Apple File System

Slack Analysis and Detection of Hidden Data

Axel Koolhaas
Woudt van Steenbergen

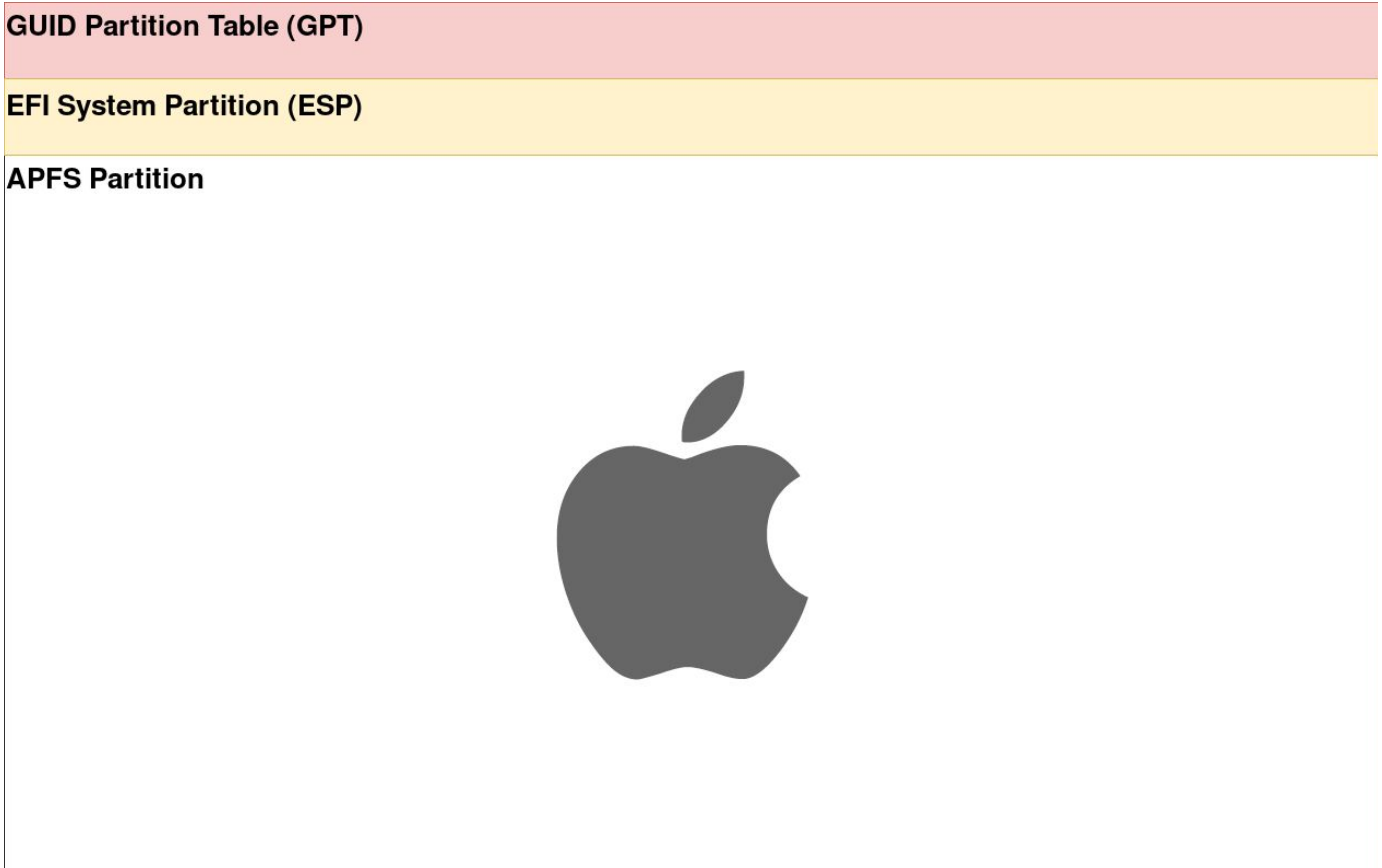
Introduction to Apple File System (APFS)

- 2016 Filesystem released, replacing HFS+
- 2017 K. H. Hansen & F. Toolan: Decoding the APFS file system
- 2018 Official specification released
- 2018 J. Plum & A. Dewald: Forensic APFS file recovery
- 2019 T. Göbel, J. Türr & H. Baier: Revisiting Data Hiding Techniques for Apple File System

Today APFS is the default filesystem in use across Apple devices:

iOS, macOS, tvOS, watchOS

APFS partition overview



GUID Partition Table (GPT)

EFI System Partition (ESP)

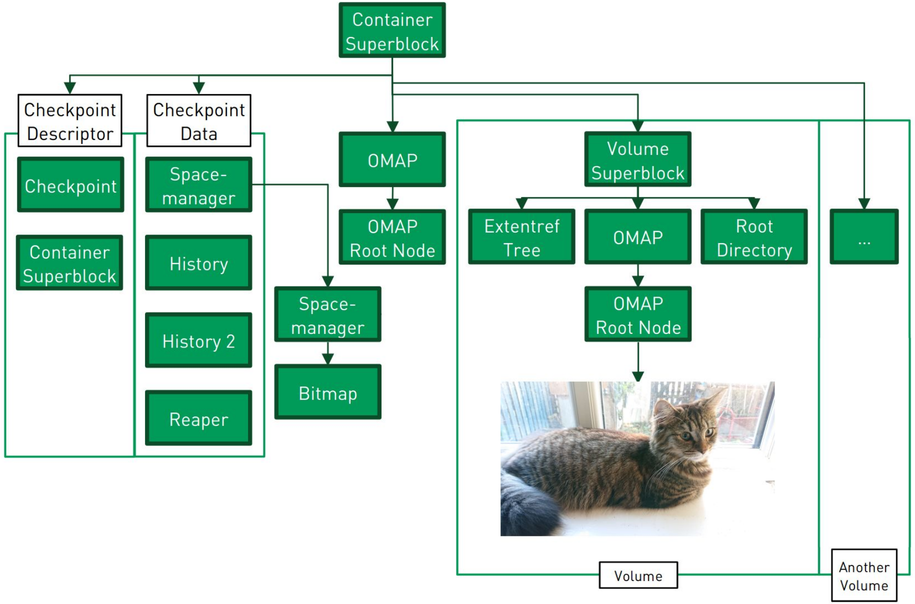
APFS Partition

APFS partition overview

GUID Partition Table (GPT)

EFI System Partition (ESP)

