

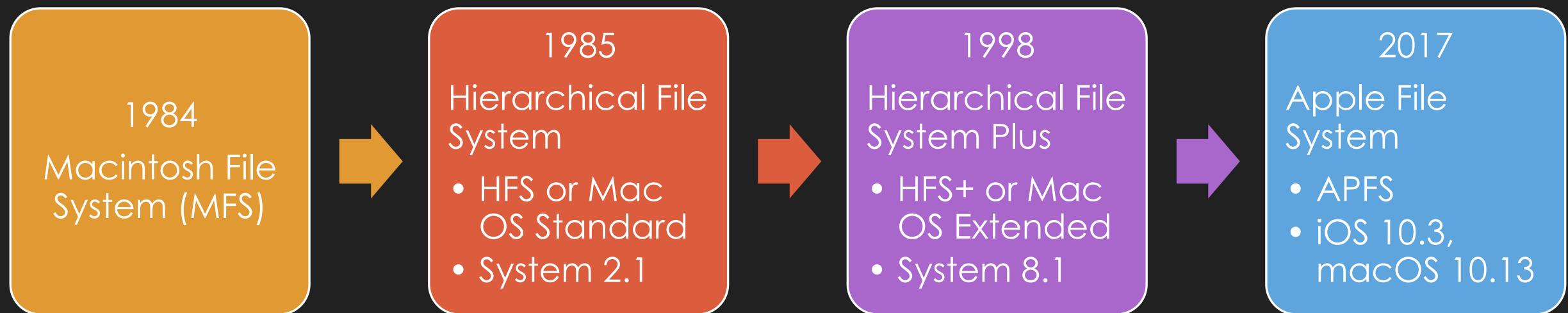
# Getting Saucy with APFS!

The State of Apple's New File System

Sarah Edwards | @iamevtwin | oompa@csh.rit.edu | mac4n6.com

# Apple File System History

# Apple File Systems – Let's Reminisce



# APFS Timeline

June 26,  
2016

- Announced  
at WWDC

September  
20, 2016

- macOS 10.12
- “Experimental  
Support”

March 27,  
2017

- iOS 10.3
- tvOS 10.2
- watchOS 3.2

September  
25, 2017

- macOS 10.13

# APFS Gist

- New default file system for iOS 10.3, macOS 10.13 (with caveats), watchOS 3.2, & tvOS 10.2
  - Some basic APFS functionality available with Sierra (10.12)
  - iOS upgrade to APFS transparently in 10.3 update
  - Fusion Drives & HDDs not automatically converted to APFS
  - High Sierra (10.13) install performs in-place upgrade to APFS from HFS+
- 64-bit File System
- Optimized for Flash/SSD Drives
  - Can be used on HDDs
  - Internal & External - Bootable & Data Drives
  - Can be used across multiple drives (ie: RAID-ish, CoreStorage-ish)
- Nanosecond Timestamp Granularity
- Implements TRIM

# Acquisition

# iOS Acquisition

```
-bash-3.2# uname -a
Darwin miPhoneX 17.2.0 Darwin Kernel Version 17.2.0: Fri Sep 29 18:14:51 PDT 2017; root:xnu-4570.20.62~4/
RELEASE_ARM64_T8015 iPhone10,6
[bash-3.2# cat /etc/fstab
/dev/disk0s1s1 / apfs ro 0 1
/dev/disk0s1s2 /private/var apfs rw,nosuid,nodev 0 2
/dev/disk0s1s3 /private/var/wireless/baseband_data apfs rw,nosuid,nodev,nobrowse 0 2
/dev/disk0s1s4 /private/var/hardware apfs rw,nosuid,nodev,nobrowse 0 2]
```

```
[bash-3.2# xxd /dev/disk0
xxd: /dev/disk0: Operation not permitted
[bash-3.2# xxd /dev/disk0s1s1
xxd: /dev/disk0s1s1: Operation not permitted
[bash-3.2# xxd /dev/disk0s1s2
xxd: /dev/disk0s1s2: Operation not permitted
```

- Assumes physical/jailbroken access
- Disk Layout: /etc/fstab
- 'dd' system partition imaging limited by permissions = "Operation not permitted"
- "Logical/Physical" Acquisition – Tar bundle of logical files from physical partitions
- <https://www.mac4n6.com/blog/2018/1/7/ios-imaging-on-the-cheap-part-deux-for-ios-10-11>

# macOS Acquisition

- macOS
  - Turn off SIP (System Integrity Protection)
  - Reboot into Recovery Mode and run '`csrutil disable`'
  - Can re-enable after imaging by rebooting into recovery mode and '`csrutil enable`'
  - SIP Status – '`csrutil status`'
- Encryption
  - Password or Recovery Key Required
- Physical Disk (`/dev/disk0`) - For single drive APFS implementation
- Logical Container (`/dev/disk1`) - For systems using spanning data across multiple physical disks (Converted Fusion drives, multiple SSDs, etc.)
- Tools
  - dd/dcfldd/dc3dd
  - Access Data FTK CLI Imager
  - BlackBag MacQuisiton
  - Sumuri Recon Imager

# BlackBag MacQuisition

MacQuisition™

The screenshot shows the MacQuisition software interface. On the left, a sidebar lists available storage devices:

- Physical Memory (16.0 GB)
- disk0 - APPLE SSD AP1024J (931.8 GB) - PCI-Express
  - EFI (300.0 MB) - disk0s1 - EFI
  - [APFS Container - disk1 contains the APFS volumes] - (931.5 GB) - disk0s2
- disk1 - APFS Container (synthesized) (931.5 GB) - Virtual - data from disk0s2
  - HighSierra (931.5 GB) - disk1s1 - [ENCRYPTED APFS (unlocked)] - select the APFS container's disk(s) to image
  - Preboot (931.5 GB) - disk1s2 - APFS - select the APFS container's disk(s) to image
  - VM (931.5 GB, 1.0 GB used) - disk1s4 - APFS - select the APFS container's disk(s) to image
  - Recovery (931.5 GB) - disk1s3 - APFS - select the APFS container's disk(s) to image

On the right, imaging settings are configured:

