FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Herausforderung der Android NAND-Image Analyse

Michel Erbach B.Sc.

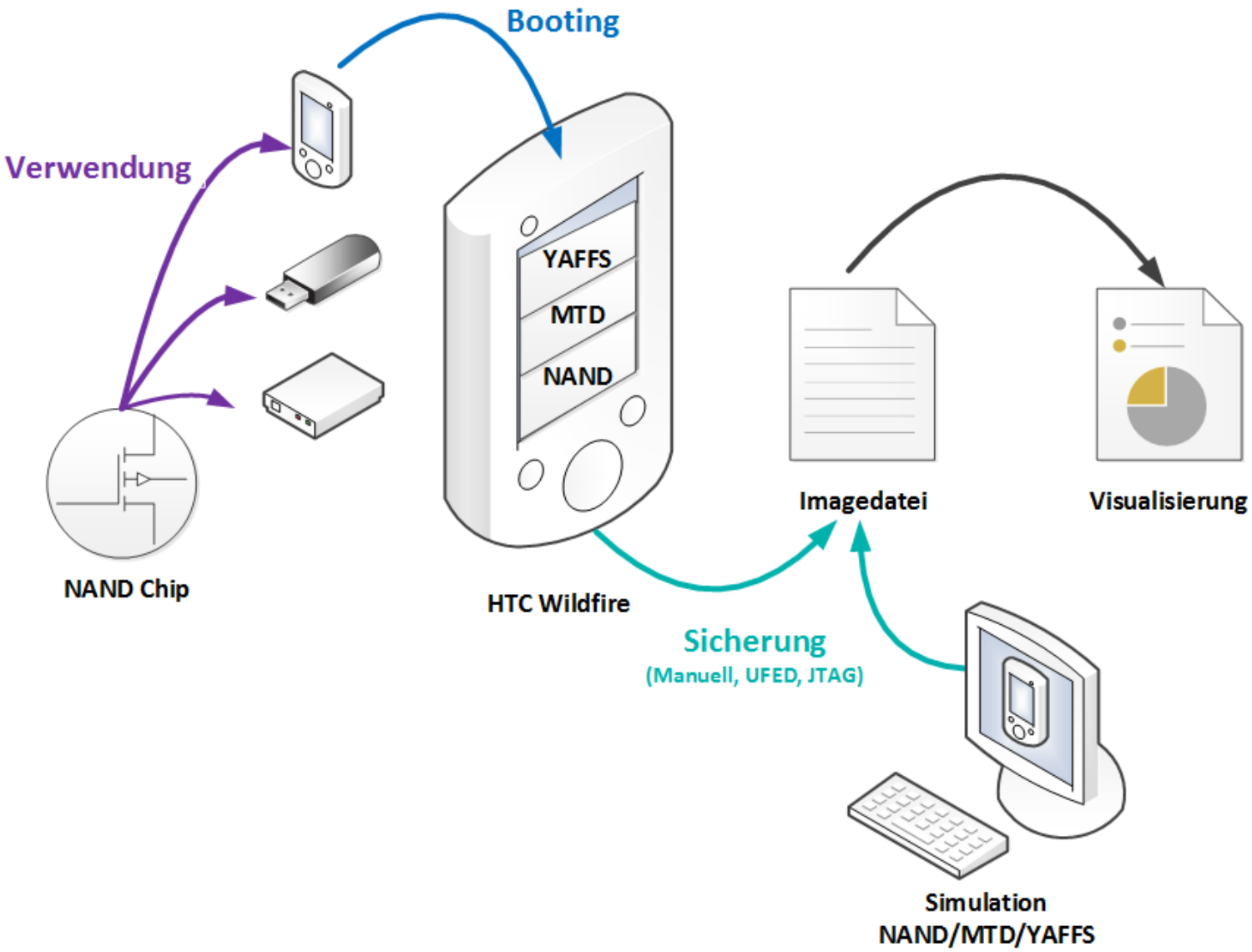
Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

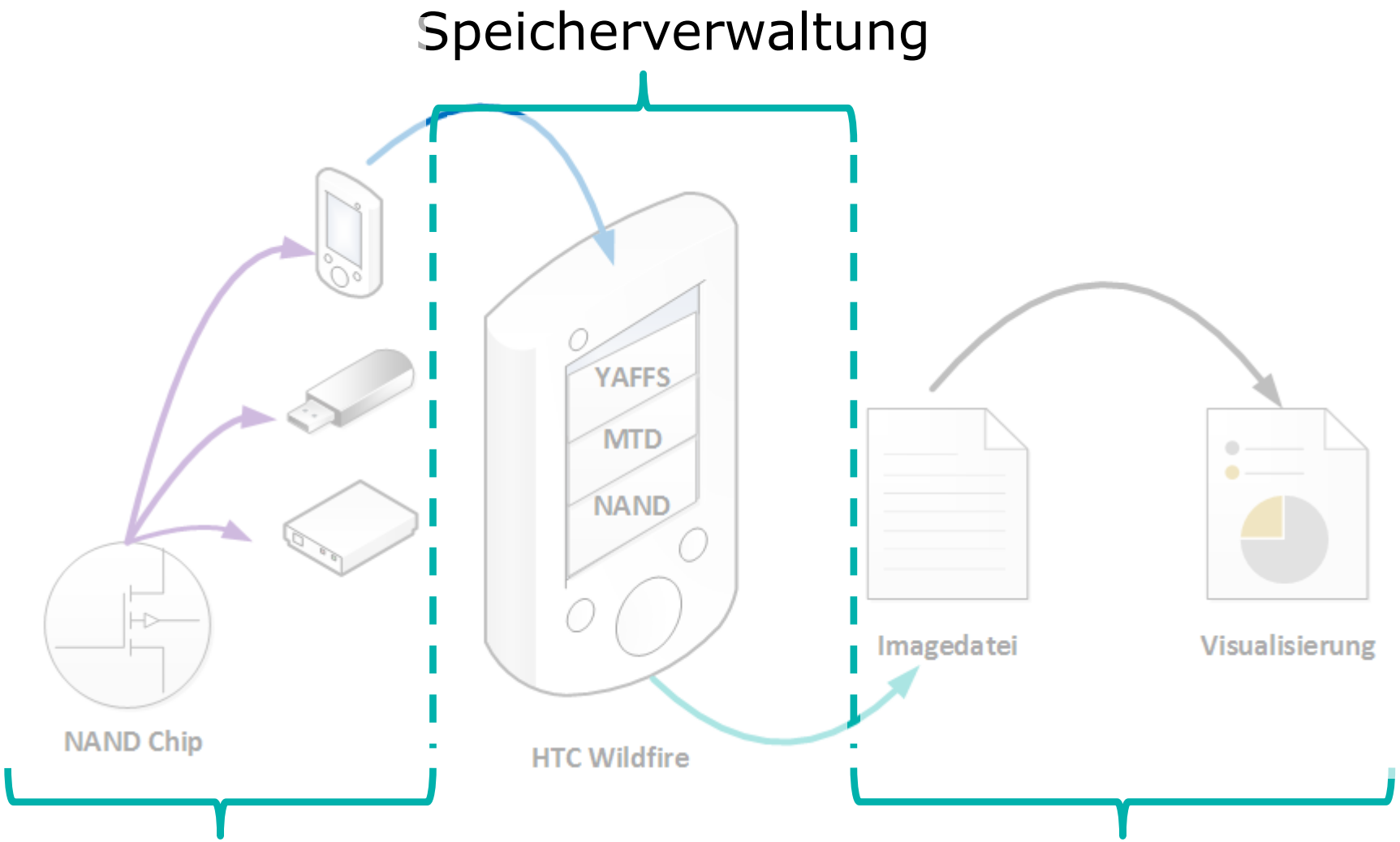
Zur Person

- Michel Erbach
- Wissenschaftlicher Mitarbeiter
- Abschluss B.Sc. im September 2013
- Thema *„IT-Forensik von Mobiltelefonen - Herausforderungen bei der Analyse von physischen Speicherabbildern basierend auf NAND-Flashspeichern“*
- In Kooperation mit LKA NRW

Themengebiete



Gliederung


Speicherverwaltung
YAFFS
MTD
NAND
NAND Chip
HTC Wildfire
Imagedatei
Visualisierung
Stand der Technik
Visualisierung

Einleitung


Neuer Absatzrekord bei Smartphones
Absatz in Deutschland
in Mio. Stück
15,9
+53 %
21,7
+36%
28,0
+29%
2011
2012
2013
Marktverteilung 2013
96 % Smartphones
4 % Klassische Handys
BITKOM
2013 = Prognose
Quelle: EITO, IDC

