Nederlands Forensisch Instituut
Ministerie van Veiligheid en Justitie

When does macOS Catalina create APFS checkpoints and which data could be retrieved from them?

Research Project 1 – Maarten van der Slik

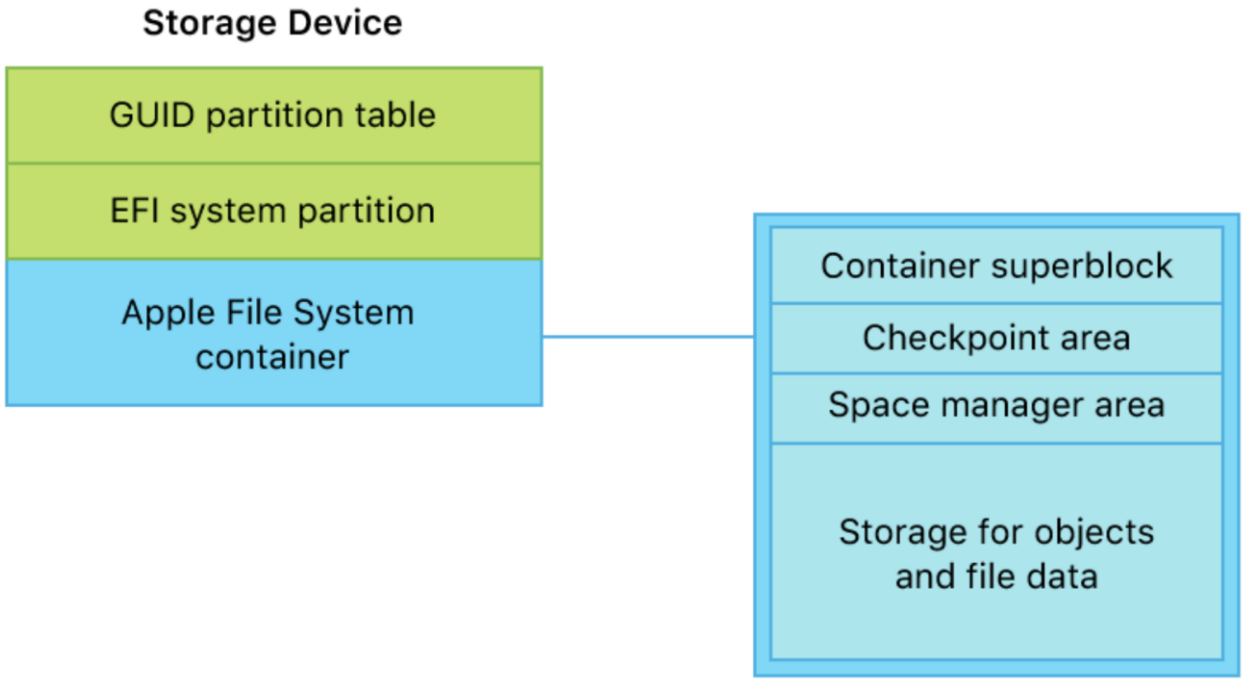

Figure 1 – Overview of APFS components (Apple Inc., 2019)

Default since High Sierra (10.13), iOS 13, tvOS 10.2, watchOS 3.2

"Copy-on-write"

