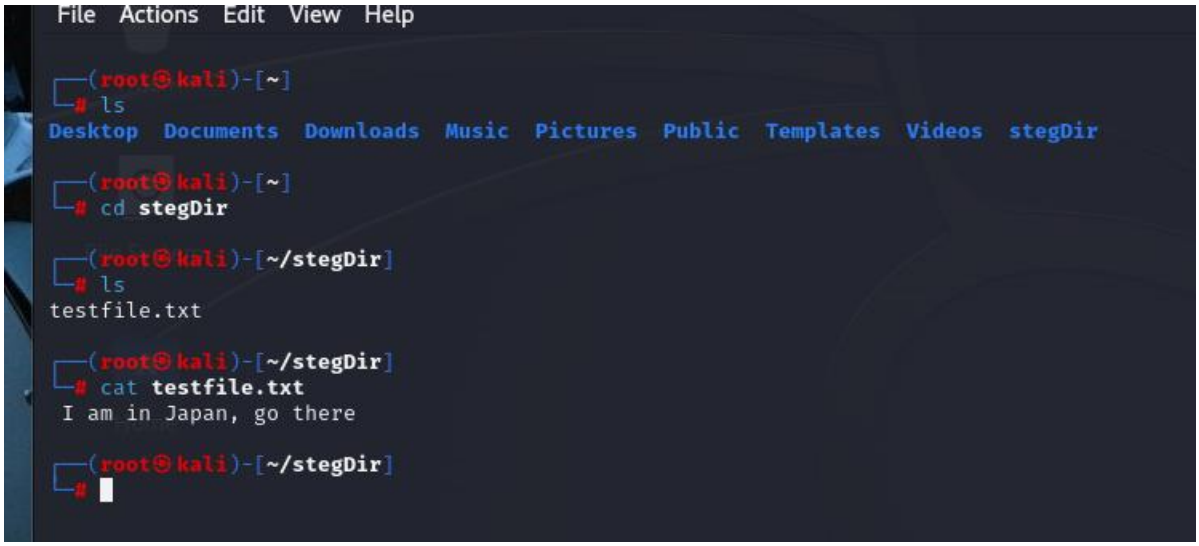
Assignment-6: Steganography

CYSE450- Ethical Hacking and Penetration Testing

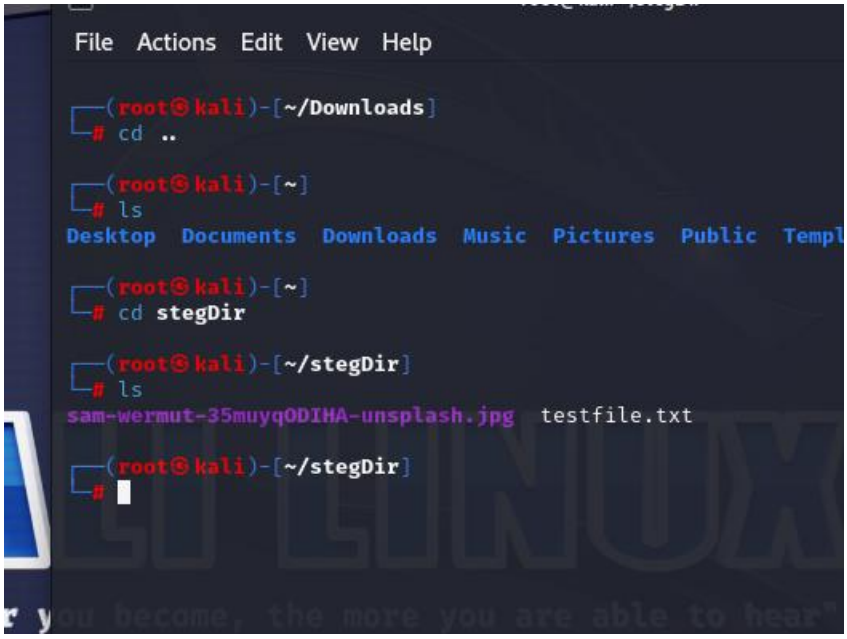
(Total: 100 Points)

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



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.]



