Data Recovery and Digital Forensics

Premise

- Users are given an exact image of a flash drive that was used by malicious attackers, they need to search through it to see if they can find any useful information, deleted files, or sensitive documents
  - NIST: T0289

Questions

- What *filesystem* is the recovered flashdrive using
- What it the name of the *image file* that has a picture of a secret message
  - When was this file created (Year-Month-Day Format)
  - What is the camera make that took the picture (Manufacturer)
  - When decoded what does the message say
  - Where was the picture taken (Geolocation)
- Encrypted Files
  - What is the *file name* of the encrypted logins
  - What is the *password hash* of the root user
  - What *hashing algorithm* was used to encrypt the root users password
  - What is the *unencrypted value* of the root password hash

FILE

- Recovered Flashdrive.img

Recommended Tools

- Autopsy
- Web Browser

Answers

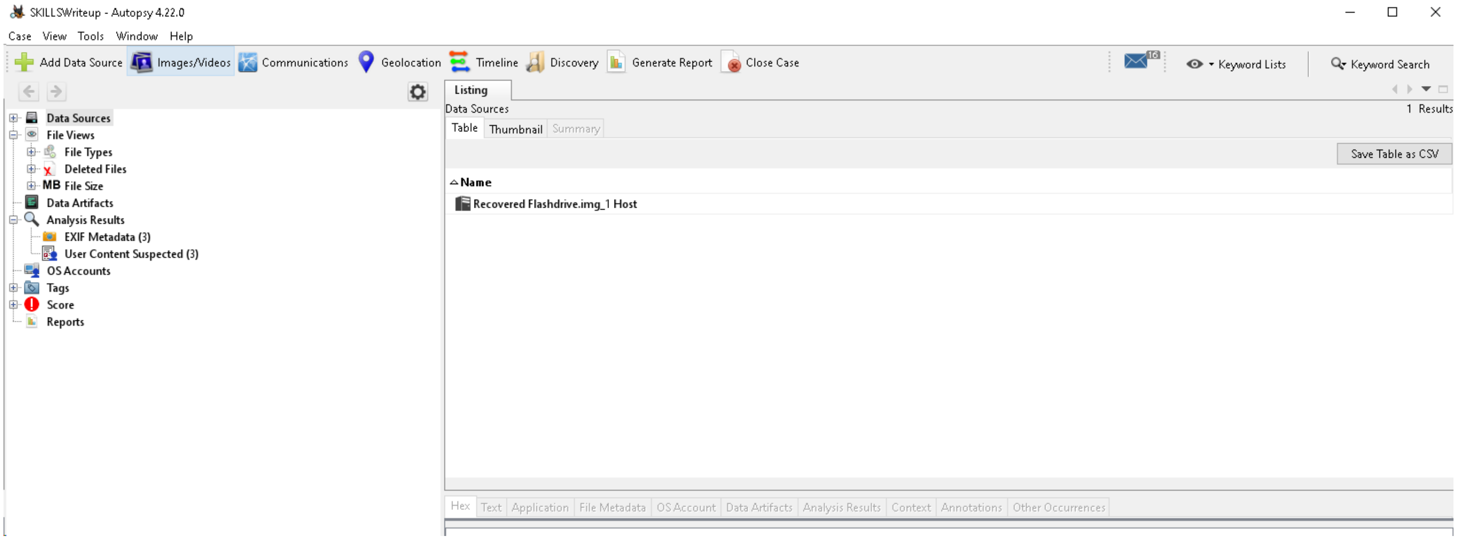
- What *filesystem* is the recovered flashdrive using

    - FAT32
- Image Questions
    - What it the name of the *image file* that has a picture of a secret message
        - `_EPS4183.jpg`
    - When was this file created (Year-Month-Day Format)
        - 2025-04-09
    - What is the camera make that took the picture (Manufacturer)
        - Epson
    - When decoded what does the message say
        - Meet Me at 7PM (Caeser Cipher 20 Shift)
    - Where was the picture taken (Geolocation Screenshot)
        -
- Encrypted Files
    - What is the *file name* of the encrypted logins
        - ENCRYPTED_ADMIN_LOGINS.txt
    - What is the *password hash* of the root user
        - U3VwZXJBZG0xbkwwZ2luMTIzNCE=
    - What *hashing algorithm* was used to encrypt the root users password
        - Base64
    - What is the *unencrypted value* of the root password hash
        - SuperAdm1nL0gin1234!

Walkthrough

1. To start this exercise open Autopsy and create a new case
2. Add a new data source and import the "Recovered Flashdrive.img" file
    1. `Add Data Source > Next > Disk Image or VM file > Browse to the File > Finish`
3. Autopsy will now import and analyze the data, this will take a few seconds

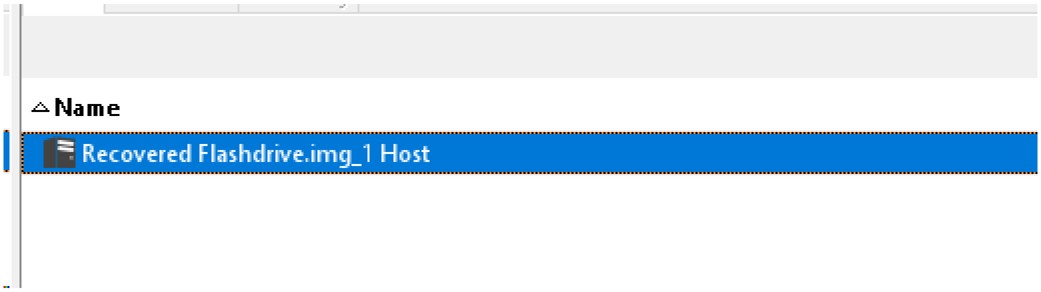
4. Autopsy should now look like this



Name
Recovered Flashdrive.img_1 Host

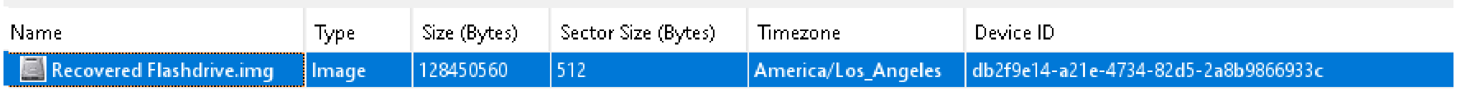
   1. Having only one data source added

5. Double Click on the "Recovered Flashdrive.img_Host"



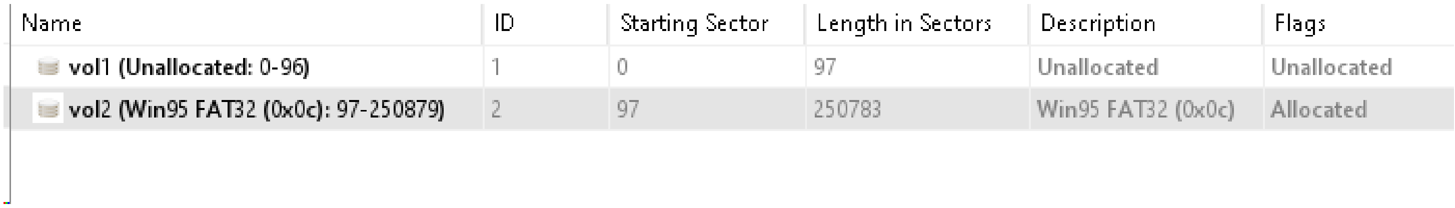
Name
Recovered Flashdrive.img_1 Host

6. Click again on the actual Image file



Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
Recovered Flashdrive.img	Image	128450560	512	America/Los_Angeles	db2f9e14-a21e-4734-82d5-2a8b9866933c

