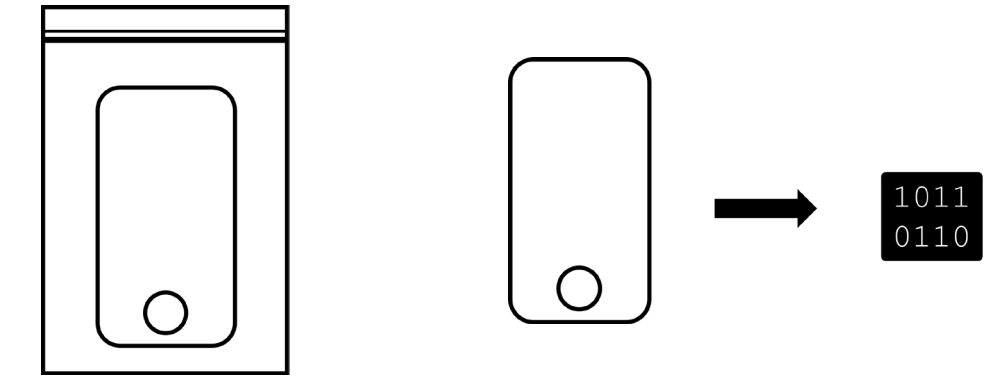


# Angepasster Semesterplan (Versuch)

## Semester-Agenda CF, HS24

	SW 1	SW 2	SW 3	SW 4	SW 5	SW 6	SW 7
Fr 09:05- 11:25	20.09: Einstieg, Der Computer als Spurenquelle		04.10: Sicherung & Acquisition	11.10: PC-Forensik- Tools	18.10: File Systems & Disk Forensik	25.10: Windows	01.11: Allerheiligen
	SW 8	SW 9	SW 10	SW 11	SW 12	SW 13	SW 14
Fr 09:05- 11:25	08.11: Linux	15.11: MacOS	22.11: Office-Files	29.11: Media-Files	06.12: Browser- Artefakte & Netzwerk	13.12: RAM-Forensik	20.12: Encryption



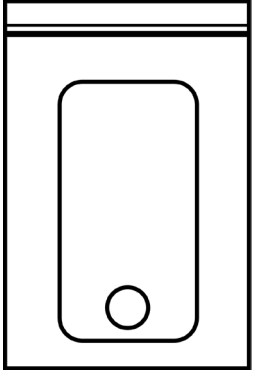
# CF: Sicherung & Acquisition

CF HS23

Dr. Hannes Spichiger

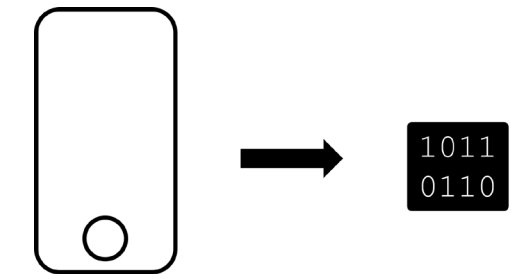
**Departement Informatik**  
21.09.2023

# Sicherung / Preservation



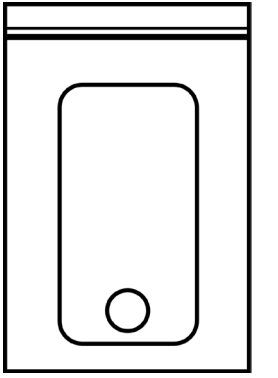
- Sicherstellen, dass sich der Zustand der Spuren nicht mehr verändert
- Dokumentieren des vorgefundenen Zustandes
- Dokumentieren von Umstands-Informationen

# Acquisition



- Erstellen einer Kopie der Daten
- Ab diesem Schritt ist die Analyse unabhängig vom Physischen Gerät
- Macht Arbeiten enorm viel einfacher
- «Save State»

# Sicherung eines PC

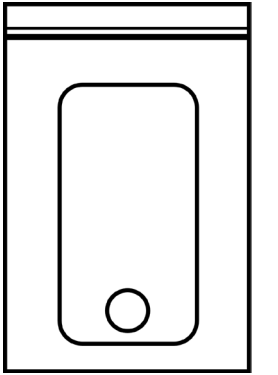


# Sichern eines PC: Flowchart



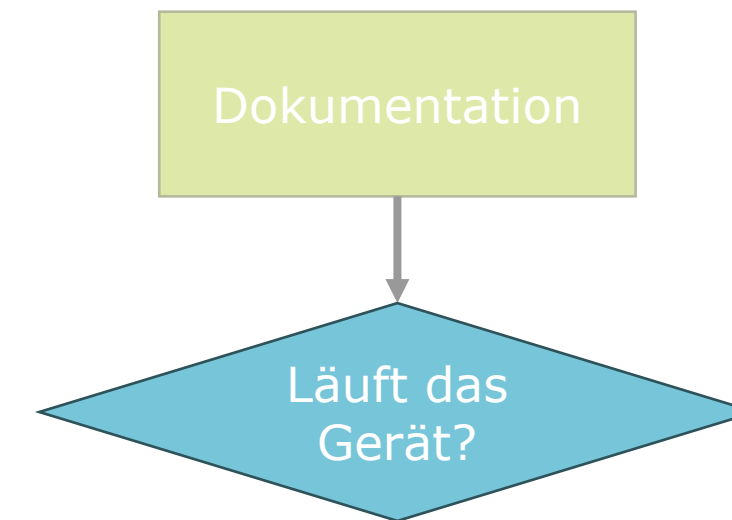
Dokumentation

# Dokumentation: Was dokumentiert ihr bei der Sicherung?



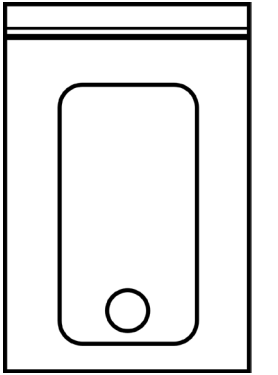
- Beschreibung des Geräts
  - Identifikatoren
- Ort des Geräts
- Zustand des Geräts
  - On / Off
  - Peripherals
  - Netzwerk-Kabel

# Sichern eines PC: Flowchart



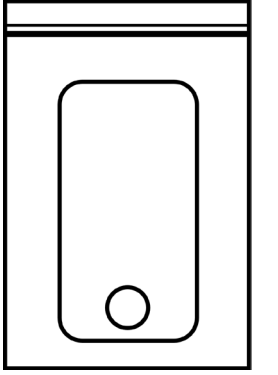


# Läuft das Gerät?



- Bildschirm, Ventilator, Elektronik-Geräusche
- Bewegen der Maus
- Pressen einer Taste wird nicht mehr empfohlen
  - Kann gerät aus Hibernation aufwecken

# Sleep & Hibernation



## Sleep:

- Das Gerät bleibt eingeschaltet
- Das Gerät führt keine Prozesse mehr aus
- Aktuell bearbeitete Informationen befinden sich im Arbeitsspeicher

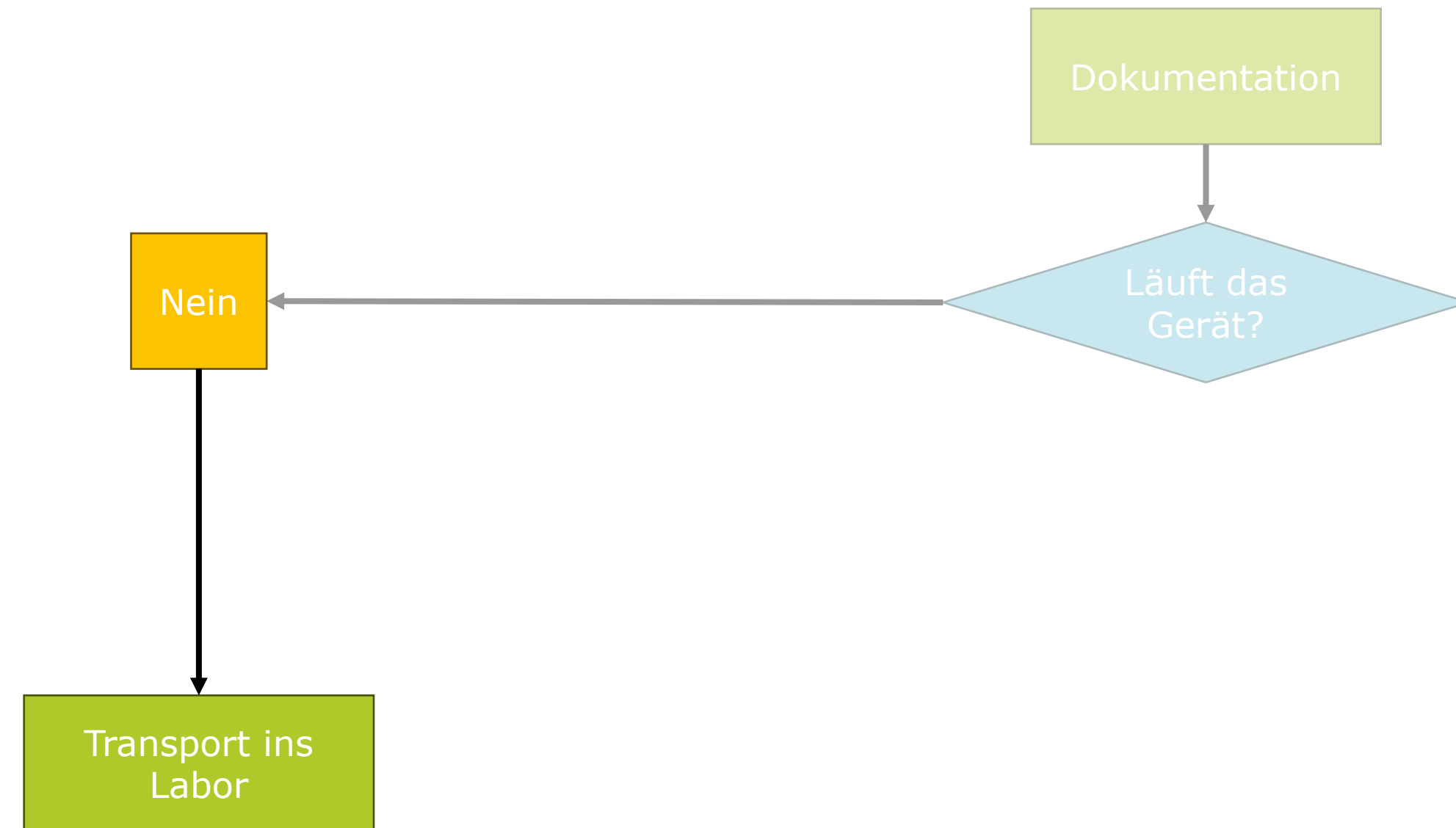
=> Ausschalten führt zu einem Informationsverlust

