AX200 Magnet AXIOM Examinations

Kurzbeschreibung:

AXIOM Examinations (AX200) ist ein Kurs für Teilnehmende, die bereits mit den Grundsätzen der digitalen Forensik vertraut sind und ihre Untersuchungen mit Magnet AXIOM durchführen möchten.

Zielgruppe:

Kunden und Kundinnen, die bereits Erfahrungen mit AXIOM gesammelt haben und erfahrene Ermittler(innen), die ihren Werkzeugkasten ergänzen möchten.

Voraussetzungen:

Keine

Sonstiges:

Dauer: 4 Tage

Preis: 2640 Euro plus Mwst.

Ziele:

Nach Abschluss des viertägigen Kurses haben die Teilnehmenden ausreichende Kenntnisse und Kompetenzen, um Beweise aus Computern und Smartphones als forensische Images zu sichern, Magnet AXIOM Process so zu konfigurieren, dass die relevantesten Artefakte wiederhergestellt werden, die Beweise mit Magnet AXIOM Examine eingehender zu untersuchen, die Analyseabläufe durch intuitive Verknüpfungen von Fakten und Daten zu vereinfachen und wichtige Artefakte für die Zusammenarbeit mit anderen Beteiligten vorzubereiten.

Inhalte/Agenda:

- ♦ VORSTELLUNG UND INSTALLATION VON MAGNET AXIOM
- ♦
  - ◊ Präsentiert werden die Lernziele und die innerhalb der vier Kurstage erwarteten Ergebnisse.
  - ◊ Bei praktischen Übungen können Sie Magnet AXIOM installieren und sich mit den dazugehörigen Programmkomponenten vertraut machen: AXIOM Process und AXIOM Examine

♦ BEARBEITUNG VON BEWEISEN UND FALLERSTELLUNG

♦
- ◊ Es werden alle Einstellungen in AXIOM Process erörtert, mit denen sich der Nutzen und die Effektivität von Magnet AXIOM bei der Bearbeitung maximieren und die Bearbeitungszeit gering halten lassen.
- ◊ Die Erfassung verschiedener Beweisquellen, wie z. B. computerbasierte Medien (Festplatten, Speicherkarten, USB-Geräte), Cloud-Daten und mobile Geräte, wird besprochen und vorgeführt.
- ◊ Bei den praktischen Übungen wird es vor allem um Detailaspekte der Bearbeitung gehen, zum Beispiel das Hinzufügen von Schlüsselwörtern zur Suche und die Bedeutung der Auswahl der jeweiligen Codierung (ASCII, Unicode...) bei Suchen in „allen Inhalten“, die Hash-Funktion und die verschiedenen Arten von Hash-Sets, wie z. B. NSRL, Project VIC und Image-Hashes von Gold-Builds. Hierbei erfahren die Teilnehmenden auch, welche Funktionen die Einstellungsoptionen für die einzelnen unterstützten Artefakte haben und wie sich durch Abschalten bestimmter Artefakte die Bearbeitungsgeschwindigkeit der Beweisdateien erhöhen lässt.
- ◊ Bei Beendigung des Moduls können die Lernenden forensische Images aus verschiedenen Beweisquellen sichern, in AXIOM Process fallspezifische und globale Einstellungen zur Wiederherstellung wichtiger Artefakte konfigurieren und einen Fall zur Analyse in AXIOM Examine erstellen.

♦ ANALYSE VON COMPUTER-ARTEFAKTEN

♦
- ◊ In diesem Modul geht es um Artefakte aus dem Betriebssystem, die am häufigsten bei der Analyse von Computerbeweisen, die aus der Windows-Registry wiederhergestellt wurden, anzutreffen sind.
- ◊ Zur Validierung von Artefakten, die aus der Registry wiederhergestellt und in der Artefaktkategorie „Betriebssystem“ eingeordnet wurden, wird der Registry-Explorer verwendet.
- ◊ Unter anderem sind Untersuchung und Nachverfolgung von USB-Geräten, Jump-Listen, Prefetch-Dateien, LNKDateien, dem Windows-Benachrichtigungszentrum, Betriebssystemdaten, Shellbags, Zeitzonen-Informationen, Benutzerkonten, User Assist, virtuellen Maschinen und Windows-Ereignisprotokollen Gegenstand dieser Lektion. Außerdem geht es darum, wie sich die Daten zueinander in Beziehung setzen lassen, um die Nutzungsgeschichte des Computers zu rekonstruieren und die Person zum Leben zu erwecken, die am Computer saß, als die kriminellen Handlungen verübt wurden.

