HOCHSCHULE MITTWEIDA
University of Applied Sciences

Bundeskriminalamt

Digitale Forensik
Betriebs- und Dateisysteme

Prof. Dr. rer. nat. Dirk Labudde

Dateisysteme

Dateisysteme

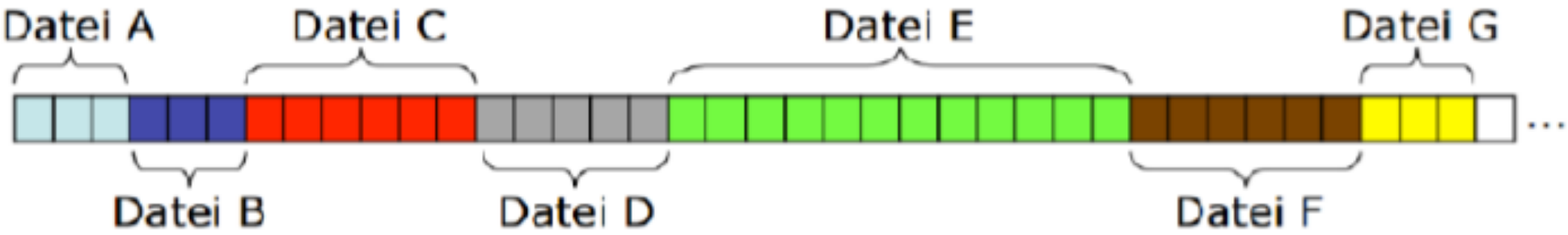
Begriffsbestimmung

- 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?

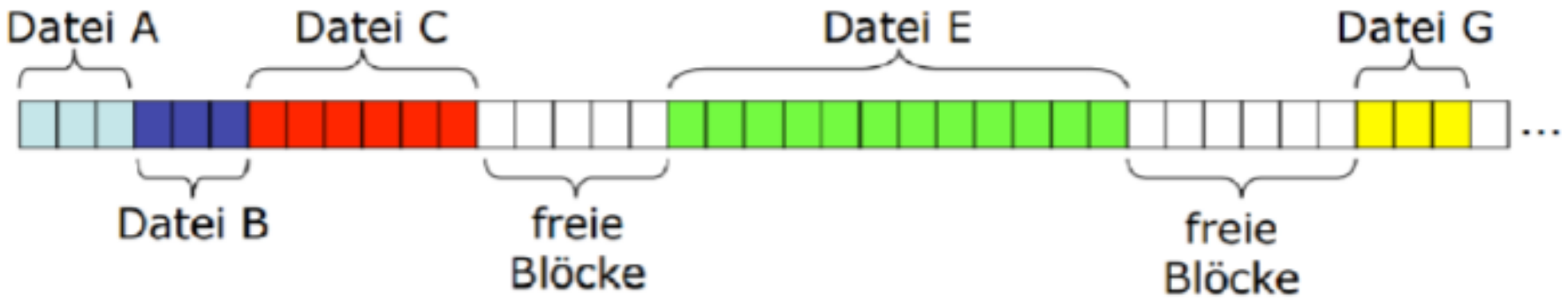


Vorteile: schnelles Lesen von Dateien mit wenigen Leseoperationen.

Welche **Nachteile** hätte eine solche Speicherorganisation?

Dateisysteme

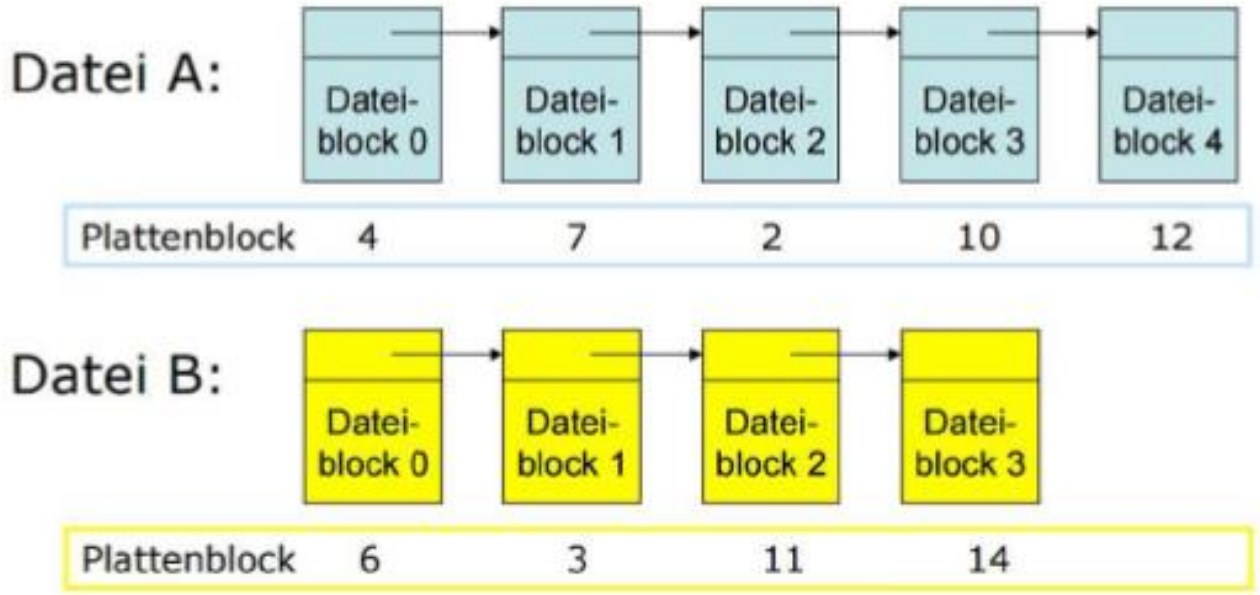
Nachteil hierbei ist die Fragmentierung des Datenträgers. Entstehende Lücken sind nur schwer zu beseitigen und ungeeignet für das Hinzufügen neuer Dateien (Graphik – gelöschte Datei D und F) . Diese Art der Datenorganisation wird daher ausschließlich für einmal Datenträger wie DVD genutzt.



Bei DVDs ist die Größe der Datei vorab bekannt und nicht veränderbar.

