# IT Forensik Workshop 2018
# FH Aachen

## Apple File System

**Marvin Blumenröder**
marvin.blumenroeder@polizei.nrw.de

# Apple File System (APFS)



- Nachfolger von HFS+
- **64-Bit** "Next-Gen"-Dateisystem
- Volle Unterstützung seit
  **High Sierra** 10.13 (09/2017)
  iOS 10.3 (03/2017)
- Bisher **keine vollständige Dokumentation** verfügbar

# Features

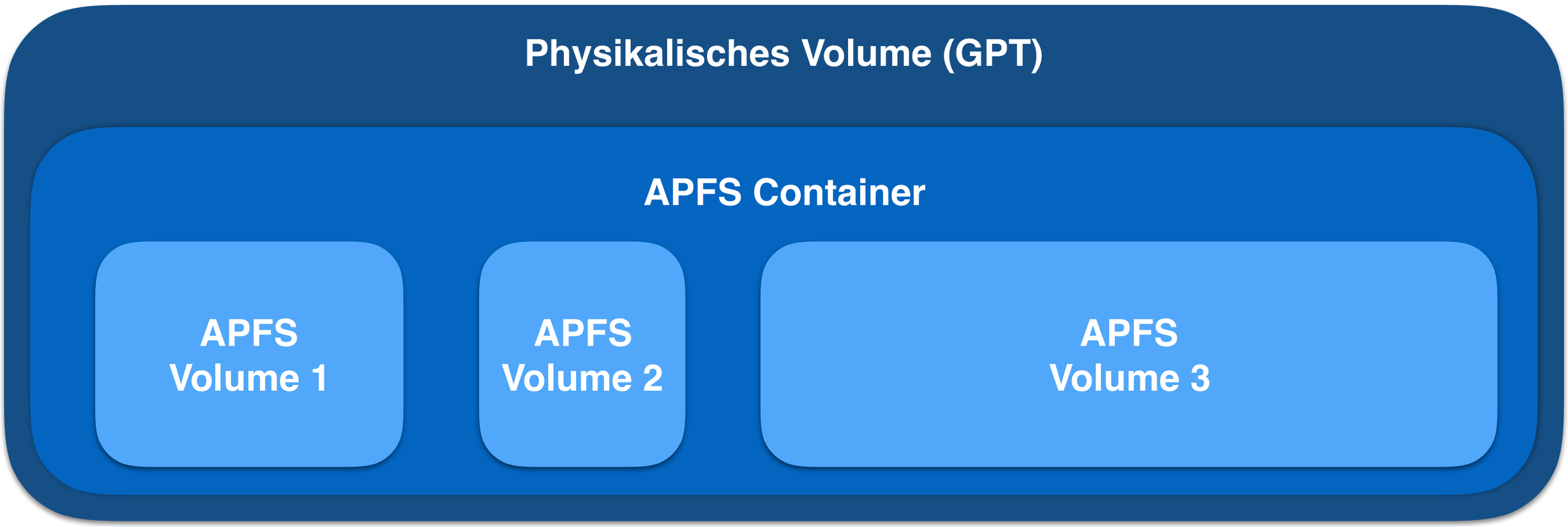


- **Was gibt es Neues?**
  Space Sharing
  Clones
  Snapshots
  Nanosekunden Zeitstempel (Unix Epoch)
  Byte-Order Little Endian
  Verschlüsselung auf FS-Ebene
  Copy-On-Write und Atomic-Safe Save
  ...

- **Was ist nicht mehr dabei?**
  Bisher kein Fusion Drive
  Kein CoreStorage
  Kein Journal

