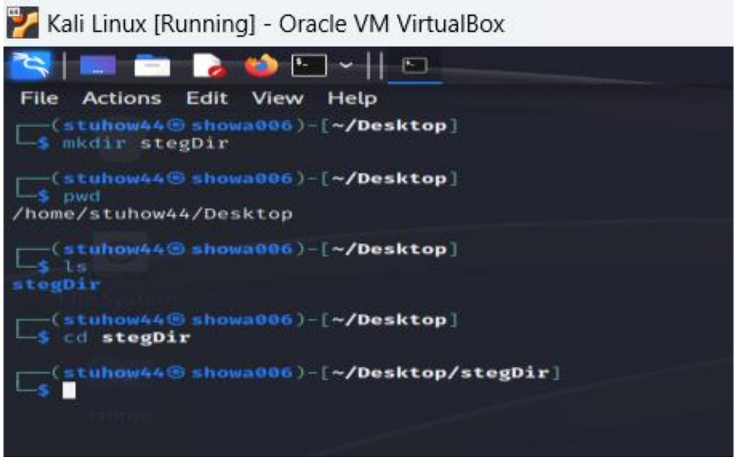
Assignment-6: Steganography

CYSE450- Ethical Hacking and Penetration Testing

(Total: 100 Points)

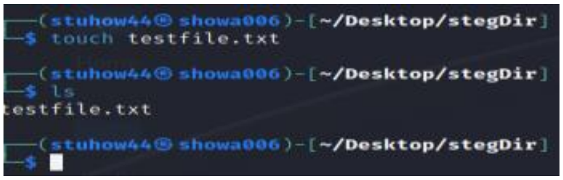
Complete all the tasks and submit the screenshot for all the steps with their respective step numbers.

1. Open the terminal in Kali Linux.
2. Create a new directory **stegDir**, using the correct Linux command.
3. Switch/change to **stegDir** directory.

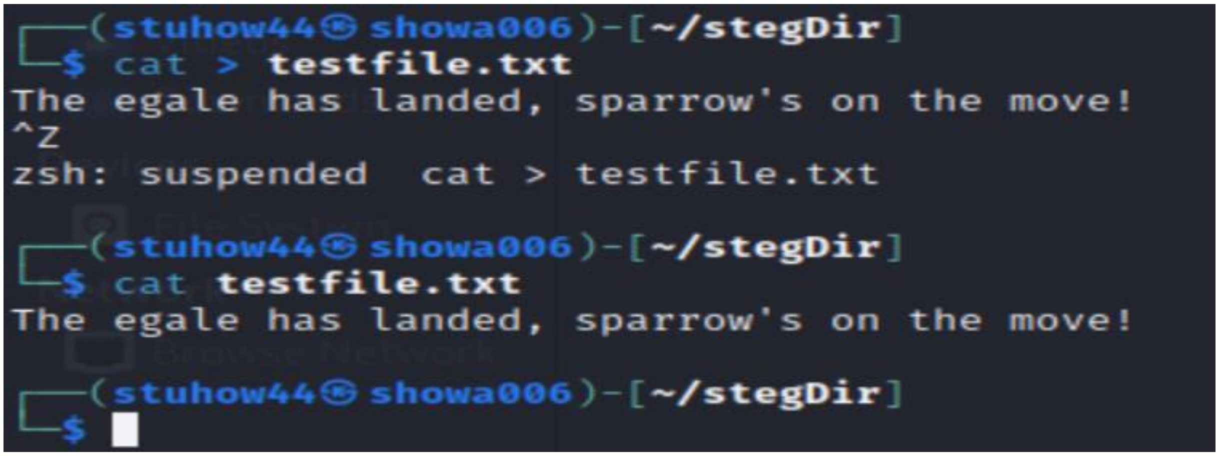


```
┌──(stuhow44㉿ showa006)-[~/Desktop]
└─$ mkdir stegDir

┌──(stuhow44㉿ showa006)-[~/Desktop]
└─$ pwd
/home/stuhow44/Desktop

┌──(stuhow44㉿ showa006)-[~/Desktop]
└─$ ls
stegDir

┌──(stuhow44㉿ showa006)-[~/Desktop]
└─$ cd stegDir

┌──(stuhow44㉿ showa006)-[~/Desktop/stegDir]
└─$ 
```

