

# macOS Forensics: The Next Level - Taming the T2 Chip & More



Yogesh Khatri  
Alexandra Cartwright



# About us

- Yogesh Khatri
- Associate Professor – Champlain College
- Program Director – Digital Forensics
- *15+ years doing Forensics*
- Author & Maintainer for *mac\_apt – Artifact Parsing Tool*



- Alexandra Cartwright
- Student (Junior) – Champlain College
- Digital Forensics Major
- Data Analytics Minor



 @swiftforensics

 Swiftforensics.com

 @alex\_cart27

# Agenda

- T2 chip
- Image Acquisition
- Snapshot data & Analysis
- Processing with mac\_apt

## About the Apple T2 Security Chip

The Apple T2 Security Chip brings a new level of integration and security to Mac.



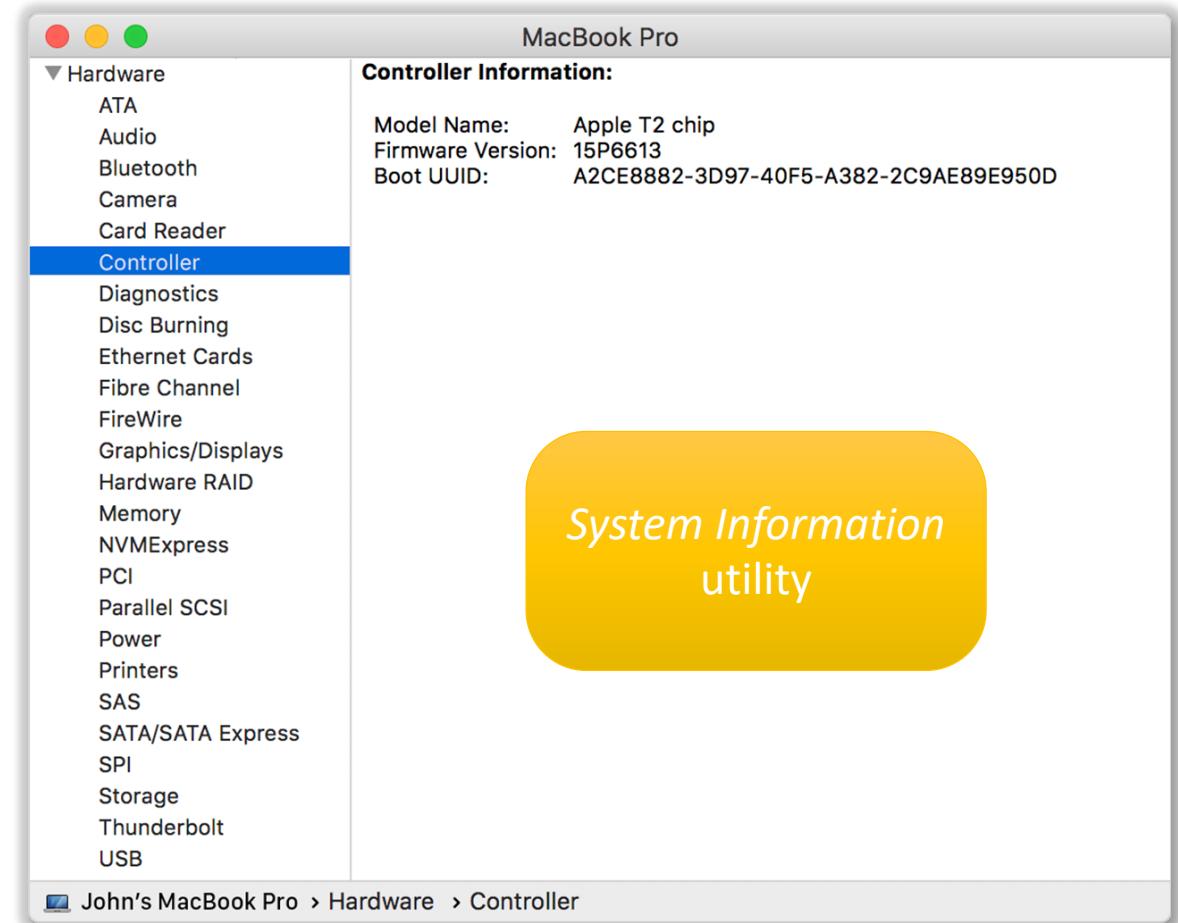
The Apple T2 Security Chip is Apple's second-generation, custom silicon for Mac. By redesigning and integrating several controllers found in other Mac computers—such as the System Management Controller, image signal processor, audio controller, and SSD controller—the T2 chip delivers new capabilities to your Mac.

For example, the T2 chip enables a new level of security by including a secure enclave coprocessor that secures [Touch ID](#) data and provides the foundation for new [encrypted storage](#) and [secure boot](#) capabilities. And the T2 chip's image signal processor works with the FaceTime HD camera to enable enhanced tone mapping, improved exposure control, and face-detection-based autoexposure and auto white balance.

# How do I know if a mac has the T2 chip?

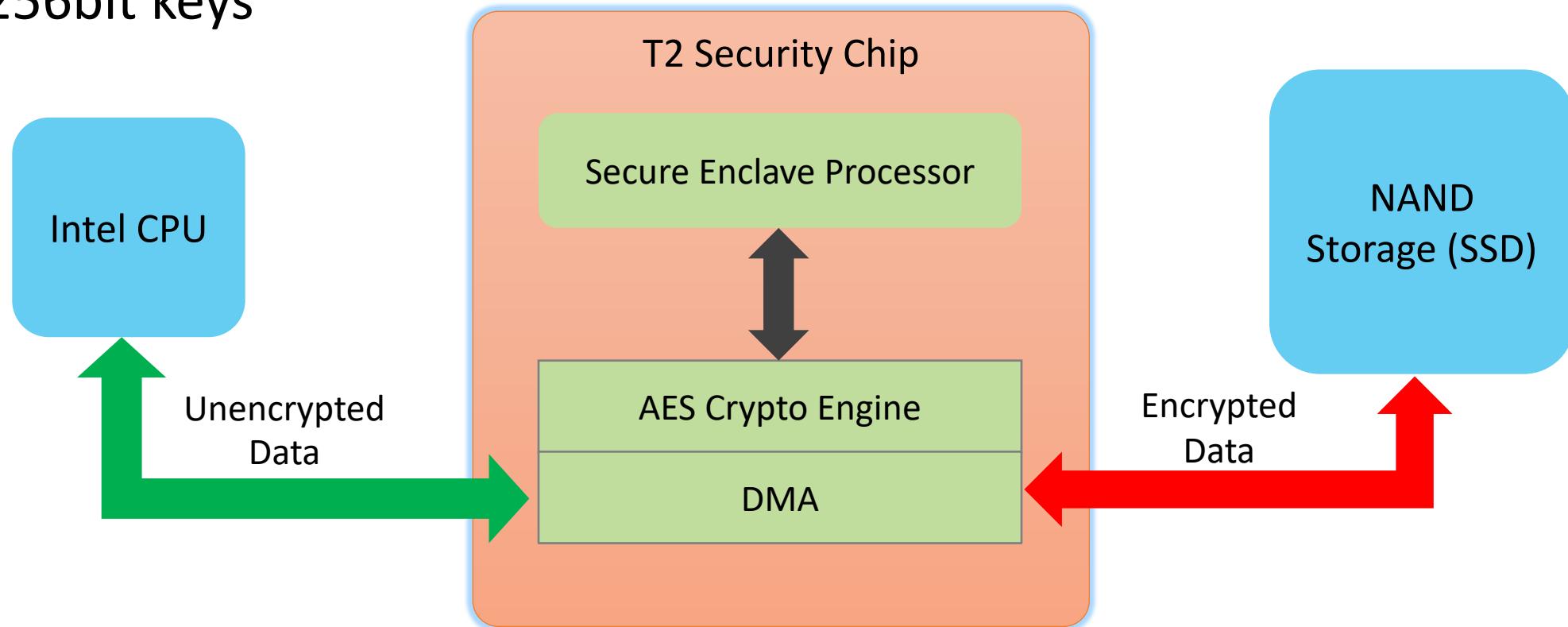
Is it one of these models?

- iMac Pro
- Mac Pro 2019 or later
- Mac mini 2018 or later
- MacBook Air 2018 or later
- MacBook Pro 2018 or later



# Encryption on T2 enabled macs

- AES-XTS
- 256bit keys



From Apple's own documentation

## About encrypted storage on your new Mac

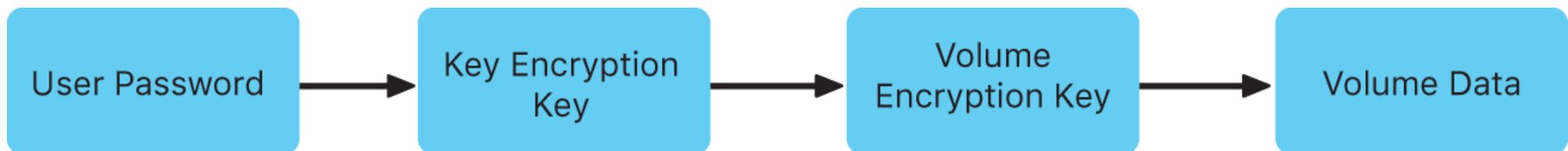
Learn about encrypted storage on computers that have the Apple T2 Security Chip, and make sure that your data is fully protected.

Mac computers that have the Apple T2 Security Chip integrate security into both software and hardware to provide encrypted-storage capabilities. Data on the built-in, solid-state drive (SSD) is encrypted using a hardware-accelerated AES engine built into the T2 chip.

