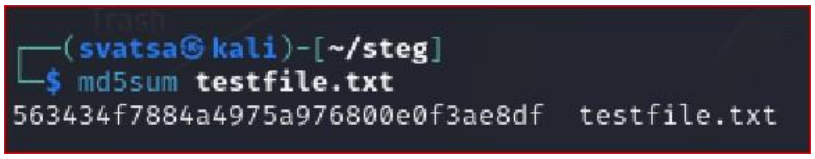
Assignment-6: Steganography

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.
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
```

9. <u>Execute the command md5sum</u> for your jpeg image file to check the hash for the image file.

   Do you see any 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:

```
┌──(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:

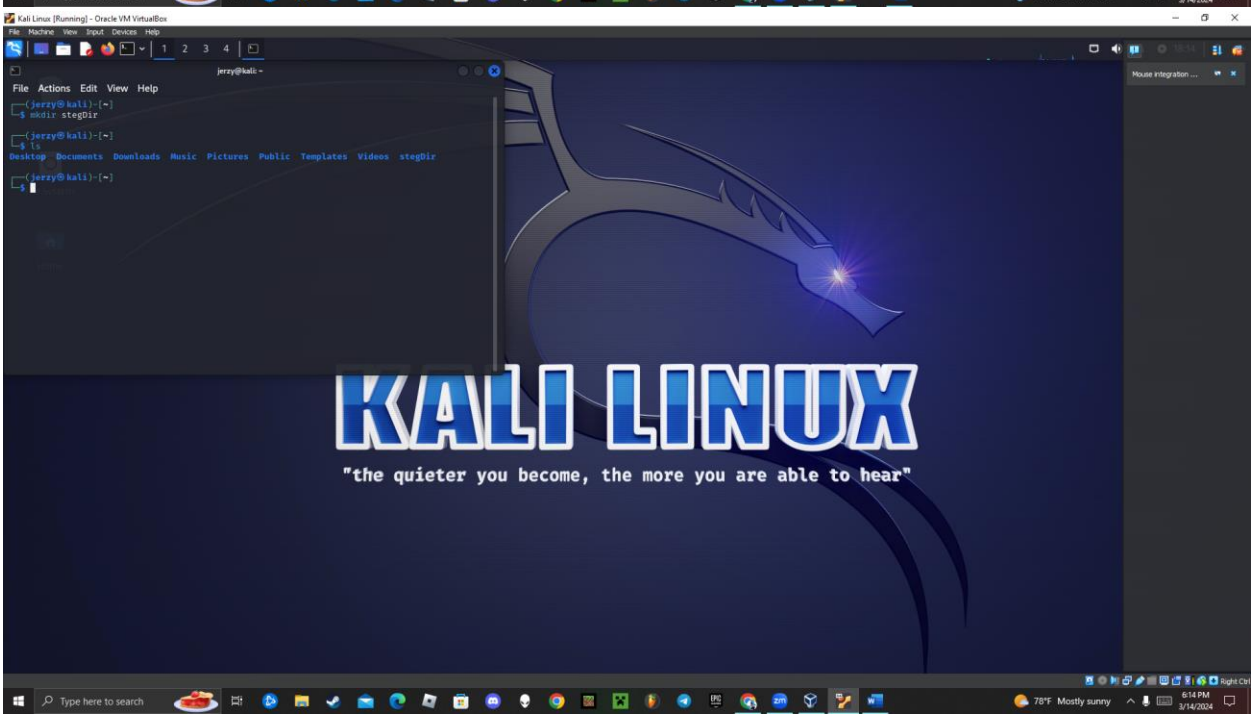
```
└─$ exiftool Flower.jpeg
ExifTool Version Number         : 12.65
File Name                       : Flower.jpeg
Directory                       : .
File Size                       : 12 kB
File Modification Date/Time     : 2023:10:19 20:31:02-04:00
File Access Date/Time           : 2023:10:19 20:31:43-04:00
File Inode Change Date/Time     : 2023:10:19 20:31:02-04:00
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                     : 189
Image Height                    : 117
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
```

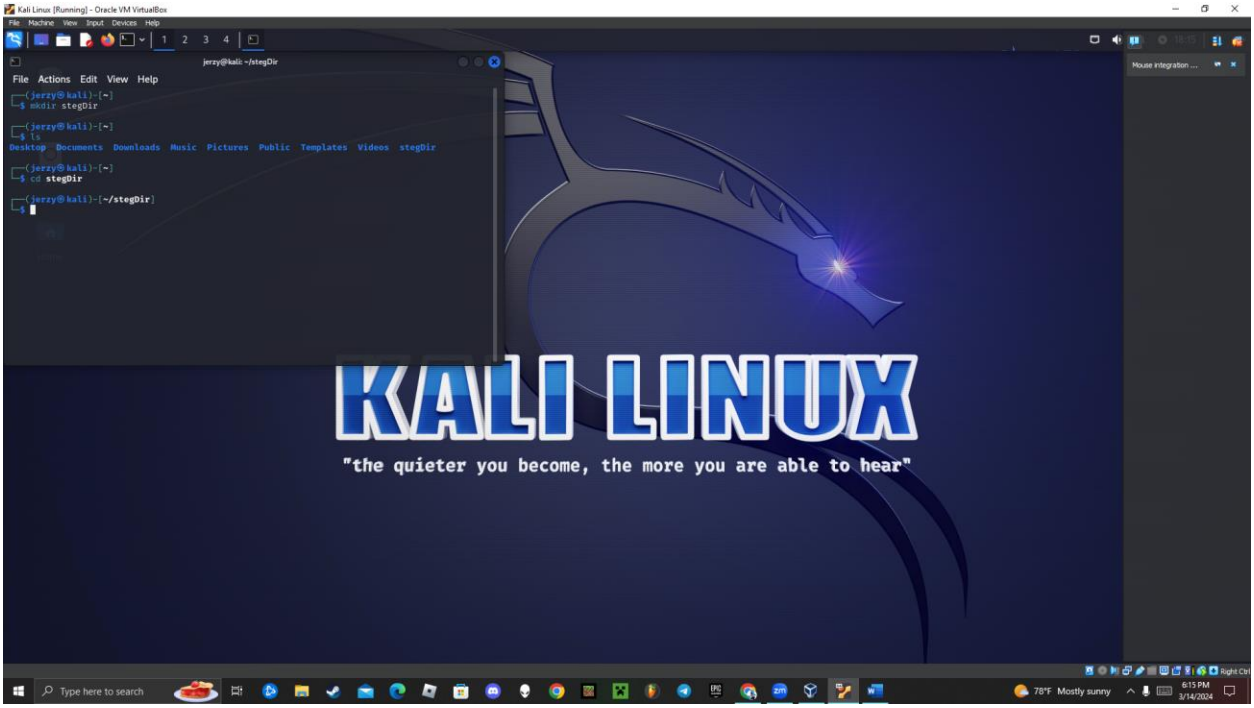
16. You can change the author of the fileusing **exiftool** command as follows:

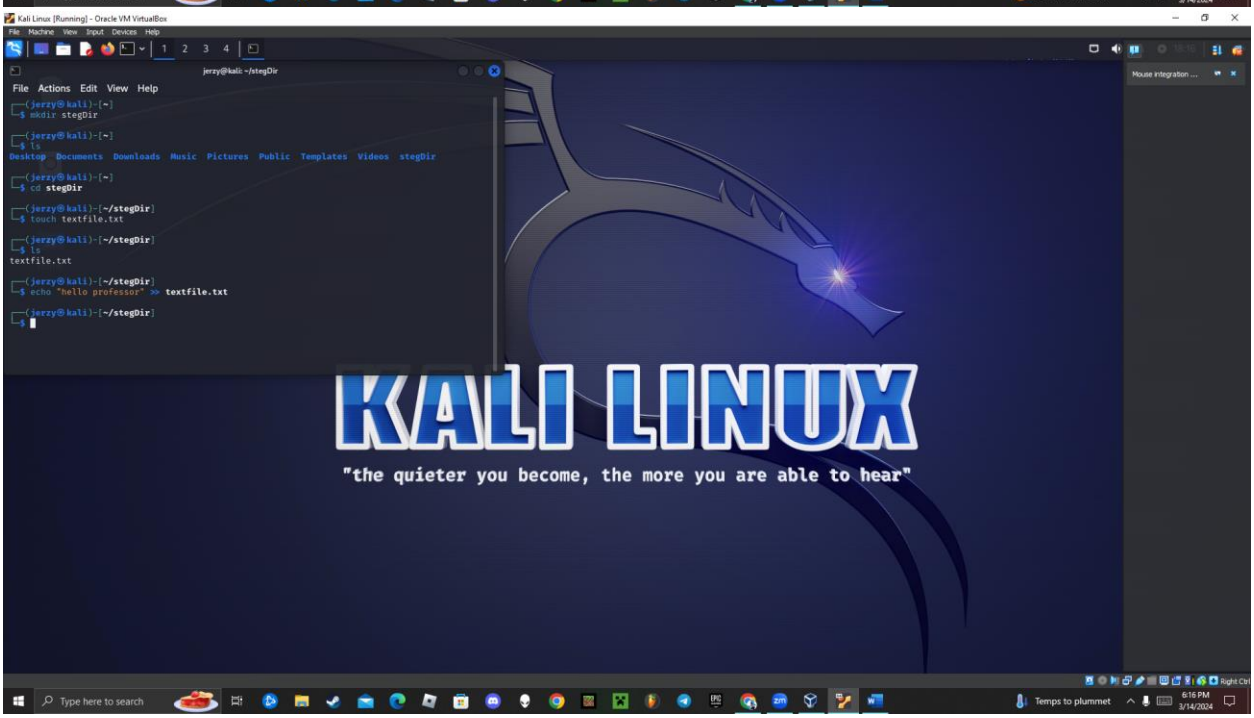
```
┌──(svatsa㉿kali)-[~/steg]
└─$ exiftool -author=Alice Flower.jpeg
    1 image files updated
```

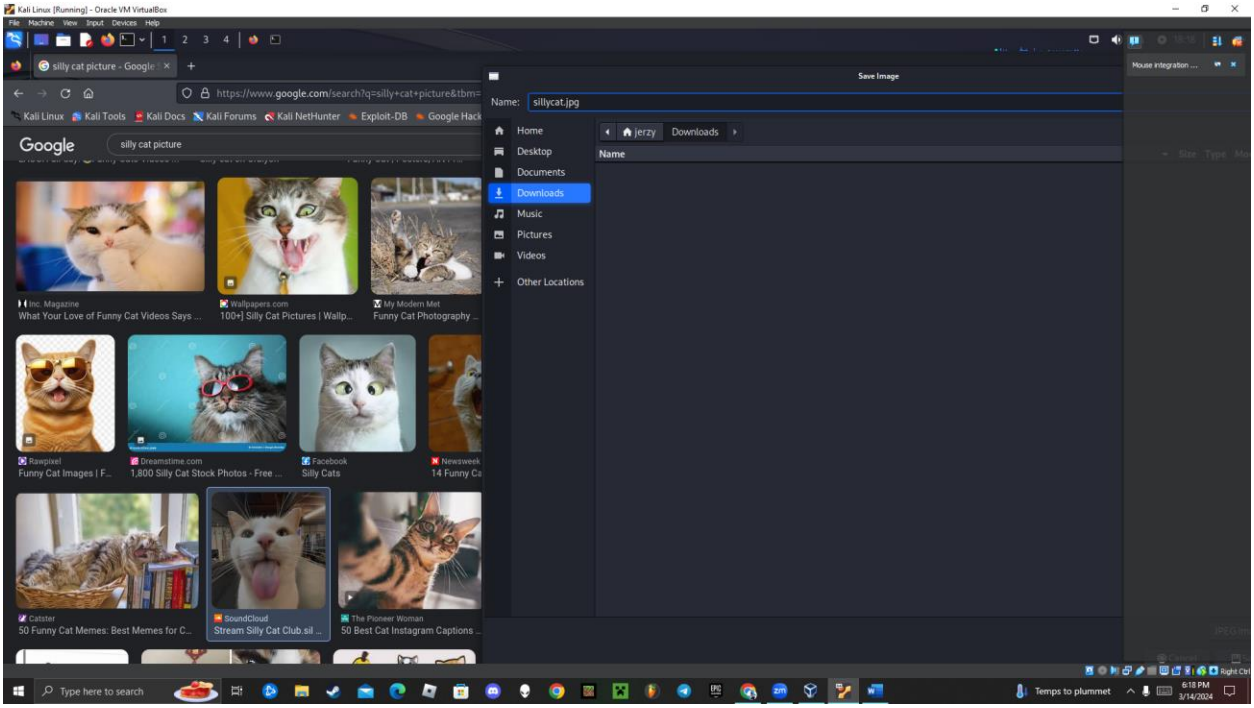
17. Execute **md5sum** command with jpeg image file. Do you see any change in the hash value?