## Hibernation:

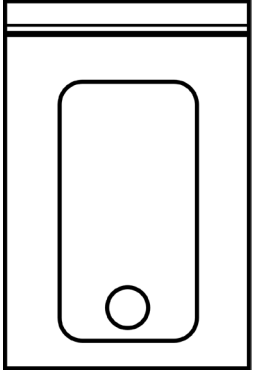
- Der Gerätezustand wird auf der Harddisk gespeichert.
  - hiberfil.sys auf Windows
- Abhängig von Einstellung auf Windows
- Standard auf MacOS

=> Trennen von Stromquelle ändert nichts

# Sichern eines PC: Flowchart

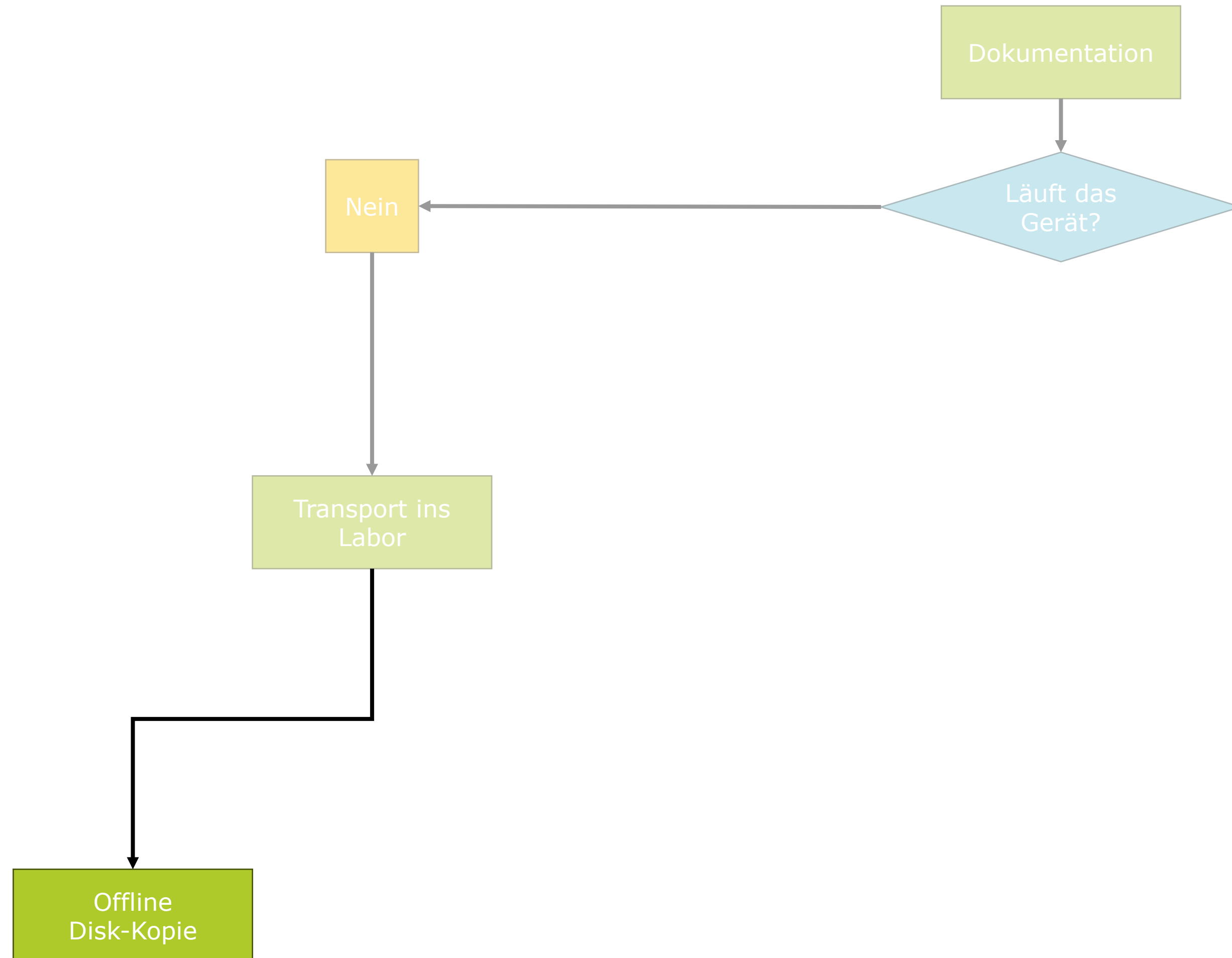


# Transport ins Labor: Was nehme ich mit?

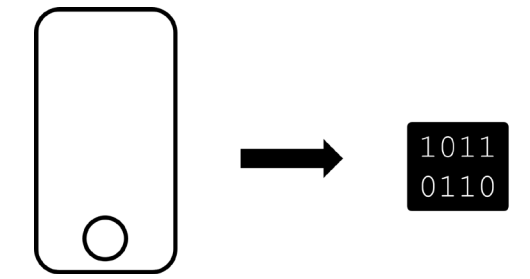


- Laptop: Ladekabel
- Tower:
  - Was habe ich für Equipment im Labor?
  - Mac & Windows Peripherals sind nicht unbedingt kompatibel
  - Insb. Tastatur auf Mac für Tastenkombinationen

# Sichern eines PC: Flowchart

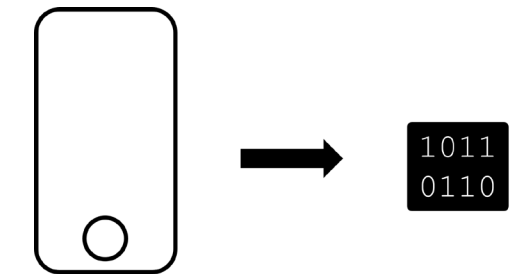


# Erstellen eines Disk-Images



- Wir bauen die Disk aus dem PC aus
- Wir erstellen direkt ein perfektes Abbild des Datenträgers

# Was ist eine Forensische Kopie?



- Ziel: Perfektes Abbild des Datenträgers
  - Mit allen Partitionen
  - Mit allen Zwischenräumen
- Ansatz:
  - Wir lesen jedes Bit des Datenträgers einzeln und schreiben es in unsere Kopie
  - «Bitwise Copy»
- Relativ Zeitaufwändig
- Garantiert dass Kopie identisch ist mit Datenträger

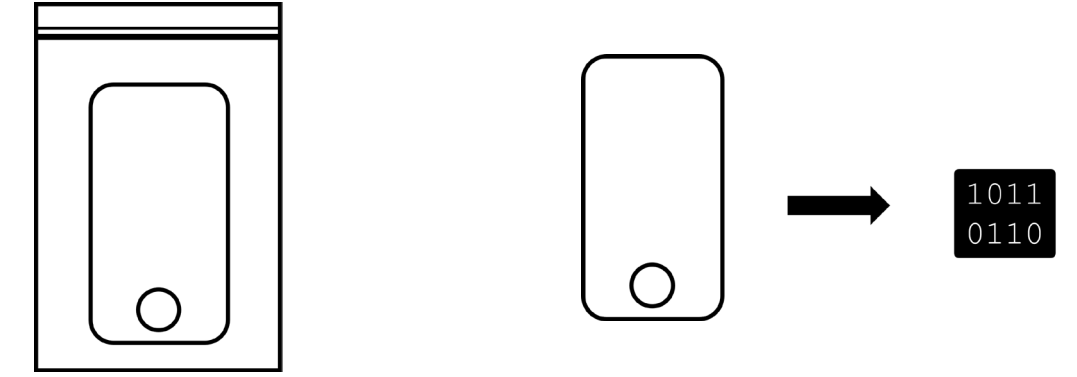
# Write Blocker

- Verhindert, dass Datenträger verändert wird
- Standard für Forensische Analysen
  - Auf Windows zwingend!
- Formate für diverse Datenträgertypen



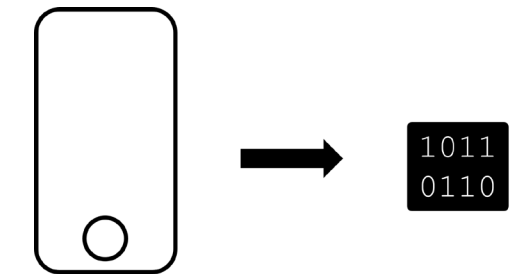


# SSD: Garbage Collection



- SSD haben einen eingebauten Mechanismus, um gelöschte Daten endgültig zu löschen.
  - «Garbage Collection»
- Dieser Prozess ist aktiv sobald die SSD Stromzufuhr hat.
- Write-Blocker stoppen diesen Prozess nicht, verlangsamen ihn jedoch
- Bei SSD lohnt es sich, Kopien so schnell wie möglich anzufertigen

