HOCHSCHULE MITTWEIDA
University of Applied Sciences

Grundlagen Digitale Forensik

Forensische Prinzipien und Digitale Spuren

Prof. Dr. Dirk Labudde

Bundeskriminalamt

Forensische Prinzipien

Forensische Fragestellungen

Basic Forensic Mindset

- Wie geht man an forensische Fragestellungen heran?
- Welche Grundregeln sind zu beachten?
- Wie gehe ich **wissenschaftlich** vor?

Was wollen wir?

- **Wahrheit herausfinden**
- Genauer:
  - Was ist passiert?
  - Wo?
  - Wann?
  - Wie?
  - Wer?
  - Warum?

Forensische Prinzipien

- Effektivität einer Untersuchung hängt entscheidend von der **Objektivität der Ermittler** ab

- Ermittler beginnen sofort, Theorien über den Tathergang zu bilden
  - Jeder Fall ist jedoch neu und einzigartig!

- Wichtig sind Fakten, nicht Vermutungen

- Die „**Erfahrungsfalle**“:
  - Wenn ein neuer Fall ähnlich zu einem alten erscheint, ist man geneigt, den neuen mit den Mitteln anzugehen, die beim alten zum Erfolg führten [Casey, p 93]

Forensische Prinzipien

- Voreilige Theorien können dazu führen, dass bestimmte Spuren nicht mit der nötigen Sorgfalt untersucht oder falsch interpretiert werden

- Beispiel: gelöschte Datei mit Namen „#orn1yr5.gif“ mit nacktem Kleinkind
  - Bei der Dateiwiederherstellung könnte der Ermittler geneigt sein, den Originalnamen als „porn1yr.gif“ statt „born1yr5.gif“ zu wählen.
  - Besser: neutrales Zeichen verwenden _orn1yr5.gif
  - Dokumentieren, dass das erste Zeichen zerstört war

Forensische Prinzipien

- Grundannahme: **Jede Beobachtung** oder Analyse kann **Fehler** enthalten
- Der Versuch, eine Theorie zu bestätigen, erhöht die Chancen, Fehler zu machen
- Besserer Ansatz: viele Theorien entwickeln und versuchen, **Theorien zu widerlegen**
  - Schwerer, von einer Theorie eingenommen zu werden
  - Höhere Wahrscheinlichkeit, objektive Ergebnisse zu bekommen

- Grundsatz: **Such immer Fehler in Deinen eigenen Theorien**
- Wissenschaftstheorie von Karl Popper (1902-1994)
  - „… das einzige Kriterium für die Wissenschaftlichkeit eines Satzes ist seine prinzipielle Falsifizierbarkeit“

Forensische Prinzipien

- **Nichts Verändern**
  - Wissen, dass nichts verändert wurde, bedeutet lediglich, dass man nichts bewusst verändert hat
- Änderungen passieren schnell, z.B. durch
  - Booten eines Systems, mounten einer Festplatte, Is –IR, …
- Alles immer und überall nachweisbar machen
  - **Dokumentieren**

Transferprinzip

- Transfer-Prinzip
  - Wenn Kräfte auf ein Objekt einwirken, zerbricht dieses in (viele kleinere) Einzelteile
  - Diese Einzelteile gehen über auf dasjenige, was die Kraft ausübt bzw. auf den Ort, an dem die Kraftausübung passiert
  - Kriminelle Handlungen erfordern in der Regel Kraft
  - Aus den kleinen Spuren kann man auf die Art des originalen Objekts schließen bzw. das originale Objekt selbst
  - typische Veränderungen des Objekts lassen Rückschlüsse auf die Krafteinwirkung zu

Forensik – Zwei Pioniere

Hans Groß

Dr. Edmund Locard

Forensik – Zwei Pioniere

Objektive Befunde und Spuren sind neben den Aussagen von Beschuldigten und Zeugen die wichtigsten Beweismittel im Strafverfahren.

„Mit jedem Fortschritt der Criminalistik fällt der Wert der Zeugenaussagen, und es steigt die Bedeutung der realen Beweise.“

Hans Groß (1899) „Handbuch für den Untersuchungsrichter“

Forensik – Zwei Pioniere

Dr. Edmund Locard

Austauschprinzip:

„Jeder und alles am Tatort
nimmt etwas mit
und lässt etwas zurück.“

- ✓ Grundprinzip und Eckpfeiler der Forensik
- ✓ Basis für jede Suche nach Spuren

Dokumentation

Automatische Doku

- Auf der Kommandozeile gibt es Toolunterstützung
  - Unix-Kommando `script` -- make typescript of terminal session

- Aus der Manual Page:

  script makes a typescript of everything printed on your terminal. It is useful for students who need a hardcopy record of an interactive session as proof of an assignment, as the typescript file can be printed out later with `lpr`(1).

  If the argument file is given, `script` saves all dialogue in file. If no file name is given, the typescript is saved in the file `typescript`.

Jedoch ist eine eigene per Hand (auf Papier) durchgeführte Dokumentation verlässlicher !