4. Create a new file **testfile.txt** and add some secret message there as the file content.

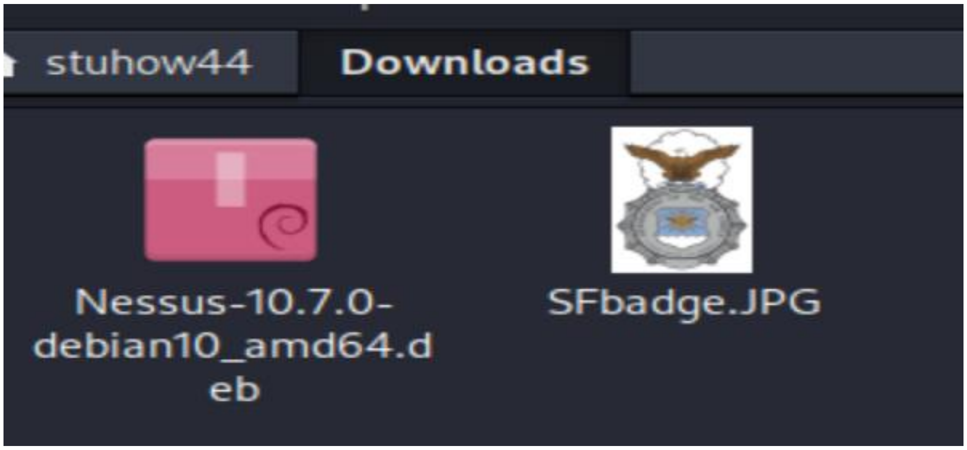


```
──(stuhow44㉿ showa006)-[~/Desktop/stegDir]
└─$ touch testfile.txt

──(stuhow44㉿ showa006)-[~/Desktop/stegDir]
└─$ ls
testfile.txt

──(stuhow44㉿ showa006)-[~/Desktop/stegDir]
└─$ 
```

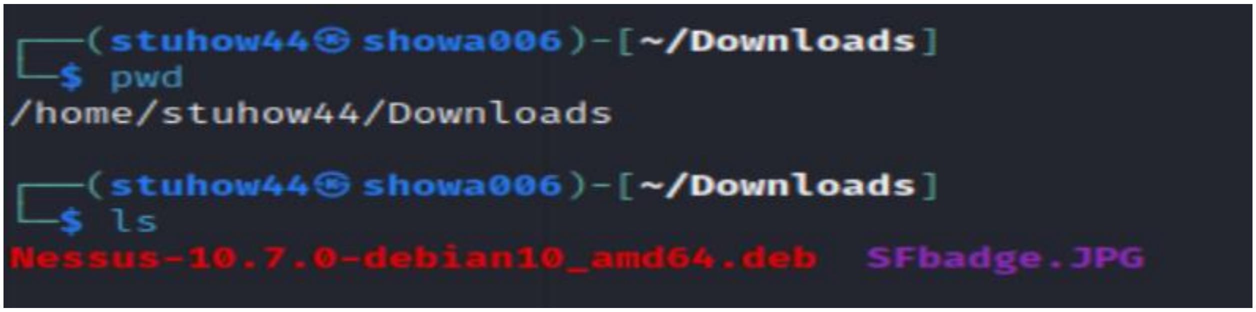


```
┌──(stuhow44㉿showa006)-[~/stegDir]
└─$ cat > testfile.txt
The egale has landed, sparrow's on the move!
^Z
zsh: suspended  cat > testfile.txt

┌──(stuhow44㉿showa006)-[~/stegDir]
└─$ cat testfile.txt
The egale has landed, sparrow's on the move!

┌──(stuhow44㉿showa006)-[~/stegDir]
└─$ 
```

