vishwaCTF

CHALLENGE NAME: [Spvault]

DEV: [Yash Swami]

CATEGORY: [Digital Forensics]

LEVEL: [MEDIUM]

2025

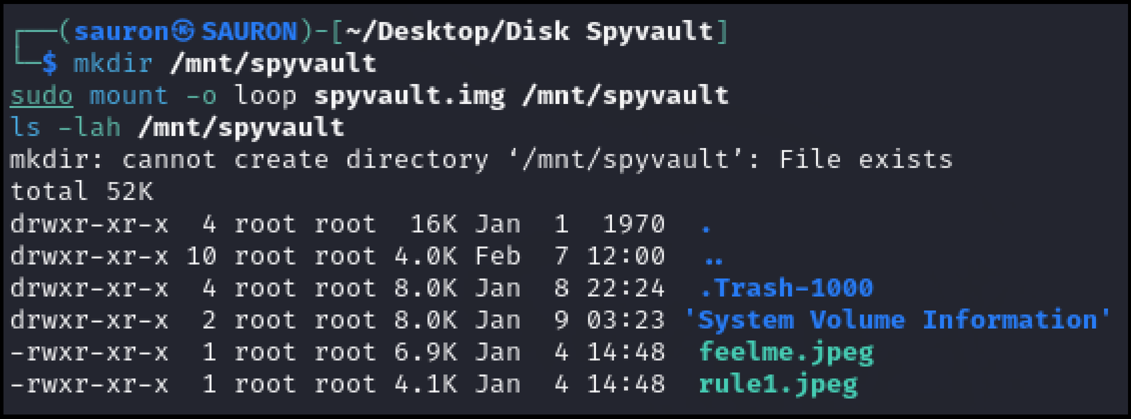
Challenge Description: A masterpiece of concealment, a labyrinth of distractions, false leads, and buried truths. Somewhere within lies the key to a covert exchange-a name and a location that could shift the tides of power. Those who held this secret are long gone, but their trail lingers like a ghost in the machine.

Solution:

Challenge Files Provided

- **Disk image**: A forensic disk image containing multiple hidden clues.
- **Hints embedded within images and text files.**
- **Dummy images and files to mislead solvers.**

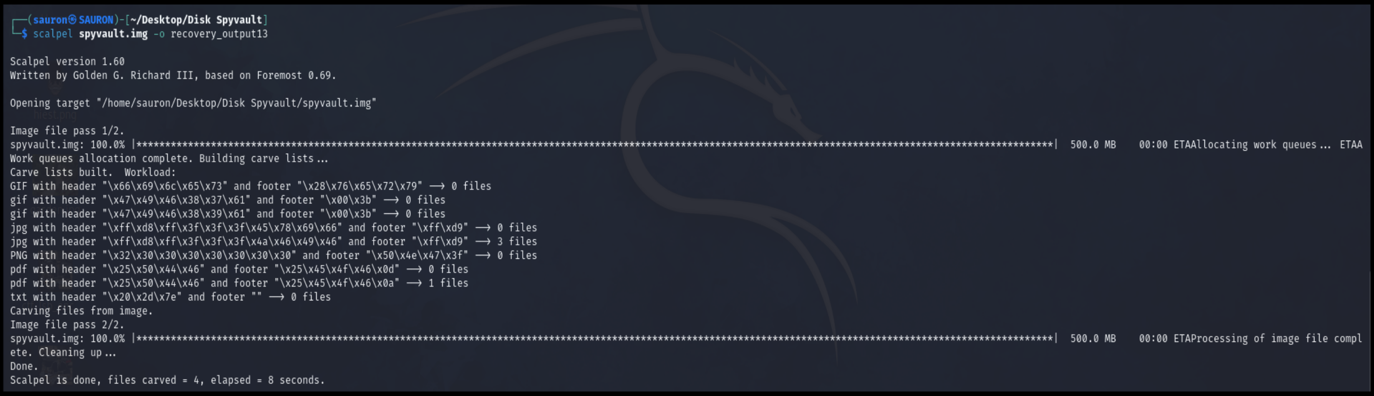
1. Mounting the Disk Image



```
┌──(sauron㉿SAURON)-[~/Desktop/Disk Spyvault]
└─$ mkdir /mnt/spyvault
sudo mount -o loop spyvault.img /mnt/spyvault
ls -lah /mnt/spyvault
mkdir: cannot create directory ‘/mnt/spyvault’: File exists
total 52K
drwxr-xr-x  4 root root  16K Jan  1  1970  .
drwxr-xr-x 10 root root 4.0K Feb  7 12:00  ..
drwxr-xr-x  4 root root 8.0K Jan  8 22:24  .Trash-1000
drwxr-xr-x  2 root root 8.0K Jan  9 03:23 'System Volume Information'
-rwxr-xr-x  1 root root 6.9K Jan  4 14:48  feelme.jpeg
-rwxr-xr-x  1 root root 4.1K Jan  4 14:48  rule1.jpeg
```