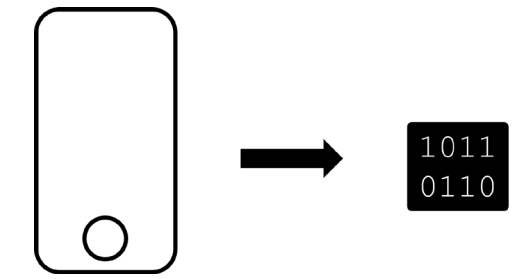
# Kopie erstellen



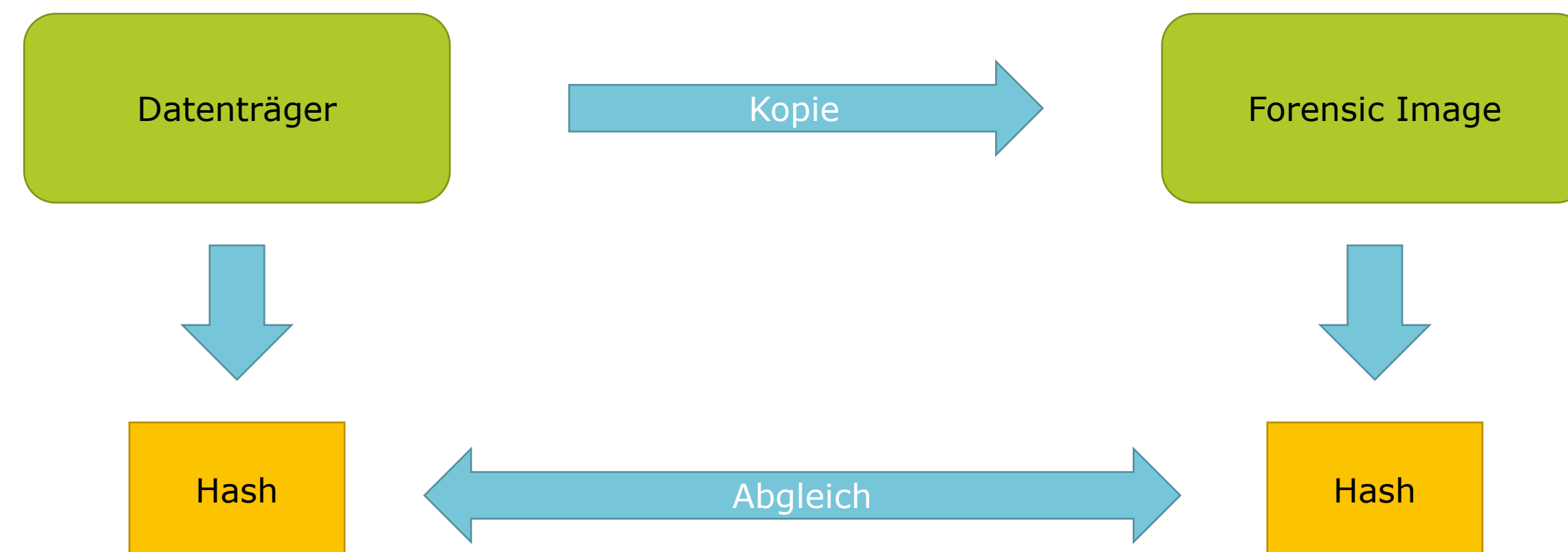
- Portable Kopier-Stationen
  - Built-In Write Blocker
- Forensische Software
  - dd-Befehl auf Linux
  - Guymager
  - FTK Imager
  - Autopsy
  - usw..



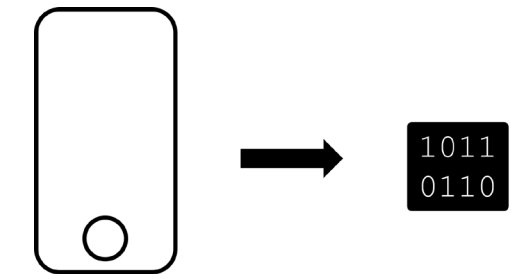
# Hashing



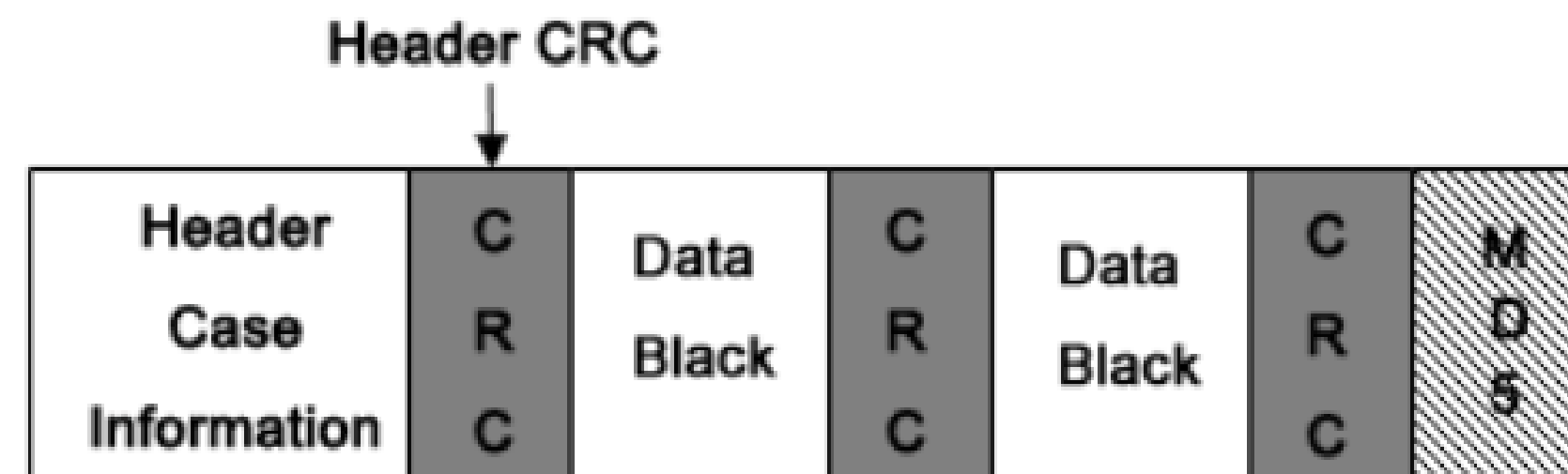
- Wir verwenden Hashes, um Authentizität und Vollständigkeit einer Kopie zu überprüfen
- Hashes werden Dokumentiert, um Authentizität bis vor Gericht zu garantieren (Chain of Custody)



# Dateiformate von Forensischen Kopien

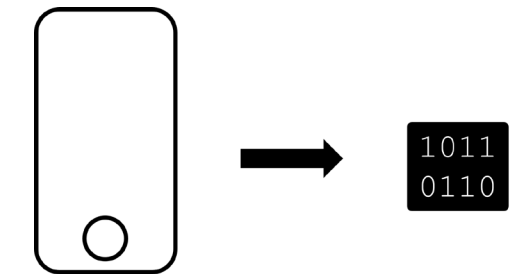


- Raw
  - .raw / .dd
  - Enthält Daten in Rohformat
  - Grösse Kopie = Grösse Datenträger
  - Hash der Kopie = Hash Datenträger
- Evidence- / Encase-Format
  - .E01
  - Komprimiert
  - In mehrere 640MB-Teile aufgeteilt
  - Grösse Kopie < Grösse Datenträger
  - Enthält Metadaten zu Acquisition
  - De-Facto Standard
  - Hash der Datei != Hash des Datenträgers



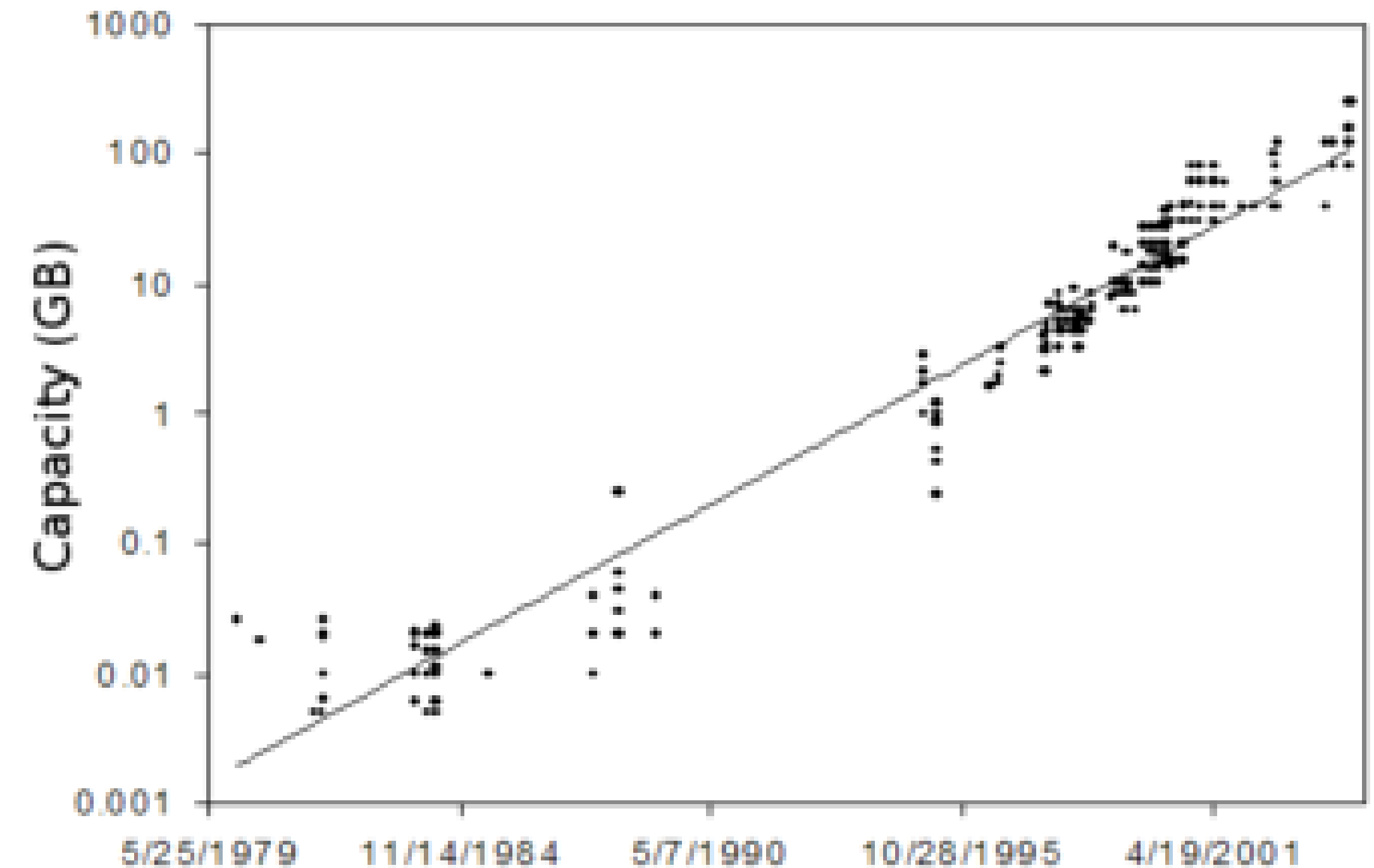
<https://www.forensicsware.com/blog/e01-file-format.html>