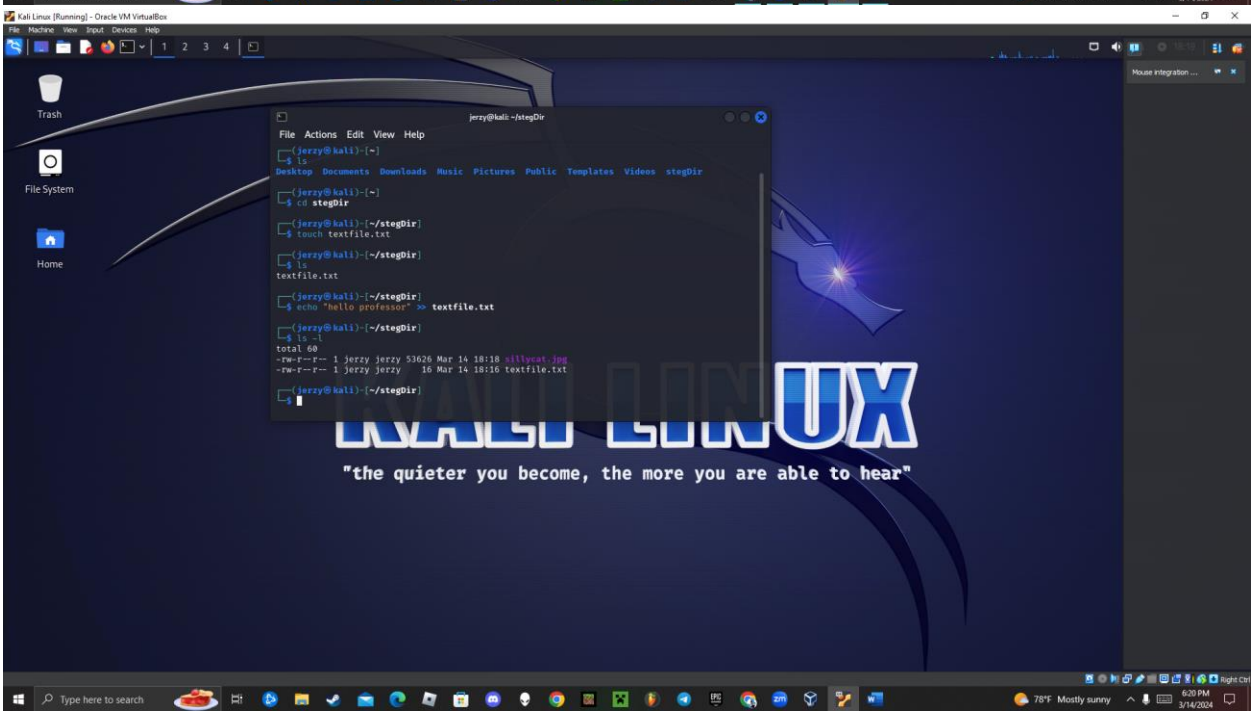
1. 
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(jerzy㉿kali)-[~]
$
KALI LINUX
"the quieter you become, the more you are able to hear"
Type here to search
Temps to plummet

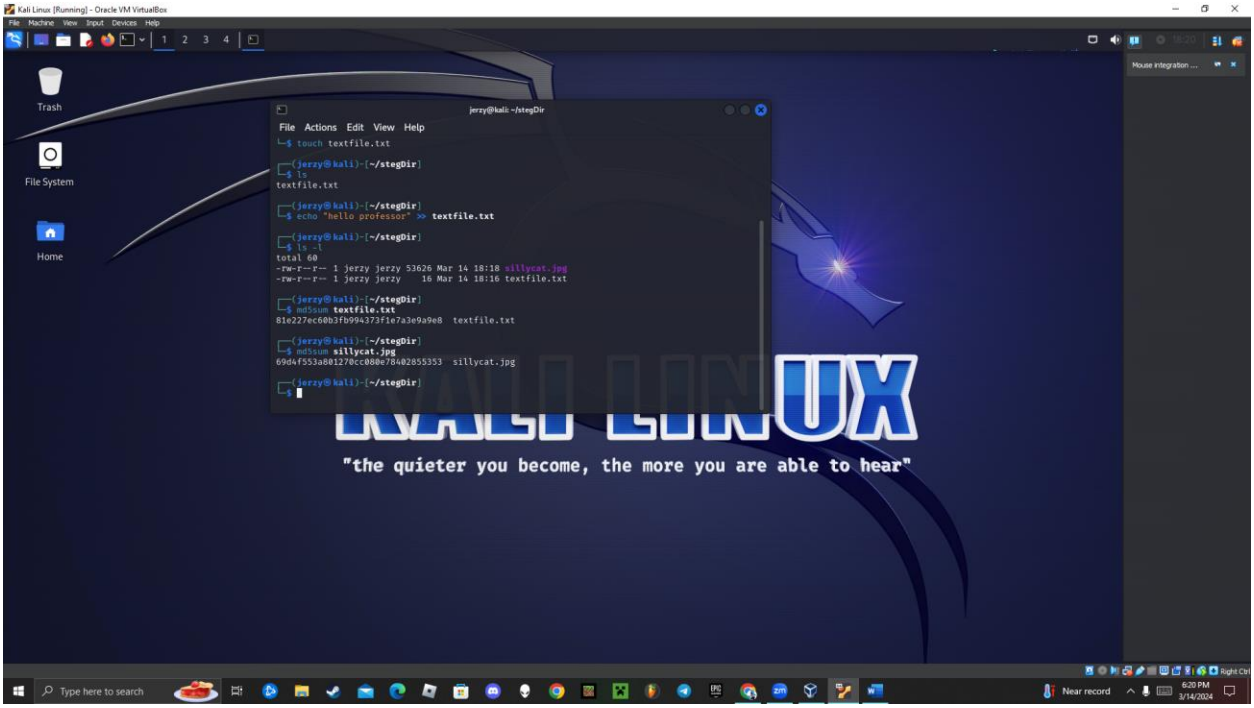
2. 
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(jerzy㉿kali)-[~]
$ mkdir stegDir
(jerzy㉿kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos stegDir
(jerzy㉿kali)-[~]
$
KALI LINUX
"the quieter you become, the more you are able to hear"
Type here to search
78°F Mostly sunny

