AX350 Magnet AXIOM macOS Examinations

Kurzbeschreibung:

Dieser Kurs ist eine viertägige Schulung auf Expertenebene und richtet sich an Teilnehmer, die mit den Prinzipien der digitalen Forensik einigermaßen vertraut sind und ihr Wissen über macOS und die forensische Analyse von Geräten mit dem APFS-Dateisystem und AXIOM erweitern möchten.

Zielgruppe:

Teilnehmer, die mit den Grundsätzen der digitalen Forensik nicht vertraut sind

Voraussetzungen:

AX200 Magnet AXIOM Examinations

Sonstiges:

Dauer: 4 Tage

Preis: 2820 Euro plus Mwst.

Ziele:

Die Prüfer werden ein Szenario untersuchen, in dem es um einen falsch konfigurierten Webserver geht, der es Hackern ermöglichte, Schwachstellen auszunutzen und sich Zugang zum Netzwerk zu verschaffen, um eine schändliche Aktivität durchzuführen und geistiges Eigentum und möglicherweise auch Kundendaten zu stehlen.

Inhalte/Agenda:

- MODUL 1: EINFÜHRUNG UND KURSÜBERSICHT
  - In diesem Modul erhalten die Teilnehmer eine Einführung in den Kurs und lernen das Szenario kennen, das während der viertägigen Schulung durchlaufen wird.

- MODUL 2: MACOS-ÜBERSICHT
  - In diesem Modul werden Informationen über das macOS-Betriebssystem und das APFS-Dateisystem vermittelt. Dazu gehören Änderungen an der Sicherheit von macOS-Geräten, einschließlich der T2-Chips, SIP und anderer Sicherheitsprotokolle, die von Apple verwendet werden. Die Teilnehmer werden auch die richtige Handhabung von macOS-Geräten besprechen.
  - Mehrere wichtige Betriebssystemartefakte für macOS werden behandelt, darunter Finder, Dateisystemereignisse, Seitenleistenelemente, Papierkorb, installierte Programme und mehr.

- MODUL 3: BEGINN DER PRÜFUNG
  - In diesem Modul besprechen die Teilnehmer Verschlüsselungsprobleme wie FileVault2 und Methoden, mit denen diese Technologie mit Passware geknackt werden kann.

- MODUL 4: PROTOKOLLDATEIEN
  - In diesem Modul werden verschiedene macOS-Protokolldateien behandelt, wie z. B. die vereinheitlichten Protokolle, Konfigurationsdateien, Datei-/Ordnerberechtigungen, tägliche Protokolle, der USB-Verbindungsverlauf und andere wichtige Protokollierungsartefakte, um den Benutzerzugriff auf Informationen zu verfolgen.

- MODUL 5: KNOWLEDGEC
  - Der Zugang zu präzisen und detaillierten Benutzer- und Anwendungsdaten kann bei einer forensischen Untersuchung äußerst nützlich sein. Die KnowledgeC-Datenbank speichert eine Fülle von Informationen über die macOS-Nutzung und die Benutzeraktivitäten.
  - Einige der wichtigsten Dinge, die in dieser Datenbank aufgezeichnet werden, werden als Artefakte dargestellt, z.B:
    - · Anwendungsnutzung
    - · Anwendungsaktivitäten
    - · Safari-Browser-Verlauf
    - · Energiestatus des Geräts
  - Zusätzlich zum besseren Verständnis von KnowledgeC wird die auf macOS gespeicherte Powerlog-Datenbank untersucht, um den Prüfern die Validierung und das Verständnis des verfolgten Benutzerverhaltens zu erleichtern.

- MODUL 6: INTERNET-ARTEFAKTE
  - Verschiedene Browserverlaufs-Artefakte von Safari, Chrome und Firefox werden untersucht, um die Untersuchung und die Sammlung von Beweisen zur Unterstützung der von den Schülern durchgeführten Untersuchung zu unterstützen.
  - Die Schüler werden auch erforschen, wie man wertvolle Informationen, die von Internet-Browsern geliefert werden, für erweiterte Attribute von Dateien nutzen kann.

- MODUL 7: BENUTZERKONTEN
  - Das Verständnis der spezifischen Daten eines Benutzerkontos kann bei einer Untersuchung entscheidend sein. In diesem Modul werden Artefakte behandelt, die sich mit Kontakten, Adressbüchern, gespeicherten Apple-Konten, Schlüsselbundinformationen, installierten Anwendungen und An- und Abmeldezeiten befassen.

- MODUL 8: EMAIL
  - Das Standard-E-Mail-Programm (Mail.App) speichert sowohl E-Mail- als auch Kalenderdaten innerhalb von macOS. In diesem Modul wird besprochen, wie Artefakte und Anhänge aus diesen gespeicherten Dateien wiederhergestellt werden können.

- MODUL 9: MAC-DESKTOP
  - Der macOS-Schreibtisch speichert mehrere wertvolle Artefakte zu den Daten, auf die ein Benutzer zugegriffen hat. In diesem Modul werden die Teilnehmer die im mac Dock gespeicherten Elemente, die Anwendungen in der Menüleiste, die zuletzt verwendeten Elemente und die Schnellansicht-Miniaturansichten betrachten und erfahren, wie sie bei einer Untersuchung verwendet werden können.
  - Die Prüfer werden auch das AXIOM-Artefakt Rebuilt Desktop - macOS untersuchen, um eine bessere visuelle Darstellung der Funktionsweise dieser Artefakte zu erhalten, die bei der Ermittlung des Benutzerverhaltens hilft.

- MODUL◊ 10: TIME MACHINE UND SCHNAPPSCHÜSSE
- ◊ Time Machine ist eine in macOS integrierte Backup-Methode. In diesem Modul werden die Teilnehmer die Time Machine- und Snapshot-Funktionen von macOS und das APFS-Dateisystem kennenlernen. Diese Informationen sind wertvoll, wenn es darum geht, Dateien wiederherzustellen, die auf dem macOS-System möglicherweise nicht mehr aktiv sind.

- MODUL◊ 11: CLOUD-DIENSTE
- ◊ MacOS-Benutzer haben in der Regel eine Apple ID und damit kostenlosen iCloud-Speicher. Dieser Cloud-Speicher kann sich bei einer Untersuchung als wichtig erweisen, ebenso wie andere Cloud-Datenquellen wie OneDrive und Google Drive. Zu verstehen, wie macOS diese Dienste nutzt und welche Datenbanken den Datenfluss zwischen dem Cloud-Dienst und dem Host-Computer steuern, ist für die Lösung dieser Art von Untersuchungen unerlässlich.

- MODUL◊ 12: KUMULATIVE PRÜFUNG
- ◊ In einem abschließenden Praktikum üben die Teilnehmer die Techniken und analysieren die in diesem Kurs besprochenen Artefakte.
- ◊