♦ WEBBEZOGEN

♦
- ◊ Hier erfahren Sie, wie die beliebtesten Browser Angaben wie zum Beispiel den Internetverlauf, die Favoriten und Lesezeichen speichern und wie sie Daten jeweils in eigenen Datenbanken abspeichern. Chrome, Firefox, Internet Explorer, Edge, Opera und Apple Safari speichern Artefakte auf unterschiedliche Weise. Bei der Lösung von Fällen ist es äußerst wichtig, Artefakte von den Webbrowsern nachzuverfolgen und wiederherstellen zu können, um sie zu den Daten aus den vorhergehenden Lektionen in Beziehung zu setzen.
- ◊ Der Browser-Cache wird in dieser Lektion zur Wiederherstellung von Webseiten verwendet, die für die Teilnehmenden von Interesse sind. Außerdem betrachten wir in dieser Lektion Autofill-Daten, mit denen Sie einen Blick auf die von Benutzern eingegebenen und abgespeicherten Daten erhalten.

♦ VERFEINERTE ERGEBNISSE

♦
- ◊ Die Artefaktkategorie „Verfeinerte Ergebnisse“ in AXIOM Examine ist darauf ausgelegt, dass die wiederhergestellten Artefakte durch Kombination und Verfeinerung in spezifische Unterkategorien für die am häufigsten gesuchten Beweisstücke eingeteilt werden.
- ◊ Ein großer Teil dieser Lektion besteht darin, das artefaktorientierte Konzept von Magnet AXIOM zu erlernen. Verfeinerte Ergebnisse spielen dabei eine wichtige Rolle. Zum Beispiel wollen die meisten Ermittler(innen) zu irgendeinem Zeitpunkt während einer forensischen Computeruntersuchung wissen, wonach die Zielperson auf Google gesucht hat, da Google die am häufigsten verwendete Suchmaschine ist. „Verfeinerte Ergebnisse“ enthält eine Artefaktkategorie, die passenderweise „Google Suche“ heißt. Hier werden alle Google-Suchen browserunabhängig zentral kategorisiert, um die Benutzerfreundlichkeit zu erhöhen.
- ◊ Durch die Erstellung von Profilen für den Verdächtigen und das Opfer anhand von Informationen, die in der Artefaktkategorie „Identifikatoren“ wiederhergestellt wurden, können Ermittler(innen) durch eine plattform und geräteübergreifende Suche Daten abrufen und per Abgleich verschiedener Beweisstücke in Beziehung zueinander setzen.
- ◊ Mit der Artefakt-Referenz und dem Benutzerhandbuch können Sie sich auch weiterhin über neue Artefakte, die in neuen Versionen von AXIOM unterstützt werden, auf dem Laufenden halten.

♦ E-MAIL◊

♦
- ◊

- ◊ Hier erfahren Sie, wie sich E-Mails und E-Mail-Anhänge von Mail-Clients wiederherstellen lassen.
- ◊ Sie können nicht nur die E-Mails prüfen, sortieren, filtern und kennzeichnen, sondern auch ihre Transport-Nachrichten-Header und Anhänge nach Informationen durchsuchen, die für die Ermittlung von Bedeutung sind.
- ◊ Sie machen sich mit der Verlinkung von Quellen, soweit sie E-Mails betrifft, und den Ergebnissen in den AXIOM-Karten „Details“ und „Inhalt“ vertraut.
- ◊ Zu guter Letzt erfahren die Teilnehmenden, wie leicht sich mit der Exportfunktion E-Mail-Artefakte und ihre Anhänge in die vielen Formate exportieren lassen, die AXIOM Examine unterstützt.