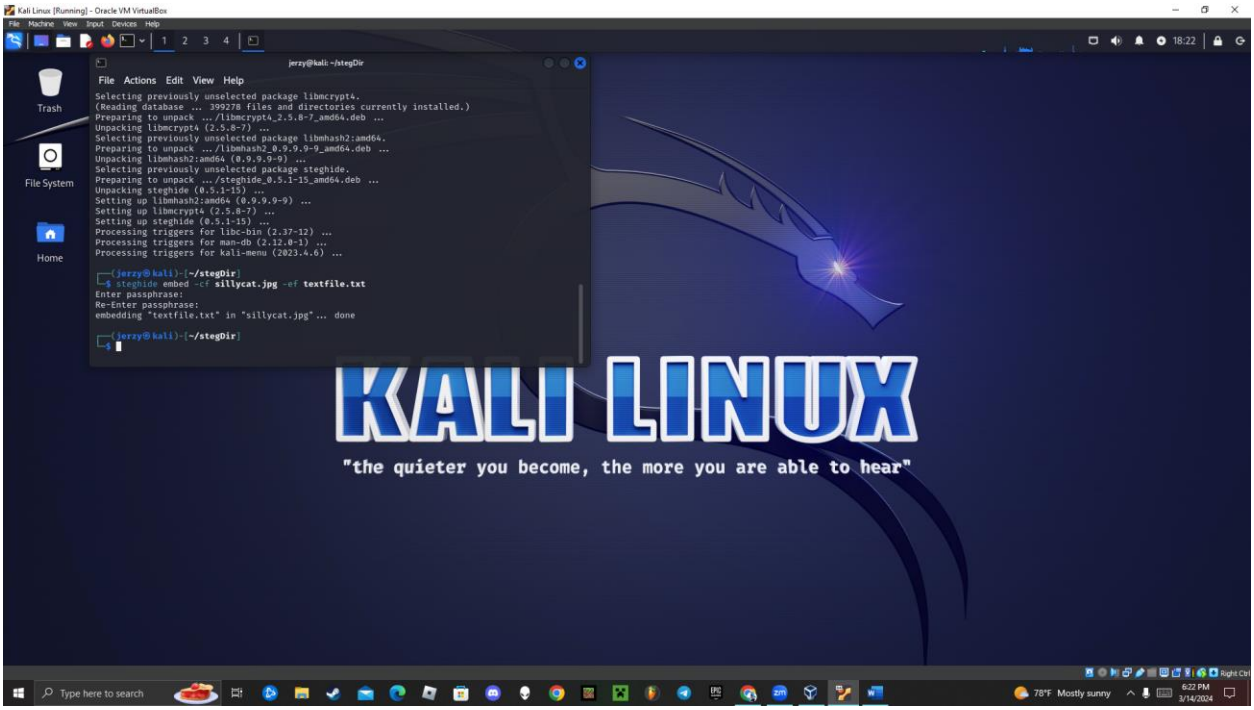
3. 
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
jerzy@kali: ~/stegDir
File Actions Edit View Help
┌──(jerzy㉿kali)-[~]
└─$ mkdir stegDir
┌──(jerzy㉿kali)-[~]
└─$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos stegDir
┌──(jerzy㉿kali)-[~]
└─$ cd stegDir
┌──(jerzy㉿kali)-[~/stegDir]
└─$
KALI LINUX
"the quieter you become, the more you are able to hear"
Type here to search
78°F Mostly sunny
6:15 PM
3/14/2024

