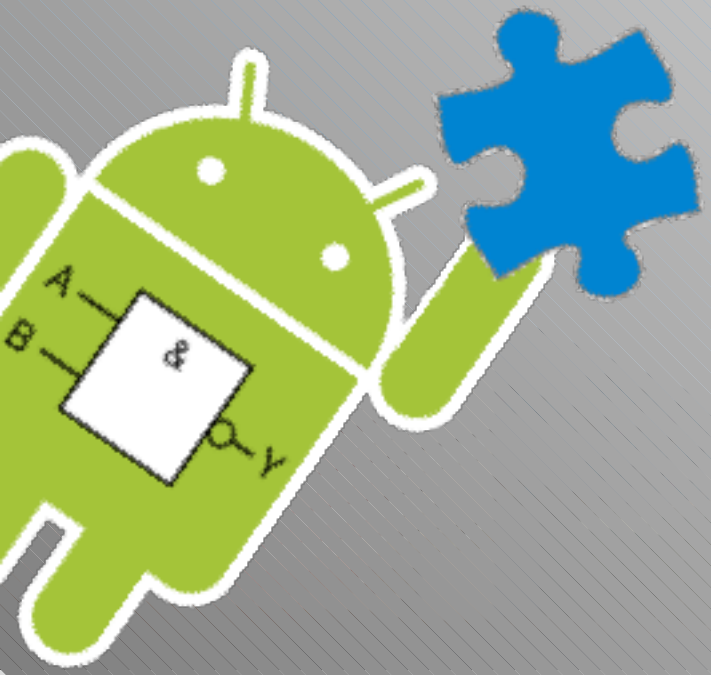
POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

FH AACHEN
UNIVERSITY OF APPLIED SCIENCES



Kurzbeschreibung einer laufenden Bachelorarbeit

„Undo(ing) the Android flash puzzle“

Eine Kooperation zwischen der FH Aachen und dem LKA NRW

Aachen, 24. April 2013

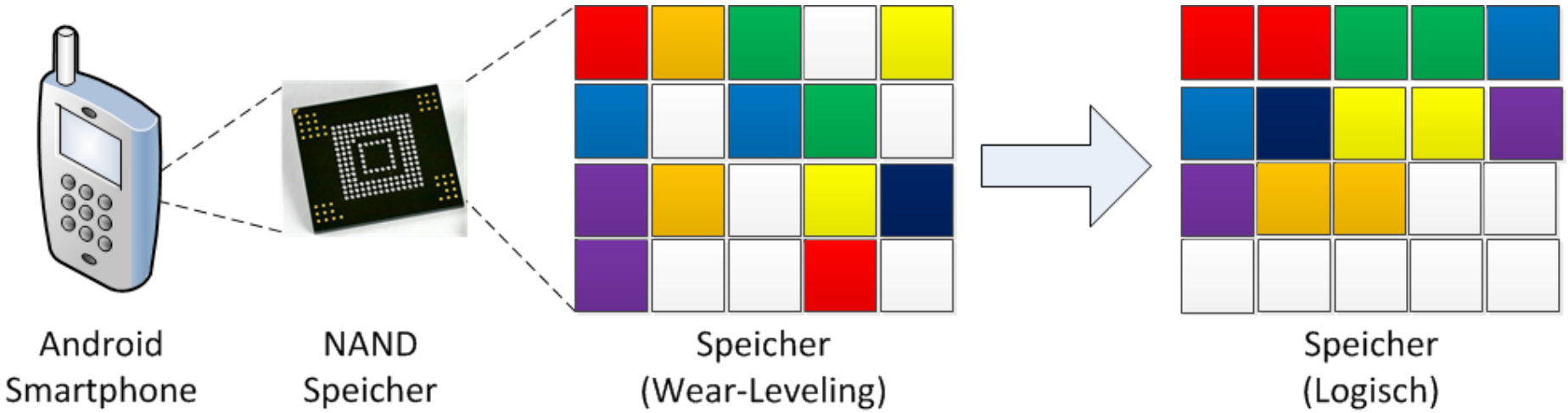
Auftakt

„Undo(ing) the Android flash puzzle“

Umkehrung des MTD/YAFFS2 Wear-Leveling und Wiederherstellung eines logischen Datenträgerabbildes, auf Basis eines via JTAG gewonnenen Rohimages eines internen Samsung NAND-Flash Bausteins, eines HTC Android Smartphones.

Auftakt

„Undo(ing) the Android flash puzzle“

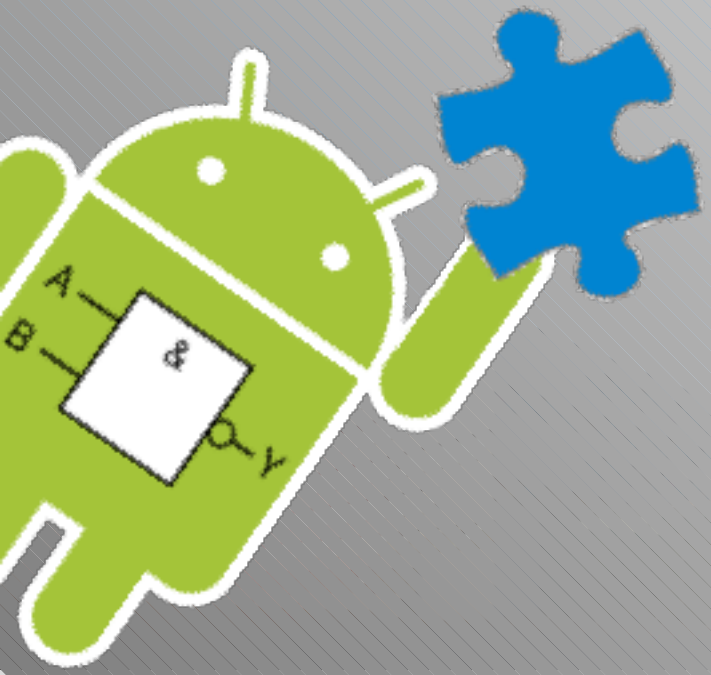


Agenda

- Warum NAND-Speicher
  - Aufbau
  - Besonderheiten des Wear-Leveling
- Warum Android
  - Zahlen und Fakten
  - Umgang mit NAND-Speicher
- Ziel der Abschlussarbeit

