



Digitale Forensik in der (Unfall-)Analytik

Jana Beyer – DEKRA Niederlassung Chemnitz



Vielfalt
Relevanz
Qualität
Zugänglichkeit
der Daten

Bildverarbeitung

Motivation – Typische Fragestellungen in der Unfallanalyse

Wachsende Rolle der Digitalen Forensik



Ablenkung

Smartphone/Smartwatch

Display aktiv, Telefonat, Nachrichten, Navigation?

Position

Wo befanden sich die Beteiligten vor der Kollision?

Fahrverhalten

Bremmung, Ausweichen, Beschleunigung?

Sichtbarkeit

Licht, Tageszeit, Witterung?

Geschwindigkeit

Wie schnell fuhren die beteiligten Fahrzeuge?

Zeitablauf

Welche Quellen geben Hinweise zur zeitlichen Abfolge?

Vielfalt der Datenträger

im Kontext der Unfall-Rekonstruktion



Fahrrad / E-Bike

Fahrradcomputer, Bordcomputer



Wearables

Sturzereignis · Vitaldaten · Zeitstempel



Smartphone

GPS · Beschleunigung · Notruf · App-Logs · Nutzeraktivität · App-/Clouddaten

Unfall- Rekonstruktion



Speichermedien

SD-Karten · USB · interne Gerätespeicher, GPS-Tracker



Kraftfahrzeugdaten

EDR · Assistenzsysteme · Infotainment · CAN-Daten



Bild- und Videodaten

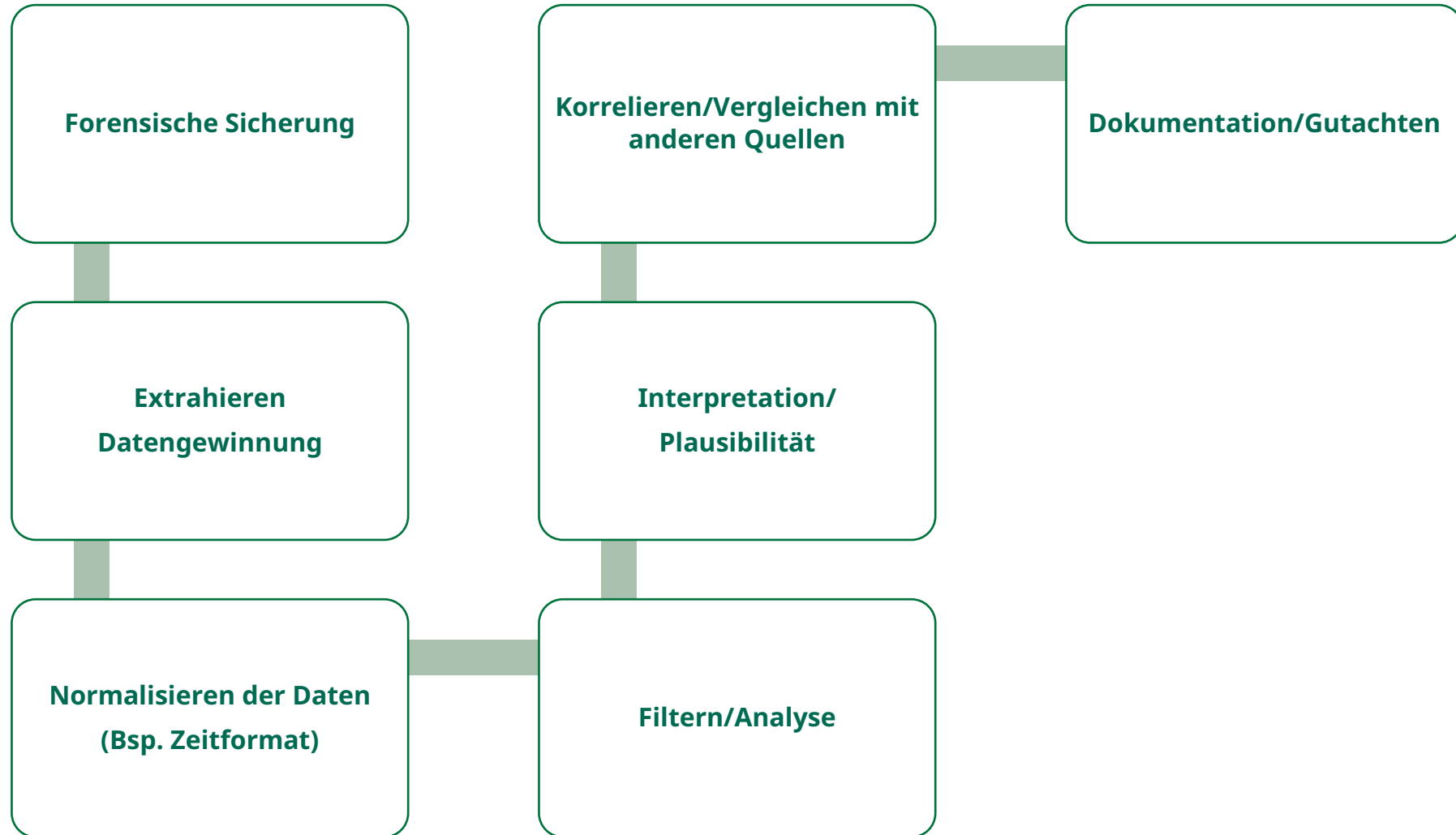
Dashcam Helm-/Actioncam, Videoüberwachungsanlagen im Umfeld

Mehr Quellen durch digitale Datenträger

→ präzisere Zeit-/Orts-/Bewegungsanalyse → effizientere Rekonstruktion

Von der Sicherung zum Gutachten

Prozesskette



Möglichkeiten der Datensicherung

Methoden



Auslesen über die vorhandene Schnittstelle

Spezifische Hardware & Software

Möglichkeiten der Datensicherung

Auslesen über die vorhandene Schnittstelle



Hardware

Schreibblocker,
spezifische Platinen,
Adapter

Software

Cellebrite, XWays, Open
Source, Python
MOBILedit, etc.