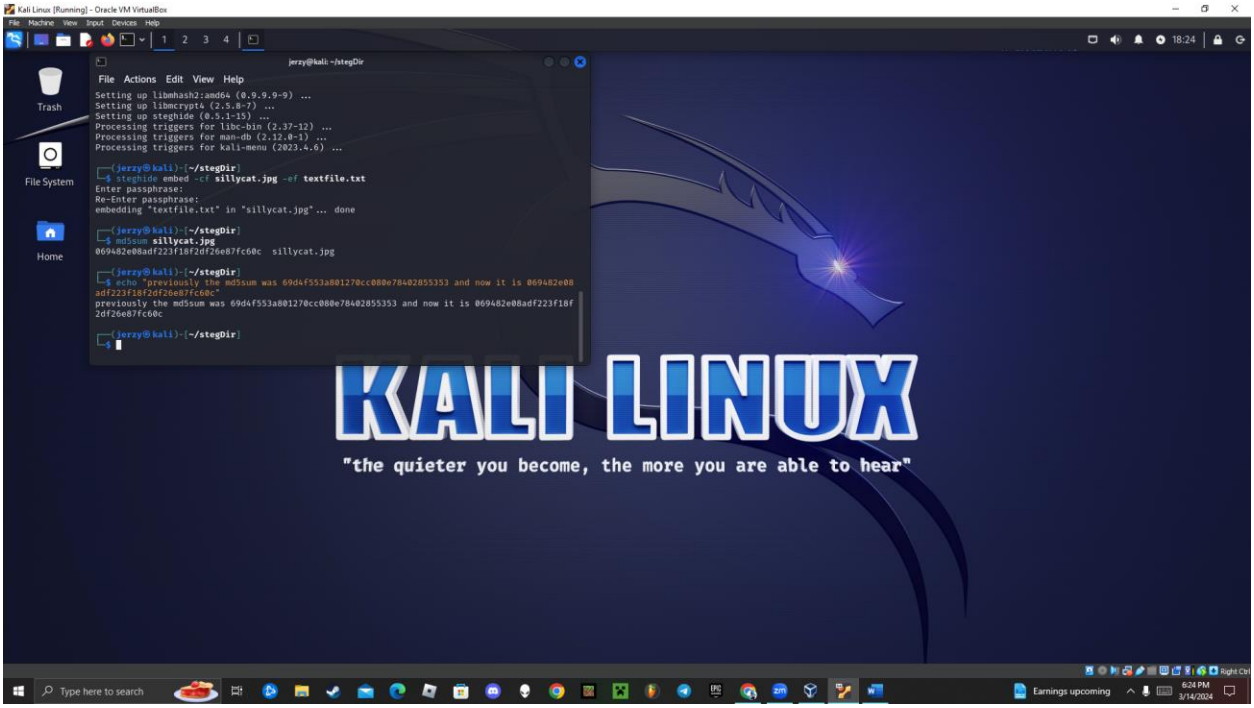
4. 
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
jerzy@kali: ~/stegDir
File Actions Edit View Help
┌──(jerzy㉿kali)-[~]
└─$ mkdir stegDir
┌──(jerzy㉿kali)-[~]
└─$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos stegDir
┌──(jerzy㉿kali)-[~]
└─$ cd stegDir
┌──(jerzy㉿kali)-[~/stegDir]
└─$ touch textfile.txt
┌──(jerzy㉿kali)-[~/stegDir]
└─$ ls
textfile.txt
┌──(jerzy㉿kali)-[~/stegDir]
└─$ echo "hello professor" >> textfile.txt
┌──(jerzy㉿kali)-[~/stegDir]
└─$
KALI LINUX
"the quieter you become, the more you are able to hear"
Type here to search
Temps to plummet
6:16 PM
3/14/2024

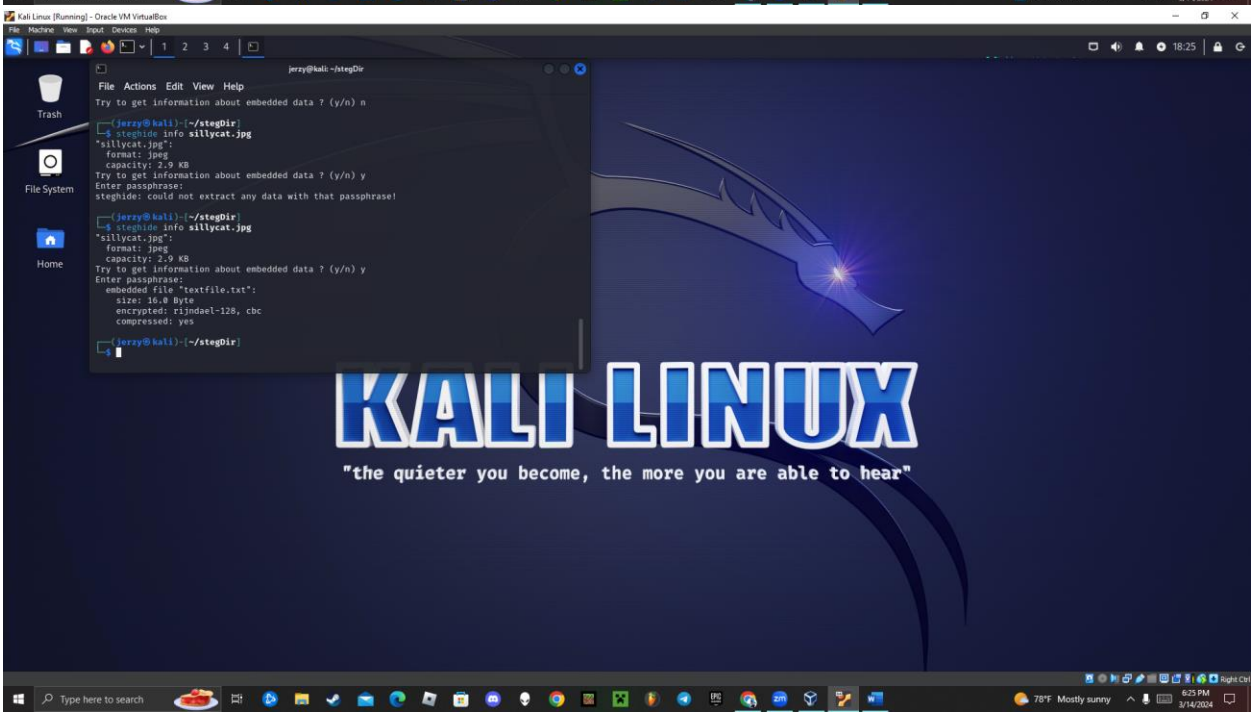
5. 
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
silly cat picture - Google
https://www.google.com/search?q=silly+cat+picture&tbm=
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hack
Google
silly cat picture
Save Image
Name: sillycat.jpg
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Other Locations
jerzy Downloads
Name
Type here to search
Temps to plummet