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]

7. Execute the command md5sum (Learn about MD5 here: https://phoenixnap.com/kb/md5sum-linux) to check the checksums for **both** the filestestfile.txt and jpeg image. For example:

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
```

```
└─# md5sum testfile.txt
022792074100d954a1eb61efdb6dd1f8  testfile.txt

┌──(root㉿kali)-[~/stegDir]
└─# md5sum sam-wermut-35muyqODIHA-unsplash.jpg
a0203ba89a8a43c06bf878a3e2b8197d  sam-wermut-35muyqODIHA-unsplash.jpg
```

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

   There is a difference:

```
┌──(root㉿kali)-[~/stegDir]
└─# md5sum sam-wermut-35muyqODIHA-unsplash.jpg
5e78903998e73f309fcbfff81097cee4  sam-wermut-35muyqODIHA-unsplash.jpg
```

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

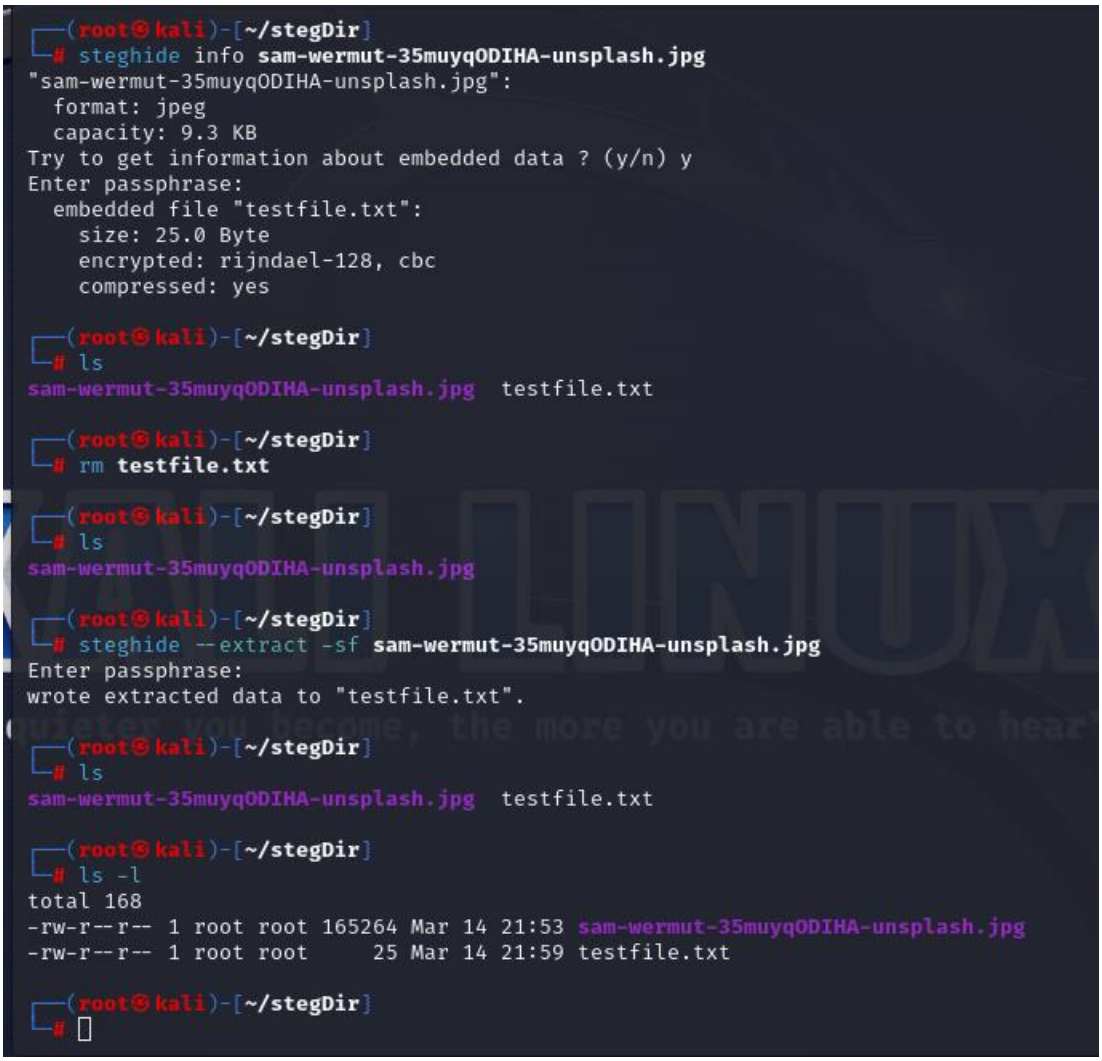
```
┌──(svatsa㉿kali)-[~/steg]
└─$ steghide info [redacted].jpeg
"[redacted].jpeg":
  format: jpeg
  capacity: 636.0 Byte
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "testfile.txt":
    size: 24.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

