Spotlight Lab (Cyber Defenders) - Walkthrough

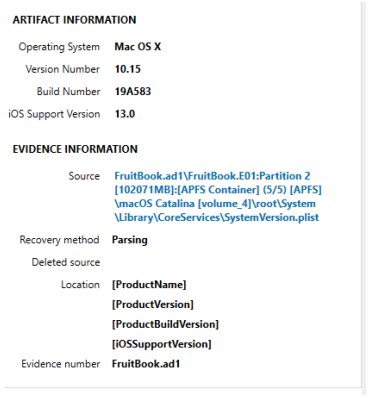
Wednesday, September 18, 2024 3:19 AM

Story:
Spotlight is a MAC OS image forensics challenge where you can evaluate your DFIR skills against an OS you usually encounter in today's case investigations as a security blue team member.

- I used Magnet AXOM to parse all the disk of the MacOS.

Q1: What version of macOS is running on this image?

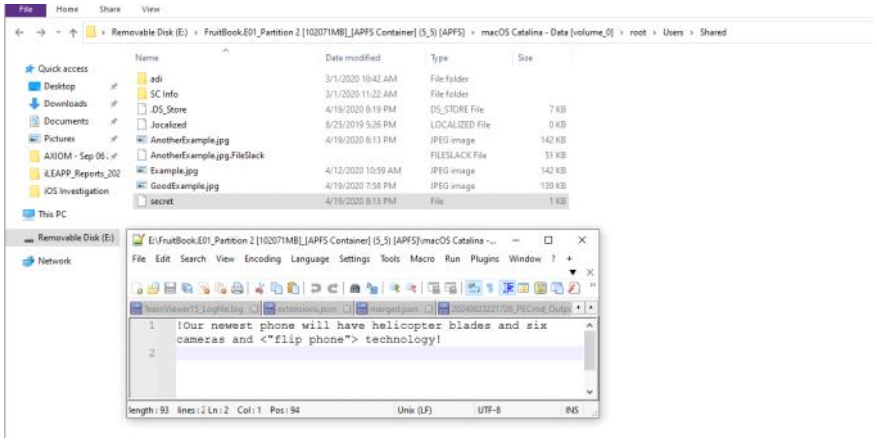
- In the 'Operation System' section, we able are to see the file '**SystemVersion.plist**' which located at \root\System\Library\CoreServices\SystemVersion.plist



Q2: What "competitive advantage" did Hansel lie about in the file AnotherExample.jpg? (two words)

- To address this question, I searched for the name of the JPG file in the file system and found several images in the '\root\Users\Shared' directory that appeared to be advertisements for winning a new phone.
  In the same folder, I discovered a file named 'secret,' which contained the answer: 'Flip Phone.'

  Note: In macOS, the \root\Users\Shared directory refers to the **Shared** folder, located at /Users/Shared. This folder is accessible to all users on the system and is commonly used for sharing files between different user accounts.



Q3: How many bookmarks are registered in safari?

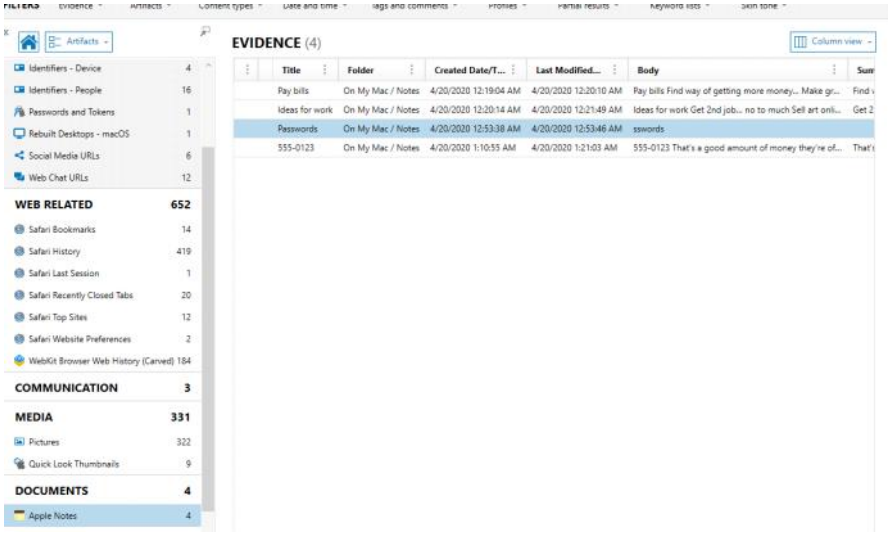
- In the 'Web Related' section, I identified the 'Safari Bookmarks' tab. Upon accessing it, I found all **13** of the user's bookmarks.
  The bookmarks are located at \root\Users\hansel.apricot\Library\Safari**Bookmarks.plist.**