6. 
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
jerzy@kali: ~/stegDir
File Actions Edit View Help
┌──(jerzy㉿kali)-[~]
└─$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos stegDir
┌──(jerzy㉿kali)-[~]
└─$ cd stegDir
┌──(jerzy㉿kali)-[~/stegDir]
└─$ touch textfile.txt
┌──(jerzy㉿kali)-[~/stegDir]
└─$ ls
textfile.txt
┌──(jerzy㉿kali)-[~/stegDir]
└─$ echo "hello professor" >> textfile.txt
┌──(jerzy㉿kali)-[~/stegDir]
└─$ ls -l
total 60
-rw-r--r-- 1 jerzy jerzy 53626 Mar 14 18:18 sillycat.jpg
-rw-r--r-- 1 jerzy jerzy 16 Mar 14 18:16 textfile.txt
┌──(jerzy㉿kali)-[~/stegDir]
└─$
"the quieter you become, the more you are able to hear"
Type here to search
78°F Mostly sunny

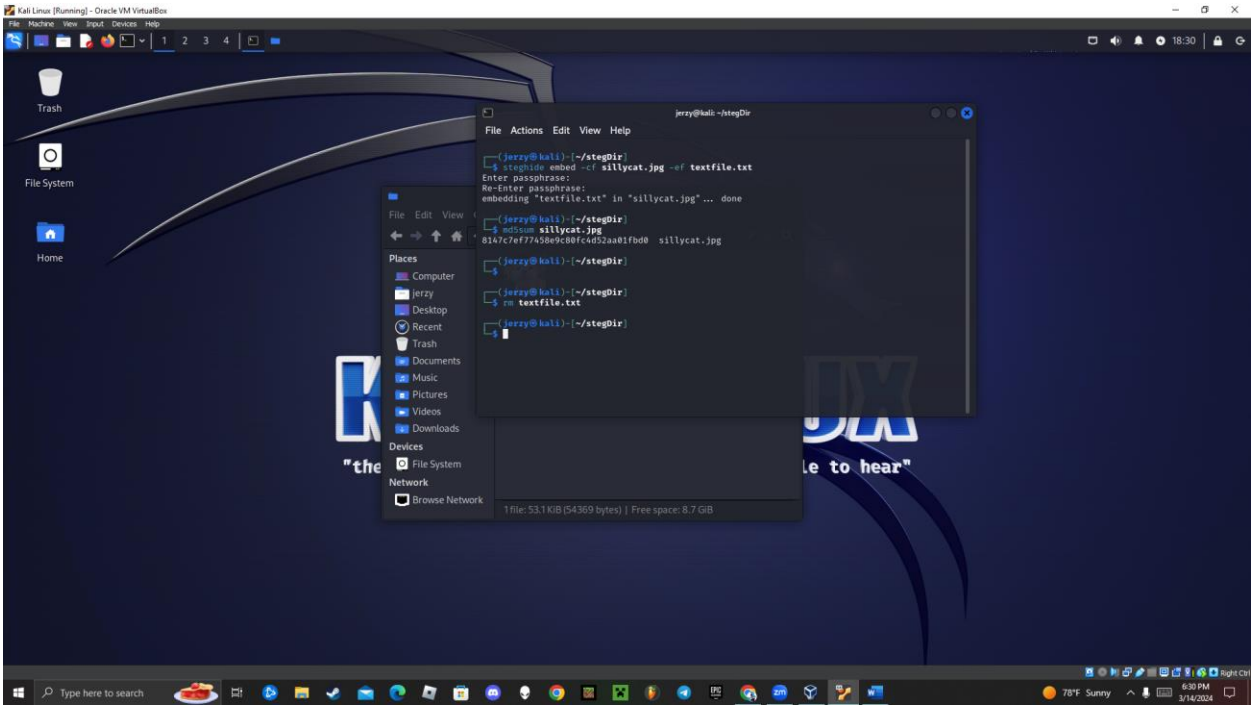
7. 
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
jerzy@kali: ~/stegDir
File Actions Edit View Help
touch textfile.txt
ls
textfile.txt
echo "hello professor" >> textfile.txt
ls -l
total 60
-rw-r--r-- 1 jerzy jerzy 53626 Mar 14 18:18 sillycat.jpg
-rw-r--r-- 1 jerzy jerzy 16 Mar 14 18:16 textfile.txt
md5sum textfile.txt
81e227ec60b3fb994373f1e7a3e9a9e8 textfile.txt
md5sum sillycat.jpg
69d4f553a801270cc080e78402855353 sillycat.jpg
KALI LINUX
"the quieter you become, the more you are able to hear"
Type here to search
Near record

