AX200 Axiom Examination

Magnet Certified Forensic Examiner (MCFE)

COURSE OBJECTIVES

Module 1: Introduction and installation of Magnet Axiom

- 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: Evidence processing and case creation

- All settings in Axiom Process will be discussed to ensure the use and effectiveness of Magnet Axiom are maximized during processing — all while decreasing processing time and increasing effectiveness.
- Collection from different evidence sources such as computer-based media (hard disks, USB devices), cloud data, and mobile devices will be discussed and demonstrated.
- Hands-on exercises will focus on processing details such as adding keywords to search and the importance of selecting the different encoding available for "All Content" searches (ASCII, Unicode…), hashing functionality and the varying types of hash sets such as NSRL, Project VIC/CAID, and gold-build image hashes. Optical character recognition and Magnet.AI will be discussed and demonstrated, during this module, students will also be shown the capabilities of setting options for each supported artifact, and how to turn off specific artifacts to speed the processing of evidence files.
- At the conclusion of this module, students will be able to successfully acquire forensic images from various evidence sources; configure case-specific and global settings in Axiom Process for the recovery of key artifacts; and, create a case for analysis in Axiom Examine whilst understanding the available functions Axiom Process offers.

Module 3: Operating system artifacts part 1

- This module will focus on operating system artifacts most encountered during the analysis of computer evidence recovered from the Windows Registry.
- The Registry and Timeline explorers will be utilized to validate and corroborate artifacts recovered from the registry and populated in the Operating System Artifact Category.
- Students will learn to collect basic information from the Operating System by using key artifacts such as Operating System Information, File System Information, User Accounts, and Installed Applications. Students will also understand where these artifacts are located and how to validate the source data.

Module 4: Encryption / anti-forensics

- Understand the importance of looking for encryption and anti-forensics tools and how Axiom categorizes those artifacts into a specific artifact category, enabling a quick identification if either category of software is being employed on the suspect media.

- Utilizing the post-processing functionality of Axiom through instructor-led exercises, students will utilize the encryption plugins of Axiom Process to identify, decrypt, and process additional evidence into an existing case.

Module 5: Refined results

- The Refined Results artifact category of Axiom Examine is defined to combine and refine artifacts recovered into specific subcategories of artifacts for commonly sought-after items of evidence.
- Learning Magnet Axiom's artifact-first forensics approach is a major part of this lesson and refined results play a huge part in that. For example, most examiners at some point during a computer forensics examination will want to know what the subject searched for using Google, as Google is the most used search engine. Refined Results contains an artifact category aptly named Google searches where all Google Searches, independent of the browser used, are categorized in one place for ease of use.
- Creating profiles of the suspect and victim on the individual items of evidence from the information recovered in the Refined Results "Identifiers Artifact" will allow the examiner to search across multiple devices cross-platform to retrieve and correlate data from one piece of evidence to another.
- Different levels of filtering will be explored, including filtering on specific columns and filtering on entire evidence sets with both 'Basic' and 'Advanced' filters, students will also learn how to save advanced filters which can be utilized in future cases.

Module 6: Web related

- Learn how the most popular browsers store items like Internet history, favorites, and bookmarks, and how each one stores information in their respective databases. Google Chrome, Firefox, and Microsoft Edge, store artifacts, and being able to track and recover artifacts from the web browsers to correlate the information discussed in previous lessons is paramount to solving cases.
- Autofill and previous search information will also be examined in this lesson to glean information that was typed in and saved by the user.

Module 7: Communications

- Learn how to recover emails and email attachments from mail clients.
- Review, sort, filter, and tag emails, as well as search through their transport message headers and their attachments to retrieve valuable information pertaining to the investigation.
- Gain an understanding of source linking as it relates to emails and understand the results found in the Details and Content cards of Axiom.
- The analytics of the Connections explorers will also help examiners connect key pieces of evidence together to tell the entire story of who, what, when, where, and how the suspect

artifacts came to be on the system and if the artifacts were distributed through cloud storage, email, or chat.

- Finally, students will discover the ease of the export functionality to export email artifacts and their attachments into numerous formats supported by Axiom Examine.
- Explore how Android devices store SMS/MMS messages in SQLite databases.
- Utilize the conversational view to rethread messages into their relevant chats and in a 'message bubble' format easily review the individual messages in a friendly-to-read format.

Module 8: Documents

- Gain an understanding of the differing views of documents as well as the metadata of files and the relevance of the numerous dates and times and what they could mean to the examination.
- Utilize Magnet Axiom to save artifacts externally from Axiom and the formats used during the export functionality.
- Explore the ability to maximize the filtering, sorting, and search potential of documents via the filters bar and metadata searches using Axiom. Utilizing optical character recognition (OCR) will easily allow for words to be extracted from PDFs and pictures making the content of those files keyword searchable.

Module 9: Operating system artifacts part 2

- This module will continue to focus on artifacts found within the Operating System category and how those artifacts will help steer the investigation.
- Students will learn to understand information from the Operating System by using key artifacts such as LNK Files, USB Devices, UserAssist, Jump Lists, and more.

Module 10: Media

- Learn about image and video artifacts and how the differing views of Magnet Axiom make it easy to review them.
- Axiom's filmstrip view concerning videos and thumbnail view for images will be introduced.
- EXIF data and how the sorting and filtering of the EXIF data including geolocation information, camera make, model, and serial number will be explained to allow for the categorization of images in an expedient and efficient manner in preparation for writing a final report.
- Understand the Officer Wellness feature and how to grade media for illicit image cases within Axiom.
- Maximize the use of Magent.AI to automatically categorize images using the power of the CPU and GPU into multiple categories including possible documents, ID cards, screen captures, and human faces and many more.

- The Media Explorer will be introduced allowing the user to deep dive into media types, identify potential distribution markers, apply extensive filtering, and sort files, and utilizing hit-stacking examiners can quickly identify multiple copies of the same videos and pictures.

Module 11: Cloud

- With the proliferation of cloud storage and the acceptance of it in both the corporate environment as well as the home-user environment, it is important for all examiners to understand the artifacts that remain on the cloud, which may not be stored on local media.
- During this discussion, we will explore Axiom's capabilities for cloud collection and examination by identifying cloud artifacts.
- Being able to combine data from computers, mobile devices, and the cloud into one case and to utilize the power of Axiom to correlate that data in case it is in multiple places on a suspect's many devices could prove to be the catalyst in solving an investigation.

Module 12: Reporting

- Explore the various exporting and reporting features available within Axiom Examine used for the presentation of case evidence and collaboration with other investigative stakeholders.
- Through the scenario-based instructor-led and student practical exercises, learn how to manage the exporting of artifacts; produce and merge portable cases; and create a final investigative case report that is easily interpreted by both technical and non-technical recipients.
- Configure the reporting wizard to easily set predefined reports allowing continuity between organizational reports.

*****