APFS Partition

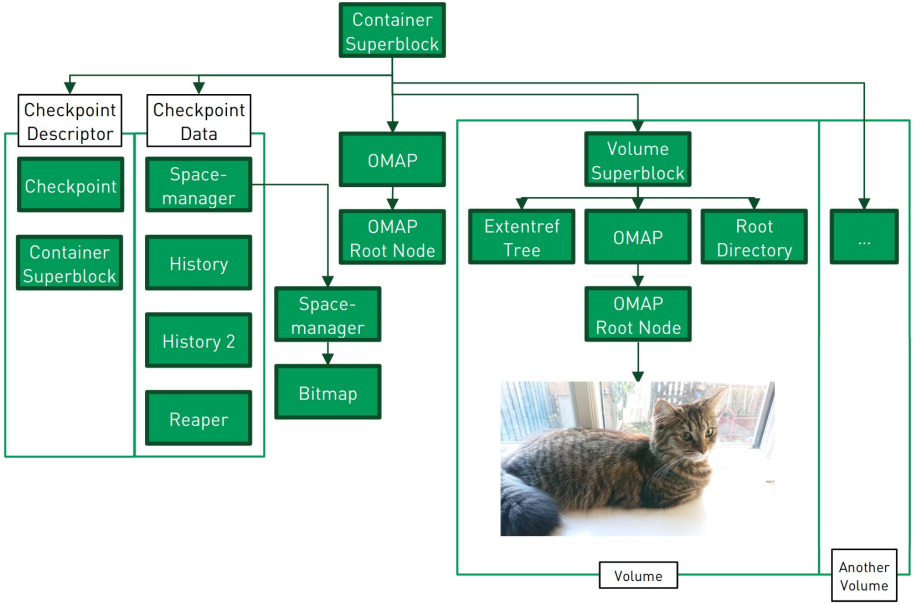


APFS partition overview

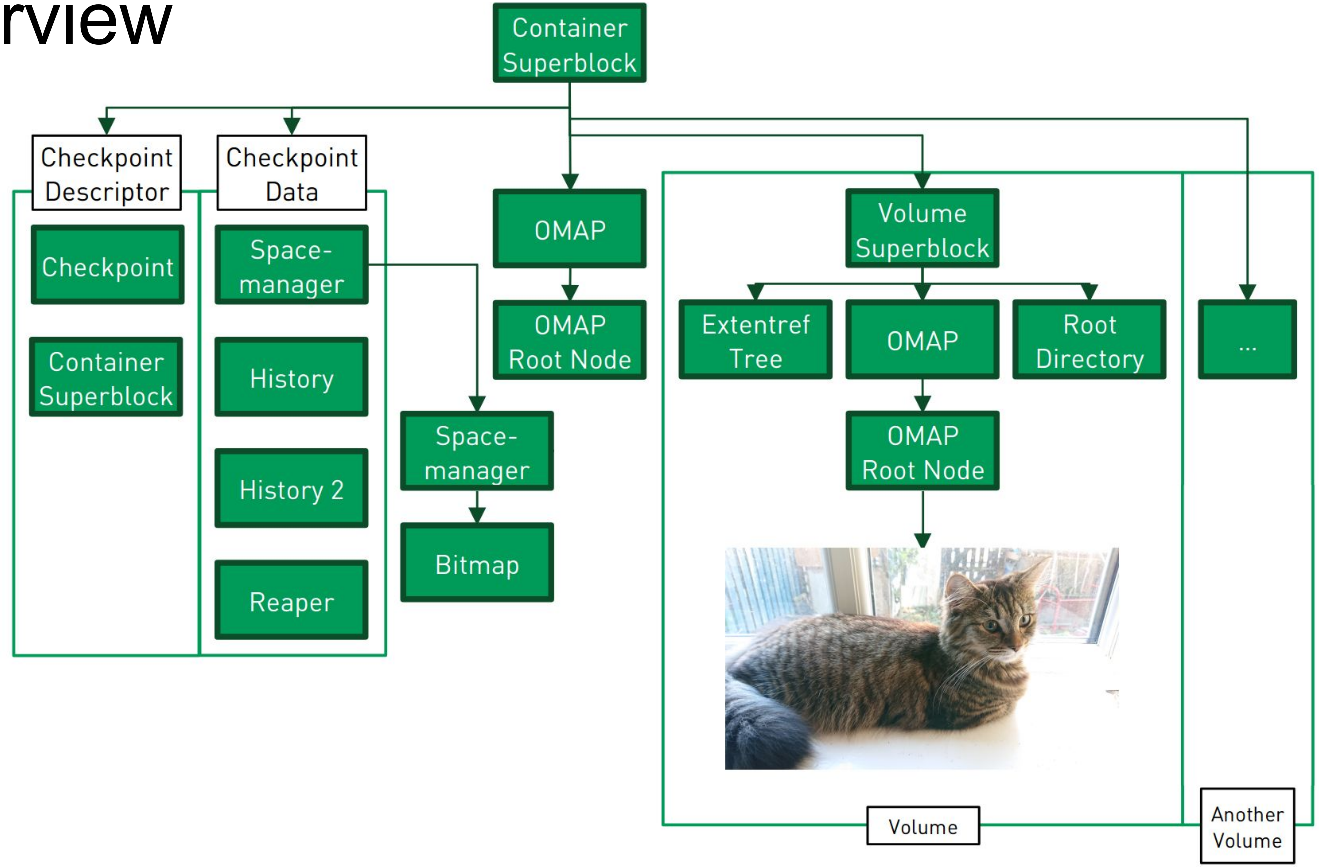
GUID Partition Table (GPT)

EFI System Partition (ESP)

APFS ~~Partition~~ container



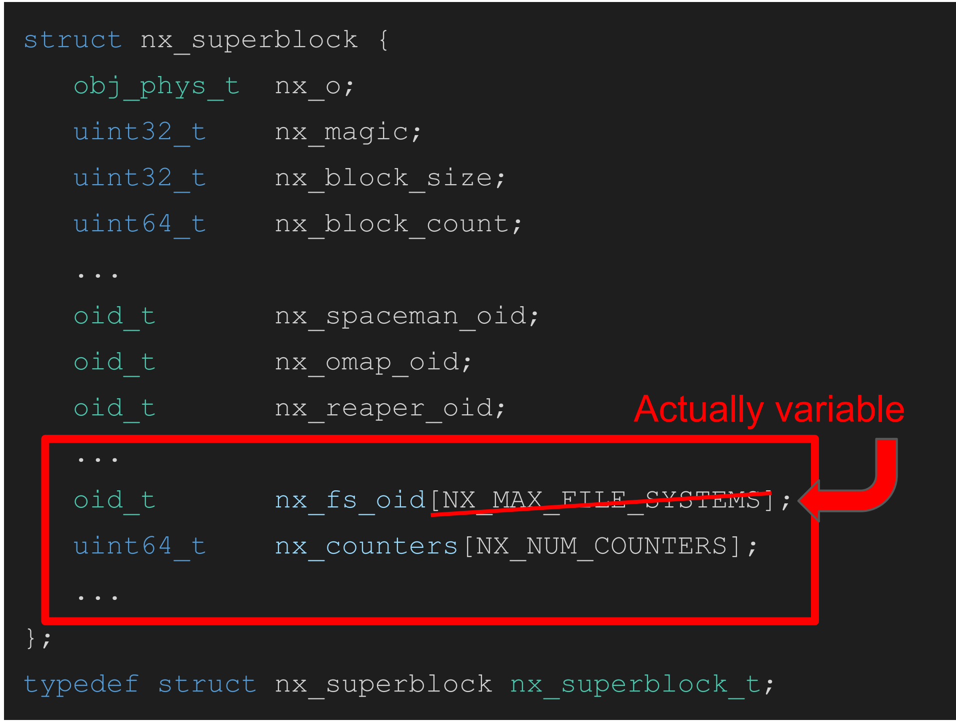
APFS overview



Edit from source: J. Plum & H. Dewald 2018

APFS overview (ctd.)

- Data structures may have variable length
- Some objects utilise padding for processor / memory alignment, 64 bit or 4096 byte
- Speed > storage space
- A block often only contains 1 object, leaving a lot of unused space

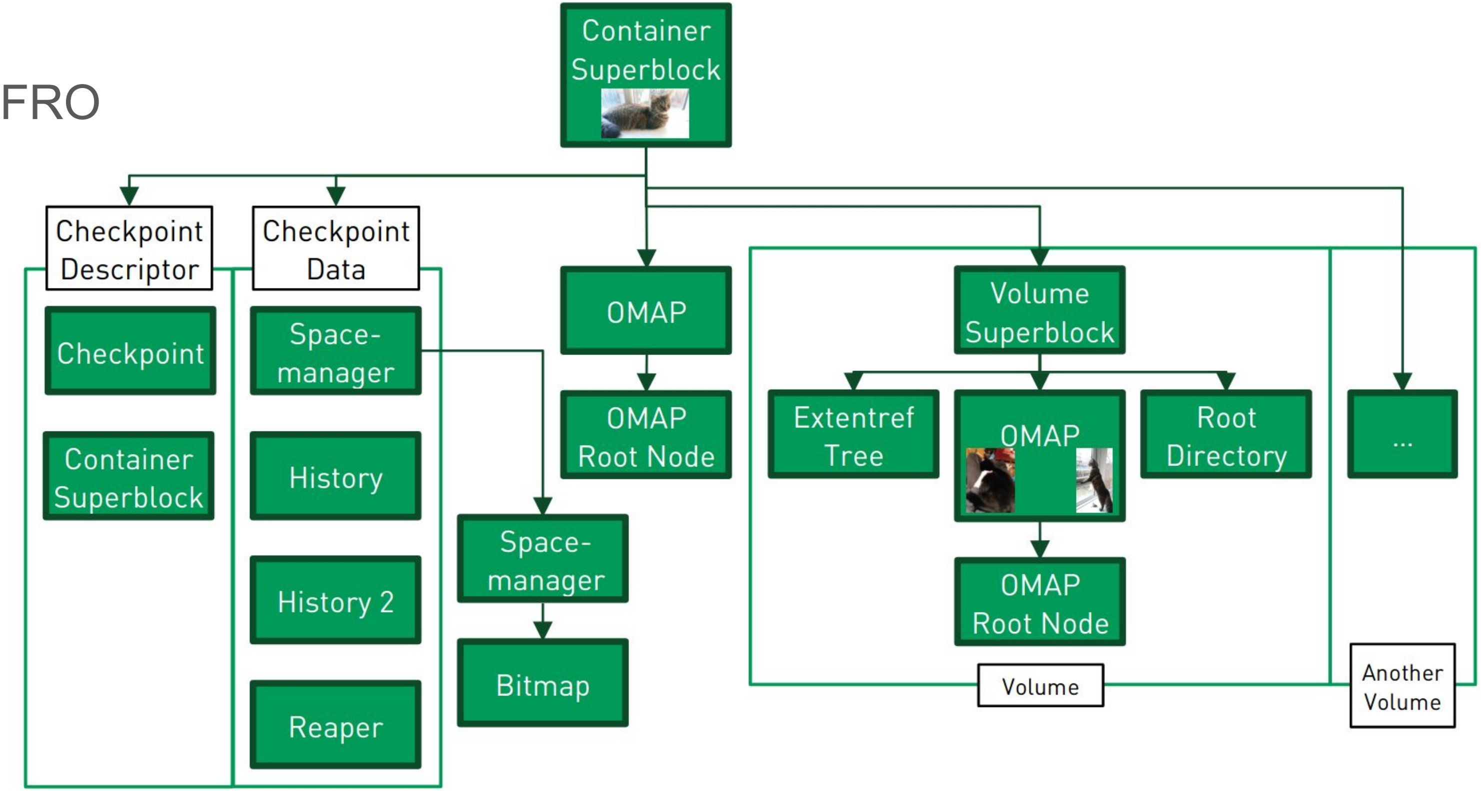


```
struct nx_superblock {
    obj_phys_t  nx_o;
    uint32_t    nx_magic;
    uint32_t    nx_block_size;
    uint64_t    nx_block_count;
    ...
    oid_t       nx_spaceman_oid;
    oid_t       nx_omap_oid;
    oid_t       nx_reaper_oid;
    ...
    oid_t       nx_fs_oid~~[NX_MAX_FILE_SYSTEMS]~~;
    uint64_t    nx_counters[NX_NUM_COUNTERS];
    ...
};
typedef struct nx_superblock nx_superblock_t;
```