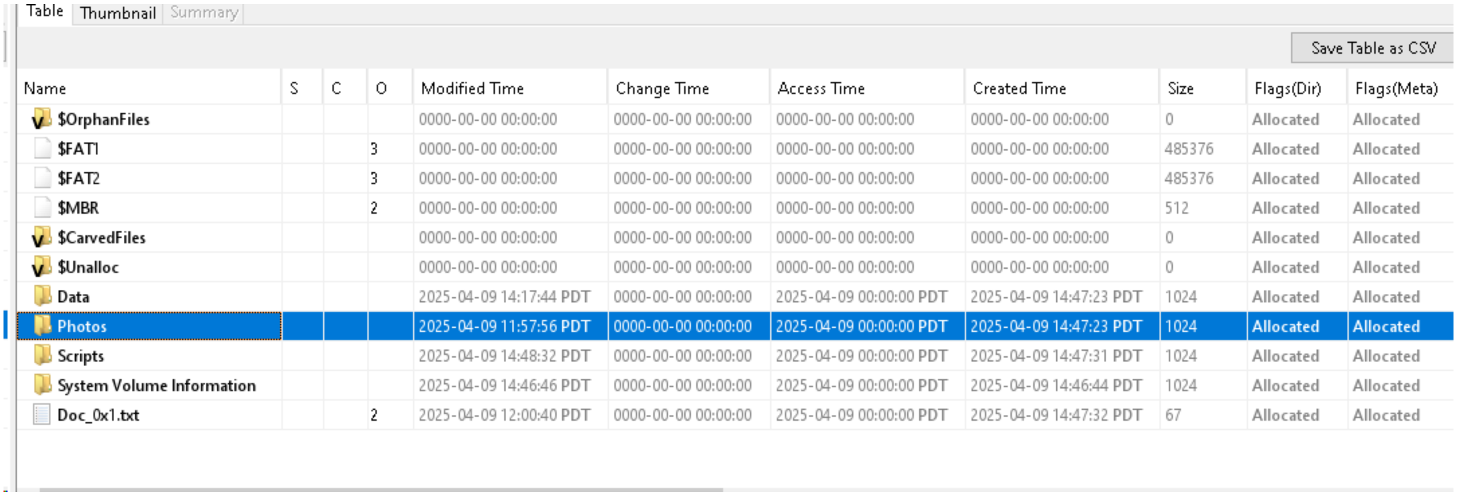
7. The next screen will show the volumes of the image. Vol1 being the base device, and Vol2 being the actual data partition on the device



Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-96)	1	0	97	Unallocated	Unallocated
vol2 (Win95 FAT32 (0x0c): 97-250879)	2	97	250783	Win95 FAT32 (0x0c)	Allocated

   1. Note the Description (This is where answer 1 lies) and the Flags, which specify if the drive has any partitions/is allocated

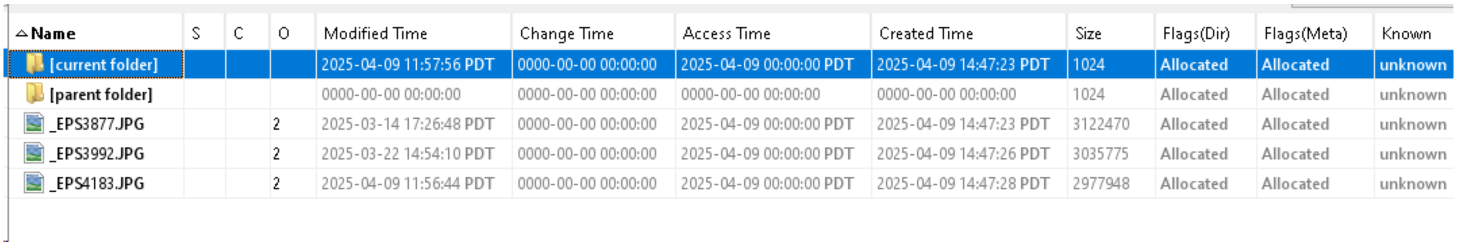
8. Inside of the Image, navigate to the photos folder



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
$OrphanFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated
$FAT1			3	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	485376	Allocated	Allocated
$FAT2			3	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	485376	Allocated	Allocated
$MBR			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	512	Allocated	Allocated
$CarvedFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated
$Unalloc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated
Data				2025-04-09 14:17:44 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:23 PDT	1024	Allocated	Allocated
Photos				2025-04-09 11:57:56 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:23 PDT	1024	Allocated	Allocated
Scripts				2025-04-09 14:48:32 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:31 PDT	1024	Allocated	Allocated
System Volume Information				2025-04-09 14:46:46 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:46:44 PDT	1024	Allocated	Allocated
Doc_0x1.txt			2	2025-04-09 12:00:40 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:32 PDT	67	Allocated	Allocated

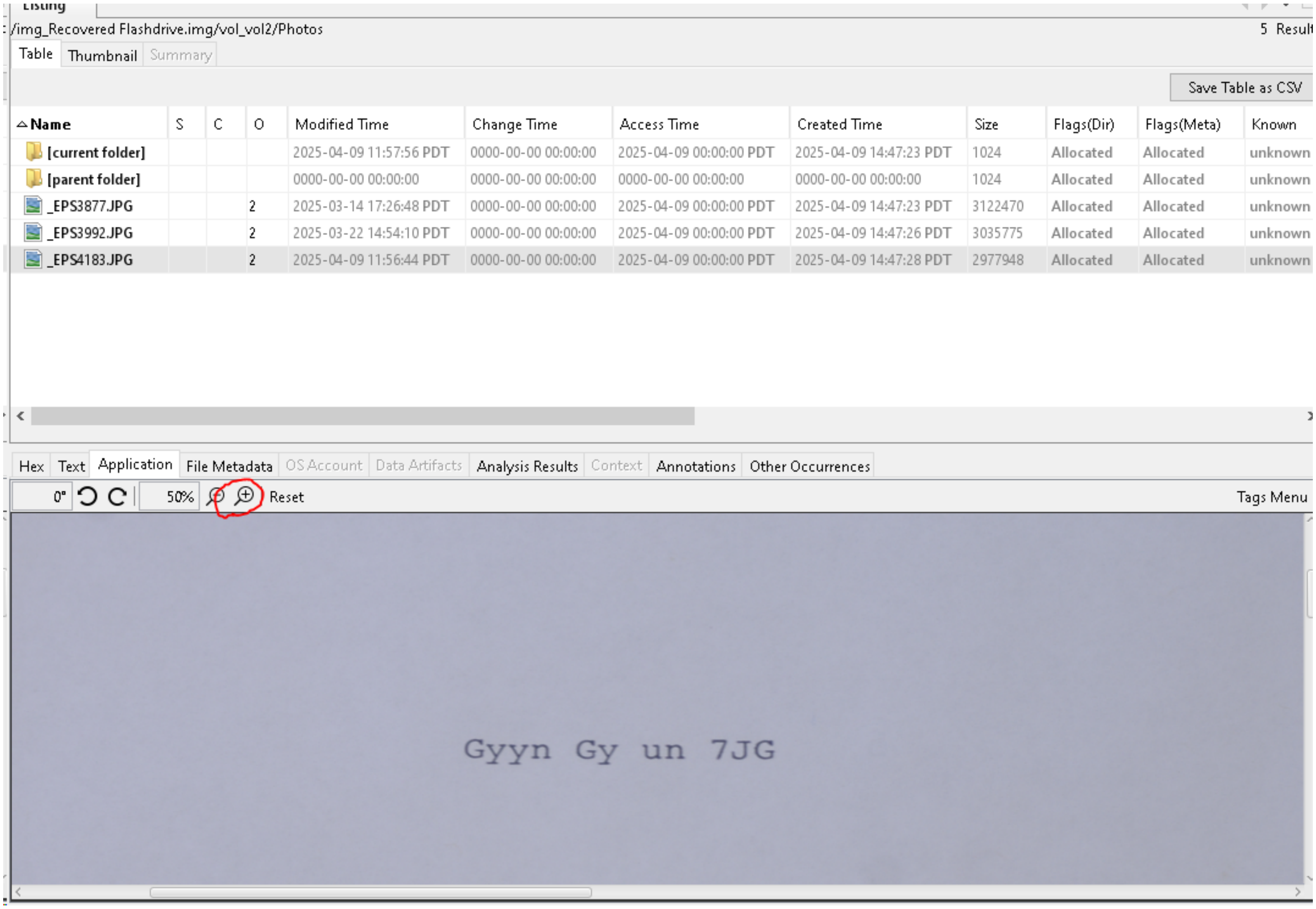
    1. This is where the original owner stored all their photographs

