

APFS File System Format Reference Sheet

By: Sarah Edwards| Twitter: @iamevltwin | Email: oompa@csh.rit.edu
FOR518 - Mac and iOS Forensic Analysis & Incident Response - for518.com



Object Header (obj_phys_t)

Offset	Size (in bytes)	Field	Notes
0	8	o_cksum	Fletcher 64 Checksum
8	8	o_oid	Object ID
16	8	o_xid	Transaction ID
24	2	o_type.type	Object Type
26	2	o_type.flags	Object Flags
28	4	o_subtype	Object Subtype

Object Type (Hex)	Object Type (Dec)	Object Type/Subtype
0x0000	0	None
0x0100	1	Container Super Block
0x0200	2	B-Tree
0x0300	3	B-Tree Node
0x0500	5	Spaceman
0x0B00	11	Object Map (OMAP)
0x0D00	13	File System (Volume Super Block)
0x0E00	14	File System Tree

Container Super Block (nx_superblock_t)

Offset	Size (in bytes)	Field	Notes
32	4	magic "NXSB"	Container Magic Number: 0x4E585342 = "NSXB"
36	4	nx_block_size	Block Size (ie: 4096)
40	8	nx_block_count	Block Count (Block Count*Block Size = Container Size in Bytes)
48	8	nx_features	Features
56	8	nx_read_only_compatible_features	Read-only Compatible Features
64	8	nx_incompatible_features	Incompatible Features
72	16	nx_uuid	Container UUID (diskutil info /dev/disk#)
88	8	nx_next_oid	Next Object ID (OID)
96	8	nx_next_xid	Next Transaction ID (XID)
104	4	nx_xp_desc_blocks	Blocks used by Checkpoint Descriptor Area
108	4	nx_xp_data_blocks	Blocks used by Checkpoint Data Area
112	8	nx_xp_desc_base	Base address of Checkpoint Descriptor Area or Physical Object ID
120	8	nx_xp_data_base	Base address of Checkpoint Data Area or Physical Object ID
128	4	nx_xp_desc_next	Next Index for Checkpoint Descriptor Area
132	4	nx_xp_data_next	Next Index for Checkpoint Data Area
136	4	nx_xp_desc_index	Index for first item in Checkpoint Descriptor Area
140	4	nx_xp_desc_len	Number of blocks in Checkpoint Descriptor Area Used
144	4	nx_xp_data_index	Index for first item in Checkpoint Data Area
148	4	nx_xp_data_len	Number of blocks in Checkpoint Data Area Used
152	8	nx_spaceman_oid	Space Manager Object ID (OID)
160	8	nx_omap_oid	Container Object Map Object ID (OID)
168	8	nx_reaper_oid	Reaper Object ID (OID)
176	4	nx_test_type	Reserved for Testing
180	4	nx_max_file_systems	Maximum Number of Volumes in this Container
184	8	nx_fs_oid[0]	Array of OIDs for Volumes in this Container

Volume Super Block (apfs_superblock_t)