# APFS Layout I

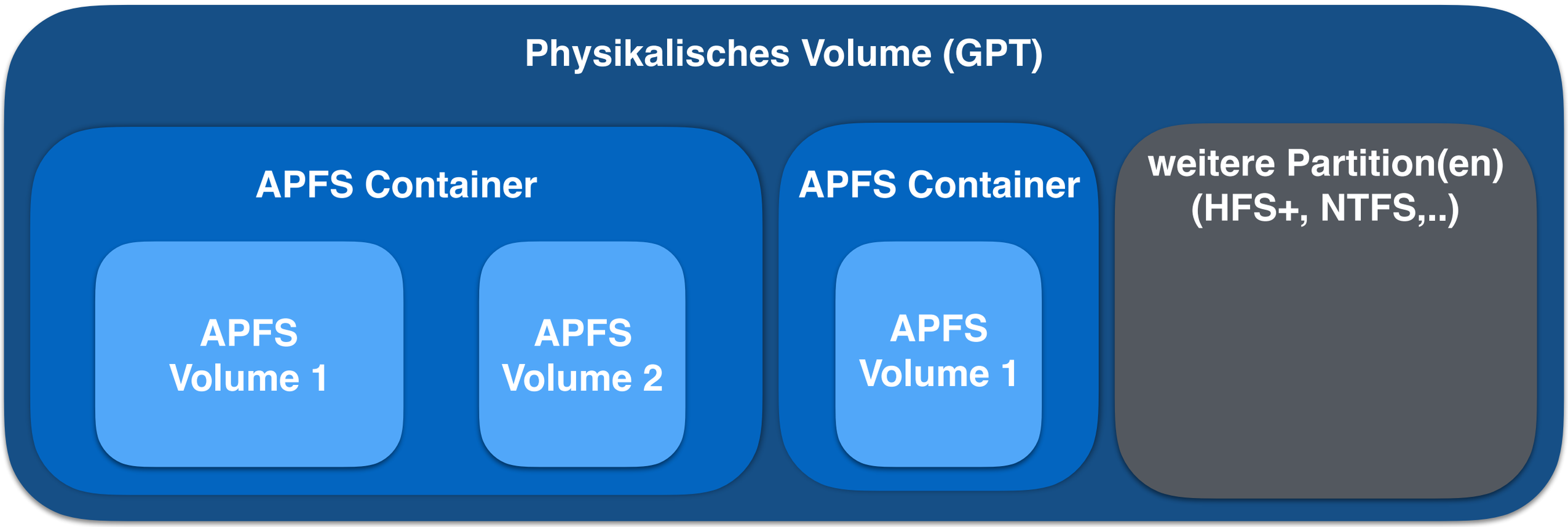





- Container stehen **im GPT**
- Container beinhalten **Volumes**

# APFS Layout II






- **Weitere Container** und **andere Dateisysteme**

# diskutil list: APFS



marvin — -bash — 80×16

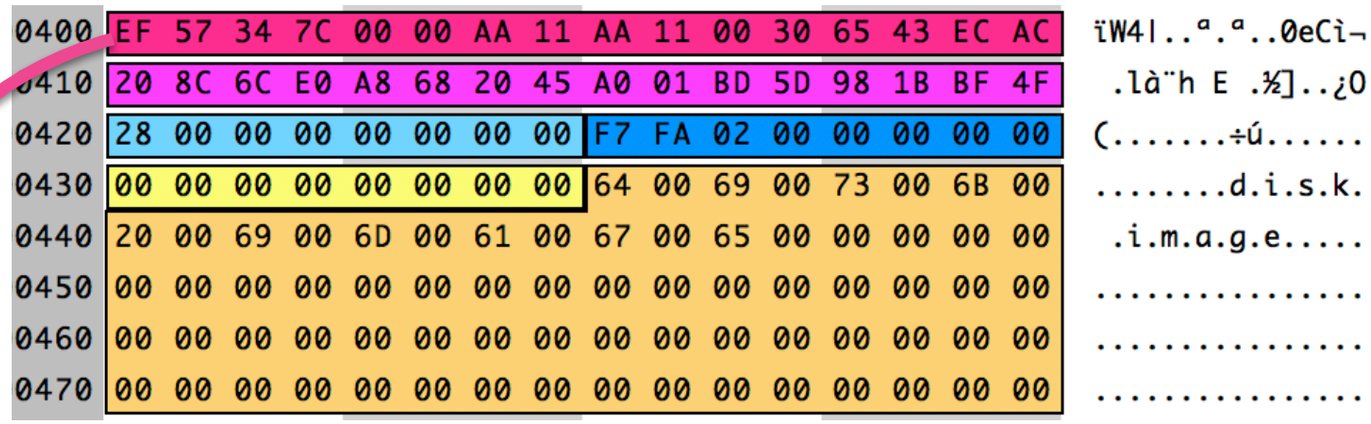
```
Marvins-MacBook-Pro:~ marvin$ diskutil list
/dev/disk0 (internal):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      GUID_partition_scheme                        1.0 TB     disk0
   1:                        EFI EFI                     314.6 MB   disk0s1
   2:                  Apple_APFS Container disk1        1.0 TB     disk0s2

/dev/disk1 (synthesized):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      APFS Container Scheme -                      +1.0 TB    disk1
                                 Physical Store disk0s2
   1:                 APFS Volume MacintoshHD            552.1 GB   disk1s1
   2:                 APFS Volume Preboot                21.9 MB    disk1s2
   3:                 APFS Volume Recovery               517.8 MB   disk1s3
   4:                 APFS Volume VM                     1.1 GB     disk1s4
   5:                 APFS Volume ArbeitHD               170.8 GB   disk1s5
```

- **1 Container** - befindlich auf /dev/disk**0**
- **5 Volumes** - *synthesized* als /dev/disk**1**

# APFS manuell erkennen



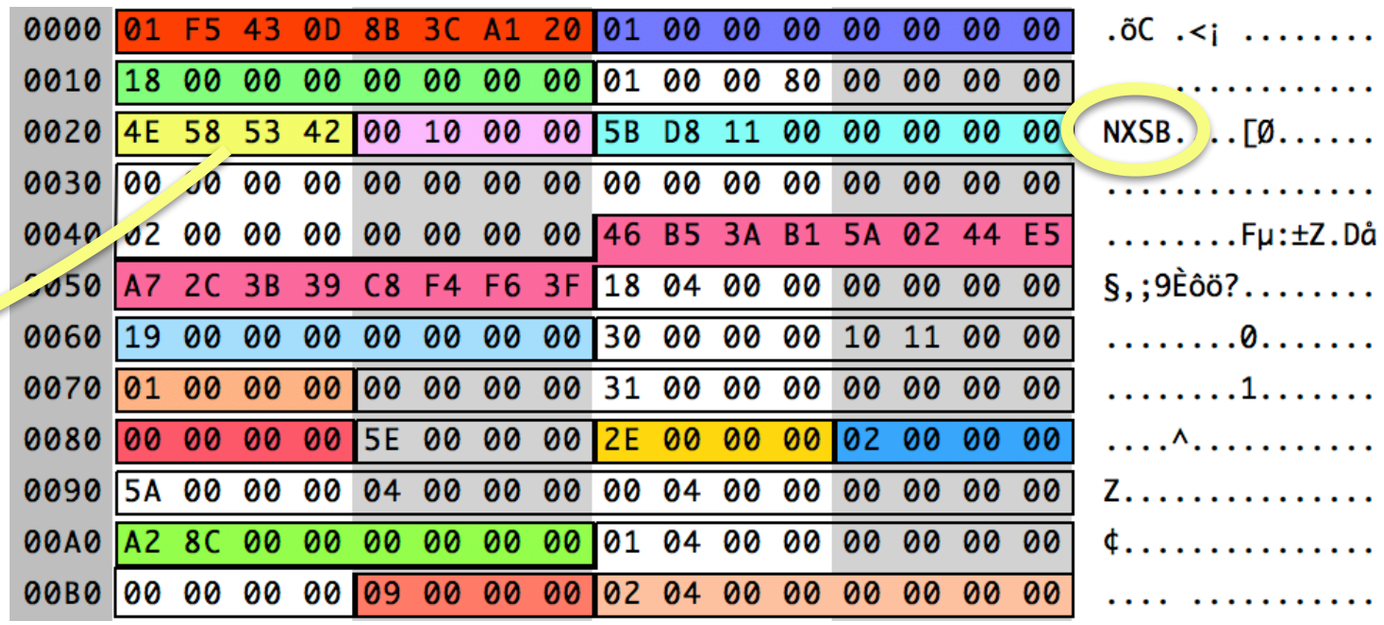
- **Partitions-Typ-GUID** im GTP Eintrag:




**EF 57 34 7C 00 00 AA 11 AA 11 00 30 65 43 EC AC**

- **Signatur** im 1. Block des Containers:

**NXSB**



# APFS Struktur Überblick



**Container Metadaten**

**Main Superblock**, Allokations-Bitmap, Volumes Liste

**Volume Metadaten**

**Volume Checkpoint Superblöcke**, **Snapshots**, Catalog B-Tree, Extents B-Tree

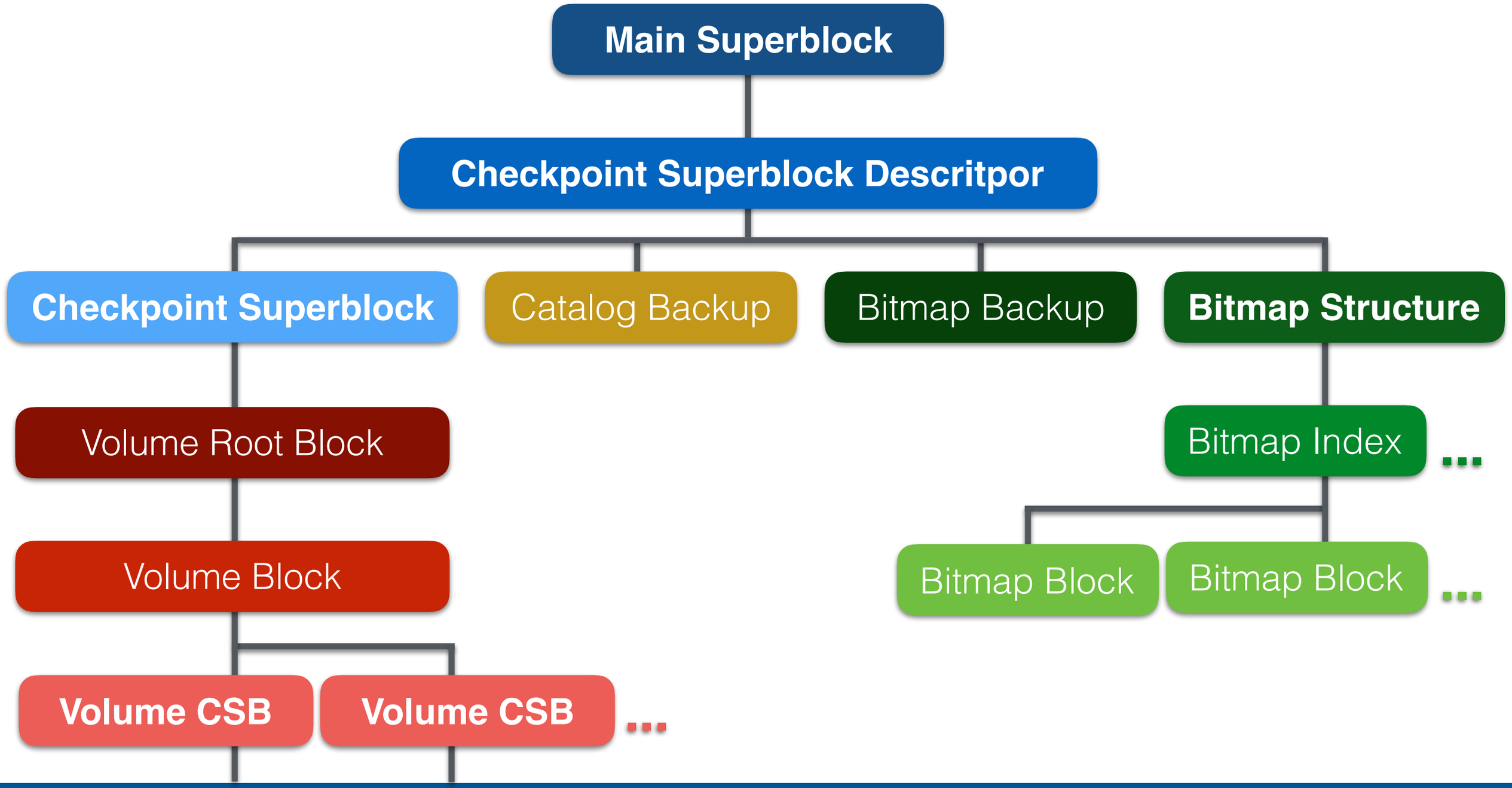
**Allokierbarer Speicherbereich**

**Daten**

# APFS Container Struktur

POLIZEI
Nordrhein-Westfalen
Landesamt für Ausbildung, Fortbildung und Personalangelegenheiten