2. Recovering Deleted Files

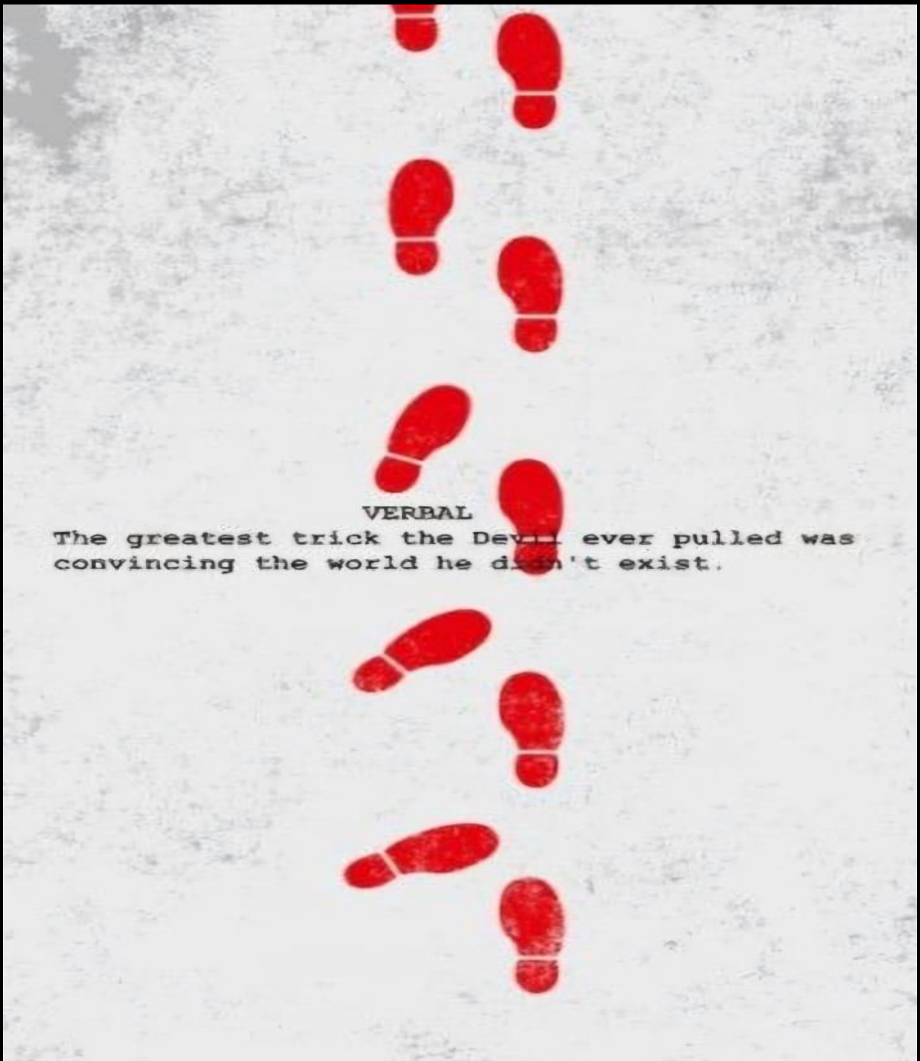
The next step is to recover deleted files, as they may contain crucial clues:



```
┌──(sauron㉿SAURON)-[~/Desktop/Disk Spyvault]
└─$ scalpel spyvault.img -o recovery_output13

Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/home/sauron/Desktop/Disk Spyvault/spyvault.img"

Image file pass 1/2.
spyvault.img: 100.0% |****************************************************************************************************************|  500.0 MB    00:00 ETAAllocating work queues...  ETAA
Work queues allocation complete. Building carve lists...
Carve lists built.  Workload:
GIF with header "\x66\x69\x6c\x65\x73" and footer "\x28\x76\x65\x72\x79" ⟶ 0 files
gif with header "\x47\x49\x46\x38\x37\x61" and footer "\x00\x3b" ⟶ 0 files
gif with header "\x47\x49\x46\x38\x39\x61" and footer "\x00\x3b" ⟶ 0 files
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x45\x78\x69\x66" and footer "\xff\xd9" ⟶ 0 files
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x4a\x46\x49\x46" and footer "\xff\xd9" ⟶ 3 files
PNG with header "\x32\x30\x30\x30\x30\x30\x30\x30" and footer "\x50\x4e\x47\x3f" ⟶ 0 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0d" ⟶ 0 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0a" ⟶ 1 files
txt with header "\x20\x2d\x7e" and footer "" ⟶ 0 files
Carving files from image.
Image file pass 2/2.
spyvault.img: 100.0% |****************************************************************************************************************|  500.0 MB    00:00 ETAProcessing of image file compl
ete. Cleaning up...
Done.
Scalpel is done, files carved = 4, elapsed = 8 seconds.
```