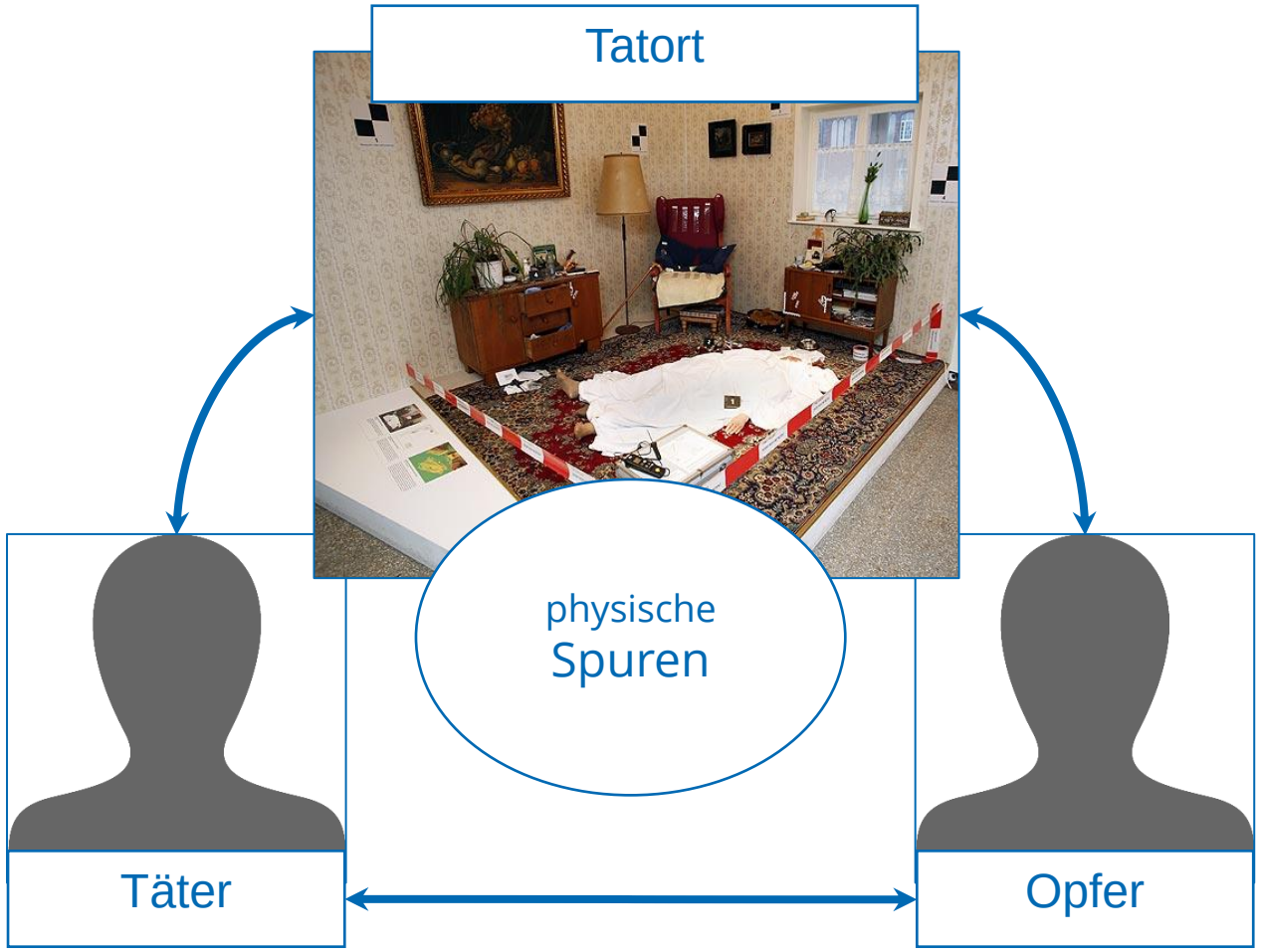
Dokumentation von Zeit

- Dokumentieren Sie, wann Sie Aktionen durchführen
- Notwendig bei automatischer Dokumentation:
  - Sorgen Sie für eine korrekte Zeit an Ihrem Arbeitsplatz (NTP)
  - Dokumentieren Sie dies
- Dokumentieren Sie auch die Zeit des Untersuchungsobjektes
  - Wichtig für die Interpretation von Zeitstempeln

Jedoch ist eine eigene per Hand (auf Papier) durchgeführte Dokumentation verlässlicher !

Spuren

Physikalische Spuren



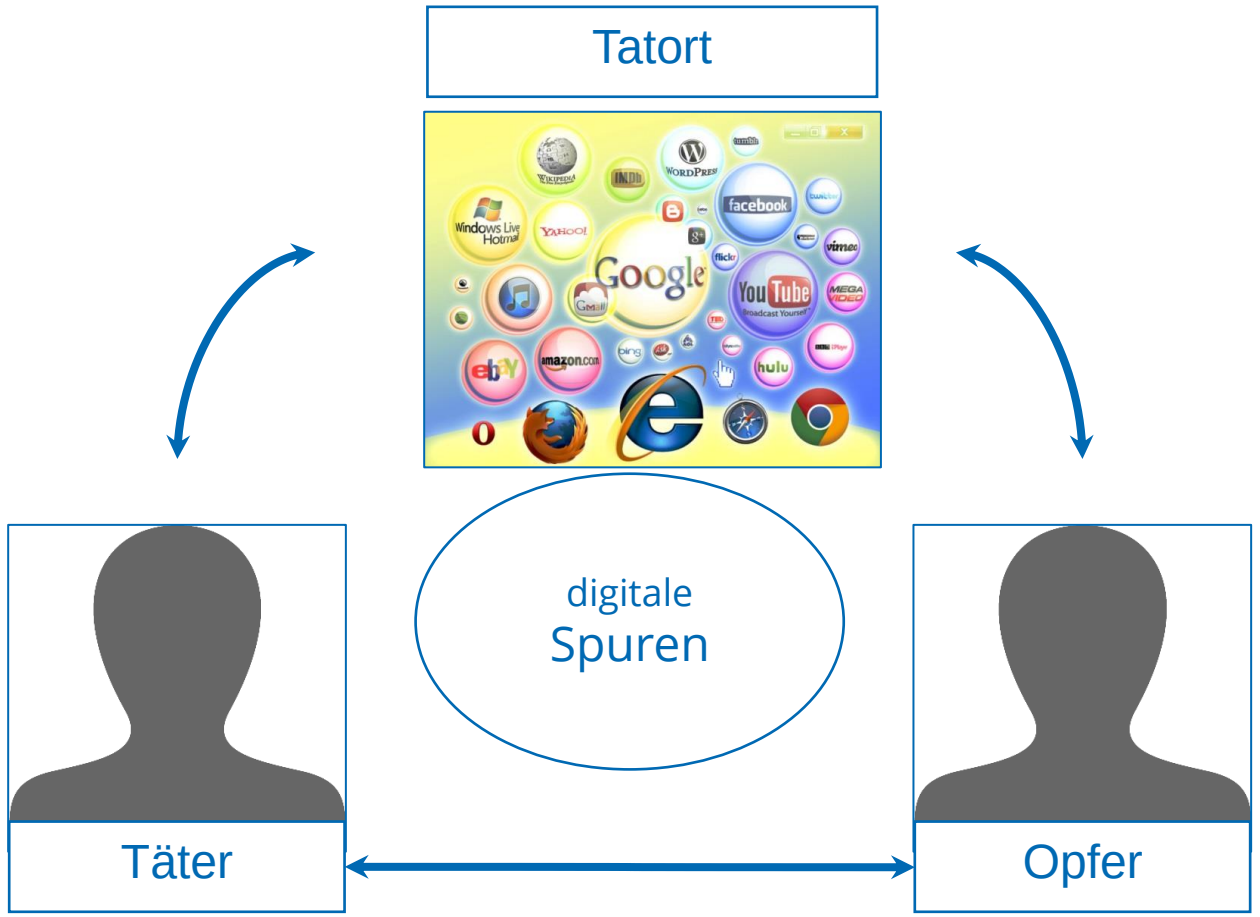
Physikalische Spuren

- alle materiellen Veränderungen an
  - Personen
  - Sachen
  - Objekten
- im Zusammenhang mit relevanten Ereignis
- tragen zur Tataufklärung bei
- Rückschlüsse auf
  - Tatablauf
  - Tatumstände
  - den / die Täter