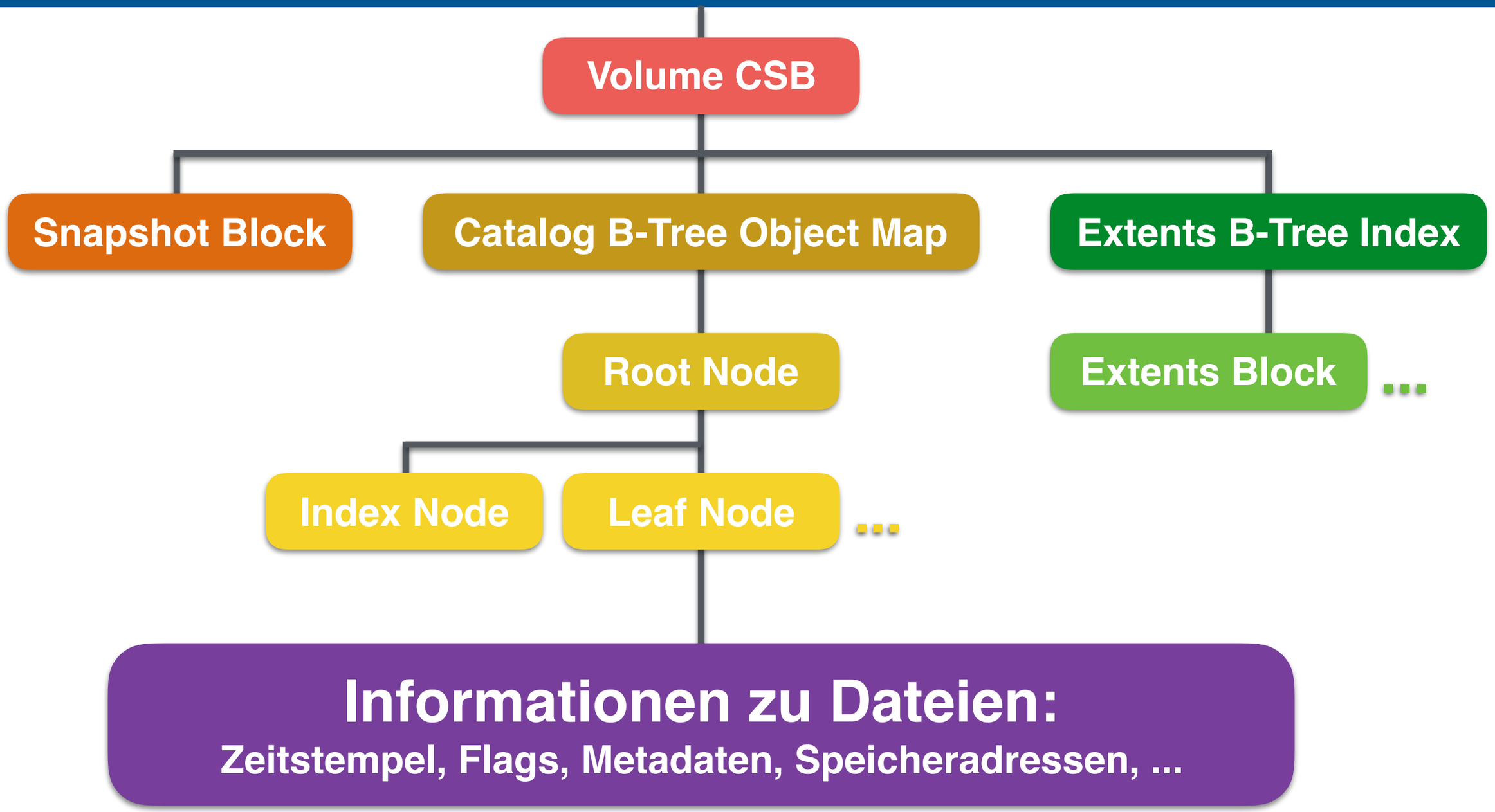




# APFS Volume Struktur

POLIZEI
Nordrhein-Westfalen
Landesamt für Ausbildung, Fortbildung und Personalangelegenheiten

bürgerorientiert · professionell · rechtsstaatlich



# Main/Container Superblock



| Offset | Größe (Bytes) | Eintrag |
|---|---|---|
| 0x0000 | 8 | Fletchers Checksum Algorithm |
| 0x0008 | 8 | Block ID (0x0100 = NXSB) |
| 0x0010 | 8 | Checkpoint ID |
| 0x0020 | 4 | **CSB Magic „NXSB“** |
| 0x0024 | 4 | **Allokationsblockgröße** |
| 0x0028 | 8 | Gesamtanzahl Allokationsblöcke |
| 0x0048 | 16 | **UUID Container** |
| 0x0060 | 8 | ID des nächsten CSB |
| 0x0070 | 4 | Base Block |
| 0x0080 | 4 | vorheriger CSBD |
| 0x0088 | 4 | aktueller CSBD |
| 0x008C | 4 | initialer CSBD |
| 0x00A0 | 8 | **Block-Nummer zum Volume Root Block** |
| 0x00B4 | 4 | maximale Nummer von logischen Volumes |
| 0x00B8 | 8 | Volume List IDs |

# Volume Checkpoint Superblock



| Offset | Größe in Bytes | Eintrag |
|---|---|---|
| 0x0000 | 8 | Fletchers Checksum Algorithm |
| 0x0008 | 8 | Block ID |
| 0x0010 | 8 | Checkpoint ID |
| 0x0020 | 4 | **VCSB Magic „APSB“** |
| 0x0024 | 4 | Volume-Nummer. Beginnend bei 0 |
| 0x0048 | 8 | Größe des Volumes in Blöcken |
| 0x0080 | 8 | **Block-Nummer zum Catalog B-Tree (BTOM)** |
| 0x0088 | 8 | Node ID des Root Node |
| 0x0090 | 8 | **Block-Nummer zum Extents B-Tree** |
| 0x0098 | 8 | **Block-Nummer zur Liste der Snapshot** |
| 0x00B8 | 8 | Anzahl der Dateien des Volumes |
| 0x00C0 | 8 | Anzahl der Verzeichnisse des Volumes |
| 0x00F0 | 8 | **UUID Volume** |
| 0x0100 | 8 | **Zeitstempel, Letzte Veränderung am Volume** |
| 0x0110 | 32 | Creator/APFS-version |
| 0x0130 | 8 | **Zeitstempel, Volume Erstellung** |
| 0x0140 | variabel | Checkpoint-Liste (ggf. mehrere Einträge) |
| 0x02C0 | 48 | Volume Name |

# Dateieintrag



| Offset | Größe in Bytes | Eintrag |
|---|---|---|
| 0x0000 | 8 | Parent ID |
| 0x0008 | 8 | Catalog Node ID (CNID) |
| 0x0010 | 8 | **Zeitstempel: Datei erstellt** |
| 0x0018 | 8 | **Zeistempel: Zuletzt verändert** |
| 0x0020 | 8 | **Zeitstempel: CNID verändert** |
| 0x0028 | 8 | **Zeitstempel: Letzter Zugriff** |
| 0x0048 | 4 | Besitzer ID |
| 0x004C | 4 | Group ID |
| 0x0050 | 8 | Flags, Attribute |
| 0x0068 | variabel | Dateiname, nullterminiert |

# Extended Attributes



- Weiterhin vorhanden
- Speicherort: **Catalog B-Tree im Dateisystem**
- Mögliche Erzeuger:
  **Browser**, **AirDrop**, **Mail**, **iChat, ...**

| Beispiele | Beschreibung |
|---|---|
| **kMDItemWhereFroms** | Download-URL, E-Mail Absender, Gerätename,... |
| **kMDItemDownloadedDate** | Downloadzeitstempel |
| **com_apple_mail_dateSent** | E-Mail Sendungszeitstempel |
| **com_apple_mail_dateReceived** | E-Mail Empfangszeitstempel |
| **com_apple_mail_isRemoteAttachment** | E-Mail Anhang |
| **com.apple.quarantine** | Hinweis auf externe Quelle |