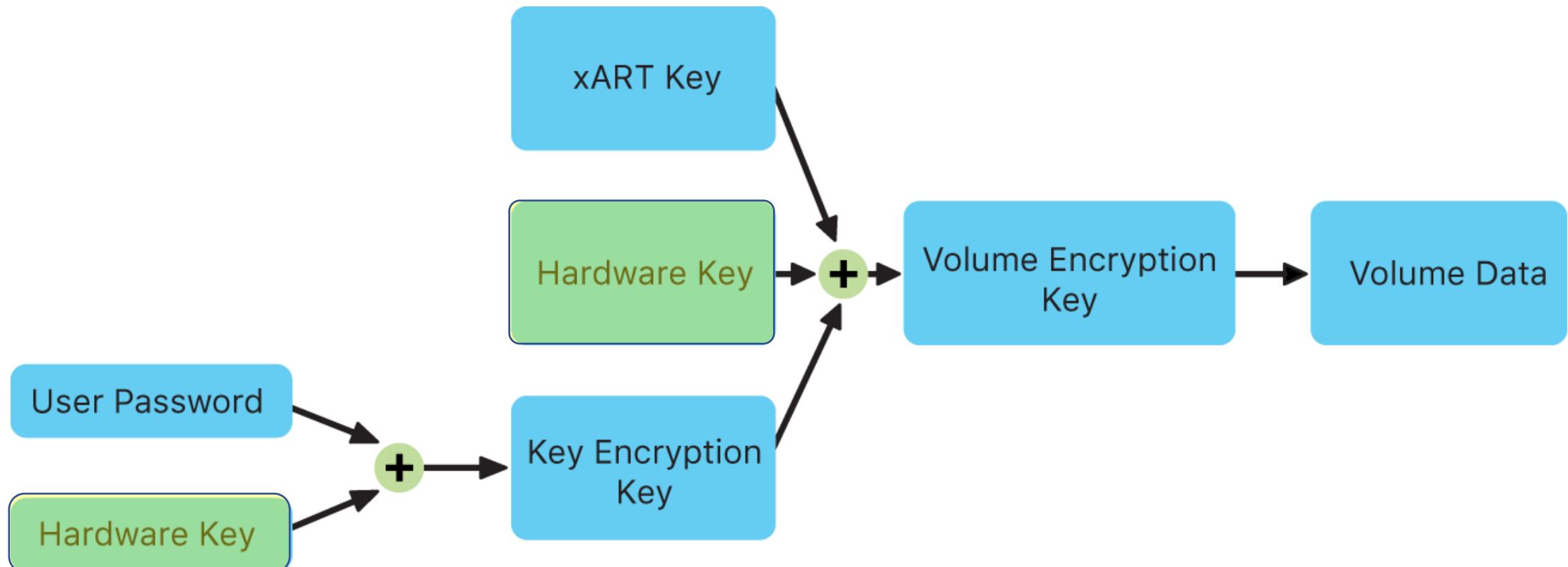
This encryption is performed with 256-bit keys tied to a unique identifier within the T2 chip.

# FileVault (APFS/HFS) without T2

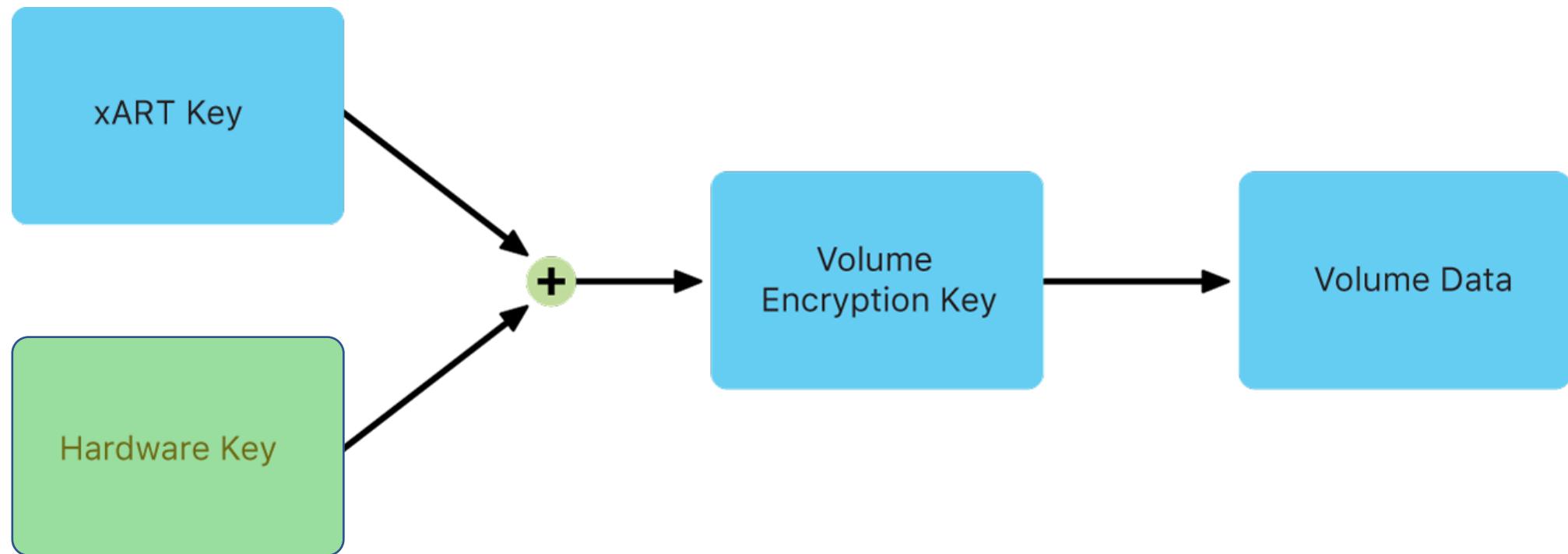
- Encryption is software based



# T2 APFS vol with FileVault ON

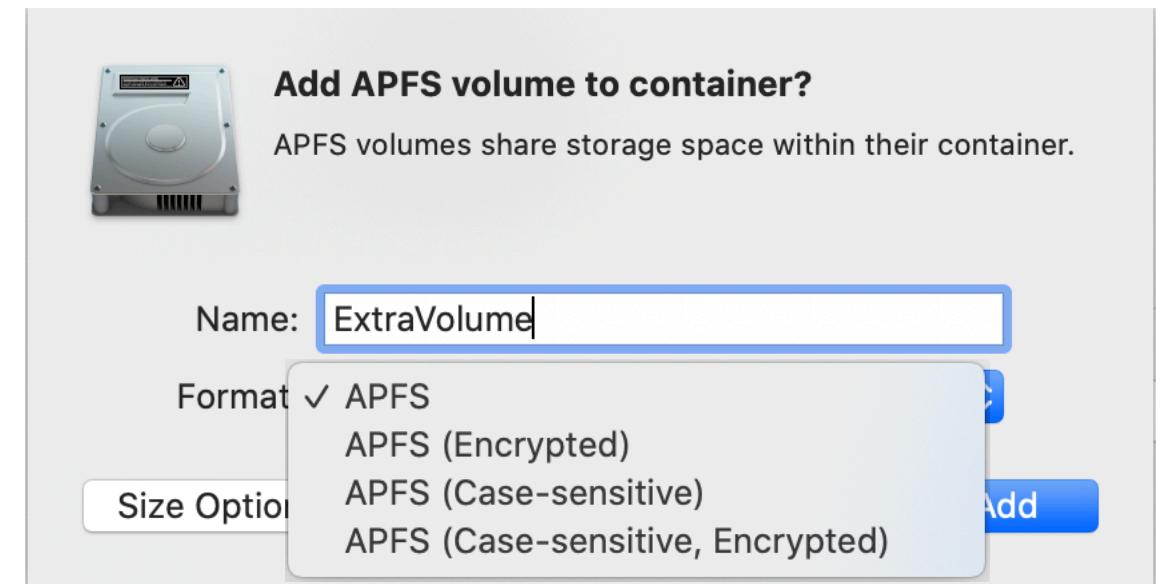


# T2 APFS vol without FileVault



# What is really encrypted for a T2 mac?

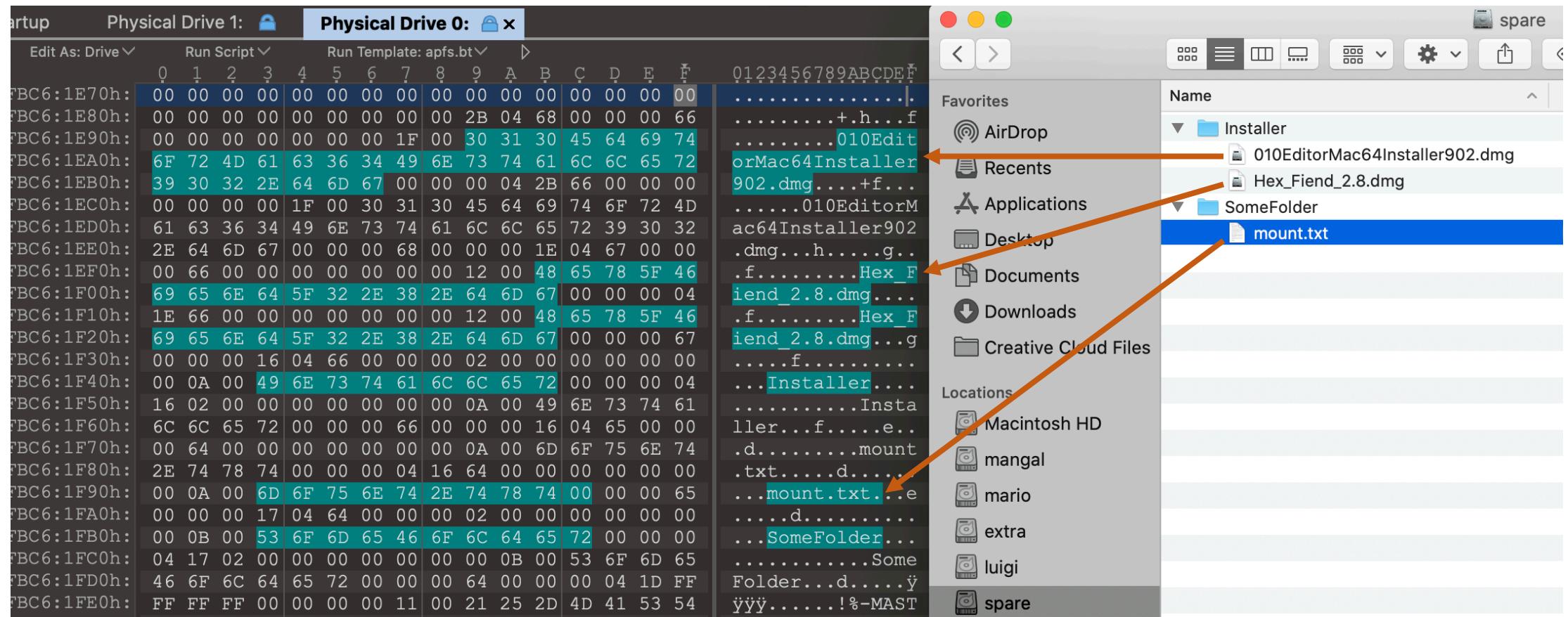
- Not everything on the SSD
- Only APFS formatted volumes are encrypted
  - Turns on encryption for all APFS volumes (*even if you choose no encryption!*)
  - This is hidden from user
- FAT, NTFS, exFAT not encrypted