Einleitung

- Verbreitung von Smartphones
- Vertrauensstellung der Telefone
- Durchschnittlich 23 Apps je Smartphone
- Informationen für Ermittlungsunterstützung
- NAND Flash als Massendatenspeicher

Aufgabenstellung

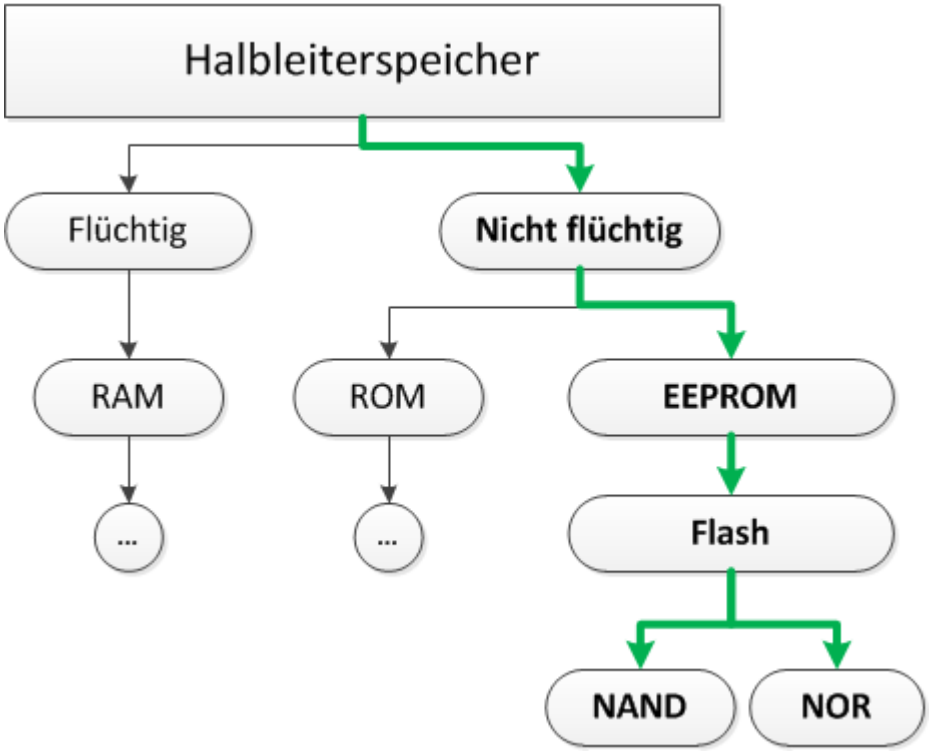
- Wie funktionieren Wear-Leveling Techniken auf NAND Speichern und kann man es umkehren ?

- Szenario:
  - Android Smartphone (HTC Wildfire A333)
  - Integrierter NAND-Flash
  - YAFFS2 Dateisystem

- Dokumentation für interessierte Mitarbeiter des LKA

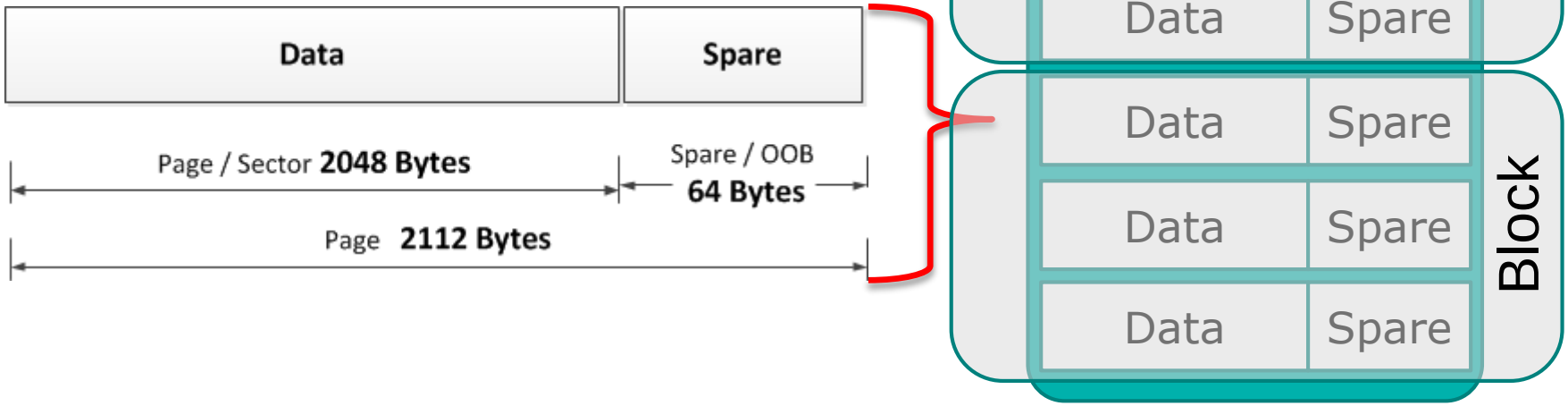
Stand der Technik

- Flash -> *NAND* Flash
- Hohe Schocktoleranz
- Schneller Zugriff
- Vibrationsfrei
- Günstige Herstellung
- Geringer Stromverbrauch
- Kompakte Bauform



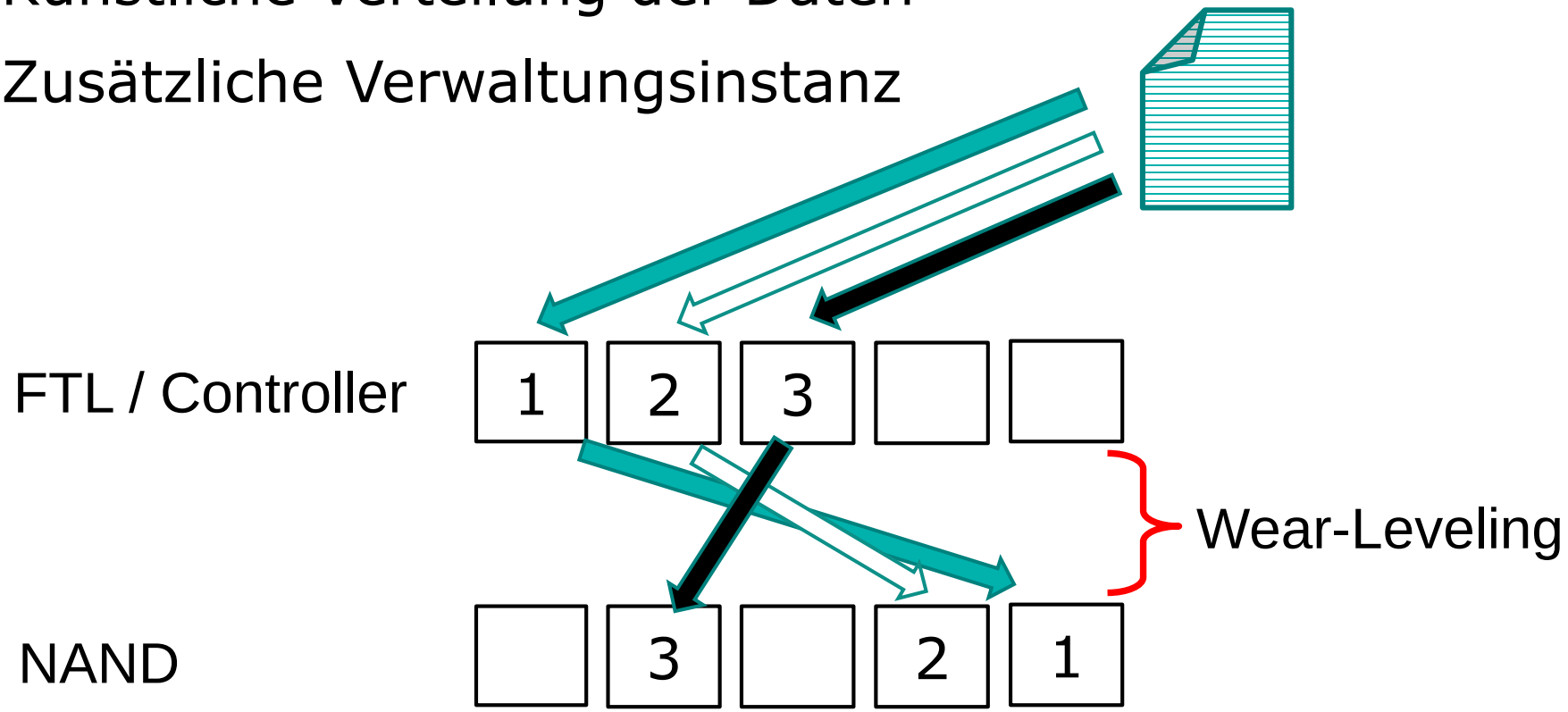
Stand der Technik

- Kein wahlfreier Zugriff
- Aufteilung des Speichers in
  - Page (Datenbereich)
  - Spare (Metadaten)
  - Block (Löscheinheit)