# Herausforderung: Moores Law



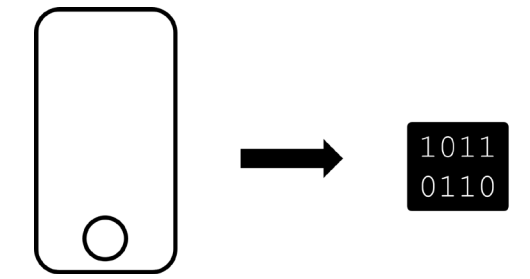
- Datenmenge wächst exponentiell
- Sichern als Kopie von allen Datenträgern benötigt unglaublich viel Speicherplatz
  - Mehr als die meisten Polizeien sich leisten können
- Im allgemeinen werden Abbilder nur bei Datenträgern durchgeführt, welche als Beweismittel verwendet werden

Hard drive capacity



[https://www.cs.mcgill.ca/~rwest/wikispeedia/wpcd/wp/m/Moore%2527s\\_Law.htm](https://www.cs.mcgill.ca/~rwest/wikispeedia/wpcd/wp/m/Moore%2527s_Law.htm)

# Ansätze gegen Moores Law: Live Analyse



- Die Analyse wird (mit Write-Blocker) direkt auf der Disk durchgeführt
- Es werden nur Disks kopiert, welche auch als Beweismittel verwendet werden

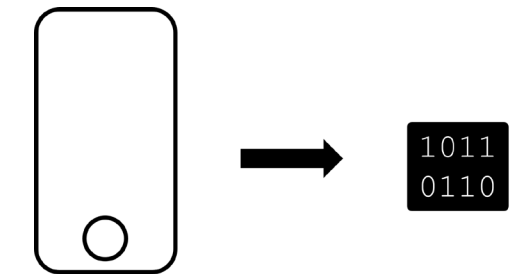
## Vorteile:

- Sehr Effizient

## Nachteile:

- Nicht genial mit SSDs (Garbage Collection)
- Risiko, dass Disk während Analyse stirbt

# Ansätze gegen Moores Law: Triage



- Nach der Kopie wird eine schnelle Analyse durchgeführt und entschieden, ob das Image behalten wird
- Bei negativ-Entscheid wird das Image gelöscht

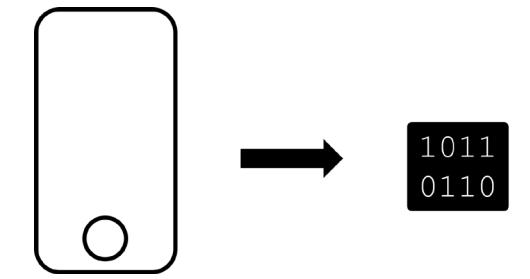
## Vorteile:

- Disk wird nur minimal belastet.

## Nachteile:

- Viel Kopier- & Löschzeit
- Risiko einer initialen Fehleinschätzung

# Ansätze gegen Moores Law: Incremental Imaging



- Beim Erstellen der Kopie wird die Kopie in einzelne Dateien aufgesplittet
- In einer zentralen Datenbank werde für jedes File die Datei, der Hash, sowie Infos über den Ort auf der Disk & Metadaten gespeichert
- Tauchen in einem 2. Fall dieselben Dateien wieder auf, werden nur die Metadaten kopiert.

## Vorteile:

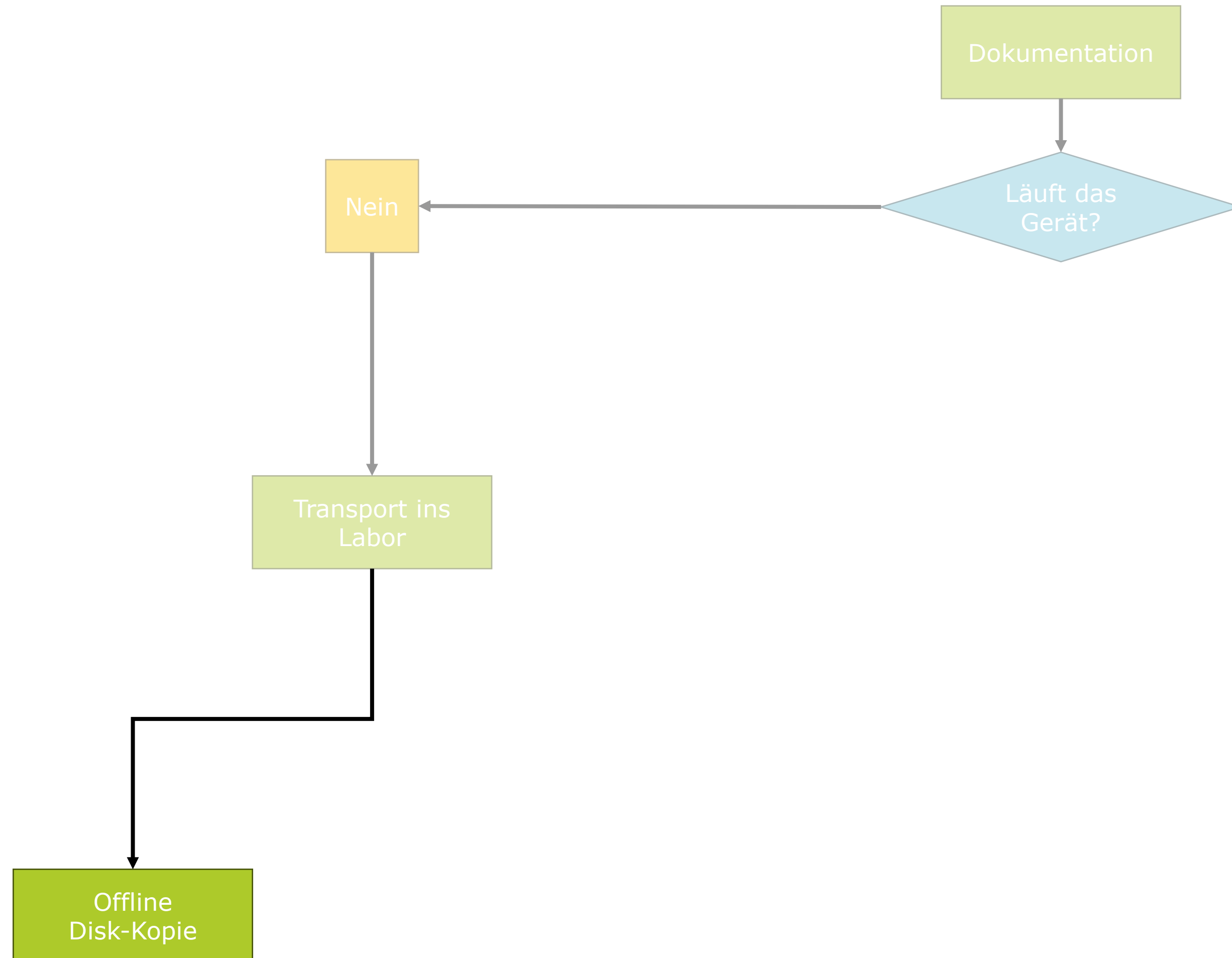
- Optimiert für Speicherplatz-Nutzung trotz vollständigen Daten