9. Inside this folder we can see three photographs, looking towards the questions we can see that we were supposed to find one that holds a secret message



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
[current folder]				2025-04-09 11:57:56 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:23 PDT	1024	Allocated	Allocated	unknown
[parent folder]				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1024	Allocated	Allocated	unknown
_EPS3877.JPG			2	2025-03-14 17:26:48 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:23 PDT	3122470	Allocated	Allocated	unknown
_EPS3992.JPG			2	2025-03-22 14:54:10 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:26 PDT	3035775	Allocated	Allocated	unknown
_EPS4183.JPG			2	2025-04-09 11:56:44 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:28 PDT	2977948	Allocated	Allocated	unknown

10. Looking through the photos using the preview below we can see that `_EPS4183.jpg` (q. 2) has some sort of code written on it.



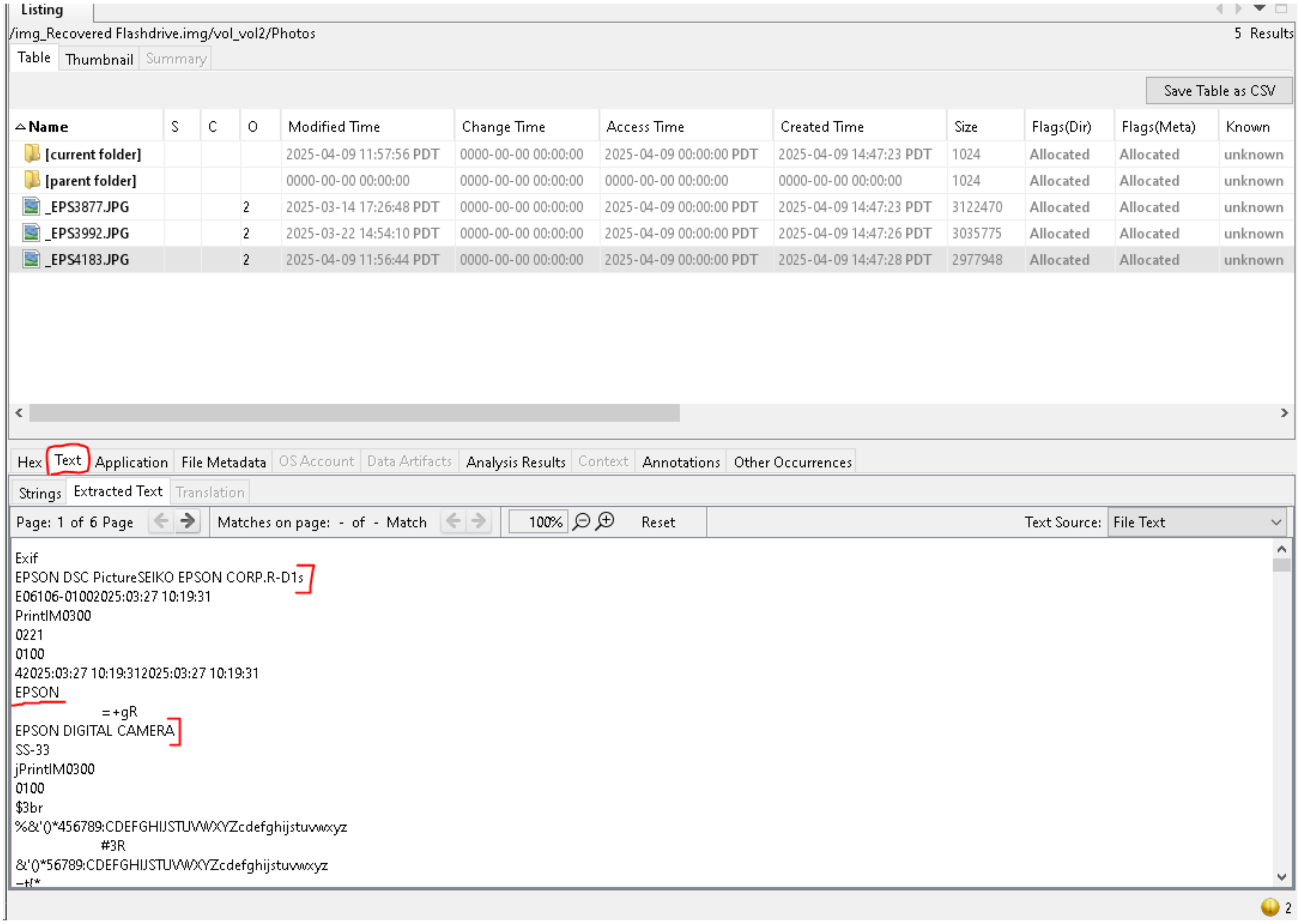
/img_Recovered Flashdrive.img/vol_vol2/Photos 5 Result

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
[current folder]				2025-04-09 11:57:56 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:23 PDT	1024	Allocated	Allocated	unknown
[parent folder]				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1024	Allocated	Allocated	unknown
_EPS3877.JPG			2	2025-03-14 17:26:48 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:23 PDT	3122470	Allocated	Allocated	unknown
_EPS3992.JPG			2	2025-03-22 14:54:10 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:26 PDT	3035775	Allocated	Allocated	unknown
_EPS4183.JPG			2	2025-04-09 11:56:44 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:28 PDT	2977948	Allocated	Allocated	unknown

Gyyn Gy un 7JG

1. Hint: Use the Plus and Minus icons to zoom into the image

11. Looking to the the Created time column will give us the date that the image was created. The format in the question is (2025-04-09)
12. To find the make of the camera used look to the **Text** tab at the bottom of the screen



/img_Recovered Flashdrive.img/vol_vol2/Photos

5 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
[current folder]				2025-04-09 11:57:56 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:23 PDT	1024	Allocated	Allocated	unknown
[parent folder]				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1024	Allocated	Allocated	unknown
_EPS3877.JPG			2	2025-03-14 17:26:48 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:23 PDT	3122470	Allocated	Allocated	unknown
_EPS3992.JPG			2	2025-03-22 14:54:10 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:26 PDT	3035775	Allocated	Allocated	unknown
_EPS4183.JPG			2	2025-04-09 11:56:44 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:28 PDT	2977948	Allocated	Allocated	unknown