- Format: Raw
- Segment Size: No Segments
- Hashes:
  - MD5
  - SHA1
  - SHA256

Destination(s):

+ -

Image Device

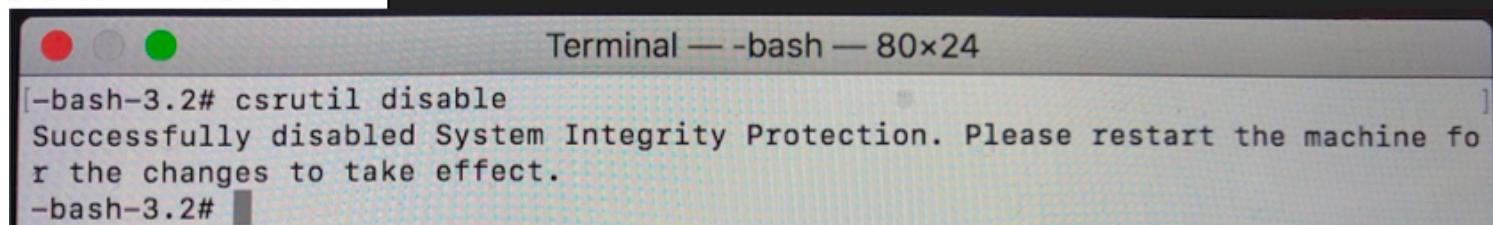
# SIP Acquisition Errors

```
[MacBook-Pro:~ oompa$ 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 HighSierra    680.2 GB  disk1s1
 2:           APFS Volume Preboot     27.4 MB   disk1s2
 3:           APFS Volume Recovery    517.8 MB  disk1s3
 4:           APFS Volume VM         1.1 GB   disk1s4

[MacBook-Pro:~ oompa$ dd if=/dev/disk0 of=/tmp/test.dd
dd: /dev/disk0: Operation not permitted
[MacBook-Pro:~ oompa$ sudo !!
sudo dd if=/dev/disk0 of=/tmp/test.dd
>Password:
dd: /dev/disk0: Operation not permitted
[MacBook-Pro:~ oompa$ sudo dd if=/dev/disk1 of=/tmp/test.dd
dd: /dev/disk1: Operation not permitted
[MacBook-Pro:~ oompa$ sudo dd if=/dev/disk1s1 of=/tmp/test.dd
dd: /dev/disk1s1: Operation not permitted
```

- Devices not available with SIP enabled
  - Even with root!
- Disable SIP using csrutil in Recover Mode
  - Reboot, CMD+R
  - csrutil disable



# macOS Disks & Partitions

## diskutil list

```
[Sarahs-MBP-6:~ oompa$ 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 HighSierra        650.4 GB  disk1s1
2: APFS Volume Preboot          27.4 MB   disk1s2
3: APFS Volume Recovery          517.8 MB  disk1s3
4: APFS Volume VM                4.3 GB   disk1s4
```

# GPT Partitions

`gpt -r show /dev/disk0`

- EFI Partition GUID - C12A7328-F81F-11D2-BA4B-00A0C93EC93B
- APFS Partition GUID - 7C3457EF-0000-11AA-AA11-00306543ECAC
- FYI: gpt command can only be run with SIP disabled

```
[Sarahs-MBP-6:~ oompa$ sudo gpt -r show /dev/disk0
      start      size  index  contents
          0          1
                      1      PMBR
          1          1
                      1      Pri GPT header
          2          4
                      2      Pri GPT table
          6        76800      1  GPT part - C12A7328-F81F-11D2-BA4B-00A0C93EC93B
    76806  244199454      2  GPT part - 7C3457EF-0000-11AA-AA11-00306543ECAC
244276260          4
244276264          1      Sec GPT table
244276264          1      Sec GPT header]
```

# APFS Containers diskutil ap list

APFS Container

Container Disk

Physical Store

## Volumes

- Roles (“None” (User/OS), PreBoot, Recovery, VM)
- Encryption Status - “HighSierra” uses FileVault

```
Sarahs-MBP-6:~ oompa$ diskutil ap list
APFS Containers (3 found)

+-- Container disk1 7AB09481-C4B7-4A1D-B551-6ADAA5D8ED24
=====
APFS Container Reference:      disk1
Size (Capacity Ceiling):     1000240963584 B (1.0 TB)
Minimum Size:                 1000655269888 B (1.0 TB)
Capacity In Use By Volumes:   656089354240 B (656.1 GB) (65.6% used)
Capacity Not Allocated:       344151609344 B (344.2 GB) (34.4% free)

+--< Physical Store disk0s2 FC80FCEE-E44F-4F25-BA57-F303E87FB108
-----
APFS Physical Store Disk:    disk0s2
Size:                         1000240963584 B (1.0 TB)

+--> Volume disk1s1 1D19162C-518C-3A34-A02C-2D428A4BC44E
-----
APFS Volume Disk (Role):     disk1s1 (No specific role)
Name:                          HighSierra (Case-insensitive)
Mount Point:                  /
Capacity Consumed:           651046686720 B (651.0 GB)
FileVault:                     Yes (Unlocked)

+--> Volume disk1s2 670CBB6D-1FE7-446D-A76A-C549A159F34F
-----
APFS Volume Disk (Role):     disk1s2 (Preboot)
Name:                          Preboot (Case-insensitive)
Mount Point:                  Not Mounted
Capacity Consumed:            27398144 B (27.4 MB)
FileVault:                     No

+--> Volume disk1s3 30817573-A0CE-4CF7-AC2B-D7C7E921B424
-----
APFS Volume Disk (Role):     disk1s3 (Recovery)
Name:                          Recovery (Case-insensitive)
Mount Point:                  Not Mounted
Capacity Consumed:            517754880 B (517.8 MB)
FileVault:                     No

+--> Volume disk1s4 38B6B6EE-C683-4FF1-8100-EE6C1A551668
-----
APFS Volume Disk (Role):     disk1s4 (VM)
Name:                          VM (Case-insensitive)
Mount Point:                  /private/var/vm
Capacity Consumed:            4295012352 B (4.3 GB)
FileVault:                     No
```