Verkettete Listen

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



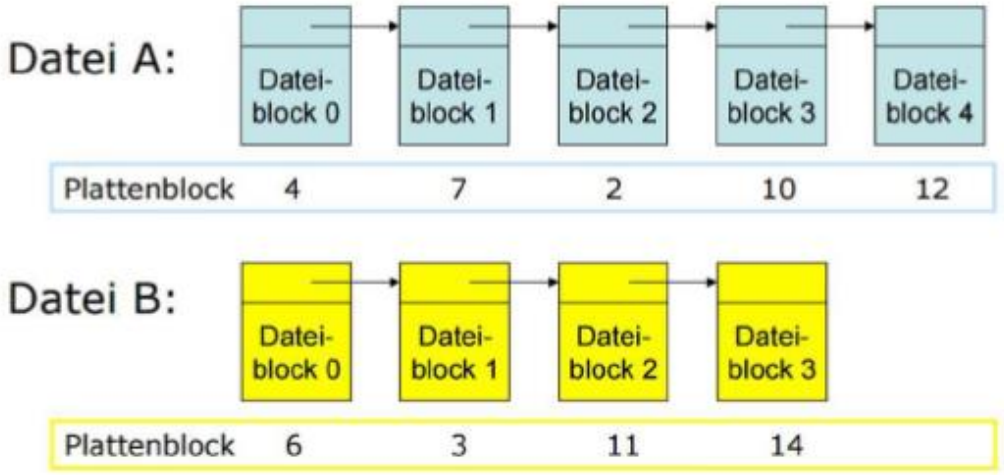
Verkettete Listen

Vorteil

- Fragmentierung führt nicht zu Speicherplatzverlust

Nachteil

- Mehrere Leseoperationen zum Auffinden eines bestimmten Blocks vom Anfang nötig (Zugriff wahlfrei)
- n-1 Zugriffe um Block n zu lokalisieren nötig
  → langsam



Verkettete Listen in einer Tabelle

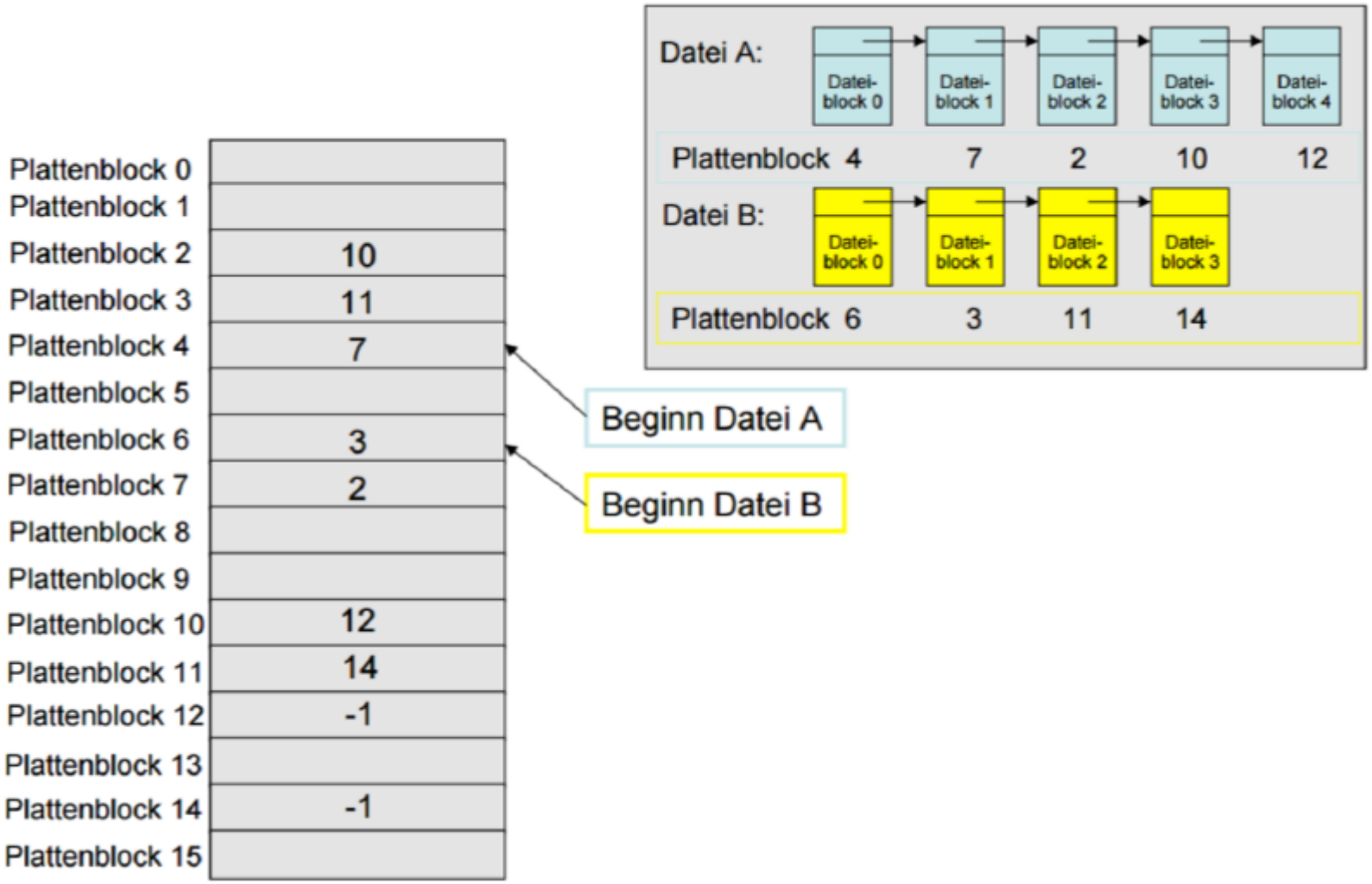
- Informationen über die Verkettung zentral außerhalb der Blöcke
  → Informationen werden im Hauptspeicher (RAM) gehalten
- Möglichkeit der Nutzung schneller Speicher für die Liste
  → bei wahlfreiem Zugriff* werden langsame Plattenzugriffe durch schnellere Hauptspeicherzugriffe ersetzt

Datei-Allokationstabelle oder File Allocation Table (FAT).

*jede einzelne Speicherstelle kann über ihre fest zugeordnete Adresse beliebig oft gelesen oder beschrieben (und damit auch gelöscht) werden

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.

