# IT Sicherheit

## 03 Forensiche Analysen

# IT Forensik Einführung

- Laut BSI:

„IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems.“

--> Strukturierter Prozess zur Untersuchung eines Vorfalls

# IT Forensik Einführung – Wichtige Fragestellungen

- Was ist geschehen?
- Wo ist es passiert?
- Wann ist es passiert?
- Wie ist es passiert?

- Wer hat es getan?
- Was kann gegen eine Wiederholung getan werden?

# IT Forensik Einführung - Prozess

1. Strategische Vorbereitung

   VORFALL

2. Operationale Vorbereitung
3. Datensammlung
4. Datenuntersuchung
5. Datenanalyse
6. Dokumentation

# IT Forensik Einführung - Prozess

Prozess wichtig, da an eine forensische Untersuchung Anforderungen an die Vorgehensweise gestellt werden:

- **Akzeptanz**

  Die angewandten Methoden und Schritte müssen in der Fachwelt beschrieben und allgemein akzeptiert worden sein. Der Einsatz neuer Verfahren und Methoden ist zwar prinzipiell nicht ausgeschlossen, jedoch sollte dann ein Nachweis der Korrektheit dieser erfolgen.
- **Glaubwürdigkeit**

  Die Robustheit und Funktionalität von Methoden wird gefordert und muss ggf. nachgewiesen werden.
- **Wiederholbarkeit**

  Die eingesetzten Hilfsmittel und Methoden müssen bei der Anwendung Dritter auf dem gleichen Ausgangsmaterial dieselben Ergebnisse liefern.
- **Integrität**

  Sichergestellte Spuren dürfen durch die Untersuchung nicht unbemerkt verändert worden sein. Die Sicherung der Integrität digitaler Beweise muss jederzeit belegbar sein.
- **Ursache und Auswirkungen**

  Durch die Auswahl der Methoden muss es möglich sein, logisch nachvollziehbare Verbindungen zwischen Ereignissen und Beweisspuren und evtl. auch an Personen herzustellen.
- **Dokumentation**

  Jeder Schritt des Ermittlungsprozesses muss angemessen dokumentiert werden.

# IT Forensik Einführung – Prozess im Detail

1. Strategische Vorbereitung

Alle Maßnahmen seitens des Anlagenbetreibers in Erwartung eines Vorfalls getroffen

Beispiele:

- Aktivierung von Logdiensten, welche in der Lage sind, die Umstände eines Vorfalls mitzuprotokollieren.
- Konfiguration einer einheitlichen korrekten Zeitbasis auf allen Geräten (RTC/NTP)

# IT Forensik Einführung – Prozess im Detail

2. Operationale Vorbereitung

Alle Maßnahmen welche zwar nach dem vermuteten Eintreten eines Vorfalls aber vor der eigentlichen Datensammlung erfolgen.

Beispiele:

- Identifikation und Enumeration potentieller Datenquellen (Netzwerkgeräte, Client-Geräte, Externe Geräte – Smartphones, Festplatten, …)

# IT Forensik Einführung – Prozess im Detail

3. Datensammlung

Sammlung aller für die Analyse notwendigen Daten

Beispiele:

- Erzeugung von Abbildern (so genannten Images) von Massenspeichern. Damit deren Bergung beweissicher geschieht, müssen sämtliche erzeugten Images mit kryptographischen Verfahren abgesichert werden, um die Integrität des Beweismittels sicherzustellen.

# IT Forensik Einführung – Prozess im Detail

4. Datenuntersuchung

Alle Maßnahmen, welche aus den gesammelten Daten zunächst allgemein forensisch wertvolle Daten extrahieren können.

Beispiele:

- Extraktion von Bilddateien aus dem Image einer Festplatte.

# IT Forensik Einführung – Prozess im Detail

5. Datenanalyse

Detailanalyse der gewonnenen Daten. Zeitliche Abläufe müssen plausibel und nachvollziehbar sein.

Beispiele:

- Maßnahmen, welche in der Lage sind, aufgrund von gefundenen Inhalten Verbindungen zwischen mehreren Daten herzustellen und evtl. auf die Urheberschaft zu schließen.
- Auswertung von Logdateien

# IT Forensik Einführung – Prozess im Detail

6. Dokumentation

Zusammenfassung aller gefundenen Ergebnisse und der durchgeführten Prozesse und angewandten Methoden.