Vorteil: zerstörungsfrei

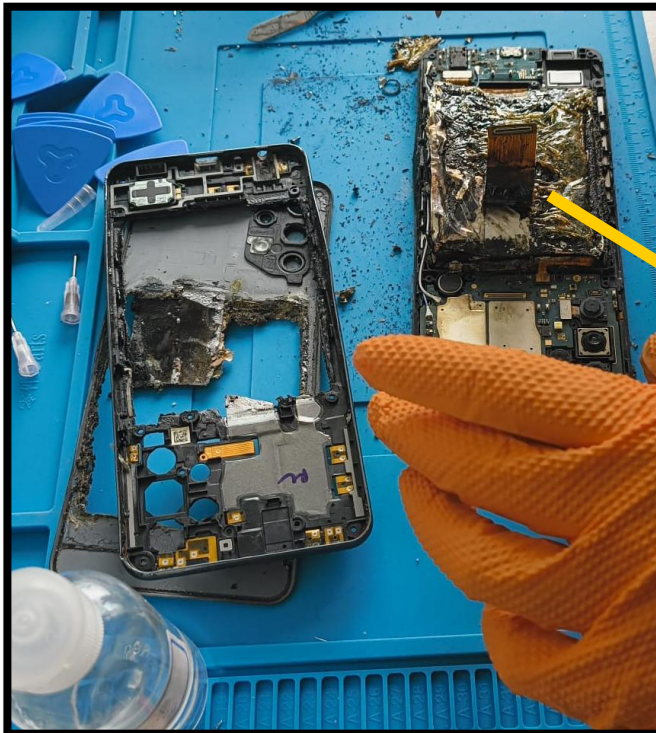


Tausch von Hardwarekomponenten

- Displays
- Akkus
- Ladeeinheiten
- Geräte

Möglichkeiten der Datensicherung

Tausch von Hardwarekomponenten





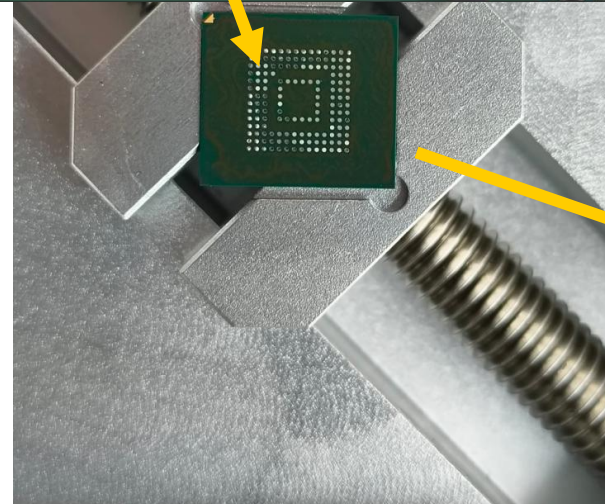
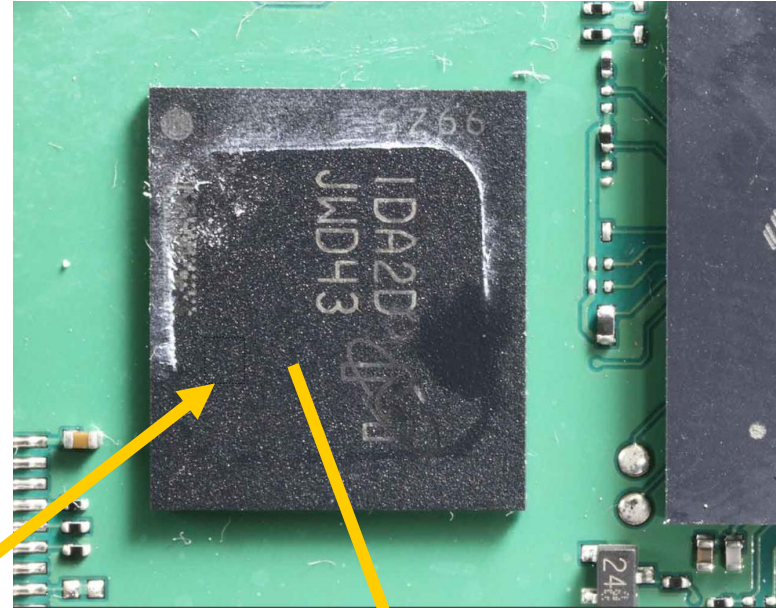
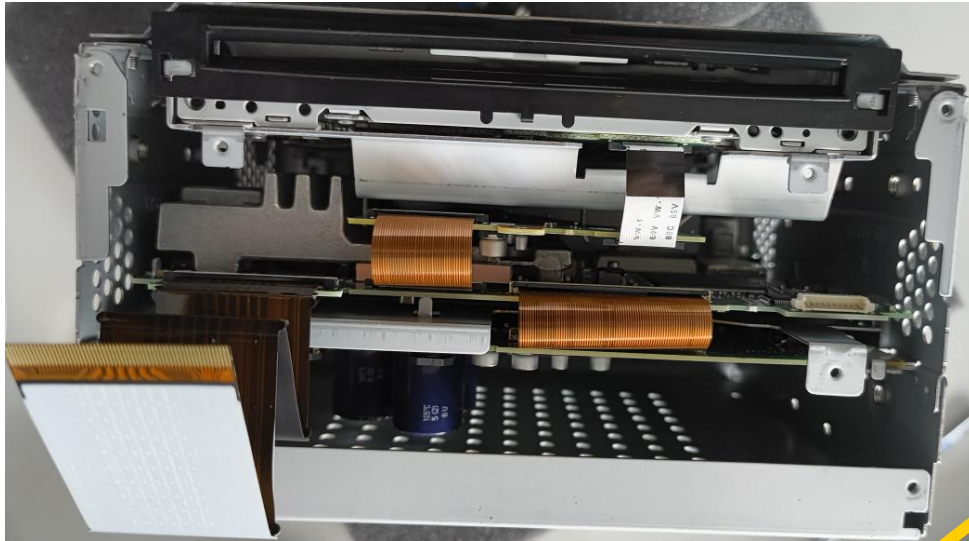
Chip-off