# exFAT partition on T2 mac – Raw disk view

Startup	Physical Drive 1:	Physical Drive 0:
A:FA60:0000h:	Ø 1 2 3 4 5 6 7 8 9 A B C D E F	Ø 1 2 3 4 5 6 7 8 9 ABCDEF
A:FA60:0000h:	EB 76 90 45 58 46 41 54 20 20 20 00 00 00 00 00	ëv.EXFAT .....
A:FA60:0010h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
A:FA60:0020h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
A:FA60:0030h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
A:FA60:0040h:	00 A6 AF 04 00 00 00 00 00 B6 DF 09 00 00 00 00	.!.....¶B.....
A:FA60:0050h:	00 01 00 00 00 14 00 00 00 15 00 00 08 FD 4E 00	.....]ýN.
A:FA60:0060h:	08 00 00 00 5D 3C E4 5D 00 01 02 00 0C 05 01 80	....<ä].....€
A:FA60:0070h:	00 00 00 00 00 00 00 F4 F4 F4 F4 F4 F4 F4 F4	.....ôôôôôôôôôôôôôô
A:FA60:0080h:	F4	ôôôôôôôôôôôôôôôôôôôô

# exFAT partition on T2 mac – Metadata



# exFAT partition on T2 mac – Data

Physical Drive 1:												Physical Drive 0:  x																				
as: Drive	Run Script				Run Template: APFS.bt								▷				0123456789ABCDEF															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
01C0h:	64	65	76	2F	64	69	73	6B	32	73	31	20	6F	6E	20	2F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
01D0h:	56	6F	6C	75	6D	65	73	2F	6D	61	72	69	6F	20	28	61	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
01E0h:	70	66	73	2C	20	6C	6F	63	61	6C	2C	20	6A	6F	75	72	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
01F0h:	6E	61	6C	65	64	29	0A	2F	64	65	76	2F	64	69	73	6B	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0200h:	35	73	31	20	6F	6E	20	2F	56	6F	6C	75	6D	65	73	2F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0210h:	6C	75	69	67	69	20	28	61	70	66	73	2C	20	6C	6F	63	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0220h:	61	6C	2C	20	6A	6F	75	72	6E	61	6C	65	64	29	0A	2F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0230h:	64	65	76	2F	64	69	73	6B	30	73	36	20	6F	6E	20	2F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0240h:	56	6F	6C	75	6D	65	73	2F	73	70	61	72	65	20	28	65	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0250h:	78	66	61	74	2C	20	61	73	79	6E	63	68	72	6F	6E	6F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0260h:	75	73	2C	20	6C	6F	63	61	6C	2C	20	6E	6F	6F	77	6E	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0270h:	65	72	73	29	0A	2F	64	65	76	2F	64	69	73	6B	33	73	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0280h:	31	20	6F	6E	20	2F	56	6F	6C	75	6D	65	73	2F	65	78	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0290h:	74	72	61	20	28	61	70	66	73	2C	20	6C	6F	63	61	6C	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
02A0h:	2C	20	6A	6F	75	72	6E	61	6C	65	64	29	0A	2F	64	65	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
02B0h:	76	2F	64	69	73	6B	34	73	31	20	6F	6E	20	2F	56	6F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
02C0h:	6C	75	6D	65	73	2F	65	6E	63	20	28	61	70	66	73	2C	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
02D0h:	20	6C	6F	63	61	6C	2C	20	6A	6F	75	72	6E	61	6C	65	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
02E0h:	64	29	0A	2F	64	65	76	2F	64	69	73	6B	36	73	31	20	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
02F0h:	6F	6E	20	2F	56	6F	6C	75	6D	65	73	2F	48	65	78	20	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0300h:	46	69	65	6E	64	20	32	2E	38	20	28	68	66	73	2C	20	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0310h:	6C	6F	63	61	6C	2C	20	6E	6F	64	65	76	2C	20	6E	6F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0320h:	73	75	69	64	2C	20	72	65	61	64	2D	6F	6E	6C	79	2C	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0330h:	20	6E	6F	6F	77	6E	65	72	73	2C	20	71	75	61	72	61	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0340h:	6E	74	69	6E	65	2C	20	6D	6F	75	6E	74	65	64	20	62	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0350h:	79	20	79	6F	67	65	73	68	29	0A	00	00	00	00	00	00	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0360h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

```
/dev/disk1s5 on / (apfs, local, read-only, journaled)
devfs on /dev (devfs, local, nobrowse)
/dev/disk1s1 on /System/Volumes/Data (apfs, local,
journaled, nobrowse)
/dev/disk1s4 on /private/var/vm (apfs, local,
journaled, nobrowse)
map auto_home on /System/Volumes/Data/home (autoofs,
automounted, nobrowse)
map -fstab on /System/Volumes/Data/Network/Servers
(autoofs, automounted, nobrowse)
/dev/disk1s6 on /Volumes/mangal (apfs, local,
journaled)
/dev/disk2s1 on /Volumes/mario (apfs, local,
journaled)
/dev/disk5s1 on /Volumes/luigi (apfs, local,
journaled)
/dev/disk0s6 on /Volumes/spare (exfat, asynchronous,
local, noowners)
/dev/disk3s1 on /Volumes/extra (apfs, local,
journaled)
/dev/disk4s1 on /Volumes/enc (apfs, local, journaled)
/dev/disk6s1 on /Volumes/Hex Fiend 2.8 (hfs, local,
nodev, nosuid, read-only, noowners, quarantine,
mounted by yogesh)
```

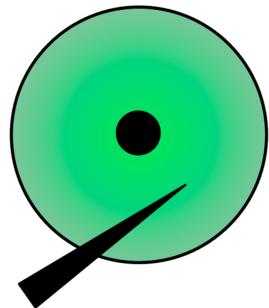
# Image a T2 mac's SSD with Target Disk Mode

- Restart the computer you want to image in Target Disk Mode by holding **T** during boot
- Connect examiner mac to the target mac using Thunderbolt USB-C cable
- All disks on the target should now be accessible on examiner's mac

Caveat – Use a disk arbitration program to turn off automatic mounting as RW



# Disk-Arbitrator tool



Screenshot of a GitHub repository page for "aburgh/Disk-Arbitrator: A Mac OS X forensic utility which manages file system mounting in support of forensic procedures." The page shows 226 commits, 1 branch, 0 packages, 13 releases, 6 contributors, and BSD-3-Clause license.

The GitHub interface includes a navigation bar with Home, GitHub, and a search bar for "github.com/aburgh/Disk-Arbitrator". Below the navigation bar are buttons for Watch (38), Star (469), Fork, and a pull request counter (31). The main content area displays the project's description, commit history, branches, releases, contributors, and a "Clone or download" button.

On the right side of the image, a screenshot of the "Disk Arbitrator" application window is shown. The window title is "Disk Arbitrator". It features four buttons: "Info" (blue circle with an "i"), "Eject" (blue circle with a downward arrow), "Mount" (blue circle with an upward arrow), and "Attach" (white square with a green circular icon). Below these buttons is a table titled "Media Description" with two columns: "Media Description" and "Device". The table lists nine entries:

Media Description	Device
92.05 GB AppleAPFSMedia	disk4
92.05 GB extra	disk4s1
199.76 GB AppleAPFSMedia	disk5
199.76 GB Macintosh HD - Data	disk5s1
199.76 GB Preboot	disk5s2
199.76 GB Recovery	disk5s3
199.76 GB VM	disk5s4
199.76 GB Macintosh HD	disk5s5
199.76 GB mangal	disk5s6

At the bottom of the Disk Arbitrator window, there are two buttons: "Activated" (checked) and "Mode: Read-only" with a dropdown arrow.

