HFS+ 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

Volume Header

Offset	Size (in bytes)	Data
0	2	Signature
2	2	Version
4	4	Attributes
8	4	Last Mounted Version
12	4	Journal Info Block
16	4	Create Date
20	4	Modify Date
24	4	Backup Date
28	4	Checked Date
32	4	File Count
36	4	Folder Count
40	4	Block Size
44	4	Total Blocks
48	4	Free Blocks
52	4	Next Allocation
56	4	rsrc Clump Size
60	4	Data Clump Size
64	4	Next Catalog ID
68	4	Write Count
72	8	Encoding Bitmap
80	4	Finder Info Array [0]
84	4	Finder Info Array [1]
88	4	Finder Info Array [2]
92	4	Finder Info Array [3]
96	4	Finder Info Array [4]
100	4	Finder Info Array [5]
104	4	Finder Info Array [6]
108	4	Finder Info Array [7]
112	80	Allocation File Size & Location
192	80	Extents File Size & Location
272	80	Catalog File Size & Location
352	80	Attributes File Size & Location
432	80	Startup File Size & Location

Location	1024 bytes from beginning of the volume
Size	512 bytes
Alternate VH	1024 bytes from the end of the volume

Special File Size & Location / File Extents [80 bytes]

Offset	Size (in bytes)	Data
0	8	Logical Size
8	4	Clump Size
12	4	Total Blocks
16	4	Extent 1 – Start Block
20	4	Extent 1 – Block Count
24	4	Extent 2 – Start Block
28	4	Extent 2 – Block Count
32	4	Extent 3 – Start Block
36	4	Extent 3 – Block Count
40	4	Extent 4 – Start Block
44	4	Extent 4 – Block Count
48	4	Extent 5 – Start Block
52	4	Extent 5 – Block Count
56	4	Extent 6 – Start Block
60	4	Extent 6 – Block Count
64	4	Extent 7 – Start Block
68	4	Extent 7 – Block Count
72	4	Extent 8 – Start Block
76	4	Extent 8 – Block Count

Catalog Node ID Reservations

CNID	Reservation
1	Root Parent
2	Root Folder
3	Extents Overflow File
4	Catalog File
5	Bad Block File
6	Allocation File
7	Startup File
8	Attributes File
14	Repair Catalog File
15	Bogus Extent File
16	First User Catalog Node

HFS+ Special File Extraction from Image File using The Sleuth Kit

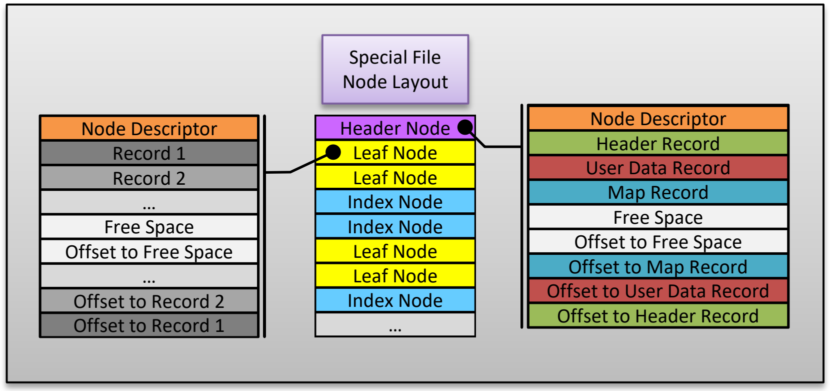
```
icat –f hfs —o <partitionoffset>
*.dd <inode> > special_file
```

HFS+ File System Format References & Resources:

- Apple Tech Note 1150 – Available at for518.com/tn1150
- The Sleuth Kit Source – Available at for518.com/tskhfs
- *Mac OS X Internals: A Systems Approach* by Amit Singh – Chapter 12
- *Mac OS X and iOS Internals: To the Apple's Core* by Jonathan Levin – Chapter 16
- Apple Open Source – for518.com/hfsformat

B-Tree Nodes

- ***Four*** types of B-Tree Nodes
- Only ***one*** Header Node per B-Tree
- Each B-Tree Specifies its size in the ***Node Size*** field of the Header Record



Node Descriptor [14 bytes]

Offset	Size (in bytes)	Field
0	4	Forward Link
4	4	Backward Link
8	1	Kind: 0xFF – Leaf Node (-1) 0x00 – Index Node (0) 0x01 – Header Node (1) 0x02 – Map Node (2)
9	1	Height
10	2	Number of Records
12	2	Reserved

Header Node
Header Record
User Data Record
Map Record

Map Node
Map Records* **See Allocation Table Format*

Index Node
Pointer Records

Size (in bytes)	Field
2	Key Length
Variable	Key (For Catalog File: Parent CNID + HFSUniStr255)
4	Node Number