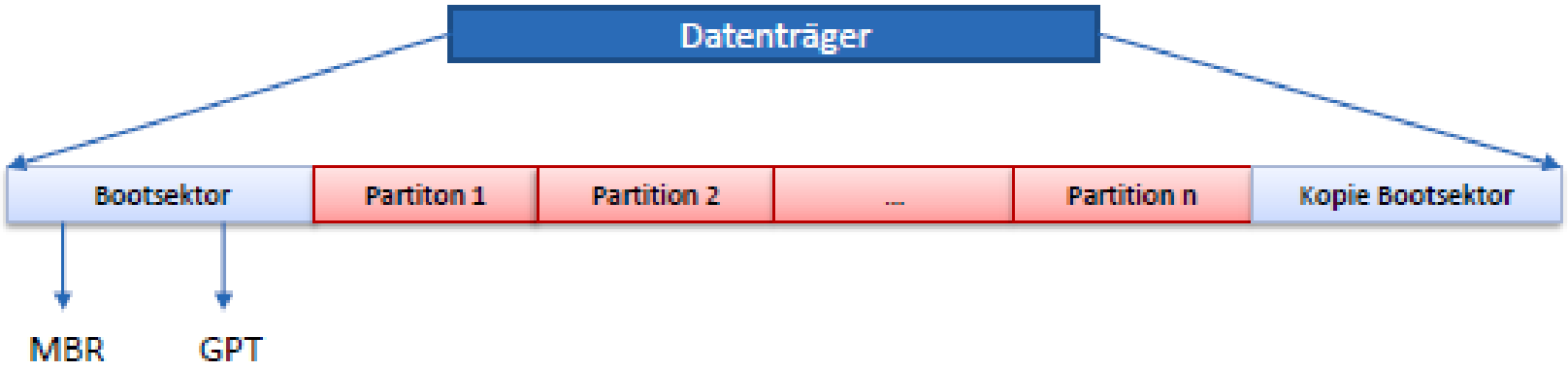
Datenblöcke einer Festplatte

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

Festplattenpartitionierung



- Am Anfang eines Datenträgers befindet sich der Bootsektor (MBR/GPT) der die Partitionstabelle mit den Eintragungen zu den einzelnen Partitionen des Datenträgers enthält.
- Am Ende eines Datenträgers kann sich eine Kopie des Bootsektors befinden.

Dateisysteme – Zusammenfassung

- Festplatten adressieren mit Sektoren, Dateisysteme mit Clustern
- Festplatten lassen sich mit Hilfe von MBR und GPT partitionieren
- Erste Hinweise für Ermittlungen schon in der Partitionstabelle
  - Bsp. Bootfähig oder nicht
- MBR und GPT außerhalb der Partition Adressierung mit Sektoren
- Immer darauf achten wo man sich gerade befindet um Fehler zu vermeiden

Die FAT Familie – FAT 12

- FAT 12 ist für DOS Disketten oder Festplatten von einer Größe von bis zu 32 MB
- 12 Bit Clusternummern --> die max. Anzahl der Cluster: 2^12 = 4.096 Byte
- Die max. Clustergröße auf Disketten: 2 KB auf Festplatten: 4 KB
- Die max. Partitionsgröße auf Disketten: 8 MB auf Festplatten: 16 MB
- Namenslänge von Einträgen: 8+3 (8 Zeichen für den Dateinamen, 3 für die Endung)
- Root Directory auf 14 Cluster beschränkt → maximal 224 Einträge (VZ und/oder Dateien)
- Die Variante der Partitionsgröße von 32 MB mit einer Clustergröße von 8 KB ist möglich, wird jedoch per Default durch Verwendung von FAT 16 erzielt

Die FAT Familie – FAT 16

- FAT 16 ist für Festplatten mit mehr als 32 MB Speicher geeignet.
- 16 Bit Clusternummern, d.h. die max. Anzahl der Cluster: (2^16) 12 = 65.524!
  - 12 Cluster werden von FAT 16 reserviert, daher nicht 65.536
- Die max. Clustergröße: 32 KB. Bei Win NT 64 KB.
- Die max. Partitionsgröße: 2 GB. Bei Win NT 4GB (nicht kompatibel mit DOS)
- Max. Einträge in das Root Verzeichnis: 256 (Größe wird festgelegt, kann nicht wachsen)
- Max. Einträge pro Volume: 65.536
- Max. Dateigröße: 2GB
- Namenslänge von Einträgen: 8+3

Die FAT Familie – VFAT

- VFAT, Virtual File Allocation Table, ist eine Erweiterung von FAT zur Verwendung von längeren Dateinamen.
- Dies geschieht durch einen Trick im Layout der Verzeichniseinträge des FAT Dateisystems.
- Der Name im Verzeichniseintrag wird regulär mit der Länge von 8+3 gespeichert. Ist der Name länger, so wird ein Alias in Form von xxxxxx~1.xxx verwendet.
- Dabei wird die Ziffer für jedes Alias das verwendet wird um eins inkrementiert. Bei FAT 12 und FAT 16, welches dieses System nicht unterstützt, werden die Alias nicht gelesen und der Dateiname wird als die ersten 8+3 gewertet.
- Somit abwärtskompatibel für zu anderen FAT Anwendungen.

Die FAT Familie – FAT 32

- 32 Bit Clusternummern, von denen 4 Bit reserviert sind (32 4 = 28 Bit).
- max. Clusternummer: 2^28 = 268.435.456 Cluster.
- Die max. Clustergröße: 32 KB. Die max. Partitionsgröße: 32 GB unter Win OS. (Tools von Drittherstellern 127 GB, theoretisch sind auch 8 TB möglich)
- Max. Einträge pro Verzeichnis: 65.536
- Max. Einträge in das Root Verzeichnis: 4.177.920
- Max Dateigröße: 4 GB
- Namenslängen von Einträgen: 255 Zeichen
- Nicht kompatibel zu FAT 16 Anwendungen.

NTFS

NTFS - das New Technologie File System (NTFS) wurde das erste Mal im Juli 1993 mit Windows NT 3.1 veröffentlicht.