# Can we boot into Linux Forensic Boot distro?

- Pre-T2 no issues
  - CAINE, DEFT ZERO, KALI, PALADIN, ..
- With T2 and NVMe SSD
  - *Secure Boot* needs to be disabled
  - NVMe kernel driver that works with T2 macs is now available
    - But no known (forensics) distros have this implemented yet!
  - Fusion disks can't be read!
  - **Won't be able to decrypt encrypted disks!**

This  
approach  
won't work  


# Creating your own macOS forensic boot disk

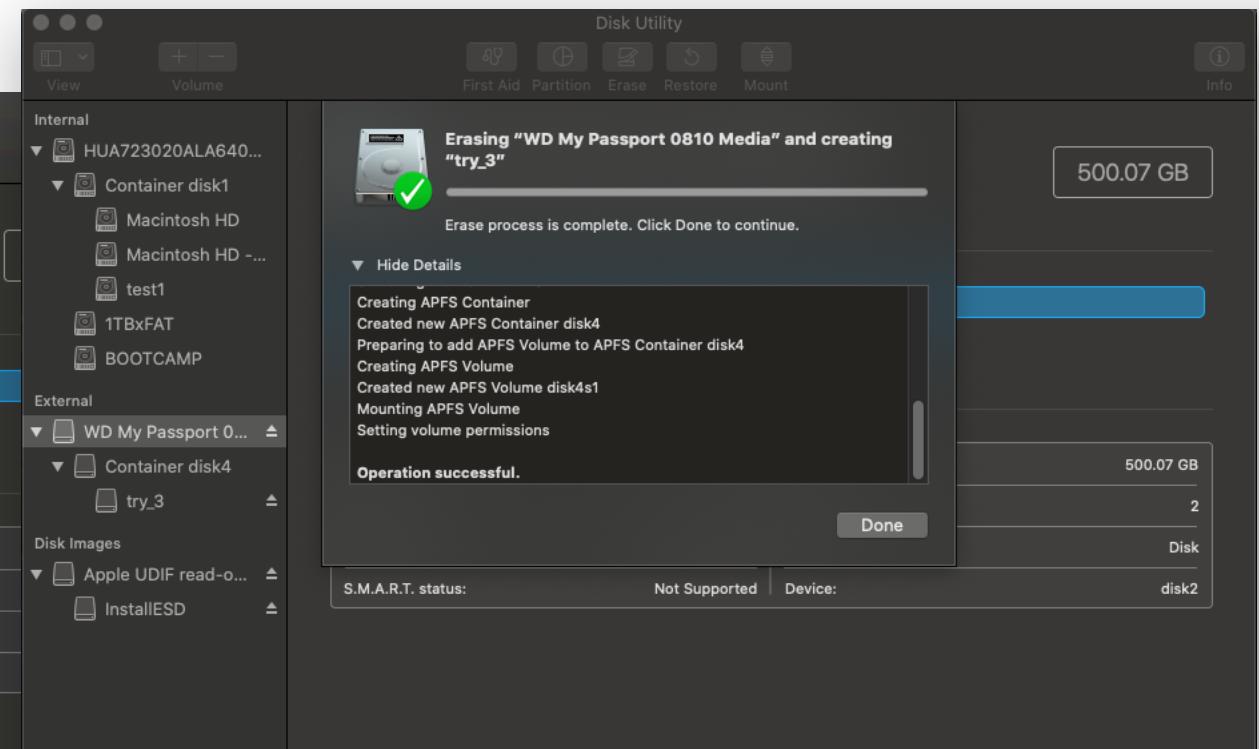
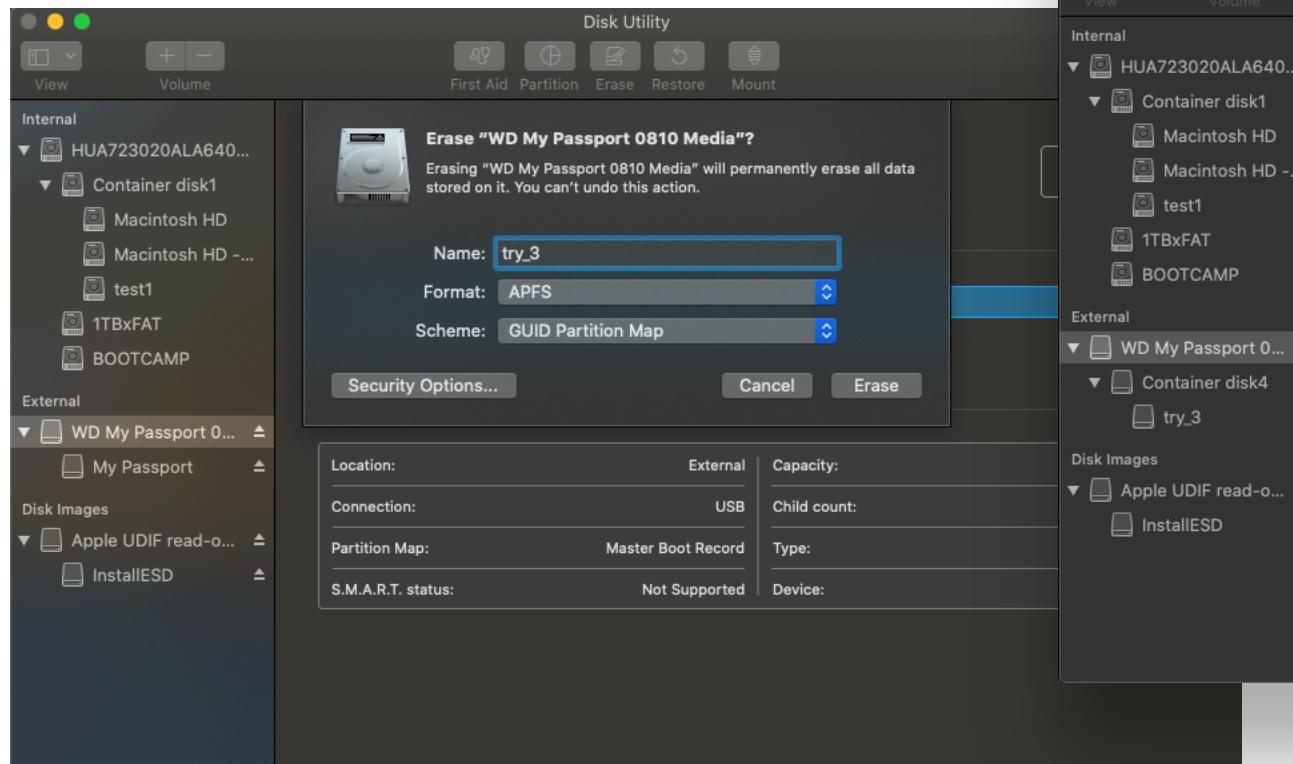
- Requirements
  - macOS Installer for 10.15
  - For Catalina (10.15) - Min 32GB external disk (SSD preferred)
  - Disk Arbitration program to prevent automating RW mounting of disks



# Step 1 - Setting up your external disk



- 1 Start Disk Utility
- 2 Select Disk on left
- 3 Click Erase



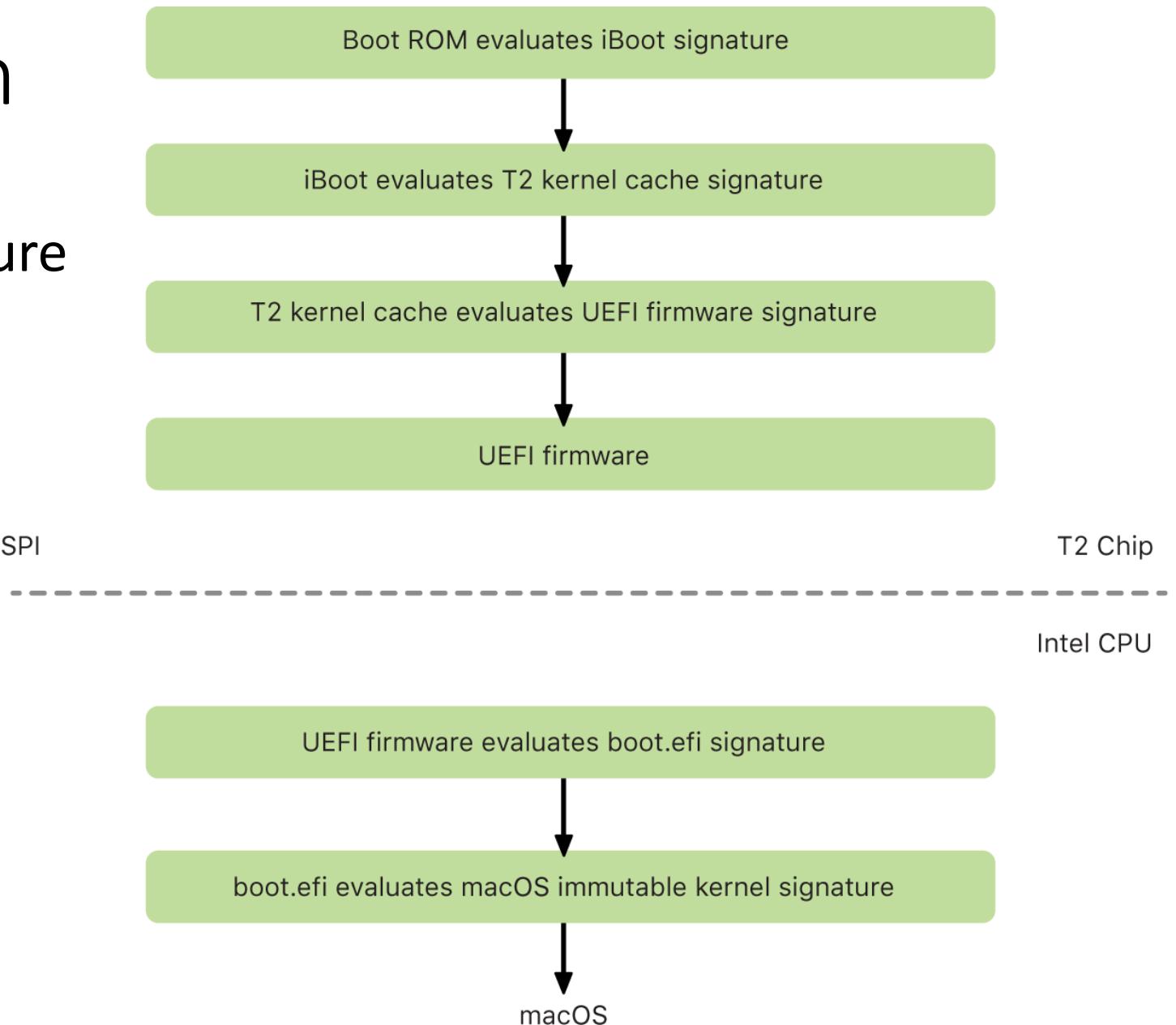
- 1 Start Disk Utility
- 2 Select Disk on left
- 3 Click Erase
- 4 Set Scheme to GUID Partition Map and Format to APFS