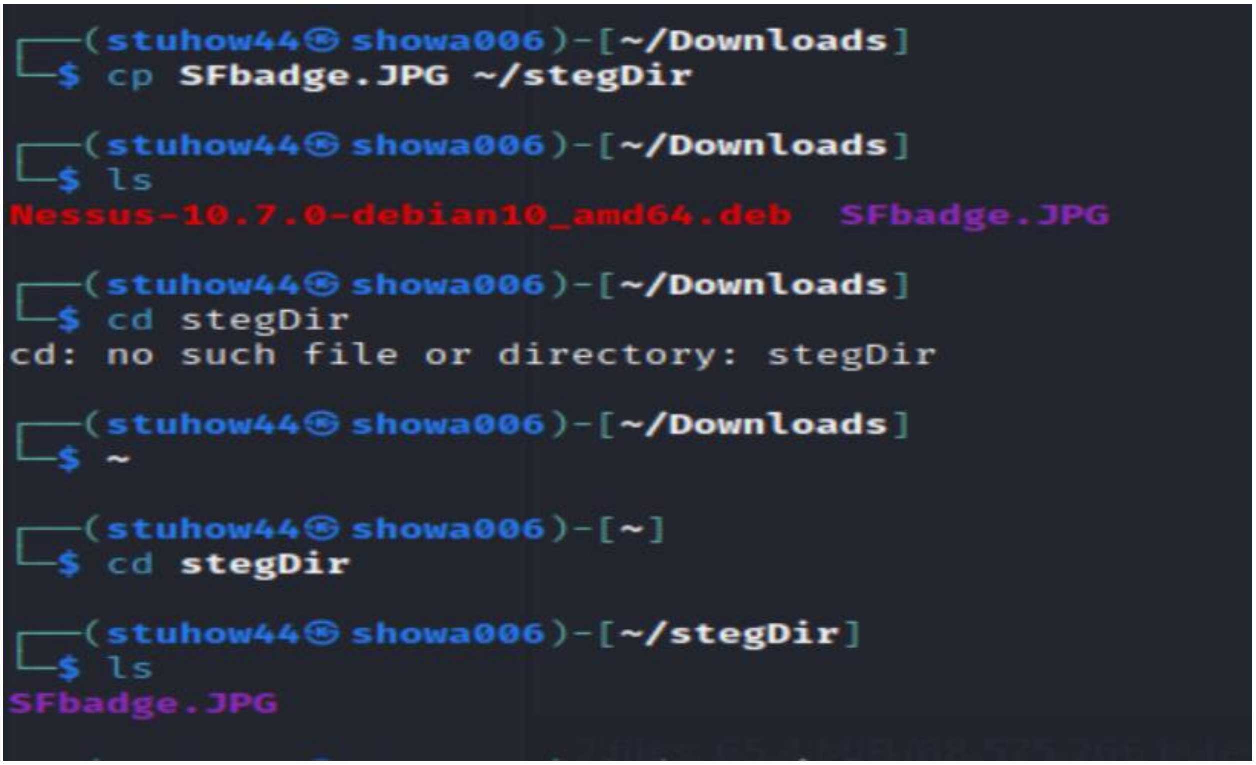
5. Open a browser (Firefox) in Kali Linux and search for image/icon of your choice. Save the image (as .jpeg, for example)to the stegDir folder/directory. [Usually, the downloaded picture will be saved in the Downloads folder by default. So, you need to copy that picture to the stegDir directory/folder. You may use Linux command to copy the image to stegDir.]



I realized that details matter, I spent probably over an hour trying to copy the JPEG image to the correct folder when I realized that it wasn't copying because I was not typing the file name incorrectly.