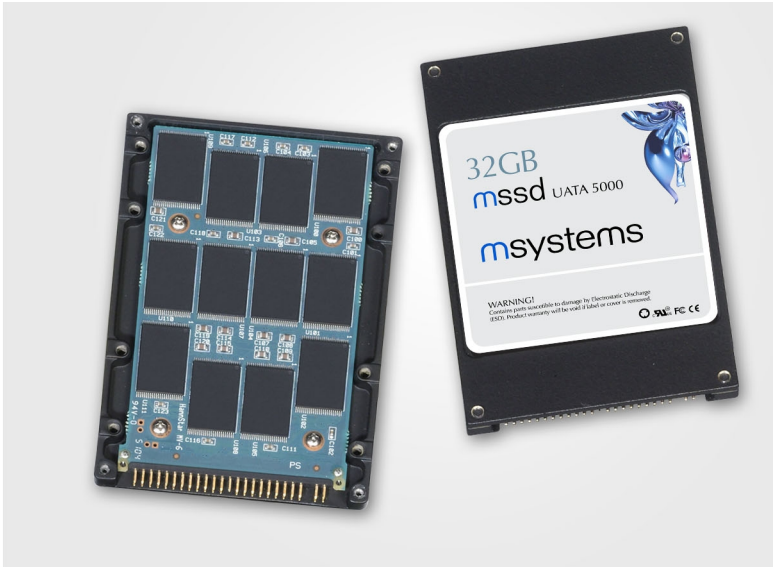
POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

FH AACHEN
UNIVERSITY OF APPLIED SCIENCES



Warum NAND-Speicher

Warum NAND-Speicher

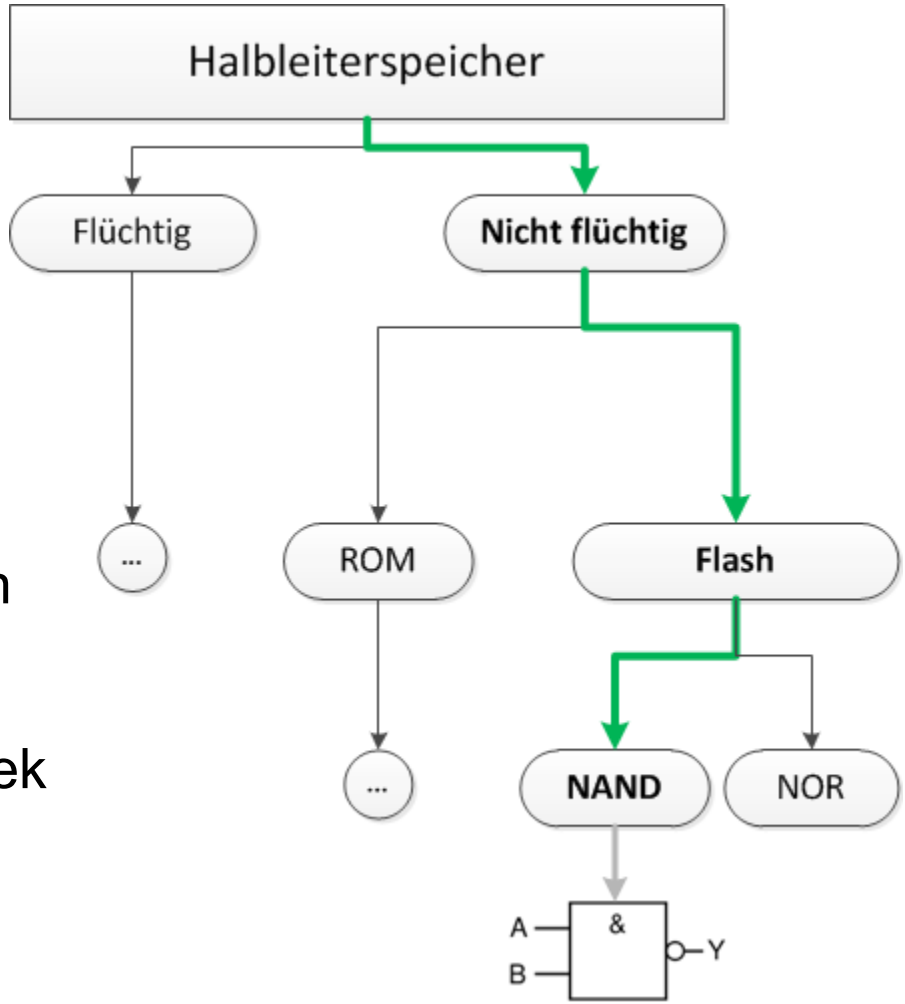


- „Echte“ digitale Speicherung
- Verbesserte, mobile Eigenschaften
- Keine „losen“ Bauteile

Warum NAND-Speicher

Warum NAND-Speicher

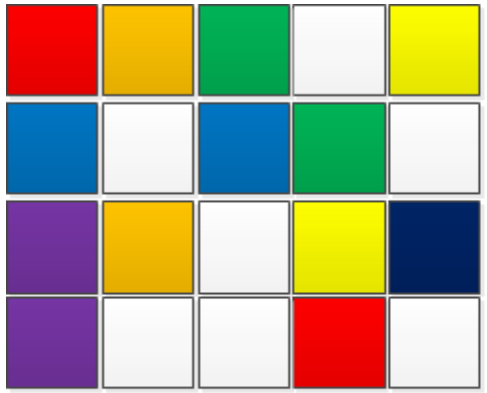
- Halbleiterspeicher
  - Hohe Schocktoleranz
  - Schneller Zugriff
  - Vibrationsfrei
  - Günstige Herstellung
  - Geringer Stromverbrauch
  - Kompakte Bauform
  - Idee seit 1978, StorageTek



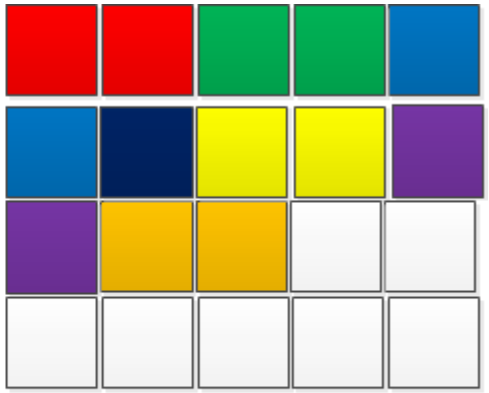
Quelle: nach [1]

Warum NAND-Speicher - Besonderheiten

- Blick vom Smartphone auf NAND: logischer Zusammenhang
- Blick direkt auf NAND: Verwürfelte Blöcke
- Wie kann das sein ?