# Pooled Storage or “Space Sharing”

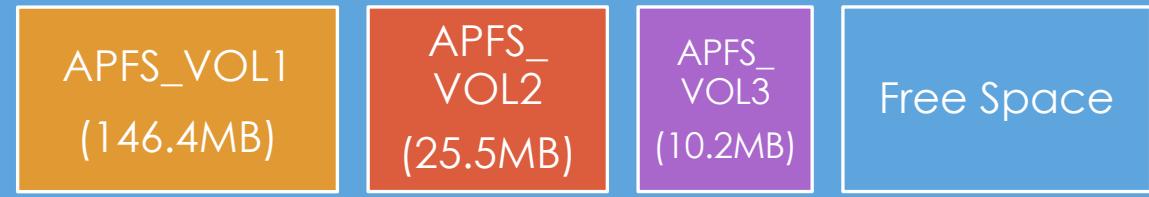
▼	APFS_VOL1		146.4 MB
	GoogleEarthProMac-Intel.dmg		73.4 MB
	WhatsApp.dmg		72.1 MB
▼	APFS_VOL2		25.4 MB
	Technical Note TN1150- HFS Plus Volume Format		23.2 MB
▼	APFS_VOL3		10.1 MB
	fistbump.gif		6.7 MB
	nails.gif		644 KB
	sleepy.gif		995 KB
	wiggle.gif		875 KB

```
[Sarahs-MBP-6:~ oompa$ df -h /Volumes/APFS_VOL1
Filesystem      Size   Used  Avail Capacity iused          ifree %iused  Mounted on
/dev/disk5s1  7.2Gi  140Mi  7.0Gi    2%     79 9223372036854775728    0%  /Volumes/APFS_VOL1
[Sarahs-MBP-6:~ oompa$ df -h /Volumes/APFS_VOL2
Filesystem      Size   Used  Avail Capacity iused          ifree %iused  Mounted on
/dev/disk5s2  7.2Gi  24Mi  7.0Gi    1%     100 9223372036854775707    0%  /Volumes/APFS_VOL2
[Sarahs-MBP-6:~ oompa$ df -h /Volumes/APFS_VOL3
Filesystem      Size   Used  Avail Capacity iused          ifree %iused  Mounted on
/dev/disk5s3  7.2Gi  9.7Mi  7.0Gi    1%     88 9223372036854775719    0%  /Volumes/APFS_VOL3
```

# “Space Sharing”

- APFS Containers may contain multiple volumes
- Disk space is shared amongst other volumes

APFS Container (8GB)



```
/dev/disk2 (external, physical):
#:          TYPE NAME               SIZE    IDENTIFIER
0:  GUID_partition_scheme          *7.9 GB   disk2
1:          EFI   EFI                209.7 MB  disk2s1
2:          Apple_APFS Container disk3        7.7 GB   disk2s2

/dev/disk3 (synthesized):
#:          TYPE NAME               SIZE    IDENTIFIER
0:  APFS Container Scheme -          +7.7 GB   disk3
                                         Physical Store disk2s2
1:          APFS Volume APFS_VOL1      146.4 MB  disk3s1
2:          APFS Volume APFS_VOL2      25.5 MB   disk3s2
3:          APFS Volume APFS_VOL3      10.2 MB   disk3s3
```

```
[Sarahs-MBP-6:~ compa$ diskutil ap list disk3
|
+-- Container disk3 387F97D2-84FA-46A1-9DD6-042E9C6124FD
=====
APFS Container Reference:      disk3
Size (Capacity Ceiling):     7709089792 B (7.7 GB)
Minimum Size:                 228675584 B (228.7 MB)
Capacity In Use By Volumes:  207392768 B (207.4 MB) (2.7% used)
Capacity Not Allocated:      7501697024 B (7.5 GB) (97.3% free)
|
+-< Physical Store disk2s2 D91E2996-2C76-4E20-B5BD-E8CEE9F83EE4
-----
APFS Physical Store Disk:    disk2s2
Size:                         7709093376 B (7.7 GB)
|
+--> Volume disk3s1 7708D723-0592-4509-A497-8BA01EC8BA64
-----
APFS Volume Disk (Role):    disk3s1 (No specific role)
Name:                         APFS_VOL1 (Case-insensitive)
Mount Point:                  /Volumes/APFS_VOL1
Capacity Consumed:           146432000 B (146.4 MB)
FileVault:                    No
|
+--> Volume disk3s2 B2551185-8A61-42A8-BB05-C8974147E8DE
-----
APFS Volume Disk (Role):    disk3s2 (No specific role)
Name:                         APFS_VOL2 (Case-insensitive)
Mount Point:                  /Volumes/APFS_VOL2
Capacity Consumed:           25513984 B (25.5 MB)
FileVault:                    No
|
+--> Volume disk3s3 7C6F51AE-D751-4F27-B23A-1BECCE4889AA
-----
APFS Volume Disk (Role):    disk3s3 (No specific role)
Name:                         APFS_VOL3 (Case-insensitive)
Mount Point:                  /Volumes/APFS_VOL3
Capacity Consumed:           10186752 B (10.2 MB)
FileVault:                    No
```

# Forensic Tool Analysis Support

# Forensic Tool Analysis Support

Tool	Support	Notes
AccessData FTK	No	
BlackBag BlackLight	Yes	FileVault Support
macOS 10.13	Yes	Native via Image Mounting, FileVault Support
Magnet Axiom	No	
Nuix	No	
OpenText EnCase	Meh.	Logical L01 File – No full native support.
SANS SIFT	Yes	Via Image Mounting, 3 <sup>rd</sup> Party Driver, No FileVault Support
Sleuthkit	No	Soon? DFRWS US 2018, Paper by Joe Sylve
Sumuri Recon	Yes	FileVault Support
XWays	Yes	Unencrypted APFS Support

# BlackBag BlackLight

The screenshot displays the BlackBag BlackLight forensic analysis interface. The top navigation bar includes icons for Case Info, Timeline, Search, Report, Details, Browser, File Filter, Actionable Intel, Communication, Media, Locations, Internet, Productivity, System, and Notifications.

The left sidebar contains sections for EVIDENCE (galaga.E01), ACTIVITY (Export Status, Evidence Status), CONTENT SEARCHES, and TAGS. A central tree view shows the directory structure of the evidence file, starting from the Root. The table below lists files with columns for Name, Date Created, Date Modified, Date Accessed, and Date Added.

