Spotlight Challenge

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.

Task 1:
What version of macOS is running on this image?

I asked the ChatGPT where can I find the version and he told me to navigate to the path "macOS Catalina [volume_4]\root\System\Library\CoreServices\SystemVersion.plist"

Then I opened the file with Notepad++ and saw the version

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>ProductBuildVersion</key>
    <string>19A583</string>
    <key>ProductCopyright</key>
    <string>1983-2019 Apple Inc.</string>
    <key>ProductName</key>
    <string>Mac OS X</string>
    <key>ProductUserVisibleVersion</key>
    <string>10.15</string>
    <key>ProductVersion</key>
    <string>10.15</string>
    <key>iOSSupportVersion</key>
    <string>13.0</string>
</dict>
</plist>
```

Answer: 10.15

Task 2:
What "competitive advantage" did Hansel lie about in the file AnotherExample.jpg? (two words)

I checked the image inside "macOS Catalina - Data [volume_0]\root\Users\Shared" and saw that there is an iPhone picture

Then I saw another file "secret" and I opened it and saw something with "flip phone" which is a lie

```
!Our newest phone will have helicopter blades and six cameras and <"flip phone"> technology!
```

Answer: flip phone

Task 3:
How many bookmarks are registered in safari?

I checked the "macOS Catalina - Data [volume_0]\root\Users\hansel.apricot\Library\Safari" and found a file Bookmarks.plist, I used strings on this file and saw several of websites and then I count them.

```
$F572AB04-332C-45A8-A531-0BAF26D39DD0
https://www.yahoo.com/
"1UYahoo
346 7_
$52A015AB-70BB-453D-9116-7AB9DAD2A63A
https://www.bing.com/
"9TBing
:;= >_
$C06DC664-6EAF-4BB2-881A-B89B2C1D8EF5
4https://www.google.com/?client=safari&channel=mac_bm
"?VGoogle
ABD E_
$EF96F8B5-83B7-4102-8898-6C3424E1DE8A
https://www.wikipedia.org/
"FYWikipedia
HIK L_
$E94031ED-C26E-4F6E-A240-FFC93A7EFFF5
https://www.facebook.com/
"MXFacebook
OPR S_
$D6E4766A-5185-4549-935D-02259E58D2BC
https://twitter.com/
"TWTwitter
WWY Z_
$4FA2BDA4-E62E-4BD5-98CB-FFD97EDF6F38
https://www.linkedin.com/
"[XLinkedIn
]^` a_
$07CA701A-896D-4655-A50C-B7EB3E91CBCD
https://www.weather.com/
```

- https://www.apple.com/ (Apple)
- https://www.icloud.com/ (iCloud)
- https://www.yahoo.com/ (Yahoo)
- https://www.bing.com/ (Bing)
- https://www.google.com/ (Google)
- https://www.wikipedia.org/ (Wikipedia)
- https://www.facebook.com/ (Facebook)
- https://twitter.com/ (Twitter)
- https://www.linkedin.com/ (LinkedIn)
- https://www.weather.com/ (The Weather Channel)
- https://www.yelp.com/ (Yelp)
- https://www.tripadvisor.com/ (TripAdvisor)
- https://mail.zoho.com/zm/#mail/folder/inbox (Zoho Mail)

Answer: 13

There is also another way to parse the Bookmarks.plist with the tool "mac_apt_artifact_only.exe" with the command:

"C:\Users\Bubble\Desktop\mac_apt_artifact_only.exe -t Safari -i "E:\FruitBook.E01_Partition 2 [102071MB]_[APFS Container] (5_5) [APFS]\macOS Catalina - Data [volume_0]\root\Users \hansel.apricot\Library\Safari\Bookmarks.plist" -o C:\Users\Bubble\Desktop\New"