## Nachteile:

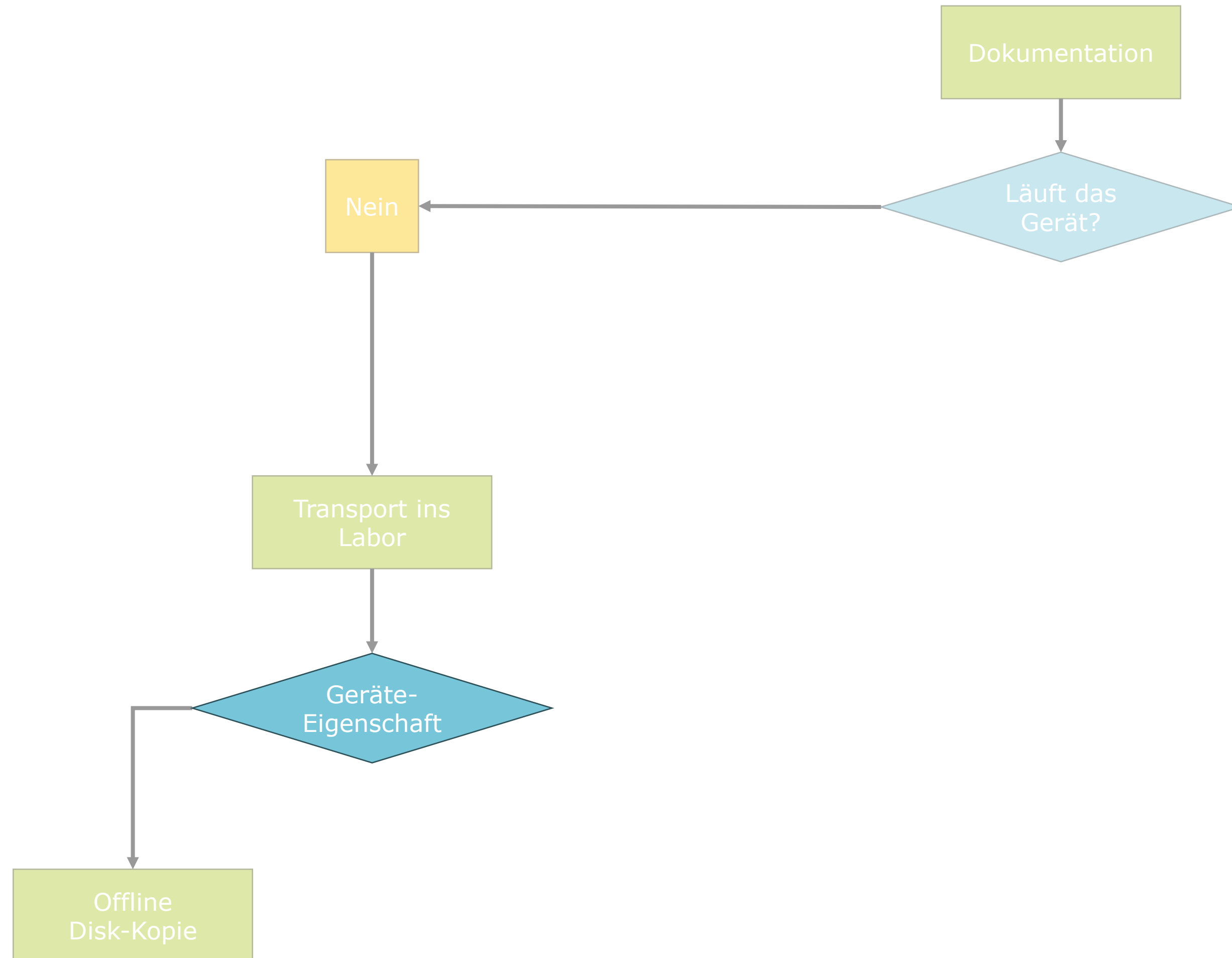
- Erfordert entsprechende Infrastruktur
- Führt zu einer Durchmischung der Falldaten
- Disk image muss rekonstruiert werden



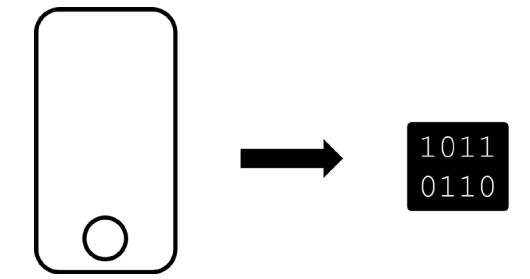
# Sichern eines PC: Flowchart



# Sichern eines PC: Flowchart



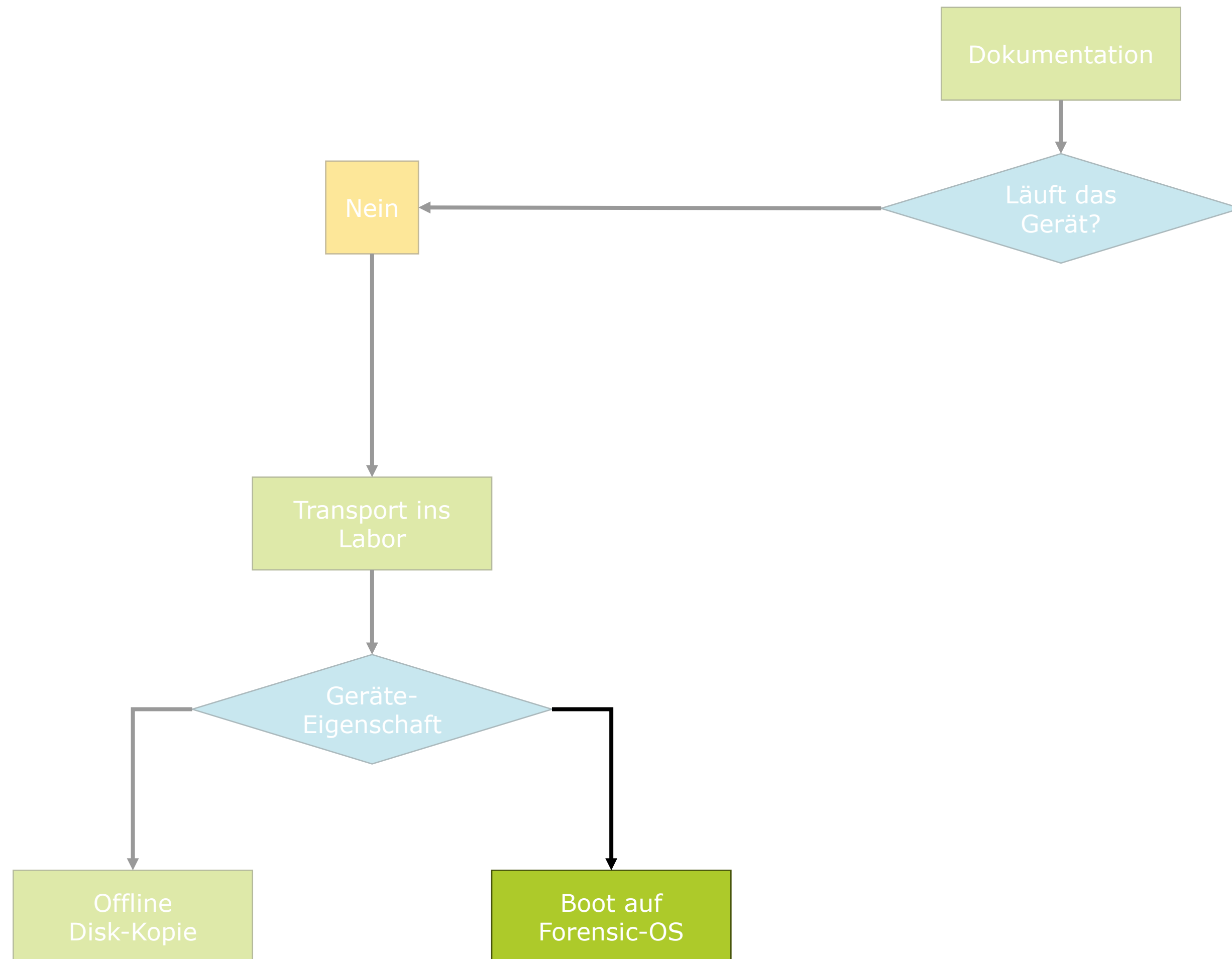
# Geräte-Eigenschaften, die Forensische Kopie verhindern



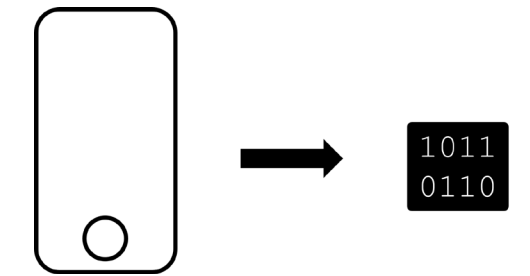
- Aufgelötete Speicher-Chips
- Wir haben keinen Adapter für den Datenträger
- Disk ist nicht ausbaubar
  - Zum. Nicht mit verhältnismässigem Aufwand
- Encryption (je nach Ebene der Verschlüsselung)

(Gerät ist ein Mac)

# Sichern eines PC: Flowchart

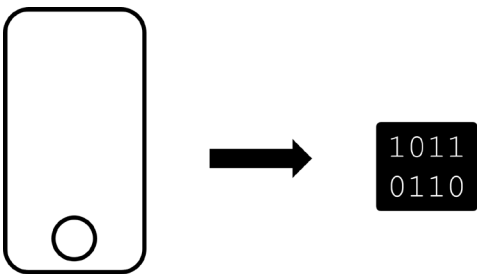


# Boot auf anderes OS



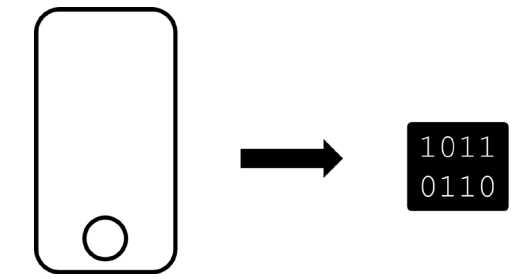
- Erstellen eines Bootable USB-Stick mit Forensic OS
  - Kali
  - CAINE
  - Parrot Sec
  - Cellebrite Digital Collector (Mac)
- Boot auf USB-Stick
  - Unterbrechen der Boot-Sequenz
  - Starten in den Boot-Manager
  - Auswählen des Sticks als Boot-Quelle
- Bedingt manchmal mehrere Re-boots

# Starten des Boot-Managers



Gerät	Start des Boot Managers
Asus	`F8`
Acer	`Esc`, `F12` oder `F9`
Apple	`⌘` option`
Compaq	`F10`
Dell	`F11`
HP	`F10`, `F2` oder `F6`
Lenovo	`F12`
MSI	`F11`
Samsung	`F10`
Toshiba	`F12` oder `F2`