Name	Date Created	Date Modified	Date Accessed	Date Added
Galaga	2017-11-12 21:17:11 (UTC)	2018-02-26 01:14:11 (UTC)	2018-03-03 21:21:48 (UTC)	
.DocumentRevisions-V100	2017-12-23 00:54:35 (UTC)	2018-02-25 22:25:19 (UTC)	2018-02-25 22:25:19 (UTC)	
.DS_Store	2017-10-03 00:36:27 (UTC)	2018-03-03 20:30:50 (UTC)	2018-02-27 01:54:47 (UTC)	
.file	2017-10-03 00:36:27 (UTC)	2017-10-03 00:36:27 (UTC)	2017-10-03 00:36:27 (UTC)	
.fseventsds	2017-11-13 01:19:01 (UTC)	2018-03-03 20:44:26 (UTC)	2018-02-25 22:26:22 (UTC)	
.PKInstallSandboxManager-SystemS...	2017-11-13 10:57:10 (UTC)	2018-03-03 21:22:33 (UTC)	2018-03-03 21:21:44 (UTC)	
.Spotlight-V100	2017-11-13 01:19:51 (UTC)	2017-11-13 01:19:51 (UTC)	2017-11-13 01:19:51 (UTC)	
.vol	2017-10-03 00:36:04 (UTC)	2017-10-03 00:36:04 (UTC)	2017-11-13 01:12:31 (UTC)	
Applications	2017-10-25 16:33:42 (UTC)	2018-03-03 20:29:22 (UTC)	2018-02-26 01:28:19 (UTC)	
bin	2017-10-25 16:37:55 (UTC)	2017-10-25 16:37:55 (UTC)	2017-11-13 01:10:59 (UTC)	
cores	2017-10-03 00:36:01 (UTC)	2017-10-03 00:36:01 (UTC)	2017-11-13 01:13:04 (UTC)	
dev	2017-10-03 00:36:01 (UTC)	2017-10-03 00:36:01 (UTC)	2017-11-13 01:12:31 (UTC)	
etc	2017-11-13 01:09:36 (UTC)	2017-11-13 01:09:36 (UTC)	2017-11-13 01:09:36 (UTC)	
home	2017-11-13 01:19:34 (UTC)	2017-11-13 01:19:34 (UTC)	2017-11-13 01:19:34 (UTC)	
installer.failurerequests	2017-09-01 01:09:23 (UTC)	2017-09-01 01:09:23 (UTC)	2017-09-01 01:09:23 (UTC)	
Library	2017-10-25 16:35:20 (UTC)	2018-02-25 22:00:50 (UTC)	2018-02-25 22:00:50 (UTC)	
net	2017-10-03 00:36:02 (UTC)	2017-10-03 00:36:02 (UTC)	2018-01-19 03:09:55 (UTC)	
Network	2017-11-13 00:52:40 (UTC)	2017-11-13 01:13:04 (UTC)	2017-11-13 01:13:04 (UTC)	
private				
sbin	2017-10-25 16:37:55 (UTC)	2017-11-13 01:10:57 (UTC)	2017-11-13 01:10:59 (UTC)	
System	2017-10-25 16:31:26 (UTC)	2017-10-25 16:31:26 (UTC)	2018-03-03 21:21:48 (UTC)	
tmp	2017-11-13 01:09:38 (UTC)	2017-11-13 01:09:38 (UTC)	2017-11-13 01:09:38 (UTC)	
Users	2017-07-15 20:35:53 (UTC)	2018-02-10 14:06:39 (UTC)	2018-02-10 13:23:48 (UTC)	
usr	2017-10-25 16:22:13 (UTC)	2018-02-25 22:00:49 (UTC)	2018-02-25 22:00:49 (UTC)	
var	2017-11-13 01:10:57 (UTC)	2017-11-13 01:10:57 (UTC)	2017-11-13 01:10:57 (UTC)	
Volumes	2017-10-03 00:36:26 (UTC)	2018-03-03 21:33:22 (UTC)	2018-03-03 21:28:10 (UTC)	

The bottom pane shows a hex editor view of the .DS\_Store file, displaying binary data and corresponding ASCII strings. A sidebar on the right provides details for selected file fields like Name, Path, Size, and Content Type, along with a preview of the file's metadata.

# Mounting

# MacOS – w/ or w/o FileVault Encryption

## 10.13 Host Required

1. \$ sudo mkdir /Volumes/apfs\_image/
2. \$ sudo mkdir /Volumes/apfs\_mounted/
3. \$ sudo xmount --in ewf apfs.E01 --out dmg /Volumes/apfs\_image/
4. \$ hdiutil attach --nomount /Volumes/apfs\_image/apfs.dmg
5. \$ *diskutil ap list*
6. \$ *diskutil ap unlockVolume <Disk GUID> –nomount*
7. \$ sudo mount\_apfs –o rdonly,noexec,noowners /dev/disk# /Volumes/apfs\_mounted/

# Windows & Linux Mounting Options

- APFS drivers from Paragon ([paragon-software.com](http://paragon-software.com))
  - Windows – Free, Currently no support for FileVault
  - Linux – Price and FileVault Support Unknown – “Contact Us”
- Open Source APFS Driver by sgan81 – APFS-fuse
  - <https://github.com/sgan81/apfs-fuse>
  - FileVault Encryption Supported (with password)
- Fantastic Tutorials from Mari DeGrazia
  - <http://az4n6.blogspot.com/2018/01/how-to-mount-mac-apfs-images-in-windows.html>
    - Using Arsenal Image Mounter
  - <http://az4n6.blogspot.com/2018/01/mounting-apfs-image-in-linux.html>

# APFS Features

# Clones

- Instant copy of files/directories
- No redundant use of space
- New/modified data to files saved in separate blocks
- File changes saved as deltas