URL	Title	Type	Read	Add...	L
https://www.apple.com/	Apple	Favorite			
https://www.icloud.com/	iCloud	Favorite			
https://www.yahoo.com/	Yahoo	Favorite			
https://www.bing.com/	Bing	Favorite			
https://www.google.com/?client=safari&channel=m...	Google	Favorite			
https://www.wikipedia.org/	Wikipedia	Favorite			
https://www.facebook.com/	Facebook	Favorite			
https://twitter.com/	Twitter	Favorite			
https://www.linkedin.com/	LinkedIn	Favorite			
https://www.weather.com/	The Weather Channel	Favorite			
https://www.yelp.com/	Yelp	Favorite			
https://www.tripadvisor.com/	TripAdvisor	Favorite			
https://mail.zoho.com/zm/#mail/folder/inbox	Inbox - Zoho Mail (hansel.apricot@fruitinc.xyz)	Favorite			

Q4: What's the content of the note titled "Passwords"?

- I found a note with the title 'Passwords', but the body of the message is missing.
  The database for the notes is located at root\Users\hansel.apricot\Library\Group Containers \group.com.apple.notes.
  I attempted to open the file manually using an SQLite database viewer, but it appeared empty.

  To address this issue, I tried using the MAC_apt tool with the Notes plugin.
  However, the file type .ad1 is not supported by the tool.
  Since the body of the note contains the word 'worrds', I suspect it might be '**passwords**'.



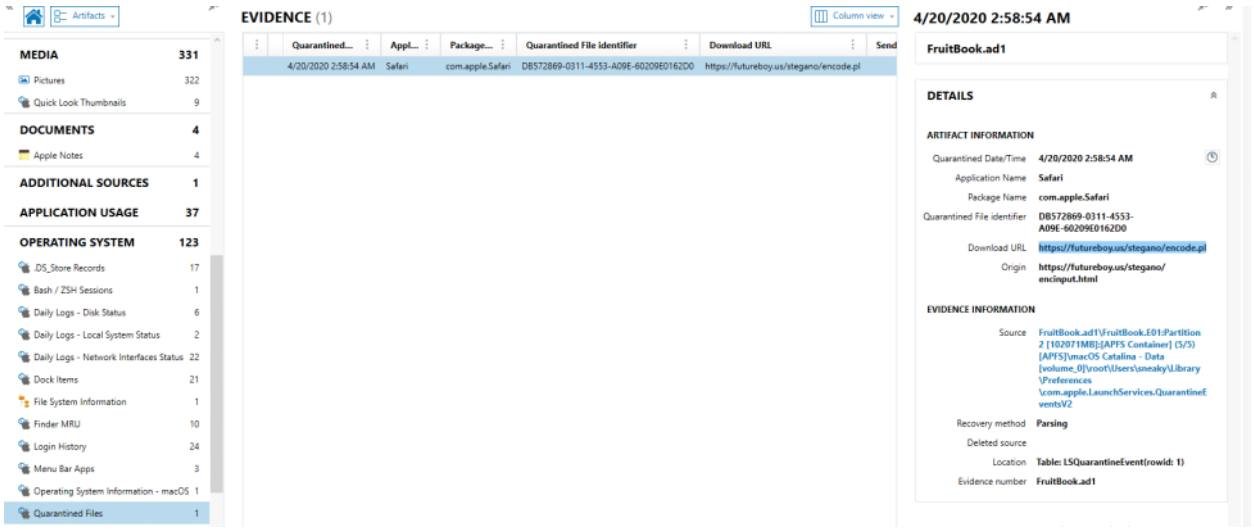
Q5: Provide the MAC address of the ethernet adapter for this machine.