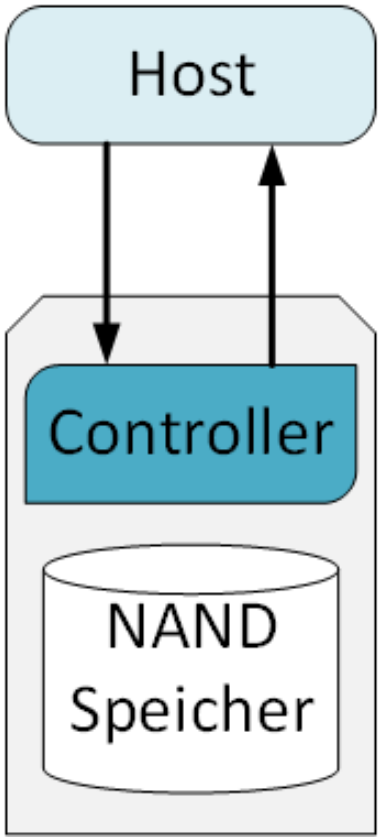
Stand der Technik

- Zellen sterben ab
- Eine defekte Zelle -> BadBlock
- Künstliche Verteilung der Daten
- Zusätzliche Verwaltungsinstanz

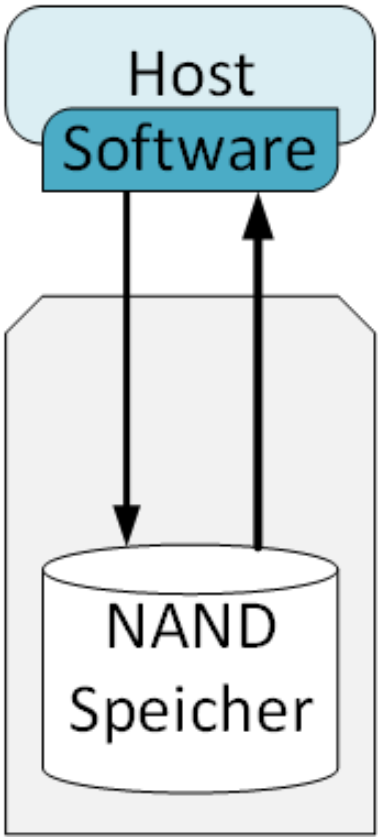


Stand der Technik

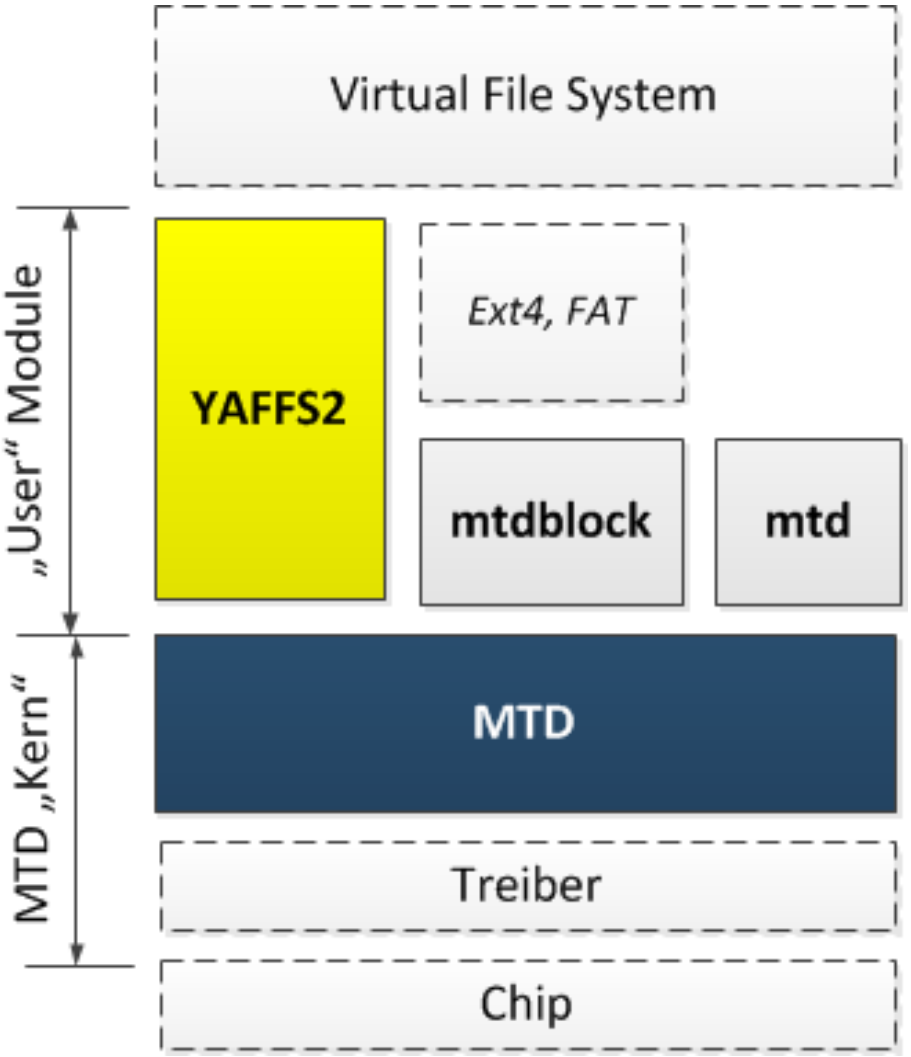
Blockgerät



RAW-Flash

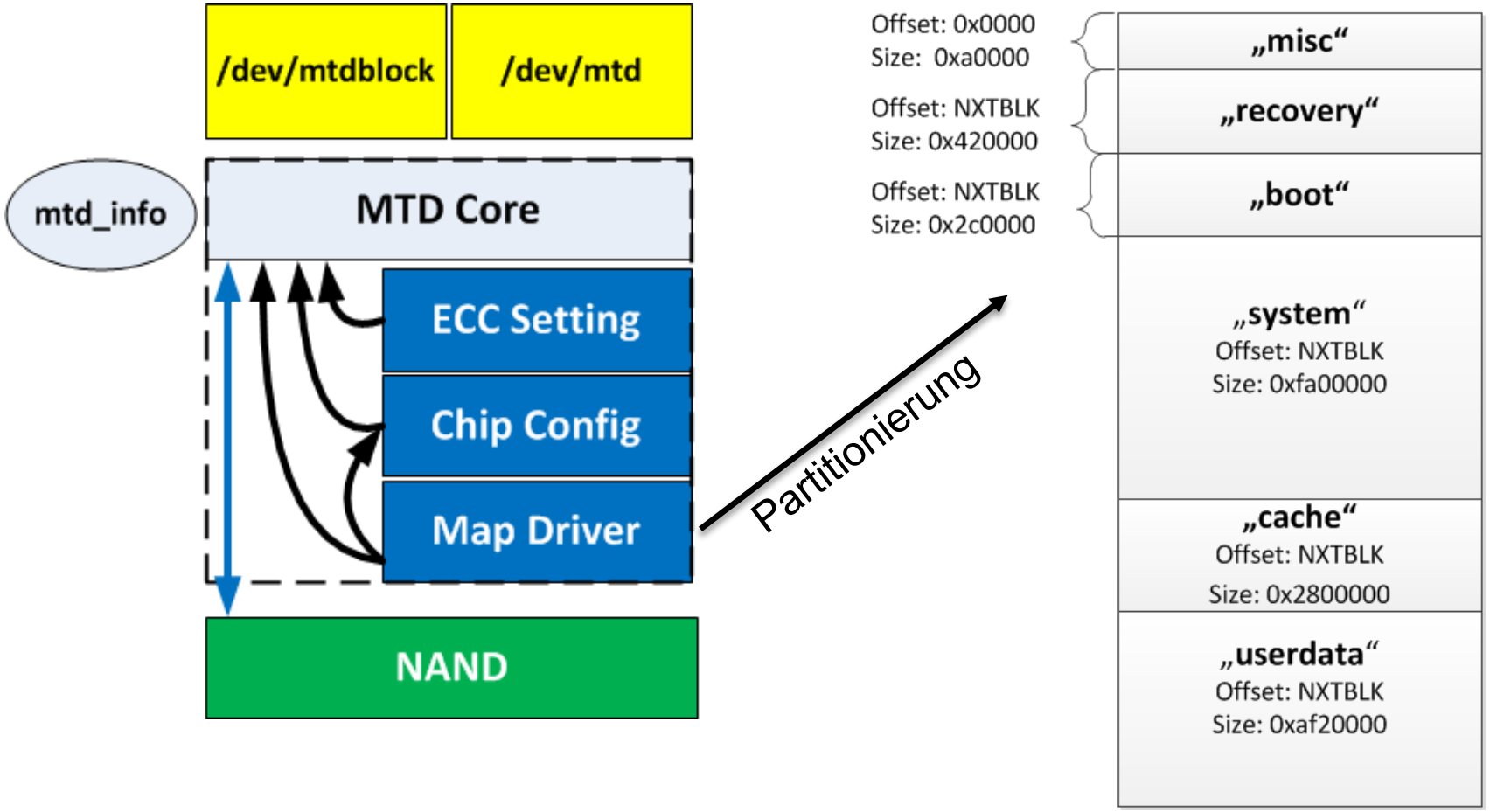


Speicherverwaltung Android



Speicherverwaltung Android

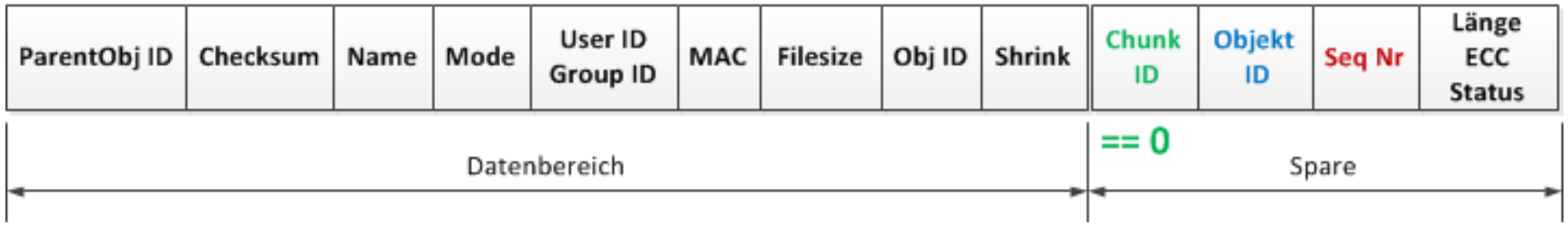
- MTD – Memory Technology Device