Name	Size
GoogleEarth...c-Intel.dmg	73.4 MB
WhatsApp copy.dmg	72.1 MB
WhatsApp.dmg	72.1 MB

```
[Sarahs-MBP-6:APFS_VOL1 oompa$ stat -x WhatsApp*
  File: "WhatsApp copy.dmg"
  Size: 72061030  FileType: Regular File
  Mode: (0644/-rw-r--r--)
Device: 1,20  Inode: 201  Links: 1
Access: Sun Apr 22 20:16:08 2018
Modify: Thu Nov 23 13:22:54 2017
Change: Sun Apr 22 20:34:35 2018
  File: "WhatsApp.dmg"
  Size: 72061030  FileType: Regular File
  Mode: (0644/-rw-r--r--)
Device: 1,20  Inode: 192  Links: 1
Access: Sun Apr 22 20:16:08 2018
Modify: Thu Nov 23 13:22:54 2017
Change: Sun Apr 22 20:16:14 2018]
```

```
[Sarahs-MBP-6:~ oompa$ df -h /Volumes/APFS_VOL1
Filesystem      Size   Used  Avail Capacity iused          ifree %iused  Mounted on
/dev/disk5s1  7.2Gi  140Mi  7.0Gi    2%     79  9223372036854775728      0%  /Volumes/APFS_VOL1
[Sarahs-MBP-6:~ oompa$ df -h /Volumes/APFS_VOL1
Filesystem      Size   Used  Avail Capacity iused          ifree %iused  Mounted on
/dev/disk5s1  7.2Gi  140Mi  7.0Gi    2%     80  9223372036854775727      0%  /Volumes/APFS_VOL1
```

# Snapshots

- Read-only snapshot of the file system
- Efficient Backups (Time Machine)
- Time Machine Local Snapshots created: Once an hour & before macOS updates
- Time Machine Local Snapshots kept for 24 hours
- Create on-demand snapshot ‘`tmutil localsnapshot`’
- 10.12 had command `apfs_snapshot`
  - Use `tmutil` and `apfs_mount` on live system
  - Still trying to determine how to use forensically from dead image
- About Time Machine local snapshots - <https://support.apple.com/en-us/HT204015>

Snapshot – An APFS Snapshot represents a read-only copy of its parent APFS Volume, frozen at the moment of its creation. An APFS Volume can have zero or more associated APFS Snapshots.

APFS Snapshots are neither listed nor discoverable when their Volume is not mounted. Snapshots are uniquely identified within their parent Volume's namespace by either a numeric identifier (preferred) or by their name; Snapshots can be renamed, but APFS will never allow duplication of names (within a Volume) to occur.

APFS Snapshots are mountable; when this occurs, its mount point (separate from and simultaneous with its parent Volume) provides a read-only historic version of the Volume content at Snapshot creation time.

# Snapshots

## Live List

- diskutil ap listsnapshots <mountpoint>
  - ...or listsnaps (for the millennials)
- tmutil listlocalsnapshots <mountpoint>

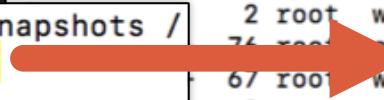
```
[Sarahs-MBP-6:/ oompa$ tmutil listlocalsnapshots /
com.apple.TimeMachine.2018-04-22-114609
com.apple.TimeMachine.2018-04-22-214754
com.apple.TimeMachine.2018-04-22-232139
com.apple.TimeMachine.2018-04-23-005036
com.apple.TimeMachine.2018-04-23-025303
com.apple.TimeMachine.2018-04-23-045139
com.apple.TimeMachine.2018-04-23-064924
com.apple.TimeMachine.2018-04-23-102309
com.apple.TimeMachine.2018-04-23-122205
com.apple.TimeMachine.2018-04-23-161716
com.apple.TimeMachine.2018-04-23-174736
com.apple.TimeMachine.2018-04-23-192417
com.apple.TimeMachine.2018-04-23-195016
```

```
[Sarahs-MBP-6:/ oompa$ diskutil ap listsnaps /
Snapshots for disk1s1 (13 found)
|
+-- Name: com.apple.TimeMachine.2018-04-22-114609
|   XID: 10964731
|   NOTE: This snapshot sets the minimal allowed size of APFS Container disk1
|
+-- Name: com.apple.TimeMachine.2018-04-22-214754
|   XID: 10969408
|
+-- Name: com.apple.TimeMachine.2018-04-22-232139
|   XID: 10969977
|
+-- Name: com.apple.TimeMachine.2018-04-23-005036
|   XID: 10970513
|
+-- Name: com.apple.TimeMachine.2018-04-23-025303
|   XID: 10971224
|
+-- Name: com.apple.TimeMachine.2018-04-23-045139
|   XID: 10972023
|
+-- Name: com.apple.TimeMachine.2018-04-23-064924
|   XID: 10972688
|
+-- Name: com.apple.TimeMachine.2018-04-23-102309
|   XID: 10973910
|
+-- Name: com.apple.TimeMachine.2018-04-23-122205
|   XID: 10974578
|
+-- Name: com.apple.TimeMachine.2018-04-23-161716
|   XID: 10975986
|
+-- Name: com.apple.TimeMachine.2018-04-23-174736
|   XID: 10976469
|
+-- Name: com.apple.TimeMachine.2018-04-23-192417
|   XID: 10977049
|
+-- Name: com.apple.TimeMachine.2018-04-23-195016
|   XID: 10978281
```