```
C:\Users\Bubble
λ C:\Users\Bubble\Desktop\mac_apt_artifact_only.exe -t Safari -i "E:\FruitBook.E01_Partition 2 [102071MB]_[APFS Container] (5_5) [APFS]\macOS Catalina - Data [volume_0]\root\Users\hansel.apricot\Library\Safari\Bookmarks.plist" -o C:\Users\Bubble\Desktop\New
Output path was : C:\Users\Bubble\Desktop\New
MAIN-INFO-Started macOS Artifact Parsing Tool - Artifact Only mode, version 1.7.5.dev (20240511)
MAIN-INFO-Dates and times are in UTC unless the specific artifact being parsed saves it as local time!
MAIN-INFO-------------------------------------------------
MAIN-INFO-Running plugin SAFARI
MAIN-INFO-------------------------------------------------
MAIN.SAFARI-INFO-Module Started as standalone
MAIN-INFO-------------------------------------------------
MAIN-INFO-Finished in time = 00:00:00
MAIN-INFO-Review the Log file and report any ERRORs or EXCEPTIONS to the developers
```

Name	Date modified	Type	Size
Log.20240919-120847.txt	9/19/2024 5:08 AM	Text Document	1 KB
mac_apt.db	9/19/2024 5:08 AM	Data Base File	8 KB
Safari.tsv	9/19/2024 5:08 AM	TSV File	6 KB

Then we can open the db file with SQL DB Browser

Table: Safari

	Type	Name_or_Title	URL	Date	Other_Info	User	Source
1	BOOKMARK	Apple	https://www.apple.com/	NULL	BookmarksBar		E:\FruitBook.E01_Partition 2 [102071MB]_[APFS ...
2	BOOKMARK	iCloud	https://www.icloud.com/	NULL	BookmarksBar		E:\FruitBook.E01_Partition 2 [102071MB]_[APFS ...
3	BOOKMARK	Yahoo	https://www.yahoo.com/	NULL	BookmarksBar		E:\FruitBook.E01_Partition 2 [102071MB]_[APFS ...
4	BOOKMARK	Bing	https://www.bing.com/	NULL	BookmarksBar		E:\FruitBook.E01_Partition 2 [102071MB]_[APFS ...
5	BOOKMARK	Google	https://www.google.com/?client=safari&channel=mac_bm	NULL	BookmarksBar		E:\FruitBook.E01_Partition 2 [102071MB]_[APFS ...
6	BOOKMARK	Wikipedia	https://www.wikipedia.org/	NULL	BookmarksBar		E:\FruitBook.E01_Partition 2 [102071MB]_[APFS ...
7	BOOKMARK	Facebook	https://www.facebook.com/	NULL	BookmarksBar		E:\FruitBook.E01_Partition 2 [102071MB]_[APFS ...
8	BOOKMARK	Twitter	https://twitter.com/	NULL	BookmarksBar		E:\FruitBook.E01_Partition 2 [102071MB]_[APFS ...
9	BOOKMARK	LinkedIn	https://www.linkedin.com/	NULL	BookmarksBar		E:\FruitBook.E01_Partition 2 [102071MB]_[APFS ...
10	BOOKMARK	The Weather Channel	https://www.weather.com/	NULL	BookmarksBar		E:\FruitBook.E01_Partition 2 [102071MB]_[APFS ...
11	BOOKMARK	Yelp	https://www.yelp.com/	NULL	BookmarksBar		E:\FruitBook.E01_Partition 2 [102071MB]_[APFS ...
12	BOOKMARK	TripAdvisor	https://www.tripadvisor.com/	NULL	BookmarksBar		E:\FruitBook.E01_Partition 2 [102071MB]_[APFS ...
13	BOOKMARK	Inbox - Zoho Mail (hansel.apricot@fruitinc.xyz)	https://mail.zoho.com/zm/#mail/folder/inbox	NULL	BookmarksBar		E:\FruitBook.E01_Partition 2 [102071MB]_[APFS ...

Task 4:
What's the content of the note titled "Passwords"?

I checked the hint for which path I should look for and I went to "root \Users\hansel.apricot\Library
\Group Containers\group.com.apple.notes" and the file containing the notes is NoteStore.sqlite

I opened the file with DB Browser for SQLite and checked the tables until I found something with
"Passwords"
I didn't find anything else besides this so I assumed the answer is Passwords

ZSNIPPET	ZTHUMBNAILATTACHMENTIDENTIFIER	ZTITLE1	ZACCOUNTNAMEFORACCOUNTLISTSORTING
Filter	Filter	Filter	Filter
NULL	NULL	New Note	NULL
NULL	NULL	NULL	3_On My Mac
NULL	NULL	NULL	3_On My Mac
NULL	NULL	NULL	3_On My Mac
Find way of getting more money...	NULL	Pay bills	NULL
Get 2nd job... no to much	NULL	Ideas for work	NULL
	NULL	Passwords	NULL
That's a good amount of money they're offering.	NULL	555-0123	NULL

Answer: Passwords

Task 5:
Provide the MAC address of the ethernet adapter for this machine.

I checked the var\log and noticed a pcap file, I opened it with Notepad and saw a MAC address

CDIS.custom	3/1/2020 10:40 AM	CUSTOM File	1 KB
daily.out	4/19/2020 4:53 PM	Wireshark capture...	4 KB

