HOCHSCHULE MITTWEIDA
University of Applied Sciences

# Grundlagen Digitale Forensik

## Prüfungsschwerpunkte

Prof. Dr. Dirk Labudde

Bundeskriminalamt

# Digitale Forensik

# Forensik

*Forensik ist die Anwendung von Wissenschaft auf das Rechtssystem.*

*- American Academy of Forensic Sciences, AAFS*

Und jetzt digital?

# Digitale Forensik

- Digitale Forensik beschäftigt sich mit der gerichtsfesten Sicherung und Verwertung digitaler Spuren
- Als forensische Wissenschaft muss die digitale Forensik wissenschaftliche Methoden anwenden
  - Beweisführung kann dazu führen, dass Menschen ihrer Freiheit beraubt werden
  - Nur eine verlässliche und objektive Methodik wird dieser Verantwortung gerecht
  - Methodik muss immer wieder neu überdacht werden

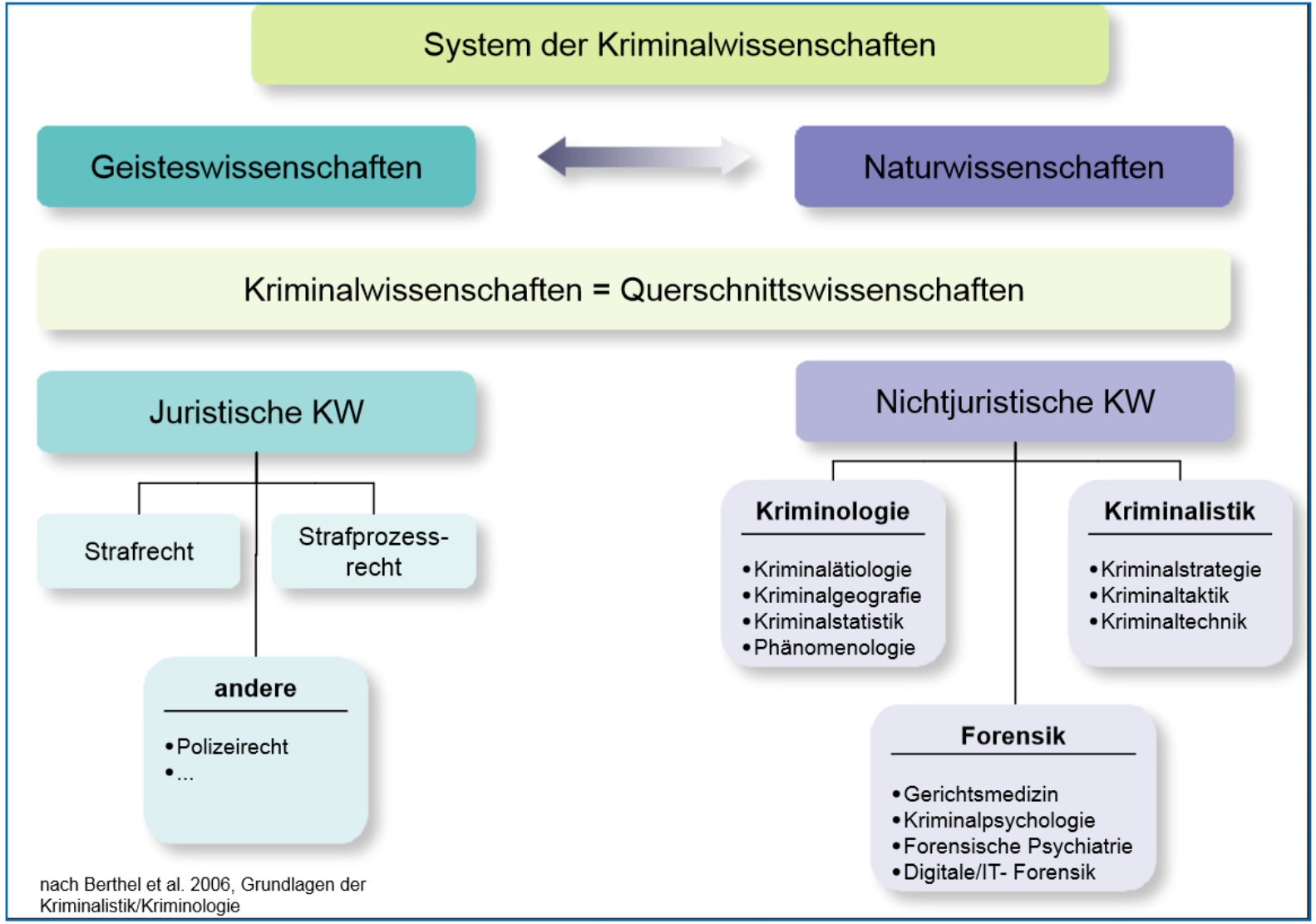
# IT-Forensik

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. [1]

→ IT-Forensik als Mittel der Strafverfolgung

→ BSI-Leitfaden als allgemeine Grundlage

# Informatik als forensische Wissenschaft



# Informatik als forensische Wissenschaft

**Forensische Informatik:** *ist die Anwendung wissenschaftlicher Methoden der Informatik auf Fragen des Rechtssystems.*[Dewald 2011]
- i.e.S. - Untersuchung technisch unvermeidbarer Beweismittel
- i.w.S. - Untersuchung technisch vermeidbarer Beweismittel

**IT-Forensik/Digitale Forensik:** ist die streng methodisch vorgenommene Datenanalyse auf Datentragern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems. [BSI 2011]

**Post-mortem-Analyse (Offline-Forensik)**
- Untersuchung von Datentragerabbildern (so genannten Images)
- Gewinnung und Untersuchung von gelöschten, umbenannten sowie anderweitig versteckten und verschlüsselten Dateien

[BSI 2011]

**Live-Analyse (Online-Forensik)**
- Untersuchung beginnt bereits während der Laufzeit des Vorfalls
- Gewinnung und Untersuchung flüchtiger Daten

[BSI 2011]

**Data-Forensik**
forensische Datenanalyse - Analyse von (meist großen) Datenbeständen aus Anwendungen und den zugrunde liegenden Datenbanken

**Disk-/Computerforensik**
Analyse von Computer- oder Mobilgeräten und der darin enthaltenen Daten

# Informatik als forensische Wissenschaft

## Digitale Forensik

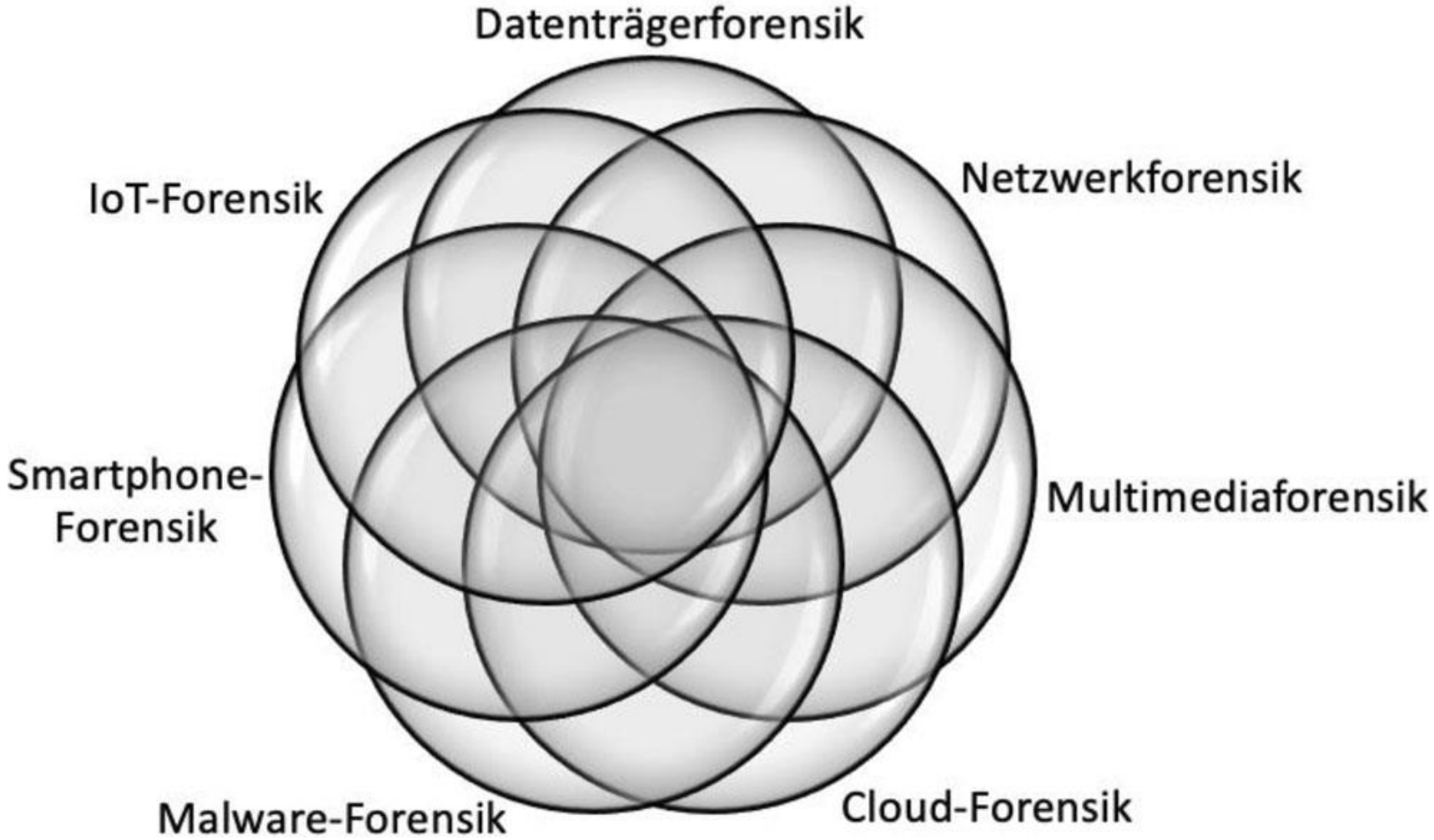
"...ein pragmatisches technisches Sachverständigenwesen...unter dem Oberbegriff 'Computerforensik' oder 'digitale Forensik'...."[Geschonneck:2006; Casey:2004]

"...[es] besteht der wesentliche Unterschied zwischen der klassischen Forensik und der digitalen Forensik in der Natur der Spuren, die in beiden Bereichen untersucht werden."[Dewald:2011]

"Fast alle Prinzipien, die man in der klassischen Forensik für physische Spuren entwickelt hat, lassen sich auch auf digitale Spuren anwenden."[Dewald:2011]

"...die Untersuchung digitaler Spuren [verlangt] manchmal neue Methoden."[Dewald:2011]

# Spezialgebiete der Forensik



# Digitale Spuren

# 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

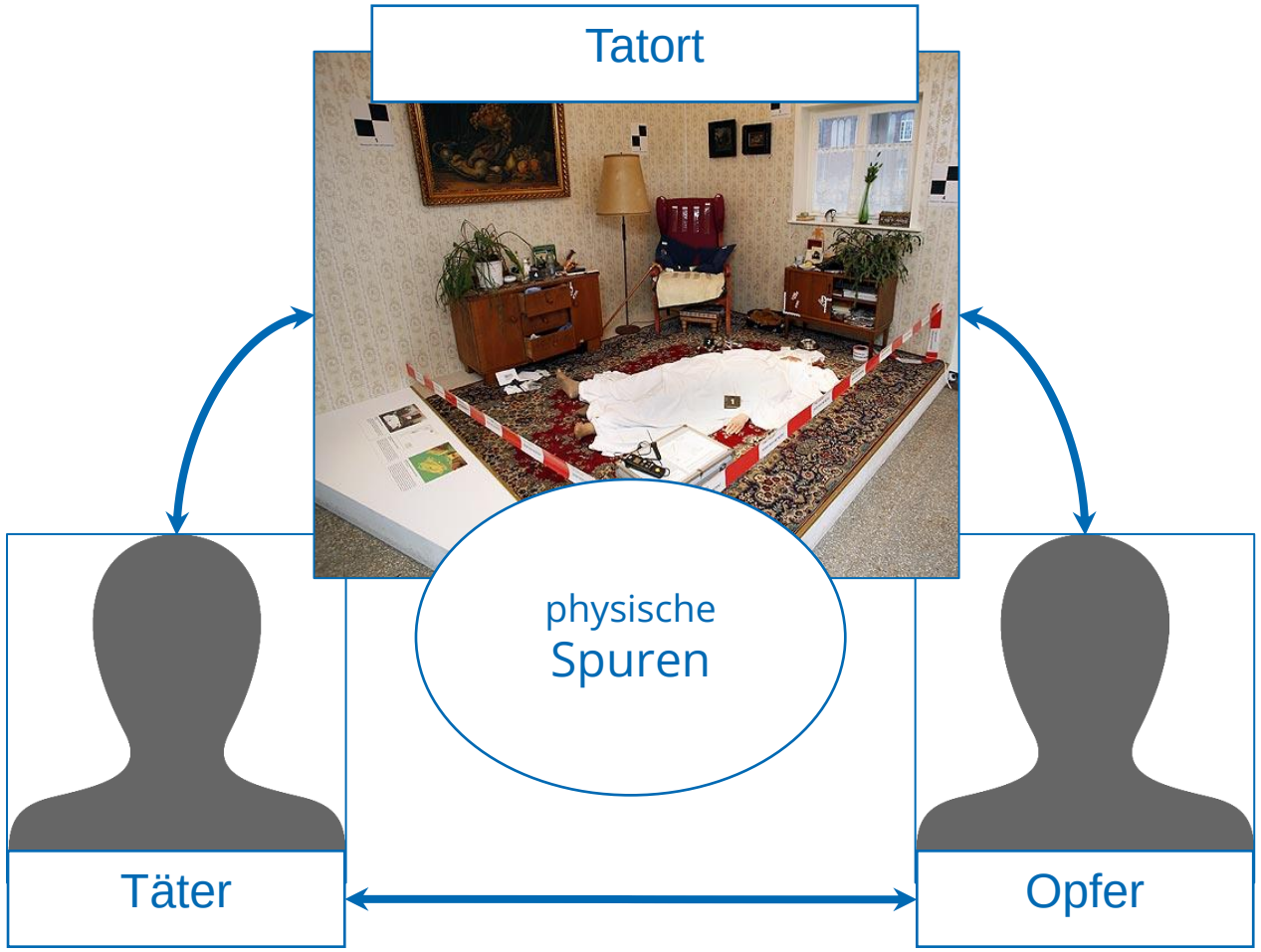
Dr. Edmund Locard

Austauschprinzip:

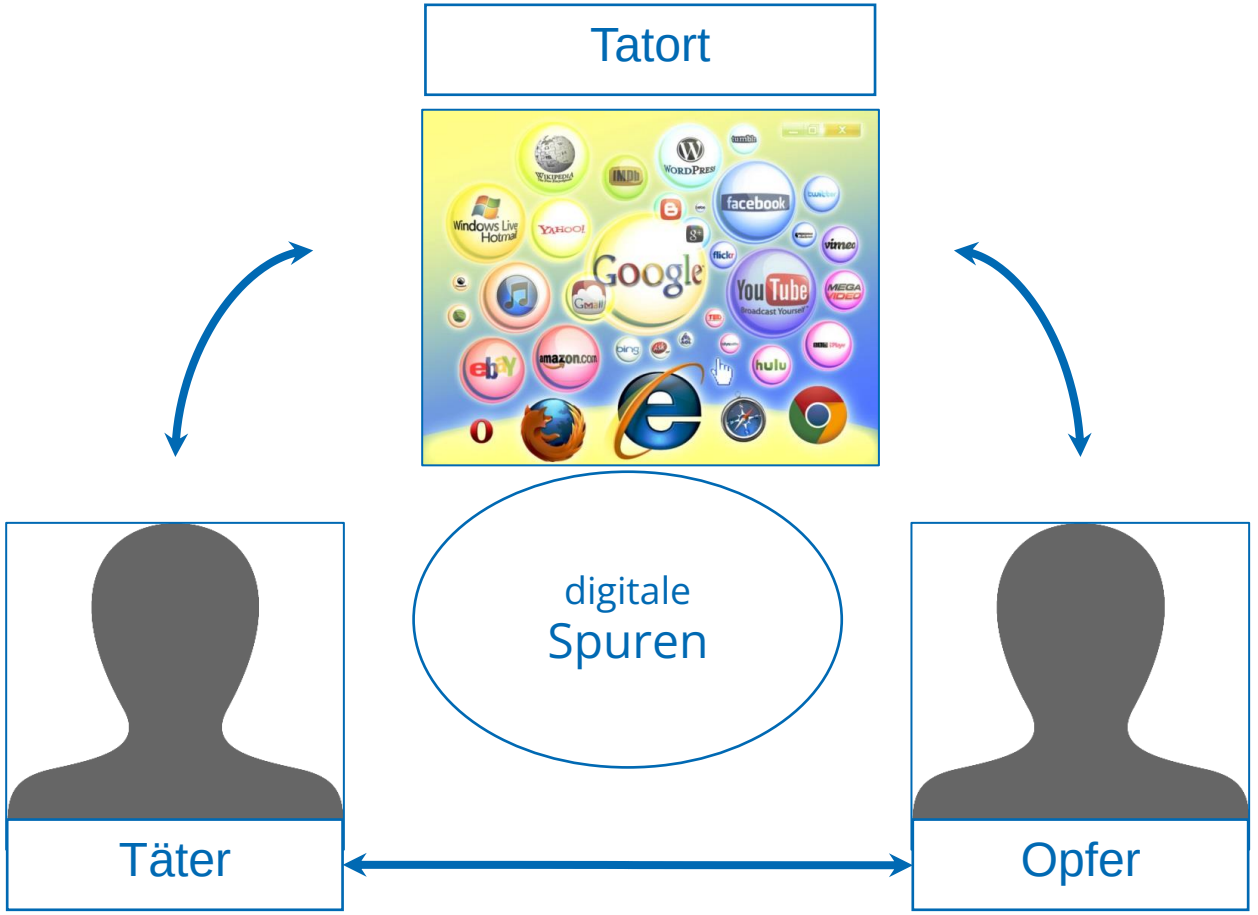
*„Jeder und alles am Tatort nimmt etwas mit und lässt etwas zurück.“*