- Auslesen der Rohdaten

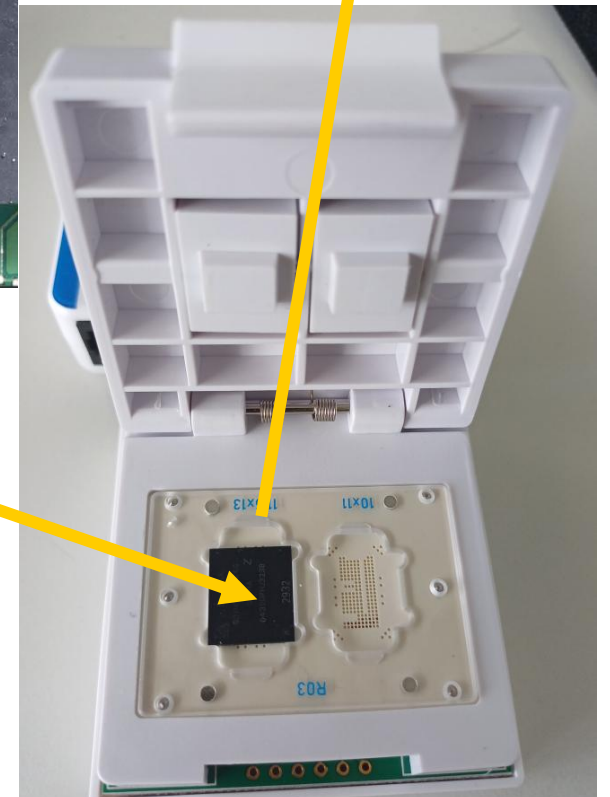
- kein Zugang über Softwareschnittstelle
- defekte Geräte

Möglichkeiten der Datensicherung

Chip-Off

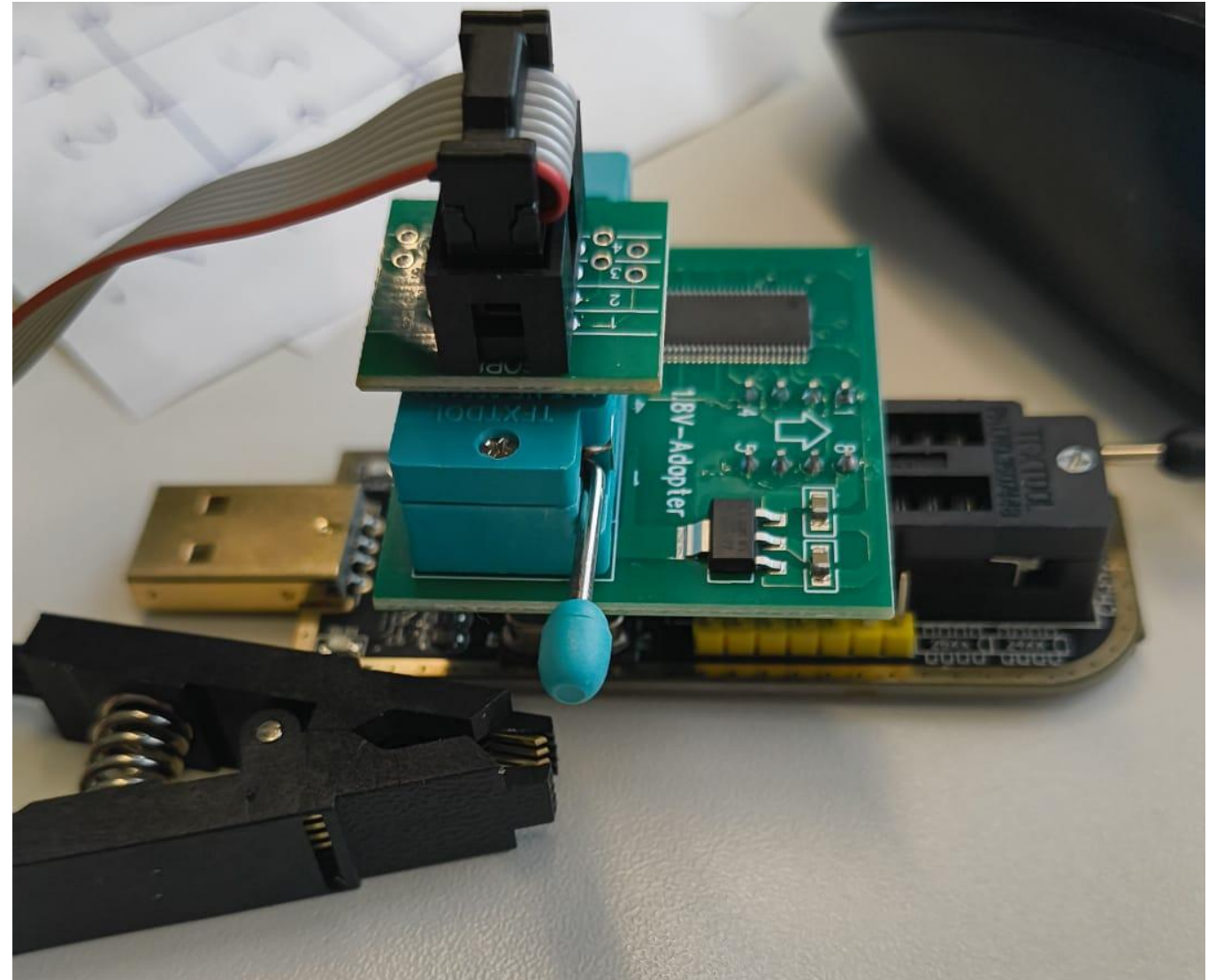
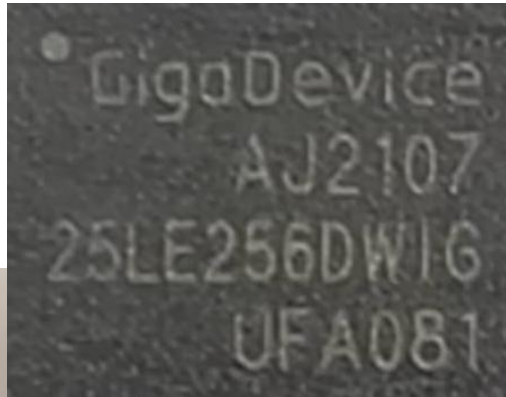