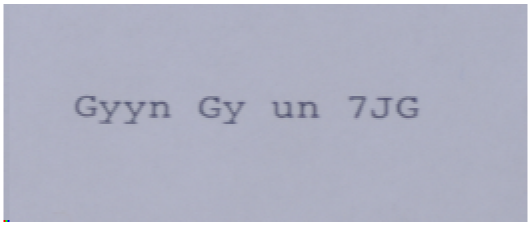
Page: 1 of 6 Page

Matches on page: - of - Match

```
Exif
EPSON DSC PictureSEIKO EPSON CORP.R-D1s
E06106-01002025:03:27 10:19:31
PrintIM0300
0221
0100
42025:03:27 10:19:312025:03:27 10:19:31
EPSON
               =+gR
EPSON DIGITAL CAMERA
SS-33
jPrintIM0300
0100
$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
               #3R
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
−t!*
```

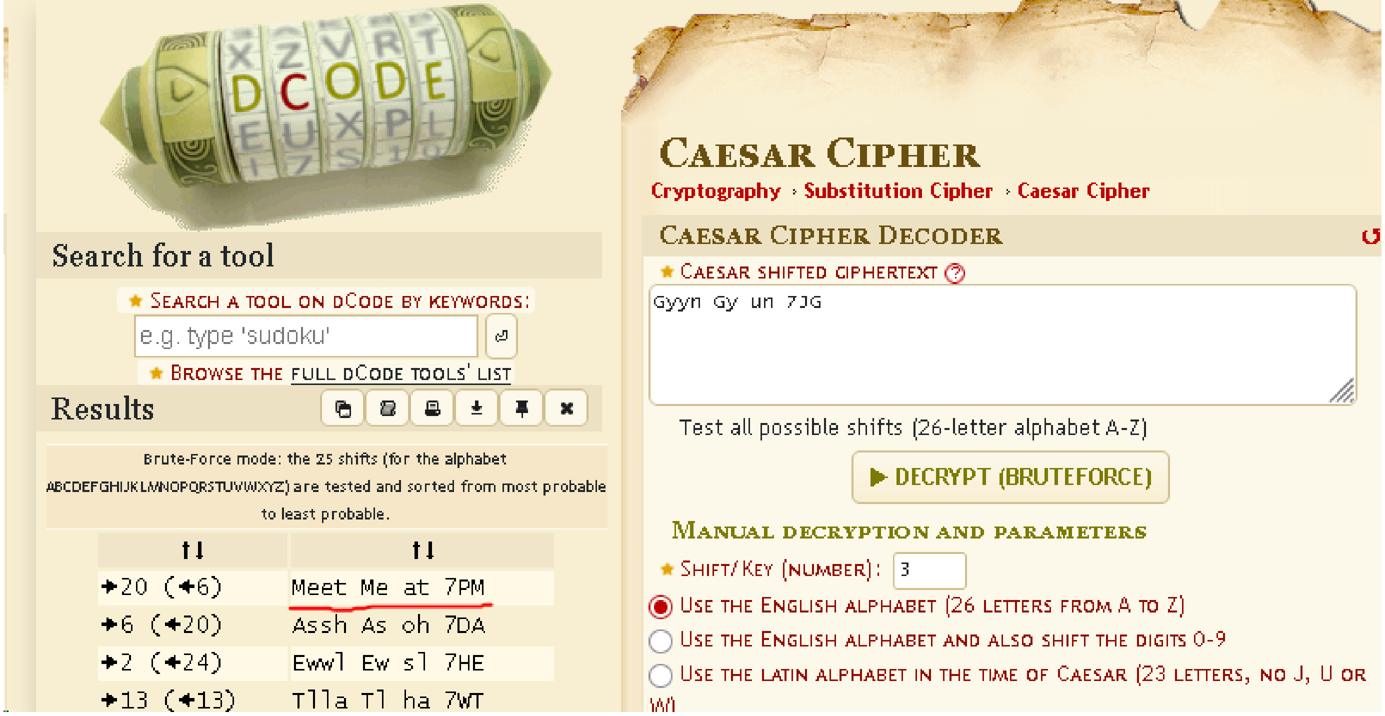
1. As highlighted in the image there are three mentions of the cameras manufacturer "Epson" with the exact model being found in the second line "RD-1s"

13. The secret message that is encoded in the picture can be solved in a number of ways. Figuring out what type of encoding or cipher is used is the first step

1. 

Gyyn Gy un 7JG

2. Looking at this snippet, multiple occurrences of "y" can be seen, using a little statistics and knowledge of the English language (knowing that "e" is the most frequently used letter) it is a solid guess that "y" is equal to "e". This type of cipher is called a shift cipher, also known as a Caeser Cipher
3. These ciphers can be solved by hand like this, or they can be solved with automated utilities. For this example dCode has a great automated cipher solver


DCODE
Search for a tool
★ Search a tool on dCode by keywords:
e.g. type 'sudoku'
★ Browse the full dCode tools' list
Results
Cryptography › Substitution Cipher › Caesar Cipher
DECRYPT (BRUTEFORCE)

Caesar Cipher

Caesar Cipher Decoder

★ Caesar shifted ciphertext

```
Gyyn Gy un 7JG
```

Test all possible shifts (26-letter alphabet A-Z)

Manual decryption and parameters

★ Shift/Key (number): 3

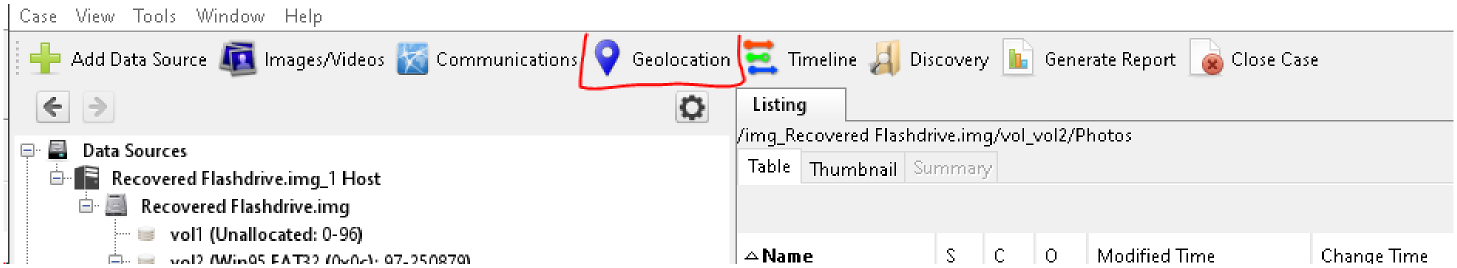
● Use the English alphabet (26 letters from A to Z)
○ Use the English alphabet and also shift the digits 0-9
○ Use the latin alphabet in the time of Caesar (23 letters, no J, U or W)

Brute-Force mode: the 25 shifts (for the alphabet ABCDEFGHIJKLMNOPQRSTUVWXYZ) are tested and sorted from most probable to least probable.