Beispiele:

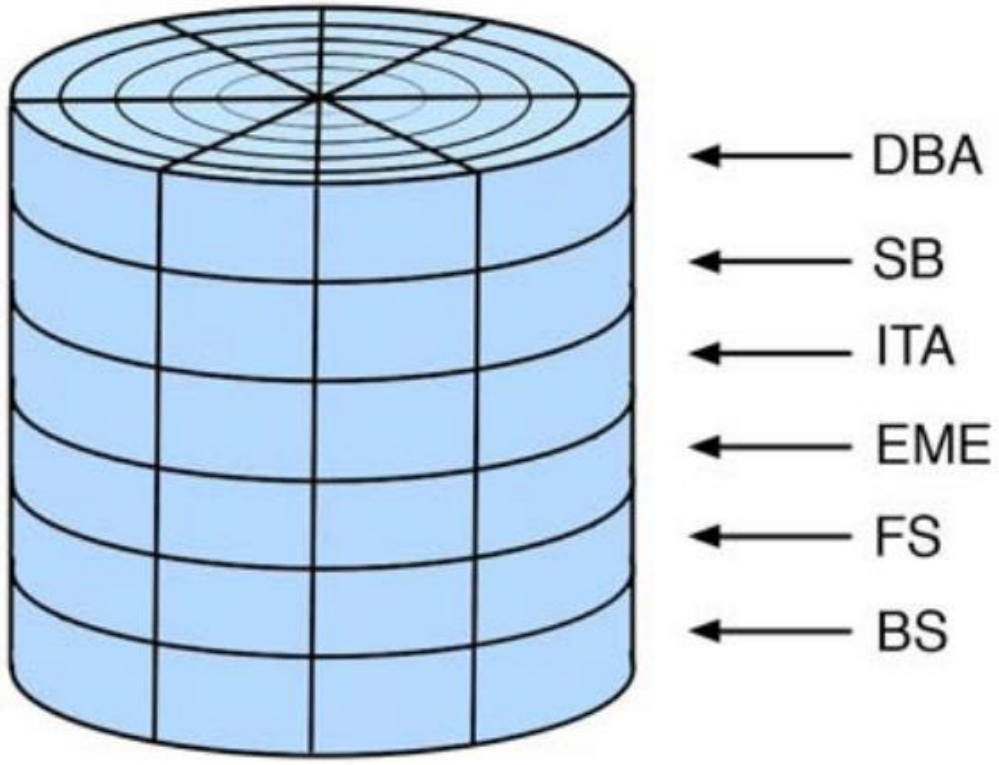
- Name und Versionsnummer des verwendeten Programms
- Kommandozeilenparameter des Aufrufs
- Forensische Absicherung dieses Werkzeugs, notfalls durch externe Schutzmechanismen wie Prüfsummen, Verschlüsselung, Signierung, Hardware-Schreibblocker oder andere Maßnahmen, die geeignet sind, Authentizität, Integrität oder Vertraulichkeit sicherzustellen
- Erfahrung des Untersuchenden mit diesem Werkzeug
- Motivation zur Auswahl dieses Werkzeugs

Ziel:

- Erstellung eines Gesamtbildes des Vorfalls
- Es Dritten ermöglichen, den angewandten Prozess nachzuvollziehen und damit abschätzen zu können, ob die gewonnen Erkenntnisse korrekt sind

# IT Forensik – Grundlegende Methoden

- Datenbearbeitung und Auswertung (DBA)
- Skalierung der Beweismöglichkeiten (SB)
- IT-Anwendung (ITA)
- Explizite Maßnahmen zur Einbruchserkennung (EME)
- Dateisystem (FS)
- Betriebssystem (BS)



# IT Forensik – Grundlegende Methoden

- Datenbearbeitung und Auswertung (DBA)

Werkzeuge, die im Zuge einer Untersuchung die relevanten Daten verarbeiten können (z.B. Logparser)

- Skalierung der Beweismöglichkeiten (SB)

Gruppe von Werkzeugen, welche erst im Zuge einer Untersuchung aktiviert werden, da im Normalbetrieb ein zu starker Einfluss vorherrscht (z.B. Aufzeichnung des kompletten Netzwerkverkehrs)

- IT-Anwendung (ITA)

Unterstützung der IT Forensik durch die Anwendungssoftware (z.B. Office-Suite, Webbrowser, …)

# IT Forensik – Grundlegende Methoden

- Explizite Maßnahmen zur Einbruchserkennung (EME)