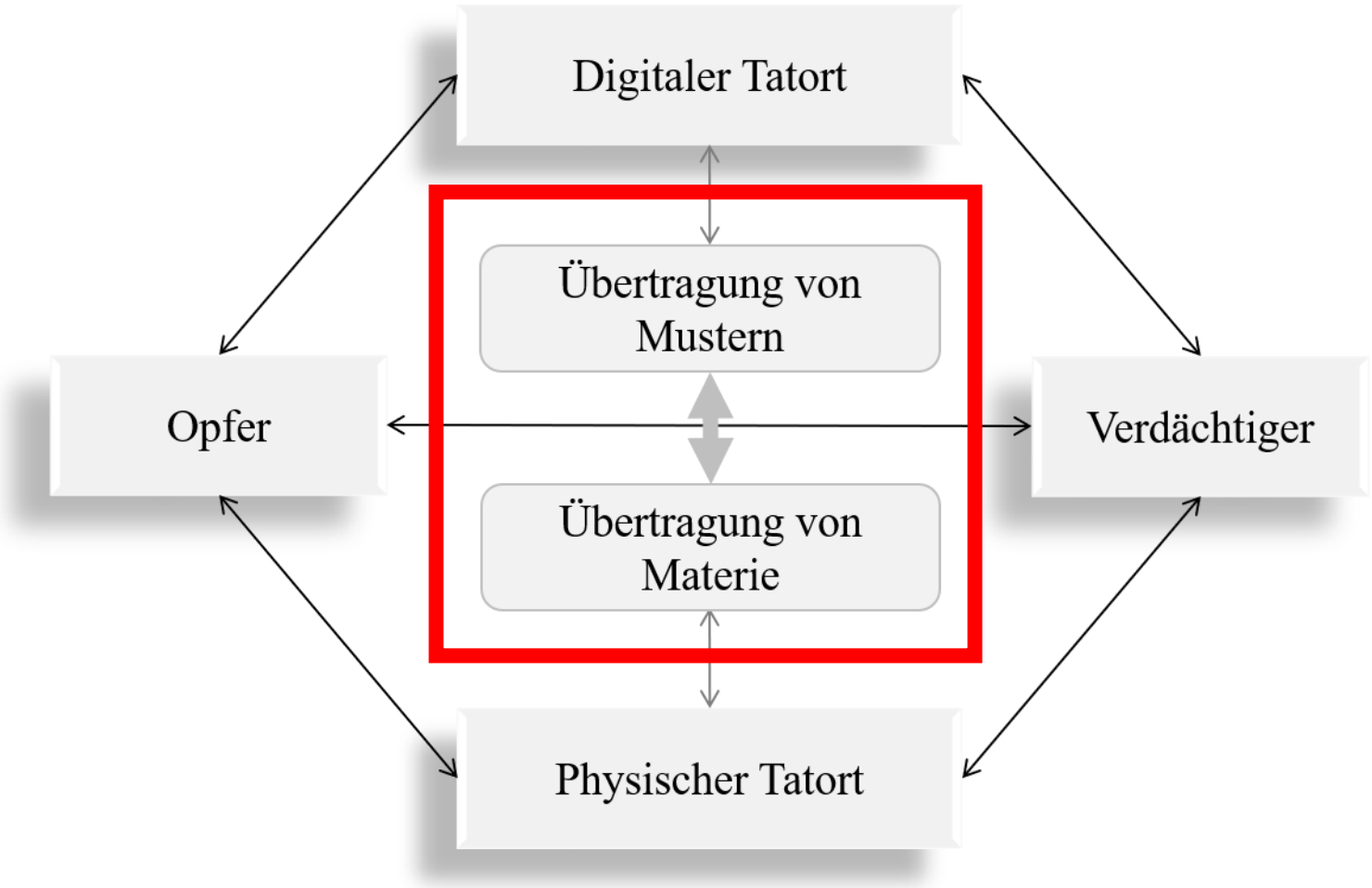
- objektive Informationspotential
- relativ beständig bis zur Begutachtung
- bestimmen Gegenstand der Spurenkunde
- Grundsätzlich gilt:

Es gibt keinen Tatort ohne Spuren!

Digitale Spuren



Übertragung von Muster und Materie



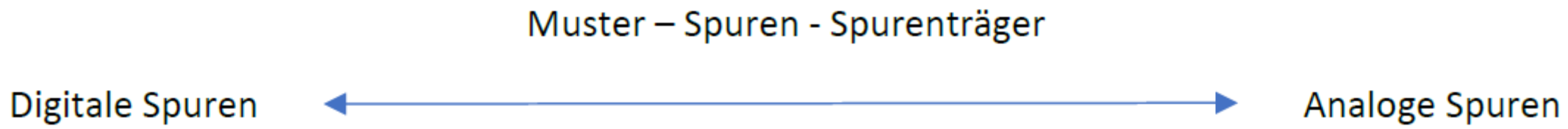
Übertragung von Mustern und Materie

1. Übertragung von Materie (physical transfer): Hierbei geht man in der Regel davon aus, dass sich unter einer gewissen Energieeinwirkung ein Objekt zerteilt und Einzelteile davon von einer Quelle auf ein Ziel übertragen werden. Typischerweise fällt die Energie beim Kontakt an.

2. Übertragung von Mustern (transfer of traits): Hierbei werden charakteristische Formeigenschaften von einem Objekt auf ein anderes übertragen, ohne dass notwendigerweise Materie ausgetauscht wird.