↑↓	↑↓
→20 (←6)	Meet Me at 7PM
→6 (←20)	Assh As oh 7DA
→2 (←24)	Ewwl Ew sl 7HE
→13 (←13)	Tlla Tl ha 7WT

4. Which provided the answer first try

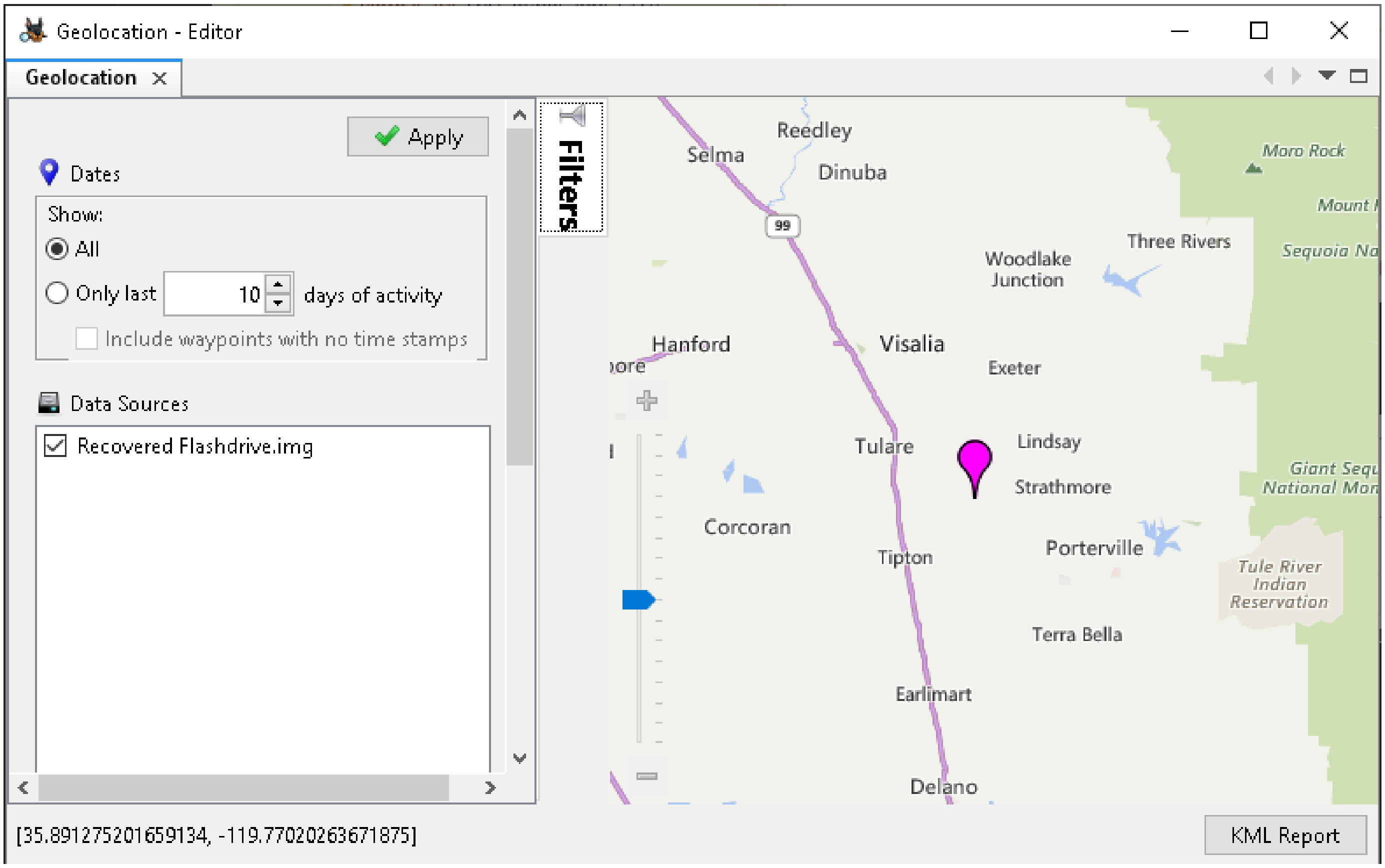
14. Looking at the "Geolocation" tab in Autopsy will provide the next answer



/img_Recovered Flashdrive.img/vol_vol2/Photos

- Data Sources
  - Recovered Flashdrive.img_1 Host
    - Recovered Flashdrive.img
      - vol1 (Unallocated: 0-96)
      - vol2 (Win95 FAT32 (0x0c): 97-250879)

1. Opening this tab will show a map with one Pin on it, that being the location the photo was taken at

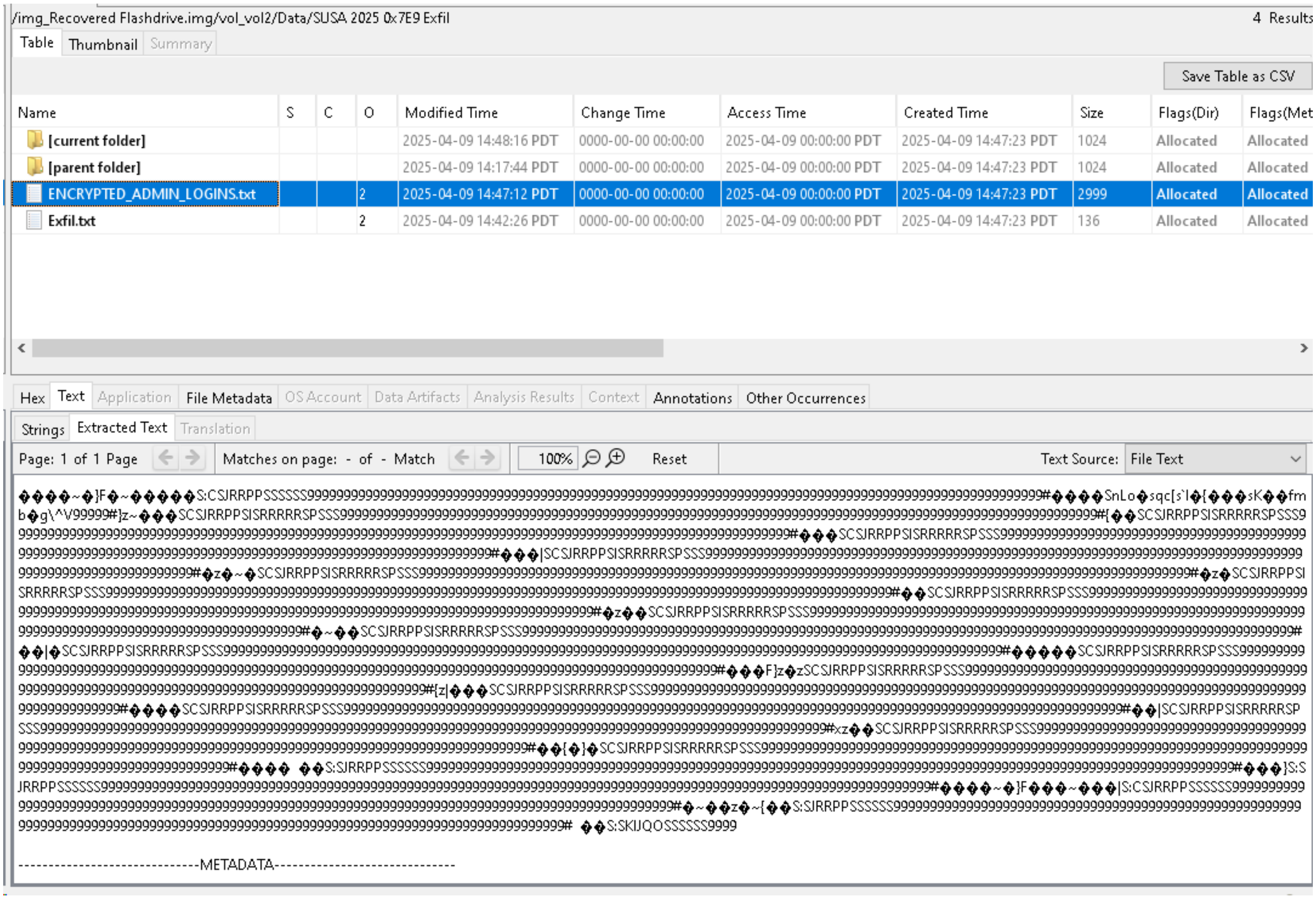


● All
○ Only last 10 days of activity
□ Include waypoints with no time stamps

☑ Recovered Flashdrive.img

[35.891275201659134, -119.77020263671875]