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

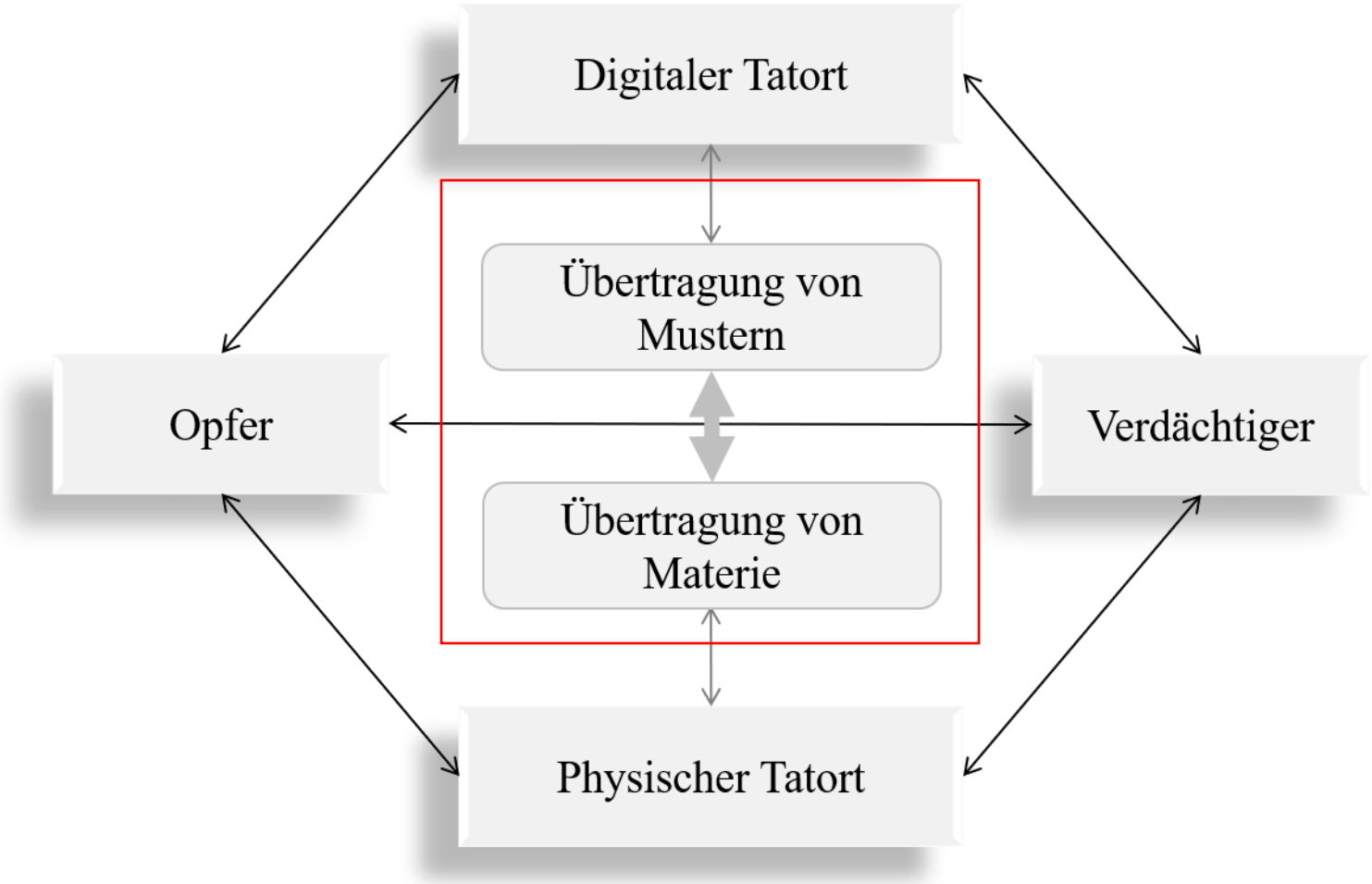
# Physikalische Spuren



# Digitale Spuren



# Übertragung von Muster und Materie



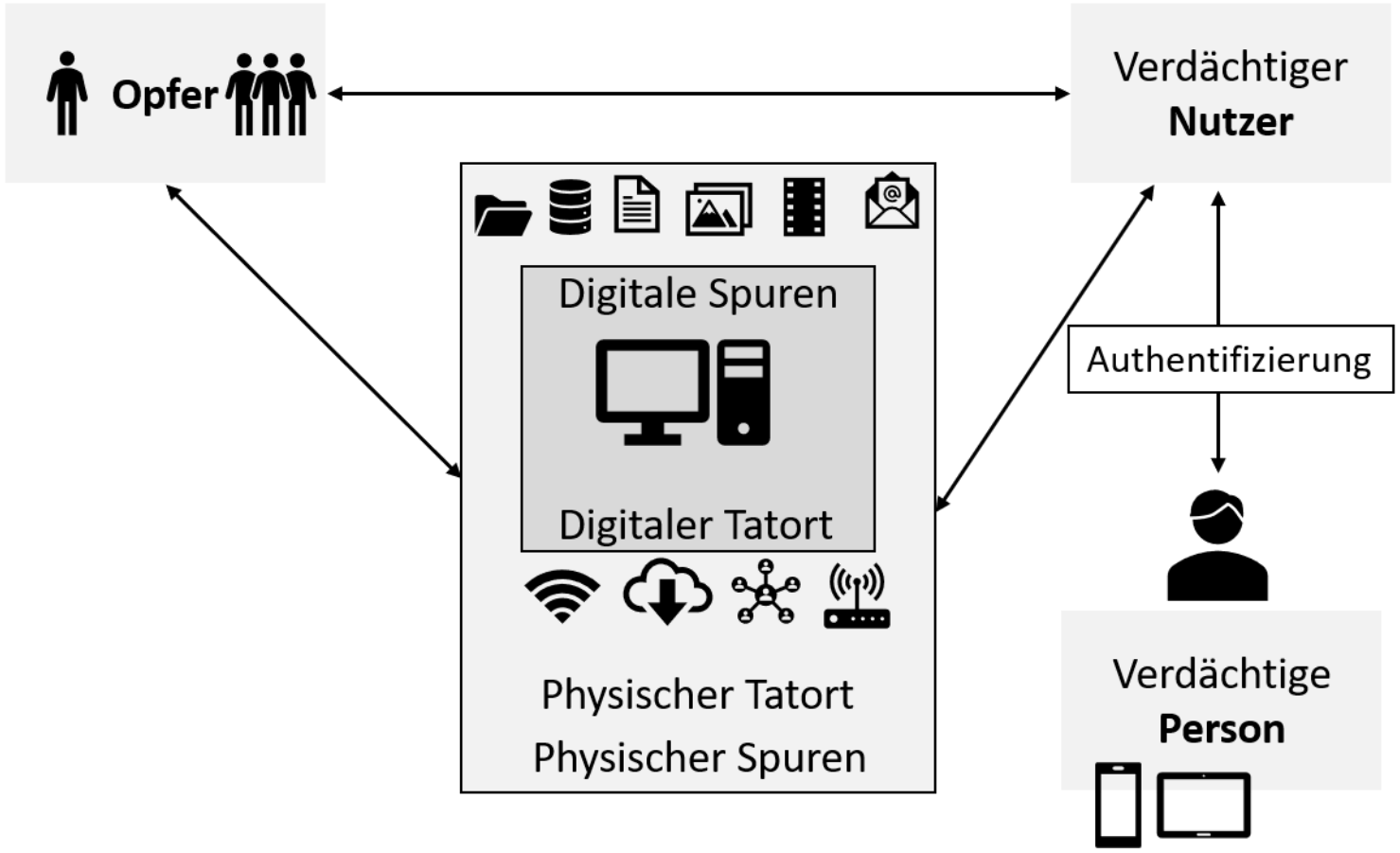
# Übertragung von Mustern und Materie

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.

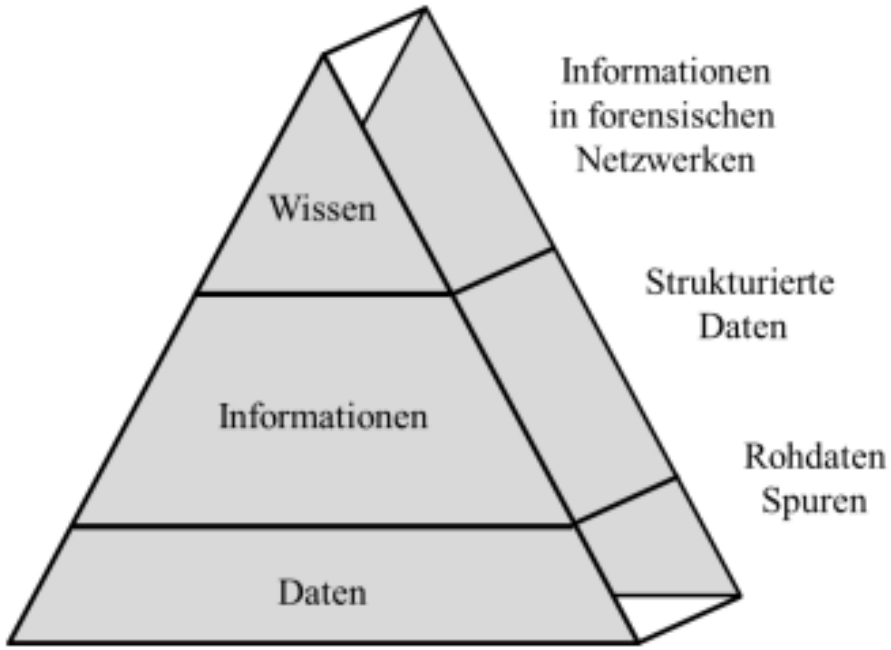
2. Übertragung von Mustern (transfer of traits): Hierbei werden charakteristische Formeigenschaften von einem Objekt auf ein anderes übertragen, ohne dass notwendigerweise Materie ausgetauscht wird.

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

# Digitale Spuren



# Analoge und Digitale Forensik




Systemverständnis

Zusammenhänge

**Klassifizierung**

Daten

# 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.

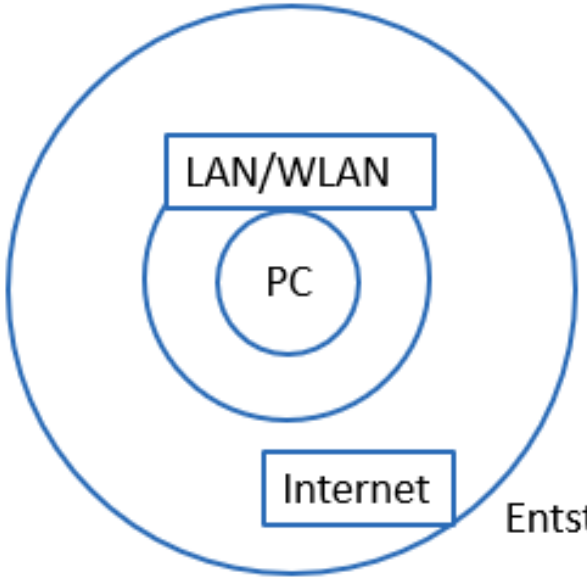
- zunächst physische Spuren
  - Magnetisierung auf der Oberfläche einer Festplatte,
  - elektromagnetische Wellen auf einem Datenkabel
  - Ladezustand von Speicherzellen im Hauptspeicher

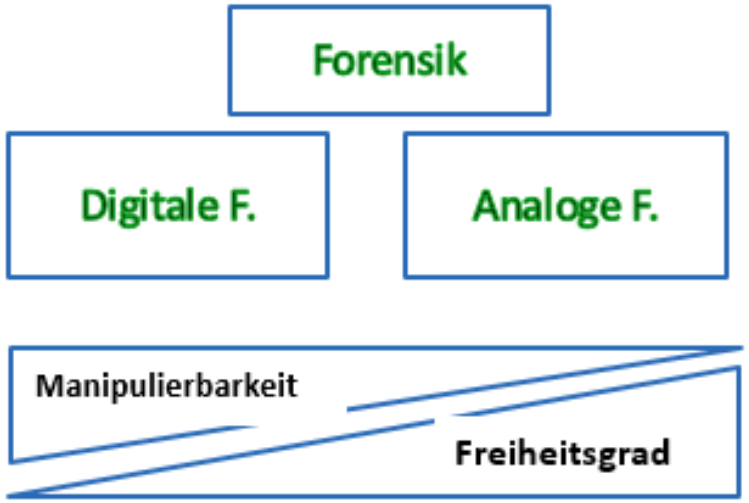
⇨ Prinzipien der klassischen Forensik anwendbar

- 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 - BEGRIFFSBESTIMMUNG

Spuren sind alle materiellen Veränderungen an Personen und / oder Sachen bzw. Objekten, die im Zusammenhang mit einem relevanten Ereignis entstanden sind und zur Tataufklärung beitragen können, da Rückschlüsse auf den Tatablauf, die Tatumstände sowie Hinweise auf den / die Täter gezogen werden können. Entscheidend ist das der Spur innewohnende objektive Informationspotential, dieses muss relativ beständig sein (Beibehaltung bis zur Begutachtung). Die materiellen Spuren bestimmen den Gegenstand der Spurenkunde unter anderem in der Kriminaltechnik. Grundsätzlich gilt: Es gibt keinen Tatort ohne Spuren!

# DIGITALE SPUREN - BEGRIFFSBESTIMMUNG

Digitale Spuren basieren auf Daten, die in Computersystemen gespeichert sind oder zwischen Ihnen übertragen wurden. Dabei sind digitale Spuren nicht mit materiellen Spuren gleichzusetzen. Digitale Spuren werden erst durch ihre Interpretation von physischen Spuren über unterschiedliche Interpretationsebenen zu einer verwertbaren digitalen Spur.

# Forensische Datenarten

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

# Zeitpunkt der Untersuchung

Post-mortem-Analyse

- Vorfall nachträglich aufklären
- Untersuchung von Datenträgerabbildern
- Gewinnung/Untersuchung von gelöschten, versteckten, verschlüsselten Dateien (aber auch „normalen“)

Live-Forensik

- Untersuchung während des Vorfalls
- Flüchtige Daten gewinnen/untersuchen
- Hauptspeicherinhalt, bestehende Netzwerkverbindungen, gestartete Prozesse

# Anforderungen an Vorgehensweisen

- Akzeptanz
- Glaubwürdigkeit
- Wiederholbarkeit
- Integrität
- Ursache und Auswirkung
- Dokumentation (Chain of Custody)

# Modell, Prozess, Methode

# Modell, Prozess, Methode

## Modell

Ein Modell beschreibt den groben Ablauf einer Untersuchung in stark vereinfachter, schematischer Weise.

## Prozess

Der Prozess beschreibt den Ablauf in detaillierter Form und hilft dadurch, Reproduzierbarkeit zu gewährleisten und unterstützt, wesentliche Teile im definierten Prozess nach Möglichkeit nicht zu vergessen.

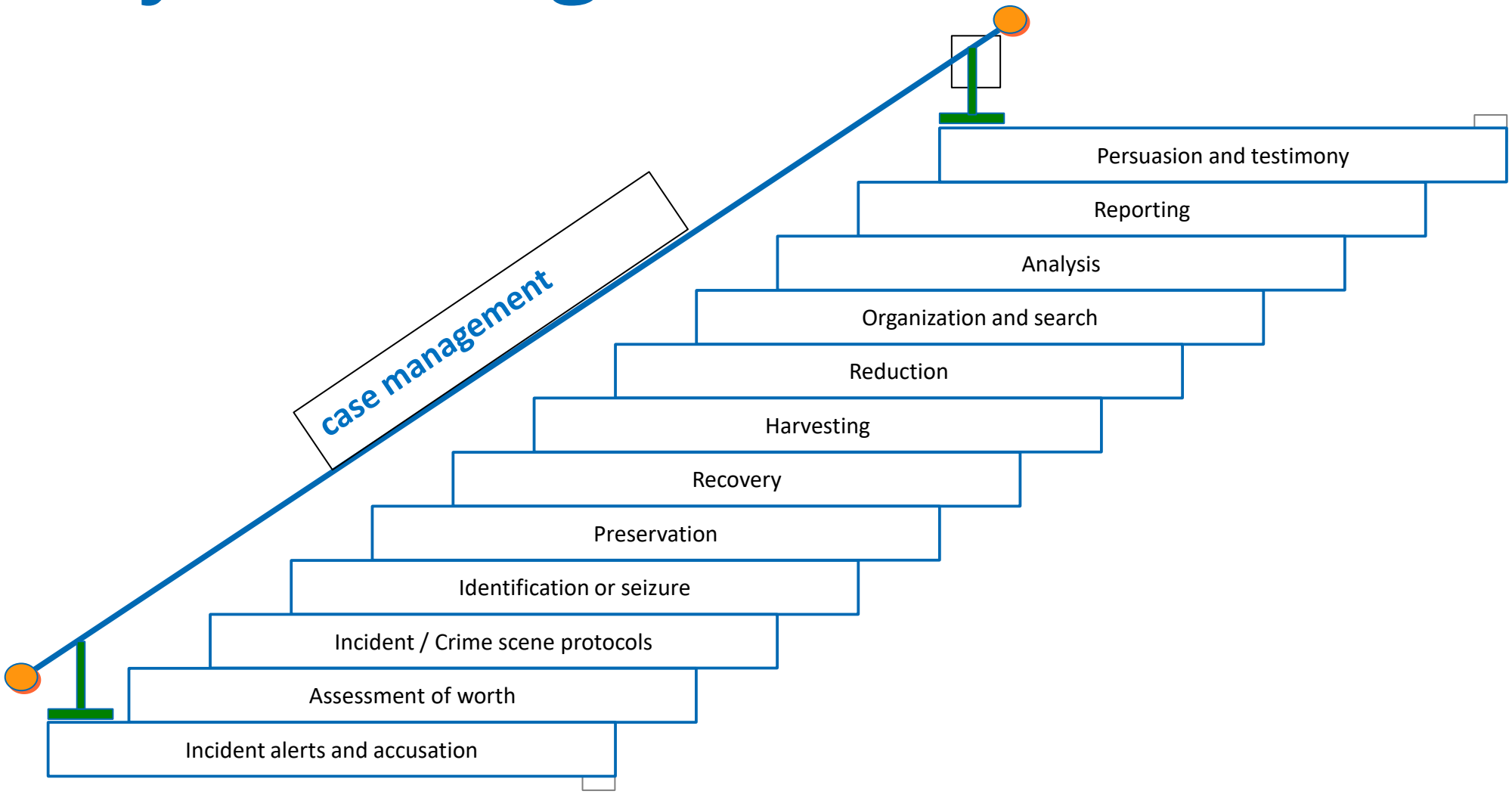
## Methode

Die Methoden wiederum definieren die einzelnen Schritte bis hinunter zu den einzelnen Werkzeugen/Tools die man verwenden kann oder sollte.