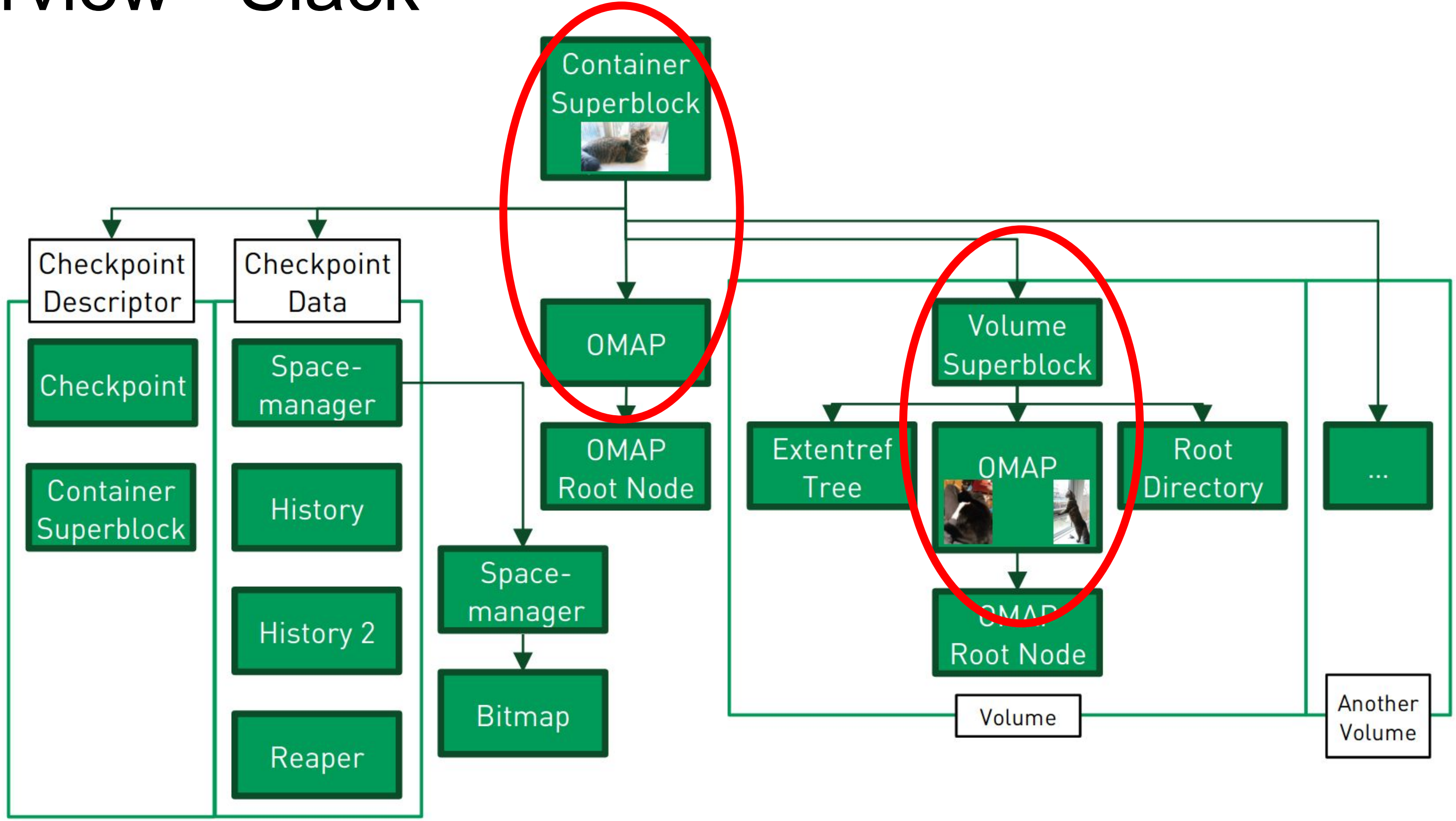
Actually variable

Our research: Detection of hidden data

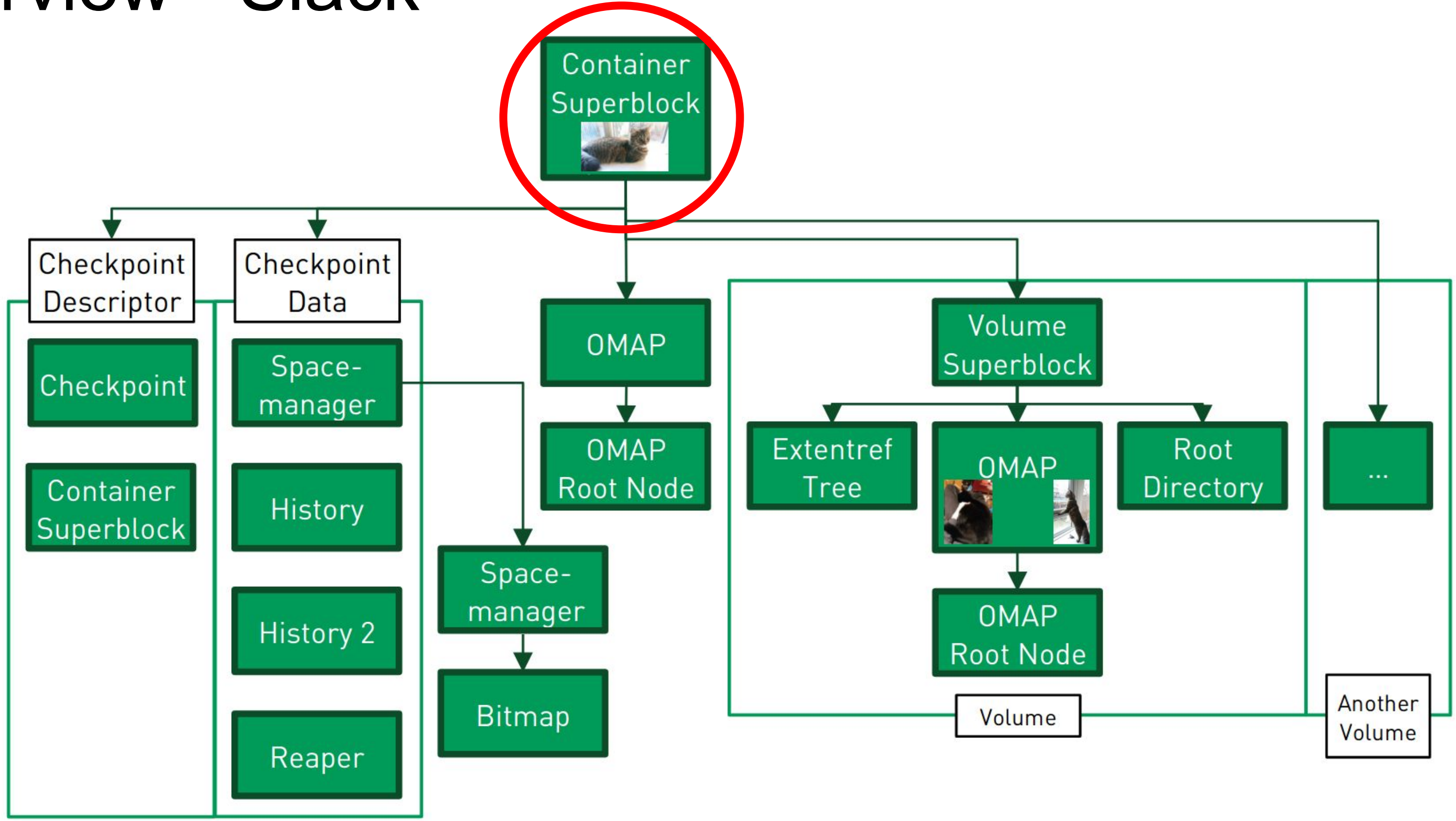
Expand tool: AFRO



Overview - Slack

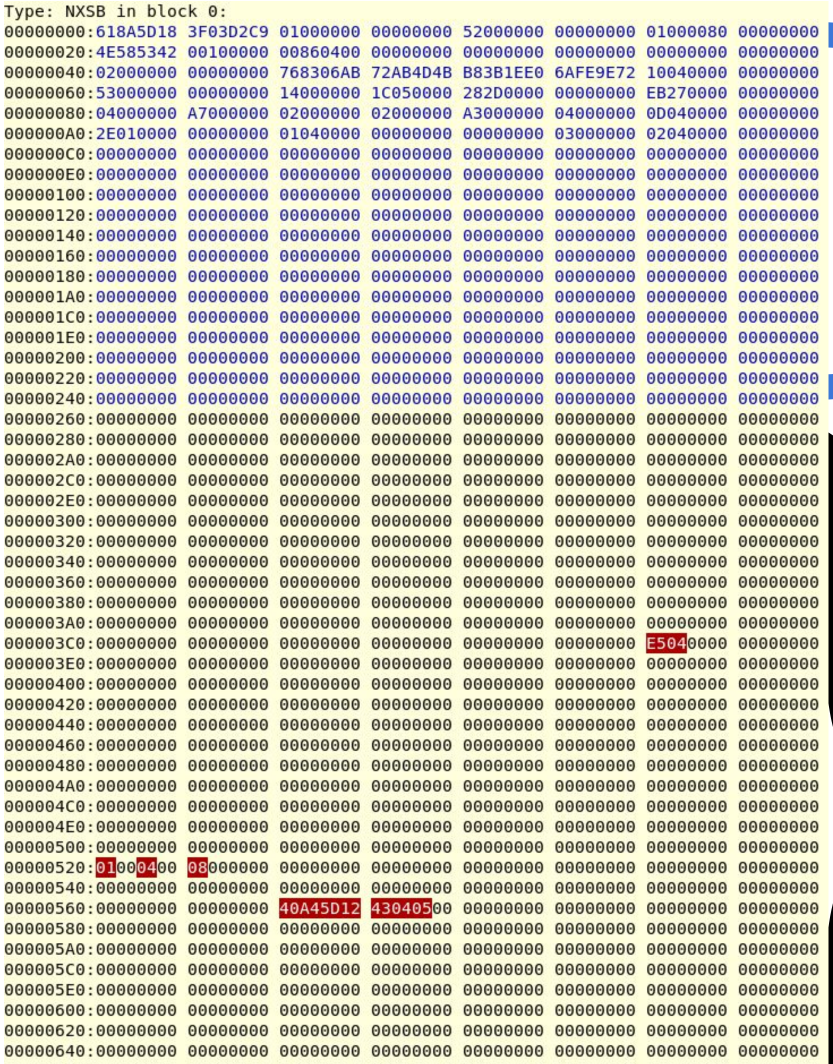


Overview - Slack



Slack hiding

Container Superblock



```
Type: NXSB in block 0:
00000000:618A5D18 3F03D2C9 01000000 00000000 52000000 00000000 01000080 00000000
00000020:4E585342 00100000 00860400 00000000 00000000 00000000 00000000 00000000
00000040:02000000 00000000 768306AB 72AB4D4B B83B1EE0 6AFE9E72 10040000 00000000
00000060:53000000 00000000 14000000 1C050000 282D0000 00000000 EB270000 00000000
00000080:04000000 A7000000 02000000 02000000 A3000000 04000000 0D040000 00000000
000000A0:2E010000 00000000 01040000 00000000 00000000 03000000 02040000 00000000
000000C0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000000E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000100:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000120:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000140:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000160:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000180:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000001A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000001C0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000001E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000200:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000220:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000240:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000260:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000280:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000002A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000002C0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000002E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000300:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000320:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000340:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000360:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000380:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000003A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000003C0:00000000 00000000 00000000 00000000 00000000 00000000 E5040000 00000000
000003E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000400:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000420:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000440:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000460:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000480:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000004A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000004C0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000004E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000500:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000520:01000400 08000000 00000000 00000000 00000000 00000000 00000000 00000000
00000540:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000560:00000000 00000000 40A45D12 43040500 00000000 00000000 00000000 00000000
00000580:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000005A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000005C0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000005E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000600:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000620:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000640:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
```