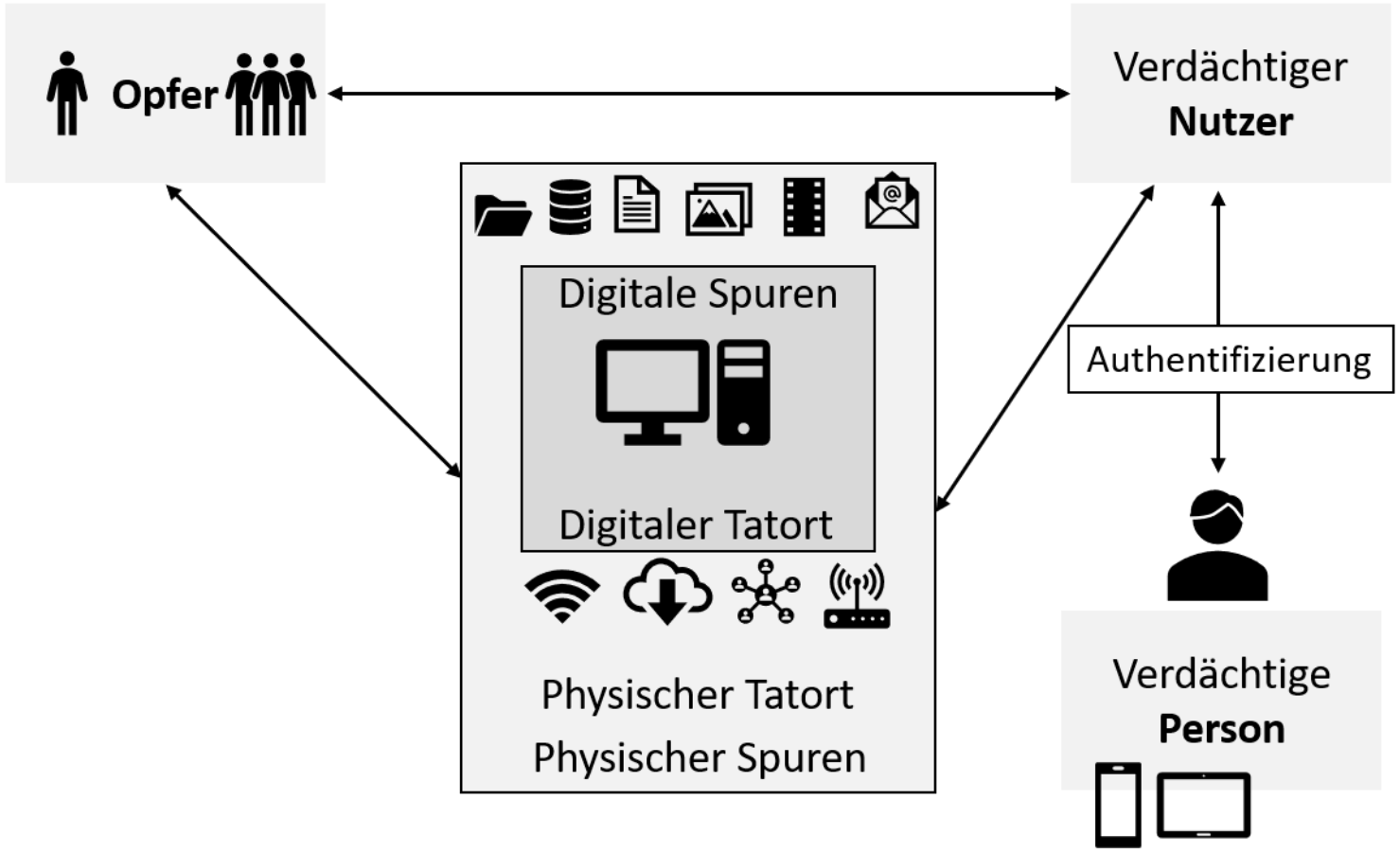
- Wenn Materie übertragen wird, ist die Zerteilung eine notwendige Voraussetzung
- Wenn Muster übertragen werden - **nicht**

Übertragung von Mustern und Materie



Jede Straftat/kriminelles Ereignis ist ein Ereignis in Raum und Zeit. Alles was für die analogen Spuren gelernt wurde lässt sich auch auf die digitalen Spuren anwenden.

Digitale Spuren



Digitale Spuren

- Digitale Spuren basieren auf Daten
- in Computersystemen gespeichert
- zwischen Computersystemen übertragen
- digitale Spuren ≠ materiellen Spuren
- digitale Spuren = materielle Spuren + Interpretation
- Beispiel:
  - Festplatte = materielle Spur
  - Interpretation mit Tools
  - Fotos, Kalender, E-Mails, ... = digitale Spur

Digitale Spuren

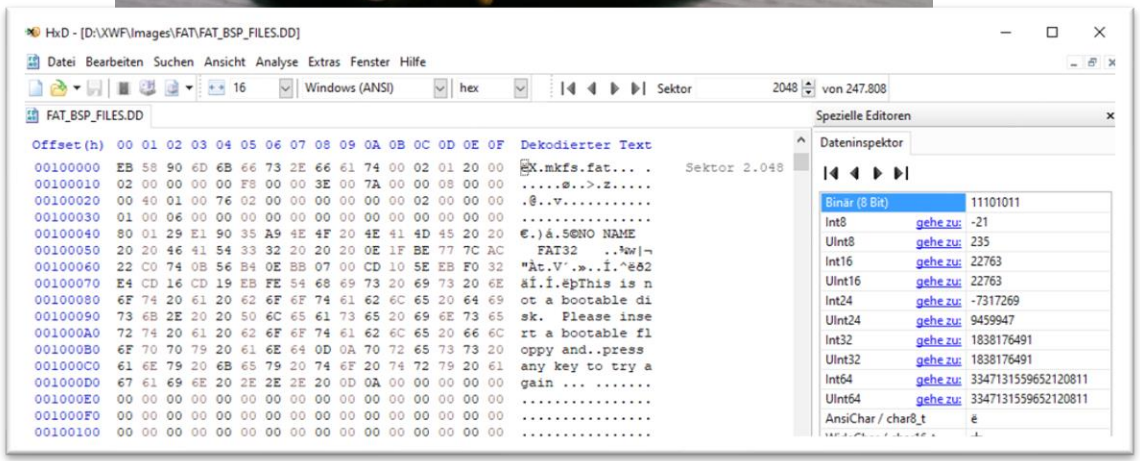
Digitale Spuren (digital evidence) sind Spuren, die auf Daten basieren, welche in Computersystemen gespeichert oder übertragen worden sind.