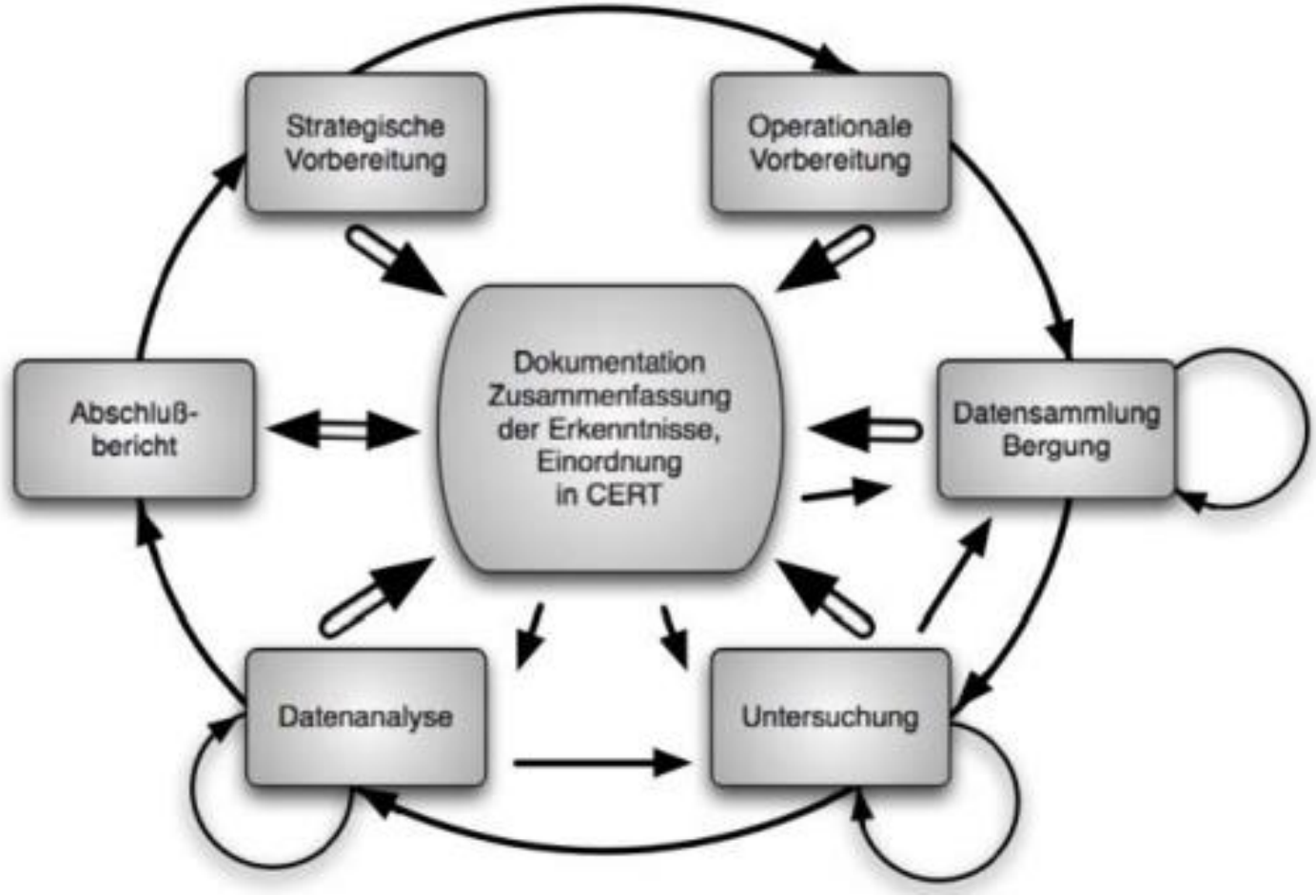
# SAP – Ein forensisches Ablaufmodell

- Eine Grundlage für die Erhebung und Verwertung digitaler Spuren
- für die Untersuchung von Beweismitteln
- S(ecure)-A(nalyse)-P(resent) Modell

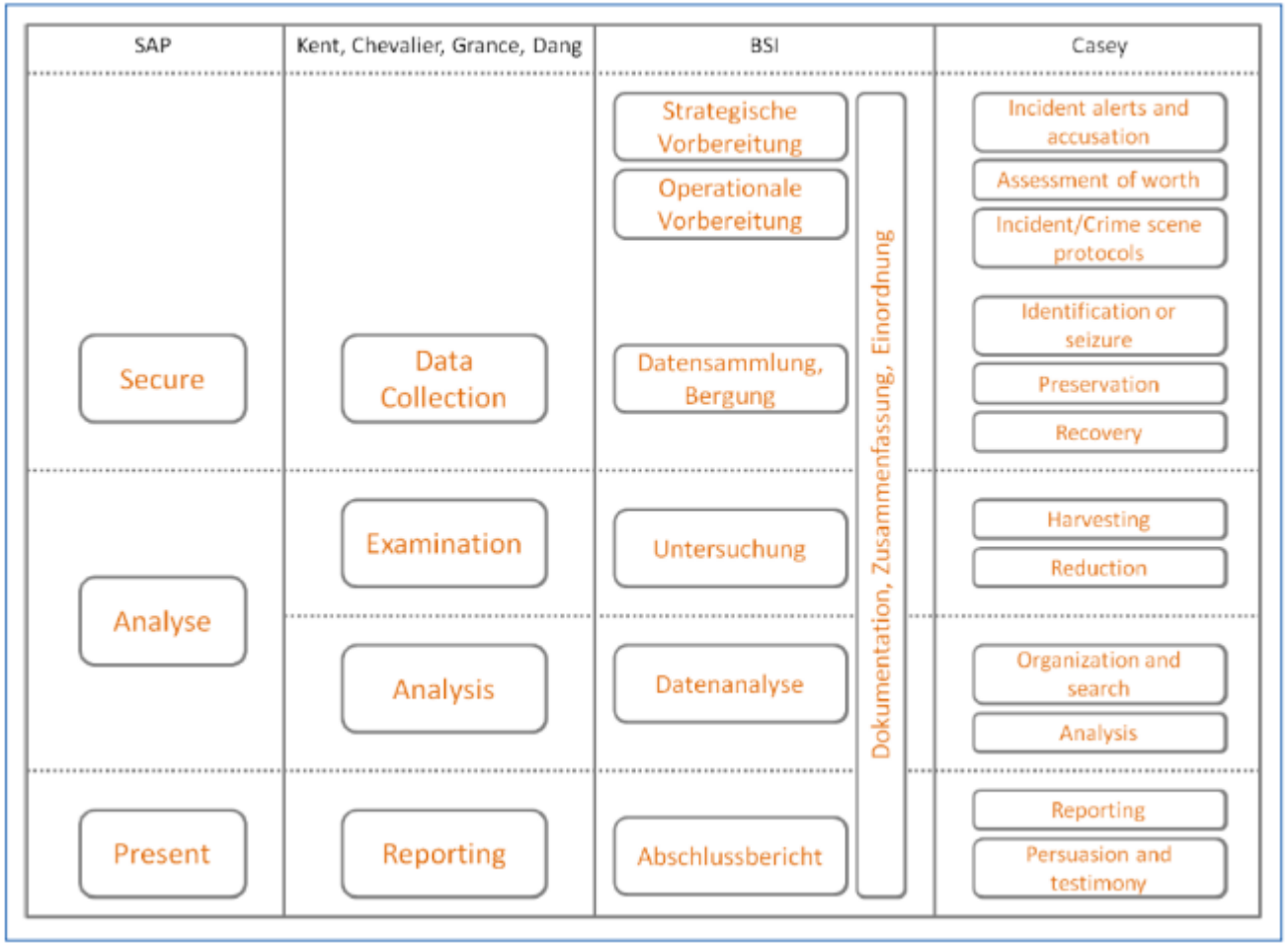
# Casey Investigative Prozess



# Erweiterter forensischer Prozess



# Verschiedene Modelle/Prozesse



# Grundlegende Methoden

- Methoden des Betriebssystems;
- Methoden des Dateisystems;
- Explizite Methoden der Einbruchserkennung;
- Methoden einer IT-Anwendung;
- Methoden der Skalierung von Beweismöglichkeiten;
- Methoden der Datenbearbeitung und Auswertung.

# Zahlensysteme

Es werden Aufgaben zur Umrechnung in der Prüfung enthalten sein!

# Darstellung von Daten im Rechner

- Damit Daten bzw. Informationen mit Computerprogrammen verarbeitet werden können, müssen sie in maschinenlesbarer Form repräsentiert werden.
- Das Problem dabei ist, dass Computerprogramme mit für den Menschen verständlichen Repräsentationsformen wie Bildern, Buchstaben, Tönen nichts anfangen können.
- Computer verarbeiten nur Zahlen: Daten jeglicher Art mussen also in ein Zahlenformat transformiert werden. Diesen Vorgang nennt man Digitalisieren.
- Im Rahmen der IT-Forensik müssen wir die Daten sichern, analysieren und auswerten.

# Bits und Bytes

- Die beiden Grundeinheiten in jedem heutigen Computer sind die Einheiten Bit und Byte
- Die elementarste Informationseinheit, mit der Computer arbeiten, ist das Bit (engl. Binary Digit = Binärziffer)
- Computer arbeiten physikalisch mit zwei alternativen Spannungszuständen: ein relativ hohes Spannungspotential oder ein relativ niedriges Spannungspotential. Diese werden mit den Ziffern 1 (hoch) und 0 (niedrig) bezeichnet.
- Informationen eindeutig durch Zahlenfolge kodierbar
- Technisch einfach realisierbar, gut speicher- und übertragbar

# ASCII

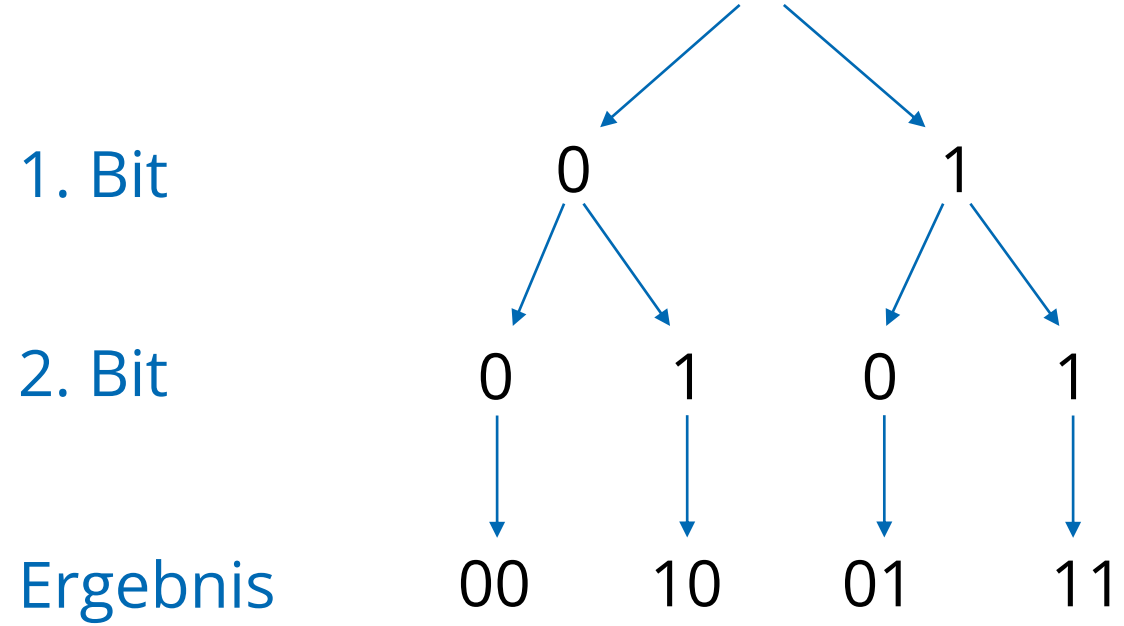
- Standard zur Darstellung von Zeichen durch elektronische Geräte
- 7 Bit zur Darstellung, 1 Bit zum Prüfen
- Kodierung von Steuerzeichen, Sonderzeichen, Ziffern und Buchstaben
- Spätere Versionen nutzen 8 Bit (256 Zeichen kodierbar)

| Binär | ASCII-Zeichen |
|---|---|
| 100 0110 | F |
| 100 1111 | O |
| 101 0010 | R |
| 100 0101 | E |
| 100 1110 | N |
| 101 0011 | S |
| 100 1001 | I |
| 100 1011 | K |

# Binärsystem

1 Bit = 2 Zustände

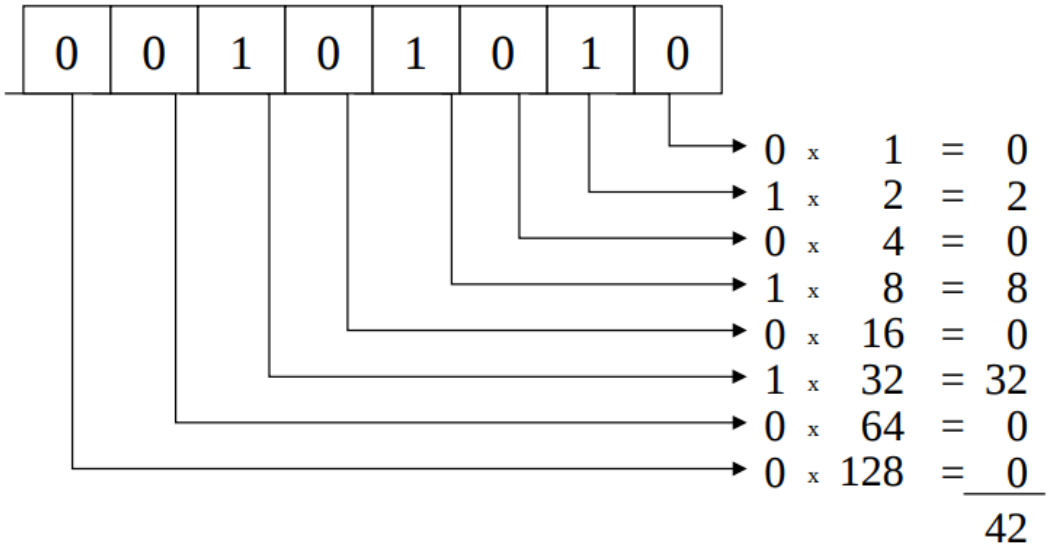
2 Bit = 4 Zustände




3 Bit = 8 Zustände
4 Bit = 16 Zustände
.
.
.
8 Bit = 256 Zustände

# Binärnotation

- Bytes und Worte können dazu verwende werden, um Ganzzahlen beliebiger Größe zu repräsentieren
- Bei der binären Kodierung wird lediglich eine andere Zahlenbasis verwendet
- Das nächst höhere Bit ist immer um Faktor 2 erhöht gegenüber dem rechts von ihm stehenden Bit.