	FAT12	FAT16	FAT32	NTFS 1	NTFS 2	NTFS 3	NTFS 3.1	NTFS 5
DOS 1.x	Keine Festplattenunterstützung							
DOS 2.x	X							
DOS 3.x	X	X						
DOS 4.x-6.x	X	X	X					
DOS 7.x-8x	X	X	X					
DOS 8	X	X	X					
Windows 95	X	X						
Windows 95B und C	X	X	X					
Windows NT 3.x	X	X	X	X				
Windows NT 4.0	X	X	X	X	X			
Windows 98	X	X	X					
Windows 2000	X	X	X	X	X	X		
Windows ME	X	X	X					
Windows XP	X	X	X	X	X	X	X	X
Windows Server 2003	X	X	X	X	X	X	X	X
Windows Vista	X	X	X	X	X	X	X	X
Windows 7/8/10...	X	X	X	X	X	X	X	X

NTFS

Ein Vorteil von NTFS ist, dass die Dateigröße nicht auf 4 GB beschränkt ist, wie es bei FAT der Fall ist.

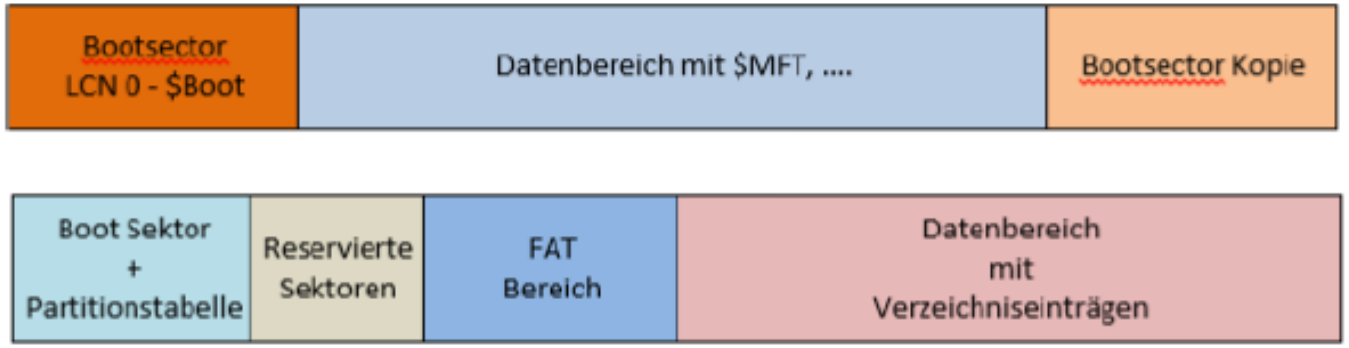
- Die max. Anzahl der Cluster: Bei Win OS: 2^32. Theoretisch aber 2^64 möglich.
- Die max. Clustergröße: 64 KB, per Default 4 KB.
- Die max. Partitionsgröße: Bei Win OS: 256 TB.
- Theoretische max. Größe: 1YB → 1 Yotabyte = 1.024 Zetabyte = 1.048.576 EB
- Die max. Dateigröße: Bei Win OS: 16 TB. Theoretische max. Größe: 16 EB.
  1 Exabyte = 1.048.576 TB = 1.073.741.824 GB
- Namenslänge von Einträgen: 255 , nicht kompatibel zu FAT16 Anwendungen

NTFS bietet im Gegensatz zu FAT Transaktionsverfolgungen, einen gezielten Zugriffschutz auf Dateiebene durch Dateirechte, eine höhere Datensicherheit durch Journaling und die Möglichkeit der Daten Komprimierung.

NTFS

Konzept: „Everything is a file“

Bei NTFS wird alles als Datei behandelt. Das bedeutet, das gesamte Dateisystem ist als EIN Datenbereich eingerichtet. Der einzige konsistente Bereich ist der Boot-Sektor.