Leaf Node
Data Records

Size (in bytes)	Field
2	Key Length
4	Parent CNID
Variable	Data Size [2 bytes] + Data *(Empty String 0x0000 in thread records)* *(+padding byte if key length is odd)*

Header Record [46 bytes]

Offset	Size (in bytes)	Field
0	2	Tree Depth
2	4	Root Node
6	4	Leaf Records
10	4	First Leaf Node
14	4	Last Leaf Node
18	2	Node Size
20	2	Max Key Length
22	4	Total Nodes
26	4	Free Nodes
30	2	Reserved
32	4	Clump Size
36	1	B-tree Type: 0x00 – HFS B-Tree (0) 0x80 – User B-Tree (128) 0xFF – Reserved (255)
37	1	Key Compare Type: 0xCF or 0xC7 - Case-insensitive 0xBC - Case-sensitive 0x00 - *Unknown*
38	4	Attributes:
42	4	Reserved [16] (64 bytes)

HFS+ Data is Big Endian
GPT is Little Endian

Catalog File

Catalog File Key

Size	Field
2	Key Length
4	Parent CNID (or CNID of file/folder for thread records)
Variable HFSUniStr255	Node Name (File or Folder Name) 2 Byte Length + Variable Unicode Name (<=255)

Catalog File/Folder Record [88 or 248 bytes]

Size (in bytes)	Field
2	Record Type (0x0001) – Folder Record (0x0002) – File Record
2	Flags
4	Valence (File Records - Reserved)
4	File or Folder ID (CNID)
4	Create Date
4	Content Modification Date
4	Attribute Modification Date
4	Access Date
4	Backup Date
HFSPlusBSDInfo [16 Bytes]	Permissions
FolderInfo or FileInfo [16 Bytes]	User Information
ExtendedFolder or FileInfo [16 Bytes]	Finder Information
4	Text Encoding
4	Reserved
Additional Fields for File Record – See "File Extents" Table	
HFSPlusForkData [80 Bytes]	Data Fork
HFSPlusForkData [80 Bytes]	Resource Fork

Catalog Thread Record

Size	Field
2 Bytes	Record Type (0x0003) – Folder Thread Record (0x0004) – File Thread Record
2 Bytes	Reserved
4 Bytes	Parent ID (CNID)
HFSUniStr255	Node Name (File or Folder Name) 2 Byte Length + Variable <=255 Unicode Name

Size (in bytes)	HFSPlusBSDInfo
4	Owner ID
4	Group ID
1	Admin Flags
1	Owner Flags
2	File Mode
4	iNode Number or Link Count or Raw Device

Attributes File

Attributes Key

Size (in bytes)	Field
2	Key Length
2	Pad
4	File ID (CNID)
4	Start Block
2	Attribute Name Length
Variable	Attribute Name

Attributes Record

Size (in bytes)	Field
4	Record Type (0x00000010) Inline Data Attribute
8	Reserved
4	Attribute Size
Variable	Attribute Data

Extents Overflow File

Extents Overflow Key [12 bytes]

Size (in bytes)	Field
2	Key Length
1	Fork Type 0x00 - Data 0xFF - Resource
1	Pad
4	File ID (CNID)
4	Start Block

Extents Overflow Record

Size (in bytes)	Field (For Each Eight Extents)
4	Start Block
4	Block Count

Allocation File (with Examples)

1 bit per allocation block (512 bytes), 8 blocks per byte (4,096)
Most Significant Bit – Status of block with lowest number
Least Significant Bit – Status of block with highest number

Hex	Binary	Allocation
0x00	00000000	No Blocks Allocated
0xFF	11111111	All Blocks Allocated
0x1F	00011111	Lowest three blocks are unallocated
0x80	10000000	Lowest block is allocated
0x07	00000111	Highest three blocks are allocated
0xF0	11110000	Highest four blocks are unallocated

Updated: 042018

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 /var/log`	Change Directory…to /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 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.spx`	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)
`mmls <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 >output_file.plist`	Extract embedded binary property list from extended attribute.
`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 system.log.0.bz2 >> system_all.log`
`cat system.log >> system_all.log`
	Create a “all-in-one” system.log file. Can also be used with gzcat for Gzip compressed log files.

`syslog –f <file> | –d <directory>`	View ASL File or Directory of ASL files
`syslog –T utc –F raw –d /var/log/asl`	Output ASL files the /var/log/asl directory and output in raw format with UTC timestamps.
`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 <machinedirectory_path>`	Show the size changes (added/removed/changed) between each snapshot.
`tmutil compare <snapshotdirectory1> <snapshotdirectory2>`	Compare the file changes (added/removed/changed) between two snapshots..