Offset	Size (in bytes)	Field	Notes
3	4	apfs_magic "APSB"	Volume Magic Number 0x41505342 = "APSB"
36	4	apfs_fs_index	Index in Volume Array
40	8	apfs_features	Features
48	8	apfs_readonly_compatible_features	Read-only Incompatible Features
56	8	apfs_incompatible_features	Incompatible Features
64	8	apfs_unmount_time	Timestamp when volume was last unmounted
72	8	apfs_fs_reserve_block_count	Block Pre-allocated for Volume (Default is none)
80	8	apfs_fs_quota_block_count	Maximum Block Allocated (Default is none)
88	8	apfs_fs_alloc_count	Number of blocks currently allocated
96	2	wrapped_crypto_state.t. wrapped_crypto_state.major_version	Key Encryption Metadata – Major Version
98	2	wrapped_crypto_state.t. wrapped_crypto_state.minor_version	Key Encryption Metadata – Minor Version
100	4	wrapped_crypto_state.t. wrapped_crypto_state.cpflds	Key Encryption Metadata – Encryption State Flags
104	4	wrapped_crypto_state.t. wrapped_crypto_state.persistent_class	Key Encryption Metadata – Protection Class
108	4	wrapped_crypto_state.t. wrapped_crypto_state.key_os_version	Key Encryption Metadata – Creator OS Version 0x39004313 = 19 C 57 – 19CS7 – Catalina 10.15.2
112	2	wrapped_crypto_state.t. wrapped_crypto_state.key_revision	Key Encryption Metadata – Key Version
114	2	wrapped_crypto_state.t. wrapped_crypto_state.key_len	Key Encryption Metadata – Key Size (0 for no Encryption)
N/A	0	wrapped_crypto_state.t. wrapped_crypto_state.persistent_key	Key Encryption Metadata – Wrapped Key No Key field is null, see key_len above
116	4	apfs_root_tree_oid_type	Type of Root File System Tree = B-Tree
120	4	apfs_extentref_tree_oid_type	Type of Extent Reference Tree = B-Tree, Physical
124	4	apfs_snap_meta_tree_oid_type	Type of Snapshot Metadata Tree = B-Tree, Physical
128	8	apfs_omap_oid	Physical Object ID (OID) of Object Map
136	8	apfs_root_tree_oid	Virtual Object ID (OID) of Root File System Tree
144	8	apfs_extentref_tree_oid	Physical Object ID (OID) of Extent Reference Tree
152	8	apfs_snap_meta_tree_oid	Virtual Object ID (OID) of Snapshot Metadata Tree
160	8	apfs_revert_to_xid	Transaction ID (XID) that volume will revert to
168	8	apfs_revert_to_sblock_oid	Virtual Object ID (OID) of Volume Superblock to revert to
176	8	apfs_next_obj_id	Next Object ID (OID)
184	8	apfs_num_files	Number of Regular Files
192	8	apfs_num_directories	Number of Directories
200	8	apfs_num_symlinks	Number of Symbolic Links
208	8	apfs_num_other_fsojects	Number of Other Files
216	8	apfs_num_snapshots	Number of Snapshots
224	8	apfs_total_blocks_allocated	Blocks Allocated by Volume
232	8	apfs_total_blocks_freed	Blocked Freed by Volume
240	16	apfs_vol_uuid	Volume UUID (diskutil info /dev/disk#s# [Volume])
256	8	apfs_last_mod_time	Last Modified Timestamp
264	8	apfs_fs_flags	Flags
272	32	apfs_modified_by_t.formatted_by.id[]	Format Program and Version
304	8	apfs_modified_by_t.formatted_by. timestamp	Format Timestamp
312	8	apfs_modified_by_t.formatted_by. last_xid	Format Transaction ID (XID)
320	32	apfs_modified_by_t.modified_by.id[]	Last Modified Program and Version
352	8	apfs_modified_by_t.modified_by. timestamp	Last Modified Timestamp
360	8	apfs_modified_by_t.modified_by. last_xid	Last Modified Transaction ID (XID)
368	336	apfs_modified_by_t.modified_by[1-7]	Array of apfs_modified_by_t[8]
704	256	apfs_volname	APFS Volume Name
960	4	apfs_next_doc_id	Next Document ID
964	2	apfs_role	APFS Role (None, System, Data, Preboot, VM, Recovery)
966	2	apfs_reserved	Reserved
976	8	apfs_root_to_xid	Transaction ID (XID) of Snapshot to Root
984	8	apfs_er_state_oid	Current State of Encryption/Decryption

B-Tree Node (btree_node_phys_t)

Offset	Size (in bytes)	Field	Notes
32	2	btn_flags	Flags (Leaf Node)
34	2	btn_level	Number of Child Levels below this Node
36	4	btn_nkeys	Number of Keys
40	2	btn_table_space.off	Offset to Table of Contents (after btree_node_phys_t)
42	2	btn_table_space.len	Length of Table of Contents
44	2	btn_freespace.off	Offset Key/Value Free Space
46	2	btn_freespace.len	Length of Key/Value Free Space
48	2	btn_key_free_list.off	Offset to Free Key Space
50	2	btn_key_free_list.len	Length of Free Key Space
52	2	btn_val_free_list.off	Offset to Free Value Space
54	2	btn_val_free_list.len	Length of Free Value Space

B-Tree Node – Table of Contents

Offset	Size (in bytes)	Field	Notes
TOC Entry + 2	2	key_offset	Key Offset
TOC Entry + 4	2	key_length	Key Length
TOC Entry + 6	2	value_offset	Value Offset
TOC Entry + 8	2	value_length	Value Length

B-Tree Node – File System Key

Offset	Size (in bytes)	Field
0	7	Object ID – Inode Number
7	1	Entry Kind
		0x30 – Inode
		0x60 – Data Stream
		0x40 – Xattr (2 byte Name Length + Variable Xattr Name)
		0x60 – File Extent (8 byte Logical Address