```
Network interface status:
Name       Mtu   Network       Address            Ipkts Ierrs    Opkts Oerrs  Coll
lo0   16384 <Link#1>                         1072     0     1072     0     0
lo0   16384 127           localhost          1072     -     1072     -     -
lo0   16384 localhost   ::1                  1072     -     1072     -     -
lo0   16384 fe80::1%lo0 fe80:1::1            1072     -     1072     -     -
gif0* 1280  <Link#2>                            0     0        0     0     0
stf0* 1280  <Link#3>                            0     0        0     0     0
en0   1500  <Link#4>    00:0c:29:c4:65:77   372733     0    73025     0     0
en0   1500  fe80::8c8:8 fe80:4::8c8:87c2:    372733     -    73025     -     -
en0   1500  184.171.151/2 stu-181-151-171    372733     -    73025     -     -
utun0 1380  <Link#5>                            0     0        2     0     0
utun0 1380  fe80::8375: fe80:5::8375:3ebe       0     -        2     -     -
utun1 2000  <Link#6>                            0     0        2     0     0
utun1 2000  fe80::feea: fe80:6::feea:9530       0     -        2     -     -
```

Answer: 00:0c:29:c4:65:77

Task 6:
Name the data URL of the quarantined item.

I asked the ChatGPT where is the path to see the quarantine items

`~/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2` file. It records information about files that were downloaded from the internet or transferred via AirDrop, among other sources.

So I searched on all the folder for preferences and found the folder under
root\Users\sneaky\Library\Preferences\com.apple.LaunchServices.QuarantineEventsV 2

I tried to parse it with mac_apt but the file output was 0kb so I used strings on it and found the URL

```
C:\Users\Bubble\Desktop
λ strings "E:\FruitBook.E01_Partition 2 [102071MB]_[APFS Container] (5_5) [APFS]\macOS Catalina - Data [volume_0]\roo
t\Users\sneaky\Library\Preferences\com.apple.LaunchServices.QuarantineEventsV2"

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

SQLite format 3
@
.4
+indexLSQuarantineTimeStampIndexLSQuarantineEvent
CREATE INDEX LSQuarantineTimeStampIndex  ON LSQuarantineEvent (  LSQuarantineTimeStamp )
AindexLSQuarantineEventIndexLSQuarantineEvent
CREATE INDEX LSQuarantineEventIndex  ON LSQuarantineEvent (  LSQuarantineEventIdentifier )
ItableLSQuarantineEventLSQuarantineEvent
CREATE TABLE LSQuarantineEvent (  LSQuarantineEventIdentifier TEXT PRIMARY KEY NOT NULL,  LSQuarantineTimeStamp REAL,
  LSQuarantineAgentBundleIdentifier TEXT,  LSQuarantineAgentName TEXT,  LSQuarantineDataURLString TEXT,  LSQuarantine
SenderName TEXT,  LSQuarantineSenderAddress TEXT,  LSQuarantineTypeNumber INTEGER,  LSQuarantineOriginTitle TEXT,  LS
QuarantineOriginURLString TEXT,  LSQuarantineOriginAlias BLOB )A
indexsqlite_autoindex_LSQuarantineEvent_1LSQuarantineEvent
DB572869-0311-4553-A09E-60209E0162D0A
Scom.apple.SafariSafarihttps://futureboy.us/stegano/encode.plhttps://futureboy.us/stegano/encinput.html
DB572869-0311-4553-A09E-60209E0162D0
DB572869-0311-4553-A09E-60209E0162D0
```

Answer: https://futureboy.us/stegano/encode.pl

Task 7:
What app did the user "sneaky" try to install via a .dmg file? (one word)

I searched on all folders with Notepad++ for .dmg files