Einlesen der Daten in Berla



Möglichkeiten der Datensicherung

Chip-Off



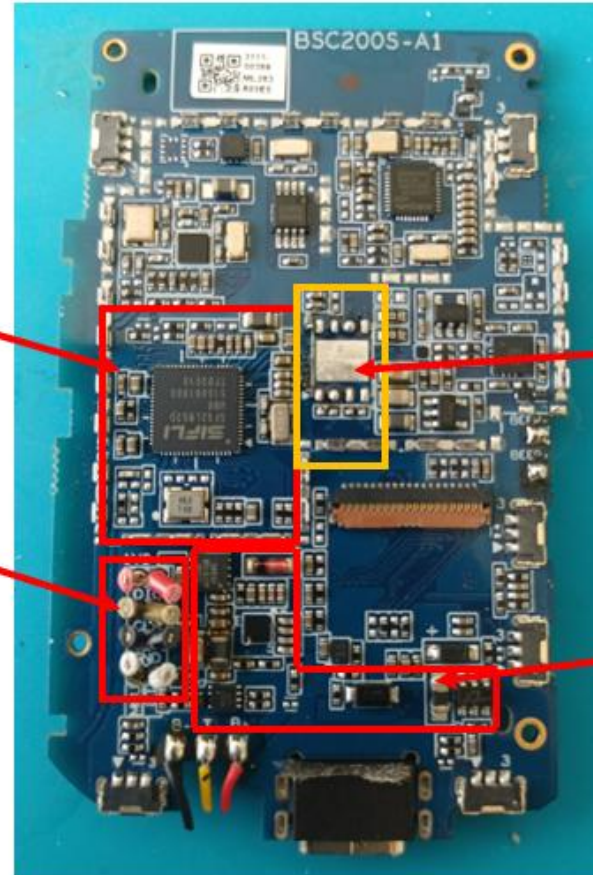
Möglichkeiten der Datensicherung

Chip-Off



Prozessor

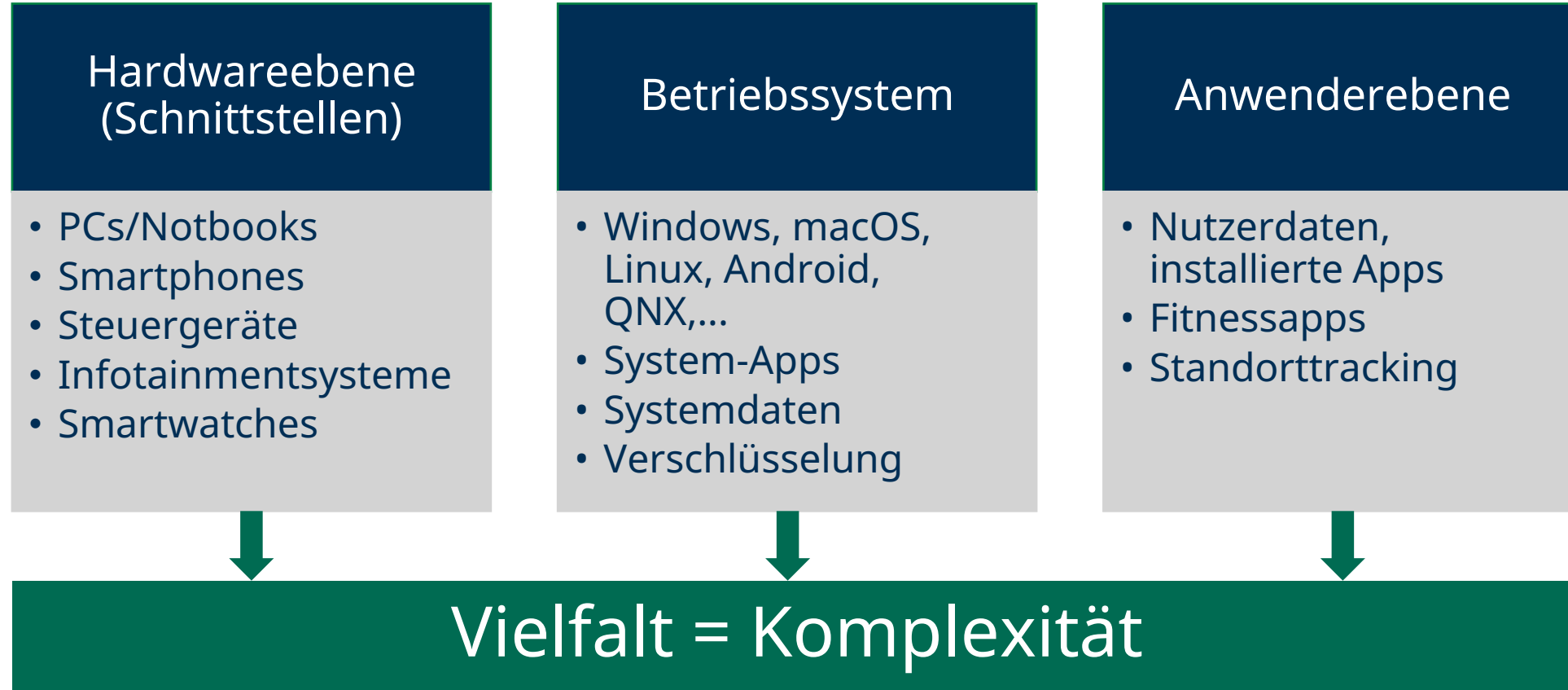
JTAG
Interface



Speicherchip

Ladeelektronik und
Spannungswandler

Ebenen der Datensicherung



Herausforderungen

Zugänglichkeit & Qualität der Daten