Value - Inode File Metadata

Offset	Size (in bytes)	Field	Notes
0	8	parent_id	Parent Inode Number
8	8	private_id	Inode Number
16	8	create_time	Create Timestamp
24	8	mod_time	Modification Timestamp
32	8	change_time	Change Timestamp
40	8	access_time	Access Timestamp
48	8	internal_flags	Internal Flags
56	4	nchildren or nlink	Children or Links
60	4	default_protection_class	Default Protection Class
64	4	write_generation_counter	Write Generation Counter
68	4	bsd_flags	BSD Flags
72	4	owner	Owner
76	4	group	Group
80	2	mode	File Mode
82	2	pad1	Pad1
84	8	pad2	Pad2
92	2	xf_num_exts	Number of Extended Fields
94	2	xf_used_data	Extended Fields Data Used
96	x_field_t[] = 4 bytes Each	Extended Field: x_type (1 byte), x_flags (1 byte), x_size (2 bytes)	
96	4		EXAMPLE EXTENDED FIELD: 0x04 = 4, 0x02 (Do Not Copy), 0x1100 = 17 (File Name)
100	4		EXAMPLE EXTENDED FIELD: 0x08 = 8, 0x20 (System Field), 0x2800 = 40 (Data Stream)
104	{17}	File Name	smudge_yoda.jpeg (w/1 padding bytes 0x00), 17 total bytes
120	{40}	Data Stream (Size: First 8 bytes, Allocated: Next 8 bytes)	0x0000000000000000 – 7 unused bytes Size: 0x261C020000000000 = 138278 bytes Allocated: 0x0020020000000000 = 139264

Value – Inode File Extent

Offset	Size (in bytes)	Field
0	8	File Size
8	8	Physical Block Location
16	8	Crypto ID

APFS Format References:

- Apple File System Reference (Apple Developer Documentation)
- 2019-02-07

APFS is Little Endian & 64-bit

SANS FOR518 Reference Sheet	
By: Sarah Edwards Twitter: @iamevltwin Email: oompa@csh.rit.edu	
Directory Commands	
cd ..	Change Directory...up one directory (../. – two directories up)
cd	Change Directory...to /var/log
/var/log	
cd ~	Change Directory...to your home directory
cd /	Change Directory...to the root directory
ls	List Directory (Short Listing)
ls -l	List Directory (Long Listing)
ls -a	List Directory items...including hidden items (files beginning with “.")
ls -lh	List Directory items...with human readable sizes
ls -R	List Directory items...recursively
open .	Open Current Directory
pwd	Print Working Directory
mkdir	Create a Directory
rmdir	Remove a Directory
rm -r	Remove a Directory (and its contents)
.	Current Directory
..	Parent Directory
File Commands	
pico <filename>	Open a file in a simple text editor (q – to quit editor)
xxd <filename>	Open a file in a hex editor
open <filename>	Opens a file in the default program
open -a <programname> <filename>	Opens a file in a specified program
cat <filename>	Concatenate a file to the terminal screen
<command> more	Pipe command output to more to show contents screen by screen
<command> less	Pipe command output to less to show contents screen by screen (and be able to go back and forth)
rm <filename>	Remove File
cp <filename> <newfilename>	Copy File
mv <filename> <newfilename>	Move File
<command> > <filename>	Redirect command output to a file
<command> >> <filename>	Append command output to a file
touch <filename>	Create an empty file
head <filename>	Show first 10 lines of a file
tail <filename>	Show last 10 lines of a file (-f to watch appended input)
strings <filename>	Show the strings of a file
exiftool <filename>	Show the exif/metadata of the file
plutil -p <propertylist>	Print the contents of a property list
file <filename>	Show a file signature type
grep -i <searchterm> <filename>	Search for term within a file (case-insensitive)
python <file>.py	Execute a Python program
Miscellaneous Commands	
sudo <command>	Execute program as another user (default is root user)
sudo -s	Open a privileged shell
su -	Substitute User to root
whoami / id	Display Effective User ID / Show UID/GID Info
history	Command History
man <command>	Command Manual (q – to exit manual)
Terminal Shortcuts	
Control + A	Jump to beginning of line
Control + E	Jump to end of line
Tab	Tab Completion
Control + C	Kill Current Command
Command + K or Control + L	Clear Screen (or clear command)
Command + T	New Terminal Tab
Command + W	Close Terminal Tab
Command +/-	Increase or Decrease Terminal Font Size
Option + Left/Right Arrow	Move back/forth by word
Option + Click in Command Line	Put command line cursor where mouse cursor is.
Generic Tool Compilation and Installation	
tar -xvf <archive>.tar.gz	
./configure	
make	
sudo make install	