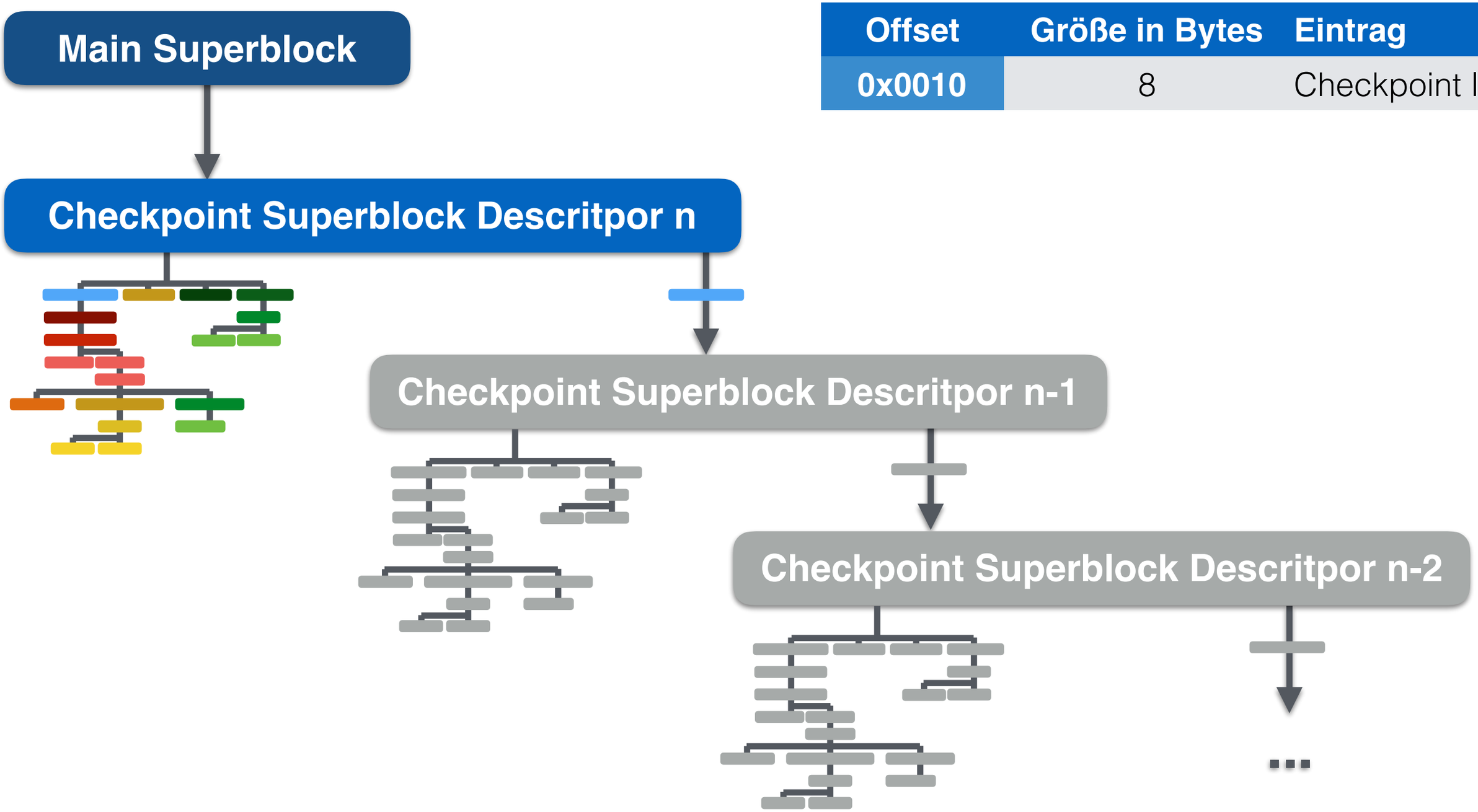
# File Recovery



- **Carving:**
  - Keine Eindeutige Zuordnung zu einem Volume durch **Space Sharing**
  - Tendenziell höhere Fragmentierung
- **Dateisystem Artefakte:**
  - **Kein Journal** mehr (im Gegensatz zu HFS+)
  - Dafür: **Checkpoints** und **Snapshots**

# APFS Checkpoints



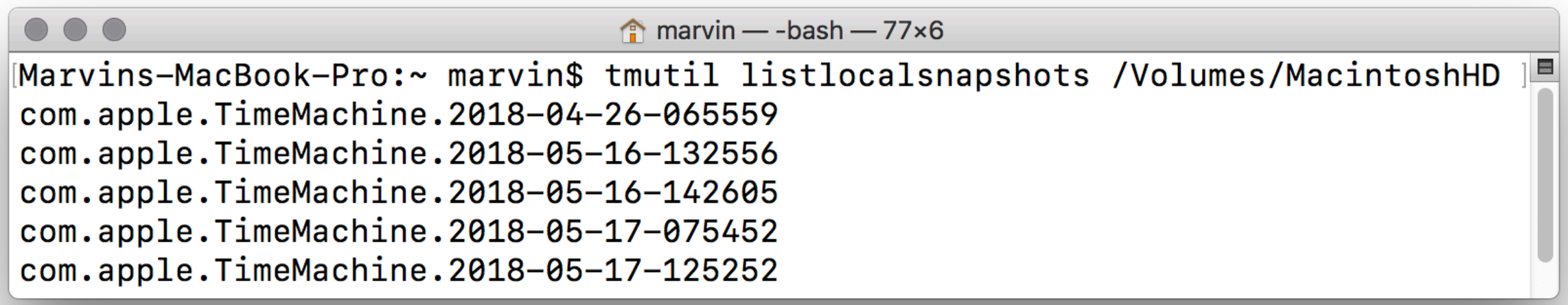



| Offset | Größe in Bytes | Eintrag |
|---|---|---|
| 0x0010 | 8 | Checkpoint ID |