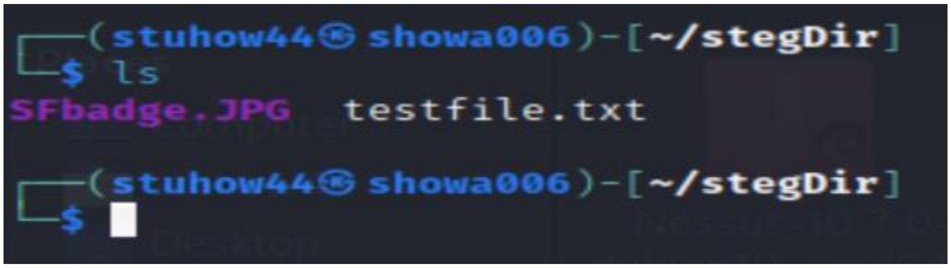
```
┌──(stuhow44㉿showa006)-[~/Downloads]
└─$ pwd
/home/stuhow44/Downloads

┌──(stuhow44㉿showa006)-[~/Downloads]
└─$ ls
Nessus-10.7.0-debian10_amd64.deb  SFbadge.JPG
```



```
┌──(stuhow44㉿showa006)-[~/Downloads]
└─$ cp SFbadge.JPG ~/stegDir

┌──(stuhow44㉿showa006)-[~/Downloads]
└─$ ls
Nessus-10.7.0-debian10_amd64.deb  SFbadge.JPG

┌──(stuhow44㉿showa006)-[~/Downloads]
└─$ cd stegDir
cd: no such file or directory: stegDir

┌──(stuhow44㉿showa006)-[~/Downloads]
└─$ ~

┌──(stuhow44㉿showa006)-[~]
└─$ cd stegDir

┌──(stuhow44㉿showa006)-[~/stegDir]
└─$ ls
SFbadge.JPG
```

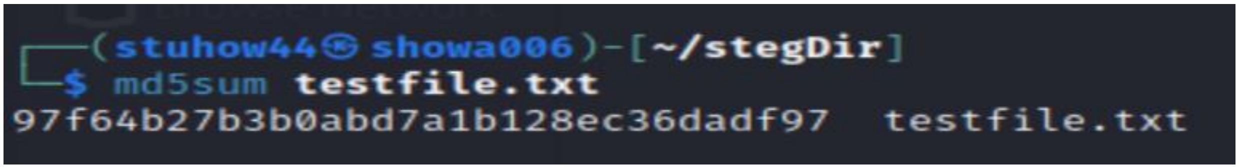
I remade the stegDir because I realized that it was in the Desktop Directory when I first made.

6. In terminal, being in the stegDir directory, execute the command for long display. [You should see Two files- textfile (testfile.txt) and the image file]

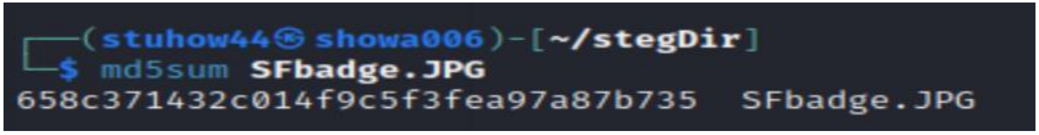


```
┌──(stuhow44㉿showa006)-[~/stegDir]
└─$ ls
SFbadge.JPG  testfile.txt

┌──(stuhow44㉿showa006)-[~/stegDir]
└─$ 
```

7. Execute the command md5sum



```
┌──(stuhow44㉿ showa006)-[~/stegDir]
└─$ md5sum testfile.txt
97f64b27b3b0abd7a1b128ec36dadf97  testfile.txt
```



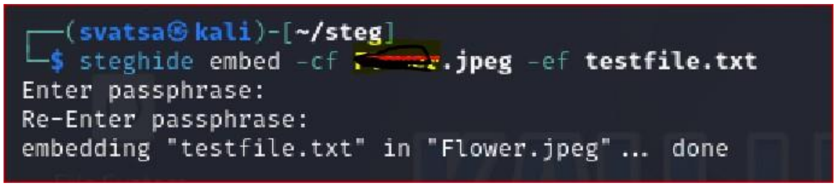
```
┌──(stuhow44㉿ showa006)-[~/stegDir]
└─$ md5sum SFbadge.JPG
658c371432c014f9c5f3fea97a87b735  SFbadge.JPG
```