Live Response	
date	Local System Time (-u for UTC)
hostname	System Hostname
uname -a	OS & Architecture Information
sw_vers	macOS Version & Build
netstat -anf inet or netstat -an	Active Network Connections
lsof -i	Active Network Connections (by process)
netstat -rn	Routing Table
arp -an ndp -an	ARP Table (IPv4 IPv6)
ifconfig	Network Interface Configuration
lsof	List Open Files
who -a, w	List Logged On Users
last	List user logins
ps aux	List Processes
system_profiler -xml -detaillevel full > file.spdx	System Profiler (XML, Full Detail Level), open with System Information.app
Disk & Partitions	
/dev/	Device Directory
diskutil list	List Connected Disks
diskutil info <disk>	Disk Information (use Disks /dev/disk#, disk#, or partitions /dev/disk#s#)
diskutil cs ap list	List partitions using CoreStorage (cs) or APFS Containers (ap)
gpt -r show [-l]	List partitions using GUID Partition Table Format (-l to show label rather than GUID) – 10.13+ SIP must be disabled.
csrutil disable enable	Disable/Enable SIP, must reboot into Recovery Mode (Reboot, Cmd+Option+R)
mmfs <diskimage>	Display partitions using The Sleuth Kit
hdiutil imageinfo *.dmg	Disk Image Information including Partition Data
Keychains	
security list-keychains	List Keychains on a system for a logged in user
security dump-keychains -d <keychain>	Dump contents of a Keychain
Extended Attributes	
xattr -xl <file>	Show Extended Attributes of a file
xattr -p <attribute name> <file> xxd -r -p	Extract embedded binary property list from extended attribute.
>output file.plist	
istat /dev/disk# <CNID>	Use The Sleuth Kit to view file information including extended attributes.
icat /dev/disk# <CNID>-<TSK Attribute Number>	View a specific extended attribute using The Sleuth Kit
Log Analysis	
bzcat system.log.1.bz2	Create a “all-in-one” system.log file. Can also be used with
system.log.0.bz2 >> system_all.log	gzcat for Gzip compressed log files.
cat system.log >> system_all.log	
syslog -f <file> -d <directory>	View ASL File or Directory of ASL files
syslog -T utc -F raw -d	Output ASL files the /var/log/asl directory and output in raw format with UTC timestamps.
/var/log/asl	
praudit -xn /var/audit/*	View audit logs in XML format without user/group resolution.
sudo log collect	Create a logarchive bundle on live system, root required
log show	View logs in logarchive bundle (use with --predicate to filter)
log stream	View live logs (use with --predicate to filter)
Time Machine	
tmutil uniquesize <machinedirectory_path>/*	Show the unique sizes of each snapshot
tmutil calculatedrift	Show the size changes (added/removed/changed) between each snapshot.
<machinedirectory_path>	
tmutil compare <snapshotdirectory1>	Compare the file changes
<snapshotdirectory2>	(added/removed/changed) between two snapshots..
Memory Analysis & Encrypted Containers	
vol.py --profile=<profile> -f <memory image>	Volatility Usage
<plugin>	
hdiutil attach -readonly -nomount -stdinpass	Mount a FileVault volume using a
filevault2image.dmg	password
security unlock-keychain FileVaultMaster.keychain	Access and mount a FileVault volume
diskutil corestorage unlockvolume <UUID> - recoverykeychain FileVaultMaster.keychain	using a master password
diskutil corestorage unlockvolume <UUID> -passphrase	Mount a FileVault volume using the
<recovery key>	Recovery Key
hdiutil attach -readonly -nomount -stdinpass	Mount an Encrypted DMG File
sekretestuff USB.dmg	
strings <MemoryImage> sort -u > dictionary.txt	Create a dictionary file
Spotlight	
mdls <file>	List the Spotlight metadata for a file
mdfind “<attribute_name> == *”	Find files based on a specific metadata query
mdfind -onlyin /Volumes/mounted_disk	Find files only in a certain directory or mounted image.
mdimport -X -A	Print a list of attributes that can be queried.
Disk Arbitration	
sudo launchctl load /System/Library/LaunchDaemons/com.apple.diskarbitrationond.plist	Enable
sudo launchctl unload /System/Library/LaunchDaemons/com.apple.diskarbitrationond.plist	Disable
ps auxw grep diskarbitrationd	Determine Status