# Step 2 - Installing macOS on external disk



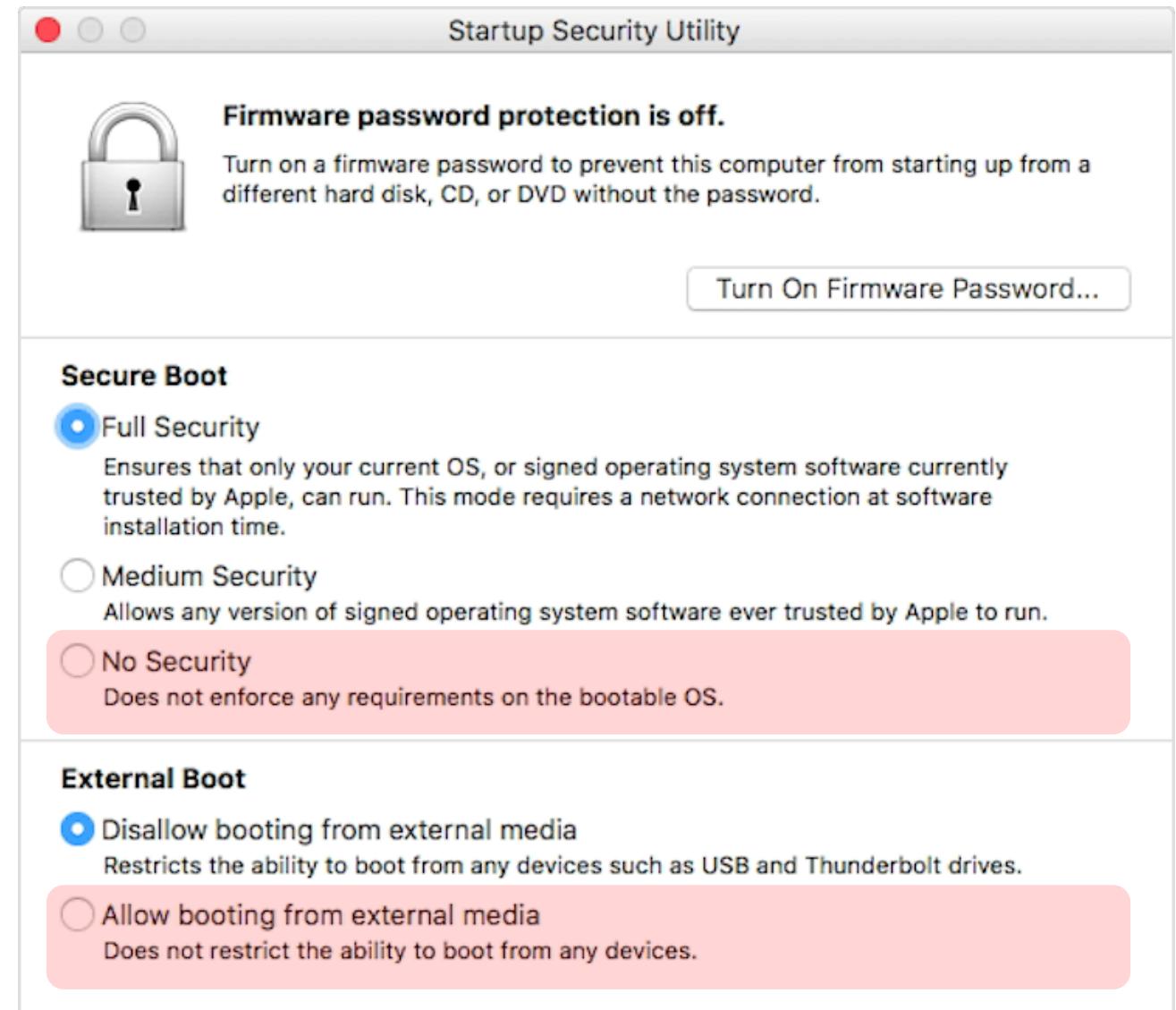
# Secure Boot chain

On error or Verification failure  
this will boot into  
macOS Recovery Mode



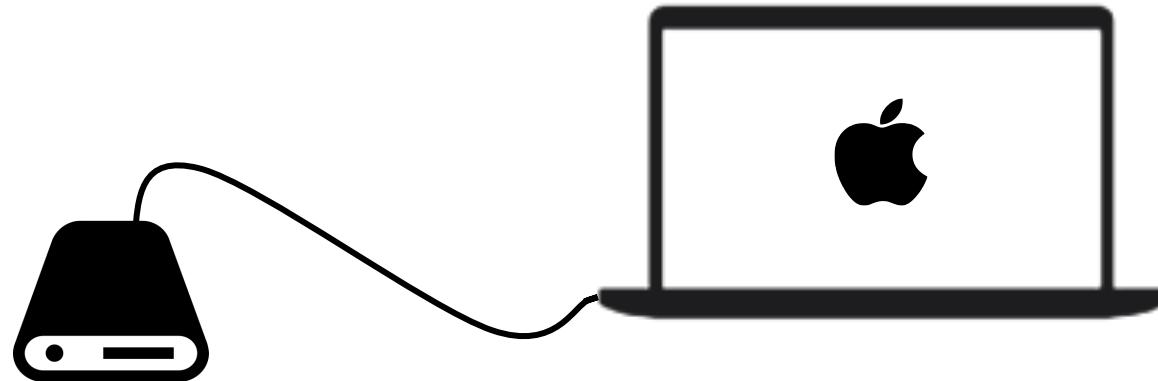
# Go to Recovery Mode

- To access this menu, boot the computer holding keys **Command (⌘)** and **R** together
- Then choose from menu Utilities → Startup Security Utility



# Booting into your external disk

1. Connect the disk



2. Boot the computer holding down the **Option** key



3. Select the external disk when asked



# Blocking disk mounts for Internal disks

- Disk-Arbitrator does not block internal disks at boot
- So.. we wrote our own *disk\_block\_daemon*
  - Uses Disk Arbitration Framework
  - Runs as root
  - Blocks all internal disk from mounting
    - *Explicit mounts using ‘sudo mount’ are still allowed*
    - [https://github.com/ydkhatri/macOS\\_FE/NoMountDaemon](https://github.com/ydkhatri/macOS_FE/NoMountDaemon)



Caveat – This is *NOT* a full proof method of preventing disks from mounting at boot! There are conditions under which this may fail.

# disk\_block\_daemon – compile

## To compile and set as service

```
clang -Wall -Werror -g -v stop_mounts.m -lobjc -framework  
DiskArbitration -framework Foundation -o stop_mount
```

## Change permissions so anyone can execute

```
chmod +x stop_mount
```

## Rename and copy to /usr/local/bin

```
cp stop_mount /usr/local/bin/disk_block_daemon
```

## Copy the plist to /Library/LaunchDaemons/

```
cp com.swiftforensics.diskblock.plist /Library/LaunchDaemons/
```



# LaunchDaemon configuration

```
$ plutil -p com.swiftforensics.diskblock.plist
{
    "Label" => "com.swiftforensics.diskblock"
    "ProgramArguments" => [
        0 => "/usr/local/bin/disk_block_daemon"
    ]
    "RunAtLoad" => 1
    "StandardErrorPath" => "/tmp/diskblock.err.log"
    "StandardOutPath" => "/tmp/diskblock.out.log"
    "UserName" => "root"
}
```

# disk\_block\_daemon *in action*

The image shows two terminal windows side-by-side. The top window has a title bar "admin — zsh — 124x34". It displays disk information for two volumes:

	Type	Name	Size	Identifier
#: 0:	APFS Container Scheme -		+10.0 GB	disk3
		Physical Store disk0s5		
1:	APFS Volume enc		4.9 MB	disk3s1

**/dev/disk4 (synthesized):**

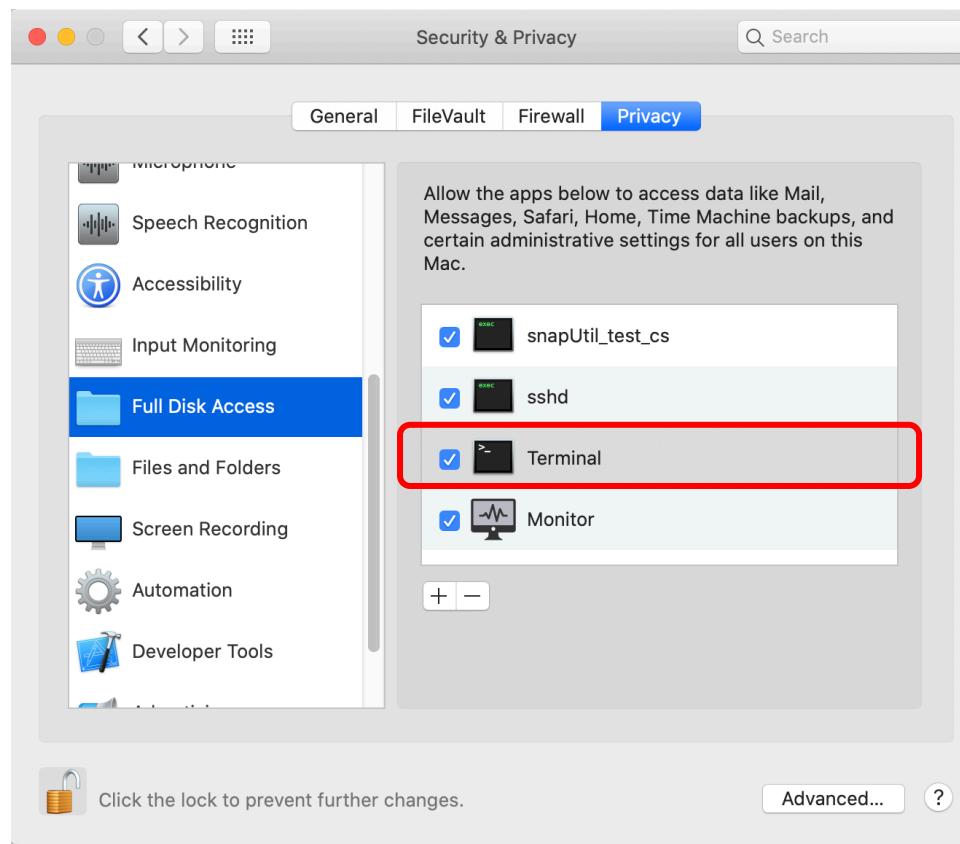
	Type	Name	Size	Identifier
#: 0:	APFS Container Scheme -		+92.0 GB	disk4
		Physical Store disk0s4		
1:	APFS Volume extra		2.4 MB	disk4s1

