MAGNET AXIOM EXAMINATIONS (AX200)

AXIOM EXAMINATIONS MODULE DESCRIPTIONS

Module 1: Intro and Installation of Magnet AXIOM(Day1)

In this introductory module, participants will be presented with the learning objectives and expected outcomes for the four-day training event, and all related course materials. The module will conclude with hands-on exercises during 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(Day1)

This module of instruction will focus on the many features available in AXIOM Process. At the conclusion of this module, participants will have 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, and the module includes instructor-led, and student practical exercises, to reinforce the learning objectives.

Module 3: Computer Artifact Analysis(Day2~3)

The Computer Artifact Analysis section of the course is composed of several modules, each of which focusing 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. For each of the modules, scenario-based instructor-led and student practical exercises will be used to demonstrate the navigation, searching, filtering, and tagging features in AXIOM, and reinforce the learning objectives.

Part1 : Refined Results	Part2 : Chat Artifacts
Part3 : Documents	Part4 : Email
Part5 : Media	Part6 : Social Networking
Part7 : Web Related Artifacts	Part8 : Operating System Artifacts

Module 4: Mobile Artifact Analysis(Day4)

The Mobile Artifacts Analysis section is composed of two modules, one focusing on iPhone artifacts, and the second on Android artifacts. Participants will explore smartphone evidence, parsed by Magnet AXIOM, from each operating system. In addition, the modules 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. Scenario-based instructor-led, and student practical exercises will be used to demonstrate the navigation, searching, filtering, and tagging features in AXIOM, and reinforce the learning objectives.

Module 5: Reporting(Day4)

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. Through the scenario-based instructor-led, and student practical exercises, 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(Day4)

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.