# Snapshot Mounting – Live System

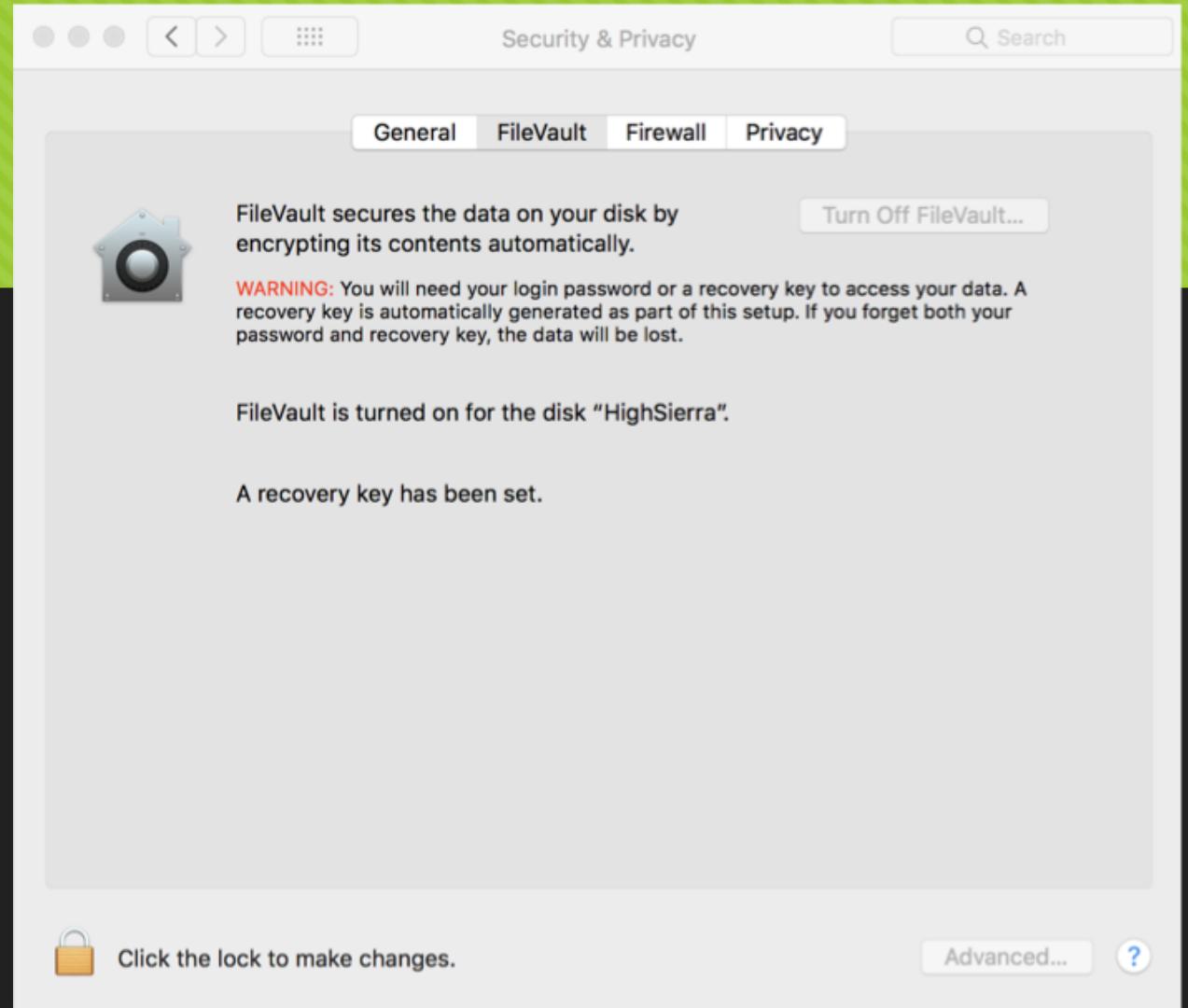
```
[Sarahs-MBP-6:/ oompa$ sudo mkdir /Volumes/snapshot_mounted
[Sarahs-MBP-6:/ oompa$ sudo mount_apfs -s com.apple.TimeMachine.2018-04-22-114609 / /Volumes/snapshot_mounted
mount_apfs: snapshot implicitly mounted readonly
[Sarahs-MBP-6:/ oompa$ ls -la /Volumes/snapshot_mounted/
total 40
drwxr-xr-x@ 29 root  wheel  928 Apr 16 22:24 .
drwxr-xr-x+ 11 root  wheel  352 Apr 22 21:22 ..
-rw-rw-r--  1 root  admin 14340 Apr 15 10:31 .DS_Store
d--x--x--x  9 root  wheel  288 Apr 16 22:24 .DocumentRevisions-V100
dr-xr-xr-t@ 2 root  wheel   64 Nov 11 12:56 .HFS+ Private Directory Data?
drwxr-xr-x@ 2 root  wheel   64 Apr 12 19:34 .PKInstallSandboxManager-SystemSoftware
drwx-----  5 root  wheel  160 Nov 11 13:18 .Spotlight-V100
srwxrwxrwx  1 root  wheel    0 Apr 16 22:24 .dbfsevents
-----  1 root  admin    0 Jul 25 2017 .file
drwx----- 242 root  wheel  7744 Apr 22 10:26 .fsevents
                2 root  wheel   64 Jul 25 2017 .vol
                74 root  admin  2432 Apr 15 10:31 Applications
                67 root  wheel  2144 Apr  1 17:56 Library
                2 root  wheel   64 Jul 25 2017 Network
                4 root  wheel  128 Sep 21 2017 System
                8 root  admin  256 Mar 24 21:22 Users
                7 root  wheel  224 Apr 22 10:26 Volumes
drwxr-xr-x@ 38 root  wheel  1216 Apr 10 18:25 bin
drwxrwxr-t  2 root  admin   64 Jul 25 2017 cores
dr-xr-xr-x  2 root  wheel   64 Jul 25 2017 dev
lrwxr-xr-x@ 1 root  wheel   11 Nov 11 13:12 etc -> private/etc
dr-xr-xr-x  2 root  wheel   64 Nov 11 13:18 home
-rw-r--r--  1 root  wheel  313 Aug 10 2017 installer.failurerequests
dr-xr-xr-x  2 root  wheel   64 Nov 11 13:18 net
drwxr-xr-x  6 root  wheel  192 Nov 11 13:13 private
drwxr-xr-x@ 63 root  wheel  2016 Apr 10 18:25 sbin
lrwxr-xr-x@ 1 root  wheel   11 Nov 11 13:12 tmp -> private/tmp
drwxr-xr-x@ 10 root  wheel  320 Nov 11 16:58 usr
lrwxr-xr-x@ 1 root  wheel   11 Nov 11 13:13 var -> private/var
```

```
[Sarahs-MBP-6:/ oompa$ tmutil listlocalsnapshots /
com.apple.TimeMachine.2018-04-22-114609
com.apple.TimeMachine.2018-04-22-195720
com.apple.TimeMachine.2018-04-22-202457
com.apple.TimeMachine.2018-04-22-204859
com.apple.TimeMachine.2018-04-22-205540
```