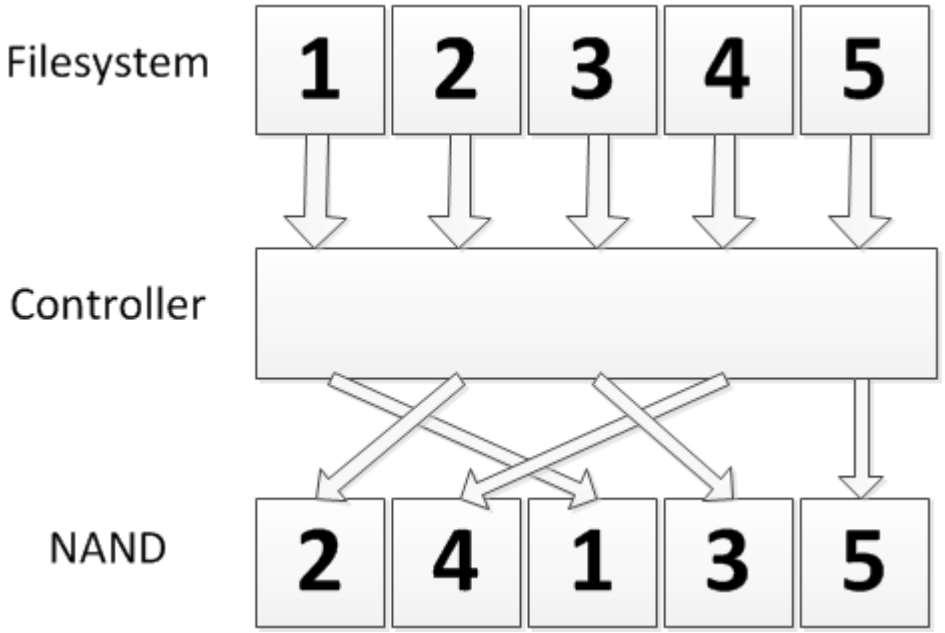
Physischer Speicher



Logischer Speicher

Warum NAND-Speicher - Besonderheiten

- Wear-Leveling
  - Bemühung um gleichmäßige Abnutzung der Zellen
  - Kein direkter Zugriff auf Speicherplatz
  - Geschwindigkeitszuwachs durch Multichannel



Quelle [2]

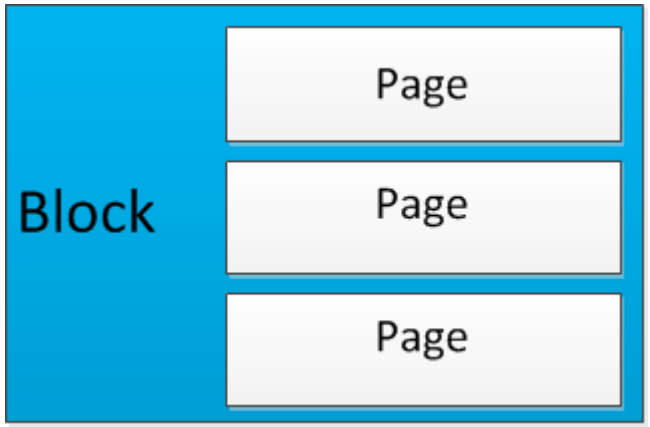
Warum NAND-Speicher - Besonderheiten

- Page direkt lesbar
- Page direkt beschreibbar, wenn leer
- Löschen nur als Block

- Page, 2048 Bytes + 64 Bytes Flags
- Block, 64x Pages
- Größe der Pages und Block abhängig von Gesamtgröße des Speichers

Warum NAND-Speicher - Besonderheiten

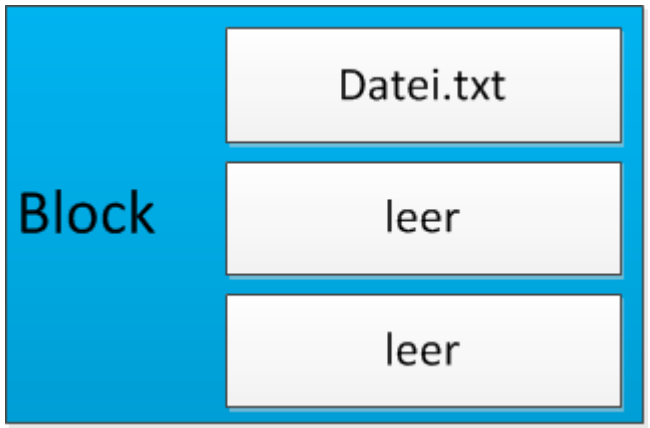
- Page direkt lesbar
- Page direkt beschreibbar, wenn leer
- Löschen nur als Block
- Beispiel: „Datei.txt“ entspricht Größe der Page, 2048 Bytes



Quelle: Bsp nach [3]