Verwendung von Maßnahmen, welche im Zuge der strategischen Vorbereitung aktiviert wurden (z.B. IDS)

- Dateisystem (FS)

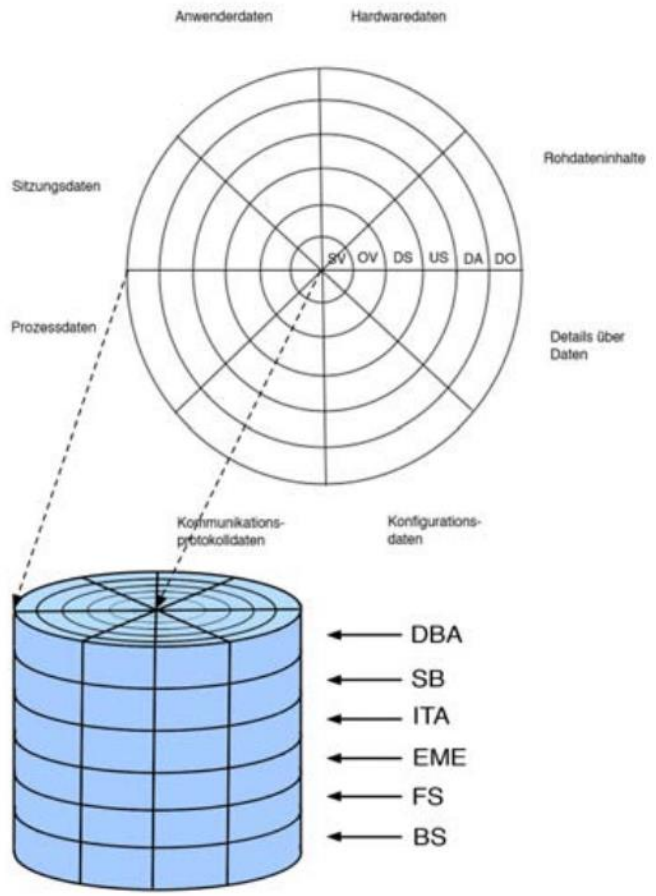
Die Möglichkeiten des verwendeten Dateisystems im Zuge der Forensik (z.B. Journaling, Schattenkopien, Versionierung)

- Betriebssystem (BS)

Die Möglichkeiten des verwendeten Betriebssystems im Zuge der Forensik (z.B. Windows Registry)

# IT Forensik – Detaillierte Vorgehensweise

- Details über Daten
- Konfigurationsdaten
- Kommunikationsprotokolldaten
- Prozessdaten
- Sitzungsdaten
- Anwenderdaten



# IT Forensik – Detaillierte Vorgehensweise

- Details über Daten

Daten über die eigentlichen Daten -> Metadaten (z.B. EXIF-Informationen eines Bild, Zeitstempel)

- Konfigurationsdaten

Daten, die das Verhalten des OS oder von Applikationen verändern (z.B. MySQL Konfiguration)

- Kommunikationsprotokolldaten

Kontrolle des Kommunikationsverhaltens von Systemen (extern) und Prozessen (intern) (z.B. netstat Information)

# IT Forensik – Detaillierte Vorgehensweise

- Prozessdaten

Beschreibung eines auf einem OS laufenden Prozesses (z.B.ID, Status, Besitzer, Priorität)

- Sitzungsdaten

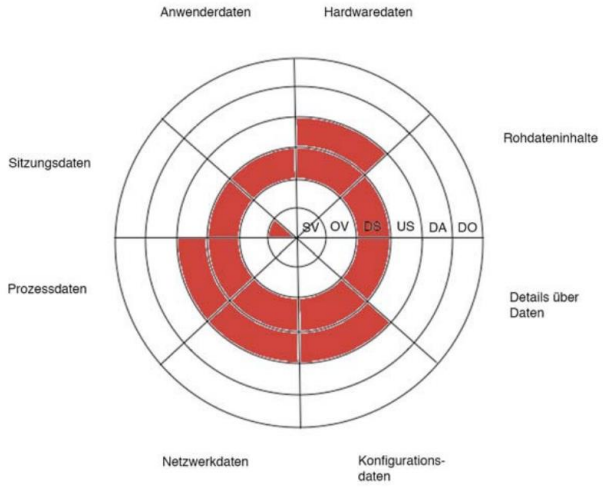
Vom OS, Anwendersoftware oder Benutzer im Zuge einer Sitzung gesammelte Informationen (z.B. Browser-Verlauf)

