Vorlesungsbeschreibung Wahlpflicht: Technische Aspekte der IT-Forensik

Lernergebnisse

Das Ziel dieser Lehrveranstaltung ist es, die Lernenden in die Lage zu versetzen, folgende Kenntnisse und Fertigkeiten zu erlangen:

- Erlernen IT-forensischer Vorgehensweisen und technischer Analysemethoden
- Durchführung IT-forensischer Untersuchungen am Beispiel zweier unterschiedlicher Filesysteme

Inhalte

Den Studierenden werden hierbei vertiefte Kenntnisse zu folgenden Themen vermittelt: Grundsätze und Anforderungen, speziell im internationalen Kontext und vor dem Hintergrund unterschiedlicher rechtlicher Situationen:

Datenträgeranalyse

- Übersicht Typen von Festplatten (SCSI, xATA, xIDE, etc.)
- Übersicht physische Aufteilung einer Platte (cylinder, head, sector)
- Übersicht logische Aufteilung einer Platte (partitions, raw data)
- Übersicht Dateisysteme (FAT, NTFS als Schwerpunkt, ggfls. ext2, ext3)
- Übersicht Dateiverwaltung (Cluster, slack space [drive slack, RAM slack])
- Details Festplattenanalyse (Sicherheitsmaßnahmen, tools, hands on)
- Dateien und ihre Eigenschaften (Metadaten)
- Arten von Dateien (normal, hidden, deleted, encrypted, alternate datastream, ...)
- string search (logisch vs. physisch, Kodierung)
- Details FAT
- Historische FAT-Systeme (FAT 12, FAT 16)
- FAT32 (Strukturen, Namenskonvention)

Betriebssystemanalyse

- Server vs. Workstation
- Lokation OS auf Platte
- Prozessanalyse
- Netzwerkverbindungen
- Registry
- NTFS (Metadaten und Details)
- Details Alternate Datastreams

- Details Filetypen
- Windows-Artefakte (cookies, temporary files, MRU, print jobs, ...)
- timelining
- Details Registry
- Email-Analyse

Netzwerkanalyse

- Grundlagen
- Protokolle
- Detail-Analyse
- Anomalien
- verdeckte Kommunikation
- Angriffstypen

Lehrmethoden

Vorlesung, Übungen in Kleingruppen.

Lehrsprache

Deutsch

Studien-/Prüfungsleistung

Hausarbeit

Credits

6
(180 h = 72 h Präsenz- und 108 h Eigenstudium)

Alle öffnen Alle schließen