- In the 'Operating System' section, I discovered the 'Network Interfaces Status'.
  Upon reviewing this section, I found the MAC address **00:0c:29:c4:65:77**, which is also recorded in the file located at **root\private\var\log\daily.out.**

  Note: The daily.out file in /private/var/log/ typically contains output from daily system maintenance tasks or scripts.
  If the MAC address appears in this file, it may be part of the routine logging of network activity or configurations.
  Checking this file can provide insights into network interface details and other system activities performed on a daily basis.

Q6: Name the data URL of the quarantined item.

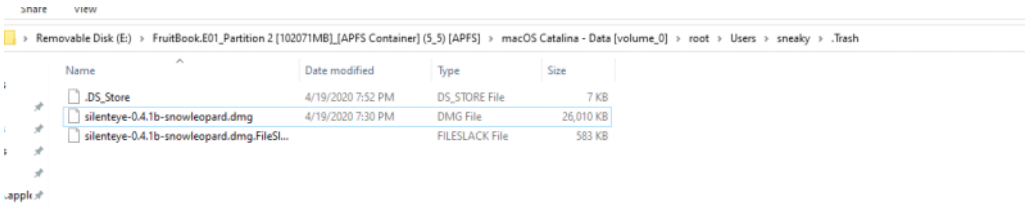
- In the 'Operating System' section, I discovered the 'Quarantined Files' section, which lists packages that have been quarantined by the system along with their download URLs.
  The relevant information is stored in the file located at root\Users\sneaky\Library\Preferences \com.apple.LaunchServices.QuarantineEventsV2.



Q7: What app did the user "sneaky" try to install via a .dmg file? (one word)

- While navigating the 'Sneaky' folder, I discovered a DMG file named silenteye-0.4.1b-snowleopard.dmg located in the .
  Trash directory. This file is associated with the **SilentEye** application.

  Note: A .dmg (Disk Image) file is a versatile file format used on macOS for various purposes, primarily involving the distribution and installation of software.



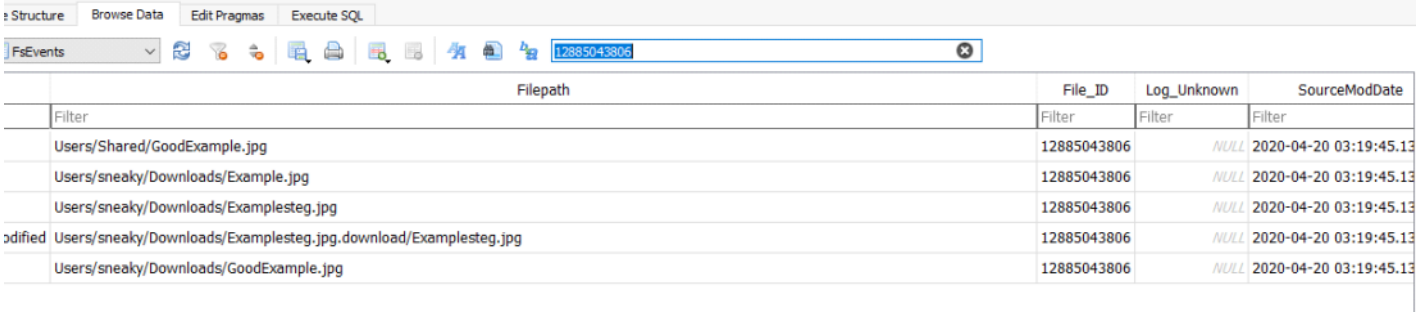
Q8: What was the file 'Examplesteg.jpg' renamed to?