# Binärsystem

- Umrechnung Binär → Dezimal

| | Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
|---|---|---|---|---|---|---|---|---|
| Byte: Bit | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 |
| Wertigkeit | $2^7 = 128$ | $2^6 = 64$ | $2^5 = 32$ | $2^4 = 16$ | $2^3 = 8$ | $2^2 = 4$ | $2^1 = 2$ | $2^0 = 1$ |
| | 1*128 | 0*64 | 1*32 | 1*16 | 1*8 | 1*4 | 0*2 | 1*1 |
| | 128 | + | 32 | + 16 | + 8 | + 4 | + | 1 |

Aufaddieren der gesetzten Wertigkeiten: 189

→ $1011\ 1101_{(2)} = 189_{(10)}$

Kennzeichnung des Zahlensystems

# Binärsystem

- Umrechnung Dezimal → Binär

167

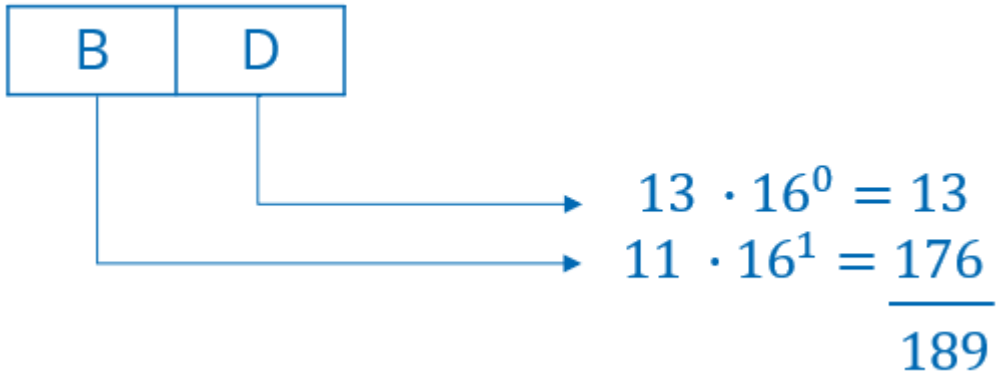
| Wertigkeit | Enthalten? | Rest |
|---|---|---|
| 128 | 1 | 39 |
| 64 | 0 | 39 |
| 32 | 1 | 7 |
| 16 | 0 | 7 |
| 8 | 0 | 7 |
| 4 | 1 | 3 |
| 2 | 1 | 1 |
| 1 | 1 | 0 |

108

| Wertigkeit | Enthalten? | Rest |
|---|---|---|
| 128 | 0 | 108 |
| 64 | 1 | 44 |
| 32 | 1 | 12 |
| 16 | 0 | 12 |
| 8 | 1 | 4 |
| 4 | 1 | 0 |
| 2 | 0 | 0 |
| 1 | 0 | 0 |

# Hexadezimales Zahlensystem

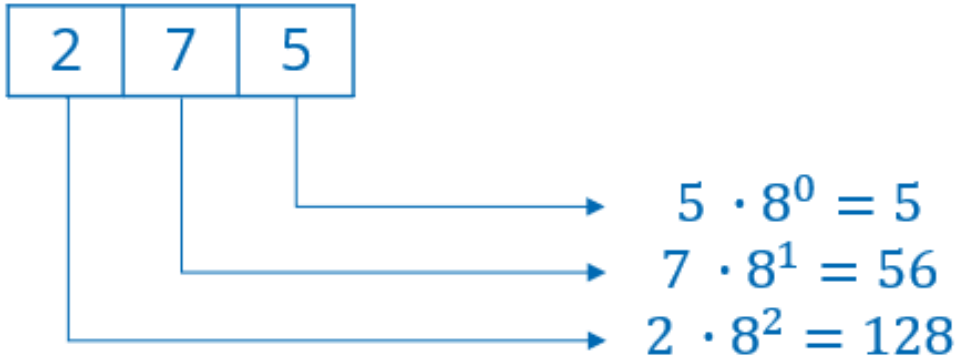
- Binäre Darstellung oft sehr lang
- → Hexadezimale (oder oktale) Darstellung verwendet
- Basiert auf 16 Ziffern:
  - 0 bis 9
  - A bis F für 10 bis 15
- Ein Byte darstellbar in 2 Stellen




| | |
|---|---|
| 0 | 0 |
| 1 | 1 |
| … | … |
| 9 | 9 |
| 10 | A |
| 11 | B |
| 12 | C |
| 13 | D |
| 14 | E |
| 15 | F |

# Oktales Zahlensystem

- Basiert auf 8 Ziffern (0 bis 7)



# Dateisysteme

# Dateisysteme

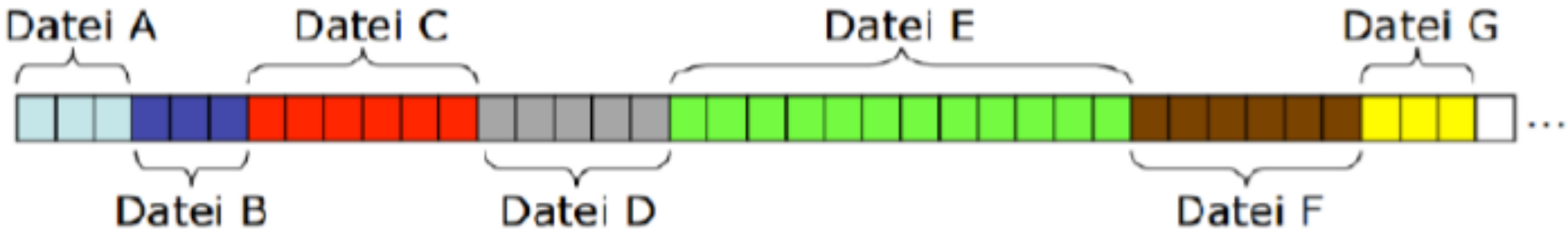
Begriffsbestimmung

- Die Grundlage für die Speicherung von Daten auf einem Datenträger, ist das Vorhandensein eines Dateisystems.
- Dateisysteme bilden dabei die Schnittstelle zwischen den Betriebssystemen und der Hardware des Datenträgers.
- Eine der wesentlichen Aufgaben eines Dateisystems ist dabei, die für den Nutzer nicht ersichtliche Speicherung bzw. Auslesung der Daten und die Möglichkeit der Organisation in Hierarchieebenen .

# Dateisysteme

Weshalb sind Dateien überhaupt auf einem Datenträger organisiert?

Könnten nicht alle Daten hintereinander auf einen Datenträger geschrieben werden?

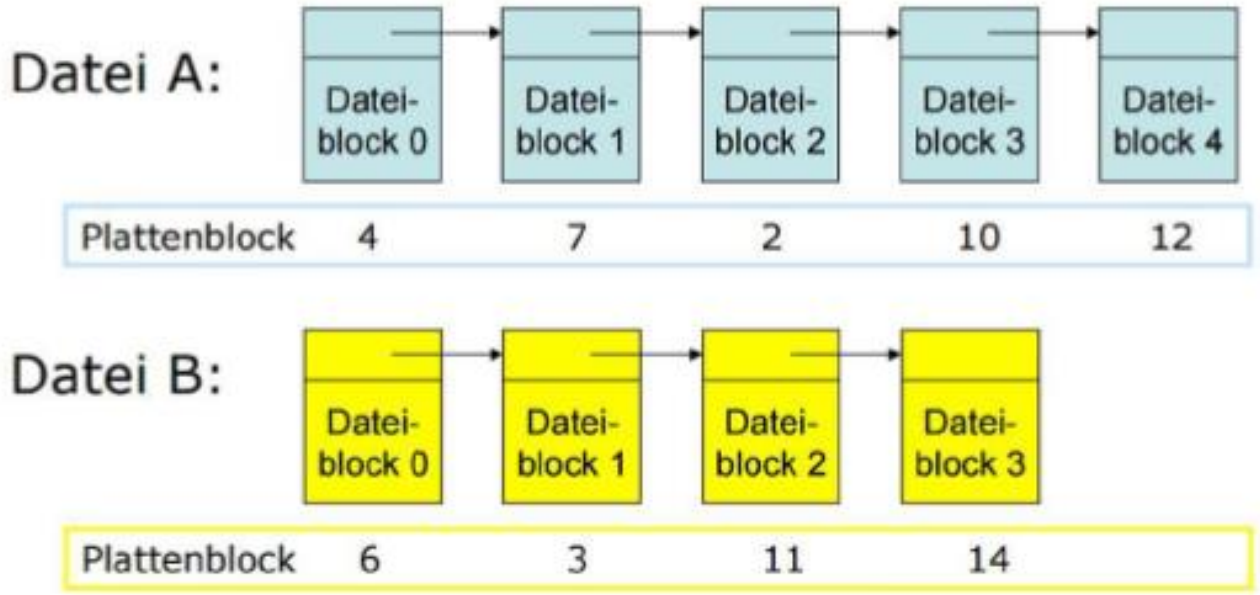



Vorteile: schnelles Lesen von Dateien mit wenigen Leseoperationen.

Welche Nachteile hätte eine solche Speicherorganisation?

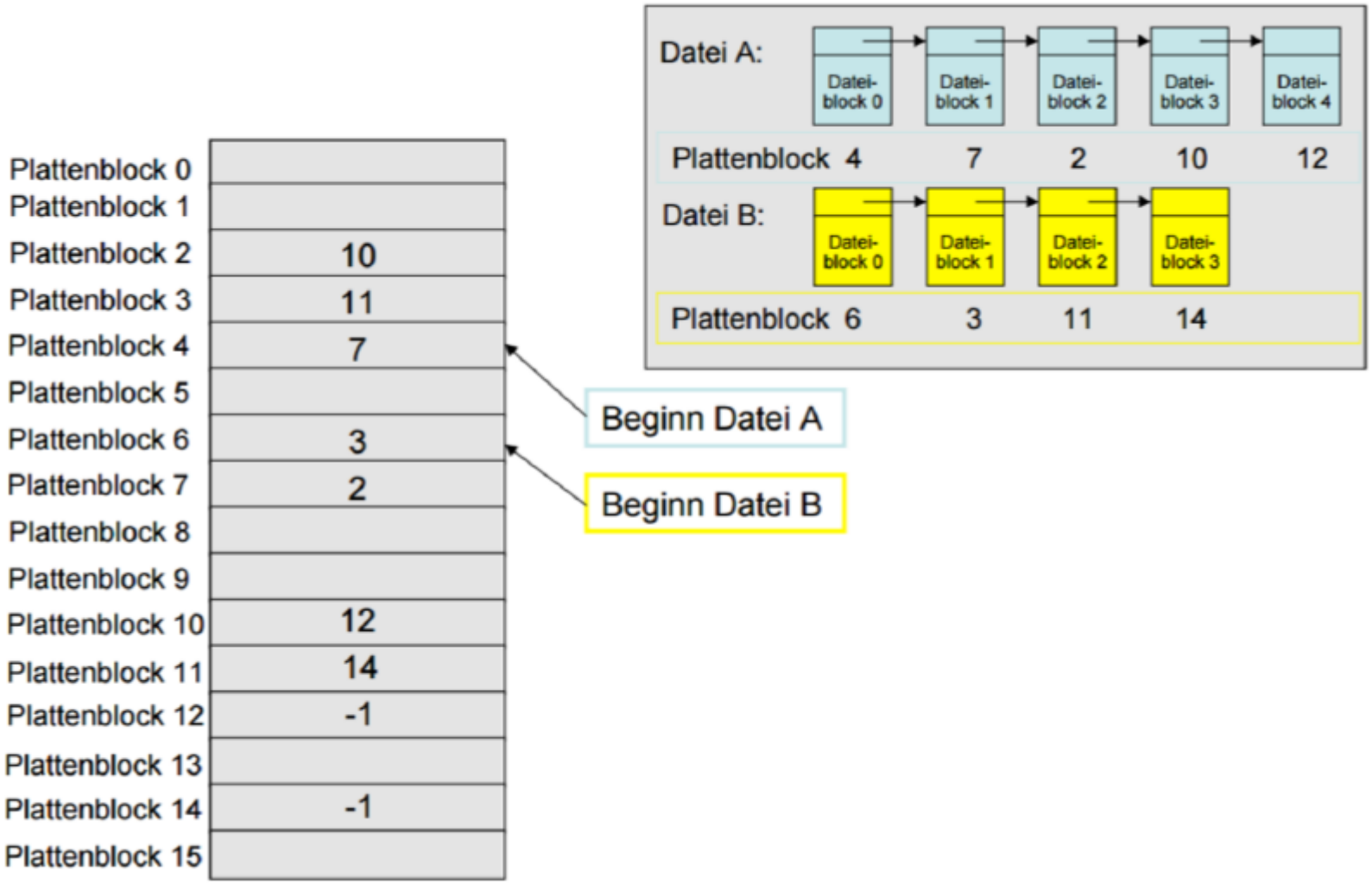
# Verkettete Listen

- Speicherung von Dateien in Datenblöcken mit fester Blockgröße
- zuvor Aufteilung der Datei in gleichgroße Blöcke
- jeder Block verweist auf den nächstfolgenden Block.



# Dateisystem FAT

Beispiel für zwei Dateien A und B unter FAT



# Grundbegriffe in Dateisystemen

## Sektor

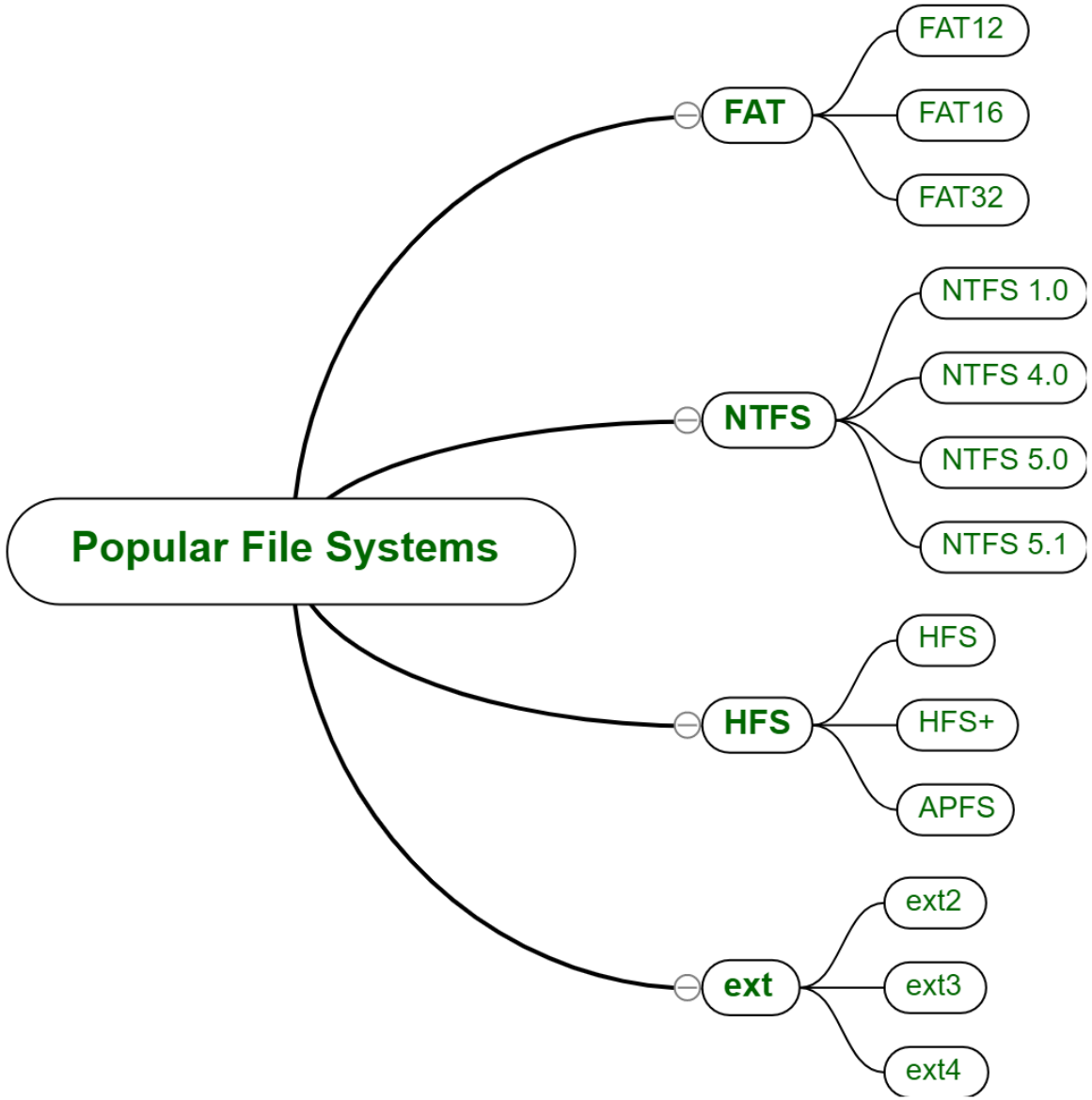
- Die Zusammenfassung einzelner Bytes zu einem Block bezeichnet man als Sektor.
- Die Zusammenfassung wird auf Ebene der Festplattenfirmware realisiert.
- Die gebräuchlichste Sektorgröße sind 512 Bytes.

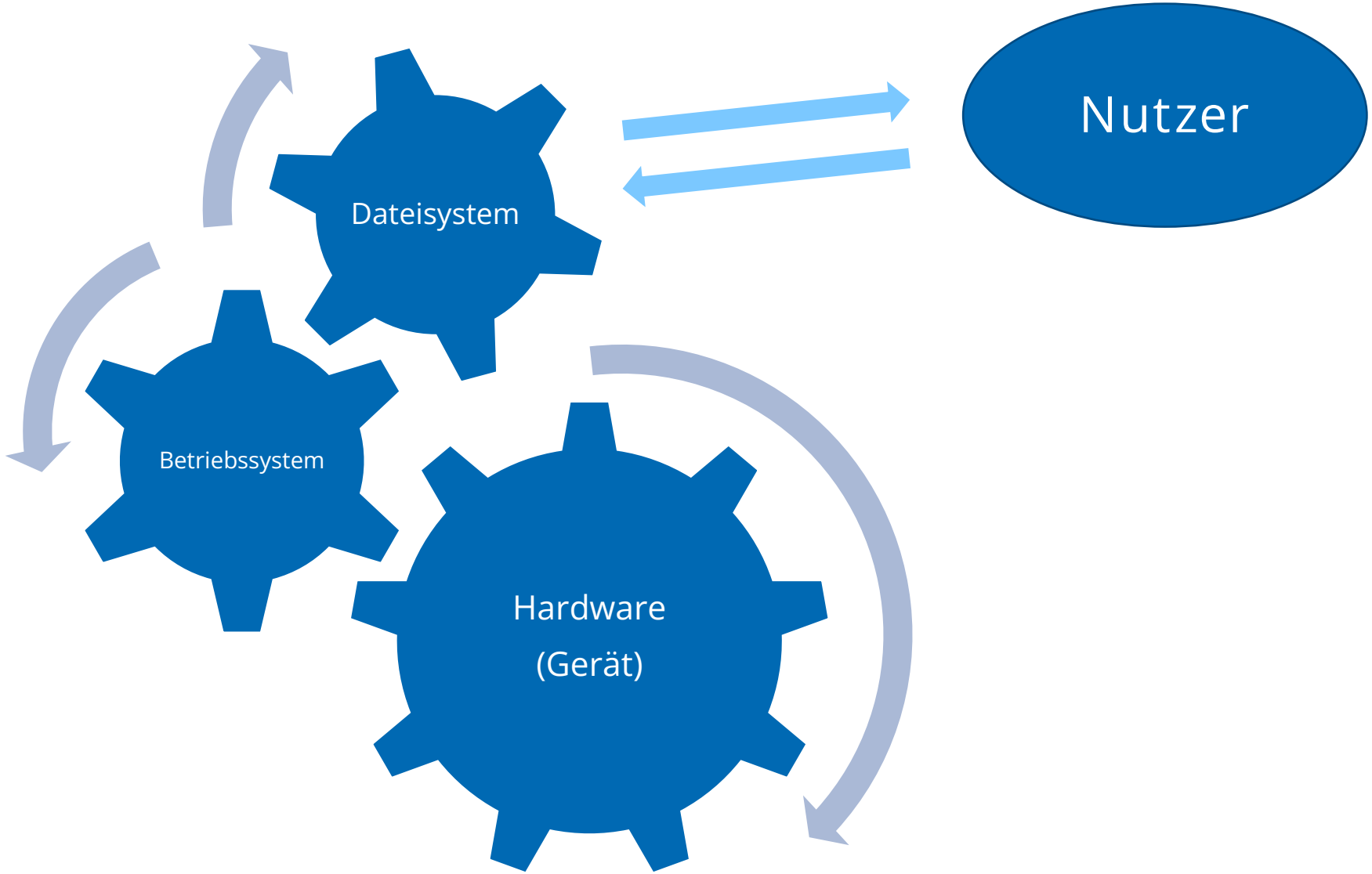
Datenblöcke einer Festplatte

## Cluster

- Die Zusammenfassung einzelner Sektoren zu einem Block bezeichnet man als Cluster.
- Die Zusammenfassung wird auf Ebene der Betriebssysteme realisiert.
- Die Clustergröße ist abhängig vom Dateisystem.