# APFS Snapshots



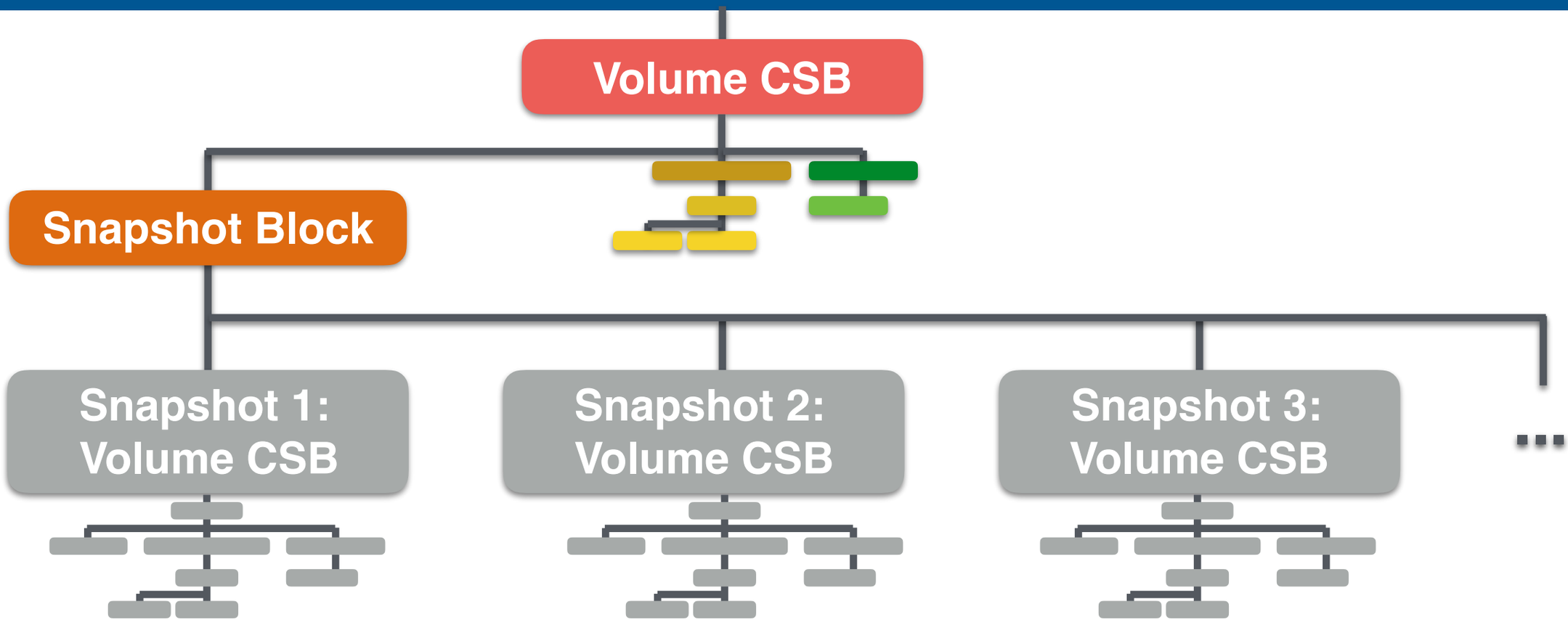
- Dateisystem-Backup
- Verhindert **endgültiges** Löschen
- **Manuelle** Erstellung (`tmutil`)
  **Automatische** Backups (TM)
  OS-**Updates**

# APFS Snapshots

POLIZEI
Nordrhein-Westfalen
Landesamt für Ausbildung, Fortbildung und Personalangelegenheiten






- Snapshots analysieren:

```
tmutil listlocalsnapshots <Volume>
mount_apfs -s <Snapshot> <Volume> <Mountpoint>
```

# Auswertung von APFS



- **Tools** mit **eingeschränkter** Unterstützung:
  Recon, EnCase, Biskus, Blacklight

- **Checkpoints** und **Snapshots** bieten
  *voraussichtlich* gute Möglichkeiten gelöschte Daten wiederherstellen zu können

- Empfehlung zur Auswertung unter Windows:
  `cp –a` mit einem **HFS+** Datenträger als Ziel