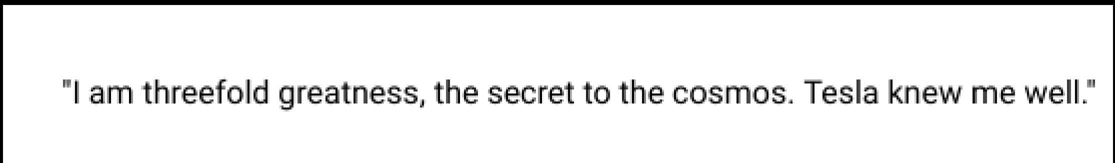
3. Analyze recovered files

The recovered files include one image and a pdf file.



VERBAL
The greatest trick the Devil ever pulled was convincing the world he didn't exist.

The image shows there is more to reveal.



"I am threefold greatness, the secret to the cosmos. Tesla knew me well."

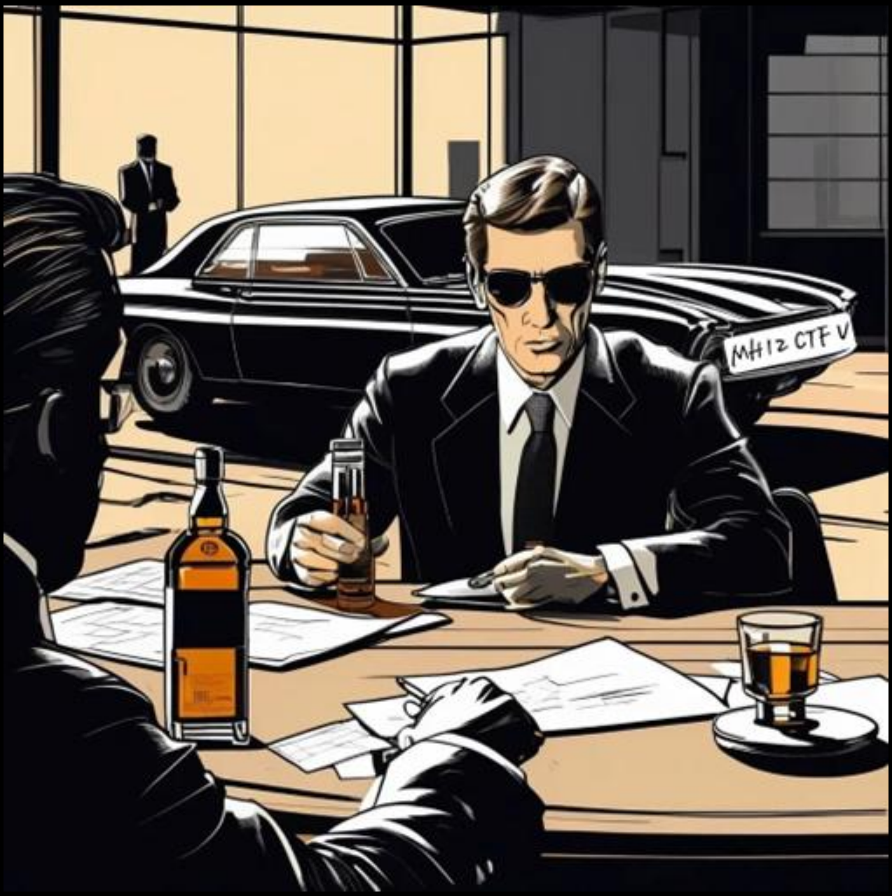
The pdf file holds some kind of riddle

ANSWER:”369”