Digitale Spuren

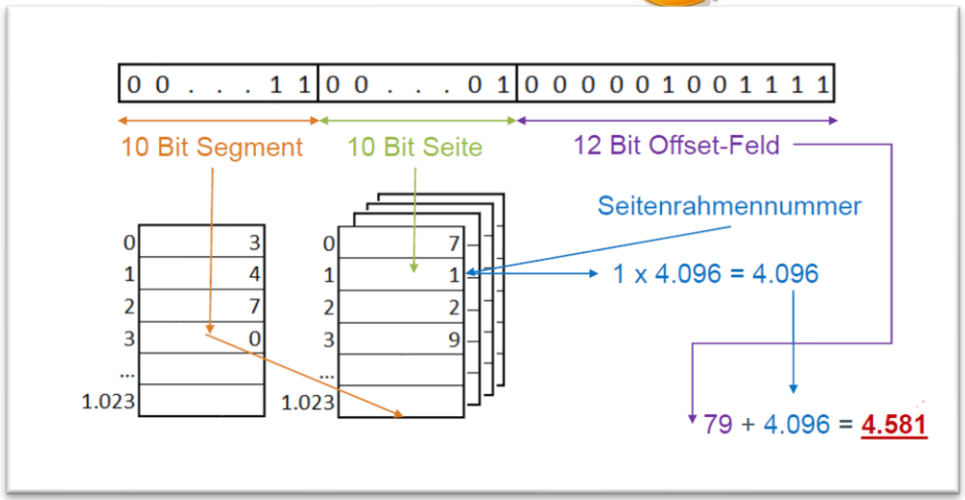
- IT Forensiker benötigt Kenntnisse über
  - Funktion der unterschiedlichen Dateisysteme
  - Arbeitsweisen von Betriebssystemen
  - verwendete Softwareprodukte
    - Software in Business- und Privatumfeld
    - Eigene Analysetools (Limit, Anwendungsbereich)
- Ziel
  - beweiserhebliche digitale Spuren ermitteln
  - korrekte Bewertung der digitalen Spuren
- schnelle Einarbeitung in unbekannte Softwareprodukte unerlässlich

Ausblick

Grundlagen von Dateisystemen



Grundlagen der Betriebssysteme



Identität Analog und Digital

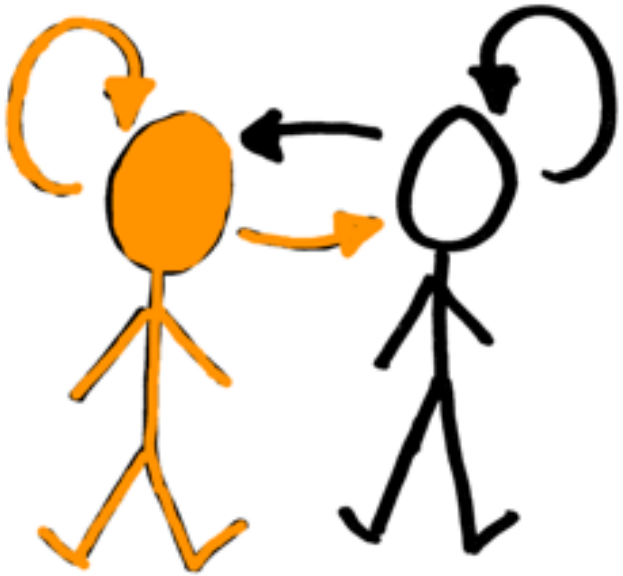
Gestalt & Verhalten

Merkmale
Identität
(Identifizierung)

Identität

- Leib / Leiblichkeit
- soziales Netzwerk / soziale Bezüge
- Arbeit und Leistung
- materielle Sicherheit
- Werte & Normen

Identität Analog und Digital



Reale Welt und digitale Welt

Moral – Anonymität – Umgang (mit anderen) –
Technische Entwicklungen - Kriminalität

Entstehung neuer Phänomenen

Am Ende hat immer ein Mensch (an einem anderen Menschen) die Straftat begangen.

Digitale Spuren

"On the Internet, nobody knows you're a dog."

Digitale Spuren

Digitale Spuren sind nicht personenbezogen!

- Spuren in der digitalen Welt sind zunächst getrennt von der physischen Welt.
- Zuordnung von Handlungen einer Person zu digitalen Spuren ist nur durch einen starken Authentifikationsmechanismus möglich
- Ausschließliche Beweisführung aufgrund von digitalen Spuren ist nicht durchführbar!
- Man benötigt immer andere (zusätzliche) Spuren oder Daten – **Vergleich!**

Digitale Spuren

Digitale Spuren (digital evidence) sind Spuren, die auf Daten basieren, welche in Computersystemen gespeichert oder übertragen worden sind.

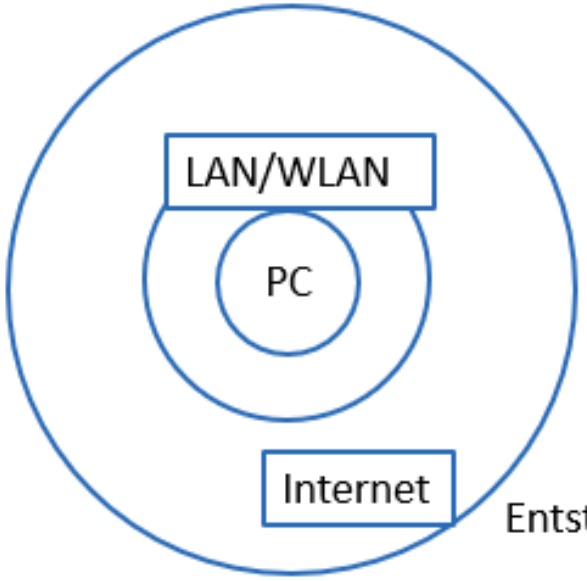
- zunächst physische Spuren
  - Magnetisierung auf der Oberfläche einer Festplatte,
  - elektromagnetische Wellen auf einem Datenkabel
  - Ladezustand von Speicherzellen im Hauptspeicher