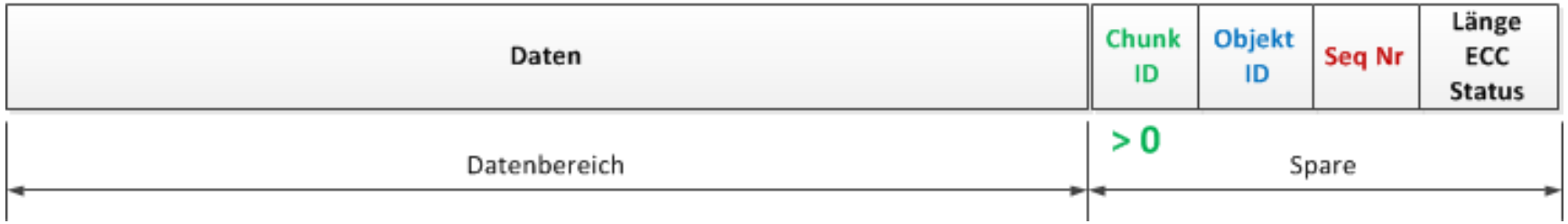
Speicherverwaltung Android

- YAFFS2 – Yet Another Flash File System

- Objektheader-Chunk

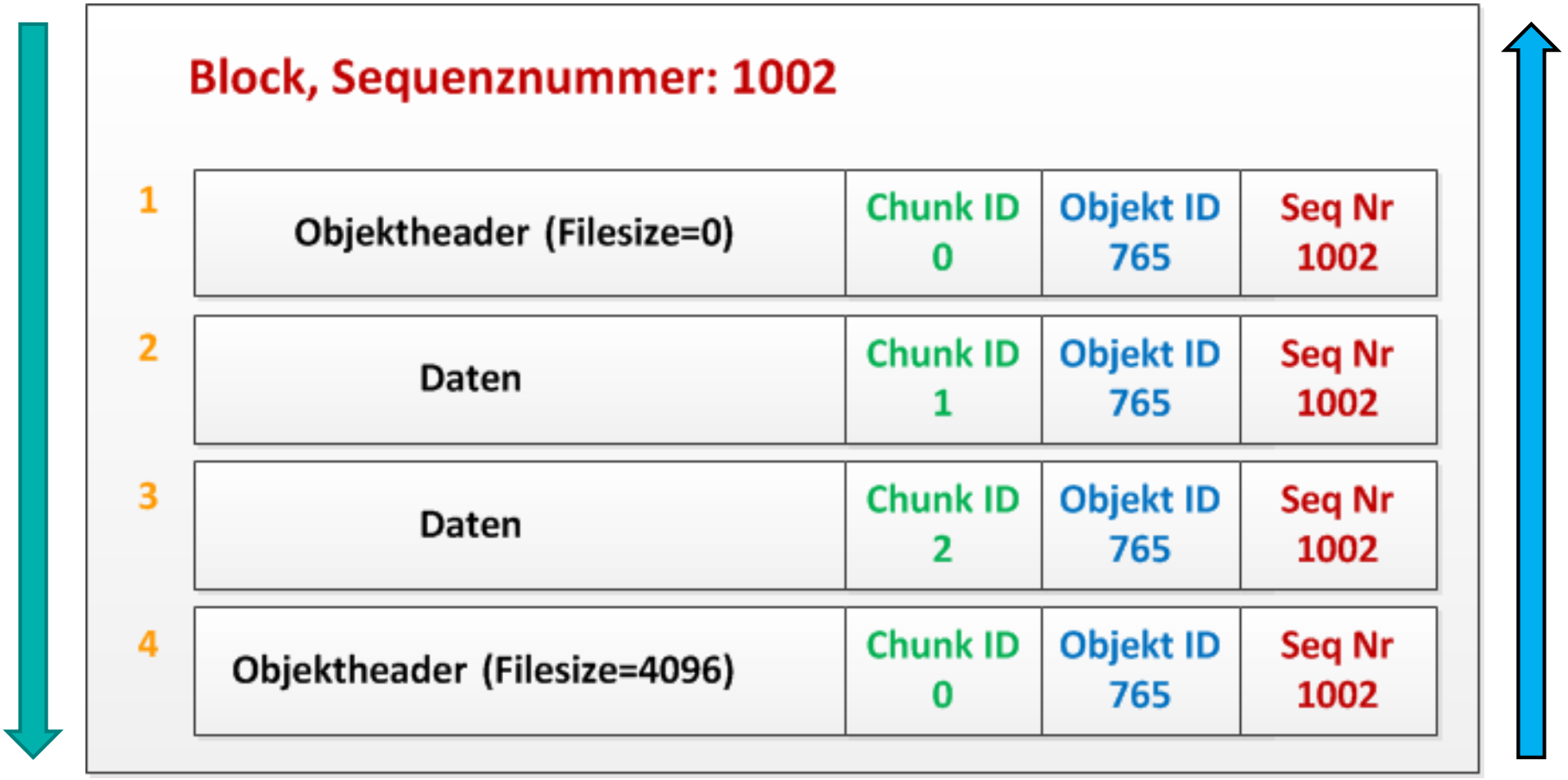


- Daten-Chunk



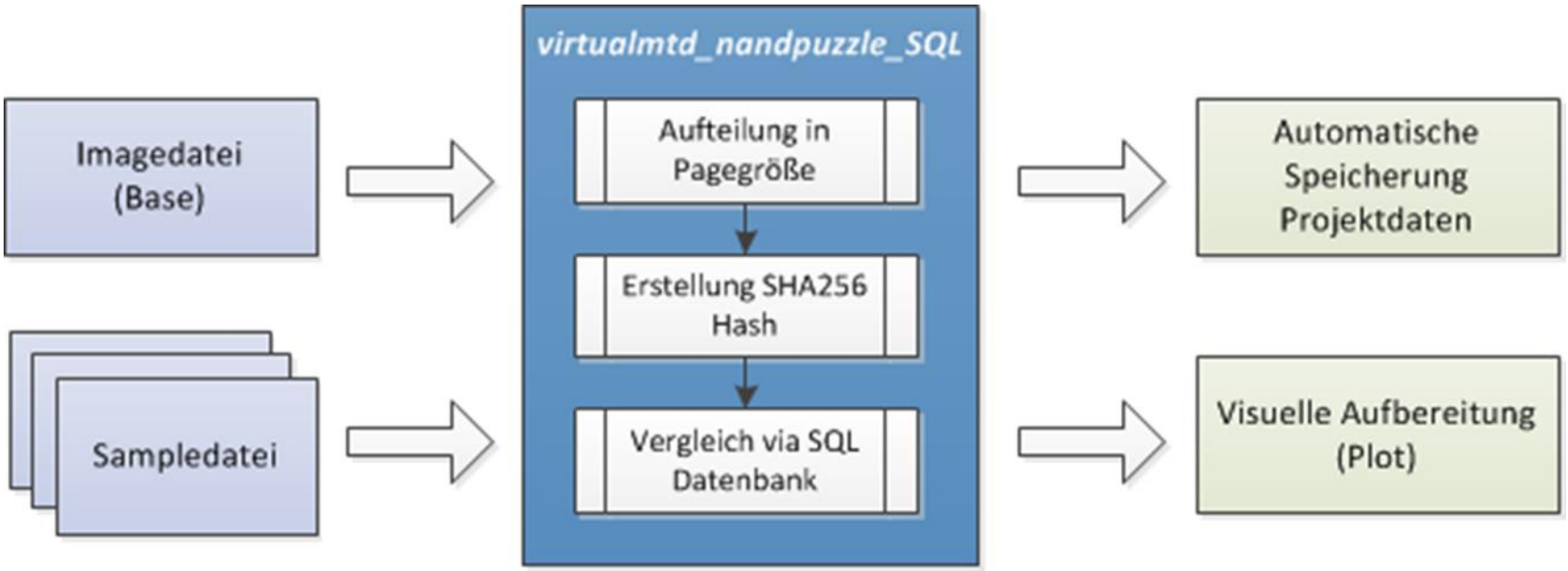
Speicherverwaltung Android

- Operationen mit YAFFS2



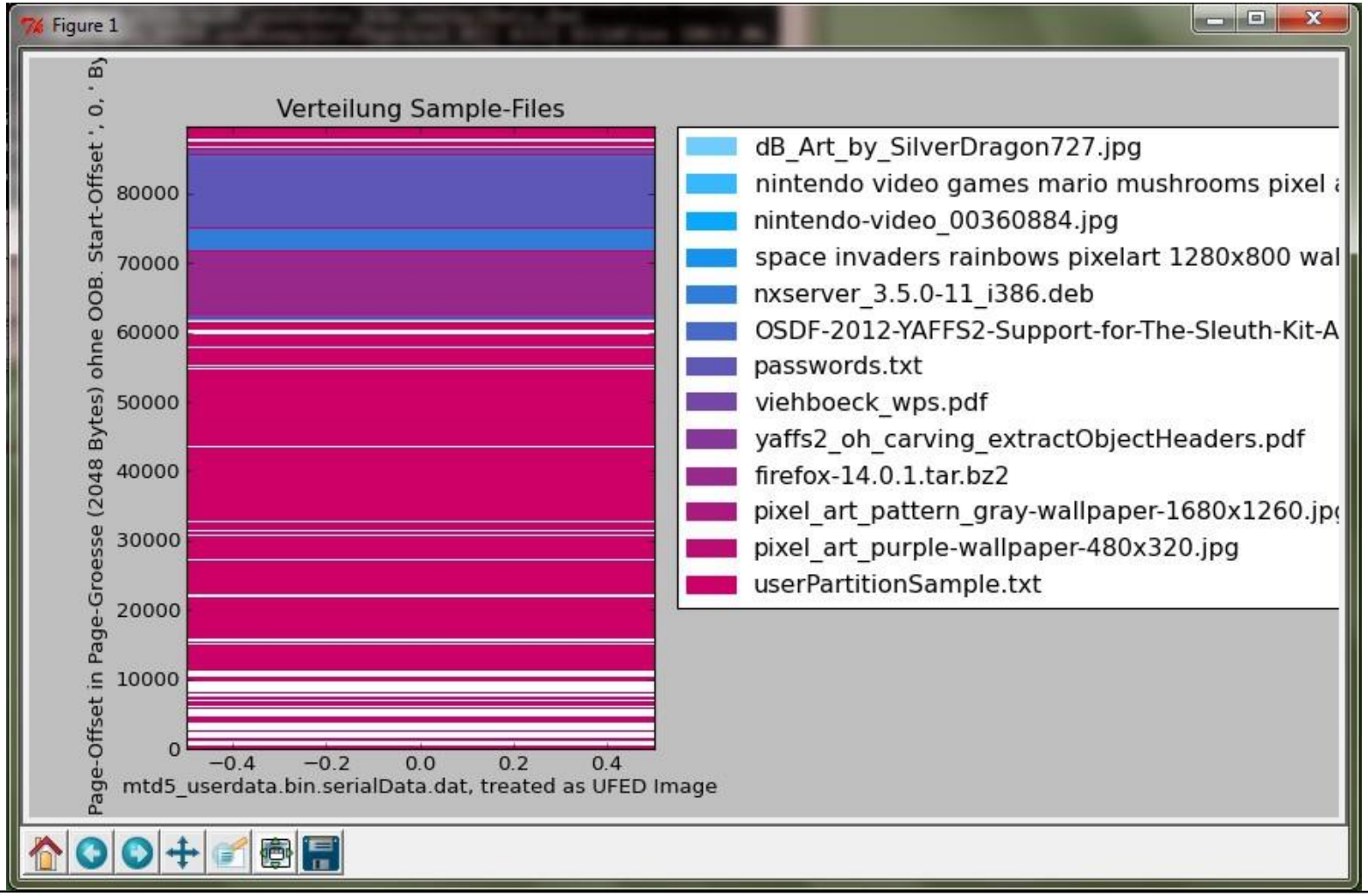
Visualisierung

- Entwicklung „Proof-of-concept“ Anwendung
- Verteilung durch Wear-Leveling
- Erkennung von MTD Partitionen
- Beobachtung Abnutzung