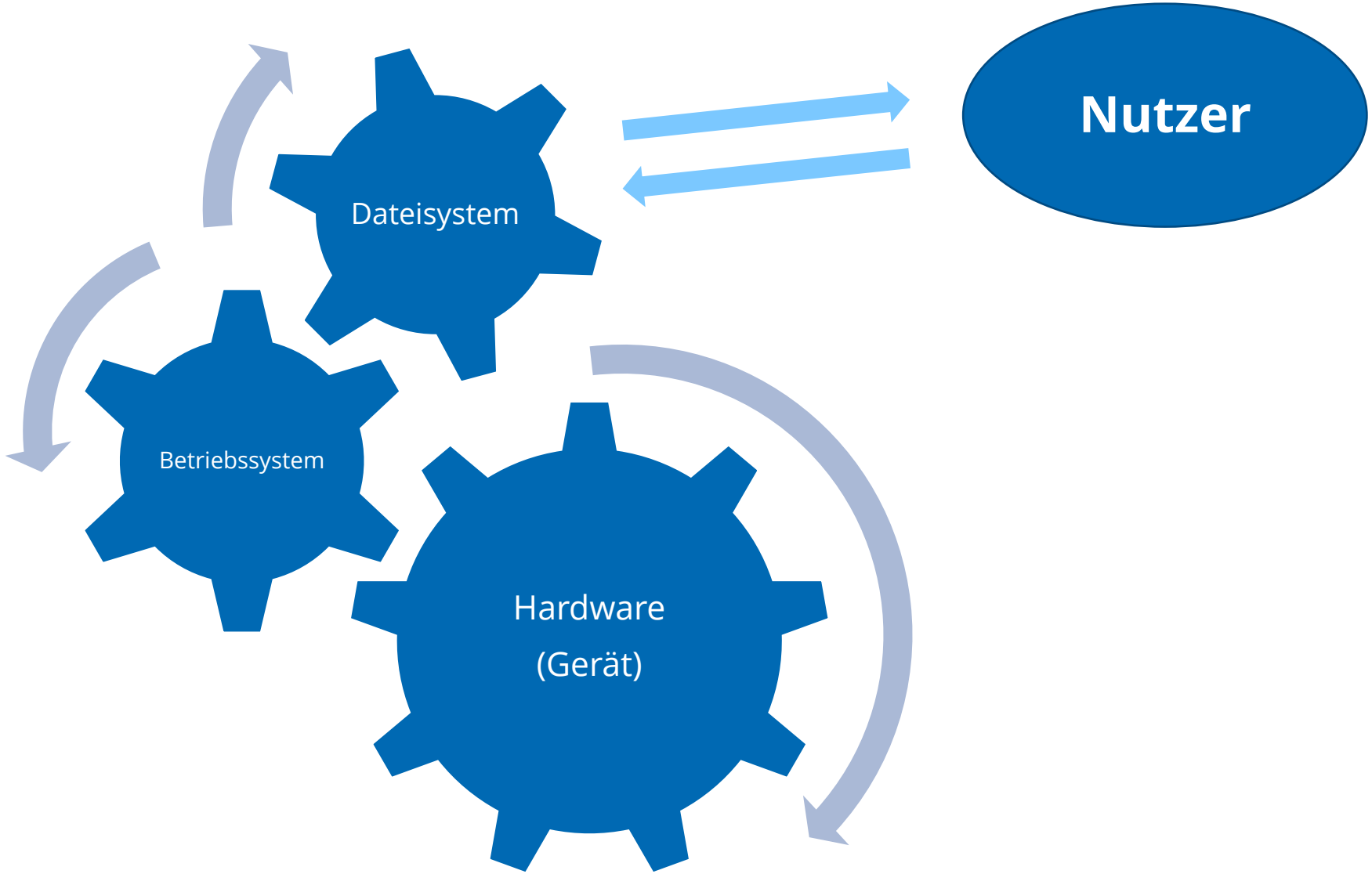


Vergleich NTFS und FAT

Entwicklung

Da die Technologieentwicklung die Grenzen von Wechselmedien sprengte, wurde ein neues Dateisystem benötigt, um die größeren Kapazitäten und schnelleren Zugriffsgeschwindigkeiten zu unterstützen.

Die Antwort von Microsoft darauf ist das Extended FAT File System (exFAT), welches 2006 entwickelt wurde für Windows CE, das auf seinen neueren Betriebssystemen seit 2010 verfügbar gemacht wurde und auf neuen SDXC-Speichermedien (Secure Digital Extended Capacity) die 2009 eingeführt wurden, unterstützt wird


Nutzer
Dateisystem
Betriebssystem
Hardware
(Gerät)

Betriebssysteme und deren Kompatibilität:

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

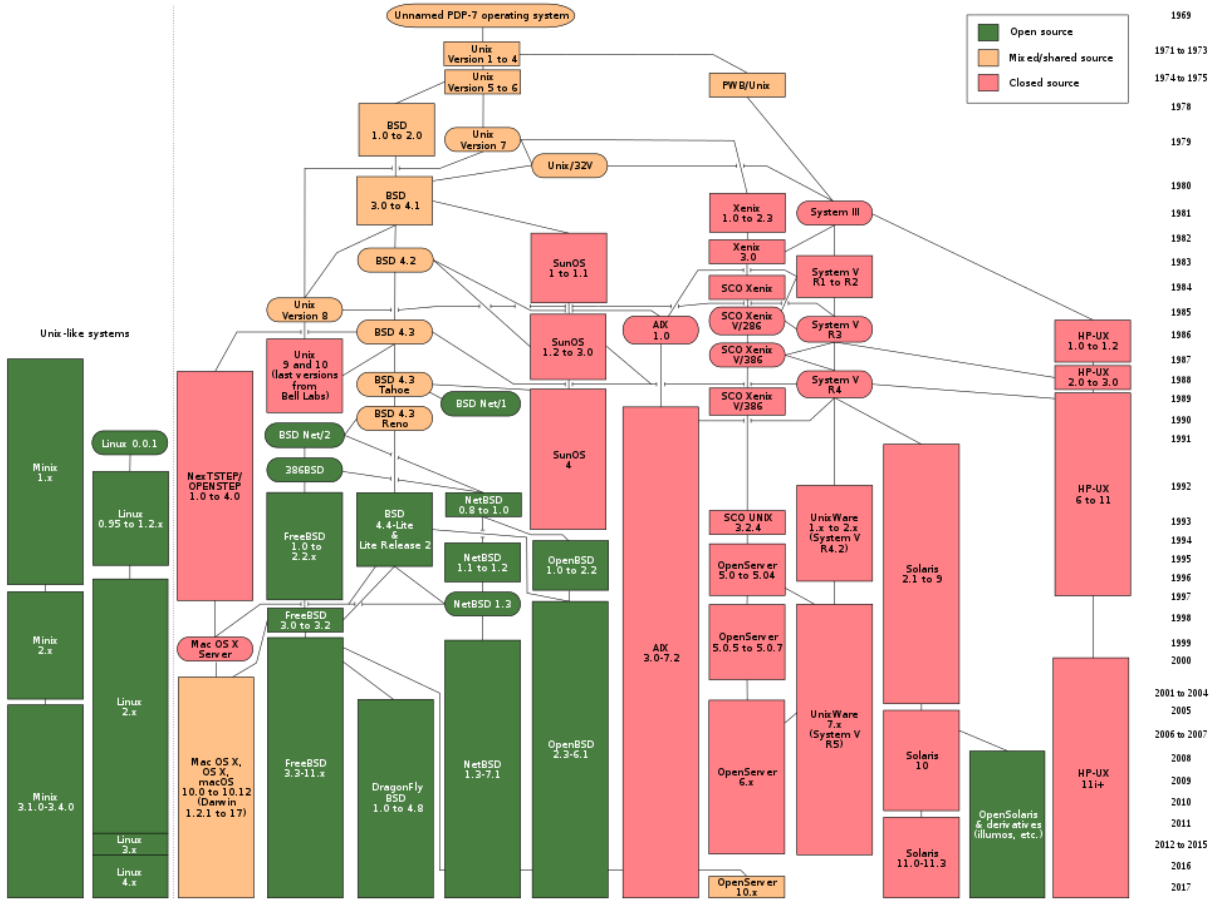
Linux

Allgemeines und Historie

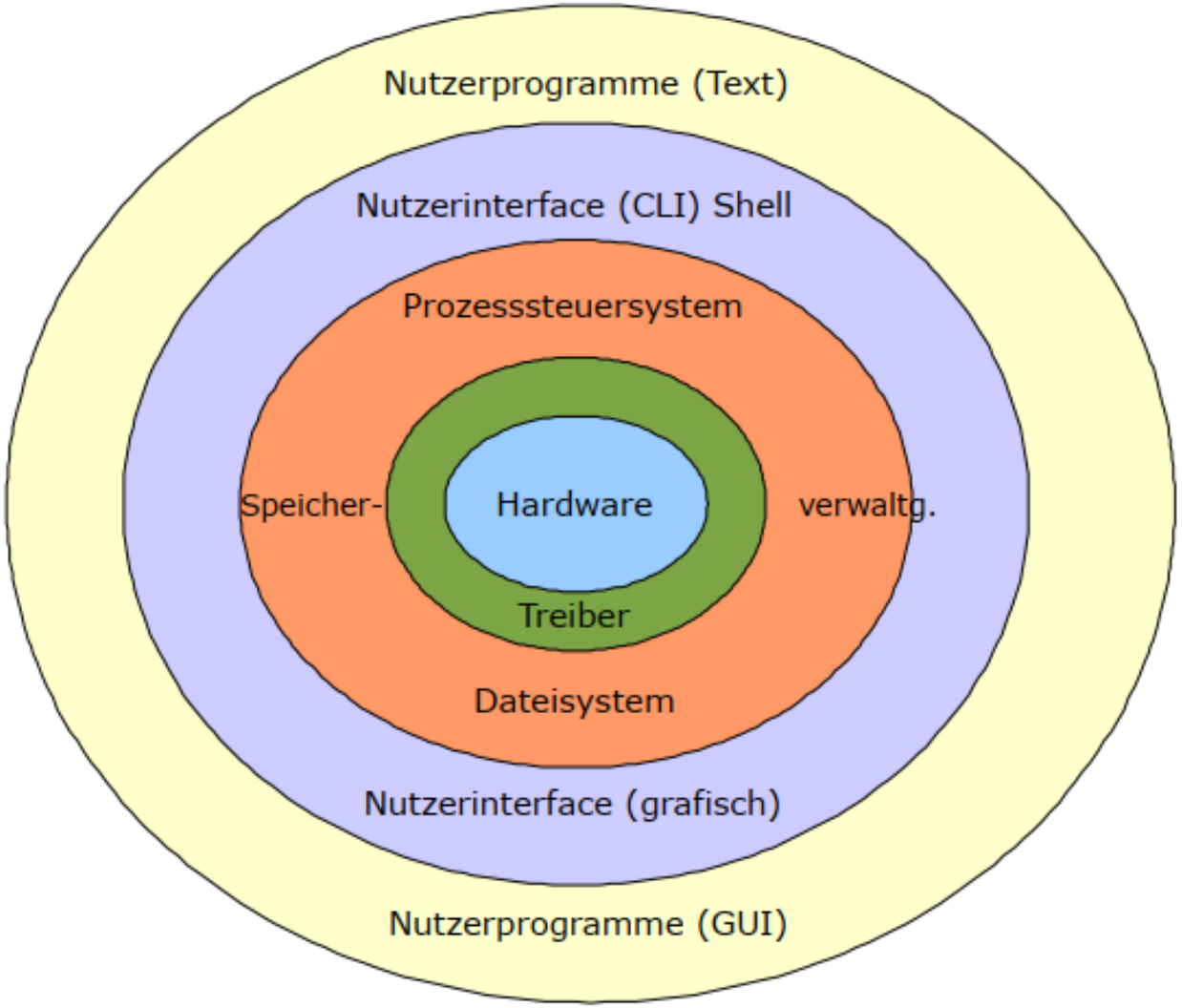
ALLGEMEINES

Die Unix Familie aus der Linux letztlich abstammt ist breit gefächert.

Auch Mac OS X hat seinen Ursprung im Unix Betriebssystem.