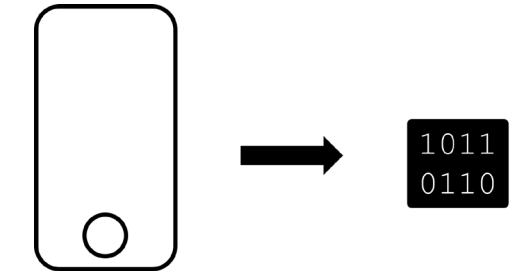
# Boot Manager: Windows 10 & 11



- Auf Windows 10 und 11 ist es möglich, dass der Boot Manager deaktiviert ist.
  - PC normal starten
  - Unter `Settings > Recovery > Advanced Startup

**/!\ Dies hinterlässt viele Spuren und ist aus Spurenerhaltungs-Sicht nicht ideal /!\**

# Windows: UEFI / BIOS Passwort

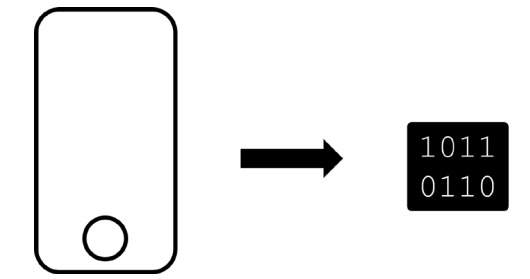


- Falls Passwort bekannt:
  - Eingeben des Passworts
- Falls Passwort unbekannt:
  - Je nach Hersteller können spezifische Resets existieren
- CMOS Reinitialisieren:
  - CMOS jumper
  - CMOS-Batterie entfernen

=> Macht das nur, wenn ihr sicher seid, was ihr macht!

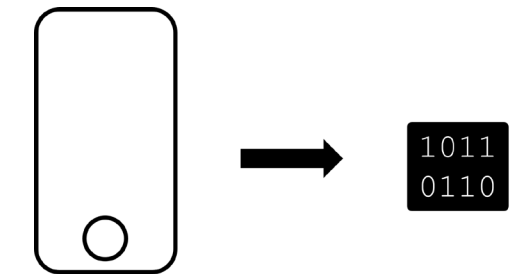


# Geschützte Firmware: Mac



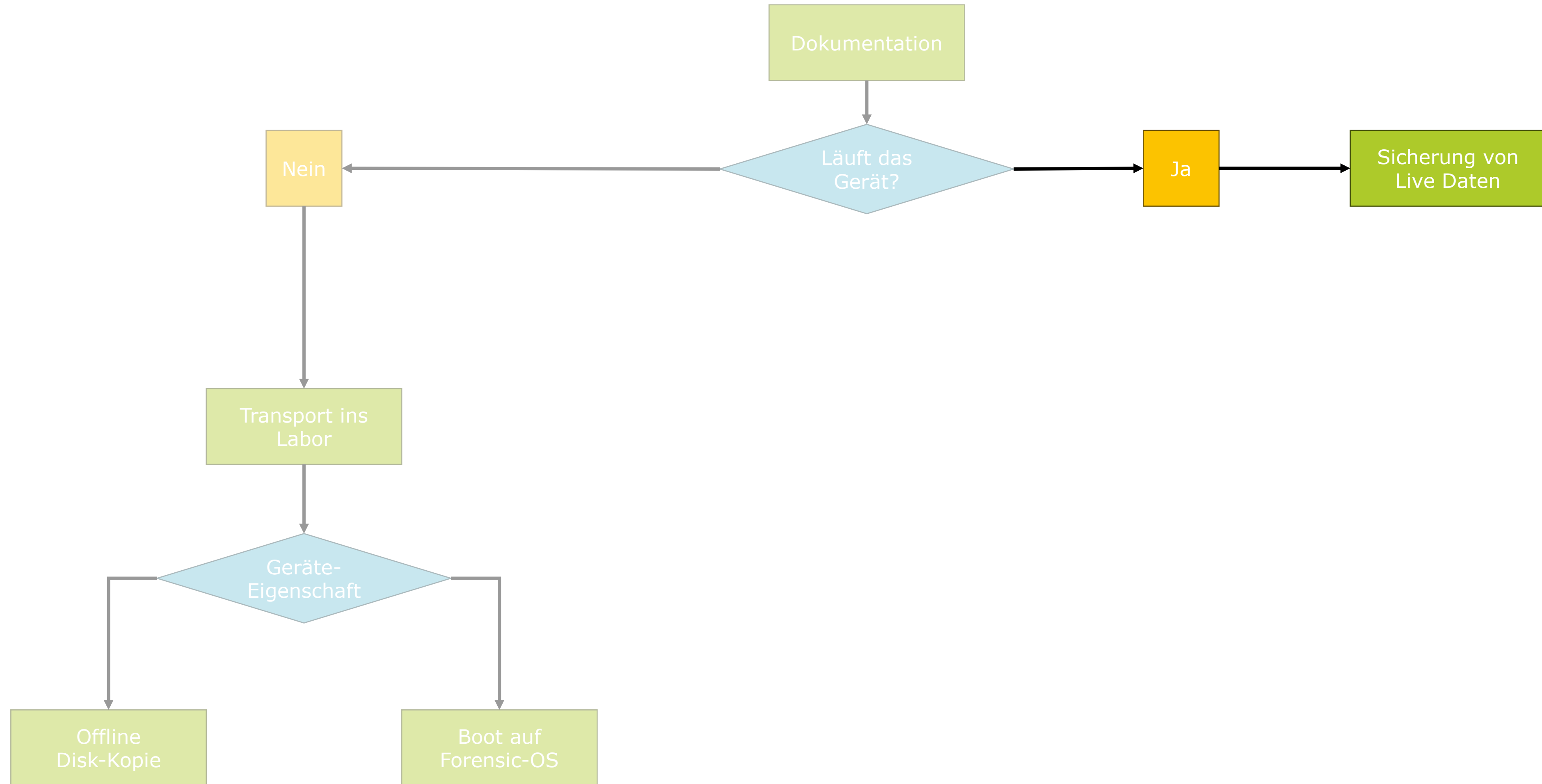
- Auf Mac kann die Firmware mit Passwort geschützt werden
  - Dies deaktiviert alternative Boot-Methoden
- Falls Passwort bekannt:
  - '⌘' + 'R' während Boot um Passwort zu entfernen
- Falls Passwort unbekannt:
- NVRAM reinitialisieren:
  - RAM-Menge verändern während OFF
  - Boot während die Tasten '⌘' + '⇧' + 'P' + 'R' gedrückt sind
  - Gerät 4x starten lassen
  - Beim 4. Startup ist das Passwort gelöscht

# Boot auf Forensic OS

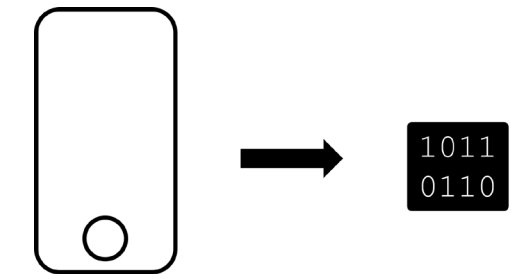


- Forensic OS verwendet Hardware des analysierten Geräts
  - Disks des Geräts werden nicht verändert
  - Disks des Geräts sind für das Forensic OS zugänglich
- Wir können eine Forensische Kopie der Disks erstellen
- Forensic OS enthalten Tools zum Erstellen von Images
  - dd-command, Guymager...
- Typischerweise benötigen wir einen 2. Datenträger auf den wir das Image schreiben können
  - Benötigt zusätzlichen USB-Port / USB-Hub
  - Je nach dem kann das schreiben sehr langsam sein

# Sichern eines PC: Flowchart

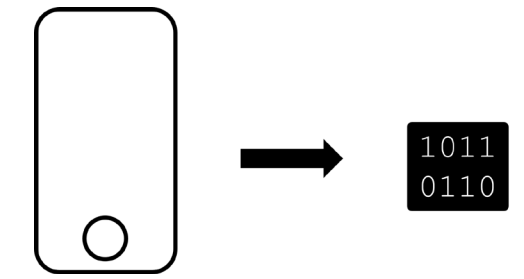


# RAM-Capture



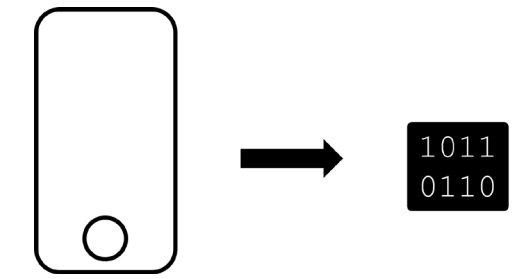
- Verwendung eines spezifischen Programms
  - Eg. FTK Imager
- Programm wird direkt von USB aus ausgeführt
- Dump wird auf USB-Stick gesichert (Integrität der Disk)
- Sicherungsprozess wird Spuren hinterlassen:
  - USB-Stick-ID in Registry
  - Programmausführung in Logs, Systemdateien & RAM
- RAM verändert sich während der Sicherung
  - Es ist möglich, dass der Start und das Ende des Dumps nicht konsistent sind.

