AX200 Magnet AXIOM Examination

Magnet AXIOM Examinations (AX200) is ideal for those who require intermediate-level training with a digital investigation platform that covers cases involving smartphones, tablets, computers, and cloud data in a single collaborative interface. This course is the perfect entry point for examiners who are new to AXIOM.

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, memory cards, USB devices), cloud data, and mobile devices will be discussed and demonstrated.
- Hands-on exercises will focus around 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, and gold-build image hashes. During this exercise, 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.

MODULE 3: OPERATING SYSTEM ARTIFACTS Part 1

- This module will focus on operating system artifacts most commonly encountered during the analysis of computer evidence recovered from the Windows Registry.
- The Registry Explorer will be utilized to validate 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.

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.
- Track keys used to decrypt encrypted disks and then re-ingest that information using AXIOM post-processing.

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 most commonly sought-after items of evidence.
- Learning Magnet AXIOM's artifact-first forensics approach is a major part of this lesson and refined results plays a huge part of 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 commonly 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" category will allow the examiner to search across multiple devices cross platform to retrieve and correlate data from one piece of evidence to another.

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. Chrome, Firefox, Internet Explorer, Edge, Opera and Apple Safari store artifacts differently 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.
- Webcache will be used in this lesson to rebuild webpages of interest to the student. Autofill information will also be examined in this lesson to glean information that was typed in and saved by the user.

MODULE 7: EMAIL

- 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.
- Finally, students will discover the ease of the export functionality to export email artifacts and their attachments into numerous formats supported by AXIOM Examine.

MODULE 8: DOCUMENTS

- Gain an understanding of the differing views of documents as well as the metadata of files and what 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 a stacked filter approach will allow the separation of large amounts of data found within evidence files from the actual data being sought after.

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.
- Learn about the Timeline and Connections explorers and how the utilization of those explorers help visualize how artifacts are connected to one another. The analytics of Timeline and 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.

MODULE 11: MOBILE & Mobile Artifacts

This module is comprised of two parts: Extracting information from an Android device and exploring its artifacts as well as artifacts from the CHAT category in AXIOM.

- Learn about device file systems and structures to recover additional information, including device owner information; third party application data; core operating system data; internet browser data; and more.
- The hands-on exercise will also work through AXIOM's Dynamic App Finder so that examiners who are conducting mobile device examinations can look for SQL databases belonging to apps currently unsupported by AXIOM in the core product. This will allow them to be produced as an

artifact within AXIOM Cyber as an artifact within AXIOM Examine, thereby supporting mobile apps which are new.

- Magnet AXIOM employs several different explorers that can be used in Magnet AXIOM Examine to view Artifacts and information within the casefile in a much more efficient and expedient workflow. The Dashboard, Artifact, File System, and Connections explorers are utilized to look at evidence associated with chat related activities including Skype and Windows Your Phone.
- Conduct searches, as well as how to use the many AXIOM Examine filtering options and functionality to identify key Chat artifacts from file, folder, and database structures. Utilizing the built-in SQLite browser within AXIOM Examine, students will validate what artifacts are recovered from the Your Phone SQLite database.
- AXIOM Examine will be used to rebuild chats into a conversation view, as seen on most mobile devices, commonly used on mobile devices which examiners and users are accustomed to.
- Also learn how to tag and comment on key artifacts in preparation for case reporting and how to enable Magnet.AI to assist in investigations dealing with Chat classification.

MODULE 12: 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.
- Discovering cloud artifacts and putting together what the capabilities of AXIOM are in reference to cloud collection and examination will be discussed.
- 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 13: 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 which is easily interpreted by both technical and non-technical recipients.

MODULE 14 : CUMULATIVE REVIEW EXERCISES

- A final scenario-based practical exercise will be administered, which represents a cumulative review of the exercises conducted in each of the previous modules.