Vorlesungsbeschreibung Wahlpflicht: Technische Aspekte der IT-Forensik

Lernergebnisse

Die Studierenden sind in der Lage, die Kenntnisse und Fertigkeiten zu IT-forensischer Vorgehensweisen und technischer Analysemethoden einzusetzen. Die Studierenden führen IT-forensische Untersuchungen am Beispiel zweier unterschiedlicher Filesysteme durch und können diese anwenden. Sie beherrschen die theoretischen Grundlagen, um diese kognitiv, intuitiv und kreativ in der Studienarbeit umzusetzen.

Inhalte

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

- 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)

    - timelining
    - Details Registry
    - Email-Analyse

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

Lehrmethoden

Vorlesung, Übungen in Kleingruppen.

Lehrsprache

Deutsch

Studien-/Prüfungsleistung

Hausarbeit

Alle öffnen Alle schließen