New features

Apple File System

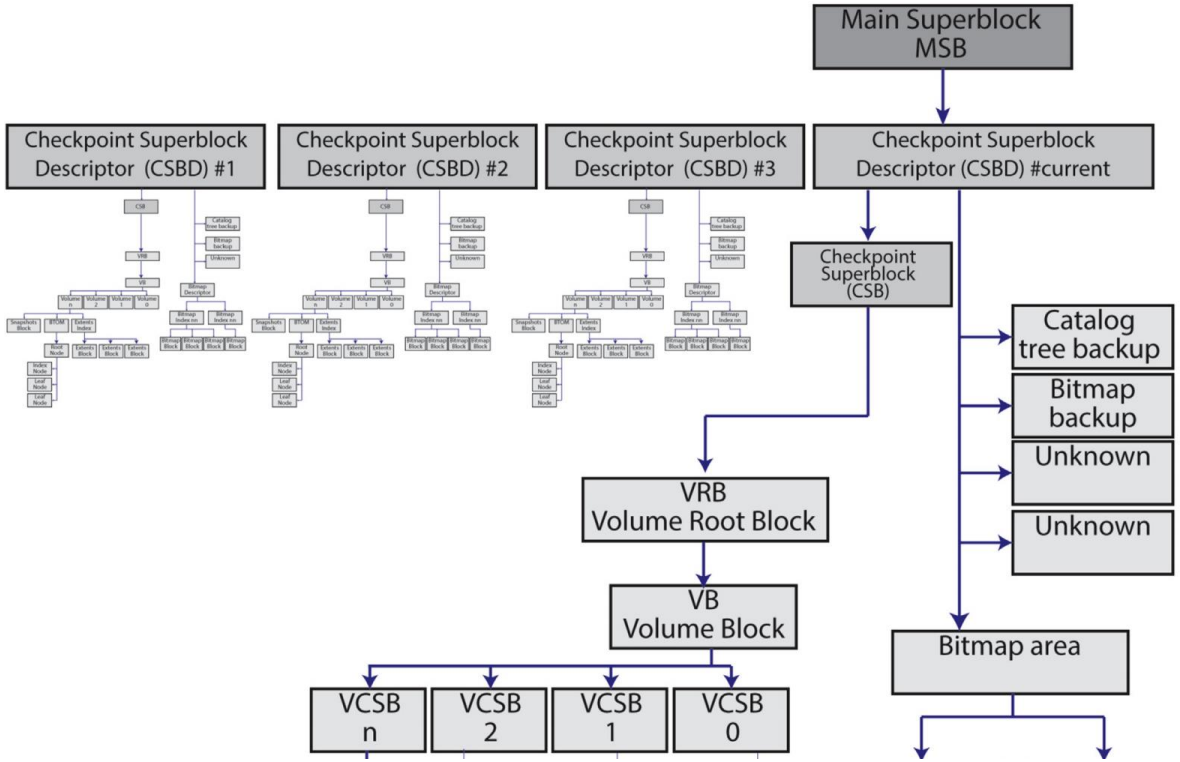

Figure 2 – APFS Structure (Hansen & Toolan, 2017)

- Pointers to checkpoints
- Read-only
- User ability to create and restore

Snapshots

Hansen & Toolan (2017), *Decoding the APFS File System*

Apple Inc (2018), Apple File System Reference

Plum & Dewald (2018), *APFS internals for forensic analysis*

Plum & Dewald (2018), *Forensic APFS File Recovery*

Related work

macOS Catalina (10.15.2) VM

48 raw disk images

12 experiments

Setup

Experiments

File experiments

- Seek & write
- Rewrite
- Append
- High-level API

Layout experiments

- Create folders
- Clone folders
- Move folders
- Remove folders
- Create files
- Clone files
- Move files
- Remove files

macOS Catalina (10.15.2) VM

48 raw disk images

12 experiments

Magic bytes in files

Magic bytes in volume meta-data

Method

Results after file operations

	Operation	Checkpoints w/ restart	Checkpoints w/o restart	Versions available w/ restart	Versions w/o restart
1	**Seek & write**	**67,163**	**65,127**	**1,1**	**1,1**
2	**Rewrite**	**108,67**	**84,285**	**24 (1 corrupted),23**	**65,65**
3	**Append**	**91,116**	**80,30**	**22,31**	**21,18**
4	**Foundation**	**111,175**	**218,278**	**1,1**	**1,1**

Results after layout operations

	Operation	Checkpoints w/ restart	Checkpoints w/o restart	Versions available w/ restart	Versions w/o restart
1	**mkdir**	**85,54**	**35,38**	**37,22**	**19,21**
2	**Folder cp -c**	**48,70**	**49,49**	**31,34**	**29,33**
3	**Folder mv**	**32,63**	**38,55**	**8,30**	**20,17**
4	**Folder rm**	**32,56**	**44,24**	**13,9**	**27,19**
5	**Touch**	**20 (1 overwritten root tree),60**	**39,37**	**10,28**	**19,19**
6	**File cp -c**	**38,16**	**37,39**	**11,10**	**17,19**
7	**File cp -c**	**86,31**	**38,56**	**35,12**	**19,20**
8	**File cp -c**	**62,57**	**42,57**	**15,11**	**25,16**

Metadata

Root tree

Timeline by iterate checkpoints

Inode Value

pos	size	type	id
0	8	u8le	parent_id
8	8	u8le	file_id
16	8	u8le	creation_timestamp
24	8	u8le	modified_timestamp
32	8	u8le	changed_timestamp
40	8	u8le	accessed_timestamp
48	8	u8le	flags
56	4	u4le	nchildren_or_nlink
68	4	u4le	bsd_flags
72	4	u4le	owner_id
76	4	u4le	group_id
80	2	u2le	mode
92	2	u2le	xf_num_ext
94	2	u2le	xf_used_data
96	...	xf_hea	xf_header

Figure 3 – Inode Entry Value (Plum & Dewald, 2018)

Metadata

Root tree

Timeline by iterate checkpoints

Afro & The Sleuth Kit

```
01-02 2020 19:34:59   409959 m..b f 0      0      0-103-128 /root/Test1A/Higher-level/1
01-02 2020 19:35:00   409959 .a.. f 0      0      0-104-128 /root/Test1A/Higher-level/1
                      409959 .a.. f 0      0      0-105-128 /root/Test1A/Higher-level/1
                      409959 .a.. f 0      0      0-106-128 /root/Test1A/Higher-level/1
                      409959 .a.. f 0      0      0-107-128 /root/Test1A/Higher-level/1
                      409959 .a.. f 0      0      0-108-128 /root/Test1A/Higher-level/1
                      409959 .a.. f 0      0      0-109-128 /root/Test1A/Higher-level/1
                      409959 .a.. f 0      0      0-110-128 /root/Test1A/Higher-level/1
                      409959 .a.. f 0      0      0-111-128 /root/Test1A/Higher-level/1
                      409959 .a.. f 0      0      0-112-128 /root/Test1A/Higher-level/1
                      409959 .a.. f 0      0      0-113-128 /root/Test1A/Higher-level/1
                      409959 .a.. f 0      0      0-114-128 /root/Test1A/Higher-level/1
```

Figure 4 – mactime output

- Leaves many older iterations of the container
- Access mode
- Not copy on write

Conclusion

- Leaves many older iterations of the container
- Access mode
- Not copy on write

- Few samples
- Low-level searches
- Small disks

Discussion

- Leaves many older iterations of the container
- Access mode
- Not copy on write

- Few samples
- Low-level searches
- Small disks

Questions?