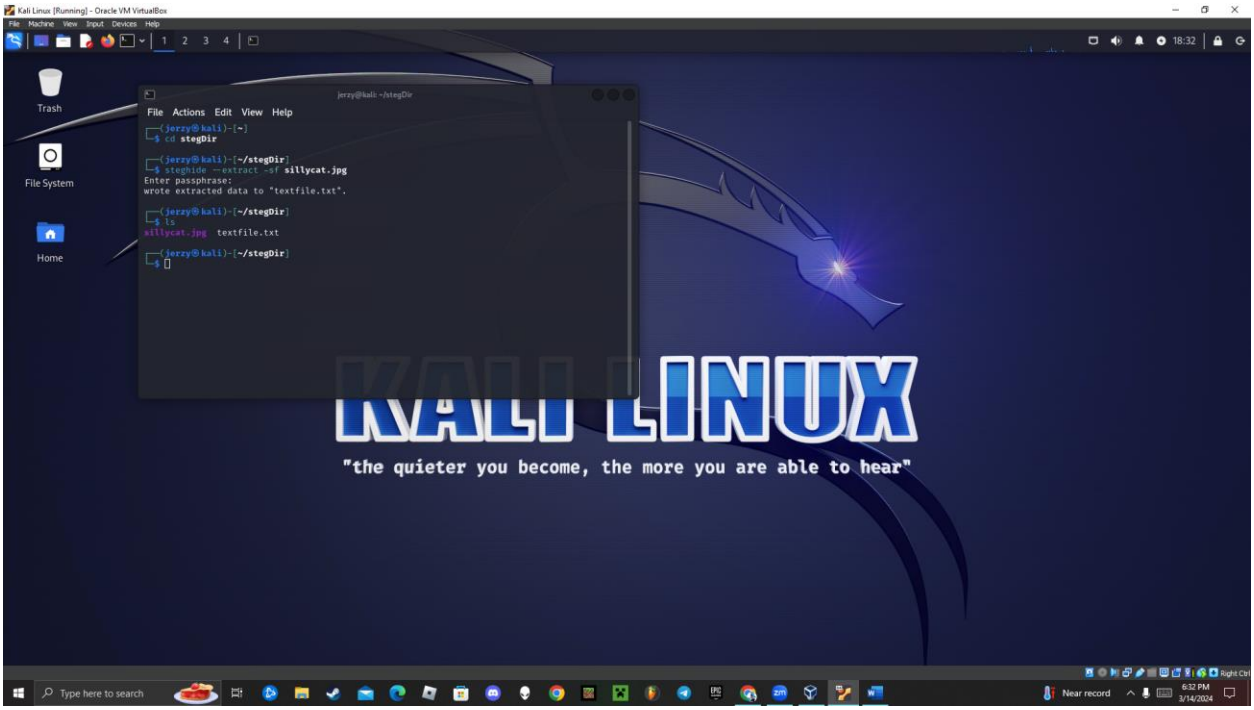
8. 
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
jerzy@kali: ~/stegDir
File Actions Edit View Help
Selecting previously unselected package libmcrypt4.
(Reading database ... 399278 files and directories currently installed.)
Preparing to unpack .../libmcrypt4_2.5.8-7_amd64.deb ...
Unpacking libmcrypt4 (2.5.8-7) ...
Selecting previously unselected package libmhash2:amd64.
Preparing to unpack .../libmhash2_0.9.9.9-9_amd64.deb ...
Unpacking libmhash2:amd64 (0.9.9.9-9) ...
Selecting previously unselected package steghide.
Preparing to unpack .../steghide_0.5.1-15_amd64.deb ...
Unpacking steghide (0.5.1-15) ...
Setting up libmhash2:amd64 (0.9.9.9-9) ...
Setting up libmcrypt4 (2.5.8-7) ...
Setting up steghide (0.5.1-15) ...
Processing triggers for libc-bin (2.37-12) ...
Processing triggers for man-db (2.12.0-1) ...
Processing triggers for kali-menu (2023.4.6) ...
steghide embed -cf sillycat.jpg -ef textfile.txt
Enter passphrase:
Re-Enter passphrase:
embedding "textfile.txt" in "sillycat.jpg" ... done
KALI LINUX
"the quieter you become, the more you are able to hear"
Type here to search
78°F Mostly sunny

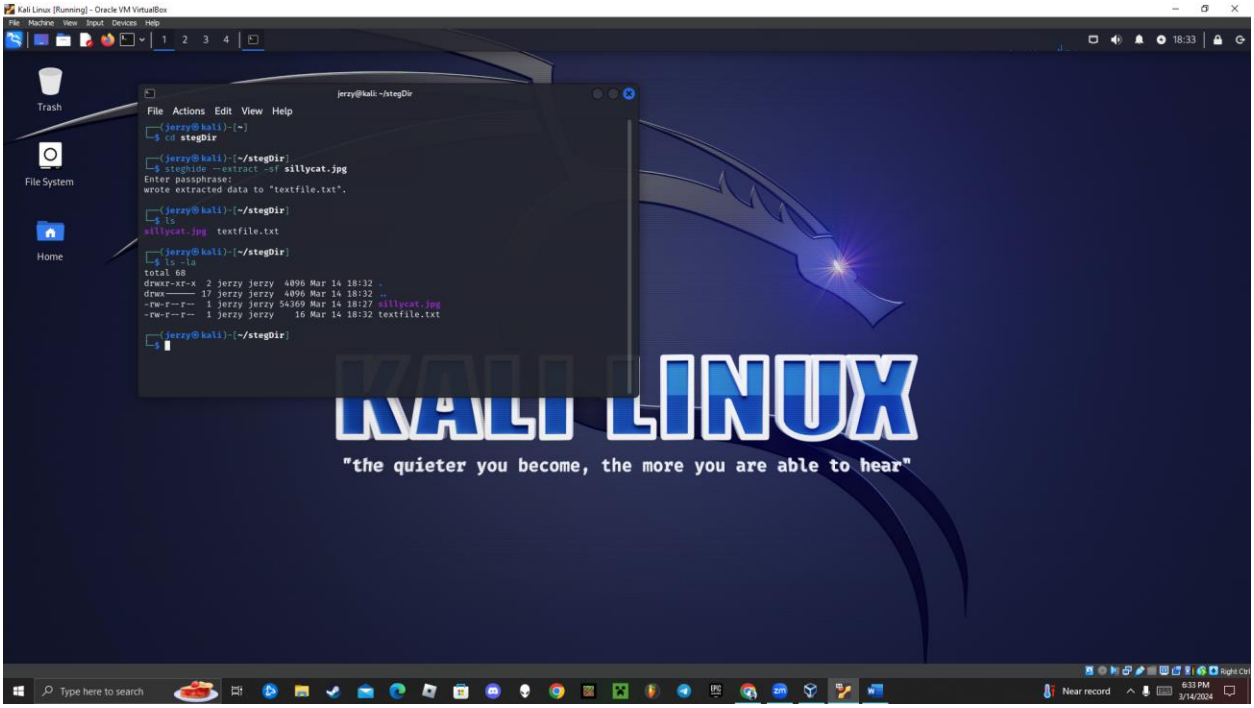
9. 
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
jerzy@kali: ~/stegDir
File Actions Edit View Help
Setting up libmhash2:amd64 (0.9.9.9-9) ...
Setting up libmcrypt4 (2.5.8-7) ...
Setting up steghide (0.5.1-15) ...
Processing triggers for libc-bin (2.37-12) ...
Processing triggers for man-db (2.12.0-1) ...
Processing triggers for kali-menu (2023.4.6) ...
┌──(jerzy㉿kali)-[~/stegDir]
└─$ steghide embed -cf sillycat.jpg -ef textfile.txt
Enter passphrase:
Re-Enter passphrase:
embedding "textfile.txt" in "sillycat.jpg" ... done
┌──(jerzy㉿kali)-[~/stegDir]
└─$ md5sum sillycat.jpg
069482e08adf223f18f2df26e87fc60c sillycat.jpg
┌──(jerzy㉿kali)-[~/stegDir]
└─$ echo "previously the md5sum was 69d4f553a801270cc080e78402855353 and now it is 069482e08adf223f18f2df26e87fc60c"
previously the md5sum was 69d4f553a801270cc080e78402855353 and now it is 069482e08adf223f18f2df26e87fc60c
┌──(jerzy㉿kali)-[~/stegDir]
└─$
Trash
File System
Home
KALI LINUX
"the quieter you become, the more you are able to hear"
Type here to search
Earnings upcoming
6:24 PM
3/14/2024