To address this issue, I used the first hint, which suggested checking the fseventsd database located at /root/fseventsd/ for file renaming logs.
After reviewing 'Mac_apt,' I found a relevant plugin called 'FSEVENTSa' that parses these logs. I executed the following command:

python mac_apt_artifact_only.py -i"E:\FruitBook.E01_Partition 2 [102071MB]_[APFS Container] (5_5) [APFS]\macOS Catalina - Data [volume_0]\root\.fseventsd" -o . FSEVENTS

This produced a database file containing the log information.
I opened the database using SQLite and searched for the filename 'Examplesteg.jpg.' Several logs were related to this file, and I identified its File ID as '12885043806.' Upon searching this ID, I discovered that the file had been renamed to 'GoodExample.jpg.'

Note: FSEvents files are written to disk by macOS APIs and contain historical records of file system activity that occurred for a particular volume.



```
LARE-VM Wed 09/18/2024  3:57:32.75
:\Users\FlareVM\Desktop\iOS Investigation\mac_apt-master>python mac_apt_artifact_only.py -i"E:\FruitBook.E01_Partition
 [102071MB]_[APFS Container] (5_5) [APFS]\macOS Catalina - Data [volume_0]\root\.fseventsd" -o . FSEVENTS
utput path was : .
AIN-INFO-Started macOS Artifact Parsing Tool - Artifact Only mode, version 1.9.1.dev (20240914)
AIN-INFO-Dates and times are in UTC unless the specific artifact being parsed saves it as local time!
AIN-INFO-------------------------------------------------
AIN-INFO-Running plugin FSEVENTS
AIN-INFO-------------------------------------------------
AIN.FSEVENTS-INFO-Module Started as standalone
AIN.FSEVENTS-INFO-Writing 231662 fsevent(s)
AIN.FSEVENTS-INFO-The source_date field on the fsevents are from the individual file modified date (metadata not data)
This may have changed if you are not on a live or read-only image.
AIN.FSEVENTS-INFO-231662 logs found
AIN-INFO-------------------------------------------------
AIN-INFO-Finished in time = 00:00:06
AIN-INFO-Review the Log file and report any ERRORs or EXCEPTIONS to the developers

LARE-VM Wed 09/18/2024  3:58:26.30
:\Users\FlareVM\Desktop\iOS Investigation\mac_apt-master>
```

Q9: How much time was spent on mail.zoho.com on 4/20/2020?

- This was a challenging task, as we needed to determine the screen usage.
  The relevant file for screen time usage is located at:

  root\private\var\folders\bf\r04p_gb17xxg37r9ksq855mh0000gn\0\com.apple.ScreenTimeAgent
  \Store\RMAdminStore-Local.sqlite.

  To extract the necessary data, I used **Mac_Apt** with the **ScreenTime** plugin by running the following command:

  python mac_apt_artifact_only.py -i "MacOS Investigation\Store" -o "MacOS Investigation" SCREENTIME

  This provided an SQLite database containing timestamps for both websites and applications. I filtered for mail.zoho.com and calculated the time spent on the specified date.

  The final answer is **20:58**

	Application	Total_Time	Start_Date	End_Date	Notification_Count	Pickup_Count	Pickups_Without_Usage	Device_Name	Apple_ID	Full_Name	Family_Mer
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	mail.zoho.com	00:01:07	2020-04-12 17:00:00	2020-04-12 18:00:00	0	0	0	Hansel's Mac	NULL	NULL	Unknown
2	mail.zoho.com	00:00:31	2020-04-12 18:00:00	2020-04-12 18:21:46	0	0	0	Hansel's Mac	NULL	NULL	Unknown
3	mail.zoho.com	00:04:34	2020-04-20 01:00:00	2020-04-20 01:50:21	0	0	0	Hansel's Mac	NULL	NULL	Unknown
4	mail.zoho.com	00:16:24	2020-04-20 03:00:00	2020-04-20 03:26:23	0	0	0	Hansel's Mac	NULL	NULL	Unknown

Q10: What's hansel.apricot's password hint? (two words)

- On macOS, the directory path **/private/var/db/dslocal/nodes/Default/users** is related to the local directory services used by macOS for managing user accounts.