# Alternative Live-Capture Methoden



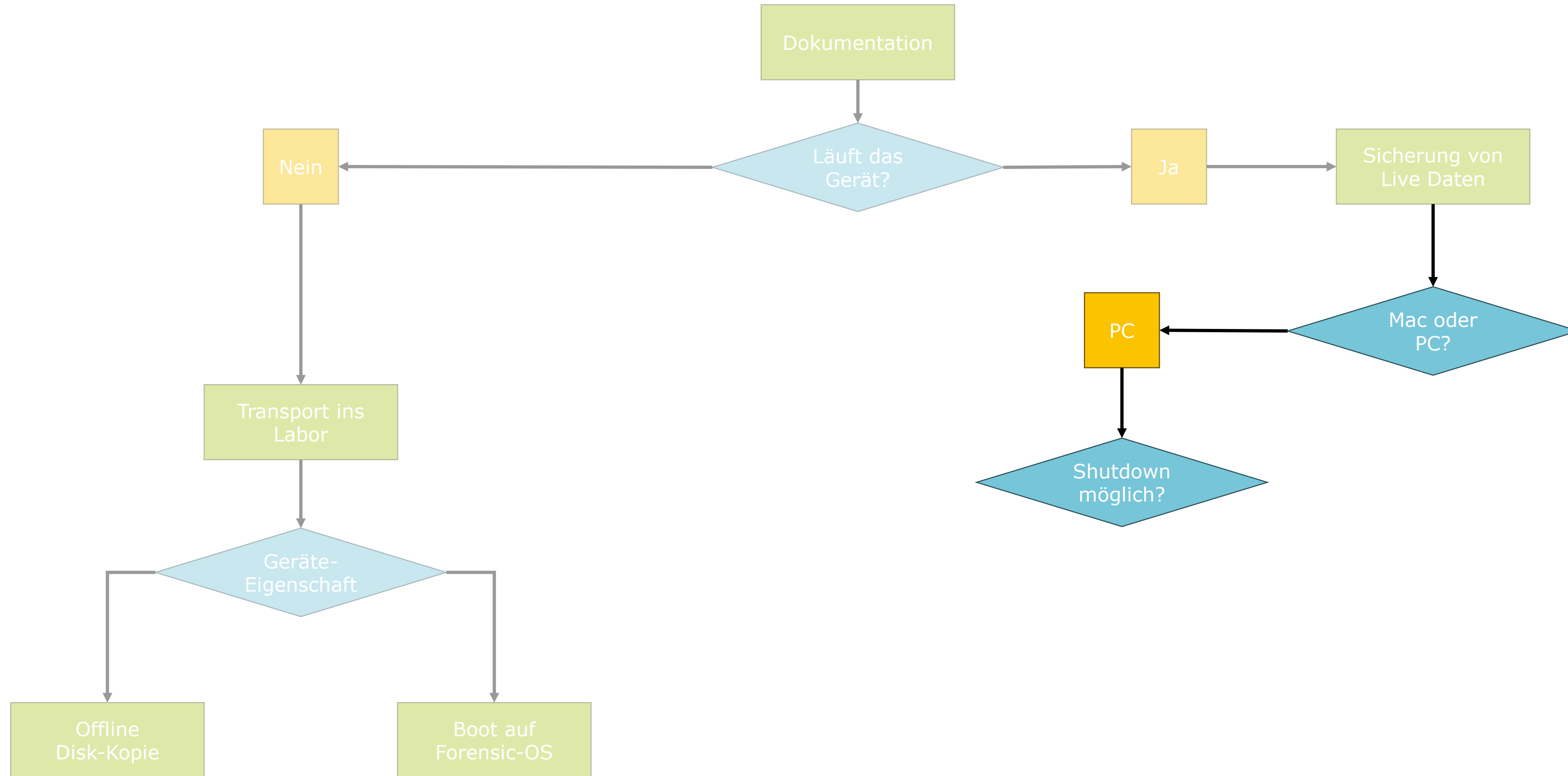
- Wir können eine Reihe von Informationen vom laufenden System sammeln
  - Laufende Prozesse
  - Netzwerk-Konfig
  - Aktive Nutzer
  - ...
- Wir können dies entweder über Command-Line Skripts oder mit extra Programmen machen
- Auch dies wird auf dem Gerät Spuren hinterlassen

# RAM vs. Live-Capture

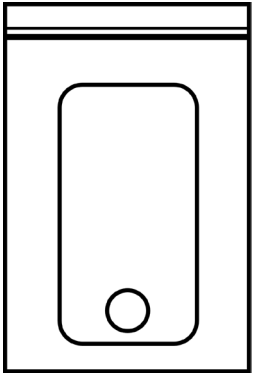


- RAM ist die vollständigere Variante.
- Wenn ihr den Verdacht habt, dass die Maschine mit Malware infiziert ist, lohnt sich Sicherung der RAM.
- Ansonsten ist Live-Capture meistens mehr als ausreichend.

# Sichern eines PC: Flowchart



# Disk-Encryption




- BitLocker on?
  - Control Panel > System and Security > Bitlocker Drive Encryption


Betriebssystemlaufwerk

OSDisk (C:) BitLocker aktiviert



 Schutz anhalten

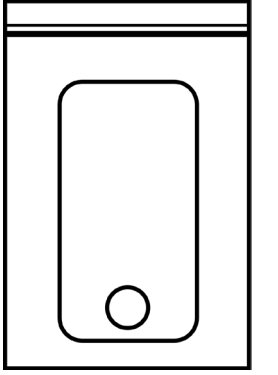
 Wiederherstellungsschlüssel sichern

 BitLocker deaktivieren

- Hinweise auf Crypto-Drives?
  - PGP, VeraCrypt o.ä. auf dem PC?
  - Namen der Drives?

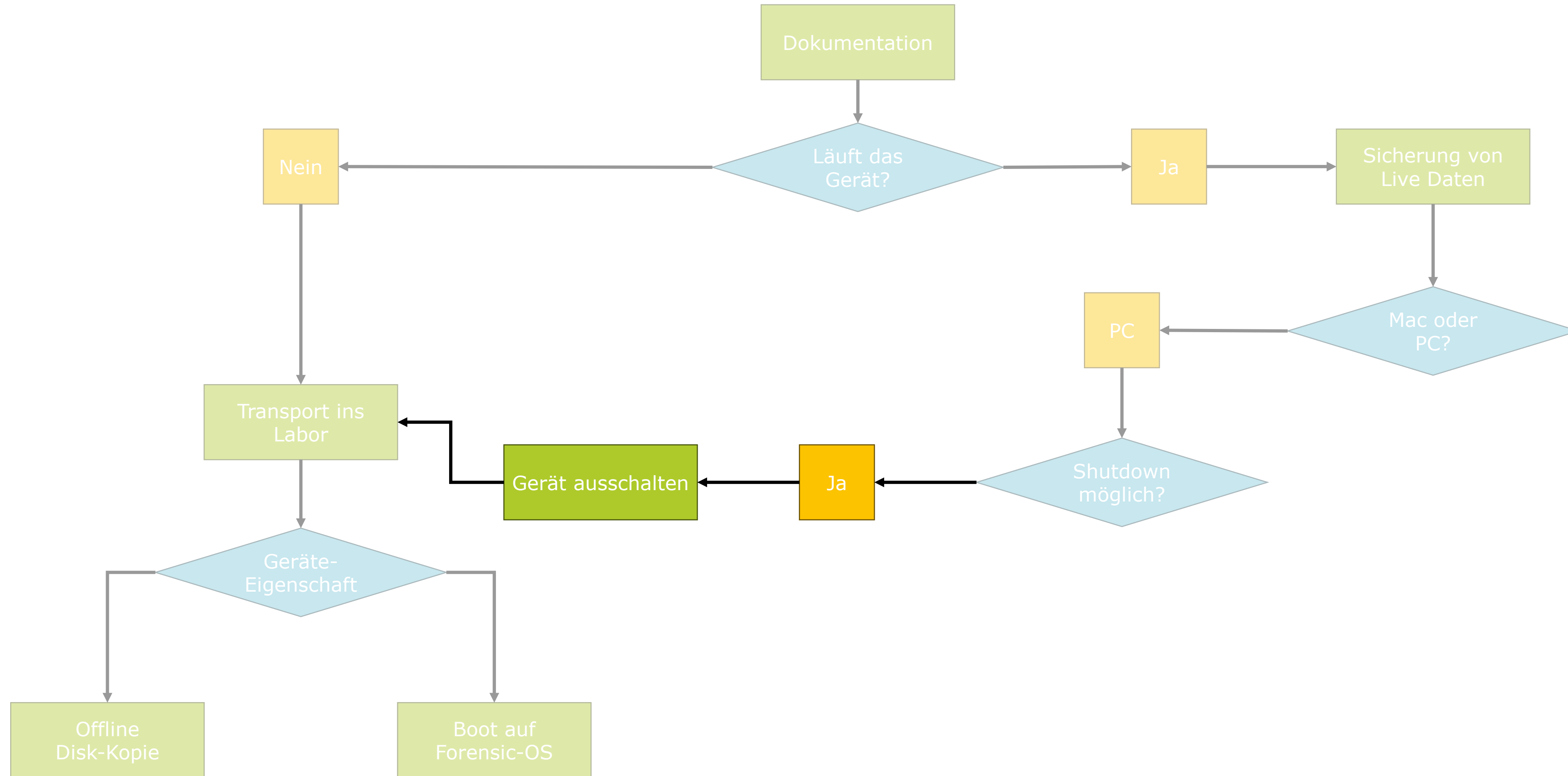


# Andere Gründe gegen Shutdown?

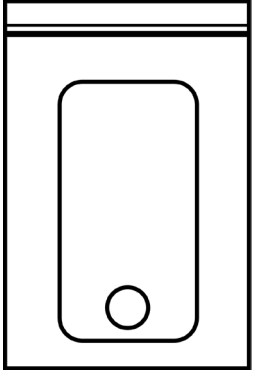


- Der Shutdown des Geräts würde weitreichende negative Konsequenzen nach sich ziehen
  - Kritische Infrastruktur
  - Medizinalgeräte
- Operationelle Gründe
  - Die Maschine ist Teil eines kriminellen Netzwerks
  - Abschalten der Maschine könnte Komplizen alarmieren