8. Learn about steghide command here:

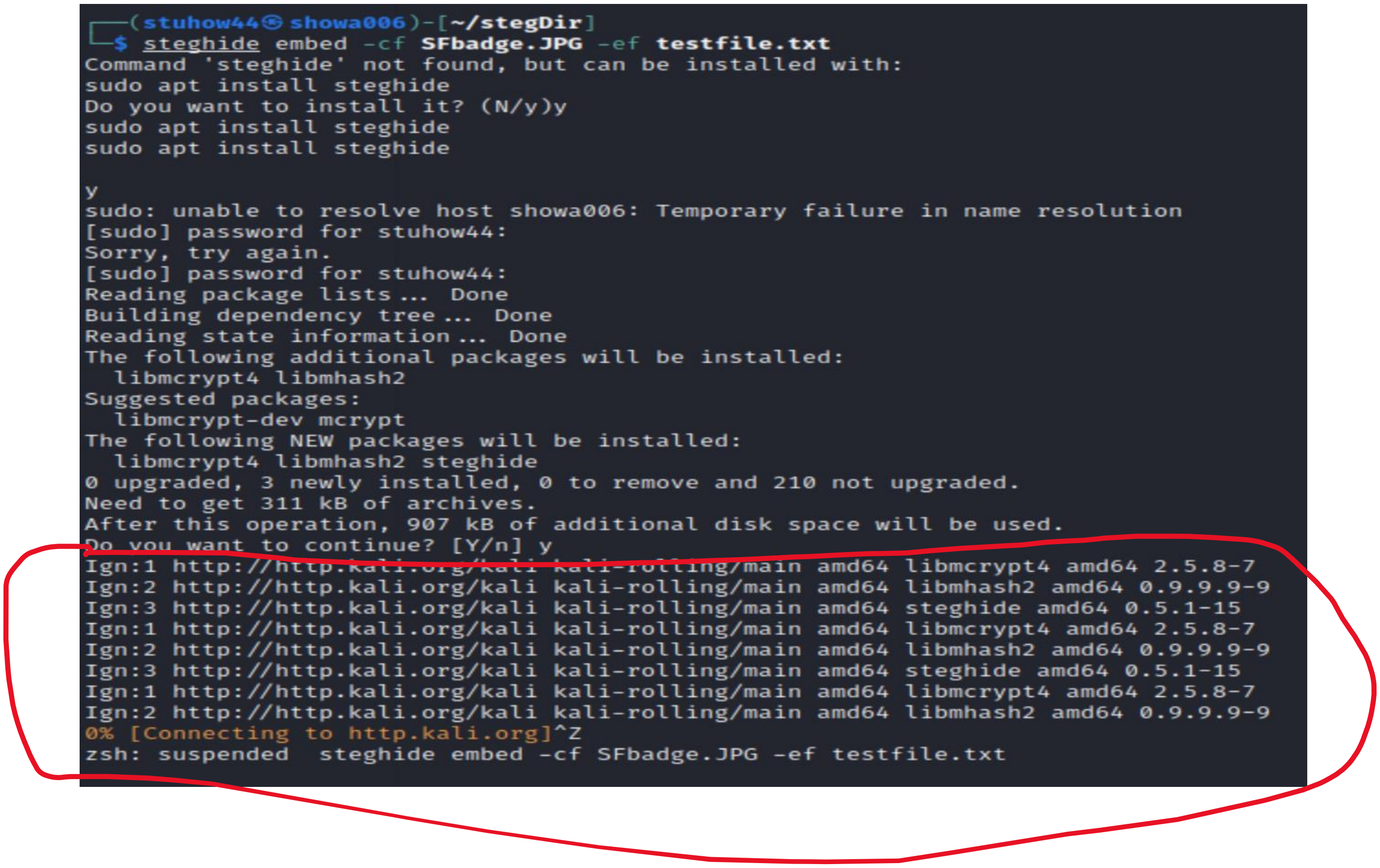
   https://steghide.sourceforge.net/documentation/manpage.php

   Use **steghide** command to embed your testfile.txt (with secret message) with the image file as shown in the following example screenshot:

   (When prompted for the passphrase, you may type any password of your choice)