♦ DOKUMENTE ◊

♦
- ◊ Hier machen Sie sich mit den verschiedenen Dokumentansichten und den Dateimetadaten vertraut. Außerdem erfahren Sie, inwiefern die verschiedenen Daten und Uhrzeiten relevant sind und was sie für die Ermittlung bedeuten können.
- ◊ Sie verwenden Magnet AXIOM, um Artefakte außerhalb von AXIOM und den beim Export verwendeten Formaten zu speichern.
- ◊ Sie lernen die erweiterten Möglichkeiten zur Filterung, Sortierung und Durchsuchung von Dokumenten über die Filterleiste und Metadatensuchen mit AXIOM kennen. Mit gestapelten Filtern lassen sich die großen Datenmengen in Beweisdateien von den Daten trennen, nach denen Sie eigentlich suchen.

♦ MEDIEN ◊

♦
- ◊ Hier machen Sie sich mit Bild- und Videoartefakten vertraut und erfahren, wie Sie sich mit den verschiedenen Ansichten in Magnet AXIOM leicht überprüfen lassen.
- ◊ Sie lernen die Filmstreifen-Ansicht für Videos und die Miniaturansicht für Bilder kennen.
- ◊ Es werden EXIF-Daten (wie zum Beispiel Geolokalisierungsdaten und Marke, Modell und Seriennummer der Kamera), mit denen Sie die Bilder bei der Vorbereitung für den Abschlussbericht sinnvoll und effizient kategorisieren können, und ihre Sortierung und Filterung erklärt.
- ◊ Sie verstehen die Funktion „Wohlbefinden der Beamten“ und wie sich Medien in AXIOM in Bezug auf die Gesetzeswidrigkeit der Bilder einstufen lassen.
- ◊ Ziehen Sie maximalen Nutzen aus Magnet.AI, indem Sie Bilder mit der Rechenkraft von CPU und GPU automatisch in verschiedene Kategorien wie zum Beispiel „In Frage kommende Dokumente“, „Ausweisdokumente“, „Bildschirmaufnahmen“, „Menschliche Gesichter“ usw. einteilen.
- ◊ Lernen Sie den Zeitachsen- und Beziehungen-Explorer kennen, und erfahren, wie Sie mit diesen Explorern die Verbindungen zwischen den einzelnen Artefakten visualisieren können. Die Analyse des Zeitachsen-Explorers und des Beziehungen-Explorers hilft Ermittlern und Ermittlerinnen außerdem, wichtige Beweisstücke zueinander in Verbindung zu setzen, um ein vollständiges Bild zu gewinnen, durch wen, wann, wo und wie welche verdächtigen Artefakte in das System gelangt sind und ob sie durch Speicherung in der Cloud, durch E-Mails oder im Chat weiterverbreitet wurden.

♦ MOBIL ◊

♦
- ◊ Sie lernen die Dateisysteme und -strukturen der Geräte kennen, um zusätzliche Informationen (z. B. Informationen über den/die Besitzer(in) des Geräts), Daten aus Anwendungen von Drittanbietern und Internetbrowsern usw. wiederherzustellen.
- ◊ Bei den praktischen Übungen wird außerdem der dynamische App-Finder von AXIOM behandelt, mit dem Ermittler(innen) bei der Untersuchung von Mobilgeräten nach SQL-Datenbanken suchen können, deren Apps im Kernprodukt von AXIOM derzeit noch nicht unterstützt werden. Dadurch lassen sie sich in AXIOM Cyber und AXIOM Examine als Artefakt produzieren, sodass auch mobile Apps unterstützt werden, die noch neu auf dem Markt sind.

