

Seminarziel

Die Teilnehmer des Seminars sollen am Ende in der Lage sein, für eine Aktion in einem Browser oder einer anderen Anwendung die charakteristischen und damit beweiskräftigen Spuren auf einem Computer herauszufinden.

Zielgruppe

- IT Sachverständige
- IT-Security Experten
- Privatermittler
- IT-Forensiker
- Datenschutzbeauftragte

Teilnahmevoraussetzung

Voraussetzungen sind Grundkenntnisse über Hard- und Software von Computern, Virtuelle Maschinen und ein Grundverständnis über die forensische Arbeitsweise von IT-Sachverständigen.

Für den praktischen Teil sollten die Teilnehmer einen Laptop dabei haben, auf dem das kostenlose Tool "Autolt" und der Browser "Safari" vorinstalliert ist.

Teilnahmezertifikat

Alle Seminarteilnehmer erhalten im Anschluss an die erfolgreiche Teilnahme ein Zertifikat des Schulungsveranstalters, welches z.B. als Weiterbildungsnachweis genutzt werden kann.

Noch Fragen?

Wir haben in der Kürze sicherlich nicht alle Ihre Fragen beantworten können.

Um offene Fragen zu klären, steht Ihnen unser Team per Email oder Telefon zur Verfügung.

Sachverständigen-Ausbildung

Datenschutz-Ausbildung

Energieberater-Ausbildung

Praxis-Schulungen

Sachverständigen-Software

Europaweite
Sachverständigenvermittlung

Zertifizierung nach
DIN EN ISO 9001:2015

Empfohlene Schulungsstätte
für das Sachverständigenwesen

AZAV - Zertifiziert

modal[®]

Sachverständigen
Ausbildungs- u. Kompetenz-Center

Rennekoven 9
41334 Nettetal

Fon: 02153 - 40984-0

Fax: 02153 - 40984-9

Web: www.modal.de

Email: info@modal.de

Stand 10/2017



Browser- und Anwendungsforensik

In der heutigen Zeit interagiert ein Nutzer mit dem Computer größtenteils über Anwendungsprogramme wie Browser, E-Mail-Clients oder Office-Produkten. Die dabei entstehenden Spuren auf der Festplatte oder im Speicher sind für Ermittlungen in der Regel hochgradig relevant. Für die Interpretation der Spuren ist allerdings ein tiefes Verständnis der Anwendungen selbst nötig. Im Rahmen einer eintägigen Lehrveranstaltung soll ein Überblick über Techniken und Werkzeuge zur Analyse von Spuren von Anwendungsprogrammen insbesondere Browsern vermittelt werden.

Seminaraufbau

Das Seminar besteht aus einem theoretischen und einem praktischen Teil, welche jeweils 3-4 Stunden dauern.

Theoretischer Teil

Der theoretischen Teil führt über drei Unterabschnitte von allgemeinen Betrachtungen zur konkreten Browserforensik. Als Einleitung werden zunächst wichtige Begriffe erläutert. Am Dijkstras "Guarded Commands" Modell werden die Begriffe Spuren, charakteristische Spuren und Kontras Spuren eingeführt, sowie die Beweiskraft dieser Spuren dargelegt.



Nachdem die Grundbegriffe klar sind, wird ein Überblick zu Spuren in verschiedenen Anwendungen und Dokumenten gegeben. Es wird erläutert, wie beweiskräftig derartige Spuren sind und wie leicht oder schwer sich diese manipulieren lassen. Hier wird es auch einen themenbezogenen Seitenblick auf die Mobilfunkforensik und die Multimediaforensik geben.

Beim Thema Browserforensik werden anhand von verschiedenen Browsern Spuren vorgestellt, die beim Internet-Surfen oder beim Download von Dateien auf den eigenen und fremden Rechnern entstehen können.

Ein Schwerpunkt ist die Frage, wie man herausfinden kann, was der Nutzer mit dem Browser gemacht hat. Dabei gibt es auch einen Seitenblick auf den "Private mode" der verschiedenen Browser. In einem anderen Schwerpunkt wird sich der Frage gewidmet, wie eindeutig Nutzer und Computer durch Spuren ihres Browsers auf Webservern identifiziert werden können.

Praktischer Teil

Im praktischen Teil wird für den Browser Safari vorgeführt, wie man charakteristische und damit beweiskräftige Spuren für bestimmte Handlungen mit dem Browser herausfindet. Hierzu gehören:

- Starten des Browsers
- die Wikipedia-Seite besuchen
- den Cache löschen
- den privaten Modus aktivieren

Geplant ist, dass die Dozentin die Untersuchung für die erste Aktion (Starten des Browsers) mit vorgefertigten Skripten und einer vorinstallierten Virtuellen Maschine vorführt und die charakteristischen Spuren für diese Aktion herausarbeitet. Die Teilnehmer haben dann die Möglichkeit, in drei Gruppen je ein Autolt-Script für eine der drei anderen Aktionen zu entwerfen und diese mit der Virtuellen Maschine der Dozentin zu testen. Hierfür ist es sinnvoll, dass die Teilnehmer eigene Laptops mitbringen, auf denen das kostenlose Tool Autolt und der Safari-Browser vorinstalliert sind (Eine Installation während des Seminars ist auch möglich).

Die Seminarteilnehmer werden in die Handhabung der Tools Autolt und Fiwalk eingearbeitet. Am Ende des Praktikums werden die Seminarteilnehmer in der Lage sein, für jede beliebige und auch unbekannte Anwendung die charakteristischen Spuren herauszufinden.

Teilnehmerzertifikat

Alle Seminarteilnehmer erhalten im Anschluss an die erfolgreiche Teilnahme ein Zertifikat des Schulungsveranstalters, welches z.B. als Weiterbildungsnachweis genutzt werden kann.

Anmeldeformular

Browser- und Anwendungsforensik

ANMELDUNG FÜR:

PREIS pro Teilnehmer:

MoBAF-001 Berlin*
25.09.2019

606,90 € inkl. MwSt.
(510,00 € netto + 96,90 € MwSt.)

* Seminare können im Großraum der genannten Orte stattfinden (+40 km)

FIRMA

NAME, VORNAME

STRASSE

PLZ, ORT

TELEFON

ORT/DATUM UND 1. UNTERSCHRIFT

Mit meiner zweiten Unterschrift bestätige ich den Erhalt und die Kenntnisnahme der "Allgemeinen Teilnahmebedingungen". Aus dieser Anmeldung entstehen keine weiteren Verpflichtungen über das Seminarende hinaus. Unsere Allgemeinen Teilnahmebedingungen für Seminare finden Sie unter: <http://www.modal.de/agb/>

ORT/DATUM UND 2. UNTERSCHRIFT

Sie erhalten eine Rechnung und Informationen zum Seminarablauf ca. 3 Wochen vor Seminarbeginn.

Anmeldeformular bitte per Post oder per Fax der modal gmbh + co. kg zukommen lassen.

modal gmbh & co. kg
rennekoven 9
41334 nettal

tel. 02153 / 40984-0
fax 02153 / 40984-9

info@modal.de
www.modal.de