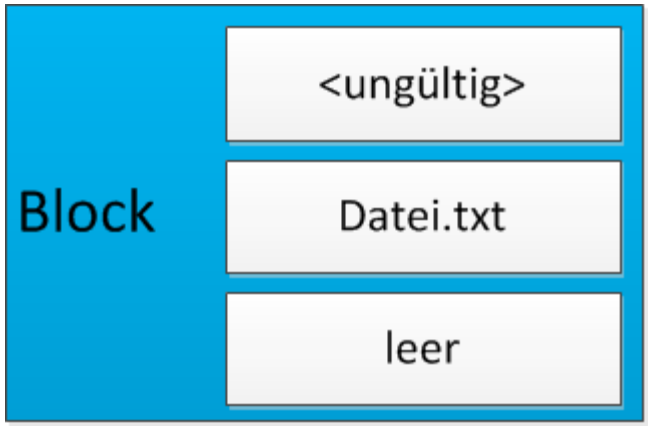
Warum NAND-Speicher - Besonderheiten

- Page direkt lesbar
- Page direkt beschreibbar, wenn leer
- Löschen nur als Block
- Beispiel: „Datei.txt“ entspricht Größe der Page, 2048 Bytes



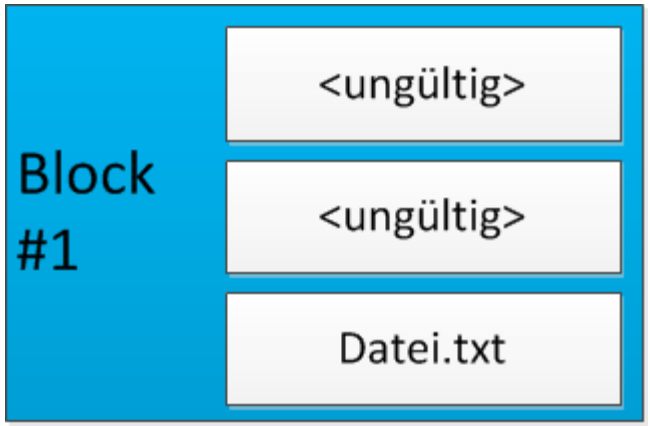
Warum NAND-Speicher - Besonderheiten

- Änderung der Datei
- Markierung Speicherbereich
- Kopiere mit Änderung in neue Page



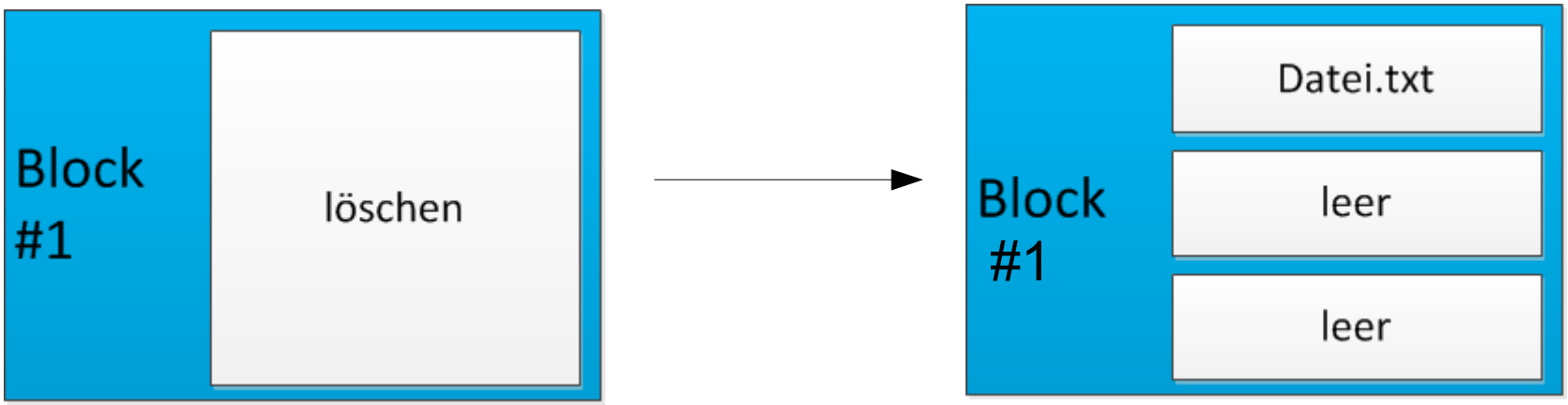
Warum NAND-Speicher - Besonderheiten

- Änderung der Datei
- Markierung Speicherbereich
- Kopiere mit Änderung in neue Page
- Problem: keine freie Page