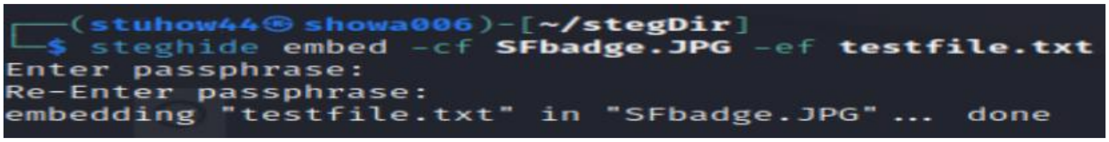


```
┌──(svatsa㉿kali)-[~/steg]
└─$ steghide embed -cf [redacted].jpeg -ef testfile.txt
Enter passphrase:
Re-Enter passphrase:
embedding "testfile.txt" in "Flower.jpeg"... done
```



```
┌──(stuhow44㉿ showa006)-[~/stegDir]
└─$ steghide embed -cf SFbadge.JPG -ef testfile.txt
Command 'steghide' not found, but can be installed with:
sudo apt install steghide
Do you want to install it? (N/y)y
sudo apt install steghide
sudo apt install steghide

y
sudo: unable to resolve host showa006: Temporary failure in name resolution
[sudo] password for stuhow44:
Sorry, try again.
[sudo] password for stuhow44:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libmcrypt4 libmhash2
Suggested packages:
  libmcrypt-dev mcrypt
The following NEW packages will be installed:
  libmcrypt4 libmhash2 steghide
0 upgraded, 3 newly installed, 0 to remove and 210 not upgraded.
Need to get 311 kB of archives.
After this operation, 907 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 libmcrypt4 amd64 2.5.8-7
Ign:2 http://http.kali.org/kali kali-rolling/main amd64 libmhash2 amd64 0.9.9.9-9
Ign:3 http://http.kali.org/kali kali-rolling/main amd64 steghide amd64 0.5.1-15
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 libmcrypt4 amd64 2.5.8-7
Ign:2 http://http.kali.org/kali kali-rolling/main amd64 libmhash2 amd64 0.9.9.9-9
Ign:3 http://http.kali.org/kali kali-rolling/main amd64 steghide amd64 0.5.1-15
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 libmcrypt4 amd64 2.5.8-7
Ign:2 http://http.kali.org/kali kali-rolling/main amd64 libmhash2 amd64 0.9.9.9-9
0% [Connecting to http.kali.org]^Z
zsh: suspended  steghide embed -cf SFbadge.JPG -ef testfile.txt
```

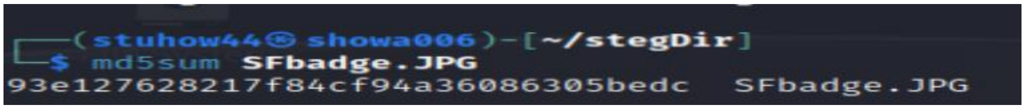
I cannot get steghide to install on my VM in Kali.



```
┌──(stuhow44㉿showa006)-[~/stegDir]
└─$ steghide embed -cf SFbadge.JPG -ef testfile.txt
Enter passphrase:
Re-Enter passphrase:
embedding "testfile.txt" in "SFbadge.JPG"... done
```

I figured out. I had to use root terminal to install steghide

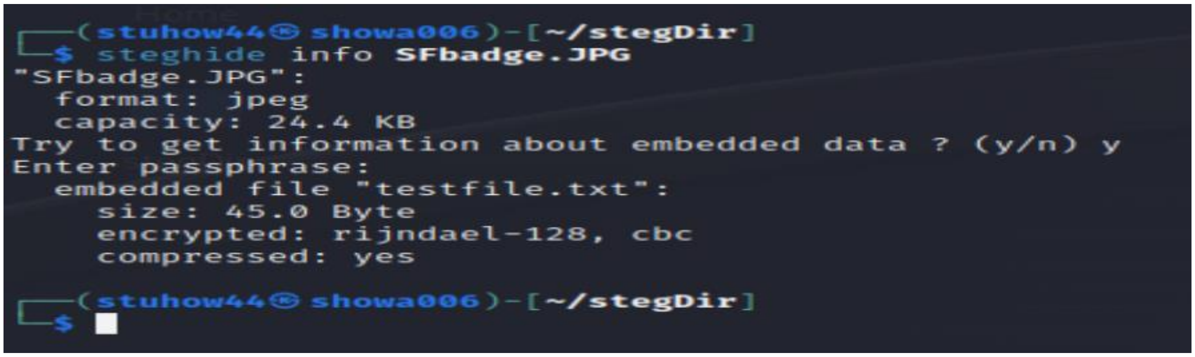
9. Execute the command md5sum for your jpeg image file to check the hash for the image file. **Do you see any difference?**



```
┌──(stuhow44㉿showa006)-[~/stegDir]
└─$ md5sum SFbadge.JPG
93e127628217f84cf94a36086305bedc  SFbadge.JPG
```