- Anwenderdaten

Vom Benutzer erstellte, bearbeitete oder gelöschte Daten (z.B. Bilder, Text-Dateien, …)

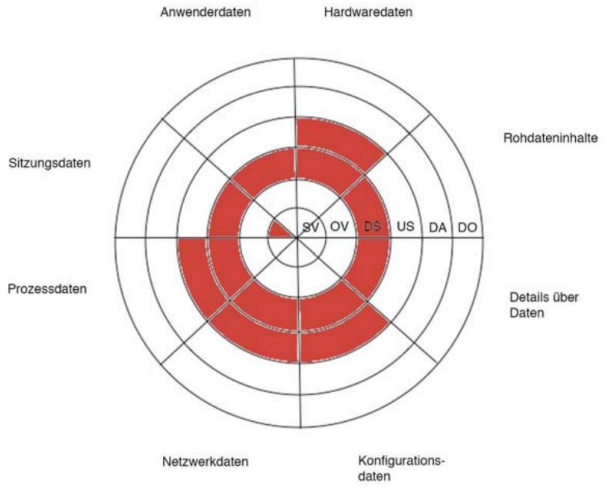
# IT Forensik – Beispiele für grundlegende Methoden

- Betriebssystem Windows
  - Strategische Vorbereitung
    - Aktivieren der Sicherheitsprotokollierung der Windows Firewall
    - Erzeugen von eigenen Ereigniskennungen und Ereignismeldungen
  - Operationale Vorbereitung
    - Ermitteln der Hardwarekomponenten
    - Versionsnummer von Windows



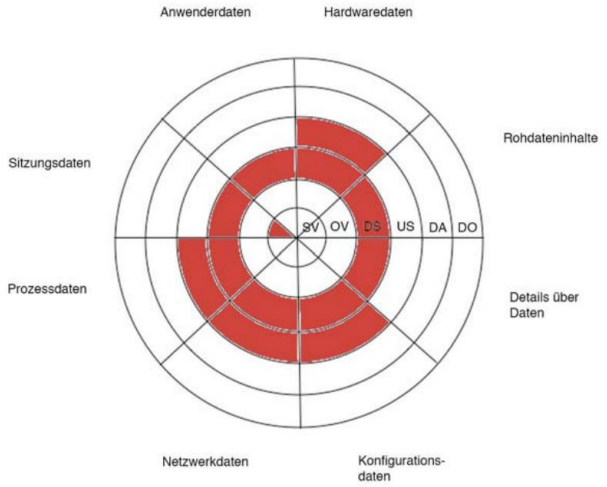
# IT Forensik – Beispiele für grundlegende Methoden

- Betriebssystem Windows
  - Datensammlung
    - Routen-Tabelle
    - ARP-Tabelle
    - MAC-Adresse
    - statistische Informationen der Netzwerkadapter
    - IP-Verbindungsinformationen
    - Domäneninformationen
    - Systemkonfiguration
    - verwendete Dateisysteme
    - Prozessinformationen
    - Informationen zu im System vorhandener Partitionen
    - Verlaufsdaten
    - Sitzungsdaten
    - Netzwerkfreigaben



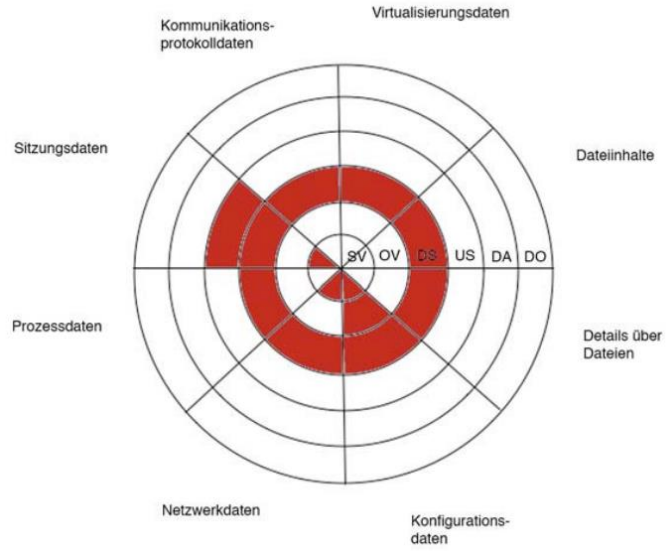
# IT Forensik – Beispiele für grundlegende Methoden