```
E:\FruitBook.E01_Partition 2 [102071MB]_[APFS Container] (5_5) [APFS]\macOS Catalina - Data [volume_0]\root\Users\sneaky\.zsh_history (2 hits)
  Line  7: hdiutil mount silenteye-0.4.1b-snowleopard.dmg
  Line 15: hdiutil eject silenteye-0.4.1b-snowleopard.dmg
```

Answer: silenteye

Task 8:
What was the file 'Examplesteg.jpg' renamed to?

I used mac_apt to parse the fseventsd data and opened it with DB Browser

```
C:\Users\Bubble\Desktop
λ mac_apt_artifact_only.exe -t FSEVENTS -i "E:\FruitBook.E01_Partition 2 [102071MB]_[APFS Container] (5_5) [APFS]\macOS Catalina - Data [volume_0]\root\.fseventsd" -o C:\Users\Bubble\Desktop\FSEventsOutput
Output path was : C:\Users\Bubble\Desktop\FSEventsOutput
MAIN-INFO-Started macOS Artifact Parsing Tool - Artifact Only mode, version 1.7.5.dev (20240511)
MAIN-INFO-Dates and times are in UTC unless the specific artifact being parsed saves it as local time!
MAIN-INFO-----------------------------------------------------
MAIN-INFO-Running plugin FSEVENTS
MAIN-INFO-----------------------------------------------------
MAIN.FSEVENTS-INFO-Module Started as standalone
MAIN.FSEVENTS-INFO-Writing 231662 fsevent(s)
MAIN.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.
MAIN.FSEVENTS-INFO-231662 logs found
MAIN-INFO-----------------------------------------------------
MAIN-INFO-Finished in time = 00:00:05
MAIN-INFO-Review the Log file and report any ERRORs or EXCEPTIONS to the developers
```

LogID	EventFlagsHex	EventType	EventFlags	Filepath	File_ID	Log_Unknown	SourceModDate *1
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
0000000000951CD8	01000184	Folder	InodeMetaMod|FolderCreated|PermissionChange	Users/sneaky/Downloads	12885032683	NULL	2020-04-20 02:04:02.505195
0000000000951BC0	00800100	File	Created|InodeMetaMod|RenamedOrMoved|PermissionChange	Users/sneaky/Downloads/.BC.T_yoVsRa	12885032684	NULL	2020-04-20 02:04:02.505195
0000000000951CDE	0080010C	File	InodeMetaMod|RenamedOrMoved|PermissionChange	Users/sneaky/Downloads/.localized	12885032684	NULL	2020-04-20 02:04:02.505195
000000000096977D	00800208	File	RenamedOrMoved|XAttrModified	Users/sneaky/Downloads/silenteye-0.4.1b-snowleopard.dmg	12885040641	NULL	2020-04-20 02:39:45.024937
00000000009684A06	01000286	Folder	Removed|InodeMetaMod|FolderCreated|XAttrModified	Users/sneaky/Downloads/silenteye-0.4.1b-snowleopard.dmg.download	12885040639	NULL	2020-04-20 02:39:45.024937
000000000096989ED	0080000A	File	Removed|RenamedOrMoved	Users/sneaky/Downloads/silenteye-0.4.1b-snowleopard.dmg.download/Info.plist	12885040643	NULL	2020-04-20 02:39:45.024937
000000000096989F0	00800219	File	Created|RenamedOrMoved|Modified|XAttrModified	Users/sneaky/Downloads/silenteye-0.4.1b-snowleopard.dmg.download/silenteye-0.4.1b-snowleopard.dmg	12885040641	NULL	2020-04-20 02:39:45.024937
000000000096803E	01000282	Folder	Removed|FolderCreated|XAttrModified	Users/sneaky/Downloads/steghide-0.5.1-win32.zip.download	12885040515	NULL	2020-04-20 02:39:45.024937
000000000096EB06	00800055	File	Created|InodeMetaMod|Modified|FinderInfoMod	Users/sneaky/Downloads/.DS_Store	12885042140	NULL	2020-04-20 02:53:25.288821
000000000096E78F	00800008	File	RenamedOrMoved	Users/sneaky/Downloads/silenteye-0.4.1b-snowleopard.dmg	12885040641	NULL	2020-04-20 02:53:25.288821
00000000097A074	00800014	File	InodeMetaMod|Modified	Users/sneaky/Downloads/.DS_Store	12885042140	NULL	2020-04-20 03:19:45.135221
00000000097 6AA9	00800008	File	RenamedOrMoved	Users/sneaky/Downloads/Example.jpg	12885043806	NULL	2020-04-20 03:19:45.135221
00000000097 6761	00800208	File	RenamedOrMoved|XAttrModified	Users/sneaky/Downloads/Examplesteg.jpg	12885043806	NULL	2020-04-20 03:19:45.135221
00000000097 6359	01000286	Folder	Removed|InodeMetaMod|FolderCreated|XAttrModified	Users/sneaky/Downloads/Examplesteg.jpg.download	12885043803	NULL	2020-04-20 03:19:45.135221
00000000097 6355	00800219	File	Created|RenamedOrMoved|Modified|XAttrModified	Users/sneaky/Downloads/Examplesteg.jpg.download/Examplesteg.jpg	12885043806	NULL	2020-04-20 03:19:45.135221
00000000097 6352	0080000A	File	Removed|RenamedOrMoved	Users/sneaky/Downloads/Examplesteg.jpg.download/Info.plist	12885043808	NULL	2020-04-20 03:19:45.135221
00000000097 6AD0	00800008	File	RenamedOrMoved	Users/sneaky/Downloads/GoodExample.jpg	12885043806	NULL	2020-04-20 03:19:45.135221

Then I searched for the user sneaky Downloads and filtered by timestamp and I saw the Examplesteg.jpg is in the same time with GoodExample.jpg

Answer: GoodExample.jpg

Task 9:
How much time was spent on mail.zoho.com on 4/20/2020?

I asked ChatGPT where can I see this information and he said it should be " \root\private\var \folders" inside the file "RMAdminStore-Local.sqlite"

I found the file inside "E:\FruitBook.E01_Partition 2 [102071MB]_[APFS Container] (5_5) [APFS]\macOS Catalina - Data [volume_0]\root\private\var\folders\bf \r04p_gb17xg37r9ksq855mh0000gn\0\com.apple.ScreenTimeAgent\Store"

I used mac_apt to parse the data