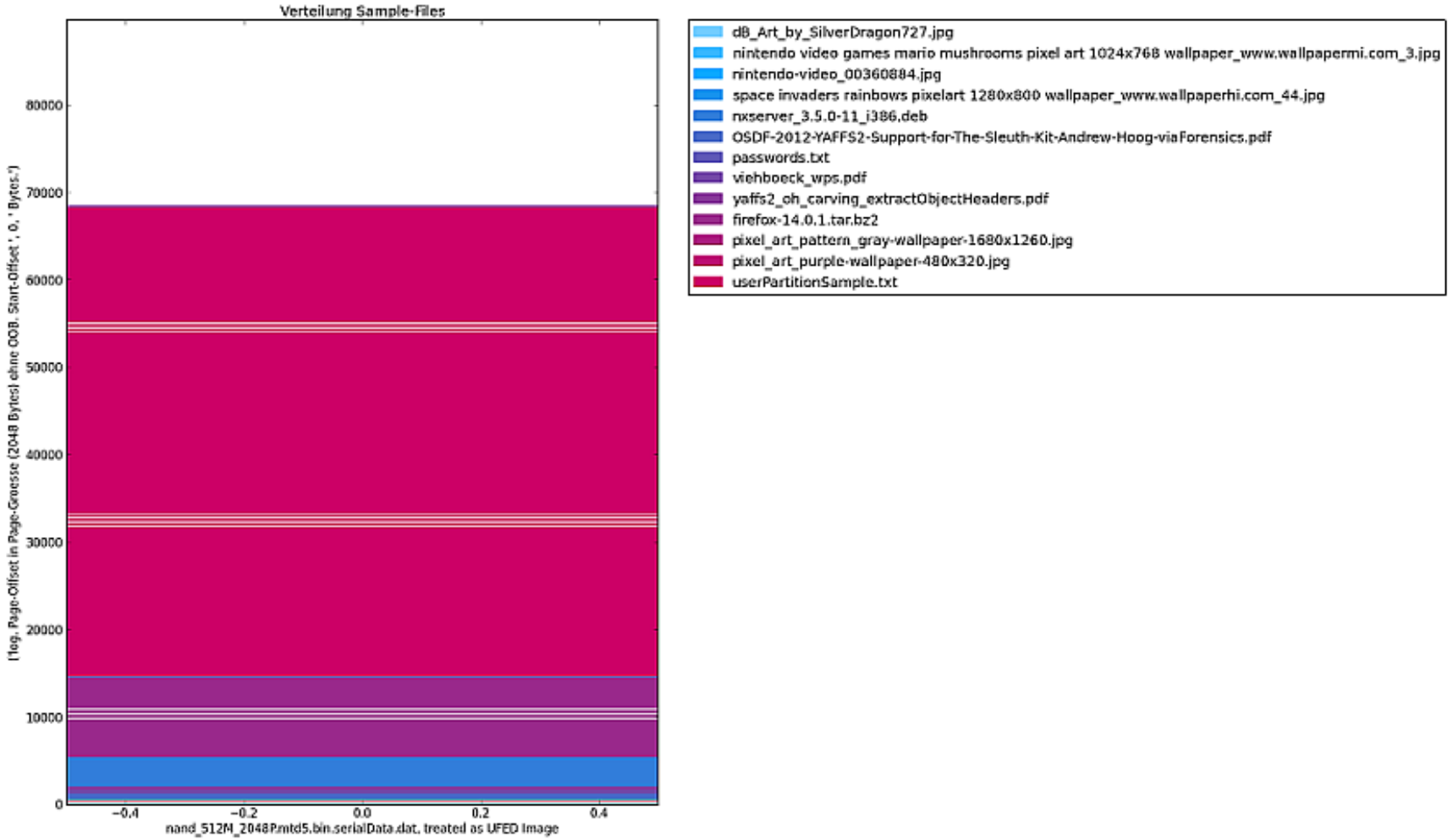
Visualisierung

- UFED Image, Nutzerpartition des HTC Wildfire



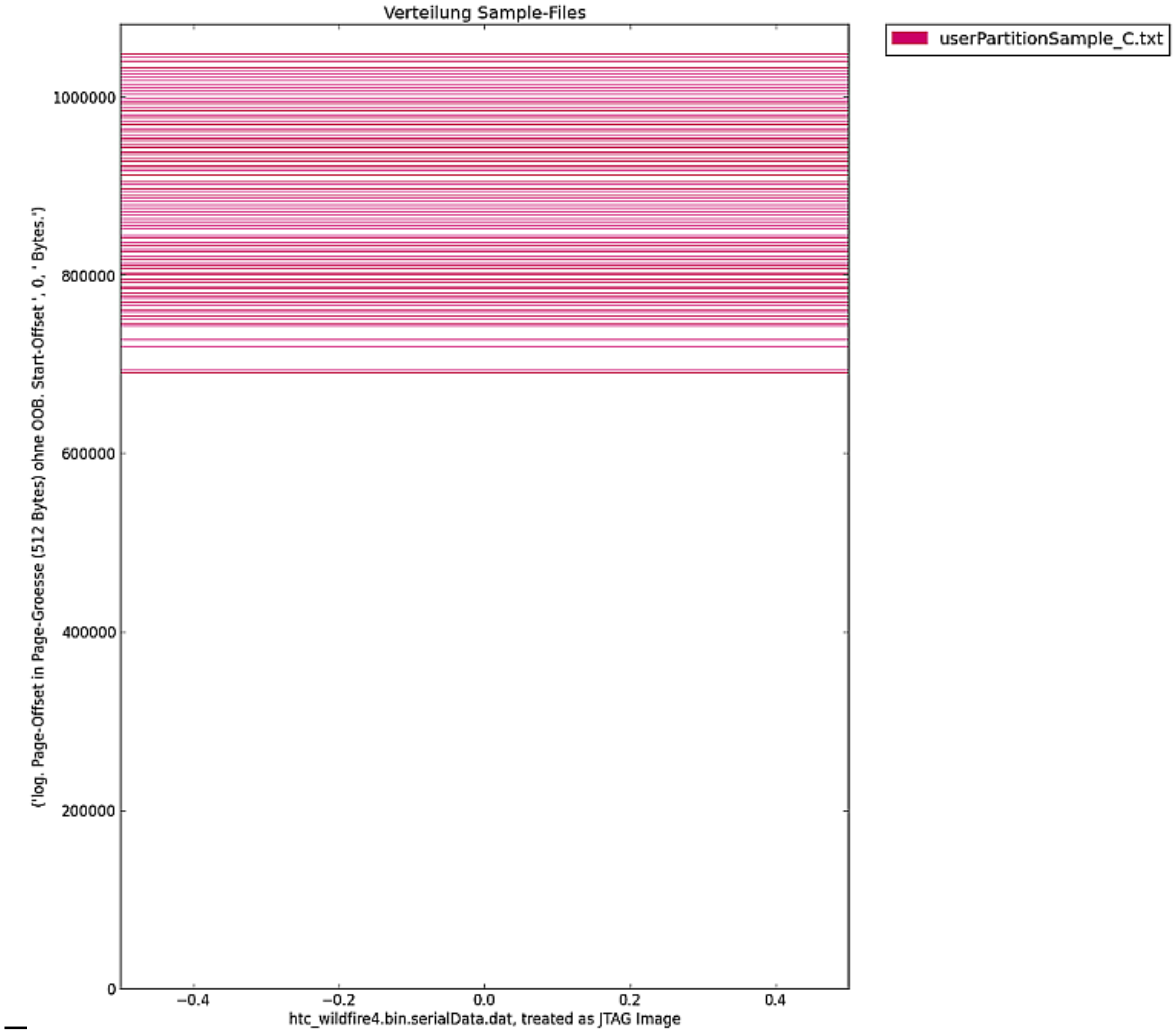
Visualisierung

- Simulierter NAND, Nutzerpartition



Visualisierung

- JTAG Image



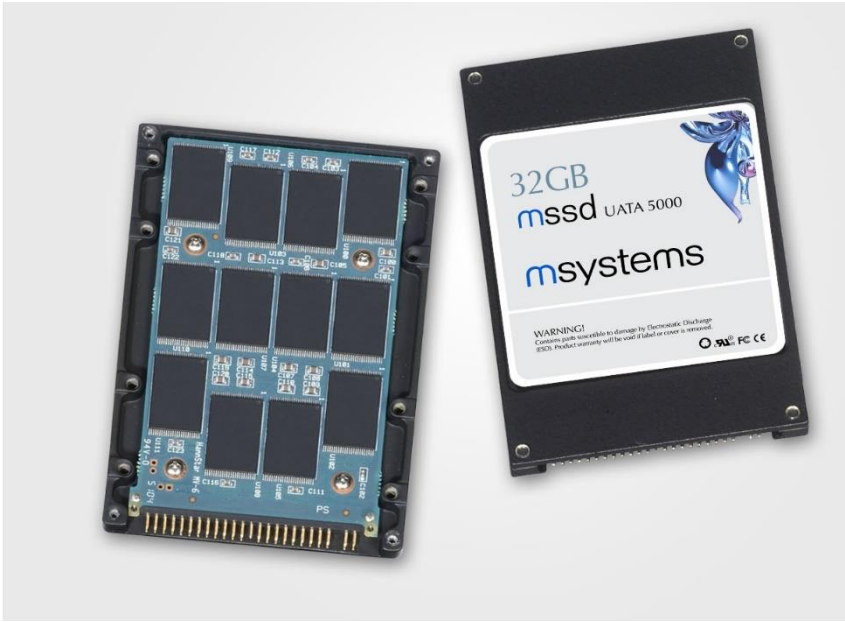
Fazit

- Viele falsche Informationen
- Unterschiedliche Möglichkeiten der Sicherung
- Ext4 ab Android 2.3
- Wechsel zu eMMC als Festspeicher
- Ein Einstieg für Interessierte

Vielen Dank für Ihre Aufmerksamkeit.

