Writeup for CID

Name : CID

Domain : Steganography

Difficulty : Medium

Description : Watch the image carefully!!!

Points : 300

Author : Ankush Kaudi

File given : case69.jpg

We have been given with a jpg file case69.jpg. Using binwalk on this image file gives info that there is 7-zip file in this image.

```
┌──(root㉿Kali)-[~/Desktop/steg]
└─# binwalk case69.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
1078146       0x107382        7-zip archive data, version 0.4
```

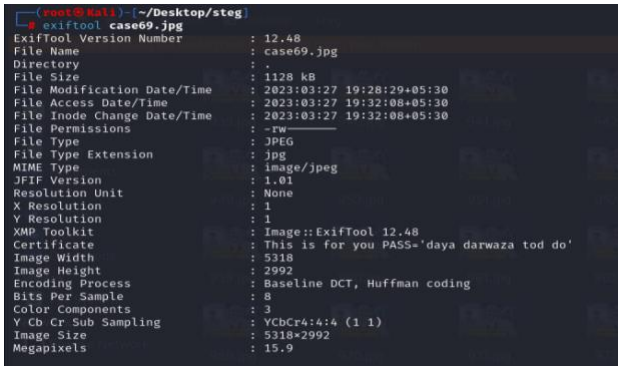
The 7-zip file can be extracted using the command “7za e code69.jpg” which gives 1000 images and 1 text file.

```
Scanning the drive for archives:
1 file, 1128202 bytes (1102 KiB)

Extracting archive: case69.jpg
--
Path = case69.jpg
Type = 7z
Offset = 1078146
Physical Size = 50056
Headers Size = 925
Method = LZMA2:24m
Solid = +
Blocks = 1

Everything is Ok

Folders: 1
Files: 1001
Size:       24381050
Compressed: 1128202
```

The text file says “You are very close mate. The flag is just around here. Hope you find it.”

The flag might be in any of the image.

Using exiftool gives the following



We can see a PASS which is “daya darwaza tod do” which might be a password to extract the flag.

Steghide is one such tool which uses password to hide secret files in images. But extracting hidden file for 1000 images might be tedious.

We can use the shell command to perform one steghide command on all the images.

We can use shell command using “export PS1=‘$ ‘” command. A shell will get created.

Executing below command will extract flag.txt which has the flag.

“ls | while read line; do steghide extract -sf $line -p "daya darwaza tod do"; done”

Using cat flag.txt will display the flag

Flag is : VishwaCTF{my_GOD_D4ya_tumn3_t0_fl4g_dhund_liy4....}