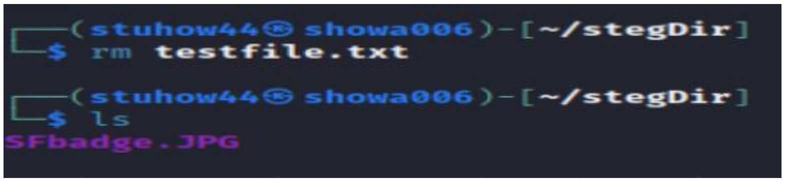
Yes there is a difference

10. Execute steghide command to get some information about it before extracting it, use the info command as shown in this following example screenshot:



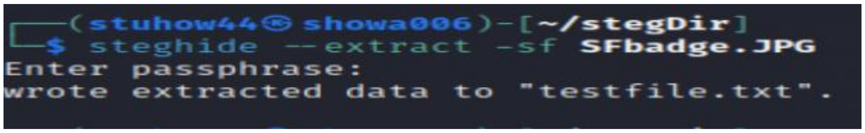
```
┌──(stuhow44㉿showa006)-[~/stegDir]
└─$ steghide info SFbadge.JPG
"SFbadge.JPG":
  format: jpeg
  capacity: 24.4 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "testfile.txt":
    size: 45.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes

┌──(stuhow44㉿showa006)-[~/stegDir]
└─$ █
```

11. Now, **delete** the file testfile.txt.



```
┌──(stuhow44㉿showa006)-[~/stegDir]
└─$ rm testfile.txt

┌──(stuhow44㉿showa006)-[~/stegDir]
└─$ ls
SFbadge.JPG
```

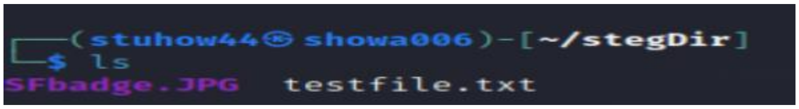
12. **Extract** the secret message by executing steghide command with **- - extract** option as follows:



```
┌──(stuhow44㉿showa006)-[~/stegDir]
└─$ steghide --extract -sf SFbadge.JPG
Enter passphrase:
wrote extracted data to "testfile.txt".
```

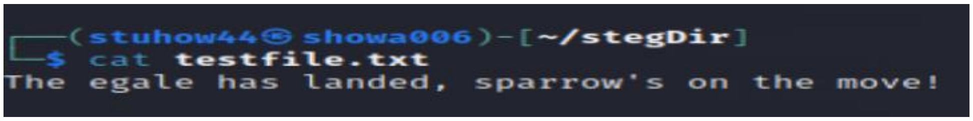
13. Execute the command to list the contents in stegDir directory.

You should see testfile.txt there because it was hidden in the jpeg image file and appeared after extracting the image file in the previous step (step-12)