- Betriebssystem Windows
  - Untersuchung
    - Andere Computer im Netzwerk (MAC-Adresse)
    - Ordnerstruktur
    - Netzwerkumgebung



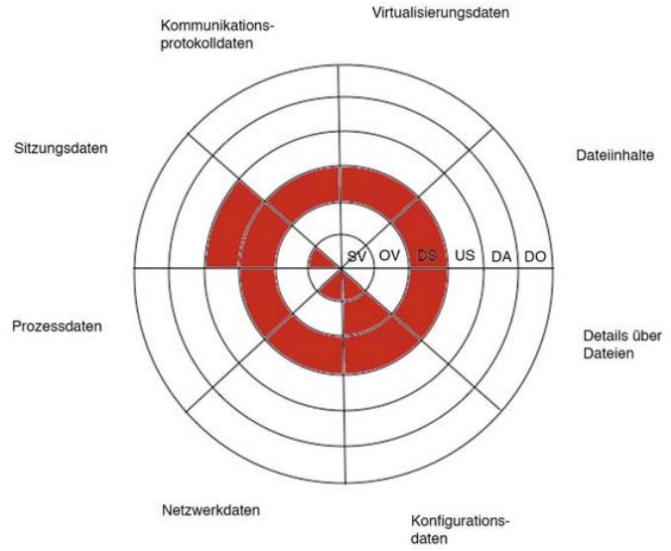
# IT Forensik – Beispiele für grundlegende Methoden

- Betriebssystem Linux
  - Strategische Vorbereitung
    - Aktivierung der Kernelkonfiguration zum Ablegen der Konfigurationsdaten
    - Anpassen der Größe des Speichers für die Kernel-Logs
    - Erstellung und Aktivierung des IP-Connectiontracking-Moduls
  - Operationale Vorbereitung
    - Liste der verwendeten Datei- und SWAP-Dateisysteme



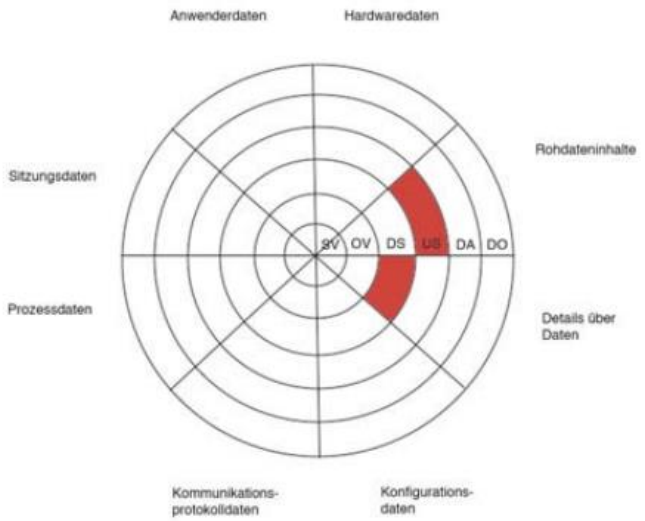
# IT Forensik – Beispiele für grundlegende Methoden

- Betriebssystem Linux
  - Datensammlung
    - Routen-Tabelle
    - ARP-Tabelle
    - MAC-Adresse
    - statistische Informationen der Netzwerkadapter
    - IP-Verbindungsinformationen
    - Systemkonfiguration
    - verwendete Dateisysteme
    - verwendete SWAP-Dateisysteme
    - Hauptspeicherinhalt
    - Prozessinformationen
    - Kernel-Log-Nachrichten
    - Informationen zu geladenen Kernelmodulen
    - Informationen zu im System vorhandener Partitionen
  - Untersuchung
    - Statistische Informationen zur Systemauslastung



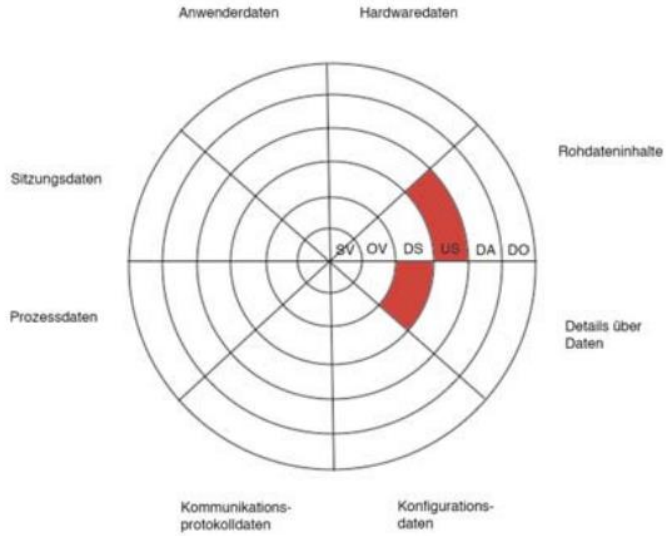
# IT Forensik – Beispiele für grundlegende Methoden