Kontakt: erbach@fh-aachen.de

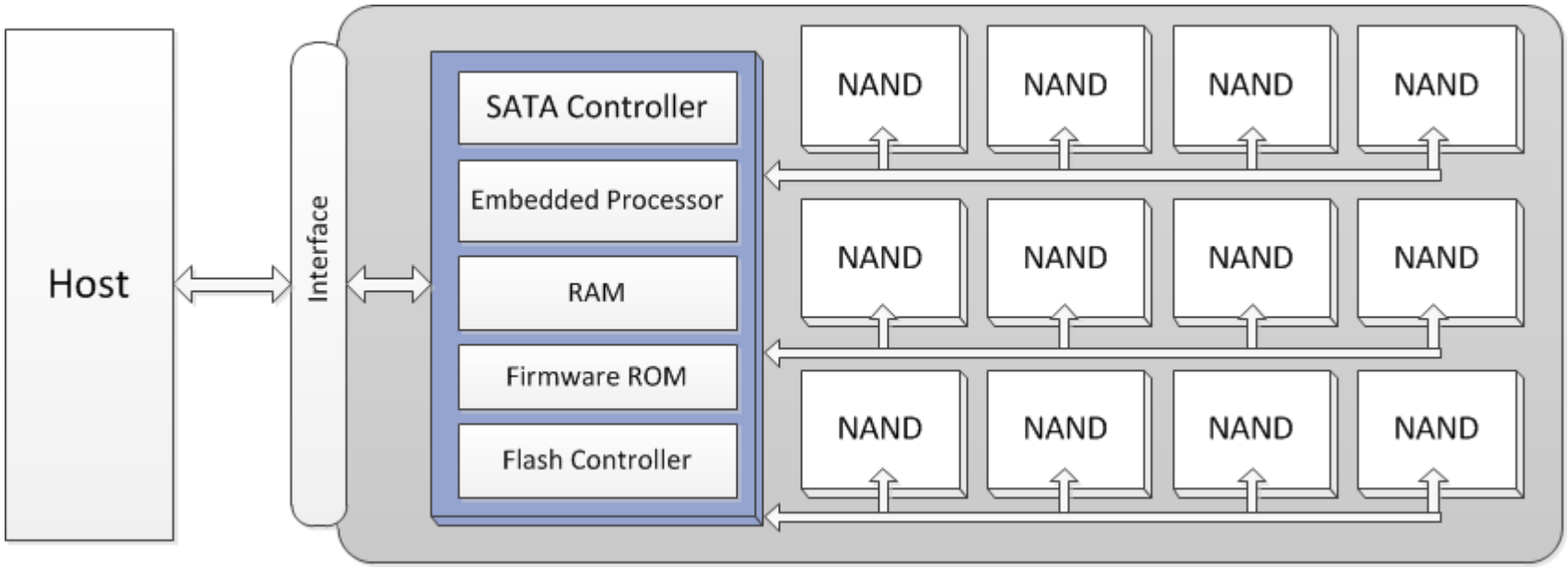
HDD vs SSD



Quelle: Wikipedia.de – SSD, http://creativecommons.org/licenses/by-sa/2.5/deed.de, ivob@stonline.sk