The bottom window has a title bar "admin — zsh — 124x19". It shows the command "diskutil mount disk4s1" failing with the error "Volume on disk4s1 failed to mount: \"Internal disks can't be mounted!\"". When run with sudo, it fails again with the same error.

```
[admin@admins-MacBook-Pro ~ % diskutil mount disk4s1
Volume on disk4s1 failed to mount: "Internal disks can't be mounted!"
[admin@admins-MacBook-Pro ~ % sudo diskutil mount disk4s1
Volume on disk4s1 failed to mount: "Internal disks can't be mounted!" ] I
admin@admins-MacBook-Pro ~ % ]
```

# Allow Terminal full disk access

System Preferences → Security & Privacy



# Other tools

- <https://naarakstudio.com/direqual/>
- <https://apps.apple.com/us/app/direqual/id1435575700?mt=12>



## DirEqual

Compare Folders

Grzegorz Staszczyk

4.8 ★★★★★

13 Ratings

The screenshot shows the DirEqual application window titled "DIREQUAL". It displays a comparison between two folders: "Left: /Volumes/Backup/Stare Projekty/DirEqual/DirEqual173" and "Right: /Volumes/Backup/Stare Projekty/DirEqual/DirEqual170". The left pane shows the contents of the first folder, and the right pane shows the contents of the second. A summary at the top right indicates "50 folders compared" and lists the total byte count and file counts for both sides. The main area is a table with columns for Name, Size, Date, and a comparison column (<>). The comparison column uses icons to indicate differences: blue for identical files, red for different files, and grey for files only in one folder. The application has a clean, modern design with a dark background and light-colored text.

DirEqual173 vs DirEqual170

Left: /Volumes/Backup/Stare Projekty/DirEqual/DirEqual173 Right: /Volumes/Backup/Stare Projekty/DirEqual/DirEqual170

Show:  Identical  Different  Only in left folder  Only in right folder  Color backgrounds Compare: All files  Compare file contents  Ignore dates  Compare subfolders  Include empty folders

Left: 1173 800 bytes, 104 files and 24 folders Right: 1120 157 bytes, 100 files and 24 folders

50 folders compared

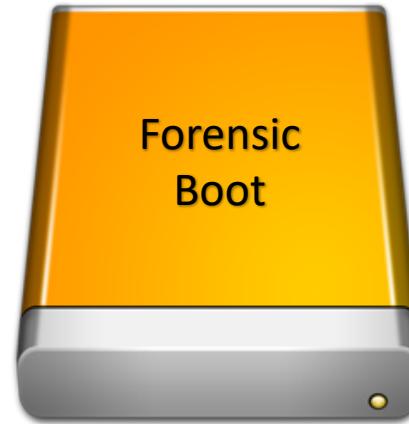
The folders differ

Name	Size	Date	<>	Date	Size	Name
Assets.xcass...	328 521 bytes	16/04/2019, 07:52:41		12/04/2019, 17:11:13	328 521 bytes	Assets.xcass...
Base.iproj	185 347 bytes	17/05/2019, 06:36:34		12/04/2019, 17:11:13	186 672 bytes	Base.iproj
DirEqual AS....	311 bytes	07/09/2018, 16:22:35		07/09/2018, 16:22:35	311 bytes	DirEqual AS....
DirEqual.entit...	252 bytes	12/04/2019, 17:14:28		12/04/2019, 17:14:28	252 bytes	DirEqual.entit...
DirEqual.xco...	406 665 bytes	17/05/2019, 07:01:17		14/04/2019, 11:22:10	361 527 bytes	DirEqual.xco...
DirEqualF	123 726 bytes	17/05/2019, 06:47:49		12/04/2019, 17:11:13	117 357 bytes	DirEqualF
Base.iproj	9 729 bytes	12/04/2019, 10:23:10		12/04/2019, 10:23:10	9 729 bytes	Base.iproj
h DirEqualF.h	524 bytes	15/04/2019, 11:52:47		08/04/2019, 12:57:17	521 bytes	h DirEqualF.h
m DirEqualFil...	14 667 bytes	16/05/2019, 07:30:40		12/04/2019, 11:54:22	14 561 bytes	m DirEqualFil...
h DirEqualM...	3 220 bytes	16/05/2019, 07:50:20		12/04/2019, 11:54:35	3 141 bytes	h DirEqualM...
m DirEqualM...	34 484 bytes	17/05/2019, 06:43:17		12/04/2019, 12:06:39	36 835 bytes	m DirEqualM...
m DirEqualO...	13 220 bytes	17/05/2019, 06:47:49		09/04/2019, 12:11:58	12 730 bytes	m DirEqualO...
Info.plist	835 bytes	16/05/2019, 11:07:21		08/04/2019, 12:48:36	835 bytes	Info.plist
h LBProgres...	1 312 bytes	15/04/2019, 12:05:48		04/01/2019, 06:17:27	1 310 bytes	h LBProgres...
m LBProgres...	11 108 bytes	15/04/2019, 12:05:48		04/01/2019, 06:17:27	11 102 bytes	m LBProgres...
h NCenterin...	595 bytes	25/10/2018, 11:31:51		25/10/2018, 11:31:51	595 bytes	h NCenterin...

QUICKLY COMPARE MAC FOLDERS

# macOS tools for imaging and analysis

- asr
- diskutil
- hdiutil
- mount & umount
- tmutil



✓ Our macOS Forensic Boot Disk is ready to use!

Listing Disks & unlocking  
encrypted volumes – demo

# T2 APFS Imaging

```
>_
hdiutil
```

create →

DMG



attach ↓



DISK/Volume  
to image



↑ read

```
>_
asr
```

← write

Caution – Be careful when running ASR. It has the same potential as DD to ruin disks if incorrect commands are entered.

# Final disk image (DMG)



## Included

- All logical disk content
  - All XATTR
- All timestamps as original
- Same inode numbers (File Id) as source disk

## Excluded

- Unallocated space
- Snapshots
  - However, snapshots can be imaged as entire new disk images

# Demo!

- Imaging
- Snapshot analysis

>\_

```
$ sudo launchctl unload /System/Library/LaunchDaemons/com.apple.revisiond.plist  
/System/Library/LaunchDaemons/com.apple.revisiond.plist: Operation now in progress
```

```
$ sudo launchctl unload /System/Library/LaunchDaemons/com.apple.revisiond.plist  
/System/Library/LaunchDaemons/com.apple.revisiond.plist: Could not find specified service
```

*Do this on every boot*

Imaging a disk/volume - demo

# Imaging the container with macOS

1. Mount external disk/volume (that's where image will be written)
  2. Creating DMG and attaching it..

# Imaging the container with macOS

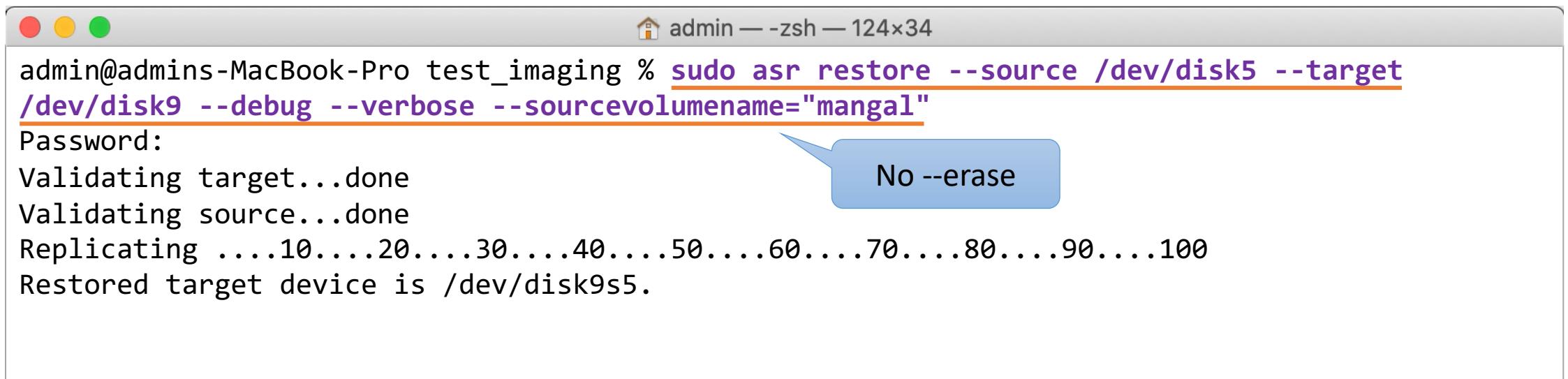
## 3. Create image with `asr`

```
admin@admins-MacBook-Pro test_imaging % sudo asr restore --source /dev/disk5 --target /dev/disk9 --debug --erase --verbose
Validating target...done
Validating source...
Source "/dev/disk5" contains multiple system/data volumes.
You must pass --sourcevolumename or --sourcevolumeUUID to specify which volume to restore.
Could not validate source - Invalid argument

admin@admins-MacBook-Pro test_imaging % sudo asr restore --source /dev/disk5 --target /dev/disk9 --debug --erase --verbose --sourcevolumename="Macintosh HD"
Validating target...done
Validating source...done
Erase contents of /dev/disk9 ()? [ny]: y
Replicating ....10....20....30....40....50....60....70....80....90....100
Replicating ....10....20....30....40....50....60....70....80....90....100
Restored target device is /dev/disk9s1.
```

# Imaging the container with macOS

## 4. Add the other volumes to this container – ‘mangal’



The screenshot shows a macOS terminal window with the following details:

- Window title bar: admin — -zsh — 124x34
- User: admin@admins-MacBook-Pro test\_imaging %
- Command: `sudo asr restore --source /dev/disk5 --target /dev/disk9 --debug --verbose --sourcevolumename="mangal"`
- Text output:
  - Password: (followed by a blue speech bubble containing "No --erase")
  - Validating target...done
  - Validating source...done
  - Replicating ....10....20....30....40....50....60....70....80....90....100
  - Restored target device is /dev/disk9s5.