```
C:\Users\Bubble\Desktop
λ mac_apt_artifact_only.exe -t SCREENTIME -i C:\Users\Bubble\Desktop\Store\RMAdminStore-Local.sqlite  -o C:\Users\Bubble\Desktop\Screentime
Output path was : C:\Users\Bubble\Desktop\Screentime
MAIN-INFO-Started macOS Artifact Parsing Tool - Artifact Only mode, version 1.7.5.dev (20240511)
MAIN-INFO-Dates and times are in UTC unless the specific artifact being parsed saves it as local time!
MAIN-INFO-----------------------------------------------------
MAIN-INFO-Running plugin SCREENTIME
MAIN-INFO-----------------------------------------------------
MAIN.SCREENTIME-INFO-Module Started as standalone
MAIN.SCREENTIME-INFO-Processing file C:\Users\Bubble\Desktop\Store\RMAdminStore-Local.sqlite
MAIN-INFO-----------------------------------------------------
MAIN-INFO-Finished in time = 00:00:00
MAIN-INFO-Review the Log file and report any ERRORs or EXCEPTIONS to the developers
```

Then I opened it with DB Browser and searched for mail.zoho.com
I saw 2 events in 4/20 so I calculate both times

Application	Total_Time	Start_Date	End_Date
Filter	Filter	Filter	Filter
mail.zoho.com	00:01:07	2020-04-12 17:00:00	2020-04-12 18:00:00
mail.zoho.com	00:00:31	2020-04-12 18:00:00	2020-04-12 18:21:46
mail.zoho.com	00:04:34	2020-04-20 01:00:00	2020-04-20 01:50:21
mail.zoho.com	00:16:24	2020-04-20 03:00:00	2020-04-20 03:26:23

Answer: 20:58

Task 10:
What's hansel.apricot's password hint? (two words)

I asked the ChatGPT what is the location for it

3. Property List Files:

- macOS often stores password hints in `.plist` files. A possible location for password hints could be `/var/db/dslocal/nodes/Default/users/hansel.apricot.plist`.

You can extract and open these files using `plutil` or a tool like **mac_apt**.

daemon.plist	8/24/2019 3:20 PM	PLIST File	1 KB
hansel.apricot.plist	4/19/2020 6:50 PM	PLIST File	775 KB

I tried to use the mac_apt on the file but I didn't find a plugin that worked so I used strings and analyzed it until I found the answer

