AX250 Magnet AXIOM Advanced Computer Forensics

Kurzbeschreibung:

Magnet AXIOM Advanced Computer Forensics (AX250) ist ein viertägiger Fortgeschrittenenkurs für Teilnehmende, die mit den Grundsätzen der digitalen Forensik vertraut sind und mit Magnet AXIOM, Magnet RAM Capture und Tools von Drittanbietern die Effizienz ihrer Computerermittlungen steigern möchten.

Zielgruppe:

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

Voraussetzungen:

Da es sich bei diesem Kurs um einen Kurs auf Expertenebene handelt, wird empfohlen, zunächst die Magnet AXIOM-Prüfungen (AX200) zu absolvieren.

Sonstiges:

Dauer: 4 Tage

Preis: 2815 Euro plus Mwst.

Ziele:

Dieser Kurs vermittelt den Teilnehmenden Kenntnisse zu den neuesten Anmeldetechnologien wie z. B. PIN-Passwörtern, Windows Hello, grafischen Passwörtern, Fingerabdrucklesern und Gesichtserkennung die nötigen Kenntnisse und Kompetenzen, um Computerzugriff und Dateinutzung nachzuverfolgen und die Beweismittel dabei mit Magnet AXIOM noch tiefgreifender als bisher zu untersuchen. In diesem Kurs wird Ihr Verständnis der Untersuchungen auf Windows-Computern vertieft, indem Artefakte, wie zum Beispiel Windows-Benachrichtigungen, die Nutzung von Windows-Systemressourcen, WER-Protokolle (Windows Error Reporting), Ereignisprotokolle (EVT) und ETL-Protokolle (Event Tracing Logs), durchsucht werden. Außerdem wird die Taskleiste und die Frage behandelt, wann ein Artefakt dort vom System und wann von Benutzern angeheftet wurde.

Inhalte/Agenda:

- ♦ ÜBERBLICK ÜBER WINDOWS 10
  - ♦ ◊ Die Teilnehmenden machen sich mit den Gründen, aus denen Microsoft Windows 10 als letzte Windows-Version bezeichnet hat, die jemals auf den Markt kommen wird, und der Wirkung vertraut, die dies auf die Forensik hat und weiter haben wird. Darüber hinaus befasst sich dieses Modul mit den neuen Windows-Anmeldetechnologien, der Erstellung von Berichten über die Datenbank zur Nutzung von Systemressourcen und der Nachverfolgung der fortlaufenden Build-Nummern von untersuchten Windows-Systemen.

- ♦ EMDMgmt und Seriennummern von Speichermedien
  - ♦ ◊ In diesem Modul geht es um den Rückgriff auf weniger bekannte Speicherorte zur Nachverfolgung der Seriennummern von Speichermedien, zu denen das Windows-Betriebssystem Zugang hat.

- ♦ AUFFINDEN FEHLENDER AUSFÜHRBARER DATEIEN
  - ♦ ◊ Die Teilnehmenden lernen, wie sie mit dem Programmkompatibilitätsassistenten und AMCache-Daten die Nutzung ausführbarer Dateien und ihre Hashes auf dem betreffenden Computer nachverfolgen können.

- ♦ SHELLBAGS UNTER DER OBERFLÄCHE UNTERSUCHEN
  - ♦ ◊ In diesem Modul werden Shellbags behandelt – worum es sich dabei handelt und wie sie bei einer Ermittlung dazu dienen können, herauszufinden, ob ein(e) bestimmte(r) Nutzer(in) auf eine Datei oder einen Dateipfad zugegriffen hat.

- ♦ PREFETCH-DATEIEN UND DATENKORRELATIONEN
  - ♦ ◊ In diesem Modul befassen sich die Teilnehmenden eingehender mit Prefetch-Dateien um herauszufinden, welche Geheimnisse sie bergen und wie Windows sie speichert und löscht – so können sie bei Zeugenaussagen kenntnisreich und selbstbewusst auftreten.

- ♦ JUMP-LISTEN, WORUM ES SICH DABEI HANDELT UND WAS SIE UNS MITTEILEN
  - ♦ ◊ Jump-Listen zu verstehen, ist erst der Anfang. In dieser Lektion geht es darum, mithilfe der gewonnenen Daten Informationen zu vormals vorhandenen Laufwerken und den Dateien darauf, die nicht mehr Teil des Systems sind, in die richtigen Zusammenhänge zu setzen.

- ♦ ZULETZT GEÖFFNETE DOKUMENTE
  - ♦ ◊ Es ist äußerst wichtig, sich die Informationen in den zuletzt geöffneten Dokumenten zunutze zu machen und entsprechende Berichte zu erstellen. Noch wichtiger ist die Fähigkeit, diese Daten zu den Daten aus den vorherigen Lektionen in Beziehung zu setzen, um wichtige Informationen lückenlos über das gesamte System hinweg zu verfolgen und zu erkennen, wie und (wenn möglich) wann und wo auf die betreffenden Daten zugegriffen wurde.