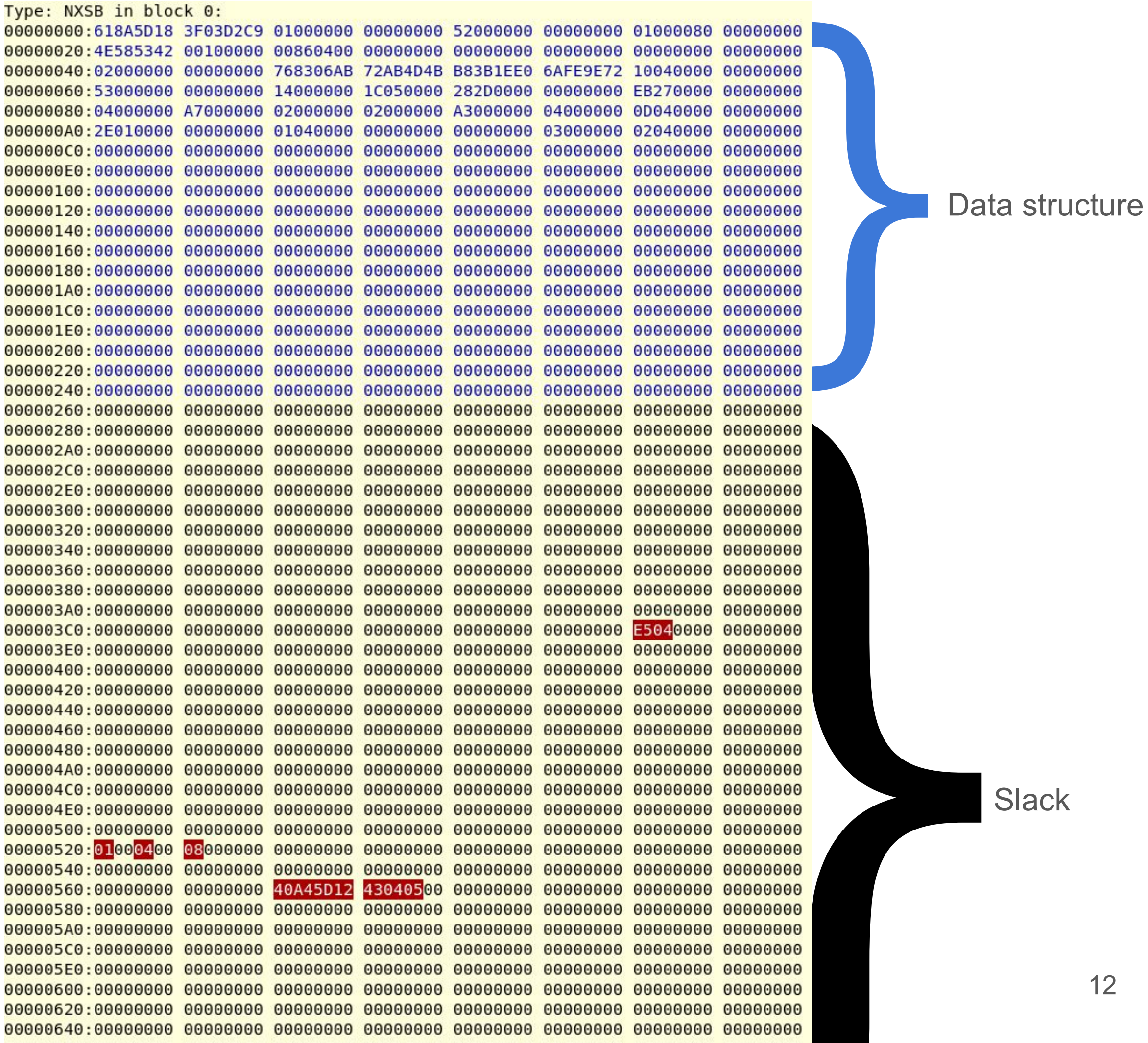
Data structure

Slack

Slack hiding

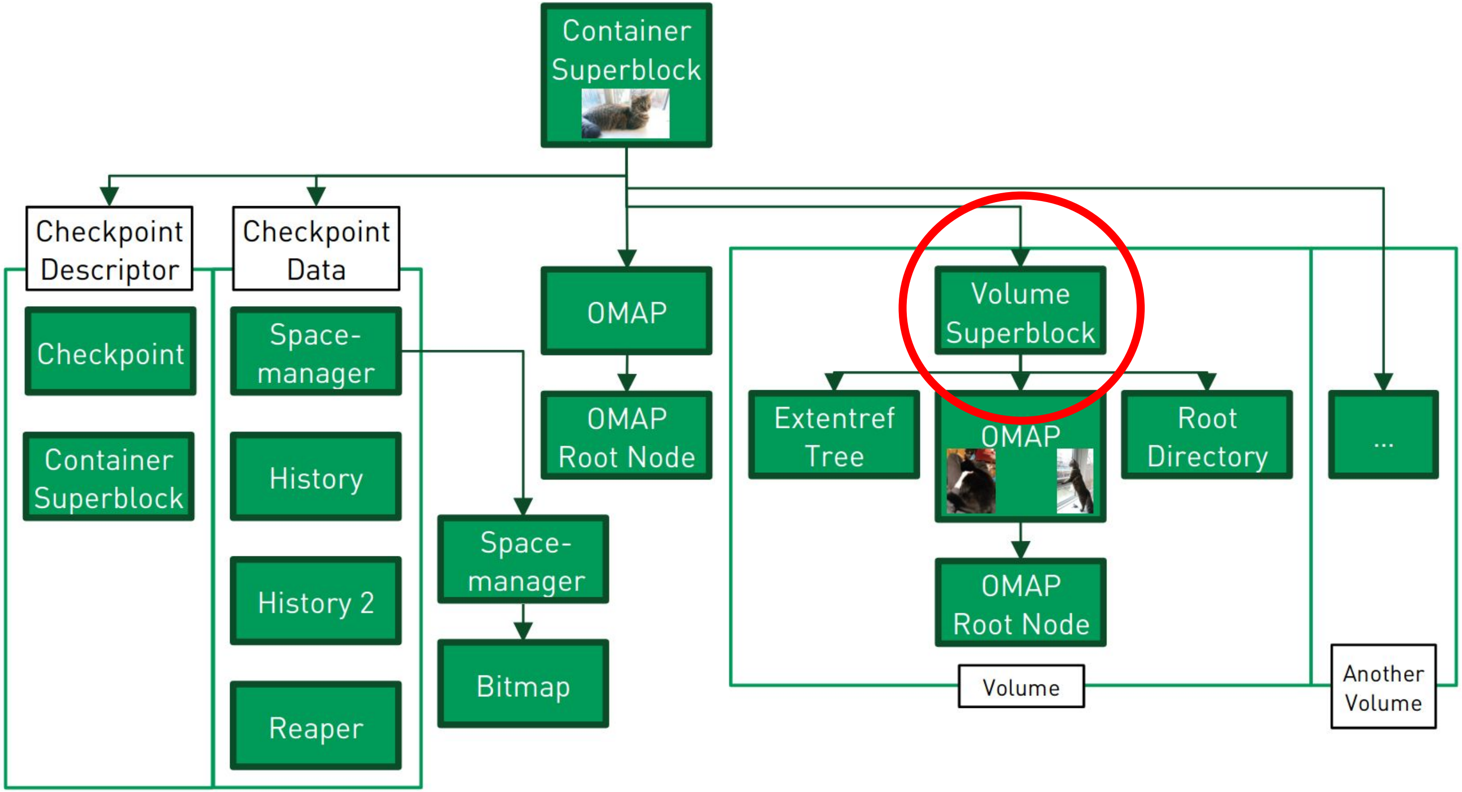
Container Superblock

Offset	Value (Little endian)
03DC	<variable 2 bytes>
0520	00000008 00040001
0568	00050443 125DA440



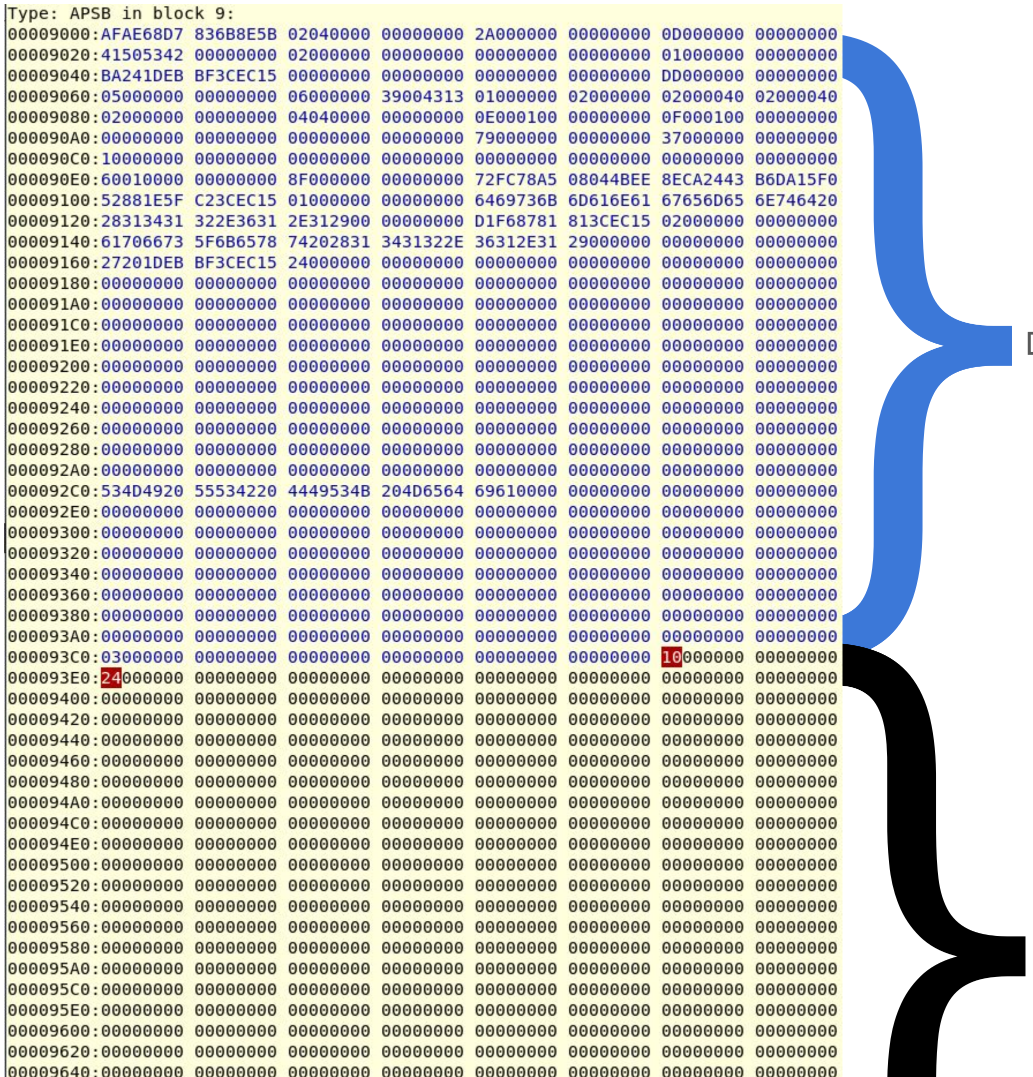
```
Type: NXSB in block 0:
00000000:618A5D18 3F03D2C9 01000000 00000000 52000000 00000000 01000080 00000000
00000020:4E585342 00100000 00860400 00000000 00000000 00000000 00000000 00000000
00000040:02000000 00000000 768306AB 72AB4D4B B83B1EE0 6AFE9E72 10040000 00000000
00000060:53000000 00000000 14000000 1C050000 282D0000 00000000 EB270000 00000000
00000080:04000000 A7000000 02000000 02000000 A3000000 04000000 0D040000 00000000
000000A0:2E010000 00000000 01040000 00000000 00000000 03000000 02040000 00000000
000000C0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000000E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000100:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000120:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000140:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000160:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000180:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000001A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000001C0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000001E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000200:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000220:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000240:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000260:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000280:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000002A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000002C0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000002E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000300:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000320:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000340:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000360:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000380:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000003A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000003C0:00000000 00000000 00000000 00000000 00000000 00000000 E5040000 00000000
000003E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000400:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000420:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000440:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000460:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000480:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000004A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000004C0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000004E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000500:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000520:01000400 08000000 00000000 00000000 00000000 00000000 00000000 00000000
00000540:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000560:00000000 00000000 40A45D12 43040500 00000000 00000000 00000000 00000000
00000580:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000005A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000005C0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000005E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000600:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000620:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000640:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
```