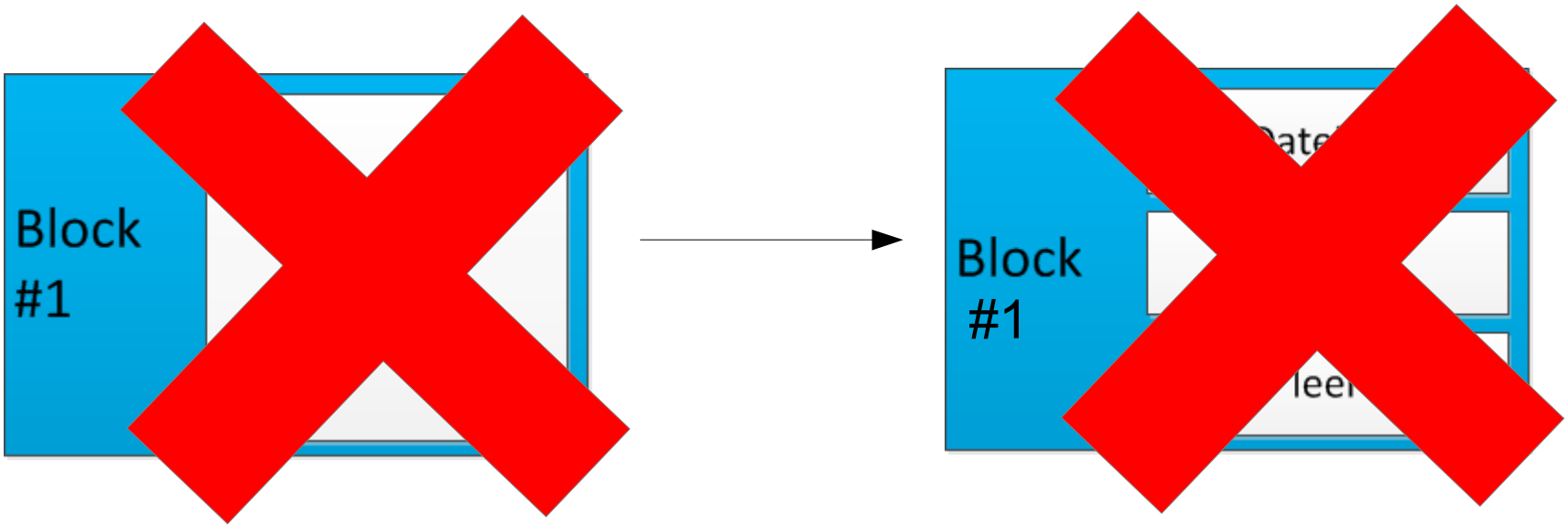
Warum NAND-Speicher - Besonderheiten

- Erinnerung: Löschen nur als Block
- 2 Operationen, löschen und kopieren
- Starke Abnutzung der gleichen Zellen



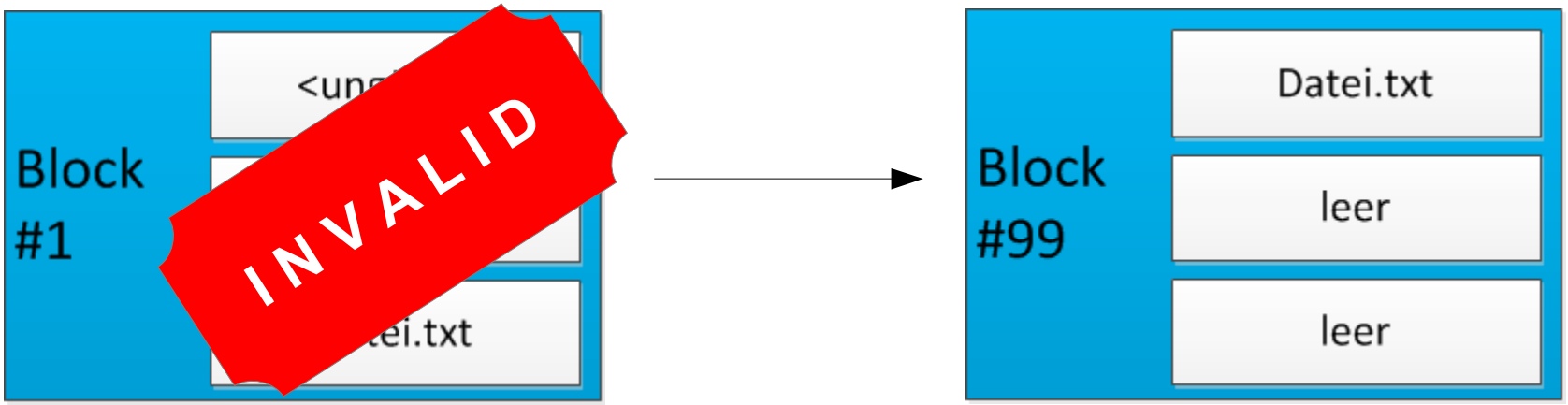
Warum NAND-Speicher - Besonderheiten

- Erinnerung: Löschen nur als Block
- 2 Operationen, löschen und kopieren
- Starke Abnutzung der gleichen Zellen



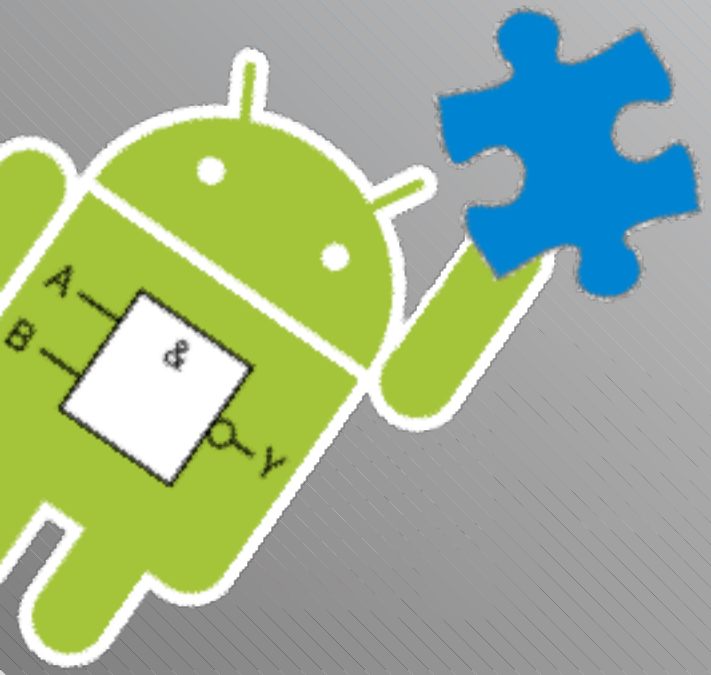
Warum NAND-Speicher - Besonderheiten

- Alter Block wird markiert
- Kopie des Blocks mit Änderung in neuen Block
- Neuer Block ist „jünger“



POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

FH AACHEN
UNIVERSITY OF APPLIED SCIENCES



Warum Android

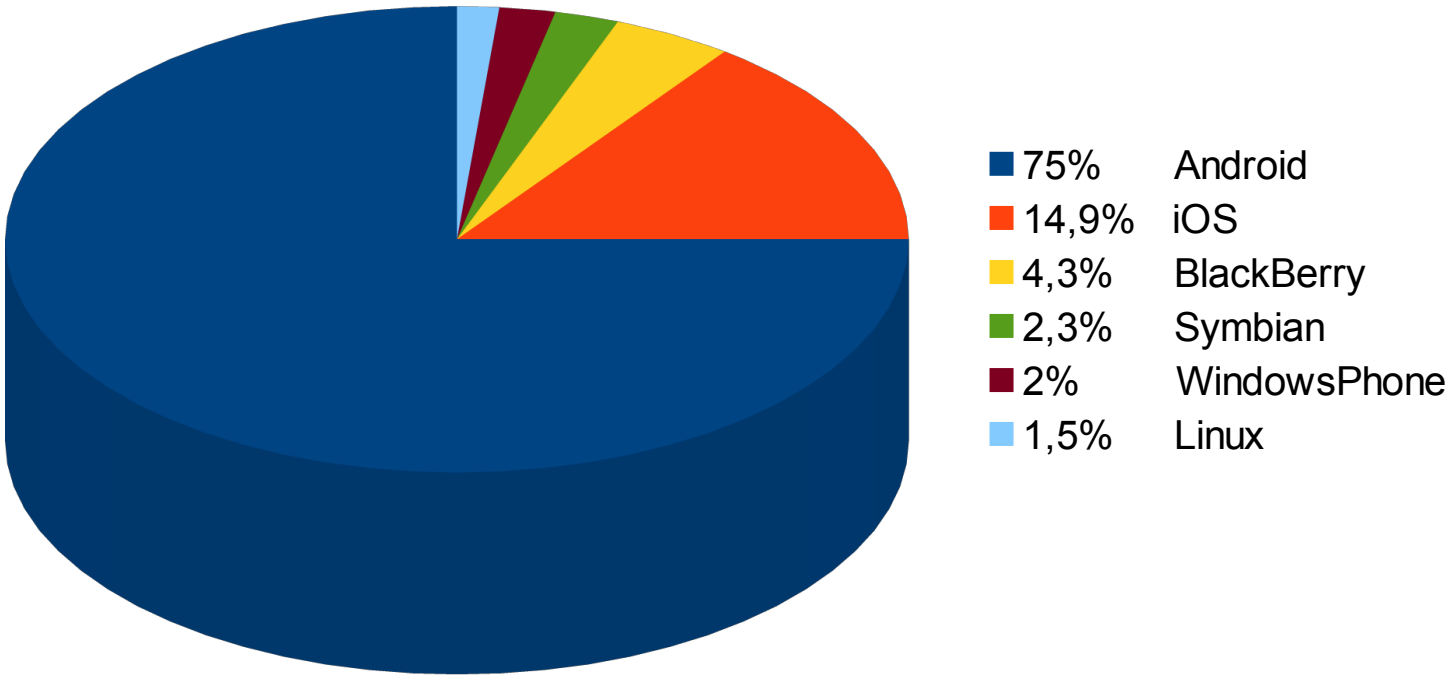
Warum Android – Zahlen & Fakten

- Stabiles Linux
- Einfache Bedienung
- Großes Angebot an Apps

- Android ist freie Software
- Der größte Teil der Plattform
  - Apache-Lizenz
- Systemkern
  - GPL 2
- Quelltext für Tablets
  - für Version 3 & 4 freigegeben

Warum Android – Zahlen & Fakten

- Marktanteile im Verkauf, 3. Quartal 2012



Quelle: *International Data Corporation, Press Release (1.Nov.2012),*
„Android Marks Fourth Anniversary Since Launch with 75.0% Market Share in Third Quarter“ [6]

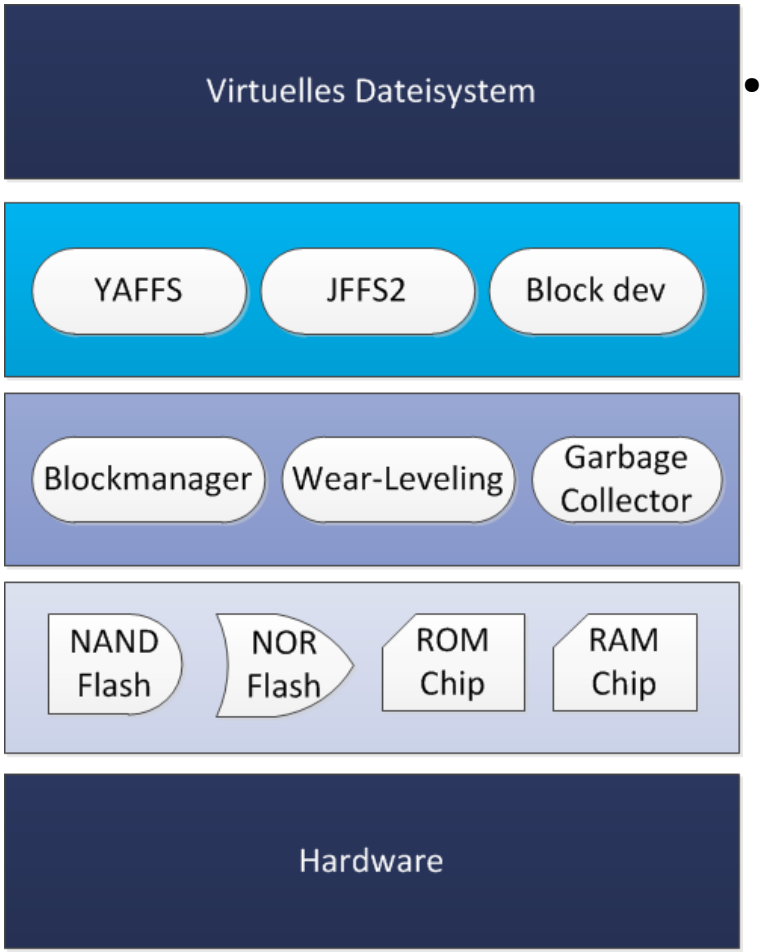
Warum Android – Umgang mit NAND

- Verwaltung des NAND-Speichers im Regelfall

- Aufgabe des Speicher-Controllers (u.a.)
  - FTL: Flash Translation Layer
  - Wear-Leveling
  - Bad-Block-Managment
- NAND und Controller aufeinander abgestimmt
- Firmware und Algorithmen proprietär
- USB-Stick, MMC, SD Card sind Blockdevices