```
^hansel.apricot
@X/bin/zsh
2Q@
4^Hansel Apricot
8^Family Opinion
:^hansel.apricot
<^hansel.apricot
bplist00
SRP-RFC5054-4096-SHA512-PBKDF2_
SALTED-SHA512-PBKDF2
XverifierTsaltZiterationsO
```

Answer: Family Opinion

Task 11:
The main file that stores Hansel's iMessages had a few permissions changes. How many times did the permissions change?

I checked the fsevents output from task 8 and searched for chat.db and then I counted all the PermissionChange events.

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: FsEvents | chat.db

	LogID	EventFlagsHex	EventType	EventFlags	Filepath
	Filter	Filter	Filter	Filter	Filter
1	0000000000B0FE74	00800100	File	PermissionChange	Users/hansel.apricot/Library/Messages/chat.db
2	0000000000B0FE77	00800004	File	InodeMetaMod	Users/hansel.apricot/Library/Messages/chat.db-shm
3	0000000000B14F61	00800004	File	InodeMetaMod	Users/hansel.apricot/Library/Messages/chat.db
4	00000000007E950F	00800100	File	PermissionChange	Users/hansel.apricot/Library/Messages/chat.db
5	00000000007E9512	00800004	File	InodeMetaMod	Users/hansel.apricot/Library/Messages/chat.db-shm
6	0000000000094E48D	00800100	File	PermissionChange	Users/hansel.apricot/Library/Messages/chat.db
7	0000000000094E490	00800004	File	InodeMetaMod	Users/hansel.apricot/Library/Messages/chat.db-shm
8	0000000000B87A34	00800100	File	PermissionChange	Users/hansel.apricot/Library/Messages/chat.db
9	0000000000B87A37	00800004	File	InodeMetaMod	Users/hansel.apricot/Library/Messages/chat.db-shm
10	00000000007E1406	00800100	File	PermissionChange	Users/hansel.apricot/Library/Messages/chat.db
11	00000000007E1409	00800004	File	InodeMetaMod	Users/hansel.apricot/Library/Messages/chat.db-shm