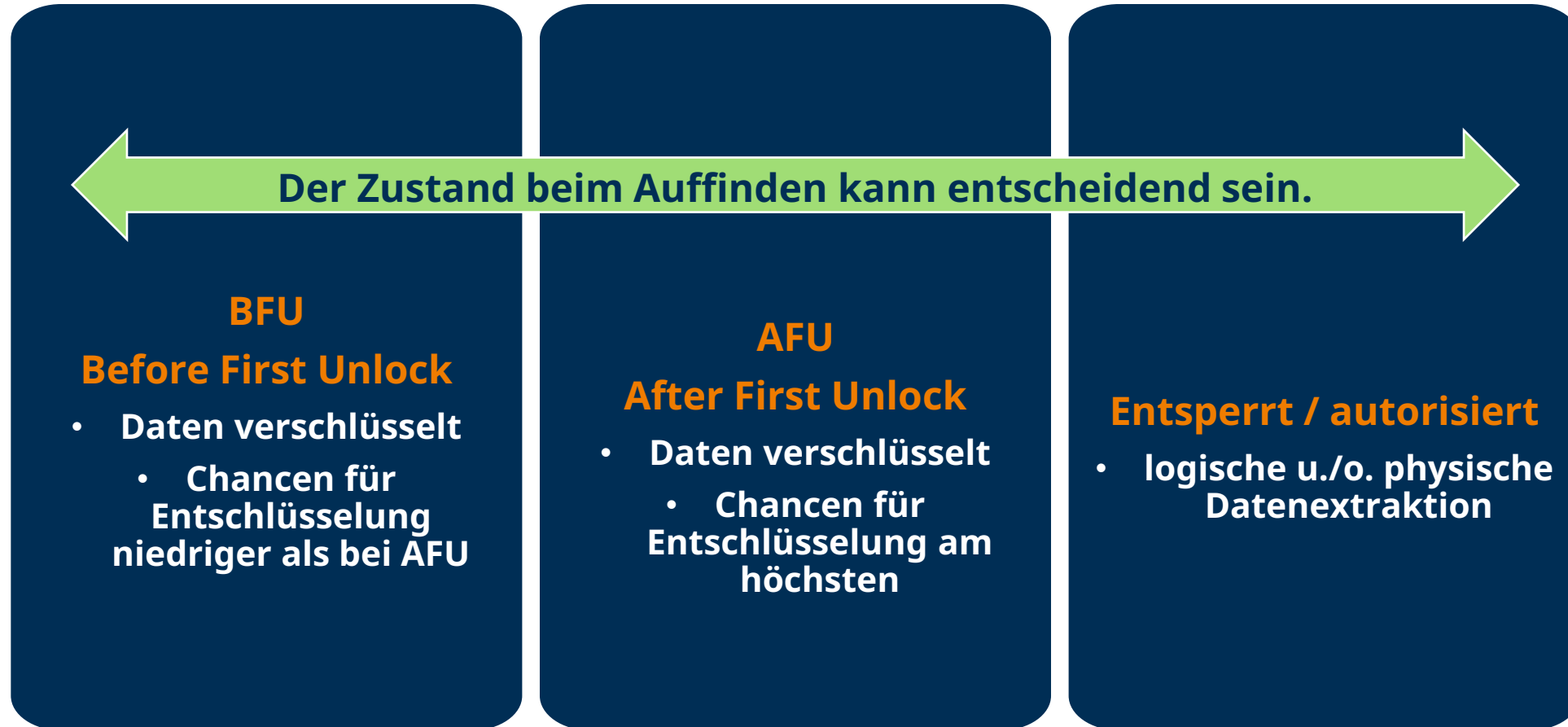
FDE – File Disk Encryption
FBE – File Based Encryption
BFU – Before First Unlock
AFU – After First Unlock



Zugriff auf externe Daten benötigt richterlichen Beschluss

Beispiel Cloud, E-Mail-Konten

Ausnahme/Grauzone: Daten sind über App auf Smartphone durch Starten ohne Eingabe von Zugangsdaten zugänglich