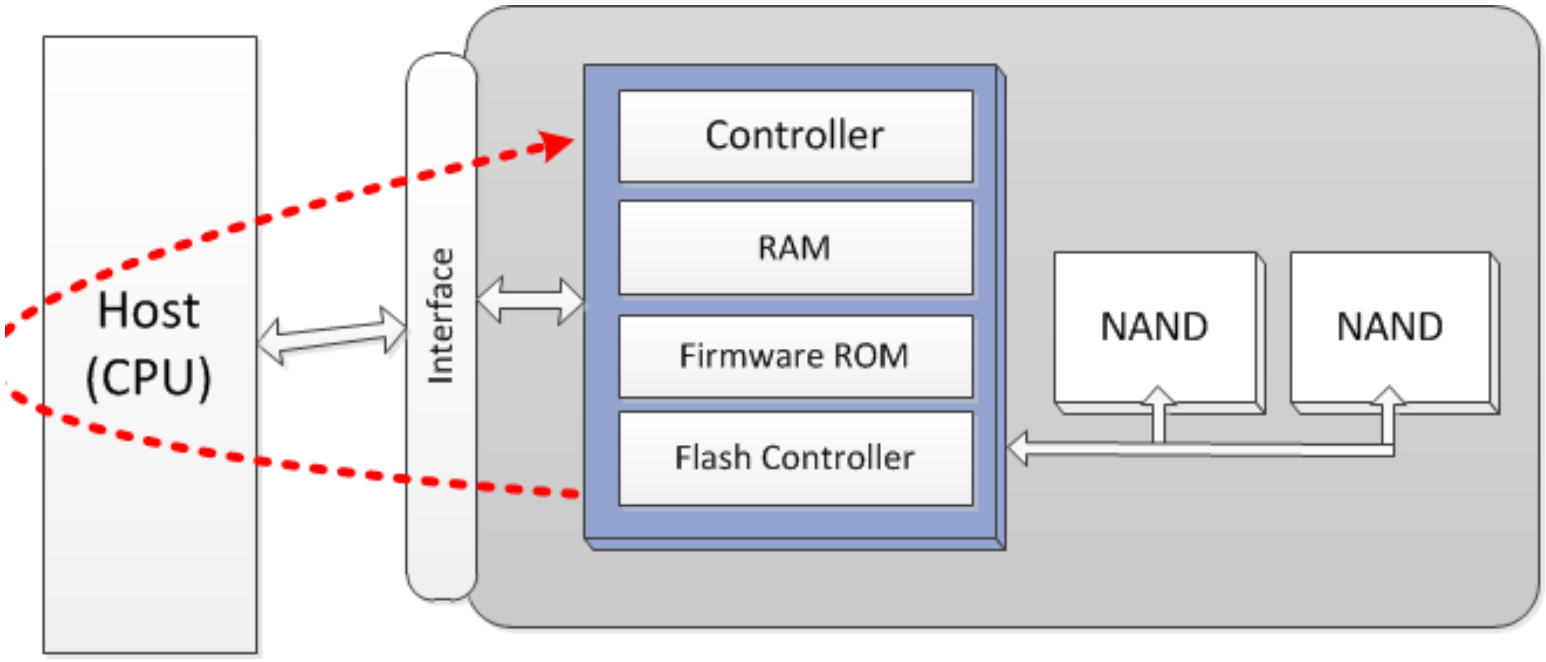
USB Stick und SSD

SSD

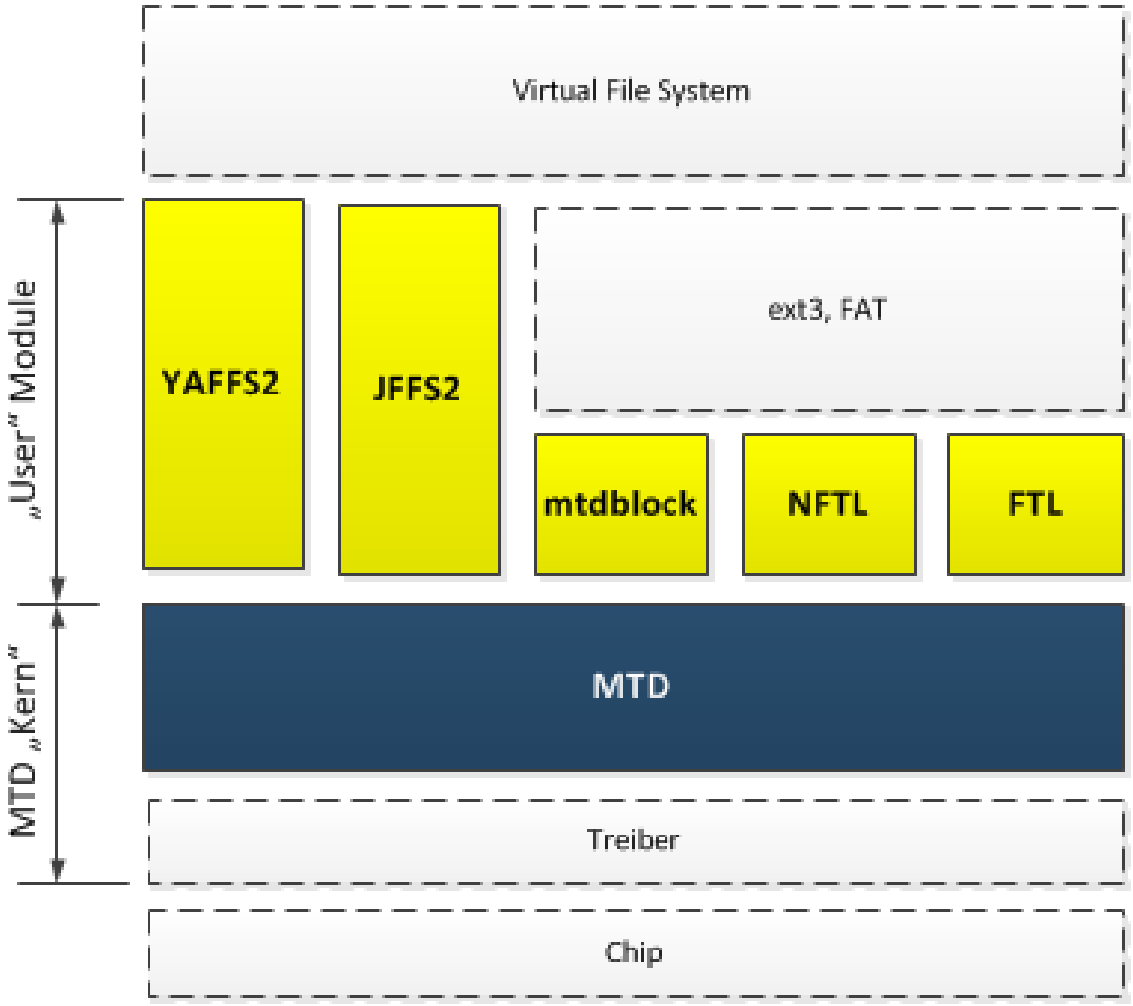


USB Stick und SSD

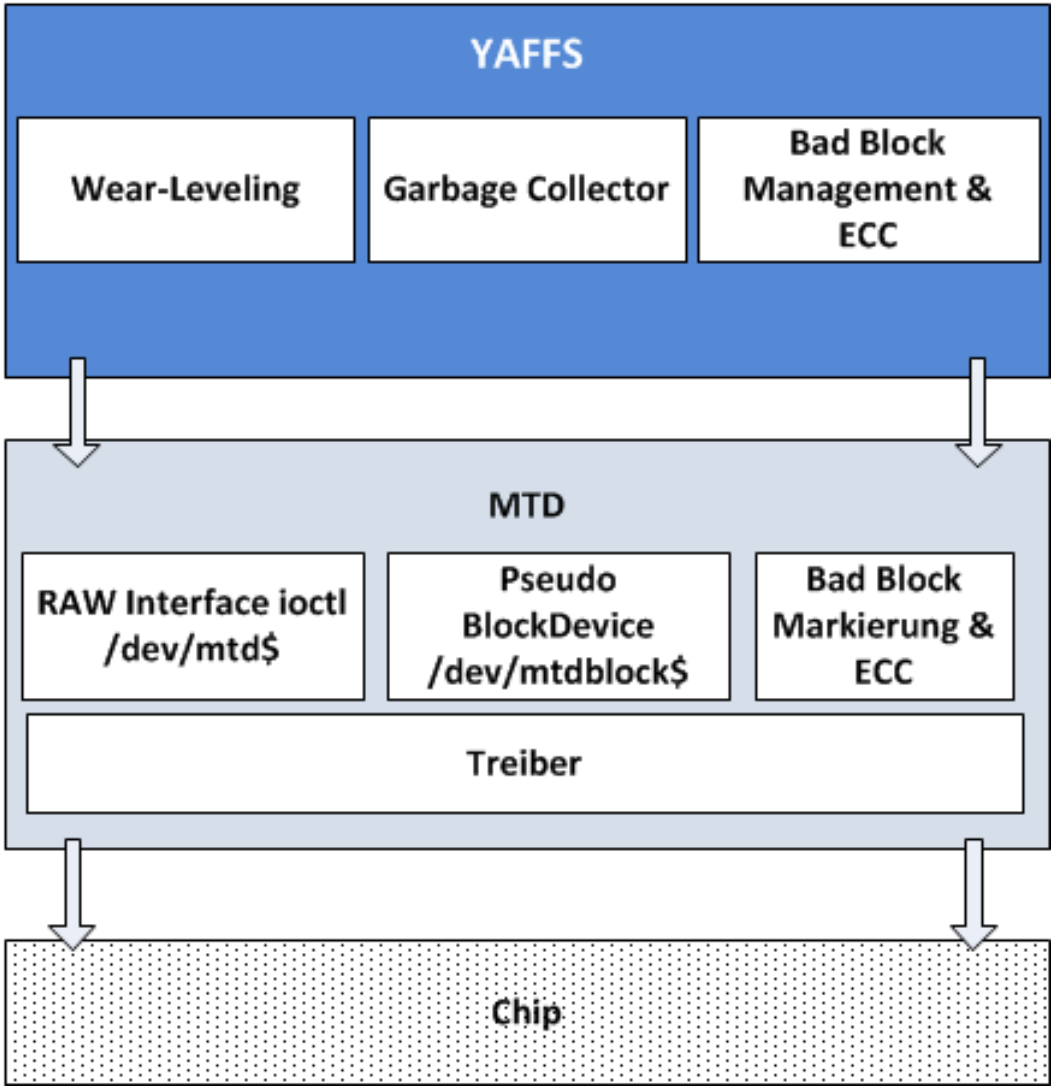
