

# IT Sicherheit: IT-Forensik

Dr. Christian Rathgeb

Hochschule Darmstadt, ATHENE, da/sec Security Group

17.06.2020

## Forensik

Forensik ist ein Sammelbegriff für wissenschaftliche und technische Arbeitsgebiete, in denen “Spuren” systematisch untersucht werden um strafbare bzw. anderweitig rechtswidrige oder sozialschädliche Handlungen nachzuweisen und aufzuklären.

Etymologie:

- ▶ Forum = Marktplatz (im antiken Rom).
- ▶ Auf Forum fanden Gerichtsverhandlungen statt.
- ▶ Beantwortung der Rechtsfragen im öffentlichen Raum.

## Spur

Spuren im forensischen Sinne sind hinterlassene Zeichen welche als Ausgangspunkt für eine Untersuchung dienen (z.B. Fingerabdruck)

Arten von Spuren:

- ▶ Materielle: Blutspritzer, Fingerabdrücke, Schuhabdruck, Haar.
- ▶ Immaterielle: Menschliches Verhalten (z.B. Unsicherheit).
- ▶ Im Kontext von IT-Forensik: digitale Spuren

## Indiz, Beweis

- ▶ Indiz: Hinweis, der alleine oder mit anderen Indizien zusammen auf das Vorliegen eines Sachverhalts schließen lässt (gewürdigte Spur)
- ▶ Beispiel: dieser Fußabdruck gehört mutmaßlich zum Schuh des Verdächtigen.
- ▶ Beweis: Feststellung eines Sachverhalts als Tatsache in einem Gerichtsverfahren aufgrund richterlicher Überzeugung (Juristische Wahrheit)
- ▶ Beispiel: dieser Fußabdruck gehört zum Schuh des Verdächtigen.
- ▶ Im Allgemeinen ist ein Indiz mehr als eine Behauptung, aber weniger als ein Beweis

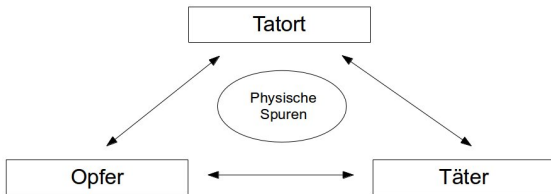
## Aufgaben der Forensik im Einzelnen

- ▶ Identifizieren, Sicherstellen, Selektieren und Analysieren von Spuren, die im weiteren Verlauf der Ermittlungen zu Indizien und Beweisen werden können.
- ▶ Dabei soll der Forensiker so wenig wie möglich in den Untersuchungsgegenstand eingreifen.
- ▶ Grundsätzlich gilt das Paradigma der **Integrität von Beweismitteln**.
- ▶ Beispiel der IT-Forensik: Unverändertheit einer zu untersuchenden Festplatte.
- ▶ Dabei stets Einhaltung der Sorgfaltskette (engl. **Chain of Custody**). Es muss immer klar dokumentiert sein, wer wann wie auf ein Beweisstück zugreifen kann.

## Das Locardsche Austauschprinzip

Locard's exchange principle:

- ▶ Jeder und alles am Tatort hinterlässt etwas und nimmt etwas mit (physische Spuren).
- ▶ Basis für die Suche nach Spuren (die immer existieren).



Spuren: Fingerabdrücke, Fußabdrücke, Schmauchspuren, Faserspuren, etc. sind oft die Hauptbelastungsbeweise für die Aufklärung zahlreicher Verbrechen.

## IT-Forensik

- ▶ Indizien, Spuren im Kontext eines IT-Systems (Computer, Smartphone, HDD, SSD, RAM, USB-Stick, SD-Karte, Router, Netzkabel, WLAN, Cloud, ...).
- ▶ Abstraktionsgrade:
  - ▶ Anwendungsebene: Applikationsdaten (z.B. sqlite, doc).
  - ▶ Dateisystemebene: Dateisystem (z.B. NTFS, ext3).
  - ▶ Datenträgerebene: Partitionen (z.B. DOS-Partitionen).
  - ▶ Bits und Bytes.
  - ▶ Physische Spur: Signal.