  User Records: This directory holds files representing user accounts on the system. Each file in this directory corresponds to a user account and contains metadata about that account.

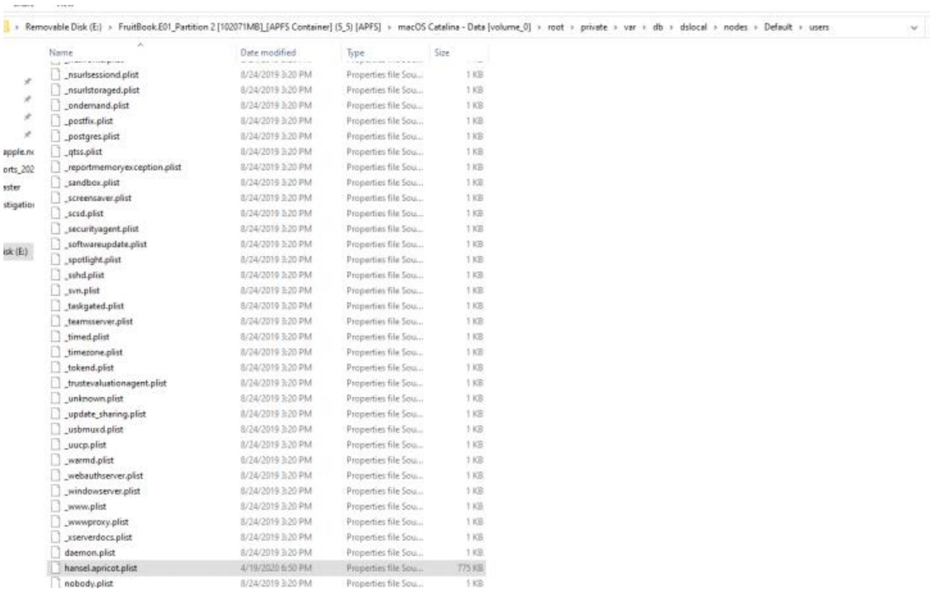
  User Plists: These files are usually property list (plist) files, which are formatted in XML or binary. They contain information such as the user's full name, user ID (UID), group ID (GID), home directory, and other attributes related to the user's account.

  Local Directory Service: This is part of macOS's Directory Service framework, which maintains local information about users, groups, and other directory-related data. The data is used by macOS to manage user accounts and authentication.

  System Configuration: The information in this directory is used for system configuration and authentication purposes, including login and user account management.=

  In the directory mentioned, I located a plist file named hansel.apricot.plist, associated with the user.
  After running strings on the file, I identified two words that appear to be a password hint: "**Family Opinion.**"

```
4^Hansel Apricot
8^Family Opinion
:^hansel.apricot
<^hansel.apricot
```



Q11: The main file that stores Hansel's iMessages had a few permissions changes. How many times did the permissions change?

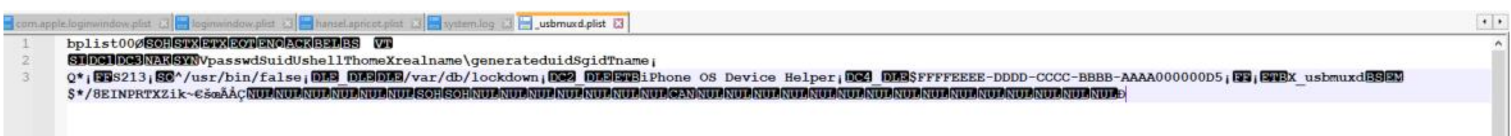
- We have already parsed the 'FSEvents' using MAC_APT and filtered for 'Messages,' where we identified a database file located in the 'Messages' directory. By filtering by the directory, we found 7 'PermissionChange' operations.