Overview - Slack



Slack hiding

Volume Superblock



```
Type: APSB in block 9:
00009000:AFAE68D7 836B8E5B 02040000 00000000 2A000000 00000000 0D000000 00000000
00009020:41505342 00000000 02000000 00000000 00000000 00000000 01000000 00000000
00009040:BA241DEB BF3CEC15 00000000 00000000 00000000 00000000 DD000000 00000000
00009060:05000000 00000000 06000000 39004313 01000000 02000000 02000040 02000040
00009080:02000000 00000000 04040000 00000000 0E000100 00000000 0F000100 00000000
000090A0:00000000 00000000 00000000 00000000 79000000 00000000 37000000 00000000
000090C0:10000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000090E0:60010000 00000000 8F000000 00000000 72FC78A5 08044BEE 8ECA2443 B6DA15F0
00009100:52881E5F C23CEC15 01000000 00000000 6469736B 6D616E61 67656D65 6E746420
00009120:28313431 322E3631 2E312900 00000000 D1F68781 813CEC15 02000000 00000000
00009140:61706673 5F6B6578 74202831 3431322E 36312E31 29000000 00000000 00000000
00009160:27201DEB BF3CEC15 24000000 00000000 00000000 00000000 00000000 00000000
00009180:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000091A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000091C0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000091E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009200:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009220:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009240:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009260:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009280:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000092A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000092C0:534D4920 55534220 4449534B 204D6564 69610000 00000000 00000000 00000000
000092E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009300:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009320:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009340:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009360:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009380:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000093A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000093C0:03000000 00000000 00000000 00000000 00000000 00000000 10000000 00000000
000093E0:24000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009400:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009420:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009440:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009460:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009480:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000094A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000094C0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000094E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009500:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009520:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009540:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009560:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009580:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000095A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000095C0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000095E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009600:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009620:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009640:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
```