12	00000000007D06E7	00800001	File	Created	Users/hansel.apricot/Library/Messages/chat.db
13	00000000007D06F9	00800013	File	Created|Removed|Modified	Users/hansel.apricot/Library/Messages/chat.db-journal
14	00000000007D0702	00800005	File	Created|InodeMetaMod	Users/hansel.apricot/Library/Messages/chat.db-shm
15	00000000007D06FC	00800001	File	Created	Users/hansel.apricot/Library/Messages/chat.db-wal
16	0000000000B7BBB2	00800100	File	PermissionChange	Users/hansel.apricot/Library/Messages/chat.db
17	0000000000B7BBB5	00800004	File	InodeMetaMod	Users/hansel.apricot/Library/Messages/chat.db-shm
18	0000000009451AA	00800100	File	PermissionChange	Users/hansel.apricot/Library/Messages/chat.db
19	0000000009451AD	00800004	File	InodeMetaMod	Users/hansel.apricot/Library/Messages/chat.db-shm
20	000000000095364E	00800001	File	Created	Users/sneaky/Library/Messages/chat.db
21	0000000000953657	00800013	File	Created|Removed|Modified	Users/sneaky/Library/Messages/chat.db-journal
22	0000000000953660	00800005	File	Created|InodeMetaMod	Users/sneaky/Library/Messages/chat.db-shm
23	000000000095365A	00800001	File	Created	Users/sneaky/Library/Messages/chat.db-wal
24	0000000000B953D6	00800004	File	InodeMetaMod	Users/hansel.apricot/Library/Messages/chat.db

Answer: 7

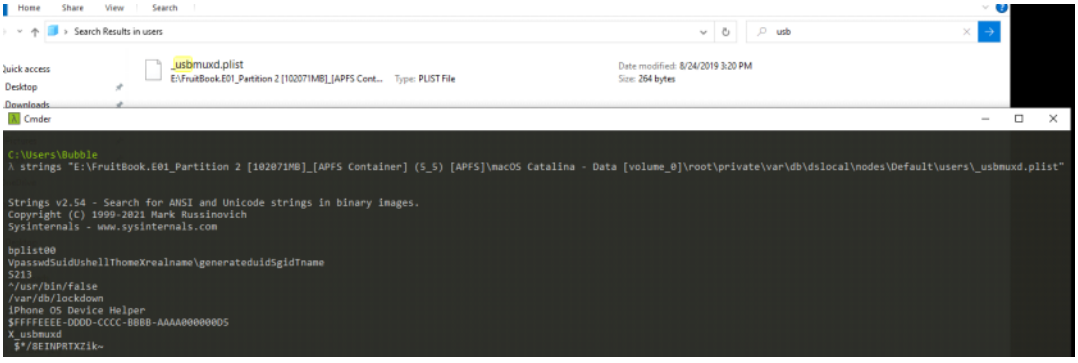
Task 12:
The main file that stores Hansel's iMessages had a few permissions changes. How many times did the permissions change?

I asked ChatGPT about this task and he told me about usbmuxd which is "The usbmuxd service (USB multiplexing daemon) manages connections to iOS devices.