Datenblöcke eines Dateisystems




Nutzer
Dateisystem
Betriebssystem
Hardware
(Gerät)

# Betriebssysteme

# Grundlagen

Die Hardware eines Computers allein reicht nicht! Betriebssystem (operating system) ist das Bindeglied zwischen der Hardware und dem Anwender bzw. dessen Anwendungsprogrammen .

Gleichzeitig bietet es dem Benutzer zahlreiche Dienste (Programme, Kommandos) an, die zusammen mit den Eigenschaften des Computers „die Grundlage der möglichen Betriebsart dieses Systems bilden und insbesondere die Abwicklung von Programmen steuern und überwachen“ (DIN 44300).

# Grundlagen

Betriebssystem = Dienstleistungs- und Verwaltungseinrichtung

- „nur“ ein Mittel zum Zweck, aber ein wichtiges!
- Teil der Systemsoftware (mit Organisations-, Dienst- und Übersetzungsprogrammen wie Compiler, Debugger, Editoren, graphischen Benutzeroberflächen, Hilfsprogrammen/Tools zum Suchen, Sortieren, Kopieren, zur Installation/ Konfiguration usw. )
- Bildet die Plattform zur Entwicklung und Ausführung von Anwendungsprogrammen
- Abstrahiert die reale (beschränkte) Hardware („virtuelle Maschine“)

# Aufgaben eines Betriebssystems

Ziel:

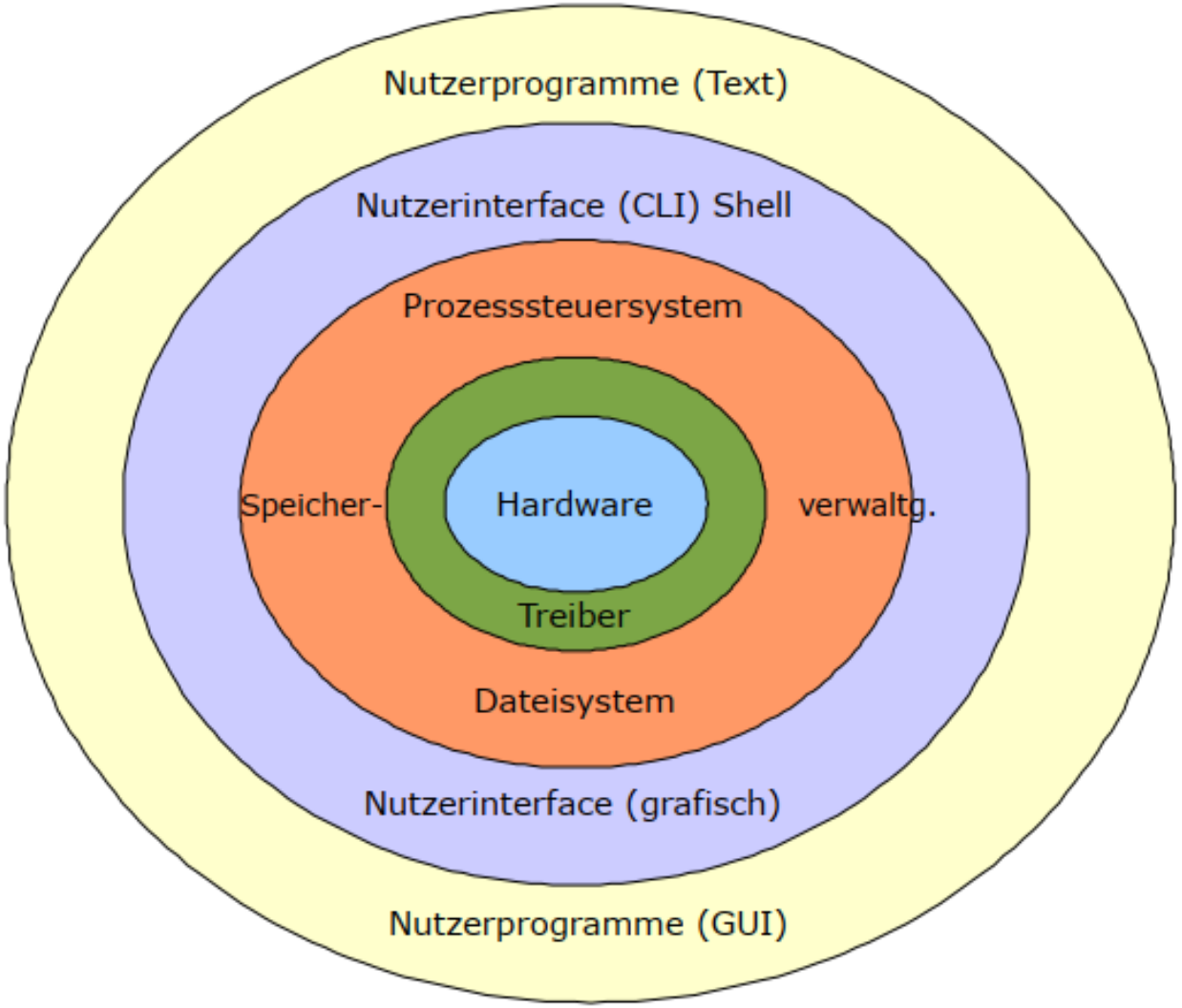
Optimale Ausnutzung
(beschränkter) Ressourcen

Erfüllung spezieller
Nutzeranforderungen

Aufgaben:

- Anpassung der Hardware-Möglichkeiten an die Bedürfnisse der Nutzer
- Organisation und Steuerung des Betriebsablaufs
- Verwaltung und ggf. Zuteilung von (begrenzt verfügbaren) Ressourcen
- Kontrolle und Durchsetzung von Schutzmaßnahmen
- Nachweisführung über relevante Abläufe

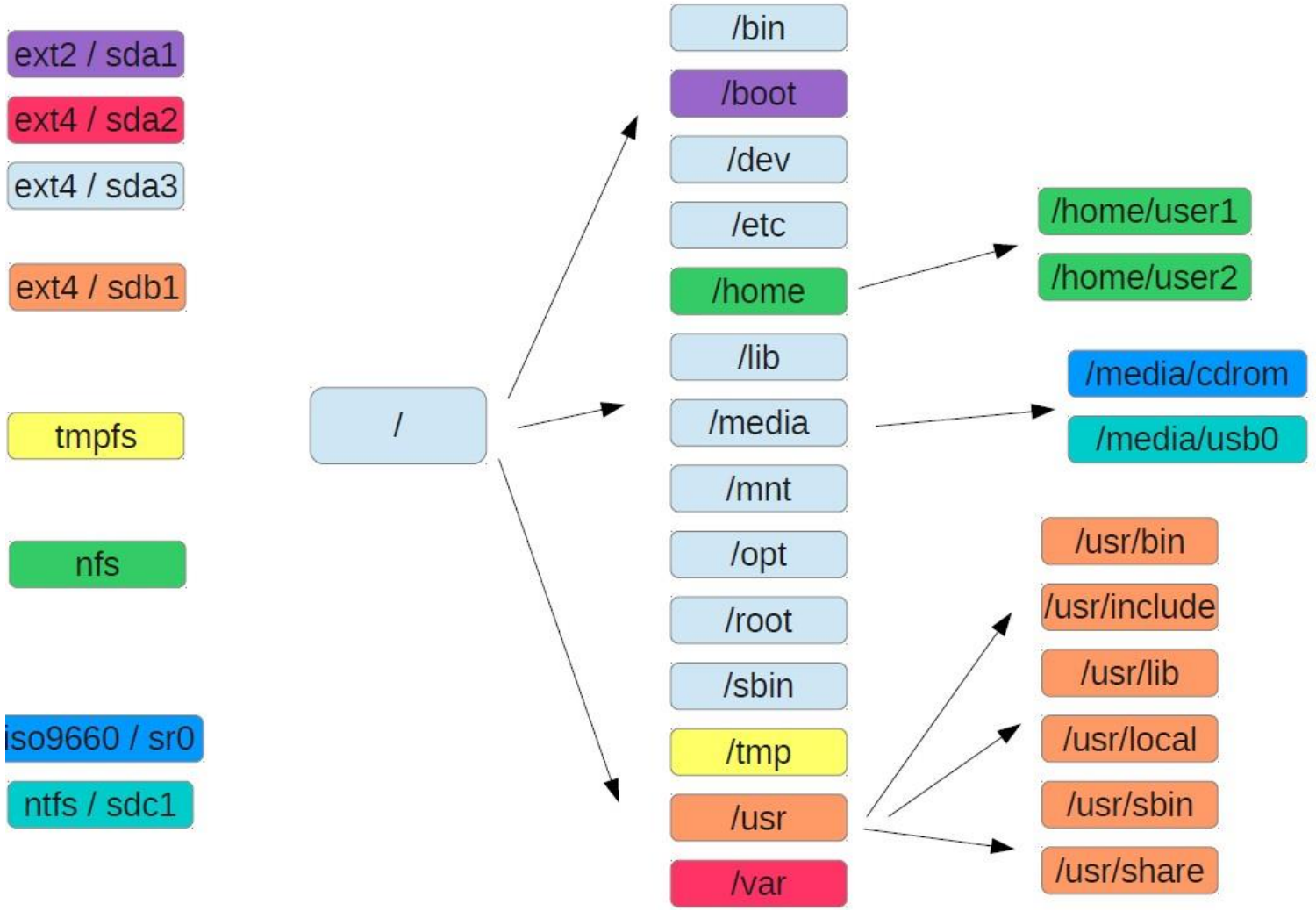
# Aufbau von Linux als Schalenmodell



# Standard Filesystem Hierarchy

In FHS, befinden sich alle Dateien und Verzeichnisse unterhalb des Root Directory “/” eingeordnet, auch wenn diese physisch oder virtuell an anderer Stelle abgelegt sind.

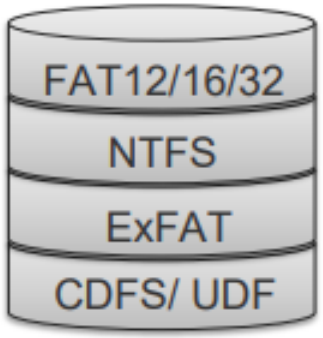
Besonderheiten:
- Einträge max. 255 Zeichen groß
- Unterscheidung in Groß und Kleinschreibung



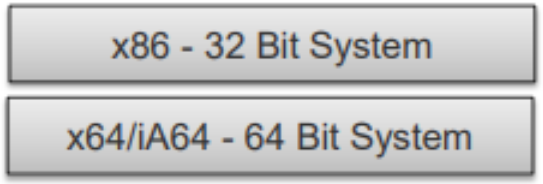
# Allgemeine Informationen Windows

## Allgemeine Informationen

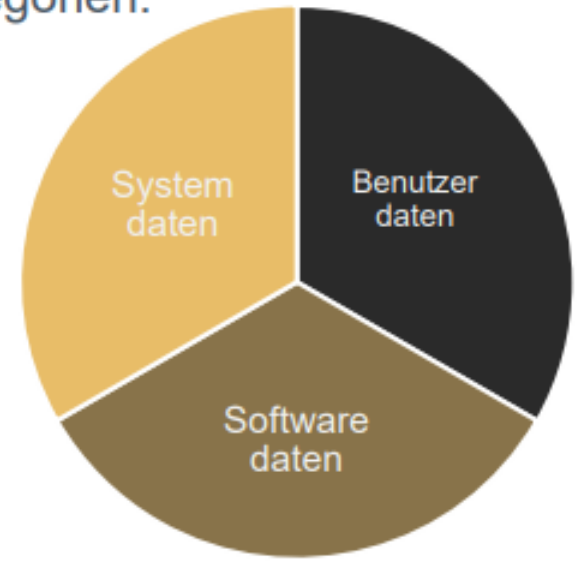
Unterstützte Dateisysteme:




Unterstützte Architekturen:




Die interne Datenaufteilung erfolgt in drei unterschiedlichen Kategorien:




Die logische Trennung dieser Daten findet sich dabei an verschiedenen Stellen im Betriebssystemaufbau wieder.

3

# Wichtige Verzeichnisfade

- Systemdaten findet man im Windows Verzeichnis, je nach Betriebssystemversion als „WINDOWS“, „WIN“ oder „WINNT“ benannt.
- Softwaredateien befinden sich im Programm Verzeichnis je nach Betriebssystemversion als „Programme“ oder „Program Files“ benannt.
- Benutzerdaten befinden sich im Benutzerdaten-Verzeichnis. Für die Windows Versionen Windows 95,98 und ME im Verzeichnis „Eigene Dateien“.
  Unter Windows NT, 2000 und XP im Verzeichnis „Dokumente und Einstellungen“ und unter Windows Vista, Windows 7, 8 und 10 im Verzeichnis „Users“ in einem Benutzerverzeichnis benannt nach dem Benutzerkontonamen.

Einstellungen und Anwenderspezifische Daten zu einzelnen installierten Software-anwendungen werden in Unterverzeichnissen gespeichert.

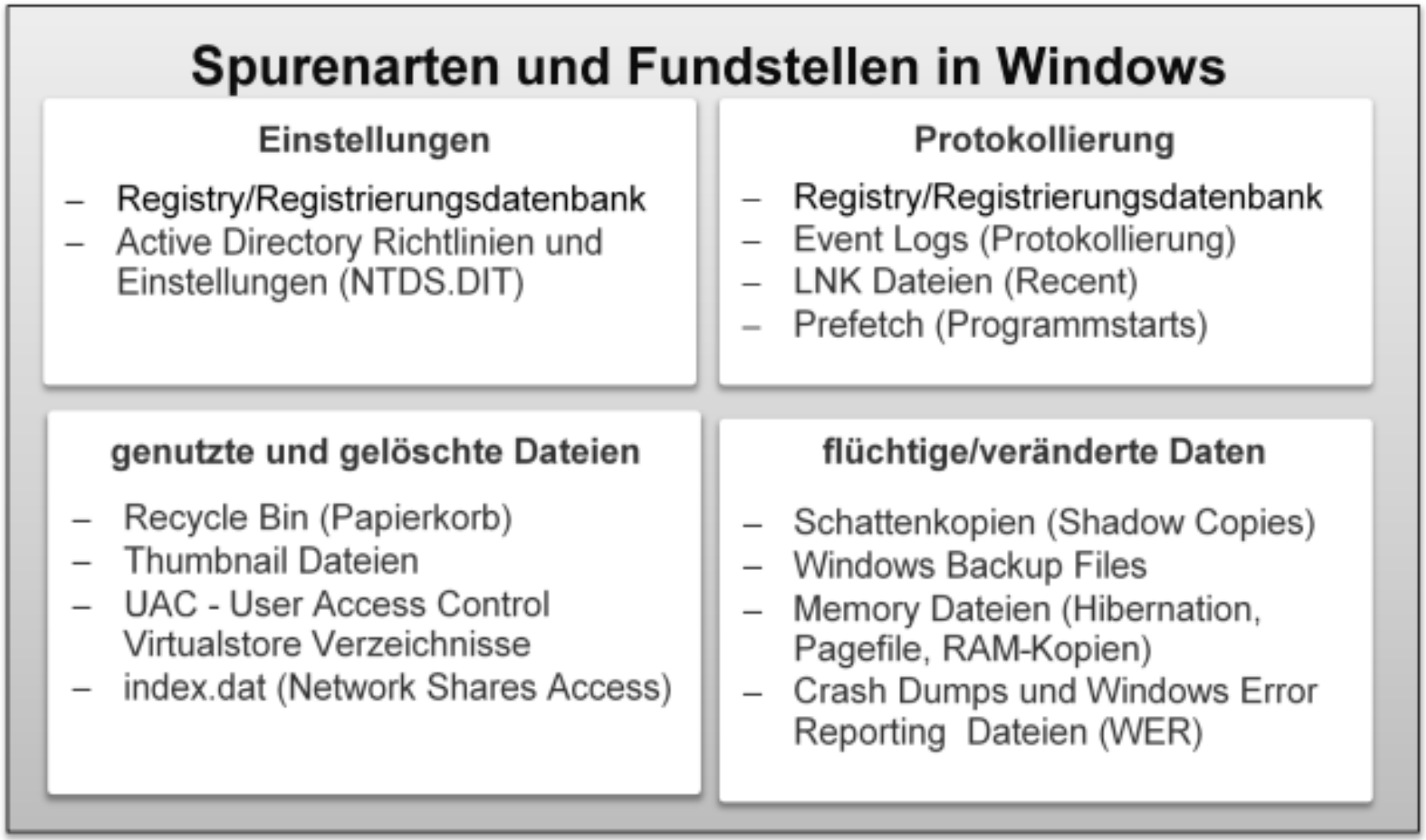
Unter Windows NT, 2000 und XP in:

- „\Anwendungsdaten“ und „\Lokale Einstellungen\Anwendungsdaten“

Unter Windows Vista, 2003, 2008, 2012, 2013, 7, 8 und 10 in:

- „\AppData\Local“, „\AppData\LocalLow“ und „\AppData\Roaming

# Spuren in Windows

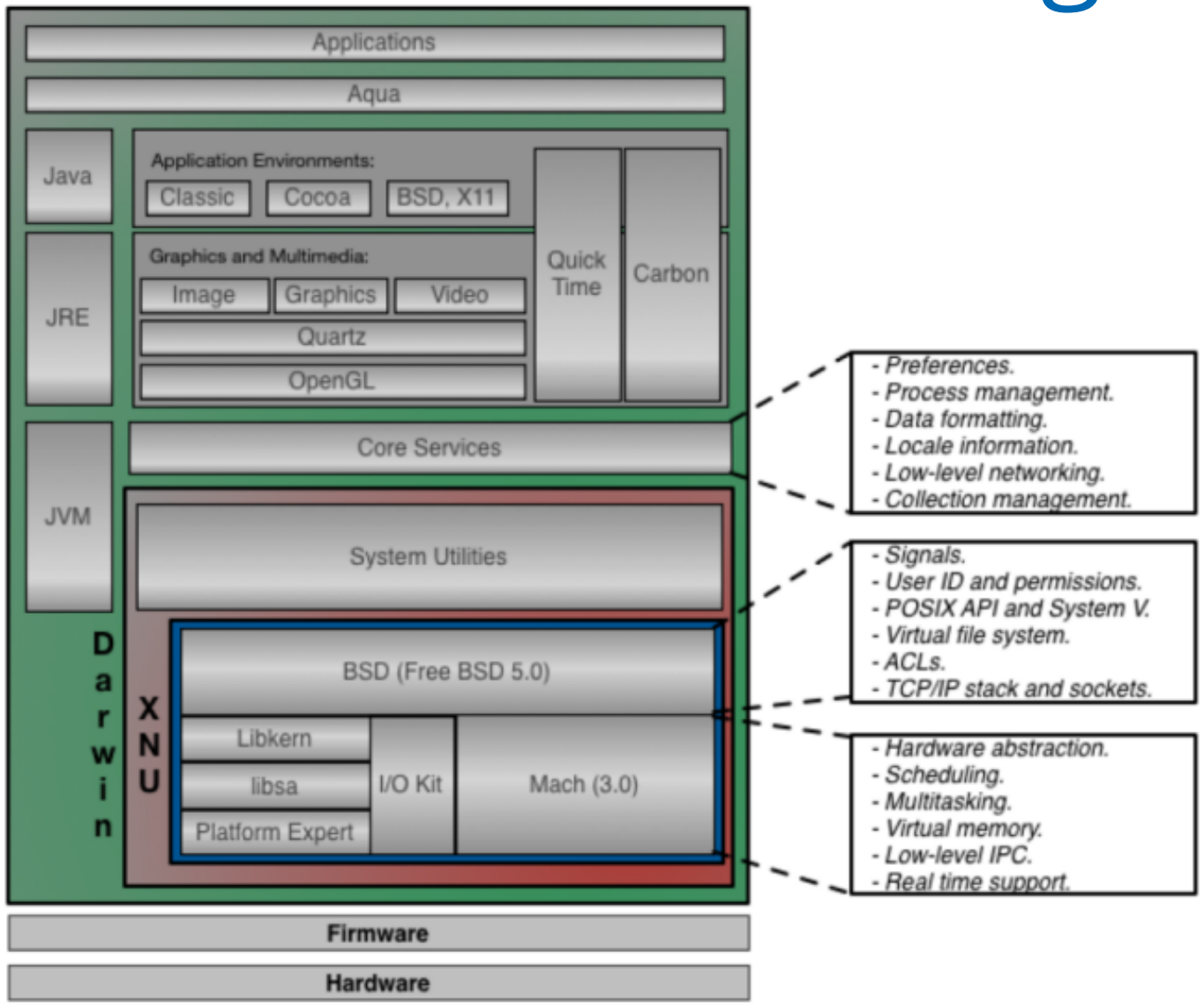


# Grundaufbau von OSX

OSX ist in vier Schichten aufgebaut:

1. Benutzerebene - Aqua, die grafische Benutzerschnittstelle (GUI)
2. Anwendungsprogrammierebene - Programmierschnittstellen (APIs) wie Cocoa (und früher Carbon), Java
3. Bereitstellungsebene - Grafik-Subsystem (Quartz mit Quartz Compositor, OpenGL), Audio/Video (QuickTime) etc.
4. Basisebene - Darwin, das Kern-Betriebssystem

# MacOSX Grundlegender Aufbau



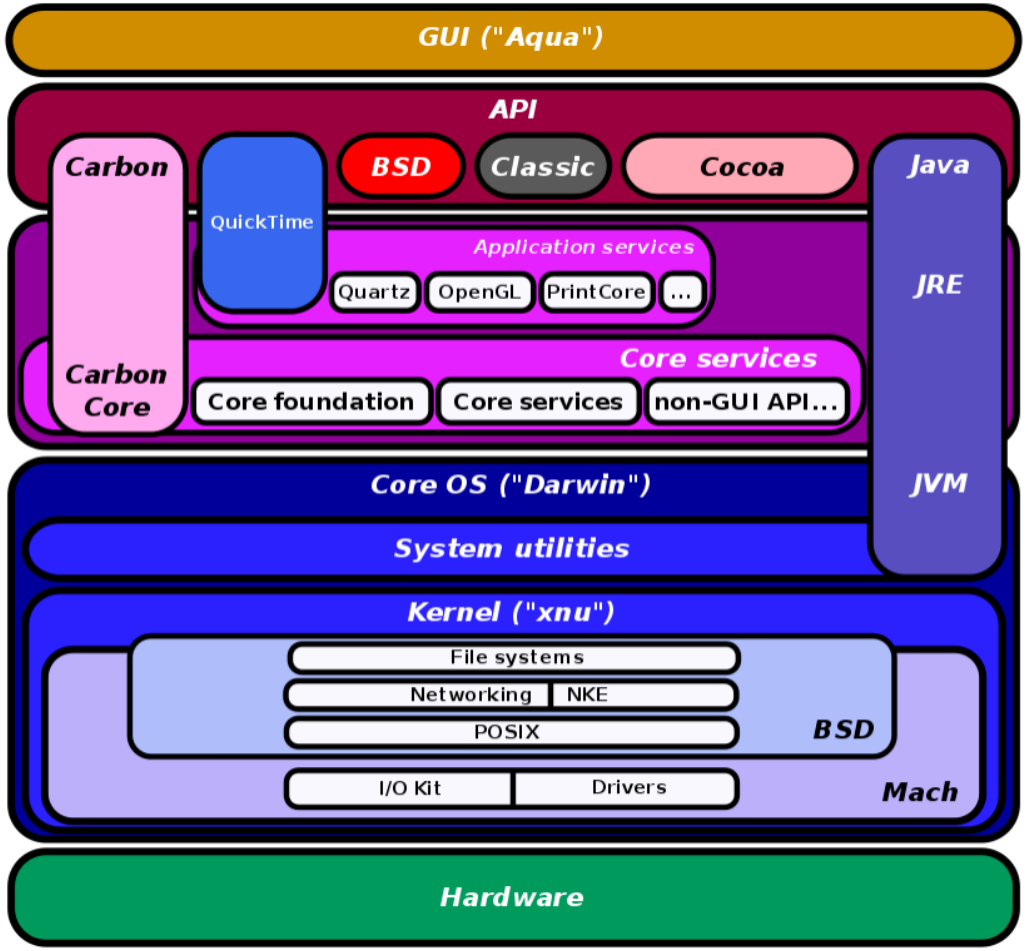




Abbildung: Grundaufbau von OSX (Bild: Joaquín Moreno Garijo)

# Dateisysteme

Mac OS X nutzt das Dateisystem HFS und dessen Erweiterung HFS+. Dieses von Apple entwickelte Dateisystem wird auch für externe Datenträger verwendet und kann mit einem Windows basierten System nicht gelesen werden.

Mac OS X kann auch das FAT12/16/32 Dateisystem lesen und schreiben. Damit ist es möglich externe Datenträger, wie Speicherkarten und USB Sticks für den Multibetriebssystembetrieb einzurichten.

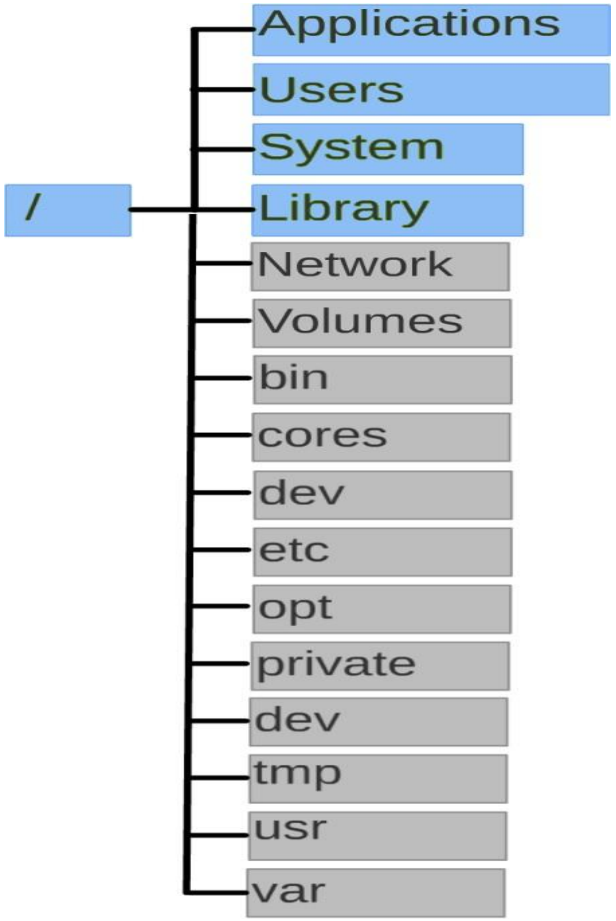
Seit der Einführung von macOS X 10.12 wurde das Apple Dateisystem HFS+ durch APFS (Apple File System) ersetzt.

# Wichtige Verzeichnisstrukturen

Die Verzeichnisstrukturen eines Mac OS X lässt den UNIX- Ursprung erkennen. Unterschiede gibt es jedoch bei den on Apple entwickelten Bestandteilen.

Apple hält sich bei seiner Verzeichnisstruktur nicht streng an den Filesystem Hierarchy Standard (FHS). Der Standard ist aber noch erkennbar.

Zudem sind viele Sytsemordner bei OSX versteckt (graue Verzeichnisse)



# Zeitstempel

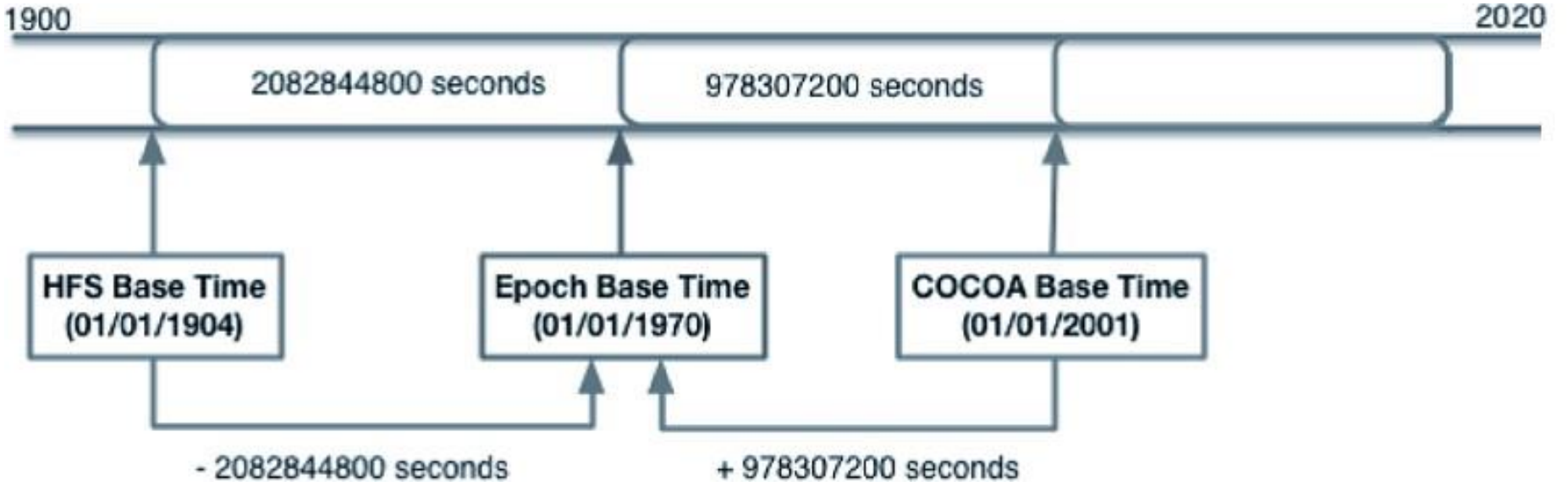
OSX verwendet drei unterschiedliche Zeitstempel:

- HFS Time: 4 Byte HexWert, der die Sekunden seit dem 01. Januar 1904 zählt
- Epoch: 4 Byte HexWert, der die Sekunden seit dem 01. Januar 1970 zählt
- Cocoa: 64 Bit - Integer der die Sekunden seit dem 01. Januar 2001 zählt

Aus Dokumentation passenden Zeitstempel ermitteln.

# Zeitstempel

OSX verwendet drei unterschiedliche Zeitstempel:



# 3 Schutzebenen

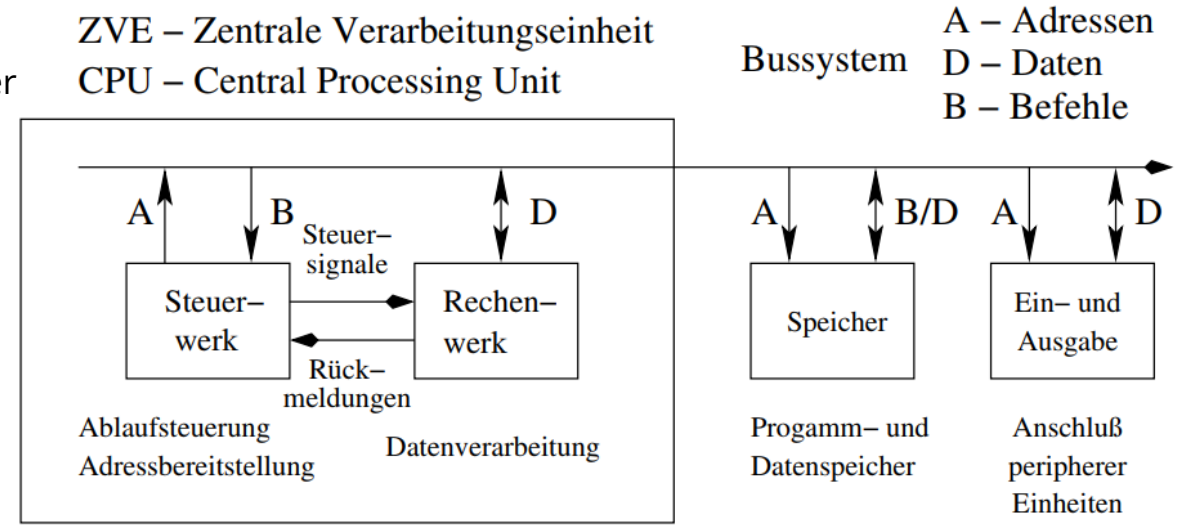
- Schutz von Inhalten und Dateisystemberechtigungen von Systemdateien und –verzeichnissen
- Schutz von Prozessen gegen Code-Injection, Laufzeitanbindung (wie Debugging) und Dtrace
- Schutz vor unsignierten Kernel-Erweiterungen ("kexts").

# Computersysteme und Datenträgertechnik

# Grundlegender Aufbau eines Computers

Grundprinzipien:

- Rechner besteht aus Hauptspeicher, Steuereinheit, Recheneinheit, Ein- und Ausgabe-Einheiten, Langzeitspeicher
- Systembus verbindet die Einheiten
- Programmsteuerung (Rechnerstruktur ist unabhängig von konkreter Aufgabe)
- Hauptspeicher enthält sowohl Daten als auch Programme




- nach John von Neumann benannt
- grundlegendes Modell eines Universalrechners
- arbeitet nach Master-Slave-Prinzip

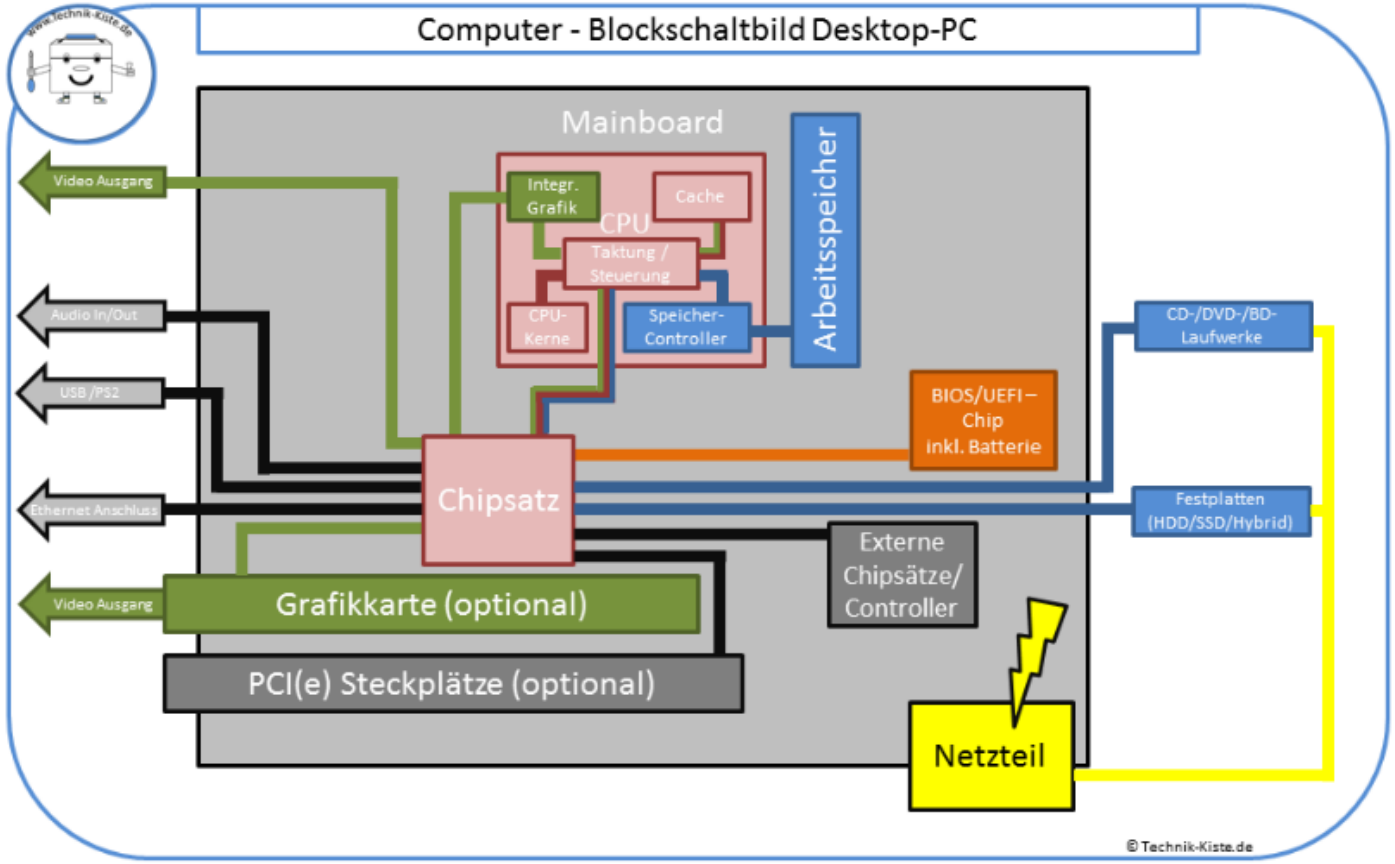
# Grundlegender Aufbau eines Computers

Von-Neumann-Architektur – Verarbeitungsprinzip

- Hauptspeicher besteht aus fortlaufend nummerierten Speicherplätzen. (je 1 Byte) Adresse: Nummer eines Speicherplatzes
- Programm ist eine Folge von Maschinen-Befehlen, die sequentiell (der Reihe nach) ausgeführt werden.
- Abweichung von der sequentiellen Programm-Ausführung ist durch Sprungbefehle möglich, dadurch wird die Programm-Ausführung an anderer Stelle fortgesetzt.
- Daten und Programme werden binär codiert, Zahlen werden dual dargestellt