- Dateisystem NTFS
  - Datensammlung
    - Informationen des Master File Table
    - Mac-Zeiten
    - Control Lists
    - Alternate Data Streams
    - Partition Boot Sector
  - Untersuchung
    - Dateiwiederherstellung



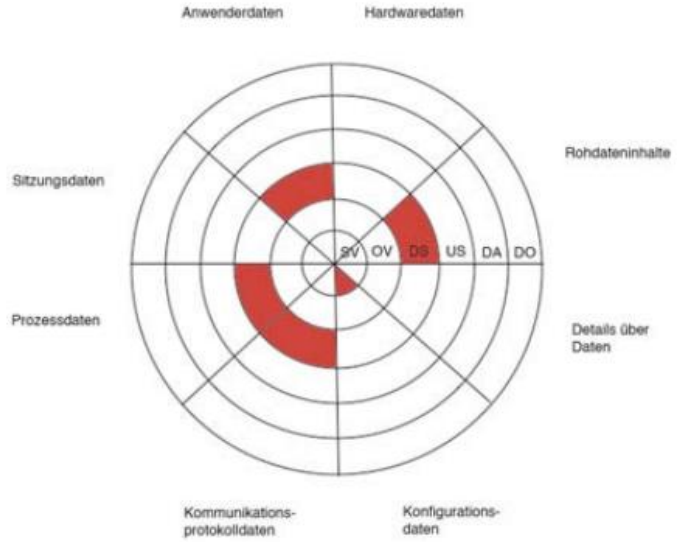
# IT Forensik – Beispiele für grundlegende Methoden

- Dateisystem FAT
  - Datensammlung
    - Daten über MAC-Zeiten
    - den FAT Root Folder
    - die FAT Folder Structure
    - den FAT Partition Boot Sector
    - das File Allocation System
    - das FAT Mirroring
  - Untersuchung
    - Dateiwiederherstellung



# IT Forensik – Beispiele für grundlegende Methoden

- Einbruchserkennung mit IDS oder on-access Virenscannern
  - Strategische Vorbereitung
    - Definition von IDS-Regeln
  - Datensammlung
    - IDS (z.B. Snort)
    - Antiviren-Software (z.B. AVGuard)



# IT Forensik – Beispiele für grundlegende Methoden

- IT-Anwendungen
  - Strategische Vorbereitung
    - Aktivierung MySQL-Slow-Query-Log
    - Aktivierung MySQLQuery-Log
    - Aktivierung des XChatLogs
  - Datensammlung
    - MySQL-Binlogs
    - MySQL-Prozesslogs
    - MySQL-Slow-QueryLog
    - MySQL-Query-Log
    - Xchat-Logs
    - XchatScrollbacklog
    - Logging der Bash CLI History
    - Microsoft Outlook
    - Mozilla Thunderbird
    - Logging des Webservers Apache
    - Mozilla Firefox
    - Microsoft DFS
    - Active Directory
    - eDirectory
    - OpenLDAP

# IT Forensik – Grundlegende Methoden

- Mit den grundlegenden Methoden der IT Forensik lassen sich:
- Alle Arten von Daten sammeln
- Alle Arten von Daten untersuchen
- Alle Arten von Daten dokumentieren

# IT Forensik – Softwareunterstützung

- Autopsy: https://www.autopsy.com/download/
  - https://thebinaryhick.blog/public_images/
  - https://www.forensicfocus.com/challenges-and-images/

# Network Forensik

- SYN Flooding
  - Überlastung eines Servers durch zu viele nicht abgeschlossene TCP-Handshakes
- ARP Spoofing
  - Fälschung von ARP Einträgen (=Mapping zwischen IP Adresse und MAC Adresse)
- SMTP
  - Einfaches, text-basiertes Protokoll für den E-Mail Versand
- Chrome History Database
  - SQLite Datenbank