11. Now, **delete** the file testfile.txt.
12. **Extract** the secret message by executing steghide command with **- - extract** option as follows:

```
┌──(svatsa㉿kali)-[~/steg]
└─$ steghide --extract -sf Flower.jpeg
Enter passphrase:
wrote extracted data to "testfile.txt".
```

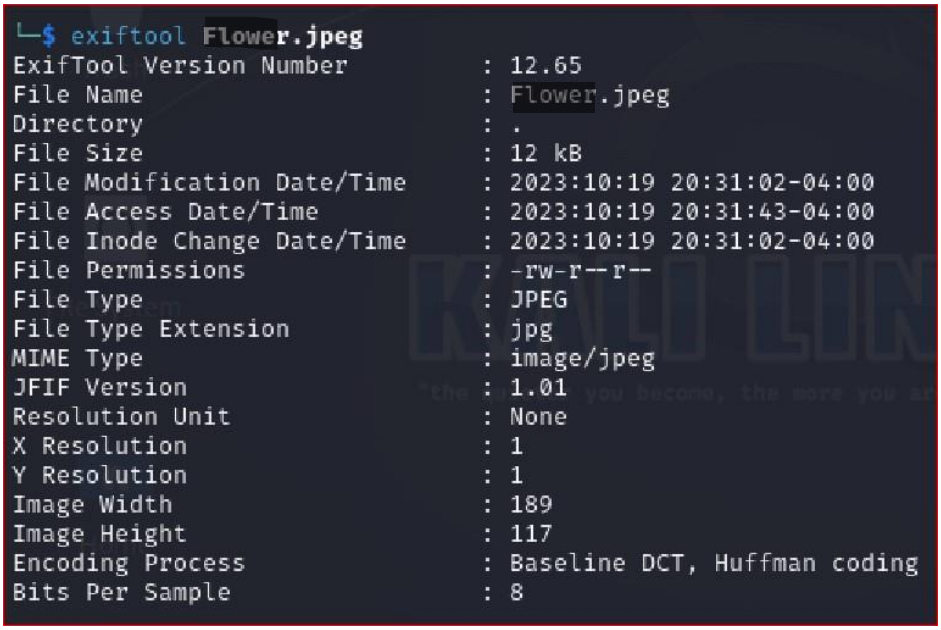
13. Execute the command to list the contents in stegDir directory.

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)



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

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



```
┌──(root㉿kali)-[~/stegDir]
└─# exiftool sam-wermut-35muyqODIHA-unsplash.jpg
ExifTool Version Number         : 12.67
File Name                       : sam-wermut-35muyqODIHA-unsplash.jpg
Directory                       : .
File Size                       : 165 kB
File Modification Date/Time     : 2024:03:14 21:53:14-04:00
File Access Date/Time           : 2024:03:14 21:54:13-04:00
File Inode Change Date/Time     : 2024:03:14 21:53:14-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Image Width                     : 640
Image Height                    : 960
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 640×960
Megapixels                      : 0.614

┌──(root㉿kali)-[~/stegDir]
└─#
```

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
```

```
File  Actions  Edit  View  Help

┌──(root㉿kali)-[~/stegDir]
└─# exiftool -author=Alex sam-wermut-35muyqODIHA-unsplash.jpg
    1 image files updated

┌──(root㉿kali)-[~/stegDir]
└─#
```

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

Yes I do


┌──(root㉿kali)-[~/stegDir]
└─# md5sum sam-wermut-35muyqODIHA-unsplash.jpg
78f2bcb1222464750bb13c7bbbe1f166 sam-wermut-35muyqODIHA-unsplash.jpg
┌──(root㉿kali)-[~/stegDir]
└─# md5sum testfile.txt
022792074100d954a1eb61efdb6dd1f8 testfile.txt
┌──(root㉿kali)-[~/stegDir]
└─#