# Encryption

- Encryption, built in.
  - HFS+ required CoreStorage wrapper
- Encryption per Volume
- Modes:
  - No Encryption
  - Single-key
  - Multi-key
    - Per-file keys for data
    - Key for sensitive metadata
- AES-XTS, AEX-CBC (depends on hardware)
- <https://www.blackbagtech.com/blog/2018/04/02/ask-expert-apfs-encryption/>



# APFS Password Bug – Unified Logs & install.log

```
Sarahs-MBP:FOR518 oompa$ log show galaga.logarchive/ --info --predicate 'eventMessage contains "SEKRET"' --style syslog
=====
/Users/oompa/FOR518/galaga.logarchive
=====
log: warning: The log archive contains partial or missing metadata
Filtering the log data using "eventMessage CONTAINS \"SEKRET\""
Skipping debug messages, pass --debug to include.
Timestamp          (process)[PID]
2018-02-25 20:48:58.712365-0500  localhost diskmanagementd[1257]: diskmanagement: execve(2) pid=1257 /System/Library/Filesystems/hfs.fs/Contents/Resources/newfs_hfs -J -v
SEKRET /dev/rdisk4s2 .
2018-02-25 20:49:04.466414-0500  localhost kernel[0]: (HFS) hfs: mounted SEKRET on device disk4s2
2018-02-25 20:49:04.518324-0500  localhost fsevents[47]: could not open </Volumes/SEKRET/.fsevents/fsevents-d-uuid> (No such file or directory)
2018-02-25 20:49:04.518334-0500  localhost fsevents[47]: Failed to load UUID. Removing all old log files in /Volumes/SEKRET/.fsevents
2018-02-25 20:49:04.518433-0500  localhost fsevents[47]: log dir: /Volumes/SEKRET/.fsevents getting new uuid: 72FEB7BC-BF24-43DE-9D71-54056CECB33E
2018-02-25 20:49:04.668388-0500  localhost deleted[414]: [com.apple.cache_delete:daemon] Purgeable Result: 0 bytes on: "/Volumes/SEKRET"
2018-02-25 20:49:04.722366-0500  localhost fsevents[47]: Events arrived for /Volumes/SEKRET after an unmount request! Re-initializing.
2018-02-25 20:49:04.722376-0500  localhost fsevents[47]: creating a dls for /Volumes/SEKRET but it already has one...
2018-02-25 20:49:06.473078-0500  localhost kernel[0]: (HFS) hfs: unmount initiated on SEKRET on device disk4s2
2018-02-25 20:49:06.602182-0500  localhost fsevents[47]: disk logger: failed to open output file /Volumes/SEKRET/.fsevents/0000000000027b06e (No such file or directory).
mount point /Volumes/SEKRET/.fsevents
2018-02-25 20:49:06.602361-0500  localhost fsevents[47]: disk logger: failed to open output file /Volumes/SEKRET/.fsevents/0000000000027b06e (No such file or directory).
mount point /Volumes/SEKRET/.fsevents
2018-02-25 20:49:08.719840-0500  localhost diskmanagementd[1276]: diskmanagement: execve(2) pid=1276 /System/Library/Filesystems/apfs.fs/Contents/Resources/newfs_apfs -A
-i -E -S frogger13 -v SEKRET disk5 .
2018-02-25 20:49:09.741614-0500  localhost kernel[0]: (apfs) apfs_vfsop_mount:1368: mounted volume: SEKRET
2018-02-25 20:49:09.794588-0500  localhost fsevents[47]: could not open </Volumes/SEKRET/.fsevents/fsevents-d-uuid> (No such file or directory)
2018-02-25 20:49:09.794596-0500  localhost fsevents[47]: Failed to load UUID. Removing all old log files in /Volumes/SEKRET/.fsevents
2018-02-25 20:49:09.794711-0500  localhost fsevents[47]: log dir: /Volumes/SEKRET/.fsevents getting new uuid: AD6ECA53-6EDE-4FC8-9B21-D9BA10C3C6A9
2018-02-25 20:49:09.798644-0500  localhost deleted[414]: [com.apple.cache_delete:daemon] Purgeable Result: 0 bytes on: "/Volumes/SEKRET"
2018-02-25 20:49:09.816415-0500  localhost storagekitd[1220]: Erase Complete, Mount Point: /Volumes/SEKRET
2018-02-25 20:49:09.830160-0500  localhost deleted[414]: [com.apple.cache_delete:daemon] Purgeable Result: 0 bytes on: "/Volumes/SEKRET"
2018-02-25 20:49:09.858039-0500  localhost storagekitd[1220]: Recache Complete, Mount Point: /Volumes/SEKRET
2018-02-25 20:49:58.326722-0500  localhost deleted[414]: [com.apple.cache_delete:daemon] Purgeable Result: 0 bytes on: "/Volumes/SEKRET"
2018-02-27 18:20:25.719892-0500  localhost kernel[0]: (apfs) apfs_vfsop_mount:1368: mounted volume: SEKRET
2018-02-27 18:20:25.828215-0500  localhost deleted[414]: [com.apple.cache_delete:daemon] Purgeable Result: 0 bytes on: "/Volumes/SEKRET"
2018-02-27 18:22:13.848939-0500  localhost deleted[414]: [com.apple.cache_delete:daemon] Purgeable Result: 0 bytes on: "/Volumes/SEKRET"
2018-02-28 18:58:39.652188-0500  localhost kernel[0]: (apfs) apfs_vfsop_mount:1368: mounted volume: SEKRET
2018-02-28 18:58:39.784029-0500  localhost deleted[414]: [com.apple.cache_delete:daemon] Purgeable Result: 0 bytes on: "/Volumes/SEKRET"
```

# The Future of APFS Forensics

# HFS+ Documentation – TechNote 1150

- HFS+ first implemented in 1998
- Published 1999
- Last Updated in 2004!
  - “Reserved for future use.”