## Sieben W-Fragen der Kriminalistik

Typische Fragen im Zusammenhang mit einem Ermittlungsverfahren:

1. Wer? - Täter
2. Was? - Straftat
3. Wo? - Tatort
4. Wann? - Tatzeitpunkt
5. Womit? - Spuren (z.B. Waffe)
6. Wie? - Tathergang
7. Weshalb? - Motiv



## Anforderungen an IT-Forensik

1. **Akzeptanz:** Untersuchungsschritte und Methoden in der Fachwelt dokumentiert und anerkannt
2. **Glaubwürdigkeit:** Robustheit und Funktionalität der angewandten Methoden (Unterschied zu Akzeptanz?)
3. **Wiederholbarkeit:** Erneute Durchführung der forensischen Untersuchung erzielt dieselben Ergebnisse
4. **Integrität:** Digitalen Spuren bleiben unverändert
5. **Ursache und Auswirkungen:** Verbindungen zwischen Ereignissen, Spuren und evtl. auch Personen herstellen.
6. **Dokumentation:** Insbesondere Chain of Custody

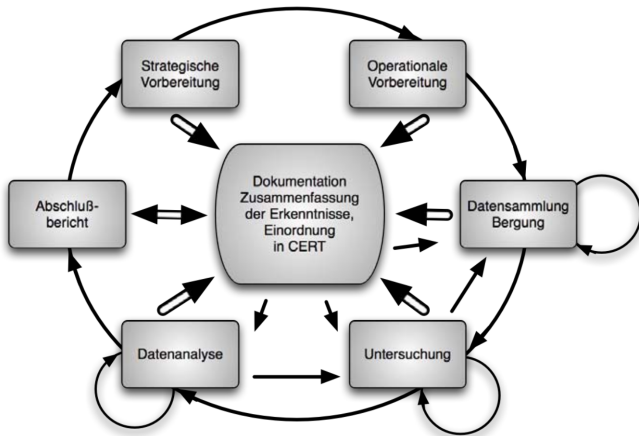
## SAP - Vorgehensmodell: Übersicht

- ▶ Das S-A-P Modell ist ein Modell zur Beschreibung der Vorgehensweise bei einer forensischen Untersuchung.
- ▶ Vorteil: Einfachheit
- 1. Secure: Identifizierung der Datenquellen, Datensicherung (zB: Erstellung von Kopien)
- 2. Analyse: Vorverarbeitung, Interpretierung
- 3. Present: Dokumentation, zielgruppenorientierte Präsentation

## BSI-Vorgehensmodell: Übersicht

- ▶ Das BSI (Bundesamt für Sicherheit in der Informationstechnik) untergliedert forensische Prozess in folgende Untersuchungsabschnitte (Phasen):
  1. strategische Vorbereitung;
  2. operationale Vorbereitung;
  3. Datensammlung;
  4. Untersuchung;
  5. Datenanalyse;
  6. Dokumentationeiner forensischen Untersuchung

## BSI-Vorgehensmodell: Übersicht



Quelle: Denise Muth, BSI

## BSI-Vorgehensmodell: Phase 1 + Phase 2

### 1. Strategische Vorbereitung:

- ▶ Vor Eintritt eines Zwischenfalls (Zwischenfall = Symptom).
- ▶ Bereitstellung von Datenquellen (z.B. Logs von Webdiensten, Verbindungsdaten von Routern).
- ▶ Einrichtung einer forensischen Workstation samt Zubehör (Tools, Write-Blocker, Kabel für Smartphones).
- ▶ Festlegung von Handlungsanweisungen (z.B. Rücksprache mit Juristen).

### 2. Operative Vorbereitung:

- ▶ Bestandsaufnahme vor Ort *nach* Eintritt eines Zwischenfalls.
- ▶ Festlegung des konkreten Ziels der Ermittlung.
- ▶ Festlegung der nutzbaren Datenquellen (Datenschutz beachten).