Image Mount & Eject

APFS with xmount (xmount v.0.7.*)\$ sudo mkdir /Volumes/galaga_image/\$ sudo mkdir /Volumes/galaga_mounted/\$ sudo xmount --in ewf ~/FOR518/galaga.E01 --out dmg /Volumes/galaga_image/\$ hdiutil attach -nomount /Volumes/galaga_image/galaga.dmg\$ sudo mount apfs -o rdonly,noexec,noowners /dev/disk# /Volumes/galaga_mounted/

HFS+ Method 1 – xmount (xmount v.0.7.*)\$ mkdir /Volumes/dademurphy_image/\$ mkdir /Volumes/dademurphy_mounted/\$ sudo xmount --in ewf ~/FOR518/dademurphy.E01 --out dmg /Volumes/dademurphy_image/\$ hdiutil attach -nomount /Volumes/dademurphy_image/dademurphy.dmg\$ mount hfs -j -o rdonly,noexec,noowners /dev/disk# /Volumes/dademurphy_mounted/

Eject Disk\$ diskutil list\$ diskutil eject /dev/disk#\$ mount\$ sudo umount /Volumes/galaga_image/

Timestamp Formats

APFS64-bit - Number of Seconds from 1/1/197000:00:00 UTC

HFS+/MacOS32-bit - Number of seconds from 1/1/190400:00:00 UTC

UNIX Epoch32-bit - Number of seconds from 1/1/197000:00:00 UTC

Mac Epoch/Mac Absolute/Cocoa/WebKit32-bit - Number of seconds from 1/1/200100:00:00 UTC

Property List Dates in XcodeLocal Host System Time

FOR518 - Mac and iOS Forensic Analysis & Incident Response - for518.com



SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

Number of 512-byte Blocks Used

nibble:/ sledwards\$ ls -la

total 1014190

drwxr-xr-x@ 41 root wheel 1462 Feb 16 21:14 .

drwxr-xr-x@ 41 root wheel 1462 Feb 16 21:14 ..

d--x--x--x+ 8 root wheel 272 Nov 5 01:11 .DocumentRevisions-V100

d-wx-wx-wt 2 root wheel 68 Nov 4 21:05 .Trashes

-rw-r--r--+ 1 sledwards admin 312 Mar 9 2013 .apdisk

srwxrwxrwx 1 root wheel 0 Feb 15 21:29 .dbfsevents

lrwxr-xr-x@ 1 root wheel 11 Sep 23 08:47 etc -> private/etc

-rwxr-xr-x@ 1 root wheel 8393032 Sep 29 22:39 mach_kernel

Entry TypePermissionsxattr/ACLsHard Link CountOwner NameGroup NameFile Size(bytes)Last ModifiedTimestampFile / Directory

GPT Reference

GPT Header

OffsetSize (bytes)Field

08Signature (EFI PART)

84Revision (1.0)

124Size of Header (bytes)

164Header CRC32

204Reserved

248LBA of GPT Header

328LBA of Backup GPT Header

408First Usable LBA

488Last Usable LBA

5616Disk GUID

728Starting LBA of GUID Partition Table (Little Endian)

804Number of Partition Entries Available (Little Endian)

844Size of Partition Entry

884Partition Entry Array CRC32

92RestReserved

GPT Table Entry

OffsetSize (bytes)Field

016Partition Type GUID

1616Unique Partition GUID

328Starting LBA (Little Endian)

408Ending LBA (Little Endian)

488Attributes

5672Partition Name

128RestReserved

TypeCommon GPT Partition GUIDs

EFI System PartitionC12A7328-F81F-11D2-BA4B-00A0C93EC93B

HFS+ Partition48465300-0000-11AA-AA11-00306543ECAC

Apple Boot Partition426F6F74-0000-11AA-AA11-00306543ECAC

Apple CoreStorage (possible FileVault or Fusion Drive)53746F72-6167-11AA-AA11-00306543ECAC

APFS Partition7C3457EF-0000-11AA-AA11-00306543ECAC

Basic Data Partition (Boot Camp)EBD0A0A2-B9E5-4433-87C0-68B6B72699C7