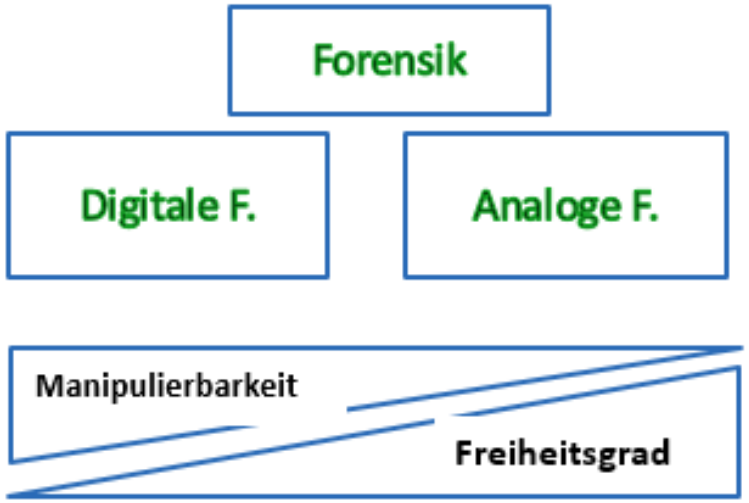
⇨ Prinzipien der klassischen Forensik anwendbar

- Diskrete Repräsentation
- Menschen nicht direkt zugänglichen Form
- zunächst extrahiert und in eine lesbare Form übersetzt werden

Eigenschaften Digitaler Spuren

- **Flüchtigkeit:**
  - Persistente – gespeicherte Daten
  - semi-persistente (Arbeitsspeicher)
  - flüchtige Spuren (nur temporär vorhanden)
- **Technische Vermeidbarkeit** (Systemdaten)
- **Manipulierbarkeit**
- **Kopierbarkeit**



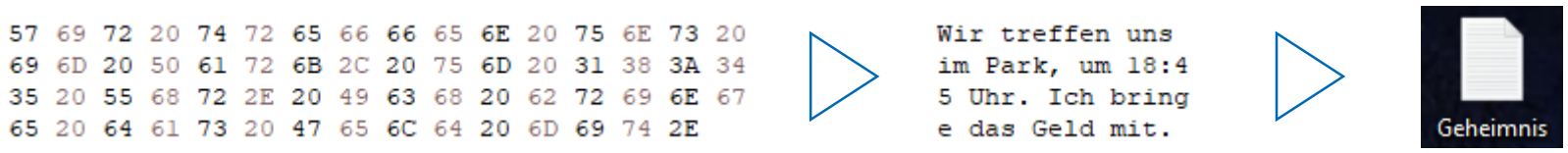


Entstehung: geographische Entfernung

Digitale Spuren und Abstraktion

- Digitale Spuren benötigen Werkzeuge zur Aufbereitung
- Werkzeuge zeigen nur eine Abstraktion/Interpretation der physischen Spuren
- Abstraktionen können mehrere Abstraktionsebenen enthalten
- Jede Abstraktionsebene kann Interpretationsfehler enthalten

1. Interpretation der Magnetisierung der Festplatte (Bits)
2. Interpretation der Bits durch eine Zeichenkodierung
3. Interpretation der Zeichen durch ein Dateisystem
4. Interpretation der Daten im Dateisystem als zusammengehörige Datei
5. Interpretation der Datei als E-Mail



Transfer Digitaler Spuren

- Transfer-Prinzip gilt in der digitalen Welt nur eingeschränkt
  - Was bedeutet es, dass „Kraft auf ein digitales Objekt einwirkt“?
  - Digitale Objekte können selbst „atomar“ (unzerteilbar) sein

- Beispiel „Löschen von Daten“:
  - Dateien bestehen aus vielen kleinen Festplattenblöcken
  - Löschen von Dateien hinterlässt Spuren
- Beispiel „Aufruf von Systembefehlen“
  - Aufruf hinterlässt Einträge in History- oder Log-Dateien
- Beispiel „Anstecken USB-Stick“
  - Hinterlässt Einträge zum Gerät und Ansteckzeiten

Eigenschaften Digitaler Spuren

- Man kann digitale Spuren **exakt Duplizieren**
  - Untersuchungen auf einer Kopie schonen das Original
  - Übereinstimmung des Originals mit der Kopie nachweisbar
- Manipulation können durch Vergleich mit einer Originalkopie nachgewiesen werden
- Digitale Spuren sind **schwer zu vernichten**
  - Auch gelöschte Dateien sind in der Regel noch lange Zeit auf der Festplatte rekonstruierbar
  - Notfalls Rückgriff auf physische Spuren (z.B. Festplattenmagnetisierung)

Manipulation Digitaler Spuren

- Digitale Spuren können **leicht manipuliert** werden
- Absichtlich, beispielsweise durch Straftäter oder auch Ermittler
- Unabsichtlich, beispielsweise durch Ermittler
- Manipulation hinterlässt theoretisch keine unmittelbar sichtbaren Zeichen

Heutige digitale Spurenlage

- Heutige Systeme sind sehr komplex
  - Verschiedene Betriebssysteme, verschiedene Versionen
  - Jedes System ist anders, keiner hat den kompletten Überblick
- Digitale Spuren entstehen heute überall
  - Es ist praktisch unmöglich, alle digitalen Spuren einer Straftat zu zerstören, die mit einem Computer verübt wurde
- Erfahrung zeigt: Locards Austauschprinzip gilt (mit gewissen Einschränkungen) auch in der digitalen Welt

Wo fallen Digitale Spuren an

- Browser-Caches
- Log-Dateien
- Backups
- Dateisystem (Zeitstempel, Swap Space, und an mindestens 32 weiteren Stellen)
- Digitale Überwachungskameras
- Geldautomaten
- Firewalls
- Virenscanner
- Temporäre Dateien
- Windows-Registry
- Browser-History
- RAM (Prozessliste, Netzwerkverbindungen, eingeloggte User)
- Wahlwiederholungsfunktion am Telefon
- Abrechnungsdaten des Mobilfunkanbieters
- Suchmaschinen
- ...

Wo fallen Digitale Spuren an

- Heizungssteuerungen
- Elektroherde
- Kühlschränke
- Türschlösser
- Videorecorder,
- Fernseher
- iPods
- Gameboys
- Videospielkonsolen
- DSL-Modems
- Autos (an mindestens 23 Stellen)
- Fotoapparate,
- Strom-/Wasser-/Heizungszähler
- Drucker
- Farbausdrucke
- Digitale Fotos (Multimediaforensik)
- ...