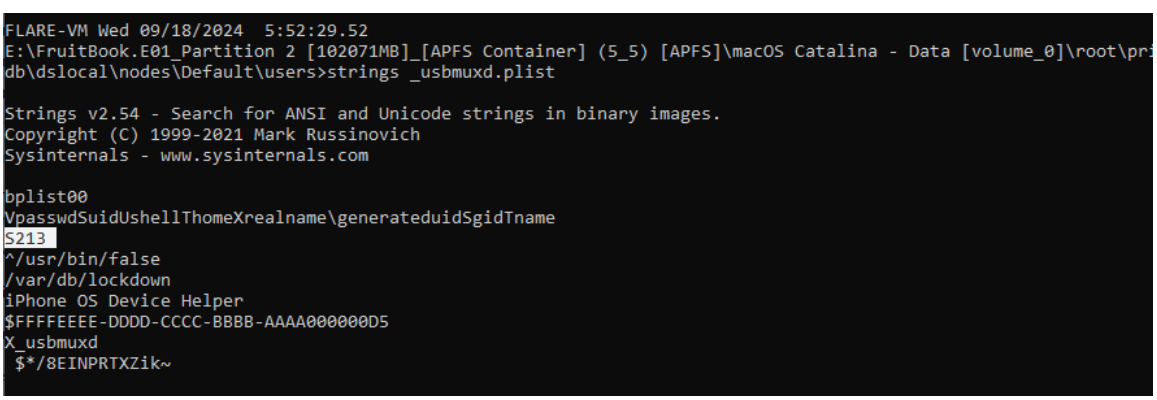
  Note: On macOS, **chat.db** is a SQLite database file used by the Messages app (iMessage) to store chat history and related information. This file contains records of conversations, including messages, attachments, and metadata associated with iMessage communications.

Q12: What's the UID of the user who is responsible for connecting mobile devices?

To address this question, I used the first hint and accessed the directory /private/var/db/dslocal/nodes/Default/users on macOS, where user accounts are managed.

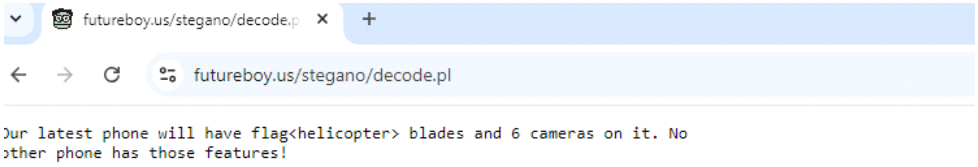
I searched for a user with 'USB' in their name, as suggested by the hint, and found the user _usbmuxd.
The property file for this user indicates that they are an 'iPhone OS Device Helper'.
After running strings on the user's plist file, I determined that the UID of the _usbmuxd user is **213**





Q13: Find the flag in the GoodExample.jpg image. It's hidden with better tools.

- While examining the Sneaky zsh history, I discovered that the user employed steganography to conceal a file within an image.
  Based on this, I suspected that steganography might have been used with another image as well. I uploaded the file to a steganography decoder and successfully uncovered the hidden note.

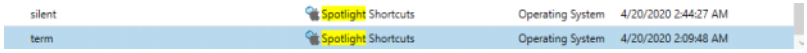


Q14:What was exactly typed in the Spotlight search bar on 4/20/2020 02:09:48

- Spotlight is a robust search feature integrated into macOS that enables users to swiftly locate files, documents, emails, applications, and other content on their Mac.

  Through 'Spotlight shortcuts' in Magent Axum, I identified relevant information in the file located at \root\Users\sneaky\Library\Application Support\com.apple.spotlight.

  These files might contain logs of past search queries, including specific keywords and their corresponding results.



Q15: What is hansel.apricot's Open Directory user UUID?

To address this question, I revisited the path \root\private\var\db\dslocal\nodes\Default\users, ran strings on the specified user property file, and located the UUID, which is **5BB00259-4F58-4FDE-BC67-C2659BA0A5A4.**