Aufbau von Linux als Schalenmodell



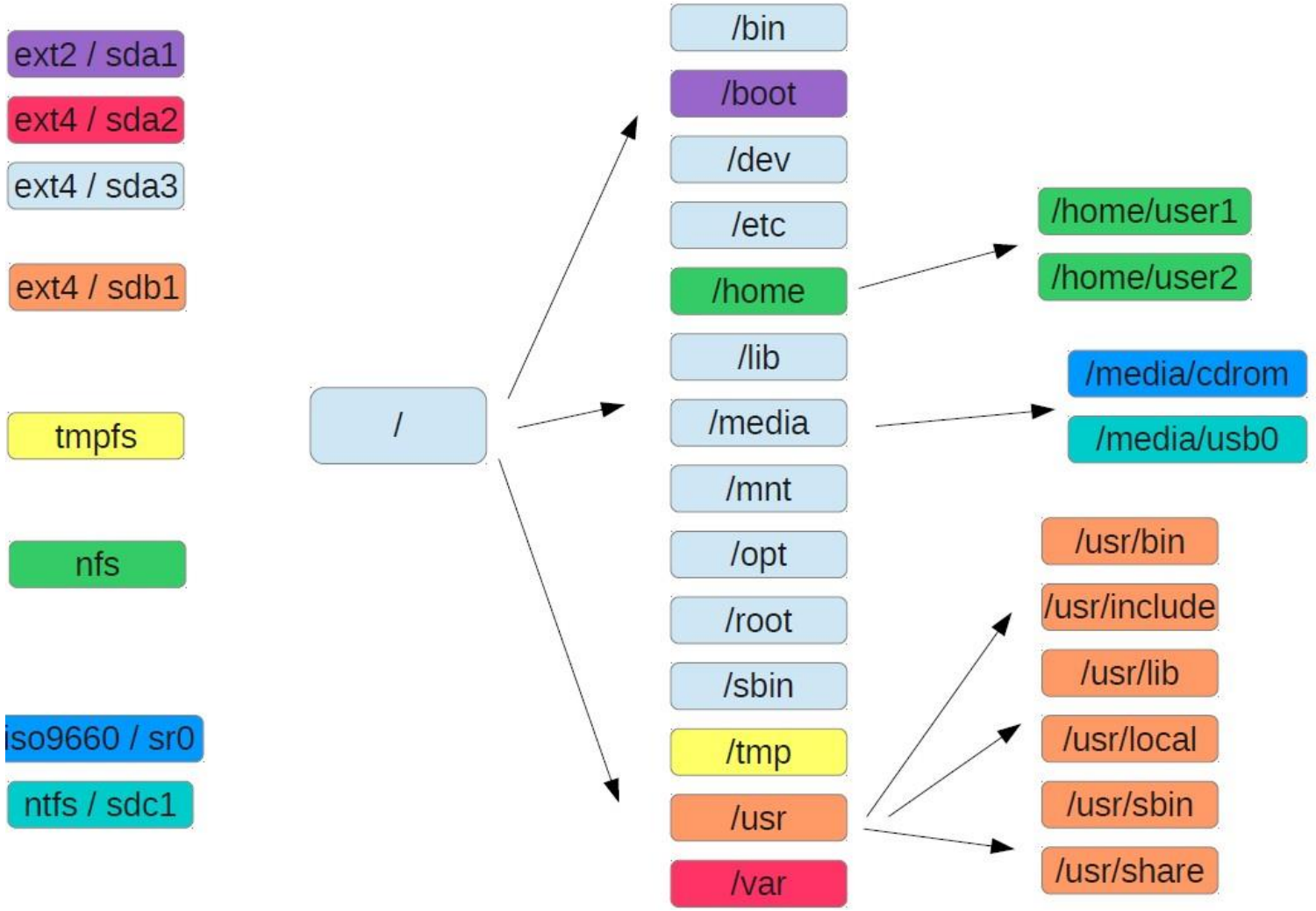
Grundlagen Dateisysteme

- Linux nutzt als Standard die File System Hierarchy (FSH).
- moderne Linux Systeme erlauben Datenträger in mehrere unterschiedliche unabhängige Einheiten zu partitionieren, wobei jede physikalische Einheit ein unterschiedliches Dateisystem unterstützen kann.
- moderne Linux Systeme sind Virtual File Systems (VFS), sie wurden designed, um verschiedene unterliegende Dateisysteme zu unterstützen.

Filesystem Hierarchy Standard

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



Historie

1969:	Filesystem eines der allerersten Komponenten des "Ur-UNIX"
April 1992:	ext Dateisystem veröffentlicht
January 1993:	ext2 Dateisystem veröffentlicht
1993:	Entwicklung des Filesystem Hierarchy Standard (FHS) Zunächst nur auf Linux bezogen
1995:	BSD-Entwickler springen auf die FHS Entwicklung auf. (Ziel Gemeinsamer UNIX-Standard)
November 2001:	ext3 Dateisystem veröffentlicht
2004:	Version 2.3 des FHS wird veröffentlicht (aktuell gültige Version)
Oktober 2006:	ext4 Dateisystem veröffentlicht

Das Extended File System ext

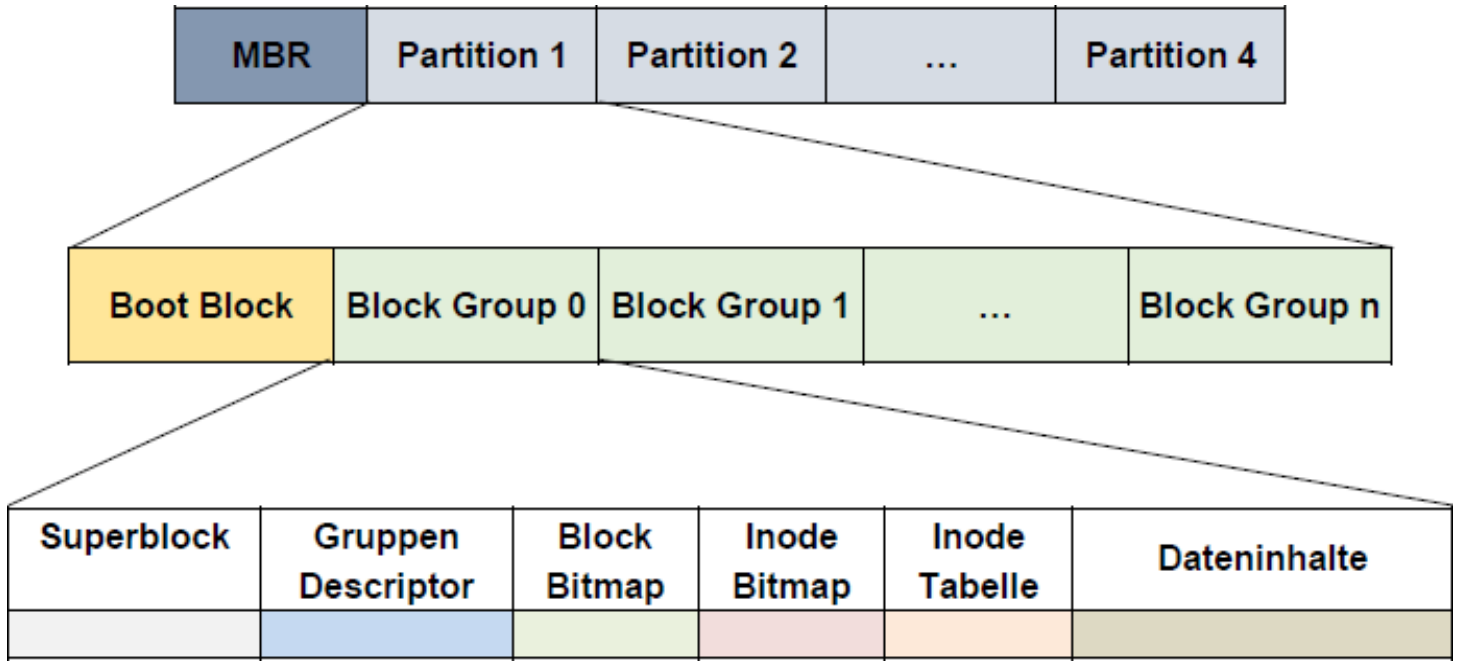
GRUNDLEGENDES ÜBER EXT

Das **Extended File System**, kurz **ext**, ist das **Standard Dateisystem** in vielen **Linux** Distributionen und der Nachfolger des Unix File Systems, UFS.

Das grundlegende **Designprinzip** von **ext** ist **Geschwindigkeit und Zuverlässigkeit**. Dafür wurden Kopien zentraler Datenstrukturen mehrfach auf dem Datenträger verteilt. Zudem werden die Datenblöcke einer Datei nahe beieinander gehalten, um so die Wege des Lesekopfes zu minimieren.

Aufbau des Ext Dateisystems

Das ext-Dateisystem besteht aus einem Bootblock und mehreren Blockgruppen in der die Partition mit dem ext Dateisystem aufgeteilt wird.



Aufbau des Ext Dateisystems

Der Bootblock ist immer 1024 Byte groß und enthält nur Bootcode, dies aber auch nur selten. Insbesondere ist er aber ohne jeglichen forensischen Wert!