- Grundsätzlich **kein** harter Shutdown

# ULS: APFS (Un-)Mounting



```
diskutil apfs list:  Container disk3 90FCC4BA-F955-41C4-A535-CBE3039D80A9
                     ========================================================
                     APFS Container Reference:     disk3
                     Capacity Ceiling (Size):      31247523840 B (31.2 GB)
                     Capacity In Use By Volumes:   74985472 B (75.0 MB) (0.2% used)
                     Capacity Available:           31172538368 B (31.2 GB) (99.8% free)
                     |
                     +-< Physical Store disk2s2 5DFA4249-62ED-4BA9-9FD6-575AD1B4371A
                     |   ----------------------------------------------------------
                     |   APFS Physical Store Disk:   disk2s2
                     |   Size:                       31247523840 B (31.2 GB)
                     |
                     +-> Volume disk3s1 03EB39FF-8E96-45F7-8F68-AB41ADE56F5F
                         ----------------------------------------------------
                         APFS Volume Disk (Role):   disk3s1 (No specific role)
                         Name:                      APFS USB-Stick (Case-insensitive)
                         Mount Point:               /Volumes/APFS USB-Stick
                         Capacity Consumed:         974848 B (974.8 KB)
                         Encrypted:                 No
```

```
Marvins-MacBook-Pro:~ marvin$ log show --predicate 'senderImagePath contains[cd] "apfs"'
Filtering the log data using "senderImagePath CONTAINS[cd] "apfs""

Timestamp                       Thread     Type        Activity             PID    TTL
2017-10-25 09:00:06.003788+0000 0x34048    Default     0x0                  0      kernel: (apfs) cryptoAlloc:649: Using 64 buffers with size 16384, 512 buffers size 65536
2017-10-25 09:00:06.020676+0000 0x34051    Default     0x0                  0      kernel: (apfs) dev_init:237: device accelerated crypto: 0 (compiled @ Sep 28 2017 22:34:50)
2017-10-25 09:00:06.020920+0000 0x34051    Default     0x0                  0      kernel: (apfs) nx_kernel_mount:1120: initializing cache w/hash_size 8192 and cache size 32768
2017-10-25 09:00:06.061118+0000 0x34051    Default     0x0                  0      kernel: (apfs) nx_kernel_mount:1364: checkpoint search: largest xid 67, best xid 67 @ 133
2017-10-25 09:00:06.061235+0000 0x34051    Default     0x0                  0      kernel: (apfs) fusion_wbc_thread_shutdown:1130:
                                                                                                Consider Fusion WBC Elevator thread of container 90FCC4BA-F955-41C4-A535-CBE3039D80A9 dead
2017-10-25 09:00:06.107585+0000 0x34072    Default     0x0                  0      kernel: (apfs) dev_init:237: device accelerated crypto: 0 (compiled @ Sep 28 2017 22:34:50)
2017-10-25 09:00:06.107886+0000 0x34072    Default     0x0                  0      kernel: (apfs) nx_kernel_mount:1120: initializing cache w/hash_size 8192 and cache size 32768
2017-10-25 09:00:06.148152+0000 0x34072    Default     0x0                  0      kernel: (apfs) nx_kernel_mount:1364: checkpoint search: largest xid 67, best xid 67 @ 133
2017-10-25 09:00:06.148169+0000 0x34072    Default     0x0                  0      kernel: (apfs) spaceman_metazone_init:347: metazone for device 0 of size 238399 blocks
                                                                                                (encrypted: 0-119199 unencrypted: 119199-238399)
2017-10-25 09:00:06.149024+0000 0x34072    Default     0x0                  0      kernel: (apfs) er_state_obj_get_for_recovery:3682:
                                                                                                No ER state object - rolling is not happening, nothing to recover.
2017-10-25 09:00:06.149037+0000 0x34072    Default     0x0                  0      kernel: (apfs) handle_mount:254: vol-uuid: 03EB39FF-8E96-45F7-8F68-AB41ADE56F5F block size: 4096
                                                                                                block count: 7628790 (unencrypted; flags: 0x1; features: 1.0.2)
2017-10-25 09:00:06.149590+0000 0x34072    Default     0x0                  0      kernel: (apfs) apfs_vfsop_mount:1331: mounted volume: APFS USB-Stick
2017-10-25 09:00:06.300870+0000 0x29304    Default     0x0                  0      kernel: (apfs) handle_encryption_rolling:4038: er: request granted[0].

2017-10-25 09:00:20.027840+0000 0x3423f    Default     0x0                  0      kernel: (apfs) apfs_vfsop_unmount:1444: unmounting devvp <private>
2017-10-25 09:00:20.064296+0000 0x3423f    Default     0x0                  0      kernel: (apfs) apfs_vfsop_unmount:1590: flushed all txn's!
2017-10-25 09:00:20.064531+0000 0x3423f    Default     0x0                  0      kernel: (apfs) fusion_wbc_thread_shutdown:1130:
                                                                                                Consider Fusion WBC Elevator thread of container 90FCC4BA-F955-41C4-A535-CBE3039D80A9 dead
2017-10-25 09:00:20.094619+0000 0x3423f    Default     0x0                  0      kernel: (apfs) apfs: total mem allocated: 187947699 (179 mb);
2017-10-25 09:00:20.094638+0000 0x3423f    Default     0x0                  0      kernel: (apfs) apfs_vfsop_unmount:1692: all done.  going home.  (numMountedAPFSVolumes 2)
```

# APFS FileVault

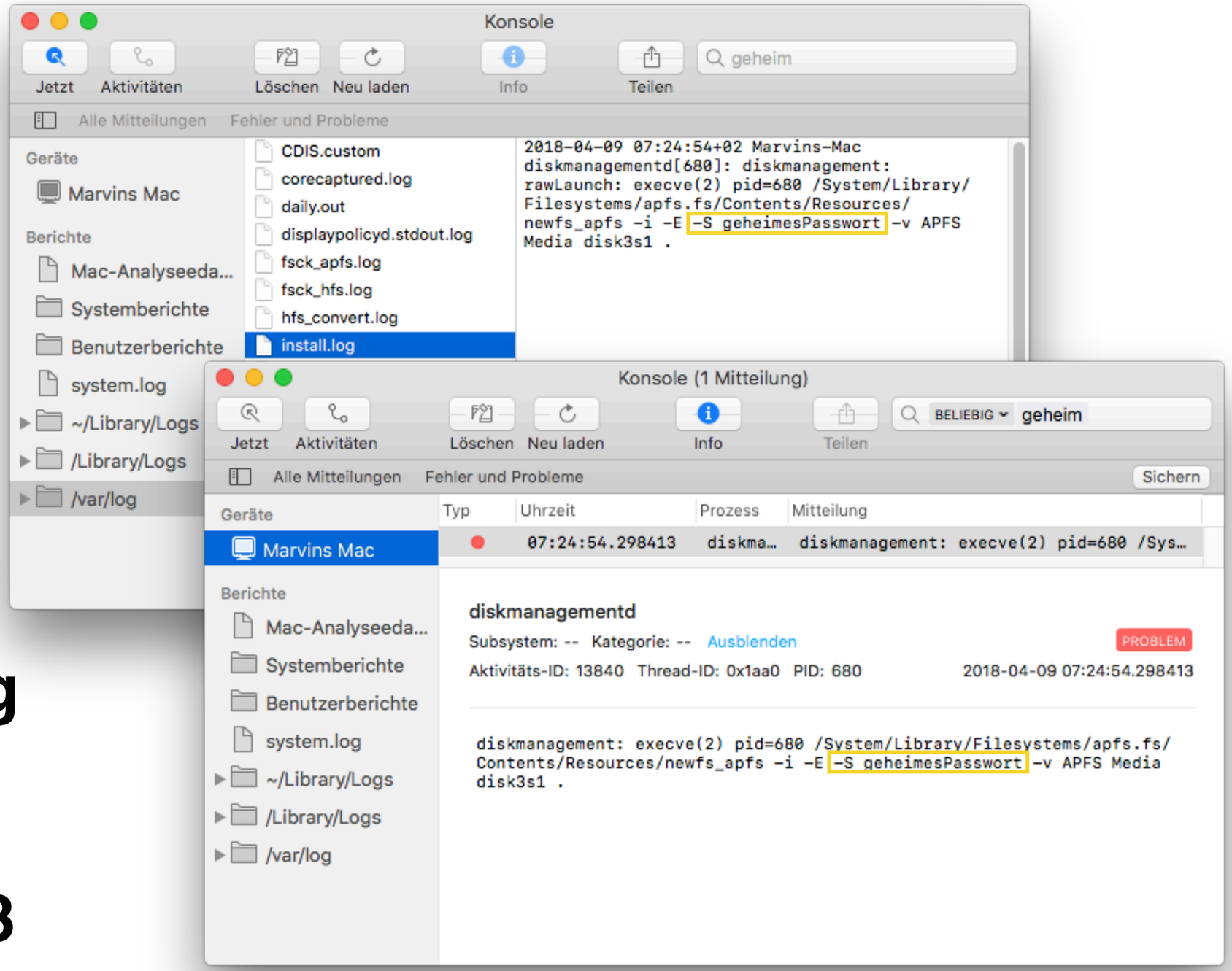


- AES-XTS oder AES-CBC
- Verschlüsselung auf **Dateisystemebene** (aktuell noch Single-Key Encryption)
- **Keine Angriffspunkte** bekannt (im Gegensatz zu HFS+)
- **Container-Metadaten** bleiben unverschlüsselt
- "*physikalische*" Sicherung des offenen APFS Volumes **funktioniert nicht**