Verifying image contents - demo

# Accessing snapshots

- Volume must be mounted (can be read-only)
- Listing them out
  - `tmutil listlocalsnapshots <mountpoint>`
  - `diskutil apfs list snapshots`
- Mounting snapshots
  - `mount_apfs -s <snapshot> <volume | device> <directory>`

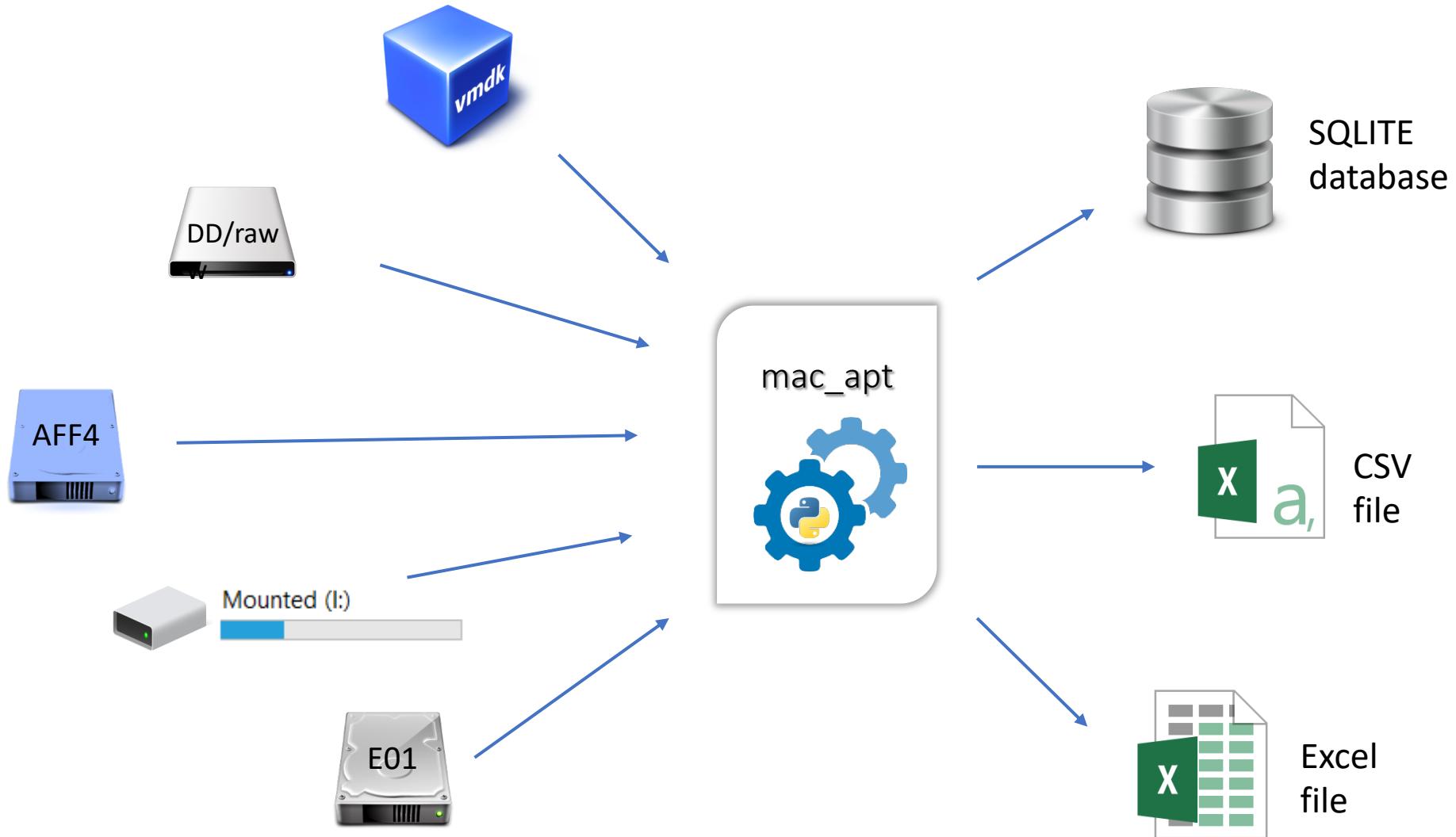


Currently mounted volume (/dev/disk2s1) or its mountpoint (/Volumes/Bob)

Folder to mount snapshot

# Snapshots - demo

# mac\_apt - Input & output types



# Scenario

- Investigators have been on a case of passport theft or forgery across New England
- Investigators intercept a suspicious transaction and confiscate a live Macintosh computer
- Traces of the passport information in the computer.
- Contact between the suspect and other individuals; sharing the information.
- Relevant locations, meeting points, or contact information.

Running mac\_apt (video)

# Plugins

FAST:

- APPS
- AUTOSTART
- **BASH\_SESSIONS**
- **BASIC\_INFO**
- COOKIES
- DOCK\_ITEMS
- FS\_EVENTS
- **IMESSAGE**
- INTERNET\_ACCOUNTS
- **INSTALLHISTORY**

- NETUSAGE
- NETWORKING/WIFI
- **NOTES**
- QUARANTINE
- QUICKLOOK
- **RECENT\_ITEMS**
- **SAFARI**
- SCREENTIME
- SPOTLIGHTSHORTCUTS
- **TERMINALSTATE**
- **USERS**

# Reading the Output (live)

# Basic Info Output

Table: Basic_Info			
INFO_TYPE	Name	Data	Description
1 SYSTEM	macOS Version	10.15.1	Catalina
2 SYSTEM	macOS Build Version	19B88	Catalina
3 HARDWARE	Mac Serial Number	VMEBHcciB7Au	Hardware Serial Number
4 HARDWARE	Model	VMware7,1	Mac Hardware Model
5 SYSTEM	ComputerName	experimental's Mac	
6 SYSTEM	LocalHostName	experimental-Mac	
7 TIMEZONE	TimeZone Set	America/New_York	Timezone on machine
8 USER-LOGIN	lastUser	Restart	Last user (Login) Action
9 USER-LOGIN	lastUserName	experimental	
10 USER-LOGIN	UseVoiceOverLegacyMigrated	True	unknown
11 USER-LOGIN	lastLoginPanic	2020-05-10 10:50:02.755967	
12 APFS	Information		Data below represents a combined SYSTEM + DATA
13 APFS	Block Size (bytes)	4096	Container Block size
14 APFS	Container Size (GB)	39.68	Container size (SYSTEM + DATA)
15 APFS	Volume Name	Macintosh HD,Macintosh HD - Data	Volume names (SYSTEM, DATA)
16 APFS	Volume UUID	CE465AAC-A681-4DD3-A0D7-6D3C...	Volume Unique Identifiers (SYSTEM, DATA)
17 APFS	Size Used (GB)	26.58	Space allocated (SYSTEM + DATA)

# Recent Items

Table: RecentItems		
Type	Name	URL
Filter	Filter	Filter
22	SSH_KNOWN... 216.93.152.89	

# Net Usage

A	B	C	D
1	Type	Name	FirstSeenDate
79	Process	sharingd	2/19/2020 11:54
80	Process	softwareupdated	11/15/2019 19:17
81	Process	ssh	5/7/2020 6:20
82	Process	studentd	2/19/2020 10:44
83	Process	swcd	11/15/2019 19:21
84	Process	syncdefaultsd	2/19/2020 11:54
85	Process	syspolicyd	11/15/2019 19:17
			5/9/2020 17:26
			5/6/2020 3:00
			5/5/2020 17:35
			5/9/2020 15:59
			5/9/2020 15:51

# TerminalState

- Reads Terminal saved state files which includes full text content of terminal window(s)
- Shows SCP file transferring and file-reading

```
experimental@experimentals-Mac ~ % history
97 vim startupscript.sh
98 cp startupscript.sh setupKali.sh
99 rm startupscript.sh
100 cat setupKali.sh
101 cp setupKali.sh setupKali.app
102 echo "Hello"
103 pwd
104 ls -la
105 pwd
106 ifconfig
107 scp root@216.93.152.89:/home/temporary/passds.txt /Users/experimental/Desktop/
108 cat /Users/experimental/Desktop/passds.txt
109 cd ~/Downloads
110 ls -la
111 scp untitled\ \(1\).csv root@216.93.152.89:/home/temporary/
112 ssh root@216.93.152.89
```

OK, we got lucky here,  
(user had printed out his  
own history!) This  
happens sometimes!

```
experimental@experimentals-Mac Downloads % cat ..//Desktop/passds.txt
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftnp:x:14:50:FTP User:/var/ftp:/sbin/nologin
```

```
experimental@experimentals-Mac Downloads % scp untitled\ \(1\).csv root@216.93.152.89:/home/
temporary/
root@216.93.152.89's password:
untitled (1).csv                                100% 699  844.8KB/s  00:00
experimental@experimentals-Mac Downloads % scp untitled\ \(2\).csv root@216.93.152.89:/home/
temporary/
root@216.93.152.89's password:
untitled (2).csv                                100% 566   38.2KB/s  00:00
```

```
experimental@experimentals-Mac Downloads % cat "untitled (1).csv"
QW5ndXMgUG93ZXI=,MTAyOTkU0,20-Apr-69,TQ==69,Rg==
```

# TerminalState

- SSH activity

```
experimental@experimentals-Mac Downloads % ssh root@216.93.152.89
root@216.93.152.89's password:
Last login: Fri May  8 15:44:25 2020 from 134-152.champlain.edu
[root@62-152 ~]# rm /home/temporary/untitled\ \(1\).csv
rm: remove regular file '/home/temporary/untitled (1).csv'? yes
[root@62-152 ~]# exit
logout
Connection to 216.93.152.89 closed.

experimental@experimentals-Mac Downloads % ssh root@216.93.152.89 mysqldump -u root -p secrets
> data-dump.sql ; cat data-dump.sql | tail -n 20
root@216.93.152.89's password:
Enter password: 2616
--
-- Dumping data for table `passpts`
--

LOCK TABLES `passpts` WRITE;
/*!40000 ALTER TABLE `passpts` DISABLE KEYS */;
INSERT INTO `passpts` VALUES (1,'Sameeha Cullen','J83421ef8','2000-01-02'),(2,'Omar Pearce','N88890D81','1992-04-03'),(3,'Jamie Carty','DF282BC9e','1961-03-05'),(4,'Sofie Forster','N78Vf6789','1968-02-18'),(5,'Hallie Colley','J823F5G78','1982-03-25'),(6,'Kyra Ross','K177M3P72','1988-08-17'),(7,'Amelia-Rose Petty','C0K4ND847','1993-09-12'),(8,'Rico Squansonson','9USS8A772','1989-10-10'),(9,'Shivani Steele','M07H3RC47','1955-11-12');
/*!40000 ALTER TABLE `passpts` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
```