Analoge und Digitale Forensik

Analoge und Digitale Forensik

Kern der Kriminalistik ist die Wahrheitsforschung. *Kriminalisten* sind Wahrheitsforscher. Sie versuchen eine der Realität möglichst entsprechende "Aktenwahrheit" zu schaffen, die es möglich macht, einem Gericht gegenüber bestimmte Behauptungen beweisen zu können. Hierzu bedienen sie sich des Sach- und des Personalbeweises.

Grundlage hierfür bildet die Annahme, dass sich das *in der Vergangenheit* liegende, kriminalistisch relevante, aufzudeckende und zu untersuchende Ereignis als Ganzes in dem Milieu, in dem es sich ereignet, widerspiegelt.

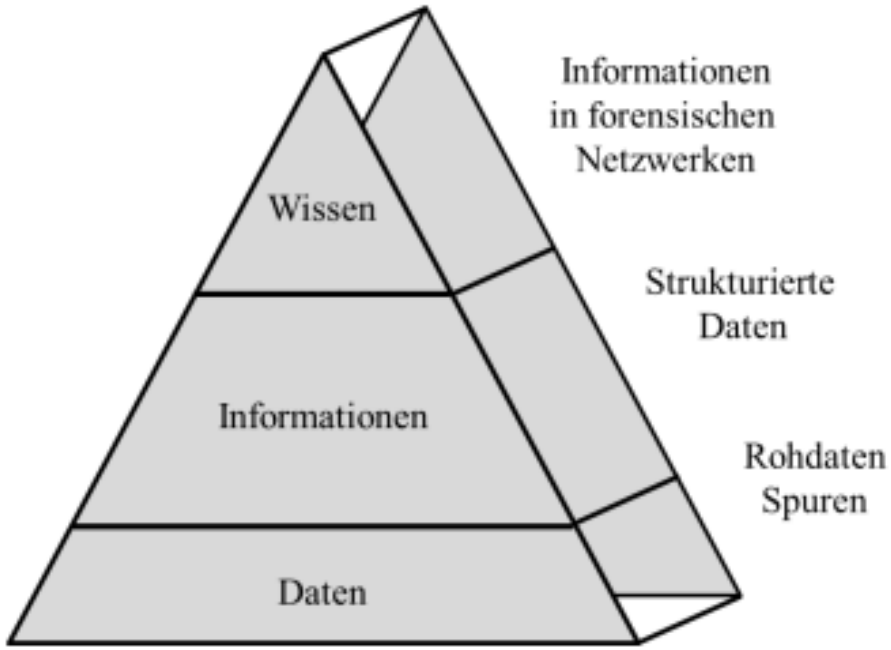
Die Wirkungen, die das zugrunde liegende Ereignis erzeugt, ergeben in ihrer Gesamtheit ein Bild des Ereignisses.

Analoge und Digitale Forensik

Die Kriminalistik befasst sich als Wissenschaft mit den strategischen, taktischen und technischen Mitteln und Methoden zur Aufdeckung, Untersuchung (Aufklärung) und Verhütung von Straftaten und kriminalistisch-relevanten Sachverhalten.

Sie befasst sich mit den Gesetzmäßigkeiten und Erscheinungen des **Entstehens von Informationen** bei der Begehung von Straftaten sowie die Methoden ihres Auffindens, Sicherns und Bewertens für Ermittlungs- und Beweiszwecke.

Analoge und Digitale Forensik



Systemverständnis

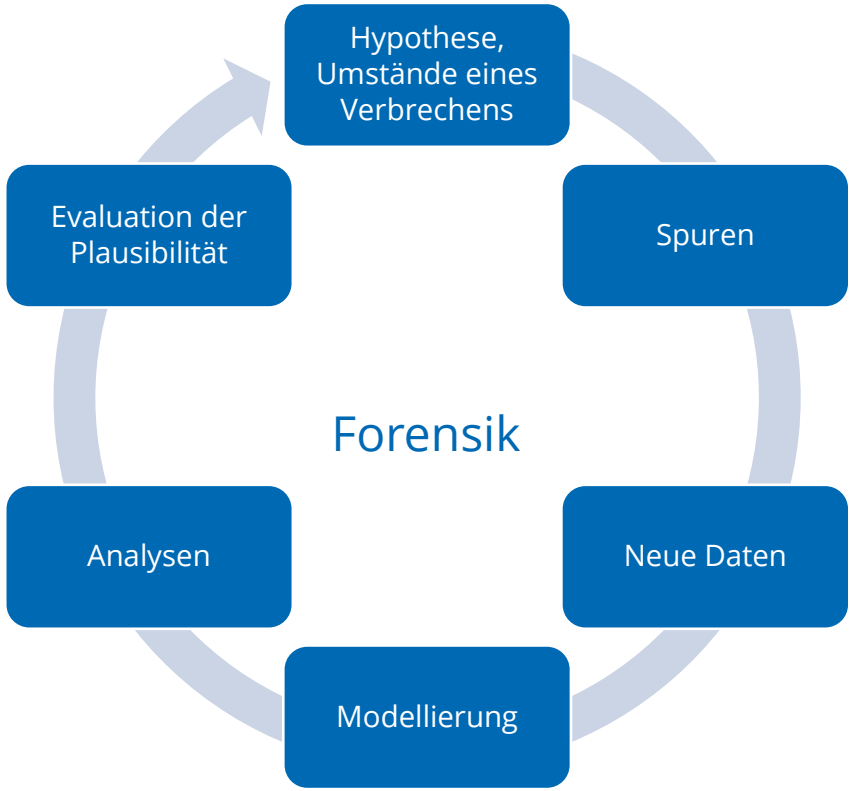
Zusammenhänge

Klassifizierung

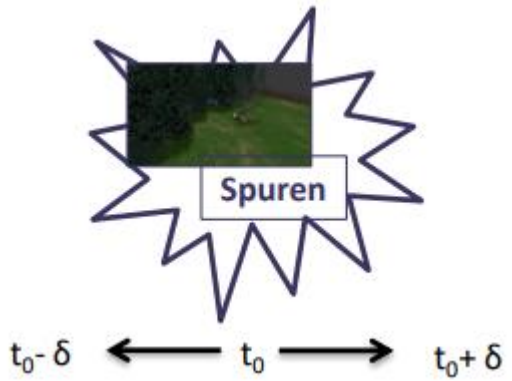
Daten

Analoge und Digitale Forensik

Analyse und Visualisierung aller Prozesse und Spuren – basierend auf einem einheitlichen Modell -