# Sichern eines PC: Flowchart

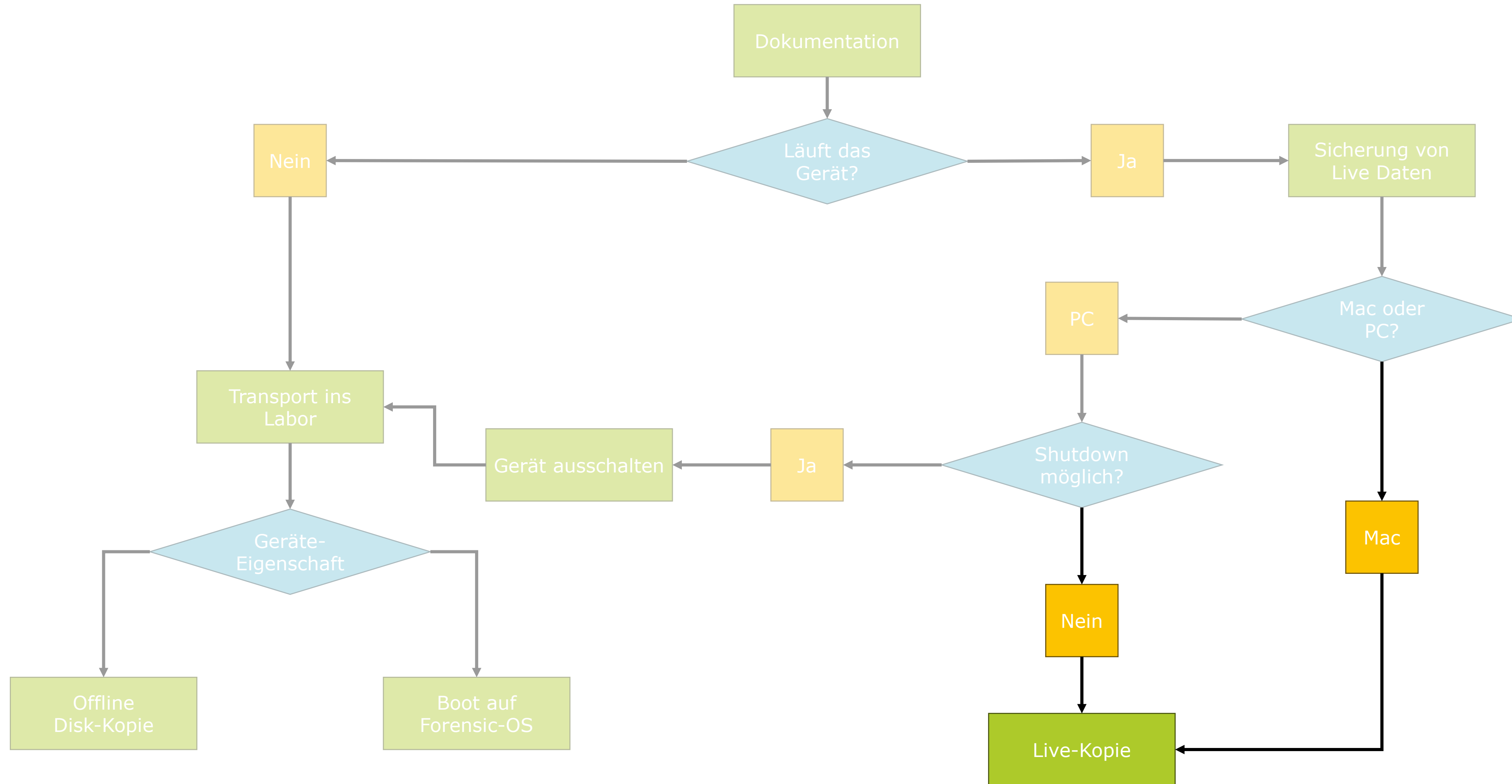


# Gerät ausschalten

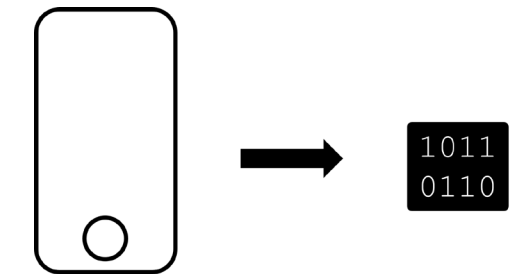


- Je abrupter desto besser
  - Führt zu weniger Veränderungen
  - Bei einem modernen PC werden alle Methoden zu Veränderungen führen
- Kabel ziehen
- Lange Power-Button drücken
- Shutdown über Menu

# Sichern eines PC: Flowchart

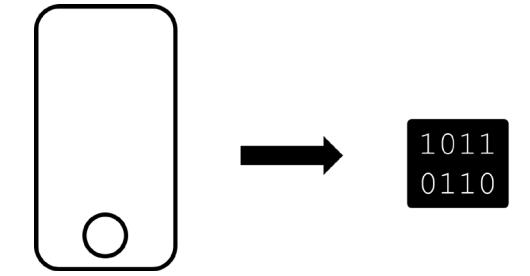


# Live Kopie



- Erstellen eines Disk-Images direkt auf dem zu Analysierenden System
- Ausführen eines Kopier-Tools von USB-Stick aus
- Kopieren auf 2. externen Datenträger

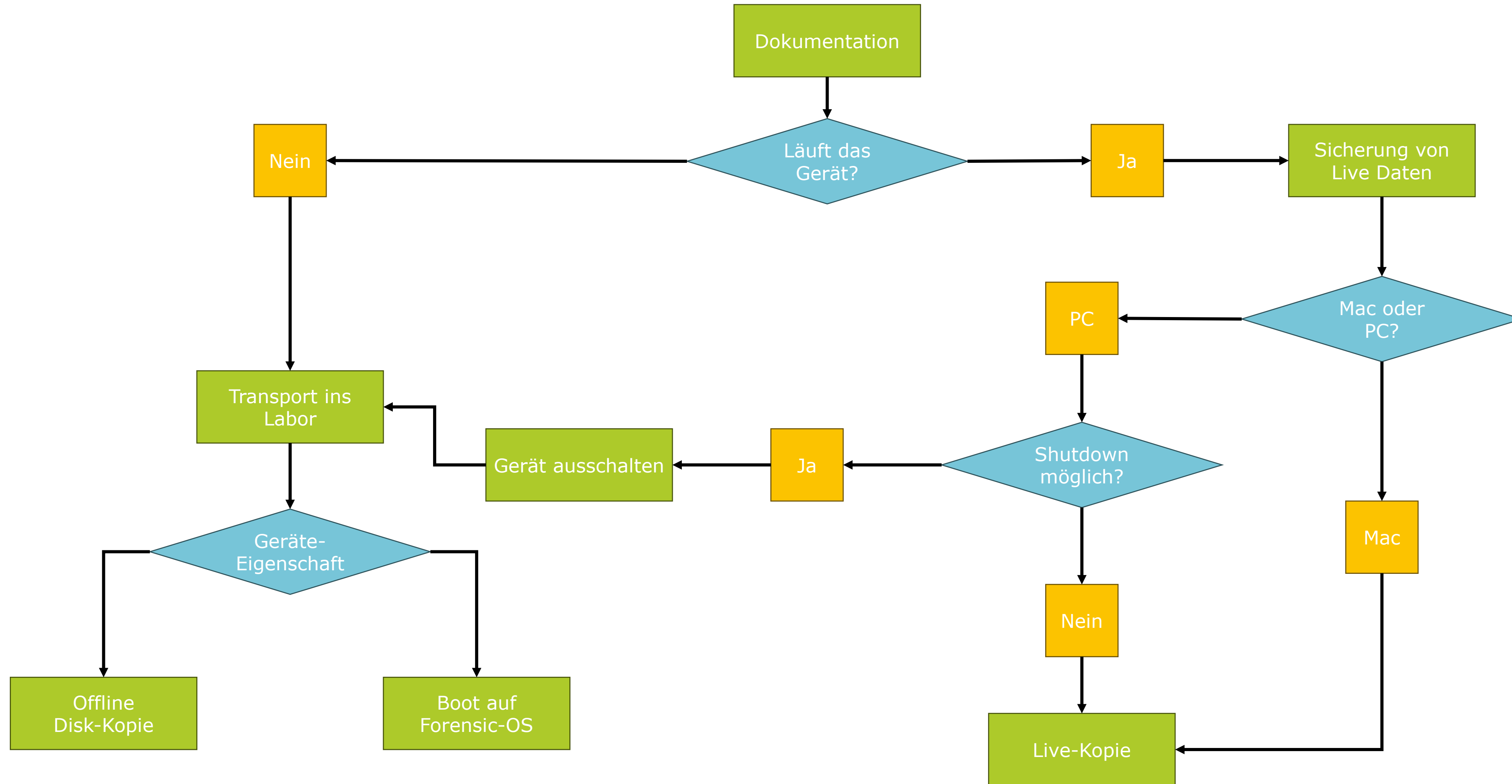
# Nachteile einer Live-Kopie



Kombiniert Nachteile aus der Live-Capture und dem Forensic OS:

- Erzeugt Spuren der Sicherung
  - USB, Speicher-Disk, Programm Launch
- Daten werden während Kopie verändert
  - Inkonsistenzen sind möglich
- Benötigt mind. Verfügbare USB-Ports oder Hub
  - Kann relativ langsam sein
- Auf Mac / Linux meist weniger ein Problem als auf Windows

# Sichern eines PC: Flowchart



# Fragen?

**Hochschule Luzern**  
**Informatik**  
**Dr. Hannes Spichiger**  
Dozent

T direkt +41 41 349 31 24  
[Hannes.spichiger@hslu.ch](mailto:Hannes.spichiger@hslu.ch)