Memory Analysis & Encrypted Containers

`vol.py --profile=<profile> -f <memory image> <plugin>`	Volatility Usage
`hdiutil attach –readonly –nomount –stdinpass filevault2image.dmg`	Mount a FileVault volume using a password

`security unlock-keychain FileVaultMaster.keychain`
`diskutil corestorage unlockvolume <UUID> –recoverykeychain FileVaultMaster.keychain`
	Access and mount a FileVault volume using a master password

`diskutil corestorage unlockvolume <UUID> -passphrase <recovery key>`	Mount a FileVault volume using the Recovery Key
`hdiutil attach -readonly -nomount -stdinpass sekretstuff_USB.dmg`	Mount an Encrypted DMG File
`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.diskarbitrationd.plist`	Enable
`sudo launchctl unload /System/Library/LaunchDaemons/com.apple.diskarbitrationd.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/
```

HFS+ Method 2 -
mountewf

```
$ mkdir /Volumes/dademurphy_image/
$ mkdir /Volumes/dademurphy_mounted/
$ ewfmount ~/FOR518/dademurphy.E01 /Volumes/dademurphy_image/
$ ln –s /Volumes/dademurphy_image/ewf1 ~/FOR518/dadeimage.dmg
$ hdiutil attach -nomount ~/FOR518/dadeimage.dmg
$ mount_hfs -j -o rdonly,noexec,noowners /dev/disk# /Volumes/dademurphy_mounted/
```

Eject Disk

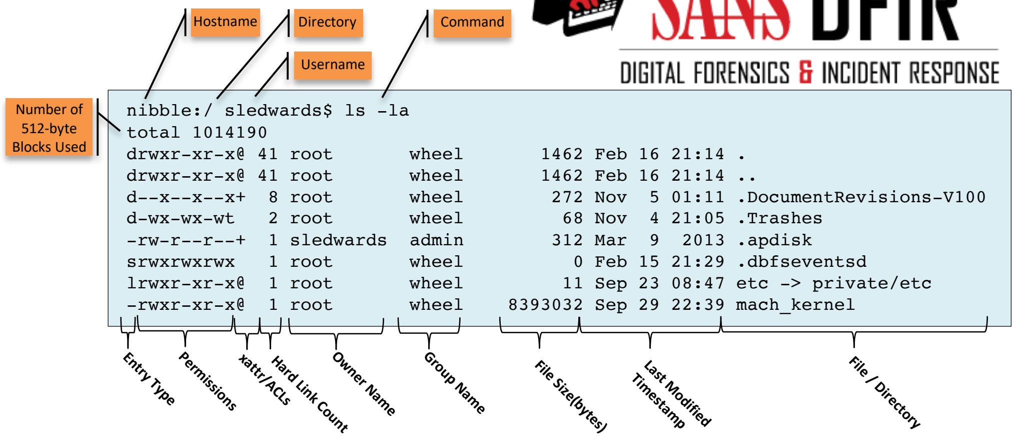
```
$ diskutil list
$ diskutil eject /dev/disk#
$ mount
$ sudo umount /Volumes/galaga_image/
```

Timestamp Formats

HFS+/MacOS	32-bit - Number of seconds from 1/1/1904 00:00:00 UTC
UNIX Epoch	32-bit - Number of seconds from 1/1/1970 00:00:00 UTC
Mac Epoch/Mac Absolute/Cocoa/WebKit	32-bit - Number of seconds from 1/1/2001 00:00:00 UTC
Property List Dates in Xcode	Local Host System Time

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

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE



```
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 .dbfseventsd
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
```

GPT Reference

GPT Header

Offset	Size (bytes)	Field
0	8	Signature (EFI PART)
8	4	Revision (1.0)
12	4	Size of Header (bytes)
16	4	Header CRC32
20	4	Reserved
24	8	LBA of GPT Header
32	8	LBA of Backup GPT Header
40	8	First Usable LBA
48	8	Last Usable LBA
56	16	Disk GUID
72	8	Starting LBA of GUID Partition Table (Little Endian)
80	4	Number of Partition Entries Available (Little Endian)
84	4	Size of Partition Entry
88	4	Partition Entry Array CRC32
92	Rest	Reserved

GPT Table Entry

Offset	Size (bytes)	Field
0	16	Partition Type GUID
16	16	Unique Partition GUID
32	8	Starting LBA (Little Endian)
40	8	Ending LBA (Little Endian)
48	8	Attributes
56	72	Partition Name
128	Rest	Reserved

Type	Common GPT Partition GUIDs
EFI System Partition	C12A7328-F81F-11D2-BA4B-00A0C93EC93B
HFS+ Partition	48465300-0000-11AA-AA11-00306543ECAC
Apple Boot Partition	426F6F74-0000-11AA-AA11-00306543ECAC
Apple CoreStorage (possible FileVault or Fusion Drive)	53746F72-6167-11AA-AA11-00306543ECAC
APFS Partition	7C3457EF-0000-11AA-AA11-00306543ECAC
Basic Data Partition (Boot Camp)	EBD0A0A2-B9E5-4433-87C0-68B6B72699C7