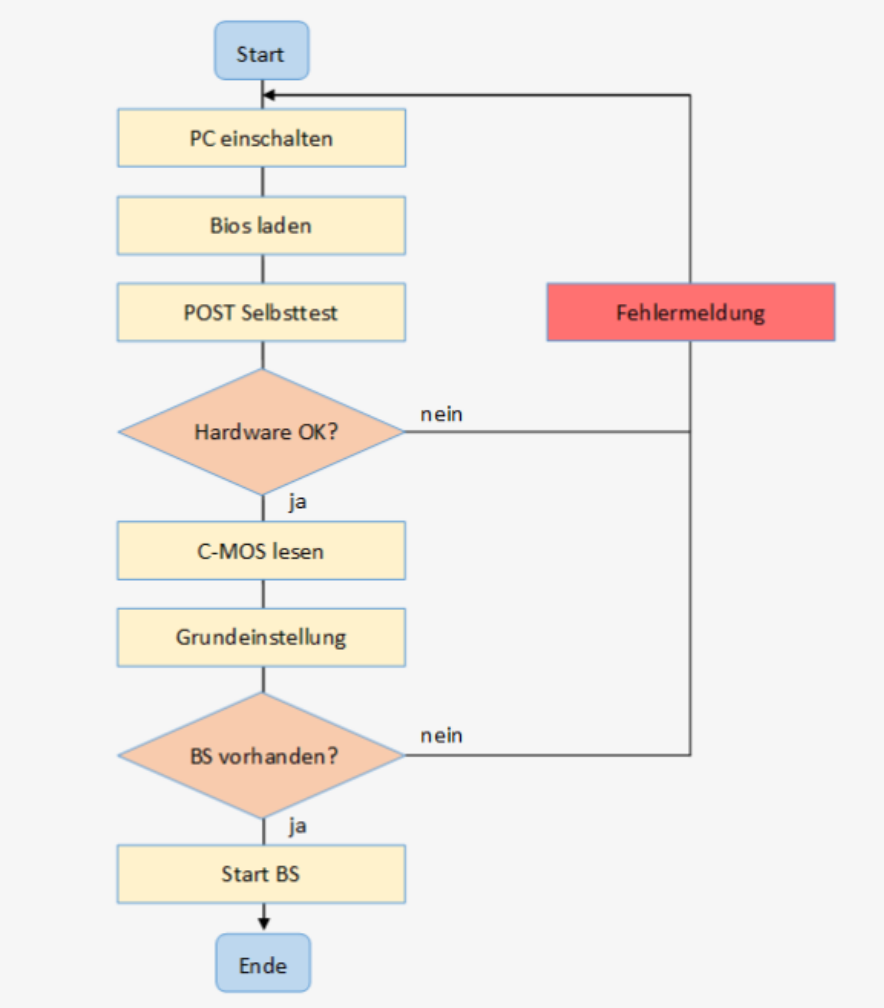
# Grundlegender Aufbau eines Computers

- Prozessor (CPU – Central Processing Unit)
- Mainboard (Hauptplatine)
- Optisches Laufwerk (optional)
- Festplatte
- Hauptspeicher
- Display/Monitor
- Maus, Tastatur

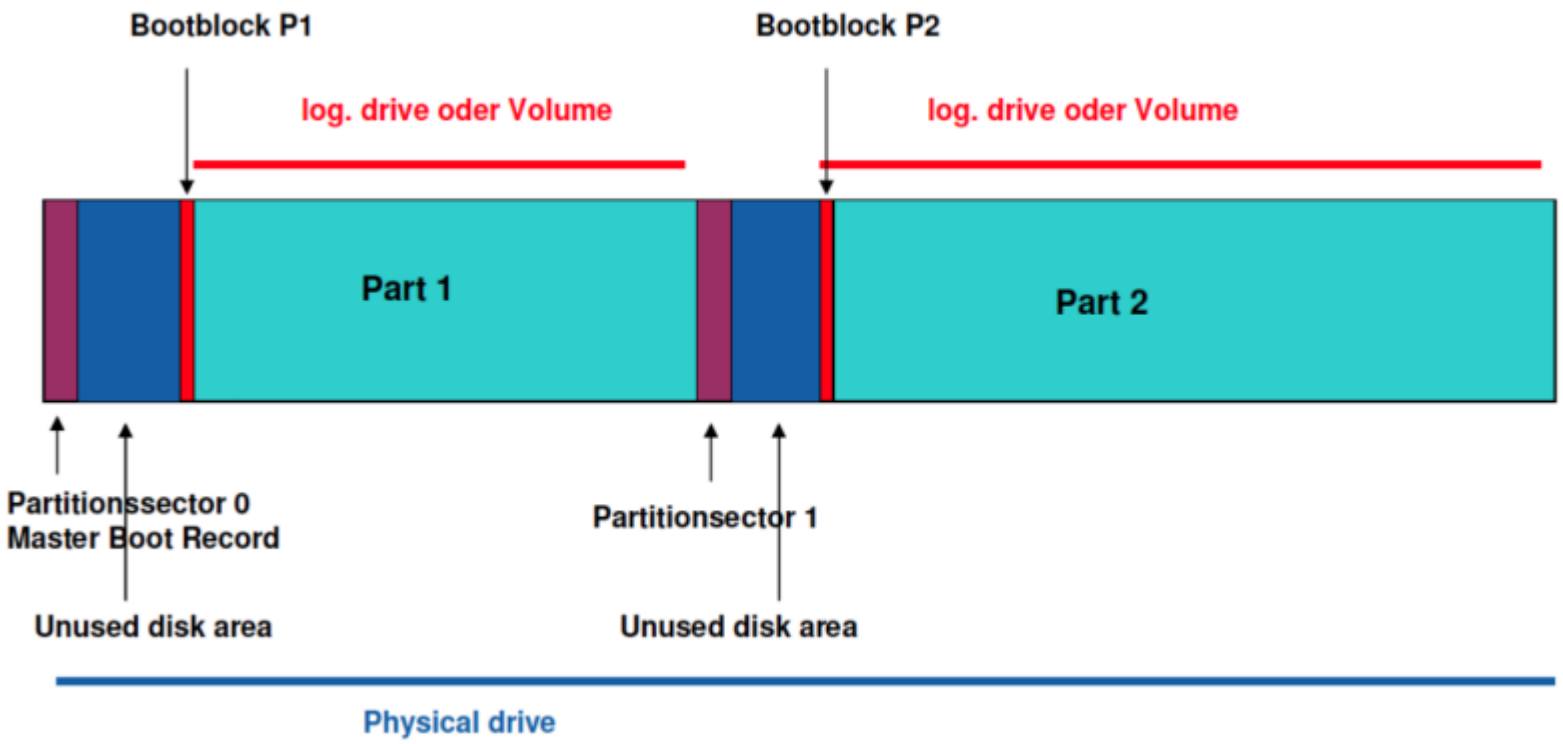


# Ablauf des Bootvorgangs

- Mehrstufiger, aufeinander aufbauender Vorgang → macht Computer arbeitsfähig
- Firmware (BIOS oder UEFI)
- Schritt 1: Aufruf des BIOS (Basic Input Output System)
- Bios stellt die klassische Variante dar
- Extensible Firmware Interface (EFI), bzw. Unified Extensible Firmware Interface (UEFI) als Nachfolger

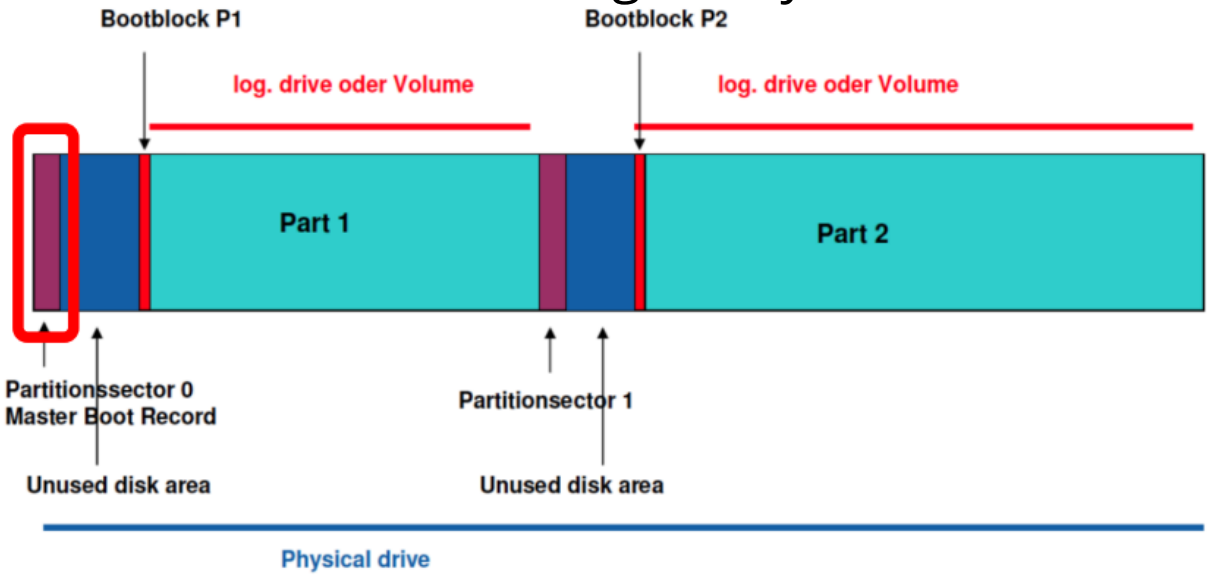


# Technischer Aufbau von Festplatten



# Grundlagen der Partitionierung

- Sektor: kleinste in einem Zugriff les- und schreibbare Einheit
- Partition: Unterteilung des Speicherplatzes eines Datenträgers in logische Bereiche
- Anwendung:
  - Exklusive Zuweisung von Speicherbereichen für Anwendungen / Systemen
  - Daten- / System-Sicherheit
  - Backup / Recovery
  - Multi-Boot Systeme



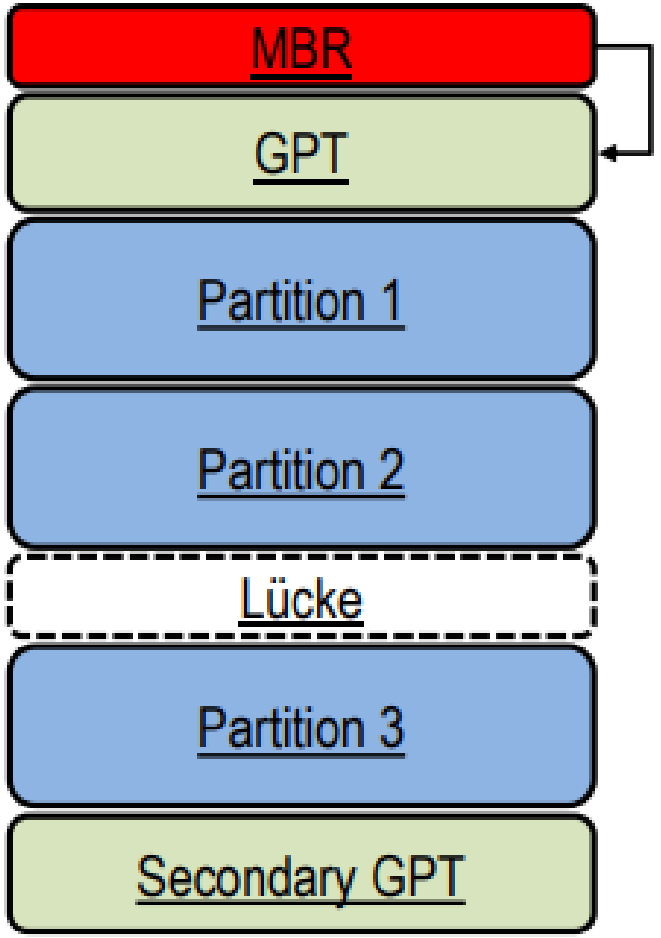
# Master Boot Record (MBR)

- Die ersten 512 Bit einer Festplatte (erster Sektor)
- Für den Boot- und Startvorgang externe Speichermedien
- Informationsquelle:
  - Bootloader/Startprogramm
  - Datenträgersignatur
  - Partitionstabelle
  - Bootsektorsignatur

| Adresse | | Funktion / Inhalt | | Größe (Bytes) |
|---|---|---|---|---|
| hex | dez | | | |
| 0x0000 | 0 | Startprogramm (Master Boot Code / Bootloader) | | 440 |
| 0x01B8 | 440 | Datenträgersignatur | | 4 |
| 0x01BC | 444 | Null (0x0000) | | 2 |
| 0x01BE | 446 | Partitionstabelle | | 64 |
| 0x01FE | 510 | $55_{hex}$ | Bootsektor-Signatur (wird vom BIOS für den ersten Bootloader geprüft) | 2 |
| 0x01FF | 511 | $AA_{hex}$ | | |

# GUID Partition Table (GPT)

- Global Unique Identifier Partition Tabel
- Löst Probleme des MBR (begrenzte Größe, Partitionsanzahl)
- Enthält Sicherungen der Partitionstabellen (verbesserte Integrität)



# RAID

- RAID = Redundant Array of Independent Disk
- Methode zur Speicherung von Daten auf Festplatten
- Schutz vor Hardwareausfall durch Redundanzen
- Zusammenfassen von Festplatten zu Gruppen die unteranderem Datenkopien beinhalten
- Techniken: Mirroring, Striping, Parität

# RAID

Hardware-RAID

- Arbeit wird hierbei vom Raid-Controller übernommen
- CPU wird nicht durch Berechnungen des RAIDs belastet

Vorteile:

- Steht bereits beim Booten zur Verfügung
- Unterstützt eine Vielzahl von Betriebssystemen
- Hohe Performance
- Niedrige CPU-Last am Host

Nachteile:

- Hohe Anschaffungskosten
- Betriebssystemabhängig

Software-RAID

- Kein separater RAID-Controller benötigt
- Preisgünstiger als ein Hardware-RAID
- Kann unter anderem direkt unter Windows erstellt werden

Nachteile:

- schlechtere Gesamtperformance durch höherer CPU-Belastung

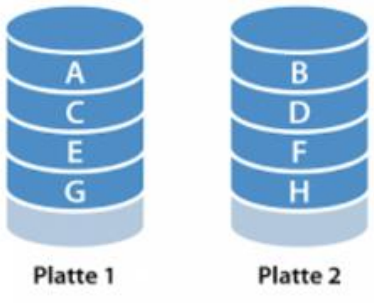
# RAID – Techniken

## Mirroring

schreibt Daten gleichzeitig auf zwei Laufwerke

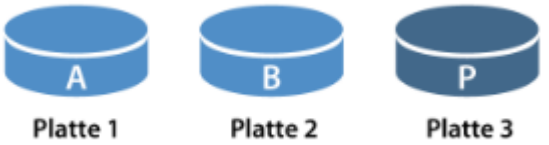

## Striping

Daten auf die verfügbaren Laufwerke in Blöcken (Streifen) verteilt




## Parität

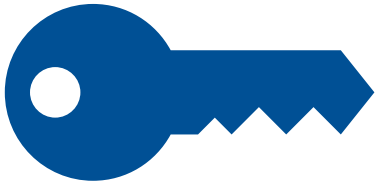
Ist eine Summenverknüpfung mit der man Verlorene Daten wiederherstellen kann ( und Kontrolle bei Veränderung)



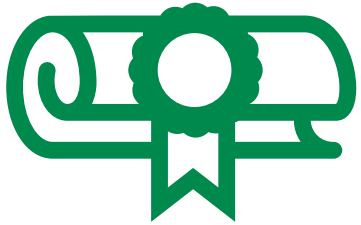

Je nach RAID-Level werden die Techniken kombiniert!

# Kryptologie

# Einführung



Kryptologie = Lehre von den Geheimschriften zur Verschlüsselung (Kryptografie) und Entschlüsselung (Kryptoanalyse)



Griech. „kryptos“ für verborgen und „logos“ für Lehre

# Aufgaben

Allgemeine Aufgaben der Kryptografie:

1. Geheimhaltung (Datenschutz)

   Lesen der Nachricht für Unbefugt nicht zulassen oder sehr schwierig zu machen.