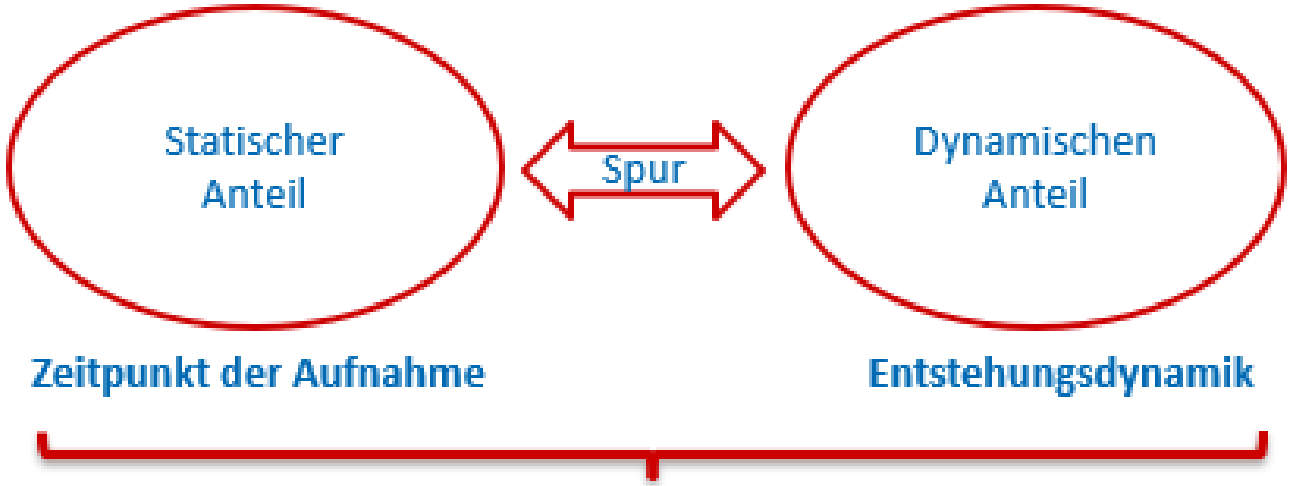


Physikalischer und zeitlicher Fokus



→ Spuren bekommen eine (neue) Bedeutung im Prozess der Rekonstruktion.

Statische und Dynamische Spur



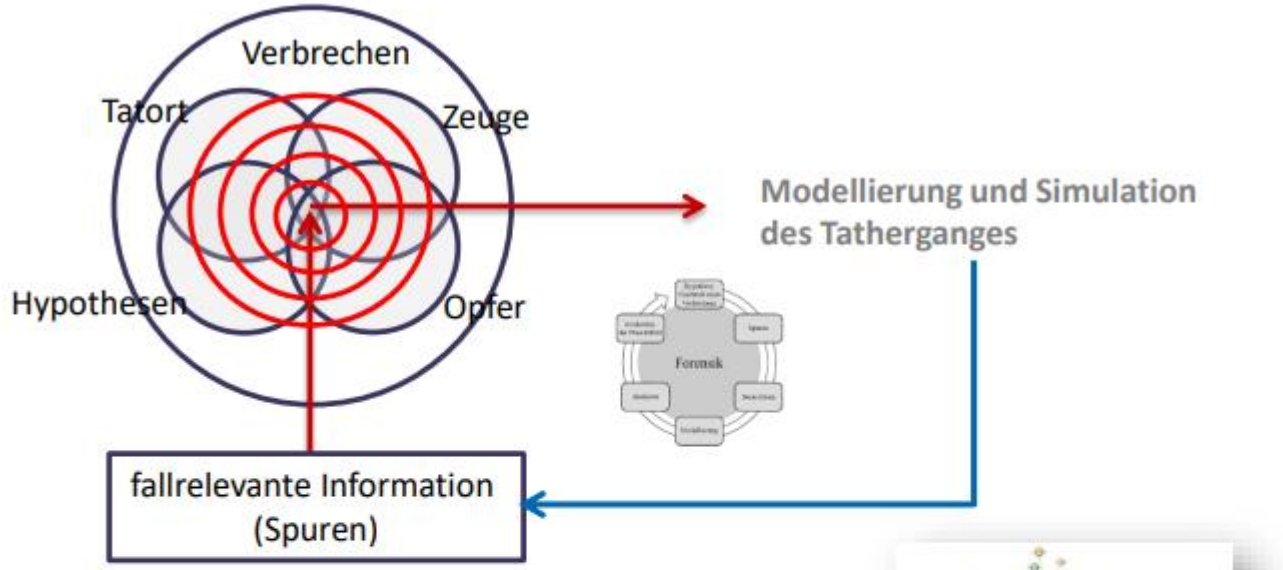
Grundlage der Analyse jeder Einzelspur

Σ Spuren = komplexes Gesamtsystem

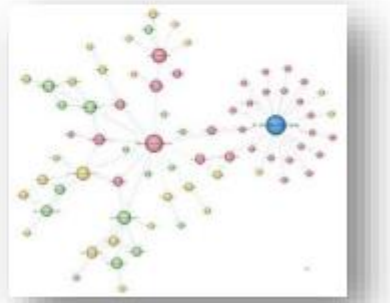
Grundlage der Modellierung und Simulation des Tatherganges

Informationsfluss

Analoge und Digitale Forensik



Inhalte der Spuren nach *verschiedenen Kriterien*
klassifizieren
Überführung in Konzepte
Graphvisualisierung



Visualisierung von Netzwerken und darin stattfindender Prozesse

Vielen Dank

Prof. Dr. rer. nat. Dirk Labudde

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Computer- und Biowissenschaften | Fraunhofer Lernlabor

T +49 (0) 3727 58-1469
F +49 (0) 3727 58-21469

dirk.labudde@hs-mittweida.de

Haus 8 | Richard Stücklen-Bau | Raum 8-105
Am Schwanenteich 6b | 09648 Mittweida

HOCHSCHULE MITTWEIDA
University of Applied Sciences

hs-mittweida.de