USB-Stick



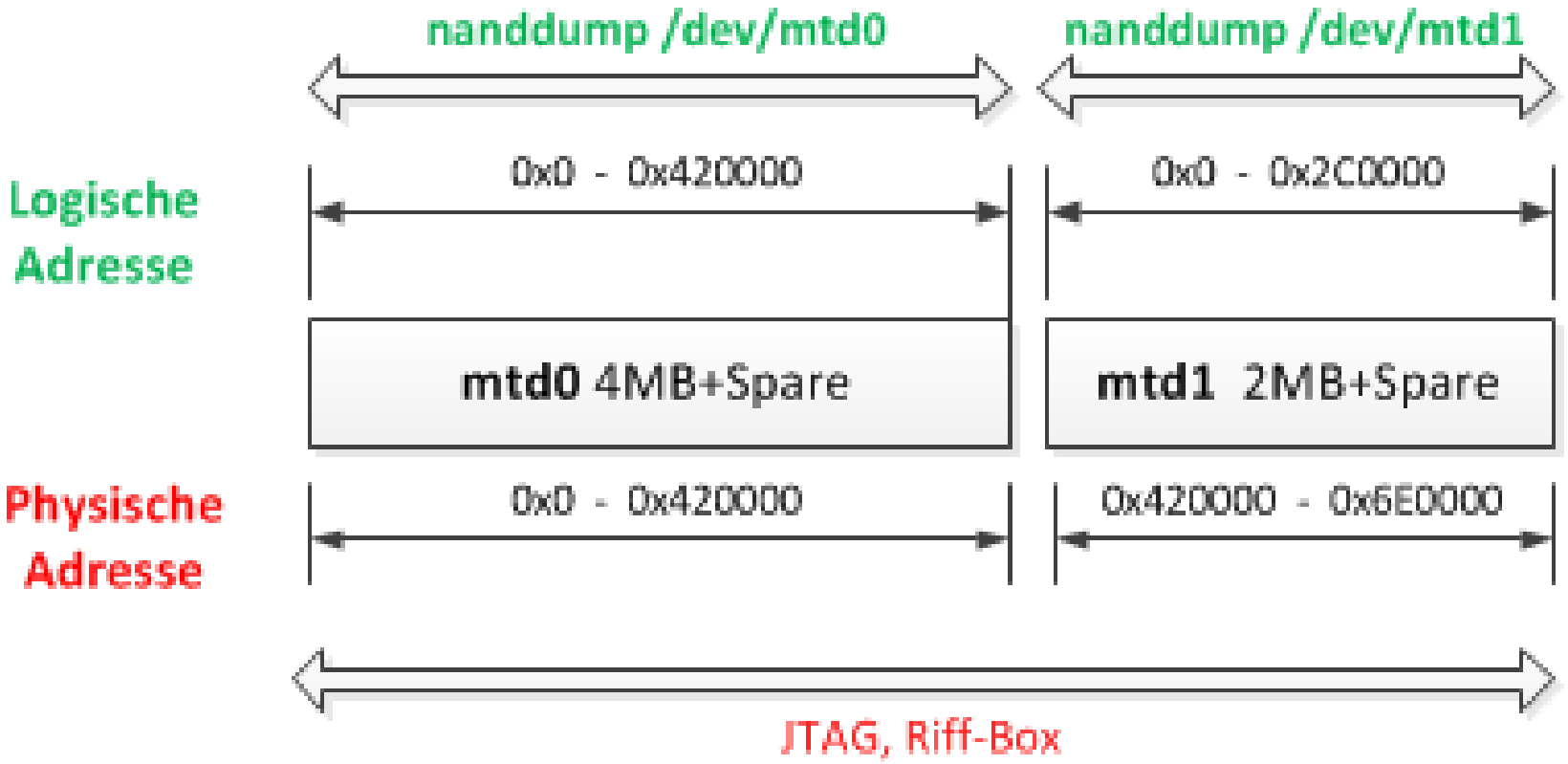
Speicherverwaltung



Speicherverwaltung



Speicherverwaltung



Speicherverwaltung