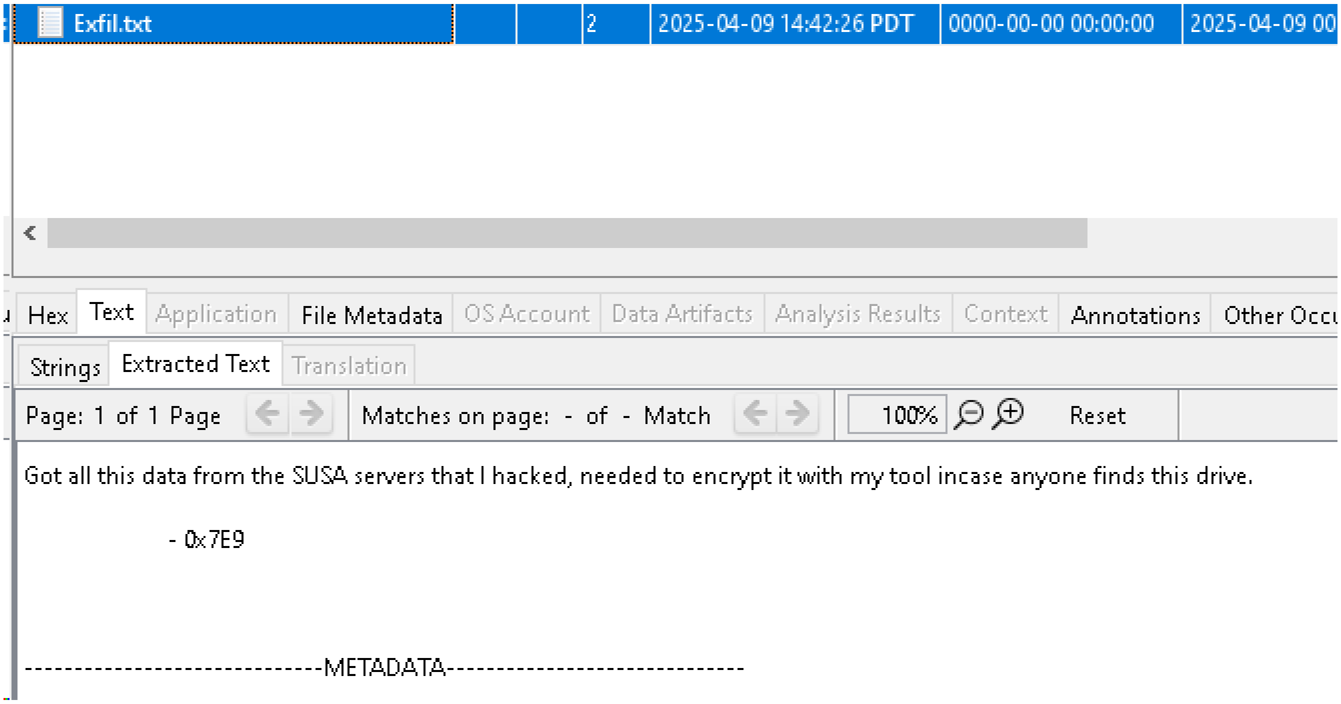
15. Looking through the image of the drive the "Data" folder can be found, which houses some sensitive password and logins in an encrypted format in the file "ENCRYPTED_ADMIN_LOGINS.txt.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Met
[current folder]				2025-04-09 14:48:16 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:23 PDT	1024	Allocated	Allocated
[parent folder]				2025-04-09 14:17:44 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:23 PDT	1024	Allocated	Allocated
ENCRYPTED_ADMIN_LOGINS.txt			2	2025-04-09 14:47:12 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:23 PDT	2999	Allocated	Allocated
Exfil.txt			2	2025-04-09 14:42:26 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:23 PDT	136	Allocated	Allocated

```
����~�}F�~�����S:CSJRRPPSSSSS999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#����SnLo�sqc[s`l�{���sK��fm
b�g\^V99999#}z~���SCSJRRPPSISRRRRRSPSSS999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#[��SCSJRRPPSISRRRRRSPSSS9
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#���SCSJRRPPSISRRRRRSPSSS9999999999999999999999999999999999999999999999999999999999999999999999
9999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#���|SCSJRRPPSISRRRRRSPSSS9999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
9999999999999999999999999999999999999999#�z�~�SCSJRRPPSISRRRRRSPSSS999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#�z�SCSJRRPPSI
SRRRRRSPSSS99999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#��SCSJRRPPSISRRRRRSPSSS99999999999999999999999999999999999999999999999999
9999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#�z��SCSJRRPPSISRRRRRSPSSS99999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999#�~��SCSJRRPPSISRRRRRSPSSS999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#
��|�SCSJRRPPSISRRRRRSPSSS99999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#�����SCSJRRPPSISRRRRRSPSSS99999999999999999999
99999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#���F}z�zSCSJRRPPSISRRRRRSPSSS99999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#{z|���SCSJRRPPSISRRRRRSPSSS999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
99999999999999999999#����SCSJRRPPSISRRRRRSPSSS99999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#��|SCSJRRPPSISRRRRRSP
SSS99999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#xz��SCSJRRPPSISRRRRRSPSSS999999999999999999999999999999999999999999999999999999999999
99999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#��{�}�SCSJRRPPSISRRRRRSPSSS999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
99999999999999999999999999999999999999999999999999#����  ��S:SJRRPPSSSSS99999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#���}S:S
JRRPPSSSSS99999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#����~�}F���~���|S:CSJRRPPSSSSS99999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#�~��z�~{��S:SJRRPPSSSSS9999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999#  ��S:SKIJQOSSSSSS9999

-----------------------------METADATA-----------------------------
```

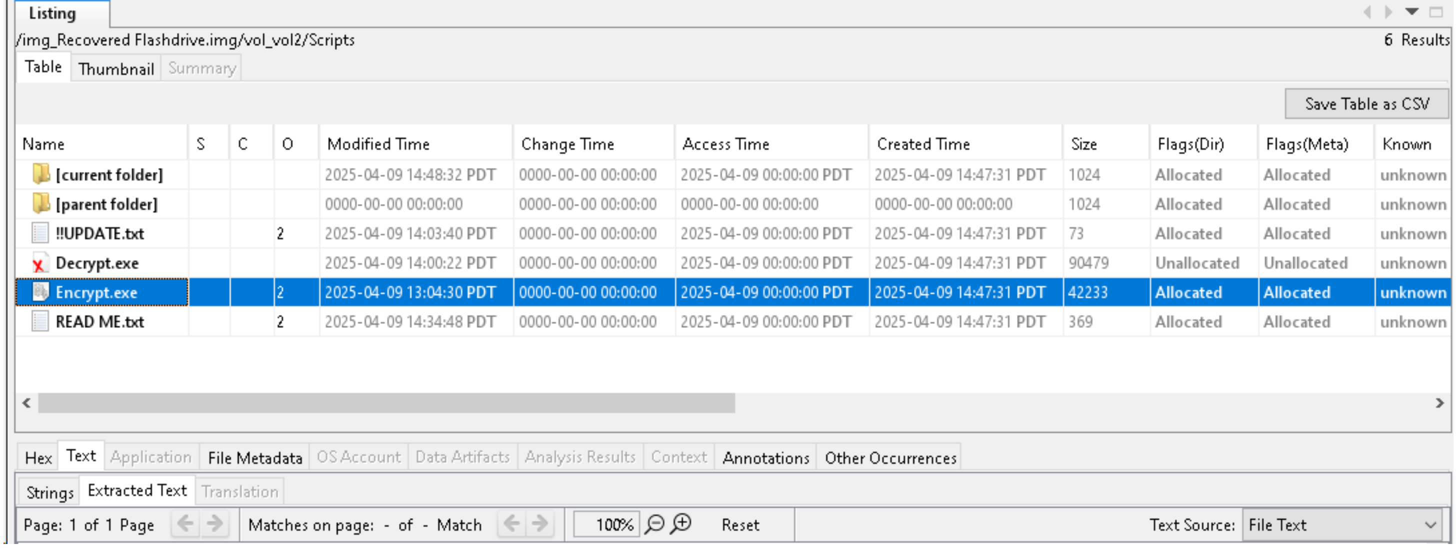
16. Opening the file "Exfil.txt" will show that the owner of the flash drive used some kind of script to encrypt this file, which means that there might also be a decryption script somewhere.