# Sicherheitslücke: APFS FileVault Logs



- **newfs_apfs**
- **Passwort** konnte im **Klartext** in den **Logs** landen
- **install.log** und **Unified Logging**
- Versionen: 10.13.**0** - 10.13.**3**



# Quellen




- **Hansen, Toolan** - Decoding the APFS file system (2017)
- **Brandt** - Mac Upgrade (APFS, ULS) - Hochschule für Polizei Baden-Württemberg (2018)
- **Brandt, Eisoldt** - Mac Dateisysteme BKA - Hochschule für Polizei Baden-Württemberg (2018)
- **Dewald, Plum** - APFS Internals For Forensic Analysis (2018)

# Fragen?

POLIZEI
Nordrhein-Westfalen
Landesamt für Ausbildung, Fortbildung und Personalangelegenheiten

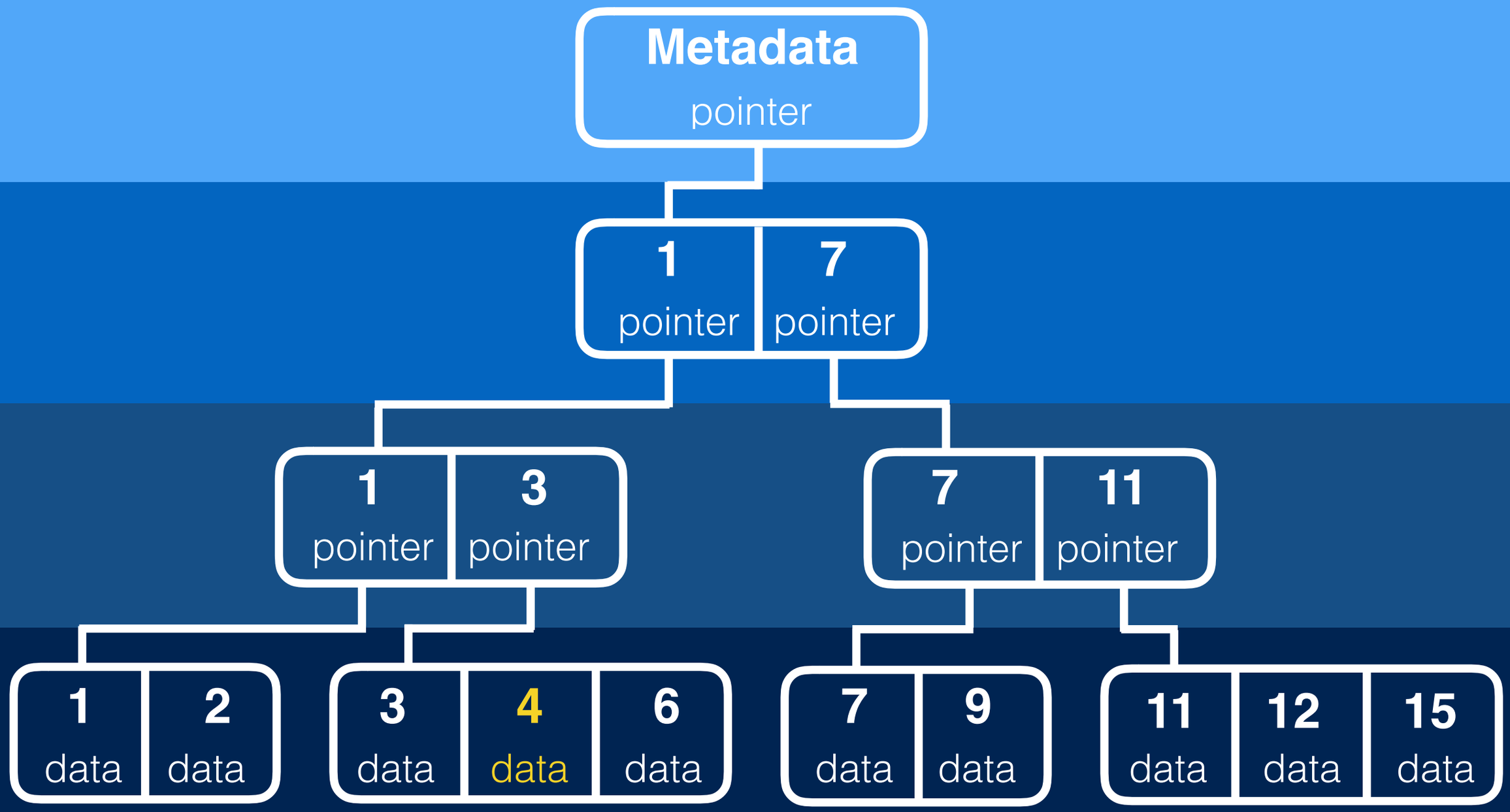
bürgerorientiert · professionell · rechtsstaatlich

# Danke für die Aufmerksamkeit!

marvin.blumenroeder@polizei.nrw.de

# Anhang:
# B-Tree - Beispiel





# Anhang:
# ULS: Post Mortem Extraktion



- Logarchiv erzeugen:

```
cd ~/Desktop
mkdir Logs
cp -R /Volumes/<Image>/var/db/diagnostics/ Logs
cp -R /Volumes/<Image>/var/db/uuidtext/ Logs
mv Logs UnifiedLogging.logarchive
sudo chown -R <Nutzer> UnifiedLogging.logarchive
```

- Logarchiv umwandeln:

```
log show --force UnifiedLogging.logarchive
```

- Rechtsklick auf die *.logarchive Datei machen und den Paketinhalt anzeigen
- Logarchiv analysieren:

```
log show UnifiedLogging.logarchive
```