# iMessage Data

MsgID	Text	versa	Contact	irectic	Account	Date	AttachmentPath
	Filter		Filter		Filter	Filter	Filter
9	Are you receiving my the file?	1	chrissaustin3c@gmail.com	—	e:janesmithmacfor@icloud.com	2020-05-07 01:51:46.434342	/Volumes/TEST/untitled (1).csv
10		1	chrissaustin3c@gmail.com	—	e:janesmithmacfor@icloud.com	2020-05-07 01:51:34.321000	NULL
11		1	chrissaustin3c@gmail.com	—	e:janesmithmacfor@icloud.com	2020-05-07 02:14:33.042905	/Volumes/TEST/untitled (1).csv
12	Hey Jane, this is Hazel	2	hazelhill010@icloud.com	—	e:janesmithmacfor@icloud.com	2020-05-08 16:36:44.388566	NULL
13	Hello hazel, I'm having trouble reaching Chris, can I forward you the file to decode for me?	2	hazelhill010@icloud.com	—	e:janesmithmacfor@icloud.com	2020-05-08 16:37:41.518922	NULL
14	Surely	2	hazelhill010@icloud.com	—	e:janesmithmacfor@icloud.com	2020-05-08 16:37:50.304400	NULL
15		2	hazelhill010@icloud.com	—	e:janesmithmacfor@icloud.com	2020-05-07 03:47:20.958276	/Volumes/TEST/untitled (1).csv
16	It doesn't seem to be going through, ill try to email it	2	hazelhill010@icloud.com	—	e:janesmithmacfor@icloud.com	2020-05-08 16:43:21.581000	NULL
17	K	2	hazelhill010@icloud.com	—	e:janesmithmacfor@icloud.com	2020-05-08 16:44:44.561443	NULL
18		2	hazelhill010@icloud.com	—	e:janesmithmacfor@icloud.com	2020-05-08 16:55:24.731872	~/Library/Messages/Attachments/...
19	This one?	2	hazelhill010@icloud.com	—	e:janesmithmacfor@icloud.com	2020-05-08 16:55:41.682888	NULL
20	Yes	2	hazelhill010@icloud.com	—	e:janesmithmacfor@icloud.com	2020-05-08 16:55:44.897000	NULL
21	I can't send files, I will attach text of it here and email you the file	2	hazelhill010@icloud.com	—	e:janesmithmacfor@icloud.com	2020-05-08 16:56:10.236733	NULL
28	I found more data!	2	hazelhill010@icloud.com	—	e:janesmithmacfor@icloud.com	2020-05-09 07:00:17.513000	~/Library/Messages/Attachments/...
29	Are you ready for tomorrow?	2	hazelhill010@icloud.com	—	e:janesmithmacfor@icloud.com	2020-05-10 06:15:51.013955	NULL
30	Yeah, same place as last time?	2	hazelhill010@icloud.com	—	e:janesmithmacfor@icloud.com	2020-05-10 06:16:42.569000	NULL
31	Centennial — yes	2	hazelhill010@icloud.com	—	e:janesmithmacfor@icloud.com	2020-05-10 06:16:57.837042	NULL
32	12pm	2	hazelhill010@icloud.com	—	e:janesmithmacfor@icloud.com	2020-05-10 06:23:35.160071	NULL
33	The best I can do is 1:30, its a long drive from boston and I don't want to wake up any earlier than 10	2	hazelhill010@icloud.com	—	e:janesmithmacfor@icloud.com	2020-05-10 06:24:44.101000	NULL

# Notes

Table: Notes Filter Sort Ascending Sort Descending Print

ID	Title	Snippet	Folder	Created	LastModified	Data	Edit
...	Filter	Filter	Filter	Filter	Filter	Filter	Mode: Text
1 9	iCloud note	This note i...	Notes	2019-10-17 03:54:20....	2019-10-17 03:54:35....	iCloud noteThis note is stored on the iCloud	<span>Text</span> <span>Code</span> <span>Table</span>
2 13	Shopping list	Milk	Notes	2020-02-19 11:56:40....	2020-02-19 11:59:10....	Shopping listMilk	<span>Text</span> <span>Code</span> <span>Table</span>
3 14	Contacts	John Smith	Notes	2020-02-19 11:59:23.747272	2020-02-19 12:11:22.091352	Contacts John Smith(656) 825-9574	<span>Text</span> <span>Code</span> <span>Table</span>
4 15	New Note	NULL	Notes	2020-05-09 15:28:56....	2020-05-09 15:28:56....		<span>Text</span> <span>Code</span> <span>Table</span>
5 25	Directions		Notes	2020-05-09 15:29:15....	2020-05-09 15:29:15....	Directions	<span>Text</span> <span>Code</span> <span>Table</span>

Contacts  
John Smith  
(656) 825-9574  
7671 Dolor Rd.  
5324271549450208

Alice Bobdale  
(226) 162-6300  
80 Rhoncus St.  
554 29602 86115 372

# Safari

Type	Name_or_Title	URL	Date
Filter	Filter	Filter	Filter
335 HISTORY	Google Maps	<a href="https://www.google.com/maps">https://www.google.com/maps</a>	2020-05-09 15:37:50....
336 HISTORY	The Andi Apartments to Centennial Woods Natural Area - Google Maps	<a href="https://www.google.com/maps/place/The+andi+apartments/@40.08111,-75.12111,15z">https://www.google.com/maps/place/The+andi+apartments/@40.08111,-75.12111,15z</a>	2020-05-09 15:37:50....
337 HISTORY	The Andi Apartments to Centennial Woods Natural Area - Google Maps	<a href="https://www.google.com/maps/place/The+andi+apartments/@40.08111,-75.12111,15z">https://www.google.com/maps/place/The+andi+apartments/@40.08111,-75.12111,15z</a>	2020-05-09 15:37:53....
338 HISTORY	The Andi Apartments to Centennial Woods Natural Area - Google Maps	<a href="https://www.google.com/maps/place/The+andi+apartments/@40.08111,-75.12111,15z">https://www.google.com/maps/place/The+andi+apartments/@40.08111,-75.12111,15z</a>	2020-05-09 15:38:01....
339 HISTORY	Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs & more.	<a href="https://www.amazon.com/">https://www.amazon.com/</a>	2020-05-09 15:38:45....
350 HISTORY	Amazon.com: Deftun Mag Card Reader Writer Compare with MSR605X For Windows and Mac OS: Computers & Accessories	<a href="https://www.amazon.com/Deftun-Mag-Card-Reader-Writer/dp/B08HJZPQK5">https://www.amazon.com/Deftun-Mag-Card-Reader-Writer/dp/B08HJZPQK5</a>	2020-05-09 15:40:47.604028
351 HISTORY	Amazon.com: passport scanner: Electronics	<a href="https://www.amazon.com/Passport-Scanner/dp/B08HJZPQK5">https://www.amazon.com/Passport-Scanner/dp/B08HJZPQK5</a>	2020-05-09 15:41:28....
352 HISTORY	Amazon.com: passport scanner: Electronics	<a href="https://www.amazon.com/Passport-Scanner/dp/B08HJZPQK5">https://www.amazon.com/Passport-Scanner/dp/B08HJZPQK5</a>	2020-05-09 15:41:28....
353 HISTORY		<a href="https://www.amazon.com/">https://www.amazon.com/</a>	2020-05-09 15:41:45....
354 HISTORY	Amazon.com: Gemalto CR100M Document Passport Reader Scanner MRZ MRTDS USB: Electronics	<a href="https://www.amazon.com/Gemalto-CR100M-Document-Passport-Reader/dp/B08HJZPQK5">https://www.amazon.com/Gemalto-CR100M-Document-Passport-Reader/dp/B08HJZPQK5</a>	2020-05-09 15:41:45.371295
355 HISTORY	Amazon.com Shopping Cart	<a href="https://www.amazon.com/">https://www.amazon.com/</a>	2020-05-09 15:42:08....

# Thanks for watching!

## Any Questions?



Tools @ [https://github.com/ydkhatri/mac\\_apt](https://github.com/ydkhatri/mac_apt)  
[https://github.com/ydkhatri/macOS\\_FE](https://github.com/ydkhatri/macOS_FE)



@*swiftforensics*  
@*alex\_cart27*



Yogesh@*swiftforensics*.com  
Alexandra.cartwright@mymail.champlain.edu

# References

- About the Apple T2 Security Chip - <https://support.apple.com/en-us/HT208862>
- About encrypted storage on your new Mac - <https://support.apple.com/en-us/HT208344>
- Apple Platform Security Spring 2020 - <https://support.apple.com/guide/security/welcome/web>
- Apple T2 Security Chip - Security Overview - [https://www.apple.com/euro/mac/shared/docs/Apple\\_T2\\_Security\\_Chip\\_Overview.pdf](https://www.apple.com/euro/mac/shared/docs/Apple_T2_Security_Chip_Overview.pdf)
- Disk Arbitrator - <https://github.com/aburgh/Disk-Arbitrator>
- disk\_block\_daemon - [https://github.com/ydkhatri/macOS\\_FE/NoMountDaemon](https://github.com/ydkhatri/macOS_FE/NoMountDaemon)
- Mounting timemachine local Snapshots - <https://derflounder.wordpress.com/2019/02/23/mounting-time-machine-local-snapshots-as-read-only-volumes/>