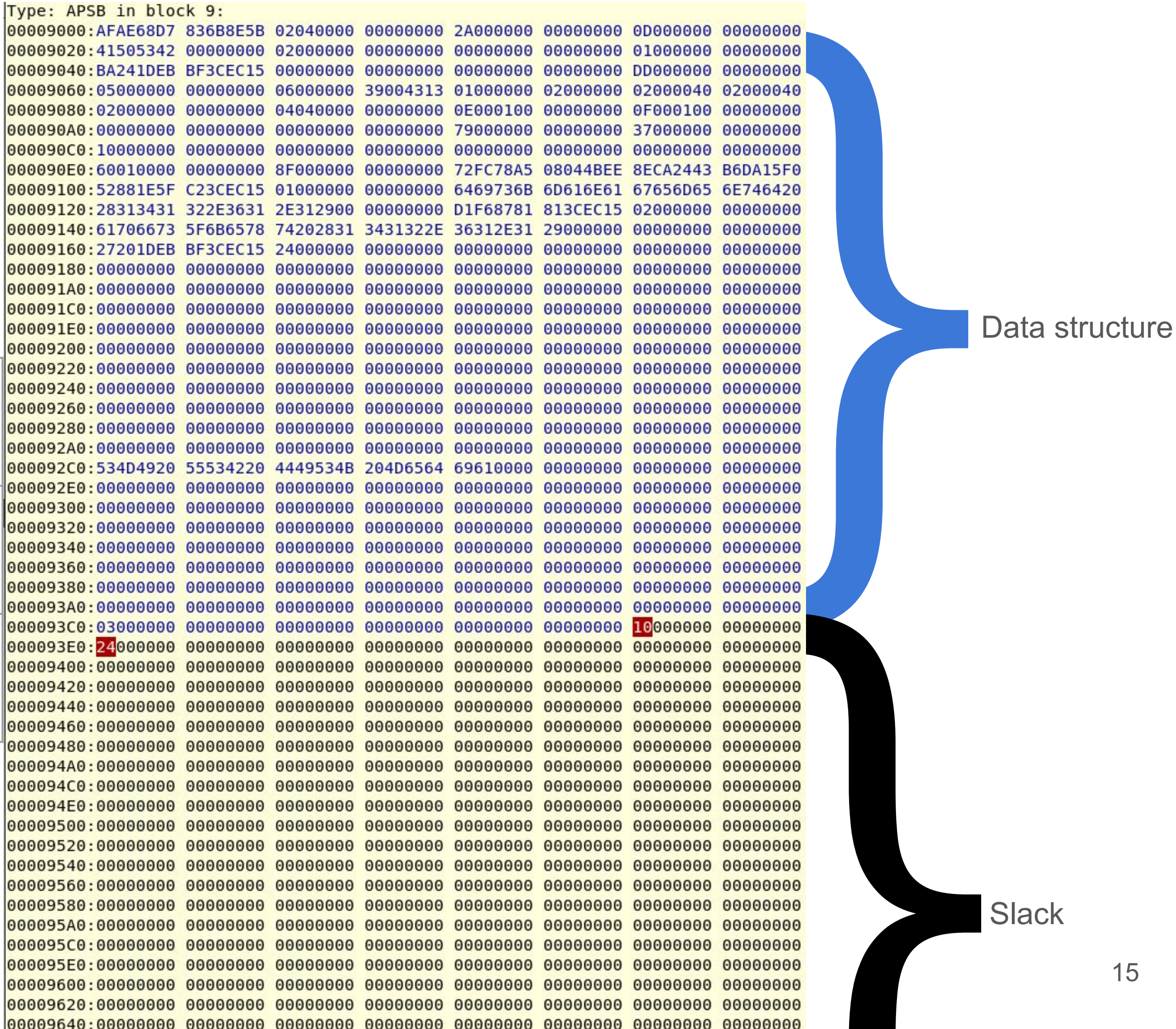
Data structure

Slack

Slack hiding

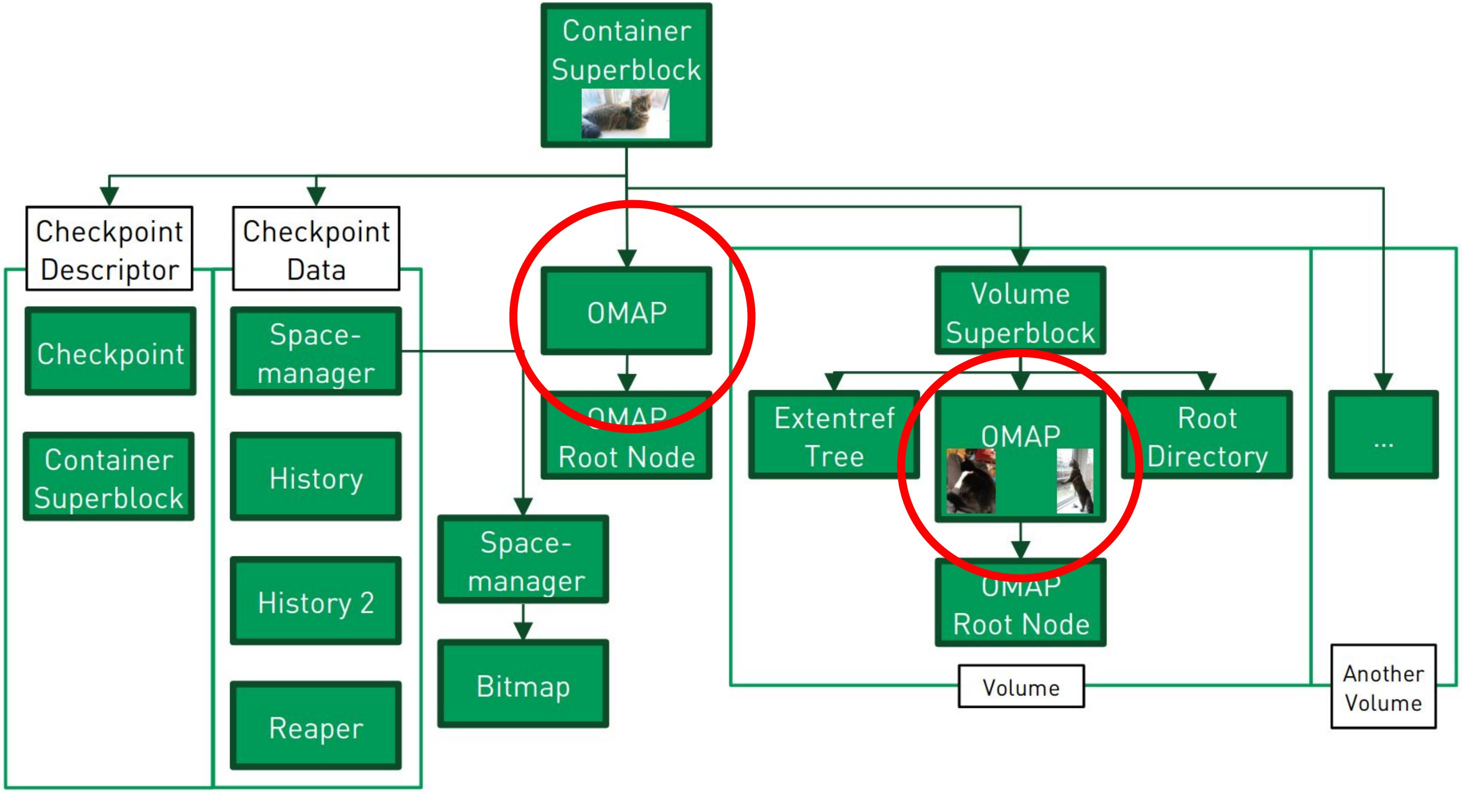
Volume Superblock

Offset	Value (Little endian)
03D8	10
03E0	<variable 1 byte>

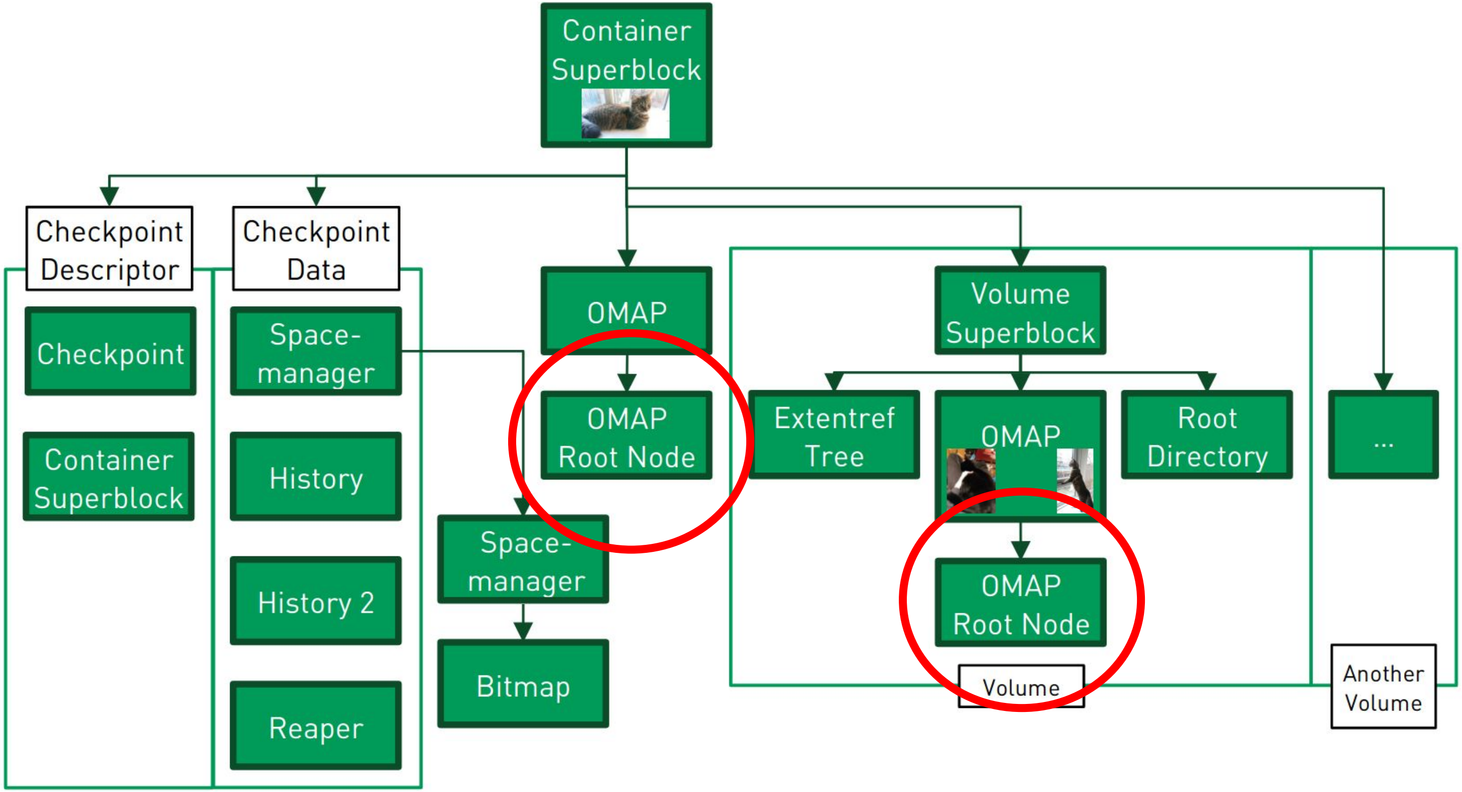


```
Type: APSB in block 9:
00009000:AFAE68D7 836B8E5B 02040000 00000000 2A000000 00000000 0D000000 00000000
00009020:41505342 00000000 02000000 00000000 00000000 00000000 01000000 00000000
00009040:BA241DEB BF3CEC15 00000000 00000000 00000000 00000000 DD000000 00000000
00009060:05000000 00000000 06000000 39004313 01000000 02000000 02000040 02000040
00009080:02000000 00000000 04040000 00000000 0E000100 00000000 0F000100 00000000
000090A0:00000000 00000000 00000000 00000000 79000000 00000000 37000000 00000000
000090C0:10000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000090E0:60010000 00000000 8F000000 00000000 72FC78A5 08044BEE 8ECA2443 B6DA15F0
00009100:52881E5F C23CEC15 01000000 00000000 6469736B 6D616E61 67656D65 6E746420
00009120:28313431 322E3631 2E312900 00000000 D1F68781 813CEC15 02000000 00000000
00009140:61706673 5F6B6578 74202831 3431322E 36312E31 29000000 00000000 00000000
00009160:27201DEB BF3CEC15 24000000 00000000 00000000 00000000 00000000 00000000
00009180:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000091A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000091C0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000091E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009200:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009220:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009240:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009260:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009280:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000092A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000092C0:534D4920 55534220 4449534B 204D6564 69610000 00000000 00000000 00000000
000092E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009300:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009320:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009340:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009360:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009380:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000093A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000093C0:03000000 00000000 00000000 00000000 00000000 00000000 10000000 00000000
000093E0:24000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009400:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009420:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009440:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009460:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009480:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000094A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000094C0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000094E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009500:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009520:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009540:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009560:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009580:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000095A0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000095C0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
000095E0:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009600:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009620:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00009640:00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
```