♦ CHAT ◊

♦
- ◊ Magnet AXIOM bringt mehrere unterschiedliche Explorer zum Einsatz, damit das Anzeigen der Artefakte und Informationen in der Falldatei in Magnet AXIOM Examine über einen effizienteren und zweckmäßigeren Workflow erfolgen kann. Mit dem Dashboard-Explorer, dem Artefakt-Explorer, dem Dateisystem-Explorer und dem Beziehungen-Explorer können Sie sich Beweismittel ansehen, die mit Chat-Aktivitäten (z. B. über Skype und Windows Your Phone) in Zusammenhang stehen.
- ◊ Sie erfahren, wie Sie eine Suche durchführen und die vielen Filteroptionen und -funktionen von AXIOM Examine nutzen können, um in Datei-, Ordner- und Datenbankstrukturen wichtige Chat-Artefakte zu erkennen. Die Teilnehmenden überprüfen mit dem in AXIOM Examine integrierten SQLite-Browser, welche Artefakte aus der Your Phone SQLite-Datenbank wiederhergestellt wurden.
- ◊ Mit AXIOM Examine werden Chats in einer Konversations-Ansicht rekonstruiert, wie sie auf den meisten Mobilgeräten (unter anderem denen der Ermittler(innen) und Benutzer und Benutzerinnen) üblich ist.
- ◊ Außerdem lernen Sie, bei der Vorbereitung auf die Fallberichterstattung wichtige Artefakte zu kennzeichnen und kommentieren, und die Magnet.AI-Unterstützung bei Ermittlungen mit Chat-Klassifizierung zu aktivieren.

♦ CLOUD ◊

♦
- ◊ Angesichts der Verbreitung und Akzeptanz der Cloud-Speicherung in der Wirtschaft und bei Privatnutzern ist es für jeden Ermittler / jede Ermittlerin xwichtig, sich die Bedeutung von Artefakten klar zu machen, die in der Cloud verbleiben und möglicherweise nicht auf lokalen Medien gespeichert werden.
- ◊ Wir werden die Entdeckung von Cloud-Artefakten und die einzelnen Funktionen von AXIOM zur Erfassung und Untersuchung von Cloud-Daten erörtern.
- ◊ Die Möglichkeit zur Kombination der Daten von Computern, von mobilen Geräten und aus der Cloud in einem Fall und der Einsatz der Rechenkraft von AXIOM, um die Falldaten zueinander in Beziehung zu setzen, wenn sie sich an verschiedenen Orten auf den vielen Geräten eines Verdächtigen befinden, können sich als Katalysator bei der Ermittlung erweisen.

- VERSCHLÜSSELUNG/ANTI-FORENSIK
  - Sie erfahren, wie wichtig es ist, nach Verschlüsselungsprogrammen und Anti-Forensik-Tools zu suchen, und wie AXIOM solche Artefakte in einer speziellen Artefaktkategorie zusammenfasst, damit Sie schnell erkennen, wenn eine der beiden Softwarekategorien auf dem Medium des Verdächtigen zum Einsatz kommt.
  - Sie verfolgen ein Verschlüsselungsprogramm nach, das auf dem System des Verdächtigen verwendet wird, vom Moment der Installation und Aktivierung an (einschließlich der damit verbundenen Zeitachse).

- BERICHTERSTELLUNG
  - Sie lernen die verschiedenen Export- und Berichterstellungsfunktionen kennen, die in AXIOM Examine zur Präsentation der Beweismittel in einem Fall und zur Zusammenarbeit mit anderen Personen, die an der Ermittlung beteiligt sind, dienen.
  - Durch angeleitete Szenarien und praktische Übungen lernen die Teilnehmenden, den Export der Artefakte zu verwalten, tragbare Fälle zu erstellen und zusammenzuführen und die Ermittlung mit einem Fallbericht abzuschließen, den sowohl Fachkundige als auch Laien problemlos verstehen können.

- ZUSAMMENFASSENDE PRÜFUNGSÜBUNGEN
  - Als Zusammenfassung der Übungen in allen vorhergehenden Modulen wird eine abschließende praktische Übung auf Grundlage eines Szenarios durchgeführt.
  -