## BSI-Vorgehensmodell: Phase 3 + Phase 4

### 3. Datensammlung:

- ▶ Eigentlich: *Datenakquise* oder *Datensicherung*.
- ▶ Sicherung der im Rahmen der operativen Vorbereitung festgelegten Daten.
- ▶ Integrität der Datenträger sowie Vier-Augen-Prinzip berücksichtigen.
- ▶ Order of Volatility (Unbeständigkeit) bei der Datensicherung beachten (z.B. RAM zuerst).

### 4. Datenuntersuchung:

- ▶ Eigentlich: *Vorverarbeitung* für anschließende Analyse.
- ▶ Datenreduktion (irrelevant vs. relevant).
- ▶ Datenrekonstruktion (z.B. Dateiwiederherstellung).

## BSI-Vorgehensmodell: Phase 5 + Phase 6

### 5. Datenanalyse:

- ▶ Eigentliche Analyse der vorverarbeiteten Daten.
- ▶ Insbesondere Korrelation der Daten.

### 6. Dokumentation:

- ▶ *Verlaufsprotokoll*: Protokollierung aller Einzelschritte im Laufe der verschiedenen Ermittlungsphasen.
- ▶ *Ergebnisprotokoll*: Adaption des Verlaufsprotokolls für eine bestimmte Zielgruppe (z.B. Staatsanwalt, Geschäftsleitung, IT-Abteilung).
- ▶ Nutzung standardisierter Terminologie (CERT-Terminologie).

## BSI-Vorgehensmodell: Phase 6

- ▶ Der prozessbegleitende Dokumentationsprozess verläuft parallel zu der Durchführung der anderen Phasen.
- ▶ Seine Aufgabe ist das Protokollieren der gewonnenen Daten und durchgeführten Prozesse.
- ▶ Der prozessbegleitende Dokumentationsprozess zeichnet also auf, welche Daten beim Durchführen der einzelnen Methoden gewonnen wurden, protokolliert aber gleichzeitig auch Parameter der Durchführung selbst. Beispiele für diese Parameter sind.
- ▶ Beispiele: Name und Versionsnummer des verwendeten Programms, Motivation zur Auswahl dieses Programms, etc.



## Erstellung der Arbeitskopien



Quelle: Denise Muth

1. Paradigma: Original so selten wie möglich verwenden.
  - ▶ Einfach bei klassischen Datenträgern wie HDDs, SSDs, SD-Karten, USB-Sticks.
  - ▶ Schwierig(er) bei Smartphones, Hauptspeicher, Cloud
2. Verwendung von Schreibschutz (typischerweise Hardware-basierte Write-Blocker).

## Kurzabriss: Tools

1. The Sleuthkit (TSK):
  - ▶ Toolsammlung zur IT-forensischen Analyse von Datenträgern.
  - ▶ Autor: Brian Carrier.
  - ▶ Frontend (insbesondere für Windows): Autopsy.
  - ▶ Tools auf unterschiedlichen Abstraktionsebenen:
    - ▶ Dateisystemebene: `fls`, `ils`, `blkcat`.
    - ▶ Datenträgerebene: `mmls`.
2. `dd`: Datensicherung.
3. `sha256sum`: Berechnung von Hashwerten.

## Fallbeispiel: Sicherung externer HDD

```
# sha256sum /dev/sdb
6a5b9a759d56beb2c76f19462fdc8c361bede4fca1d01124ef36381842dc3921 /dev/sdb

# dd if=/dev/sdb of=mastercopy.dd bs=512

# dd if=mastercopy.dd of=workingcopy.dd bs=512

# sha256sum mastercopy.dd workingcopy.dd
6a5b9a759d56beb2c76f19462fdc8c361bede4fca1d01124ef36381842dc3921
mastercopy.dd

6a5b9a759d56beb2c76f19462fdc8c361bede4fca1d01124ef36381842dc3921
workingcopy.dd
```