Overview - Slack



Hiding technique: inode pad



Inode pad fields hiding

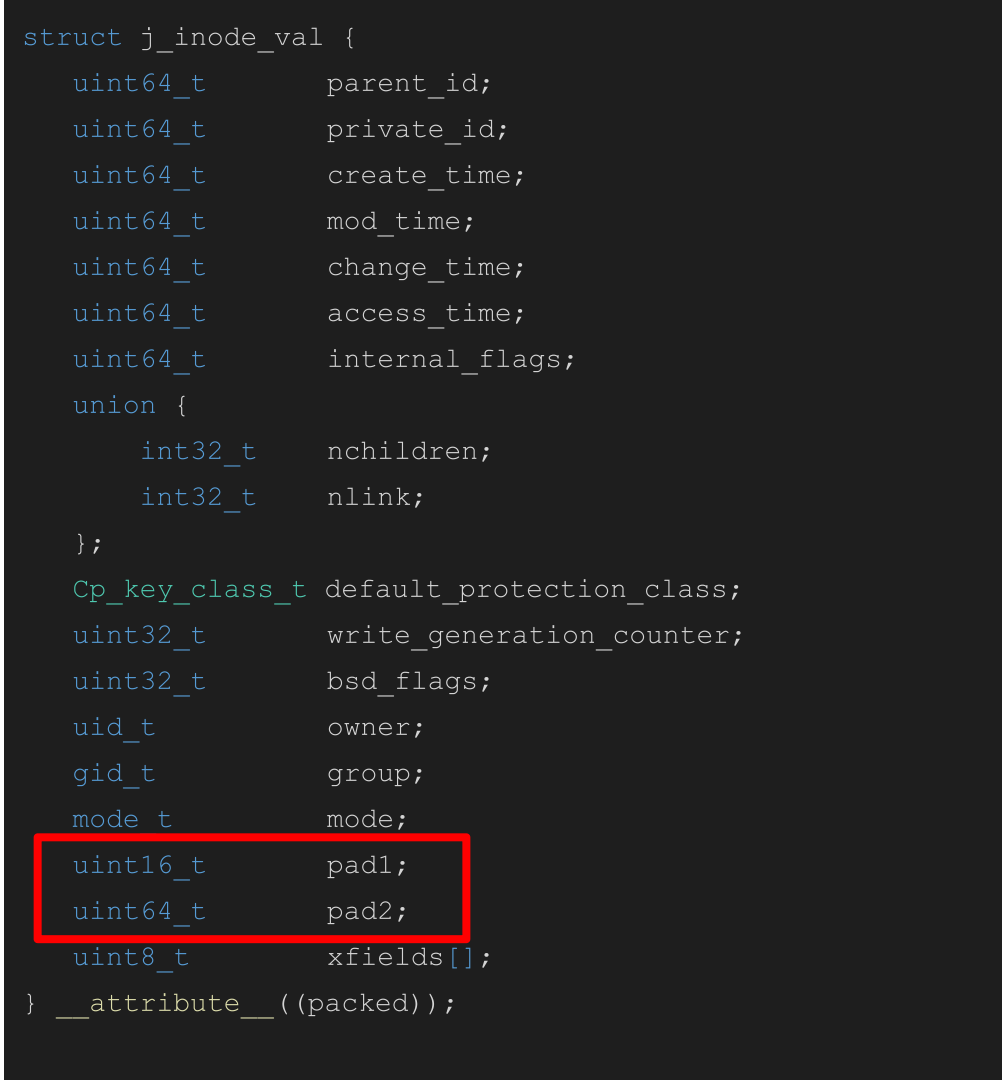
An inode consists of:

- The key half: j_inode_key_t
- The value half: **j_inode_val_t**

Inode pad fields hiding

An inode consists of:

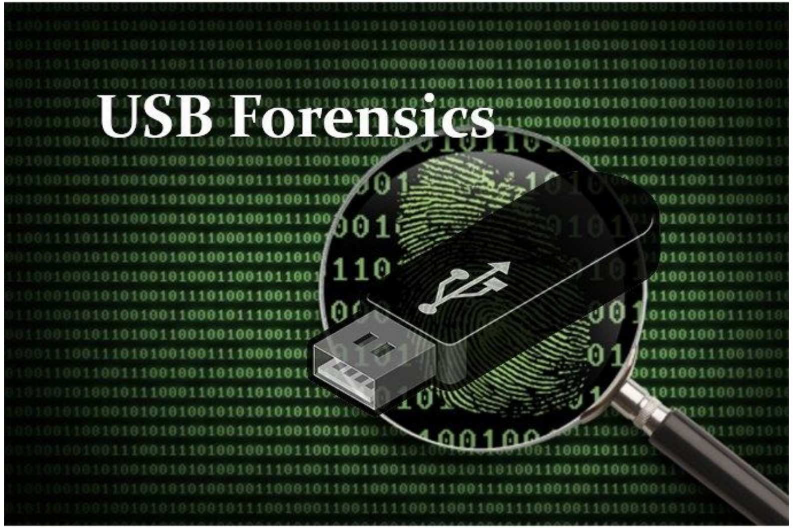
- The key half: j_inode_key_t
- The value half: **j_inode_val_t**



```
struct j_inode_val {
    uint64_t        parent_id;
    uint64_t        private_id;
    uint64_t        create_time;
    uint64_t        mod_time;
    uint64_t        change_time;
    uint64_t        access_time;
    uint64_t        internal_flags;
    union {
        int32_t     nchildren;
        int32_t     nlink;
    };
    Cp_key_class_t default_protection_class;
    uint32_t        write_generation_counter;
    uint32_t        bsd_flags;
    uid_t           owner;
    gid_t           group;
    mode_t          mode;
    uint16_t        pad1;
    uint64_t        pad2;
    uint8_t         xfields[];
} __attribute__((packed));
```

Volatility of APFS data structures

- Data structures are not permanent
- Retired data structures are zeroed out



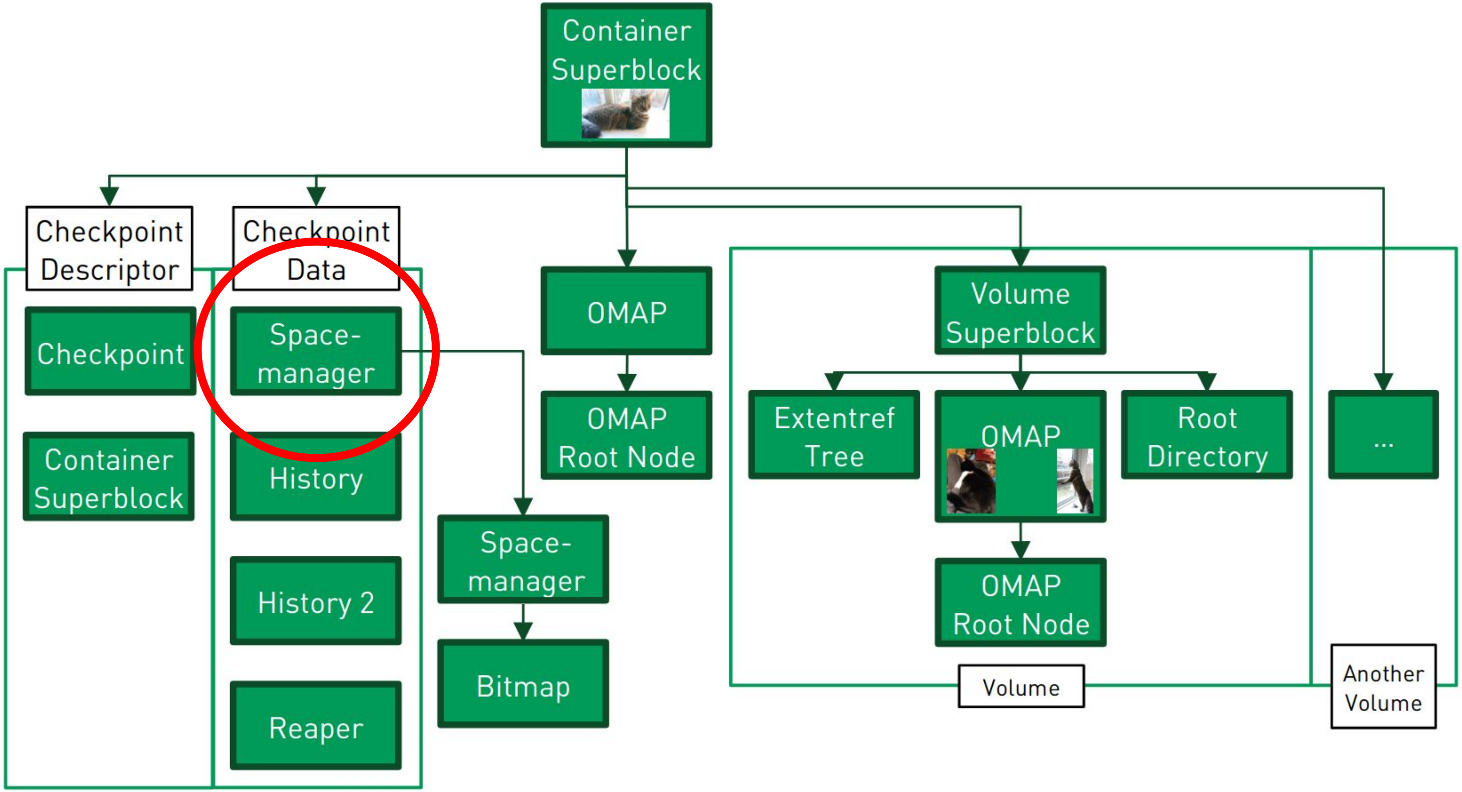
Conclusion

- Irregularities in superblock slack space are easily identifiable
  - However, the function of the unspecified fields is unknown
  - When mounting, old blocks are quickly discarded, making this volatile hiding technique
- Inode pad fields should be zero, but aren’t enforced by the APFS driver
  - Modifications are easily detectable

Future work

- Analyze values in superblock slack, and possibly other data structures
- Detection of hidden files that are detached from the filesystem
  - Spacemanager Bitmap (e.g. block aggregation abuse for write protection)
  - Remove inode entry from tree, erasing the file index
- Compare APFS drivers of different operating systems, e.g., macOS vs. iOS

Hiding technique: spacemanager?



Summary

Hiding data within/besides APFS data structures is possible, but detectable!

- Volatile for the superblock slack
- Undefined bytes should be further researched to determine their functionality