Exfil.txt			2	2025-04-09 14:42:26 PDT	0000-00-00 00:00:00	2025-04-09 00

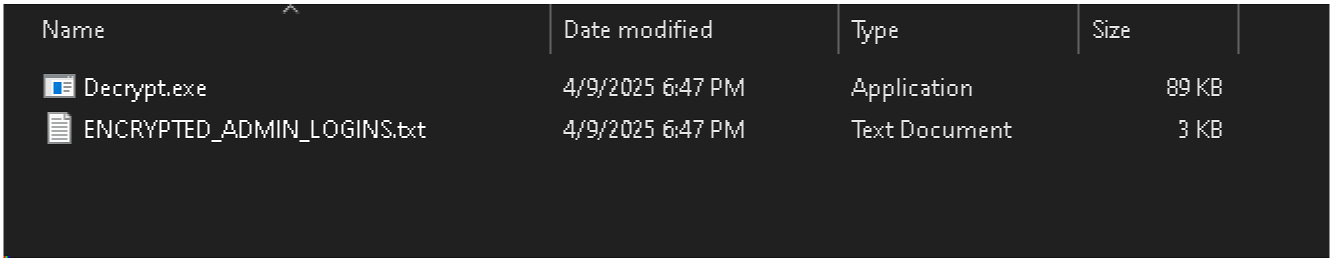
```
Got all this data from the SUSA servers that I hacked, needed to encrypt it with my tool incase anyone finds this drive.

          - 0x7E9



-----------------------------METADATA-----------------------------
```

17. Moving to the "Scripts" folder an "Encrypt.exe" file can be found ready to use, but also a "Decrypt.exe" file that has been deleted for some reason.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
[current folder]				2025-04-09 14:48:32 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:31 PDT	1024	Allocated	Allocated	unknown
[parent folder]				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1024	Allocated	Allocated	unknown
!!UPDATE.txt			2	2025-04-09 14:03:40 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:31 PDT	73	Allocated	Allocated	unknown
Decrypt.exe				2025-04-09 14:00:22 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:31 PDT	90479	Unallocated	Unallocated	unknown
Encrypt.exe			2	2025-04-09 13:04:30 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:31 PDT	42233	Allocated	Allocated	unknown
READ ME.txt			2	2025-04-09 14:34:48 PDT	0000-00-00 00:00:00	2025-04-09 00:00:00 PDT	2025-04-09 14:47:31 PDT	369	Allocated	Allocated	unknown

18. Right clicking on the "Decrypt.exe" file and selecting `Export file(s)` will show a new window to save the file.
19. After saving the file return to "Data/SUSA 2025 0x7E9 exfil/" and save the "ENCRYPTED_ADMIN_LOGIN.txt" to the host machine.
20. Navigate to the folder that has both those files

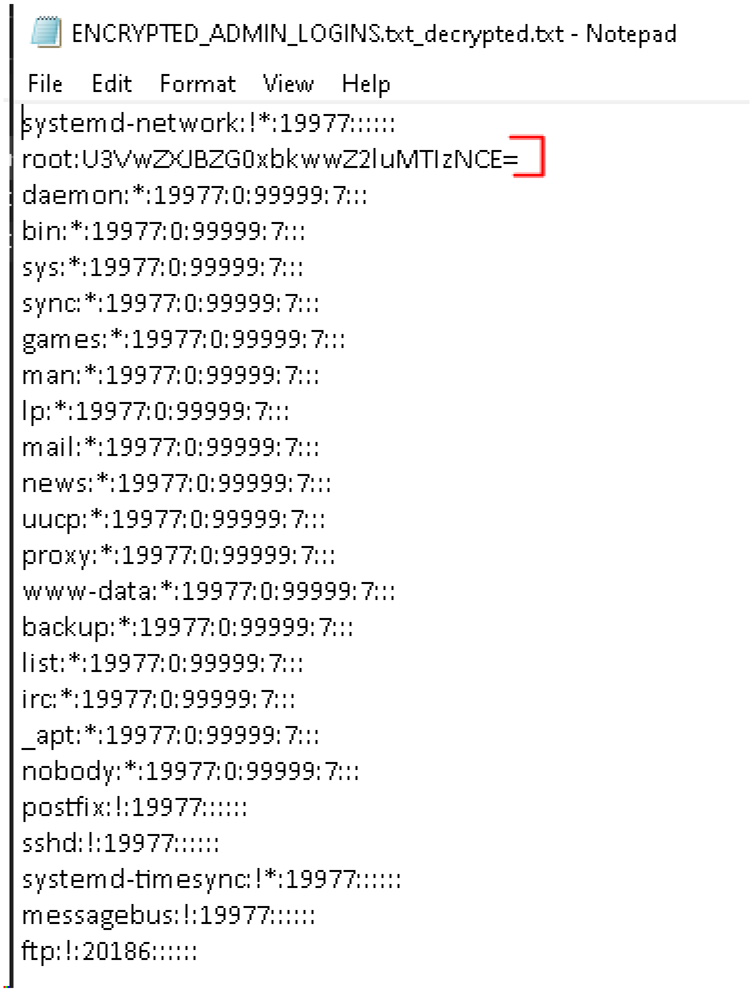


Name	Date modified	Type	Size
Decrypt.exe	4/9/2025 6:47 PM	Application	89 KB
ENCRYPTED_ADMIN_LOGINS.txt	4/9/2025 6:47 PM	Text Document	3 KB

    1. **Note:** Windows warns against running "Decrypt.exe", press "more options" and "run anyway"

21. **Either** Left click and drag the text document into the "Decrypt.exe" **OR** open the folder in command prompt and run "Decrypt.exe ENCRYPTED_ADMIN_LOGINS.txt"
    1. This will decrypt the files and make a new text document called "ENCRYPTED_ADMIN_LOGINS.txt_decrypted.txt"