Herausforderungen

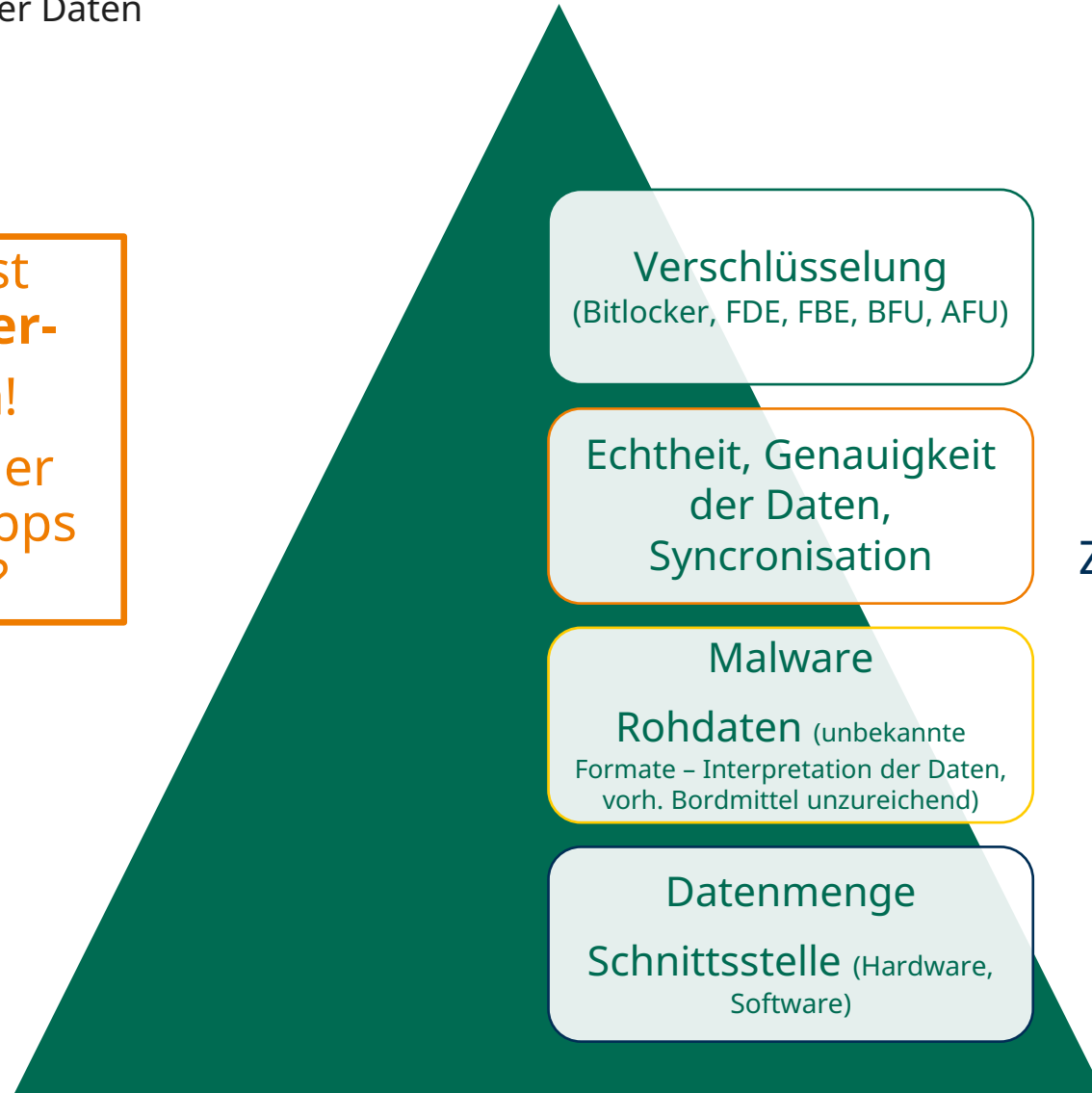
Zugänglichkeit & Qualität der Daten



Entscheidend ist
auch die **Nutzer-
konfiguration!**

Tracking an oder
aus? Welche Apps
sind installiert?

FDE – File Disk Encryption
FBE – File Based Encryption
BFU – Before First Unlock
AFU – After First Unlock



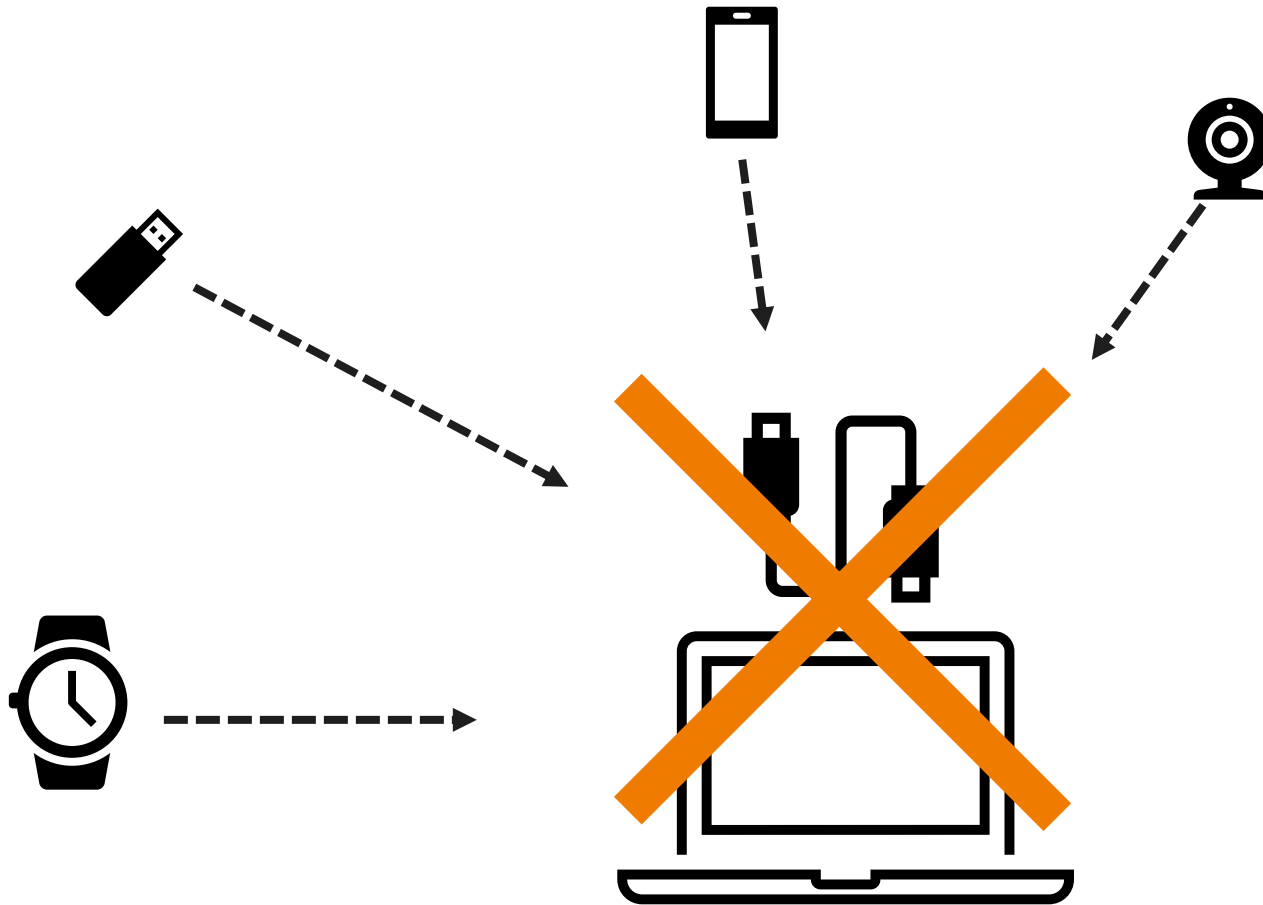
Zugriff auf externe Daten benötigt
richterlichen Beschluss