Warum Android – Umgang mit NAND

- Verwaltung des NAND-Speichers unter Android

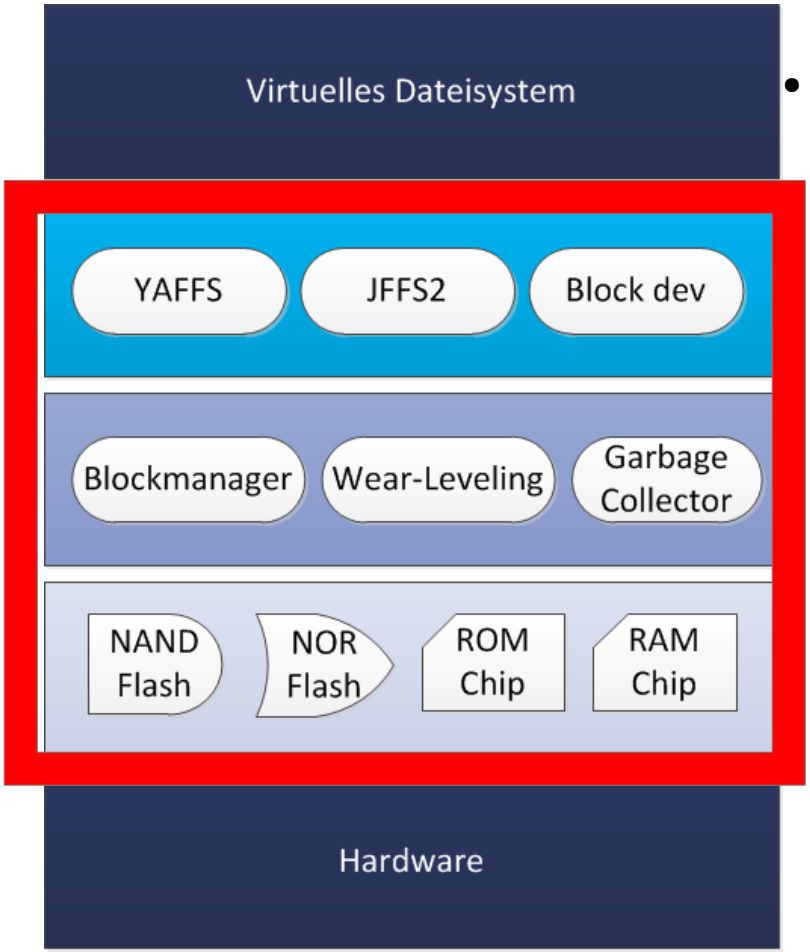


Quelle: nach [4][5]

- Linux MTD (Memory Technology Device)
  - Software-Layer des Betriebssystems
  - FTL: Flash Translation Layer
  - Wear-Leveling
  - Bad-Block-Managment
- Kompatibel mit Vielzahl an NAND Bausteinen

Warum Android – Umgang mit NAND

- Verwaltung des NAND-Speichers unter Android

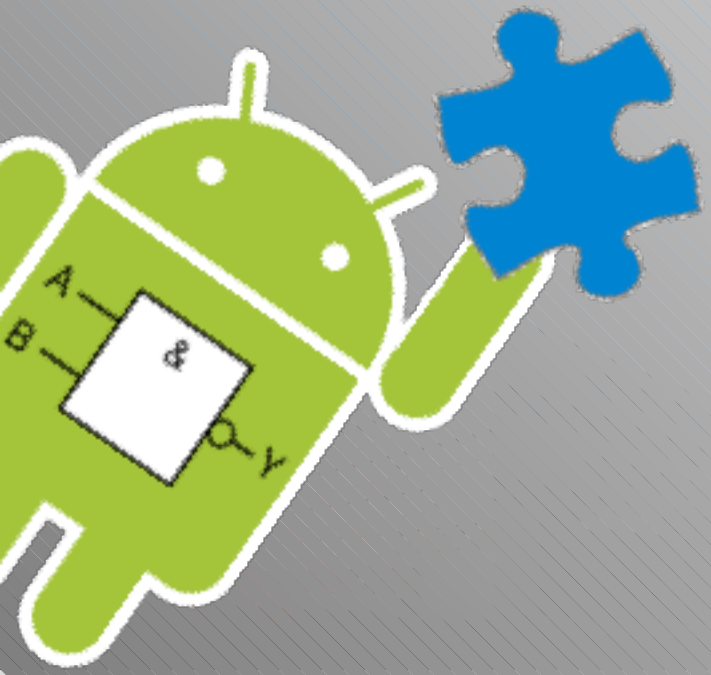


Quelle: nach [4][5]

- Linux MTD (Memory Technology Device)
  - Software-Layer des Betriebssystems
  - FTL: Flash Translation Layer
  - Wear-Leveling
  - Bad-Block-Managment
- Kompatibel mit Vielzahl an NAND Bausteinen

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

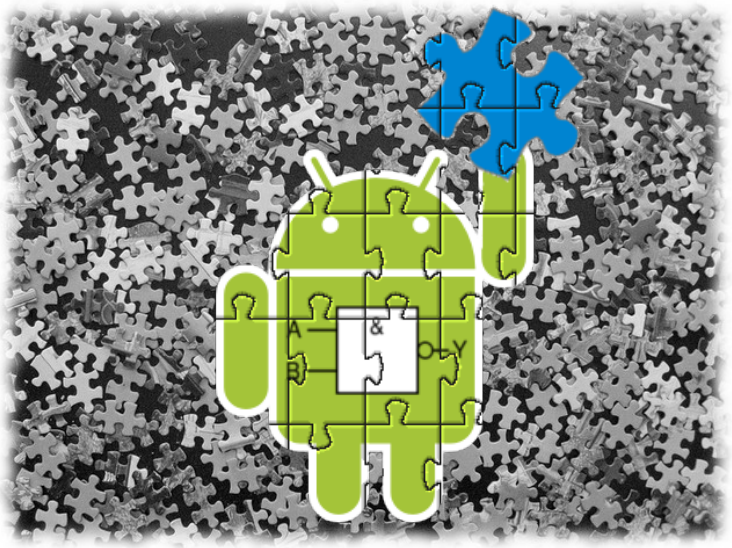
FH AACHEN
UNIVERSITY OF APPLIED SCIENCES