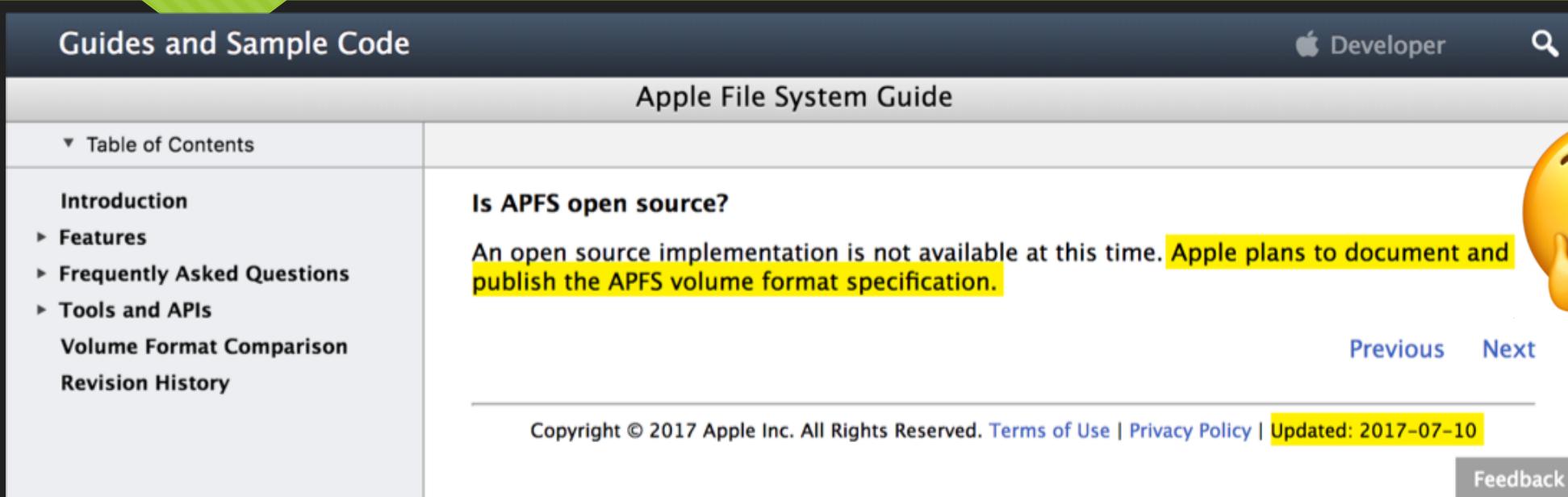
The screenshot shows a web browser window with the following details:

- Header:** Apple Inc. (with a lock icon), Developer, and a search bar.
- Title Bar:** Retired Documents Library and HFS Plus Volume Format.
- Breadcrumbs:** ADC Home > Reference Library > Technical Notes > Carbon > File Management >
- Section Title:** Technical Note TN1150 HFS Plus Volume Format
- Content Summary:** This Technote describes the on-disk format for an HFS Plus volume. It does **not** describe any programming interfaces for HFS Plus volumes.
- Content Description:** This technote is directed at developers who need to work with HFS Plus at a very low level, below the abstraction provided by the File Manager programming interface. This includes developers of disk recovery utilities and programmers implementing HFS Plus support on other platforms.
- Content Assumption:** This technote assumes that you have a conceptual understanding of the HFS volume format, as described in Inside Macintosh: Files.
- Footer:** [Mar 05, 2004]

**CONTENTS**

- HFS Plus Basics
- Core Concepts
- Volume Header
- B-Trees
- Catalog File
- Extents Overflow File
- Allocation File
- Attributes File

# In-Depth Analysis & Tools File System Documentation Resources



The screenshot shows a section of the Apple File System Guide. On the left, there's a sidebar with links like 'Table of Contents', 'Introduction', 'Features', 'Frequently Asked Questions', 'Tools and APIs', 'Volume Format Comparison', and 'Revision History'. The main content area has a heading 'Is APFS open source?'. Below it, a yellow-highlighted note states: 'An open source implementation is not available at this time. Apple plans to document and publish the APFS volume format specification.' To the right of the note is a large yellow thinking emoji. At the bottom of the page, there are links for 'Previous' and 'Next', and a 'Feedback' button.

Is APFS open source?  
An open source implementation is not available at this time. Apple plans to document and publish the APFS volume format specification.

- Kaitai Struct from cugu - <https://github.com/cugu/apfs.ksy>
- 'Decoding the APFS file system' by Kurt H. Hansen & Fergus Toolan
  - [https://www.researchgate.net/publication/319573636\\_Decoding\\_the\\_APFS\\_file\\_system](https://www.researchgate.net/publication/319573636_Decoding_the_APFS_file_system)
- ENRW Whitepaper 65 - APFS Internals for Forensic Analysis by Andreas Dewald & Jonas Plum
  - [https://static.ernw.de/whitepaper/ERNW\\_Whitepaper65\\_APFS-forensics\\_signed.pdf](https://static.ernw.de/whitepaper/ERNW_Whitepaper65_APFS-forensics_signed.pdf)

# References & Links

- [https://developer.apple.com/library/content/documentation/FileManagement/Conceptual/APFS\\_Guide/](https://developer.apple.com/library/content/documentation/FileManagement/Conceptual/APFS_Guide/)
- <https://www.blackbagtech.com/blog/2018/04/02/ask-expert-apfs-encryption/>
- <https://www.blackbagtech.com/blog/2018/04/11/apple-file-system-apfs-mac-forensic-imaging-analysis/>
- <https://www.mac4n6.com/blog/2017/11/26/mount-all-the-things-mounting-apfs-and-4k-disk-images-on-macos-1013>
- <https://www.blackbagtech.com/blog/2018/04/11/apple-file-system-apfs-mac-forensic-imaging-analysis/>
- <https://www.paragon-software.com/home/apfs-windows/>
- <https://www.paragon-software.com/business/apfs-linux/>
- <https://github.com/sgan81/apfs-fuse>
- <http://az4n6.blogspot.com/2018/01/how-to-mount-mac-apfs-images-in-windows.html>
- <http://az4n6.blogspot.com/2018/01/mounting-apfs-image-in-linux.html>
- <https://derflounder.wordpress.com/category/apple-file-system/>
- <https://developer.apple.com/videos/play/wwdc2016/701/>
- <https://developer.apple.com/videos/play/wwdc2017/715/>