Eine Partition ist aufgeteilt in einzelne **Sektionen gleicher Größe**, mit Ausnahme der letzten Sektion. Diese **Sektionen heißen Blockgruppen**. Jede **Blockgruppe** besitzt die **gleiche Anzahl an Blöcken**, welche für das Speichern der **Verzeichniseinträge**, **Metadaten** und **Dateiinhalte** zuständig sind.

Das Extended File System ext

- **Ext:** wurde im April 1992 als Nachfolger von UFS (UnixFileSystem) eingeführt und quasi sofort von ext2 abgelöst.
- **Ext2:** wurde als Nachfolger von ext im Januar 1993 eingeführt und war viele Jahre das Standarddateisystem für Linux. Es ist heute noch weit verbreitet.
- **Ext3:** wurde im November 2001 eingeführt und brachte Journaling in die Extended Filesystem Familie. Das Journal ist eine Dateistruktur, in die Metadaten (optional die Nutzdaten) geschrieben werden, bevor sie auf das tatsächliche Dateisystem geschrieben werden.
- **Ext4:** Der Nachfolger von ext3 wurde im Oktober 2008 released, dieser führte Extends in die ext Reihe ein. Extends bringen Geschwindigkeitsvorteile bei der Verwaltung großer Dateien und beugt der Fragmentierung vor.

Dateisysteme

Die ext2,3,4 Dateisysteme sind nicht die einzigen Dateisysteme, welche für Linux Distributionen existieren. Jede Distribution und jeder Benutzer kann frei entscheiden, welches Dateisystem verwendet wird.

Populär sind beispielsweise auch:

- ReiserFS
- XFS
- ZFS
- JFS
- btrFS (Butter FS – gedacht als Ablösung für Ext4)

Kompatibilität

Ext ist ein offenes Dateisystem. Es gibt viele zusätzliche Features, die in drei Kategorien fallen:

Compatible Features

- Dateisysteme mit diesen Features lassen sich uneingeschränkt nutzen (Auf- und Abwärtskompatibel)

Incompatible Features

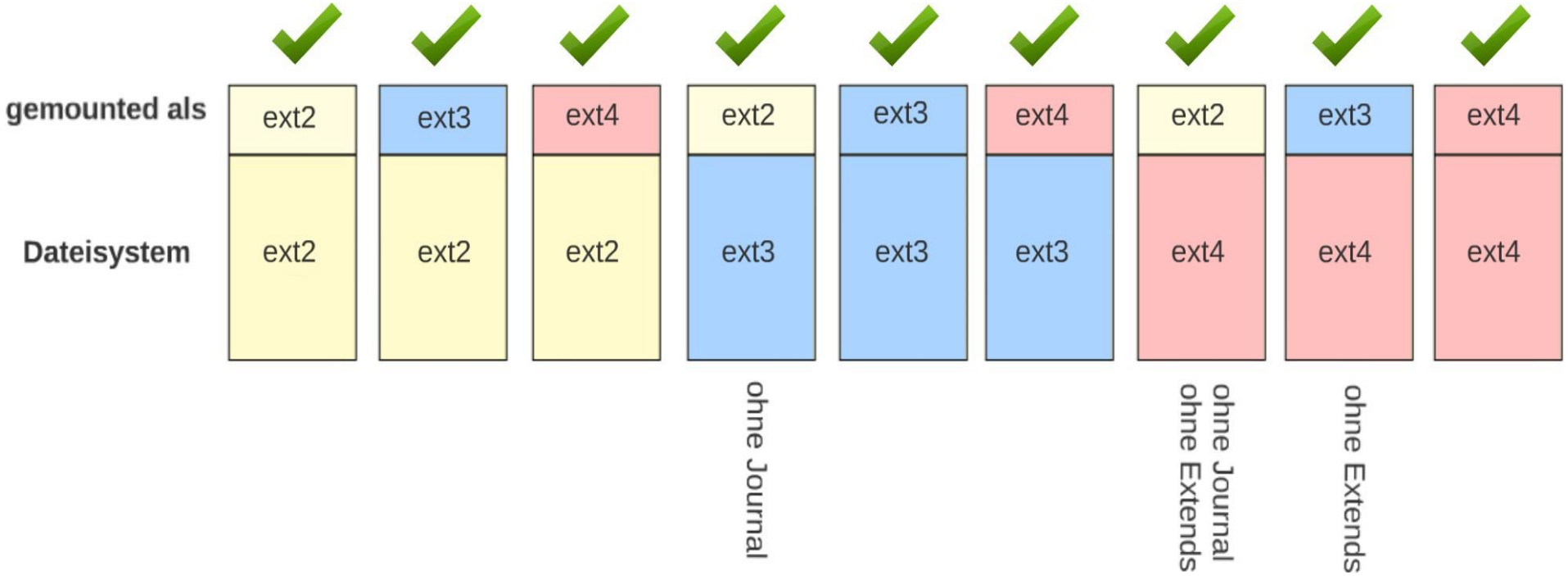
- Wenn das Betriebssystem das Feature nicht unterstützt, sollte das Dateisystem nicht gemountet werden.
- Beispiel Kompression

Read only Features

- Wenn ein Betriebssystem ein solches Feature nicht unterstützt kann es das Dateisystem dennoch lesen, sollte es aber nicht schreiben.
- Beispiel: B-Baum Verzeichnissortierung

Kompatibilität Ext

Das ext Dateisysteme sind auf- und abwärtskompatibel:



Andere Dateisysteme unter Linux

Linux ist in der Lage **fast jedes Dateisystem zu mounten** (mit entsprechendem Treiber) und einzulesen Neben den nativ verwendeten Dateisystem wie EXT und FAT, gibt etwa Module für NTFS, HFS+, VmwareFS 5, ReiserFS, NFS, UFS, XFS, YAFFS und ExFAT.

Für das Mounten von diesen Dateisystem wird eine Technik genutzt die sich **FUSE** (Filesystem in Userspace) nennt FUSE ist ein Kernel Modul für Unix Systeme, das es ermöglicht, Dateisystem Treiber aus dem Kernel Mode in den User Mode zu verlagern.

FUSE ist das laufwerksspezifische Modul (für die angeschlossene Hardware) und benötigt zur Einbindung des darauf enthaltenen Dateisystems zusätzlich den jeweils passenden dateisystemspezifischen Treiber Der wohl bekannteste ist NTFS-3G.

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