

MAGNET AXIOM™

Training & Certification

Magnet AXIOM Examinations (AX200)

AXIOM Examinations (AX200) is an intermediate-level course, designed for participants who are familiar with the principles of digital forensics, and seeking to use Magnet AXIOM for their investigations. We offer in person, online, and online self-paced courses.

After completing the four-day course, participants will have the knowledge and skills to acquire forensic images from computer and smartphone evidence; configure Magnet AXIOM Process to recover the most-relevant artifacts; use Magnet AXIOM Examine to explore the evidence in greater depth, simplifying analysis activities by intuitively linking facts and data; and, prepare key artifacts for collaboration with other stakeholders.

Each module of instruction employs extensive scenario-based exercises, to reinforce the learning objectives, and further enhance the participant's understanding of Magnet AXIOM's functionality, and its application within the forensic workflow.

Objectives of AXIOM Examinations (AX200)

- Installation of AXIOM and its core components, AXIOM Process and AXIOM Examine
- Configurations of AXIOM Process for the acquisition and processing of digital evidence — including Single Stage Evidence Processing
- Analyzing case data in AXIOM Examine
- Utilization of hash sets, keywords, regular expressions, and filters to identify key artifacts
- Navigation within the evidence set, using the Artifact, File System, and Registry explorer functionality
- Application of bookmarks, tags and comments to prepare case evidence for exporting and reporting
- Using AXIOM Examine visualization tools to emphasize user behavior patterns
- Enhancing participant understanding of key artifacts; their locations and formats; the user and system behaviors which created them; and, the manner in which AXIOM recovers them
- Building intuitive reports and sharing and managing portable cases with stakeholders

Magnet AXIOM Examinations (AX200) Modules

Module 1: Intro and Installation of Magnet AXIOM

In this introductory module, participants will be presented with an overview of the upcoming course and will take part in hands-on exercises in which participants will install Magnet AXIOM and learn about its associated programmatic components, AXIOM Process and AXIOM Examine.

Module 2: Evidence Processing and Case Creation

This module will focus on the many features available in AXIOM Process. It will give participants the knowledge and skills necessary 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. After the creation of the case, participants will be introduced to the AXIOM Examine interface.

Module 3: Computer Artifact Analysis

This section of the course is composed of several modules, each of which will focus on a specific set of key artifacts most commonly encountered during the analysis of computer evidence. The modules within this section will include presentations on refined results, chat clients, documents, email, media, social networking, internet browsers, and operating system artifact analysis, as well as demonstrate the navigation, searching, filtering, and tagging features in AXIOM.

Module 4: Mobile Artifact Analysis

This module will explore smartphone evidence, parsed by Magnet AXIOM — with two sub-modules focusing on iPhone artifacts and Android artifacts. In addition, they will explore the 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.

Module 5: Reporting

In this final instructional module of the course, participants will explore the various exporting and reporting features available within AXIOM, used for the presentation of case evidence, and collaboration with other investigative stakeholders. Participants will 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 6: Cumulative Review Exercises

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