2. Authentifizierung

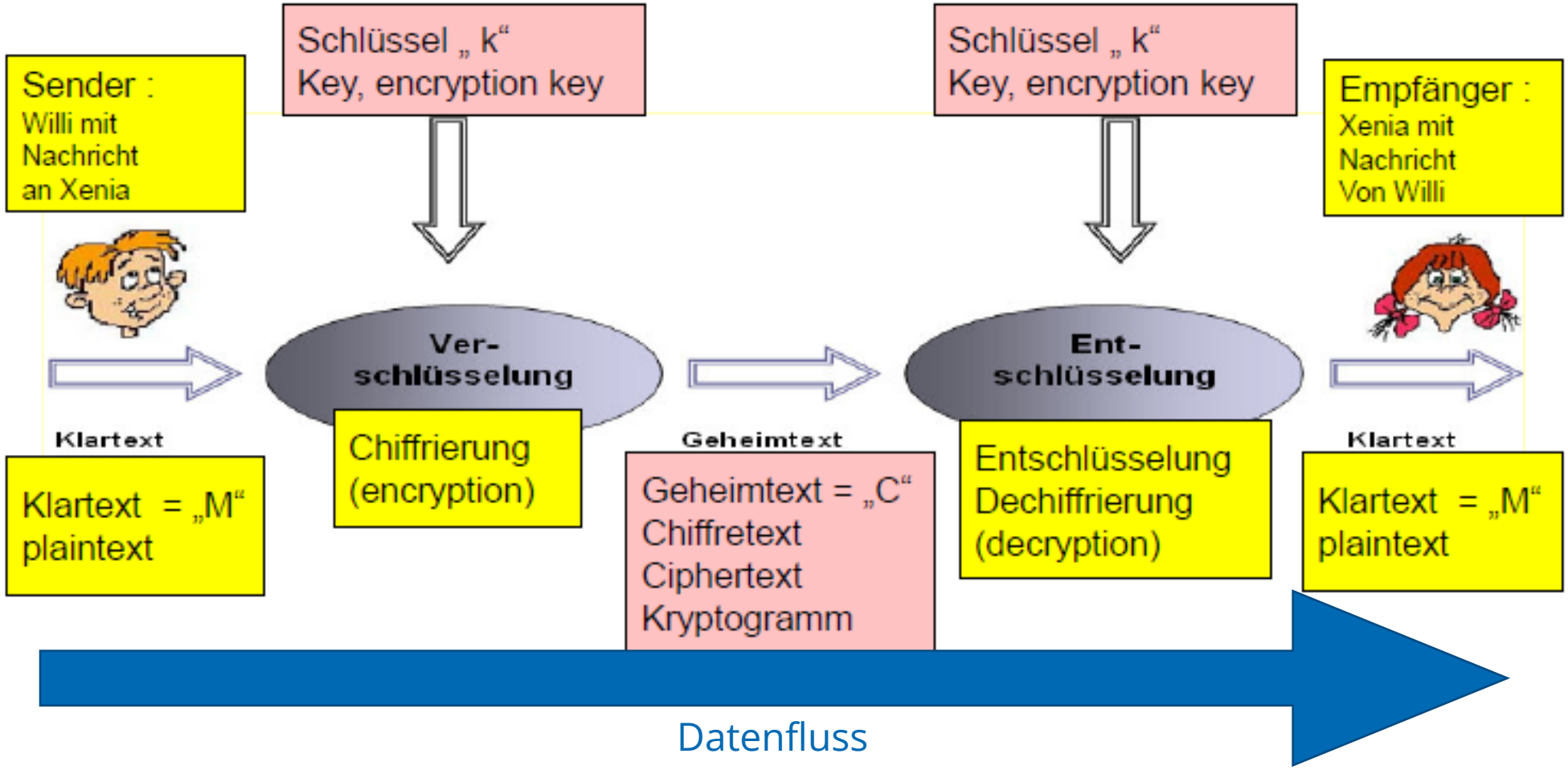
   Identitätsbeweis einer Person oder eines Kommunikationsteilnehmers gegenüber einem anderen Kommunikationsteilnehmer oder Nachweis des Ursprungs einer Nachricht

3. Integrität

   Nachweis der Unverändertheit der Nachricht, Nachricht darf nicht verändert werden

4. Anonymität

# Begriffe und Ablauf



# Verschlüsselungsverfahren

## Symmetrische Verschlüsselung

- Schlüssel zum ver- und entschlüsseln ist gleich
- Kommunikationspartner müssen gleiches Verfahren und gleichen Schlüssel nutzen
- Schlüssel muss geheim sein
- Beispiele: Rivest-Chiffre (RC4) und Advanced Encryption Standard (AES)

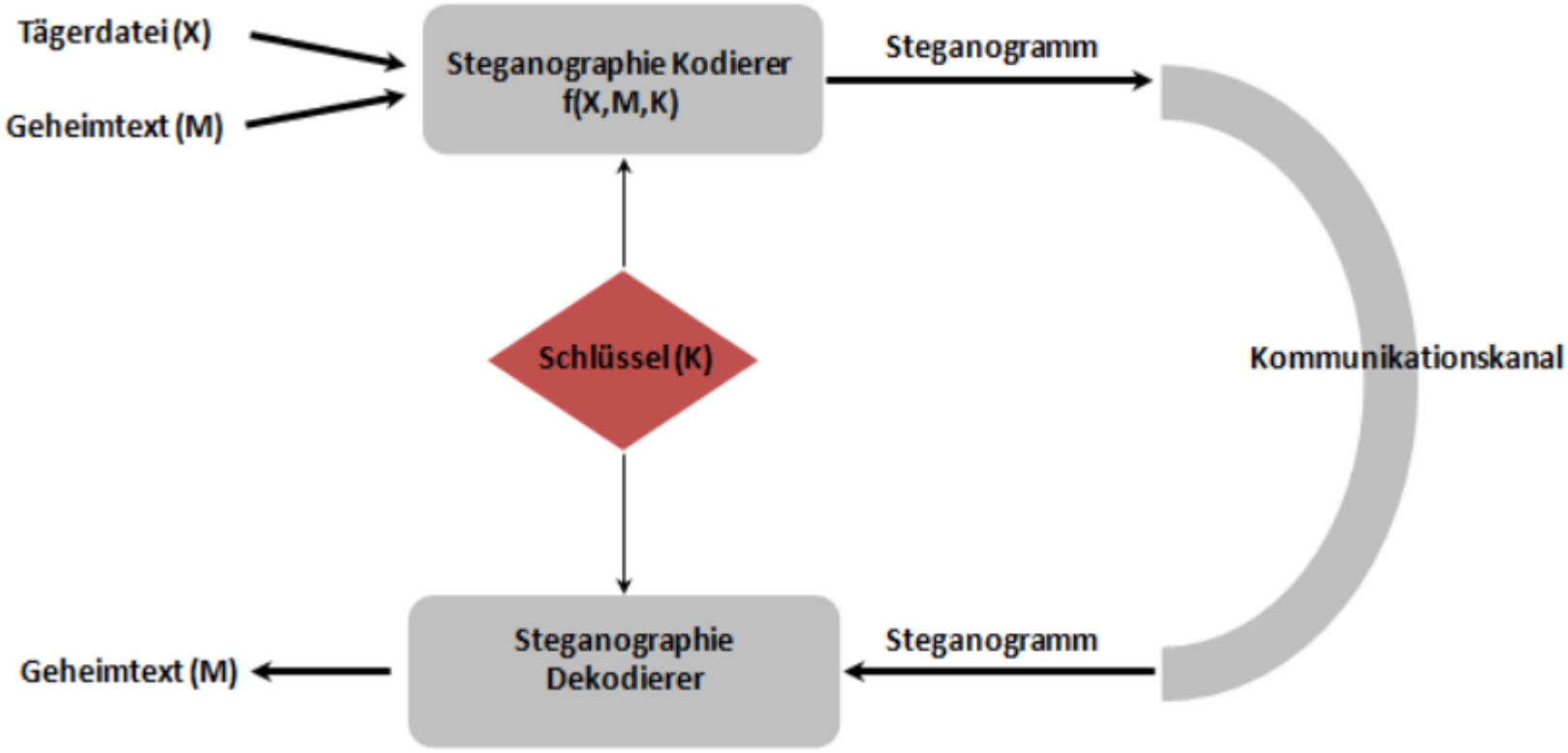
## Asymmetrische Verschlüsselung

- Schlüssel zum ver- und entschlüsseln unterschiedlich
- Basis der Public-Key-Verfahren
- Beispiele: Rivest Shamir Adleman (RSA) und Elliptic Curve Diffie-Hellman (ECDH)

# Hash-Funktion

- Einwegfunktion, die einen Eingaberaum beliebiger Größe in einen Ausgaberaum fixer Länge transformiert
- beliebige Eingabe (Datei, Datenstrom,...) wird zu einem digitalen Fingerabdruck fester Länge zusammengefasst.
- Algorithmus arbeitet stets deterministisch (gleich) und liefert immer das gleiche Ergebnis bei gleicher Eingabe
- Abbildung mit möglichst großen Abbildungsraum (Vermeidung von Kollision)

# Steganografie



# Erster Angriff

# Strategische Vorbereitung

- alle Maßnahmen die vor dem Eintreten eines Ereignisses geplant werden.
- Beispiel: Auswahl und Test verschiedener Sicherungstools, Erstellen einer Vorgehensplanung, Vorbereiten von Hardware und Software(Werkzeug, Computer).

# Operative Vorbereitung

Alle Maßnahmen die nach dem Eintreten des Vorfalls und vor der Datensammlung erfolgen.

z.B. die Suche, Identifikation und Beschriftung der in Frage kommenden Datenquellen (Computer, Handys, USB-Sticks, externe Festplatten, aber auch RAM, Routerkonfigurationen, Netzwerkstati, Logfiles, ...) und die Auswahl der geplanten Sicherungsmittel (Tools und Zieldatenträger).

# Priorisierung

- Alles sichern was später wichtig sein könnte
- Viele Einzelschritte
- Flüchtigkeit von Daten
- → Priorisierung der Daten

# Priorisierung:

1. CPU-Register, Cache-Speicher
2. Routingtabellen, ARP-Cache, Prozessliste, Netzwerkstatus, Kerneldaten, Hauptspeicherinhalt
3. temporäre Dateisysteme, SWAP-Bereiche, andere temporäre Daten
4. Massenspeicherinhalte (logisch oder physikalisch)
5. Auf anderen Systemen verfügbare Log- und Monitoringdaten des untersuchten Systems
6. Physikalische Konfiguration, Netzwerkkonfiguration
7. Archivierte Medien (Datensicherungen)

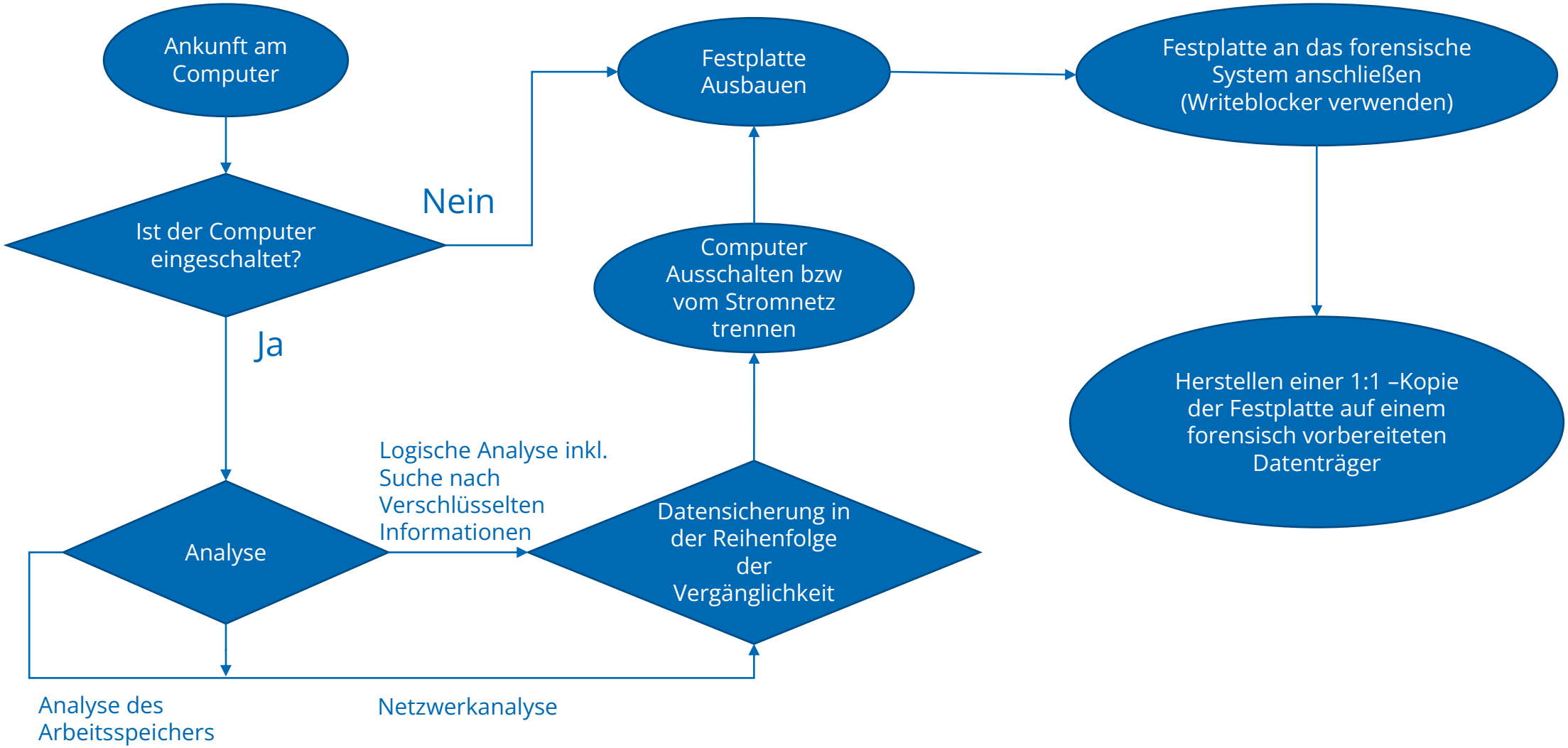
# Datenintegrität

Technische Daten sind leichter Veränder- und Manipulierbar

- Veränderungen von Digitalenspuren sind leichter durchführbar und schwerer nachweisbar.
- Um die Datenintegrität zu gewehrleisten werden mehrere Kopien erstellt. Dabei wird die Urkopie archiviert.
- Um Datenveränderungen zu vermeiden sollte wo immer es möglich ist ein Schreibschutzadapter verwendet werden. Ausnehmen sind:
  - laufendes System mit Vollverschlüsselung
  - Sicherung aus Cloud Storage
  - Sicherung aus einem großen Storage
  - Sicherung aus einem Rechenzentrum

  In diesen Fällen sind eine lückenlose Dokumentation und ein Vier-Augen-Prinzip bei der Erstellung der Kopie ratsam.

# Ablaufplan der forensischen Sicherung



# Anforderungen an eine forensische Duplikation

Physische Kopie - Von dem Datenträger muss eine physische Kopie hergestellt werden, d. h. der gesamte Sektorinhalt aller Sektoren des Datenträgers wird in die Datei hineingeschrieben;

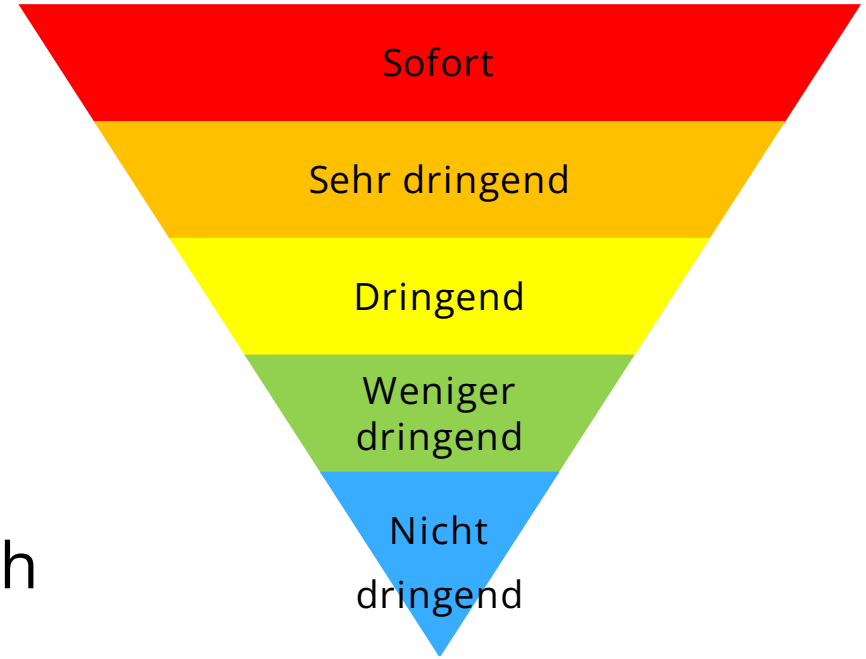
Fehlerbehandlung - Lesefehler müssen eindeutig erkannt und protokolliert werden und durch vorher festgelegte Füllmuster ersetzt werden;

Vollständigkeit des Abbildes - Reservierte Bereiche von Massenspeichern müssen sicher erkannt werden und für den Zeitpunkt der Abbilderstellung deaktiviert werden, um ein vollständiges Abbild zu erhalten;

Unveränderthеit Integrität - Die Erstellung des Abbildes muss mit der Berechnung einer kryptographischen Checksumme abgeschlossen werden, um die Unveränderthеit (Integrität) des Abbildes nachweisen zu können.

# Triage-Forensik

- Definition des Begriffs „Triage“ im medizinischen Sinn
- Selektion Verwundeter hinsichtlich ihrer Überlebenschancen und der Schwere ihrer Verletzungen
- Festlegen der Reihenfolge in der Verletzte zu behandeln sind
- „Priorisierung“
- digitale/forensische Triage: Selektion elektronischer Geräte und Internetquellen nach der Relevanz einer systematischen formalen Untersuchung zur Beweisermittlung



# 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