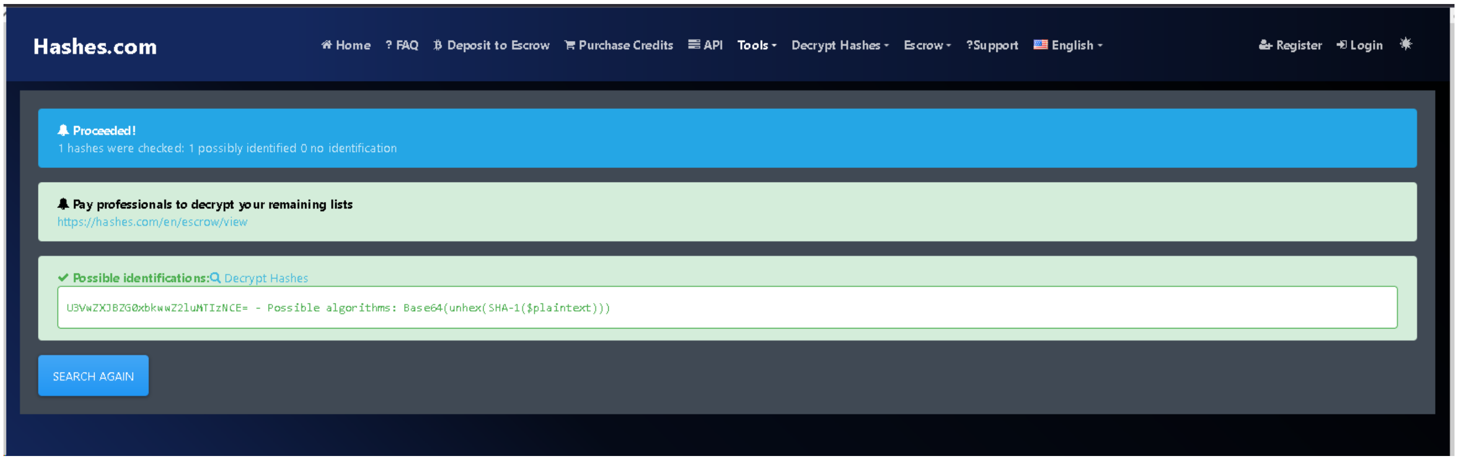
22. Open the newly made file and look for the root user



ENCRYPTED_ADMIN_LOGINS.txt_decrypted.txt - Notepad
File Edit Format View Help

```
systemd-network:!*:19977::::::
root:U3VwZXJBZG0xbkwwZ2luMTIzNCE=
daemon:*:19977:0:99999:7:::
bin:*:19977:0:99999:7:::
sys:*:19977:0:99999:7:::
sync:*:19977:0:99999:7:::
games:*:19977:0:99999:7:::
man:*:19977:0:99999:7:::
lp:*:19977:0:99999:7:::
mail:*:19977:0:99999:7:::
news:*:19977:0:99999:7:::
uucp:*:19977:0:99999:7:::
proxy:*:19977:0:99999:7:::
www-data:*:19977:0:99999:7:::
backup:*:19977:0:99999:7:::
list:*:19977:0:99999:7:::
irc:*:19977:0:99999:7:::
_apt:*:19977:0:99999:7:::
nobody:*:19977:0:99999:7:::
postfix:!:19977::::::
sshd:!:19977::::::
systemd-timesync:!*:19977::::::
messagebus:!:19977::::::
ftp:!:20186::::::
```

23. This is seemingly a linux shadow file, which means the format for entries is **USER:HASHED_PASSWORD**, looking at the file, the root user has some kind of hashed password trailing it. Using a terminal utility like *hashid* on Linux or a site like *hashes.com* will quickly analyze the hash and find that its Base64



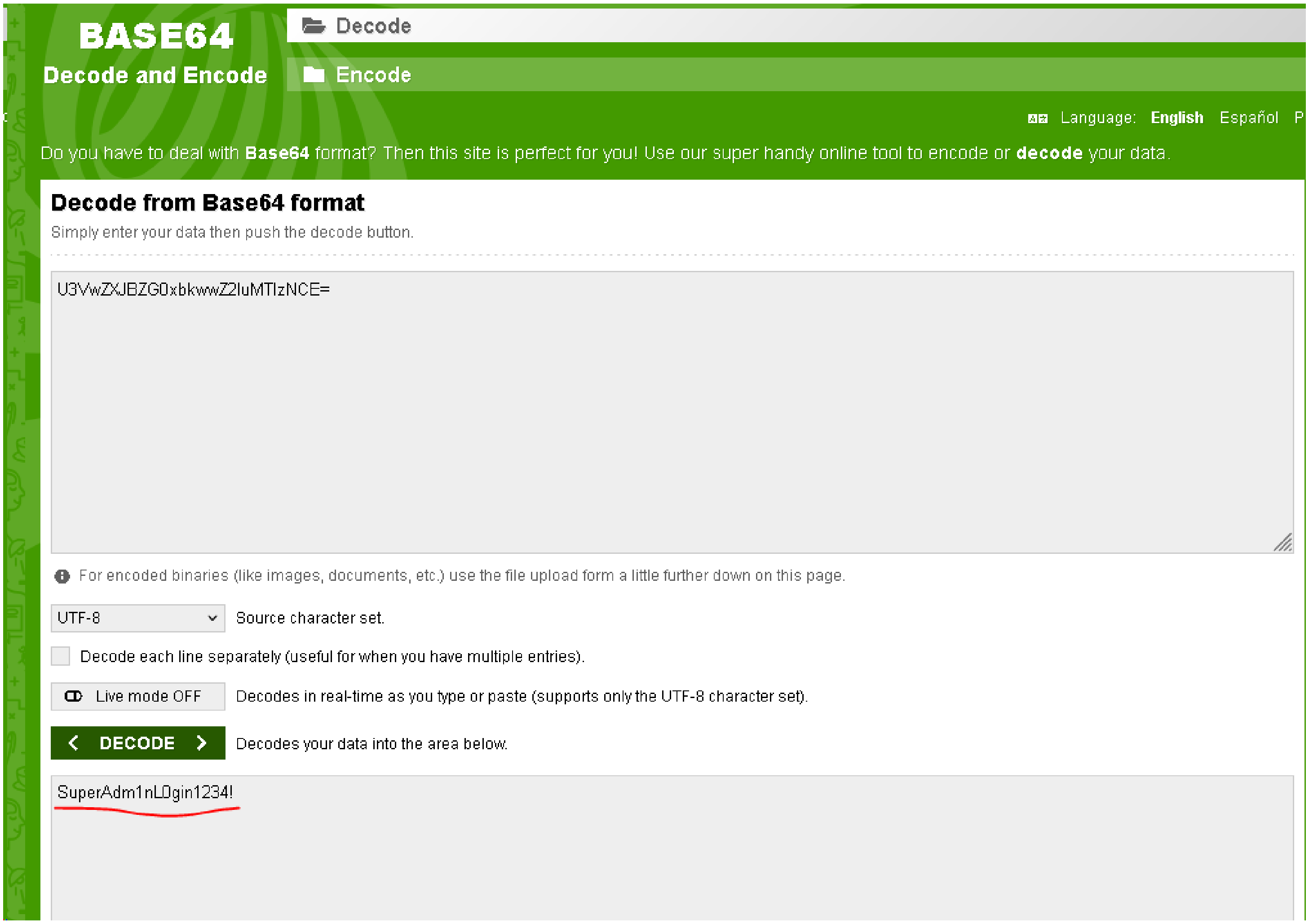
Proceeded!
1 hashes were checked: 1 possibly identified 0 no identification

Pay professionals to decrypt your remaining lists
https://hashes.com/en/escrow/view

✓ **Possible identifications:** Decrypt Hashes

```
U3VwZXJBZG0xbkwwZ2luMTIzNCE= - Possible algorithms: Base64(unhex(SHA-1($plaintext)))
```

24. Using a tool to decode the Base64 to a human readable format will provide this



Do you have to deal with **Base64** format? Then this site is perfect for you! Use our super handy online tool to encode or **decode** your data.

Decode from Base64 format

Simply enter your data then push the decode button.

```
U3VwZXJBZG0xbkwwZ2luMTIzNCE=
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

Decodes your data into the area below.

```
SuperAdm1nL0gin1234!
```

   1. "SuperAdm1nL0gin1234!" as the hashed password

25. I would highly recommend trying to reverse engineer the Encrypt and Decrypt executables! Learning how the encryption works could lead to even more answers being uncovered!