AX250 AXIOM Advanced Forensics with Windows 11

This course 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 advanced forensics and improve their computer investigations.

Course Objectives

MODULE 1: INTRODUCTION AND COURSE OVERVIEW

- Learning objectives will be presented along with expected outcomes over the course's four days.
- Hands-on exercises will allow you to install Magnet Axiom and learn about its associated programmatic components: Axiom Process and Axiom Examine.

MODULE 2: WINDOWS 11 OVERVIEW

- In addition to an overview of the course scenario, 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.
- Explore Windows sign-in technologies, such as pin password, Windows Hello, picture password, fingerprint recognition, and facial recognition and how those technologies affect investigations.
- Report on the System Resource Utilization database for applications sending and receiving data via the internet — seeing how much data was sent and received, which could be paramount to proving (or disproving) an alibi.
- Track the current Windows build number of the system being examined, which will ensure the examiner is reporting the correct facts, as some facts change based on the Windows build number currently installed.

MODULE 3: EMD MANAGEMENT AND VOLUME SERIAL NUMBERS

- Learn how to utilize not so well-known registry locations to track serial numbers of volumes being accessed by the Windows Operating System. What files on those volumes were accessed via our suspect and corroborating this information via event logs.
- Use the power of Axiom's filtering and searching to conduct exercises that reinforce the learning objectives by utilizing all of these artifacts to tell a story on the files accessed by a user on a specific drive, and the fact that the drive was accessed by that computer at a certain date and time.

MODULE 4: FINDING MISSING FILES AND FOLDERS

- The Program Compatibility Assistant of the Windows operating system tracks the compatibility of software across different Windows versions.
- The PCA tracks the usage of executables on the suspect system, regardless of it has since been removed, much like USER ASSIST within the NTUser.DAT. AMCache, a very useful

registry location, will be learned by students — including how to garner information detailing the use of executables across the suspect system.
- Learn how to utilize the PCA and AMCache Data to track the use of executables and hashes on the computer in question.

MODULE 5: PREFETCH FILES AND CORRELATING THE DATA

- 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 testifying, it's done with knowledge and confidence. Maximizing the use of the intelligence gathered from prefetch files will lead examiners to discover new avenues to explore in their forensic cases.
- Also track the use of an encrypted container, as well as a wiping utility you may or may not know is built into Windows by default.

MODULE 6: WINDOWS JUMPLISTS & MOST RECENTLY USED (MRU)

- 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: COLLECTING AND PARSING RAM

- 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. Besides collecting, this lesson also goes into the basics of RAM examination in volatility as well as Axiom for carving artifacts. Once you open this Pandora's box, watch out, as you will have a desire to investigate RAM at every opportunity knowing what it can hold.

MODULE 8: SHARING FILES AND FOLDERS AND SETTINGS ACROSS COMPUTERS

- 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.
- Use the acquired RAM from the previous module and Passware to gain access to the Truecrypt container and its contents.

MODULE 9: ITUNES, IOS, AND CLOUD DATA

- 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. Of course, we can't just unlock

the contents of the backup without looking at them and utilizing the data within to help us solve the case we are working.
- Get introduced to Axiom Cloud functionality where a complete collection of the suspects' Gmail account has taken place and entered into an Axiom case to examine and correlate further data.

MODULE 10: ENCRYPTION AND CRACKING WINDOWS 10 PASSWORDS

- Microsoft recently introduced a large anniversary update for Windows 10. The standard login workflow of Windows 10 has been slightly changed and due to these slight, yet significant changes, most hacker tools for pulling password hashes out of Windows will not work anymore. These changes may have been motivated by Microsoft's desire to discontinue support for legacy and vulnerable cryptographic algorithms.
- 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.
- Discuss the booting of the suspect device for court purposes as well as the necessity to gather as many passwords as possible as we are all creatures of habit.

MODULE 11: INVESTIGATING GOOGLE DRIVE

- Google Drive is a powerful tool which has proliferated across businesses and individuals alike. 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 12: 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. If the originals are lost, damaged, or deleted, you can restore them. Users can also browse and restore different versions of their files by browsing through a timeline, selecting the version, and restoring it.
- Learn how to determine File History.

MODULE 13: MODERN APPS OVERVIEW

- Modern Apps (originally known as Metro Apps, Windows 8 Apps, or Windows Store Apps) were designed to be immersive. There is a focus on the touchscreen, but they also work on the standard desktop with no problems.
- Understand that internet history and cache for Modern Apps are not stored in the usual locations where an examiner would expect. Mail App, Photo App, Facebook App, as well as apps from the Windows App Store will all be examined to determine who installed the App, the usage of the App, as well as forensic artifacts left behind for examiners to recover.

MODULE 14: USING FILE SYSTEM LOGGING 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. It is optional to have it on and can be configured with fsutil.exe on Windows. However, it was not turned on by default until Vista and later. Being able to track files through the USNJrnl could be the only reference to the file if it had been previously deleted form the Hard Drive.
- Learn how to investigate the USNJrnl to retrieve forensic artifacts in support of an examination.

MODULE 15: CUMULATIVE REVIEW EXERCISES

- Throughout the four-day training event, instructor-led and student practical exercises are used to reinforce the learning objectives and provide the participants with the knowledge and skills necessary to successfully utilize Magnet Axiom in their investigative workflow.
- 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.