Each user in macOS typically has a User ID (UID), and it looks like the user associated with mobile device updates in this case has the hostname or user prefix `stu`. To find the UID of the user responsible for connecting mobile devices, you would need to match this `stu-` user with their UID. You can do this by searching the user database, likely found in:

- `/etc/passwd`
- Or within user account metadata in `/var/db/dslocal/nodes/Default/users/`

Inside the users folder I searched for the usbmuxd and found a file and I used strings on it



Then I assumed the UID is 213

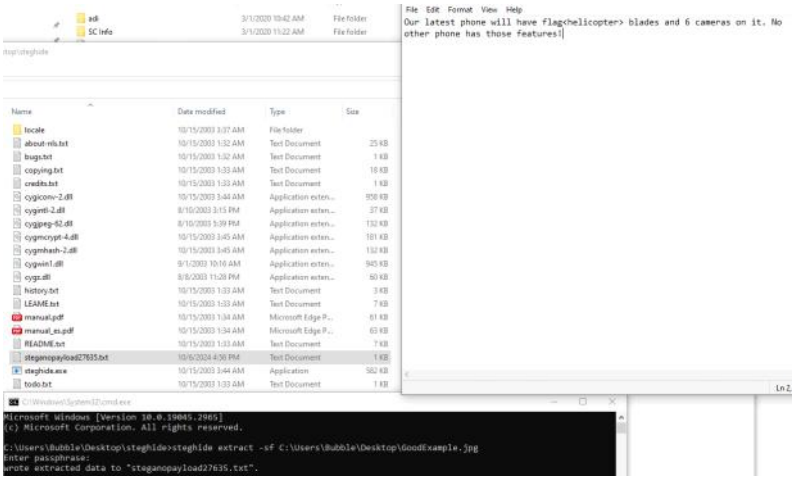
Answer: 213

Task 13:
Find the flag in the GoodExample.jpg image. It's hidden with better tools.

I asked the ChatGPT what tool can help me with this and he told me to use Steghide and then to use the following command

steghide extract -sf "filename.xxx"

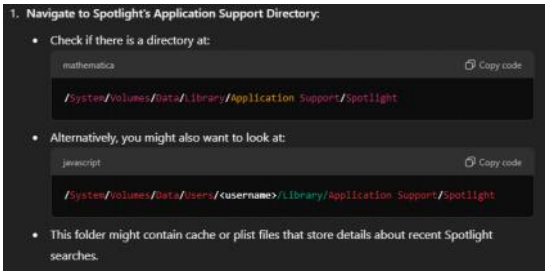
When I used the command, I asked to enter a password and because I didn 't had it I just pressed enter and a txt file was created "steanopayload 27635.txt" when I opened the file I saw <helicopter> and I assumed this is the flag



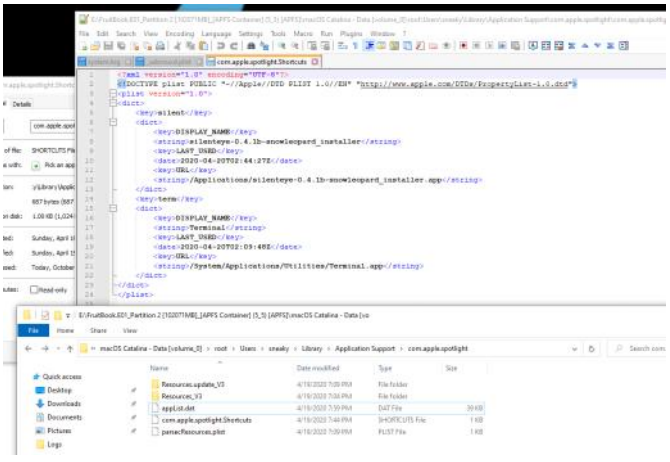
Answer: helicopter

Task 14:
What was exactly typed in the Spotlight search bar on 4/20/2020 02:09:48

I asked ChatGPT where can I find the answer for this task



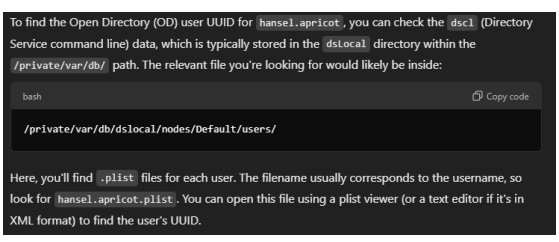
I navigated to the user sneaky and then I opened the file com.apple.spotlight.Shortcuts with Notepad++ and found the flag



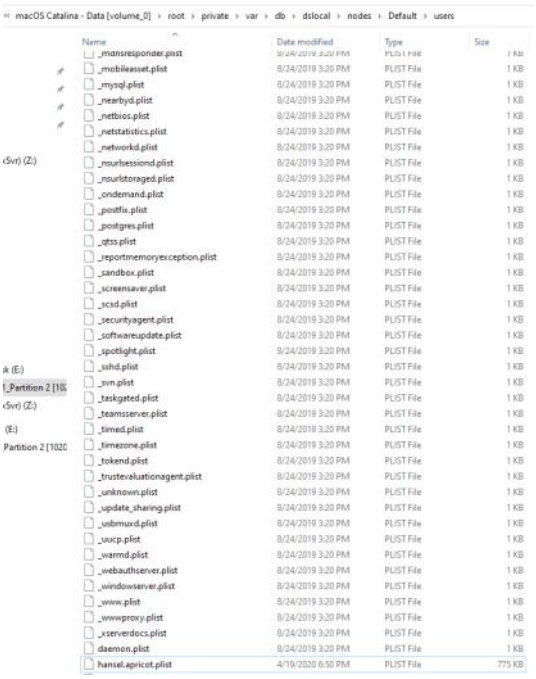
Answer: term

Task 15:
What is hansel.apricot's Open Directory user UUID?

I asked ChatGPT where can I find the answer for this task



Inside the directory I found hansel.apricot file



I used strings on the file and found the flag

Answer: $5BB00259-4F58-4FDE-BC67-C2659BA0A5A4