Beispiel Cloud, E-Mail-Konten

Ausnahme/Grauzone: Daten sind
über App auf Smartphone durch
Starten ohne Eingabe von
Zugangsdaten zugänglich

Qualität der Daten

Sicherung der Daten (am Unfallort)



- Flugmodus, SIM entfernen oder Faraday Bag verwenden
- Smartphone - wenn angeschalten, weiter laden
- Schreibschutz verwenden



Möglichkeit der Vorortsicherung/physisch

- Vorteil: Gerät muss nicht mitgenommen werden,
- funktioniert u.a. bei Festplatten, USB Sticks, Dashcams



Vorteile der forensischen Sicherung

Gerichtsverwertbarkeit - d.h. System/Daten unverändert

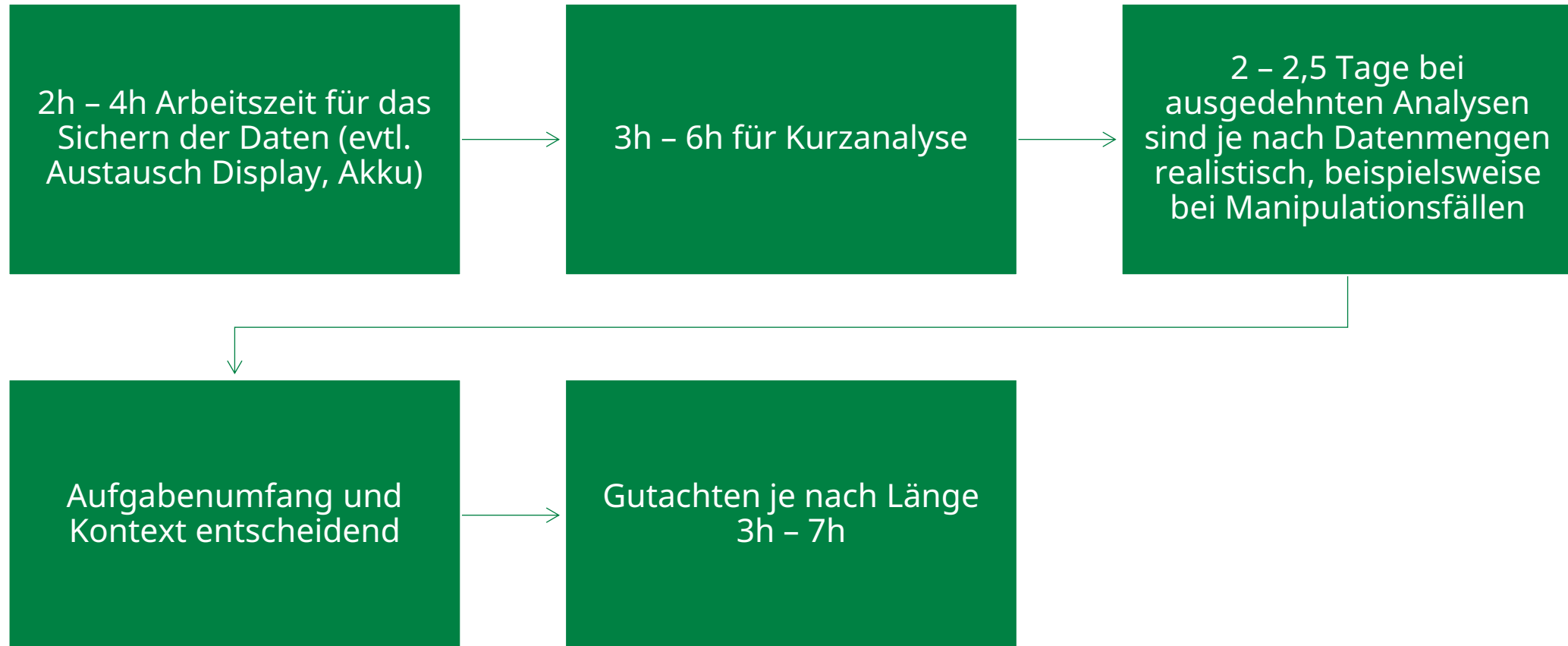
Möglichkeit der Datenwiederherstellung

kein versehentliches Löschen der Daten

(Temporäre/Cache Dateien, Aktualisieren von Datenbanken, Überschreiben, Manipulieren, kein Synchronisieren mit der Cloud)

Aufwände

Smartphone - Analyse





Weitere Praxisbeispiele

TPM – Bitlocker – Was ist das?