- ♦ RAM-ERFASSUNG UND ANALYSE VON RAM-IMAGES
  - ♦ ◊ Die Erfassung des RAM ist von höchster Bedeutung, wenn der Computer eingeschaltet ist. Kein(e) Ermittler(in) würde einen Datenstick mit 16 GB oder 32 GB am Durchsuchungsort zurücklassen, und ebenso wenig wird er/ sie auf die RAM-Erfassung verzichten. In dieser Lektion geht es um die RAM-Erfassung und darum, wo und warum sie wichtig ist.

- ♦ GERÄTEÜBERGREIFENDE FREIGABE VON DATEIEN, ORDNERN UND EINSTELLUNGEN
  - ♦ ◊ Microsoft ermöglicht die problemlose Freigabe von Dateien (mit OneDrive) und anderen Einstellungen (über das E-Mail-Konto von Microsoft). Mit der Sync-Technologie können Sie feststellen, wann Daten zum ersten bzw. letzten Mal für andere Geräte freigegeben wurden. Die Einstellungen von einem Windows-System können mit anderen Windows-Systemen geteilt werden. Dies gilt auch für WLAN-Profile und gelöschte Profile. In diesem Modul verschaffen sich die Teilnehmenden mit Passware und dem gesicherten RAM aus dem vorherigen Modul Zugriff auf den Truecrypt-Container und seinen Inhalt.

- ♦ MIT PASSWARE DAS PASSWORT DER ITUNES-SICHERUNG KNACKEN
  - ♦ ◊ Die Teilnehmenden frischen ihr Wissen über iOS-Sicherungen auf, verschaffen sich mit Passware und dem Wortlistengenerator von AXIOM (AWG) Zugang zur iOS-Sicherung und rufen dort das Passwort ab. Dieses verwenden sie dann, um auf die Keychain-Daten zuzugreifen und nicht nur die Passwörter einzusehen, die die verdächtige Person für angeschlossene WLAN-Geräte verwendet hat, sondern auch die anderen Passwörter in der iOS-Keychain.

- ♦ PASSWÖRTER FÜR WINDOWS 10 KNACKEN
  - ♦ ◊ In diesem Modul extrahieren die Teilnehmenden mit AXIOM, dem Wortlistengenerator von AXIOM und einer Softwarekombination das Passwort für Windows 10 aus dem SAM-Hive, indem sie sich den im System-Hive

gespeicherten Algorithmus zunutze machen.

- GOOGLE DRIVE ZUM LOKALEN SYSTEM ZURÜCKVERFOLGEN
  - Google Drive verwendet ein Programm mit der passenden Bezeichnung „Backup and Sync“, das eine Reihe von forensischen Artefakten hinterlässt. Die Teilnehmer werden damit forensische Artefakte wiederherstellen, die sich auf das Hoch- und Herunterladen von Dateien von einem bzw. auf ein bestimmtes Computersystem beziehen.

- WINDOWS FILE HISTORY UND WAS SICH DARAUS ABLESEN LÄSST
  - File History ist nicht mit Volume Shadow Service zu verwechseln. Es handelt sich dabei um ein Windows-10-Programm, das regelmäßig Versionen der Dateien in den Ordnern „Dokumente“, „Musik“, „Bilder“, „Videos“ und „Desktop“ und der offline auf dem PC verfügbaren OneDrive-Dateien sichert. Bei Abschluss dieses Moduls sind die Teilnehmenden in der Lage, den Dateiverlauf zu ermitteln.

- MODERN APPS (APPS AUS DEM WINDOWS STORE) UNTERSUCHEN – ÜBERBLICK
  - Modern Apps sind auf Interaktivität ausgelegt. Der Fokus liegt auf dem Touchscreen, laufen aber auch auf normalen Desktop-Computern ohne Probleme. Durch die Beschäftigung mit Modern Apps lernen die Teilnehmer(innen), dass der Internetverlauf und der Cache für Modern Apps nicht dort gespeichert werden, wo ein(e) Ermittler(in) sie vermuten würde.

- BEI ERMITTLUNGEN AUS DEM USNJRL MAXIMALEN NUTZEN ZIEHEN
  - Das USN-Journal ist ein Protokoll der Änderungen an Dateien auf einem NTFS-Laufwerk. Bei diesen Änderungen kann es sich zum Beispiel um die Erstellung, Löschung oder Änderung von Dateien oder Verzeichnissen handeln. Die Teilnehmenden erfahren, wie sie das USNJrl untersuchen können, um forensische Artefakte zu erhalten, die ihnen bei der Ermittlung weiterhelfen.

- ZUSAMMENFASSENDE PRÜFUNGSÜBUNG
  - Zur Festigung der während des Kurses erzielten Lernerfolge wird den Teilnehmenden zum Abschluss ein Szenario für eine praktische Übung vorgelegt, die eine zusammenfassende Prüfung für alle Übungen darstellt, die in den einzelnen Modulen durchgeführt wurden.

-
  -