use of the USNJrnl in Your Investigations

The USN journal is a log of changes to files on an NTFS volume. Such changes can for instance be the creation, deletion or modification of files or directories. Participants will learn how to investigate the USNJrnl to retrieve forensic artifacts in support of their examination.

Module 16: Cumulative Review Exercise

To further reinforce the instructional goals of the course, students are presented with a final scenario-based practical exercise which represents a cumulative review of the exercises conducted in each of the individual modules.

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

MAGNET FORENSICS