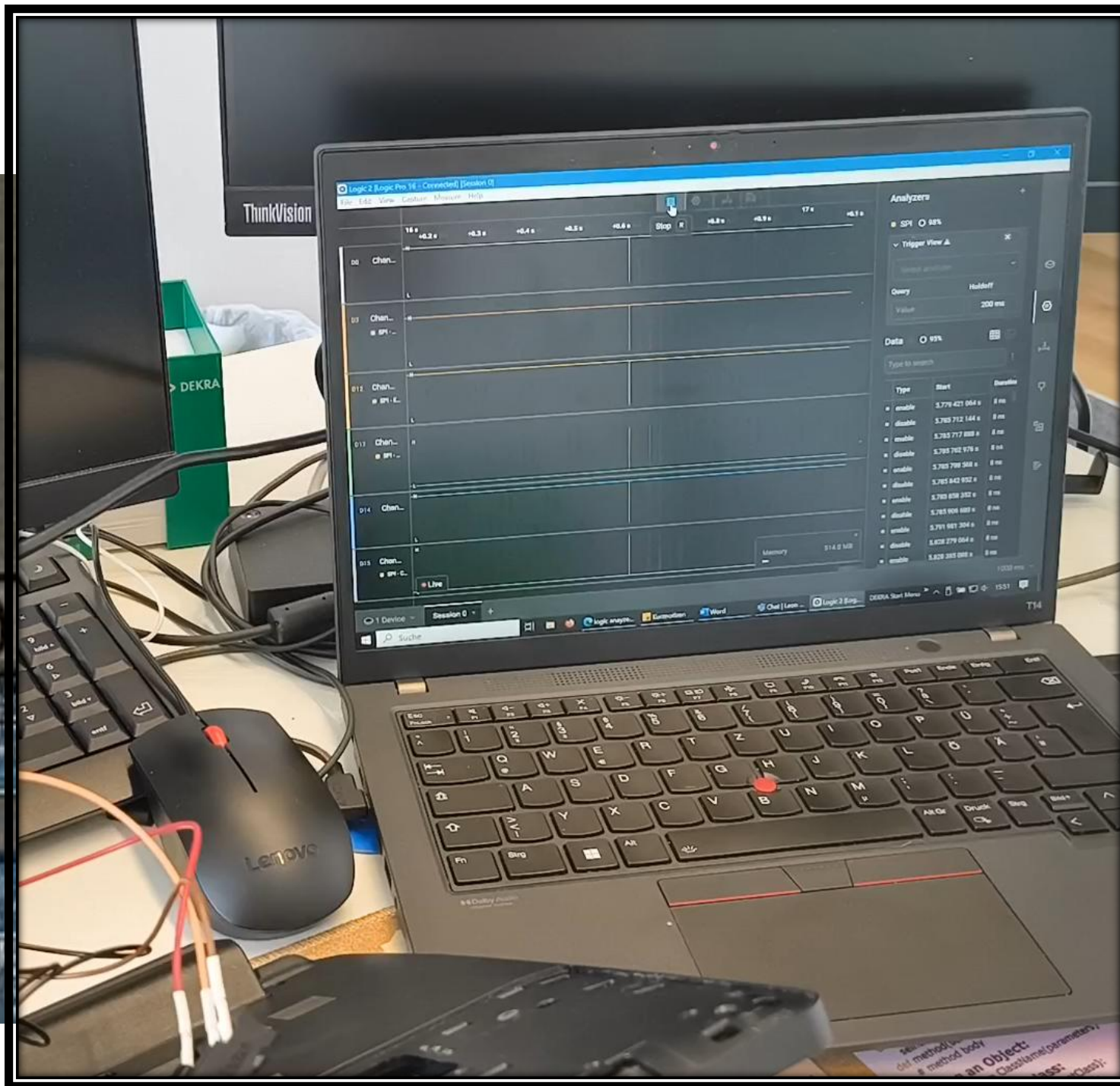
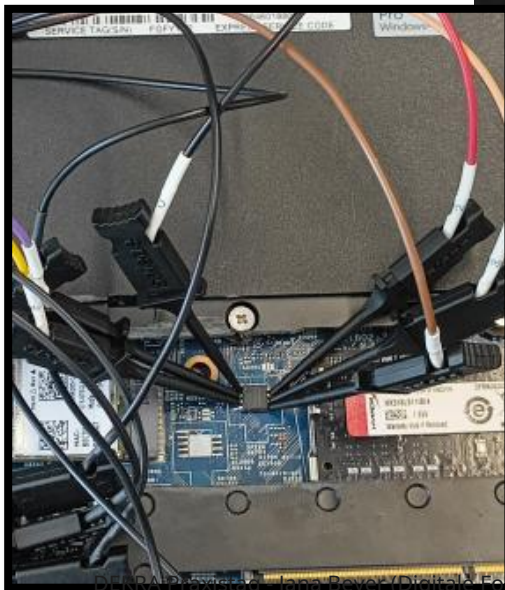
Verschlüsselung von Festplatten



- **TPM** – Trusted Plattform Module (extern/intern)
- **Bitlocker** – Code aus Zahlen und Buchstaben (48 Byte)

Beispiel externes TPM - Modul





Wiederherstellung von Daten

Case Label:

Case Evidence Number:

Summary

Captured Phone Photos

Contacts

Contact List 0

Contact Groups 0

Messages

Conversations 0 conversations, 0 messages

Detailed Messages 0

Organizer

Events 0

Tasks 0

Application List

28

Photos

0

Image Files

4

Audio Files

0

Video Files

0

Documents

3

Files

Misc Files 0 files

Internal Files 515 files

Applications Files 28 files

Activities

User Profiles 1

Activities 200

Activity Records 99805

Activity Laps 1108

Activity Lap Lengths 0

Activity Sets 0

Activity Heart Rates 0

User Weight Scale 0

Monitoring Data 859

Locations

GPS Locations 96679

Activity Routes 187

Routes 0

Tracks 0

Activities (200)

All activities

1 Activity 1 (Gehen)

 Starting Position (Google Maps)	Latitude	51.61691 °
	Longitude	8.89861 °
	Time	2022-01-14 15:33:27 (UTC+1)
 Sport	Walking - Generic	
 Start	2022-01-14 15:33:27 (UTC+1)	
 End	2022-01-14 16:32:40 (UTC+1)	
 Duration	00:59:14	
 Distance	4255.64 m	
 Calories	345 kcal	
 Average Speed	4.313 km/h	
 Top Speed	6.484 km/h	
 Average Heart Rate	109 beats/min	
 Maximum Heart Rate	141 beats/min	
Source File	acquired_data/raw0/GARMIN/Activity/2022-01-14-15-33-27.fit	

2 Activity 2 (Gehen)

 Starting Position (Google Maps)	Latitude	51.61714 °
	Longitude	8.89899 °
	Time	2022-01-16 14:36:56 (UTC+1)
 Sport	Walking - Generic	
 Start	2022-01-16 14:36:56 (UTC+1)	
 End	2022-01-16 16:01:04 (UTC+1)	
 Duration	01:24:09	
 Distance	4859.08 m	
 Calories	417 kcal	
 Average Speed	3.463 km/h	
 Top Speed	6.012 km/h	
 Average Heart Rate	99 beats/min	
 Maximum Heart Rate	133 beats/min	
Source File	acquired_data/raw0/GARMIN/Activity/2022-01-16-14-36-56.fit	

A large, stylized green arrow graphic pointing to the right, composed of two overlapping shapes: a lighter green one in front and a darker green one behind it.

Vielen Dank für Ihre
Aufmerksamkeit