Ziel der Abschlussarbeit

Ziel der Abschlussarbeit

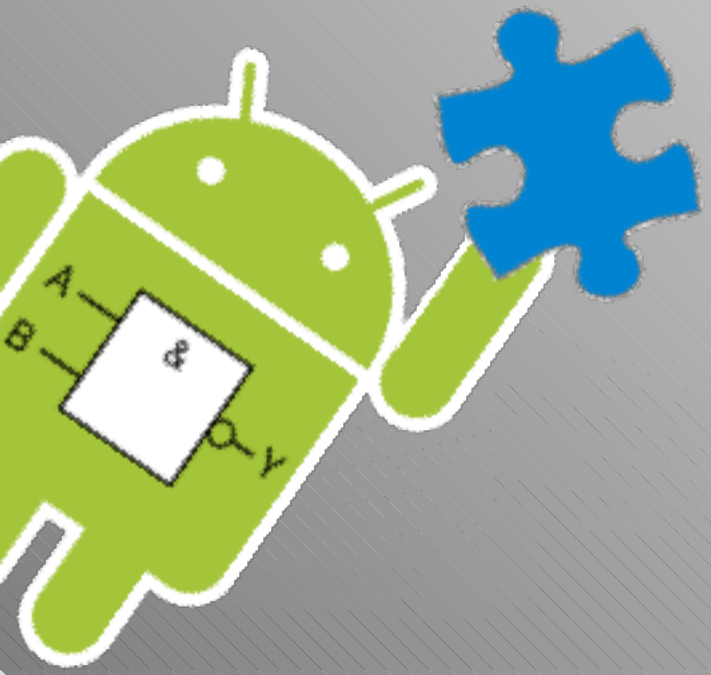
- Analyse und Rückführung des Wearleveling
- Logisches Image
- Erkennung der Partitionsgrenzen
- Wiederherstellung Filesystem
- Versionierung der Dateien



- Voraussichtliches Ende, August/September 2013

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

FH AACHEN
UNIVERSITY OF APPLIED SCIENCES



Vielen Dank für Ihre Aufmerksamkeit

Bildnachweis

POLIZEI Nordrhein-Westfalen Landeskriminalamt

FH AACHEN UNIVERSITY OF APPLIED SCIENCES

- Folie 1, Android-Logo: The Android robot is reproduced or modified from work created and shared by Google and used according to terms described in the Creative Commons 3.0 Attribution License; Android is a trademark of Google Inc. https://developer.android.com/images/brand/Android_Robot_200.png
- Folie 1 und 26, verändertes Android-Logo: „NAND-Android-Puzzle“, Michel Erbach
- Folie 3, Darstellung NAND-Chip: „Samsung Introduces Advanced Memory Storage Solution for Slim Smartphones and Tablets“, samsungtomorrow, https://secure.flickr.com/photos/samsungtomorrow/, CC BY-NC-SA 2.0
- Folie 3, Darstellung Zusammenhang Smartphone-NAND-Blocks: „Grafische Darstellung BA“, Michel Erbach
- Folie 6, Darstellung Festplatte&SSD: „Disassembled HDD and SSD“, Rochellesinger, https://commons.wikimedia.org/wiki/File:Disassembled_HDD_and_SSD.JPG?uselang=de, CC-BY-SA-2.5
- Folie7, Darstellung HTC Wildfire: „HTC Wildfire“, BestBoyZ, https://secure.flickr.com/photos/bestboyzde/, CC BY-ND 2.0
- Folie 7. Darstellung SanDisk UsbStick: „USB Flash drive“, evansonline, https://secure.flickr.com/photos/evansfam/, CC BY-NC-SA 2.0
- Folie 7, Darstellung Kingston SD-Karte: „512MB Secure Digital card“, Andrew MacKinnon, https://secure.flickr.com/photos/andrewmackinnon/, CC BY-SA 2.0
- Folie 8, Darstellung Auszug Halbleiter-Familie: „Auszug Halbleiter-Stammbaum“, Michel Erbach (Nach Quelle: https://de.wikipedia.org/wiki/Halbleiterspeicher)
- Folie 9, Darstellung physischer und logischer Speicher: „Vergleich physisch & logischer Speicher“, Michel Erbach

Bildnachweis

POLIZEI Nordrhein-Westfalen Landeskriminalamt

FH AACHEN UNIVERSITY OF APPLIED SCIENCES

- Folie 10ff, Darstellung Block & Pages: „Mini-Beispiel WriteAmp&Wear-Leveling“, Michel Erbach (Nach Quelle: https://de.wikipedia.org/wiki/Solid-State-Drive)
- Folie 10, Darstellung Wear-Leveling: „Vereinfachte Darstellung Wear-Leveling“, Michel Erbach
- Folie 20, Darstellung HTC Wildfire S: „HTC Wildfire S“, BestBoyZ, https://secure.flickr.com/photos/bestboyzde/, CC BY-ND 2.0
- Folie 22, Darstellung USB-Platine: „32GB USB thumb drive 2“, Gadget_Guru, https://secure.flickr.com/photos/28502132@N05/, CC BY 2.0
- Folie 23&24, Darstellung MTD: „Vereinfachung MTD Layer“, Michel Erbach
- Folie 26, Darstellung S/W Puzzel: „puzzled“, eworm, https://secure.flickr.com/photos/eworm/, CC BY-NC-SA 2.0

Quellen

- [1] Halbleiterspeicher, Wikipedia, https://de.wikipedia.org/wiki/Halbleiterspeicher
- [2]
- [3] Methoden der Nutzungsverteilung, Wikipedia, https://de.wikipedia.org/wiki/Solid-State-Drive
- [4] Managing flash storage with Linux, Michael Opdenacker, http://free-electrons.com/blog/managing-flash-storage-with-linux/
- [5] Anatomy of Linux flash file systems, M. Tim Jones, http://www.ibm.com/developerworks/library/l-flash-filesystems/
- [6] International Data Corporation, https://www.idc.com/getdoc.jsp?containerId=prUS23771812, Abgerufen 16. April 2013