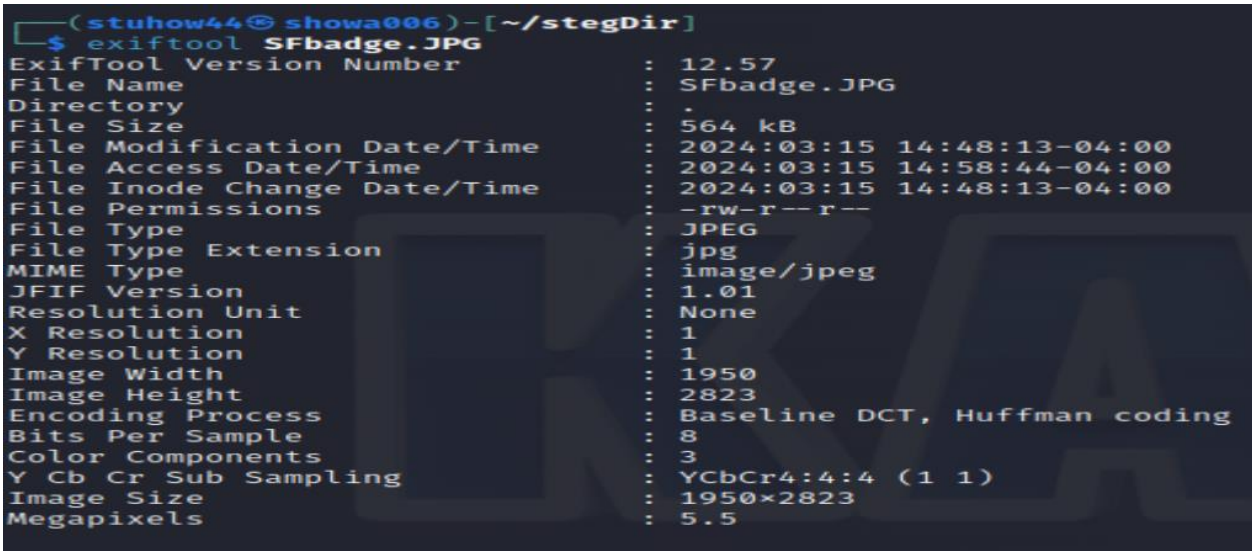
```
┌──(stuhow44㉿ showa006)-[~/stegDir]
└─$ ls
SFbadge.JPG   testfile.txt
```

14. Execute the command to display the contents of the file testfile.txt.



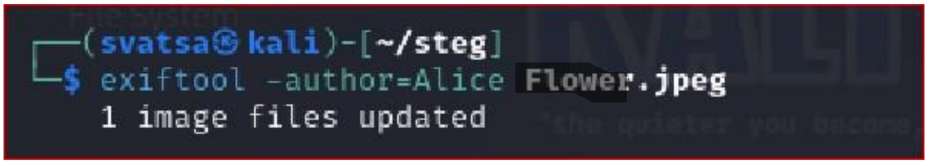
```
┌──(stuhow44㉿ showa006)-[~/stegDir]
└─$ cat testfile.txt
The egale has landed, sparrow's on the move!
```

15. You can view the related information (also known as metadata) about the jpeg image file using **exiftool** command as follows:



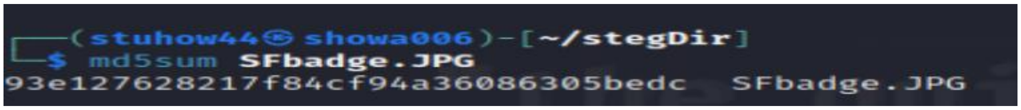
```
┌──(stuhow44㉿ showa006)-[~/stegDir]
└─$ exiftool SFbadge.JPG
ExifTool Version Number         : 12.57
File Name                       : SFbadge.JPG
Directory                       : .
File Size                       : 564 kB
File Modification Date/Time     : 2024:03:15 14:48:13-04:00
File Access Date/Time           : 2024:03:15 14:58:44-04:00
File Inode Change Date/Time     : 2024:03:15 14:48:13-04:00
File Permissions                : -rw-r--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
Image Width                     : 1950
Image Height                    : 2823
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 1950x2823
Megapixels                      : 5.5
```

16. You can change the author of the fileusing **exiftool** command as follows:



```
┌──(svatsa㉿kali)-[~/steg]
└─$ exiftool -author=Alice Flower.jpeg
    1 image files updated
```

17. Execute **md5sum** command with jpeg image file. Do you see any change in the hash value?



```
┌──(stuhow44㉿showa006)-[~/stegDir]
└─$ md5sum SFbadge.JPG
93e127628217f84cf94a36086305bedc  SFbadge.JPG
```

No it is the same as before.