AX301 Magnet AXIOM & GrayKey (MAGaK)

Kurzbeschreibung:

Dieser Kurs ist eine viertägige Schulung auf mittlerem Niveau und richtet sich an Teilnehmer, die mit den Grundsätzen der digitalen Forensik vertraut sind und ihr Wissen über tiefgreifende iOS-Untersuchungen und die Verwendung des GrayKey-Geräts erweitern möchten.

Zielgruppe:

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

Voraussetzungen:

AX200 Magnet AXIOM Examinations Die Teilnehmer müssen einer von Grayshift zugelassenen Strafverfolgungsbehörde angehören, um an diesem Kurs teilnehmen zu können.

Sonstiges:

Dauer: 4 Tage

Preis: 2820 Euro plus Mwst.

Ziele:

Die Teilnehmer lernen die praktische Anwendung des GrayKey-Geräts und seine vollständige Bedienung, einschließlich der Einrichtung eines ordnungsgemäßen Arbeitsablaufs für die Übergabe von iOS-Geräten vor Ort an das Labor und die Erstellung eines vollständigen Dateisystemabbilds von iOS-Geräten. Außerdem wird Magnet AXIOM eingesetzt, um zu lernen, wie das iOS-Dateisystem strukturiert ist, wie man wichtige Daten findet und wie Artefakte strukturiert sind. Darüber hinaus lernen die Teilnehmer Artefakte kennen, die für das vollständige iOS-Dateisystem und seine verschiedenen Datenschutzstufen spezifisch sind. Die Analyse von Drittanbieter-Artefakten verschiedener fortgeschrittener, sicherer Artefakte wird behandelt, einschließlich der Frage, wie der Schlüsselbund des Geräts mit diesen Artefakten verbunden ist. Es wird eine Methodik diskutiert, wie man iOS-Untersuchungen auf tiefer Ebene durchführt und wie man spezifische Artefakte des Betriebssystems im Kontext versteht, um Geräteinteraktionen im Laufe der Zeit aufzuzeigen. Die Teilnehmer lernen, wie sie sich in ein Gerät hineinversetzen können, das physisch mit ihm interagiert, und manchmal sogar, wo dieses Gerät gewesen ist.

Inhalte/Agenda:

- ♦ MODUL 1: KURSEINFÜHRUNG
  - ♦ ◊ Vermittlung der Grundvoraussetzungen für die AXIOM-Software und das GrayKey-Gerät.

- ♦ MODUL 2: IOS UND APPLE-SICHERHEIT VERSTEHEN
  - ♦ ◊ Diskussion über die Sicherheitsfunktionen und die Struktur des iOS-Betriebssystems.
  - ◊ Lernen Sie die Schlüssel der Geräteschutzklassen kennen, verstehen Sie die Codes für die Handy-Sperre und deren Funktion sowie weitere Funktionen des Betriebssystems.

- ♦ MODUL 3: VERWENDUNG DES GRAYKEY-GERÄTS
  - ♦ ◊ Abdeckung aller Optionen und Einstellungen des GrayKey-Geräts, um Informationen von iOS-Geräten zu extrahieren.
  - ◊ Es werden Informationen über die neuesten Versionen von iOS besprochen.
  - ◊ Lernen Sie, wie Sie Zugang zu Informationen erhalten, die mit den meisten forensischen Techniken nicht zugänglich sind.
  - ◊ Sie erfahren, wie Sie Informationen aus Geräten extrahieren können, die noch mit einem Passcode gesperrt sind, und wie Sie Passcodes umgehen können.

- ♦ MODUL 4: GERÄTEBILDTYPEN
  - ♦ ◊ Vergleichen Sie die verschiedenen Arten von Extraktionen, die mit den GrayKey-Geräten erstellt werden können, und erfahren Sie, was die Prüfer bei jeder Art von Extraktion erwarten können und wie diese Informationen auf vielfältige Weise zu weiteren Untersuchungen beitragen können.
  - ◊ Lernen Sie, wie Sie die wichtigsten Artefakte in diesen verschiedenen Bildtypen untersuchen können, die es nur bei der GrayKey-Datenextraktion gibt, und wie Sie Methoden entwickeln können, um einen effizienteren Passcode zu knacken.

- ♦ MODUL 5: DATENIMPORT IN MAGNET AXIOM
  - ♦ ◊ Verstehen Sie die verschiedenen Möglichkeiten der Datenübernahme und entwickeln Sie einen geeigneten Arbeitsablauf für die Übernahme von Informationen aus GrayKey-Extraktionen.
  - ◊ Lernen Sie verschiedene AXIOM-Funktionen kennen, z.B. den Dynamic App Finder, die Suche nach benutzerdefinierten Dateien nach Typ und wie Sie sichere Messaging-Anwendungen anvisieren.

- ♦ MODUL 6: ERKUNDEN VON ARTEFAKTEN IN MAGNET AXIOM
  - ♦ ◊ Erforschen Sie mehrere Artefakte, einschließlich eines tiefen Eintauchens in Artefakte, die für das iOS-Dateisystem von zentraler Bedeutung sind - Kernartefakte werden eingehend erforscht, einschließlich Techniken zur Wiederherstellung gelöschter Informationen aus diesen Datenbanken.
  - ◊ Fortgeschrittene Dateisystem-Artefakte wie PowerLog und KnowledgeC werden behandelt, um über Anwendungsnutzungszeiten und Datenmengen zu sprechen. Diese und andere Artefakte werden untersucht, um den Prüfern zu zeigen, wie sie nachverfolgen können, wann Ziele in einem bestimmten Zeitrahmen physisch mit einem Gerät interagieren.
  - ◊ Exklusive Artefakte des Dateisystems wie der Speicherortverlauf, Anwendungen von Drittanbietern und vieles mehr werden ebenfalls erforscht.
  - ♦ ◊