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)
  - 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 Computer F n er e , omputerstraftaten erk9

Studien-/Prüfungsleistung

Hausarbeit

Credits

3
(90 h = 30 h Präsenz- und 60 h Eigenstudium)

Literatur

- File System Forensic Analysis, Brian Carrier, Taschenbuch: 600 Seiten, Verlag: Addison-Wesley Longman, Amsterdam (17. März 2005), Sprache: Englisch, ISBN-10: 0321268172, ISBN-13: 978-0321268174
- Computer Forensik: Computerstraftaten erkennen, ermitteln, aufklären, Alexander Geschonneck, Broschiert: 342 Seiten, Verlag: dpunkt Verlag; Auflage: 4., aktualisierte ל ל c.

Alle öffnen Alle schließen