4. **Identifying Steganography**

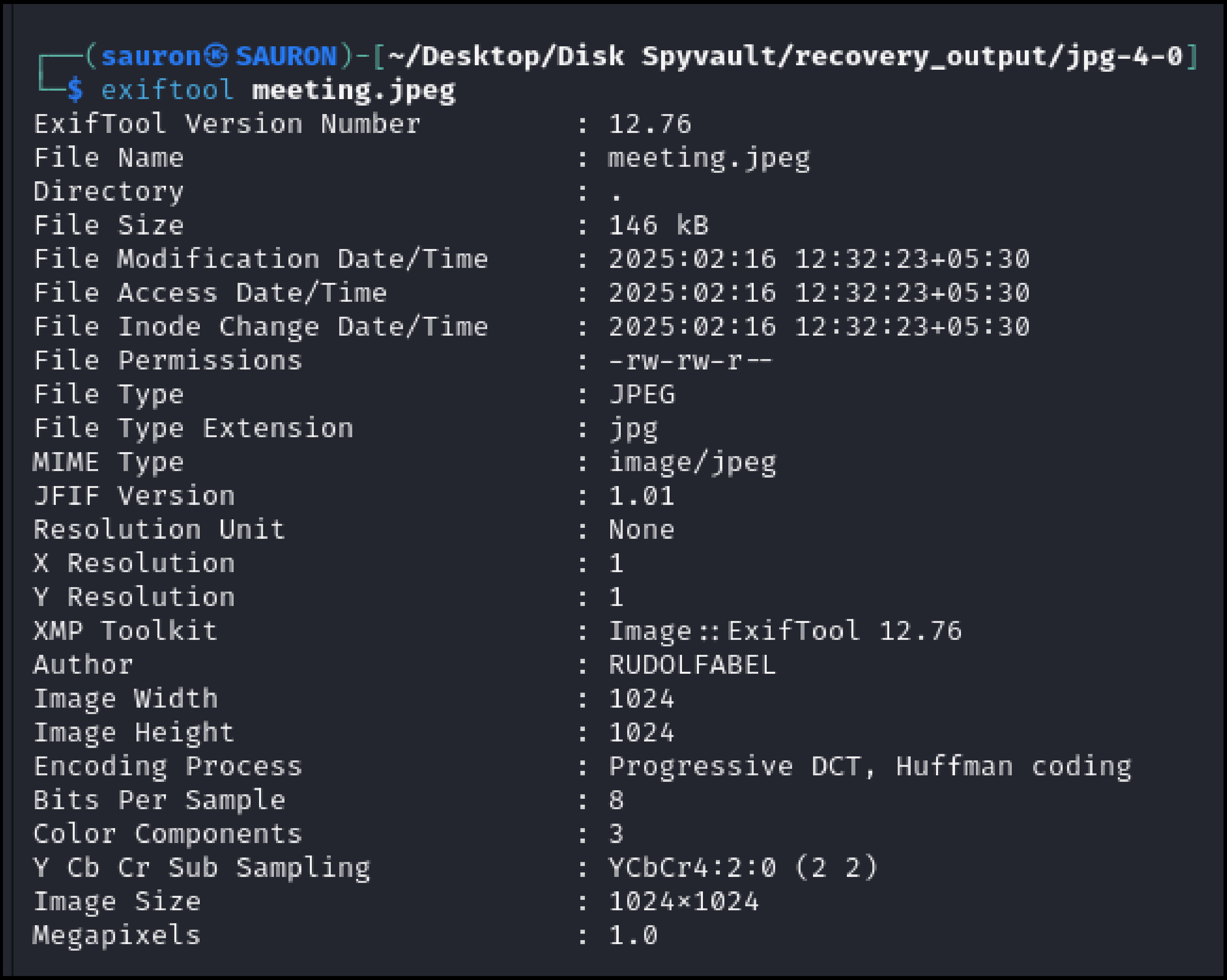
One of the images in the recovered files might contain a hidden message. Use steghide to extract it:

This you give you file named meeting.jpeg



The goal was to find the identity and location of the spy. The car in background will provide us location “MH12” -PUNE

5. **Analyzing Image Metadata**
Extracting metadata from images:



```
┌──(sauron㉿SAURON)-[~/Desktop/Disk Spyvault/recovery_output/jpg-4-0]
└─$ exiftool meeting.jpeg
ExifTool Version Number         : 12.76
File Name                       : meeting.jpeg
Directory                       : .
File Size                       : 146 kB
File Modification Date/Time     : 2025:02:16 12:32:23+05:30
File Access Date/Time           : 2025:02:16 12:32:23+05:30
File Inode Change Date/Time     : 2025:02:16 12:32:23+05:30
File Permissions                : -rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
XMP Toolkit                     : Image::ExifTool 12.76
Author                          : RUDOLFABEL
Image Width                     : 1024
Image Height                    : 1024
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1024x1024
Megapixels                      : 1.0
```

The **author field** in the metadata reveals: **RUDOLFABEL**

Flag: VishwaCtf{RUDOLFABEL_PUNE}