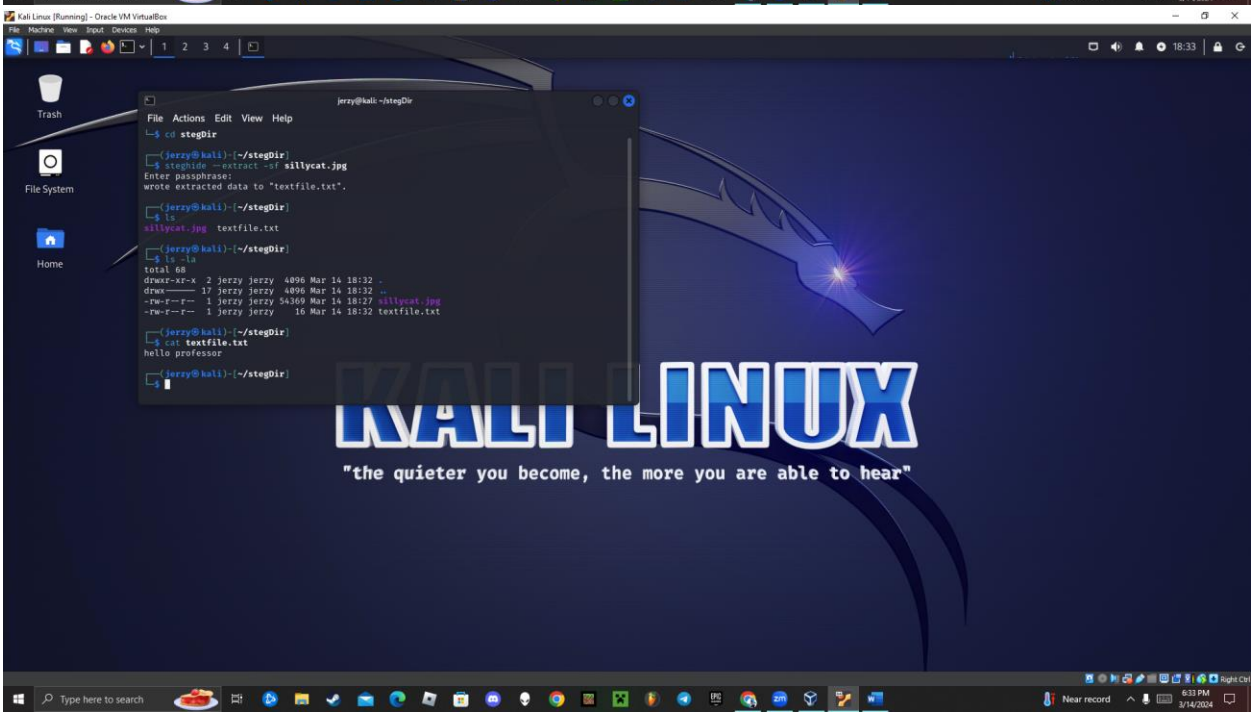
10. 
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
jerzy@kali: ~/stegDir
File Actions Edit View Help
Try to get information about embedded data ? (y/n) n
┌──(jerzy㉿kali)-[~/stegDir]
└─$ steghide info sillycat.jpg
"sillycat.jpg":
  format: jpeg
  capacity: 2.9 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
steghide: could not extract any data with that passphrase!
┌──(jerzy㉿kali)-[~/stegDir]
└─$ steghide info sillycat.jpg
"sillycat.jpg":
  format: jpeg
  capacity: 2.9 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "textfile.txt":
    size: 16.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
┌──(jerzy㉿kali)-[~/stegDir]
└─$
Trash
File System
Home
KALI LINUX
"the quieter you become, the more you are able to hear"
Type here to search
78°F Mostly sunny
6:25 PM
3/14/2024

11. NOTE: I accidentally deleted the jpeg by accident for this step so the new md5sum should be “8147c7ef77458e9c80fc4d52aa01fbd0” after I recreated the steg image



12. 

13. 
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
jerzy@kali: ~/stegDir
File Actions Edit View Help
┌──(jerzy㉿kali)-[~]
└─$ cd stegDir
┌──(jerzy㉿kali)-[~/stegDir]
└─$ steghide --extract -sf sillycat.jpg
Enter passphrase:
wrote extracted data to "textfile.txt".
┌──(jerzy㉿kali)-[~/stegDir]
└─$ ls
sillycat.jpg textfile.txt
┌──(jerzy㉿kali)-[~/stegDir]
└─$ ls -la
total 68
drwxr-xr-x 2 jerzy jerzy 4096 Mar 14 18:32 .
drwx------ 17 jerzy jerzy 4096 Mar 14 18:32 ..
-rw-r--r-- 1 jerzy jerzy 54369 Mar 14 18:27 sillycat.jpg
-rw-r--r-- 1 jerzy jerzy 16 Mar 14 18:32 textfile.txt
┌──(jerzy㉿kali)-[~/stegDir]
└─$
KALI LINUX
"the quieter you become, the more you are able to hear"
Type here to search
Near record

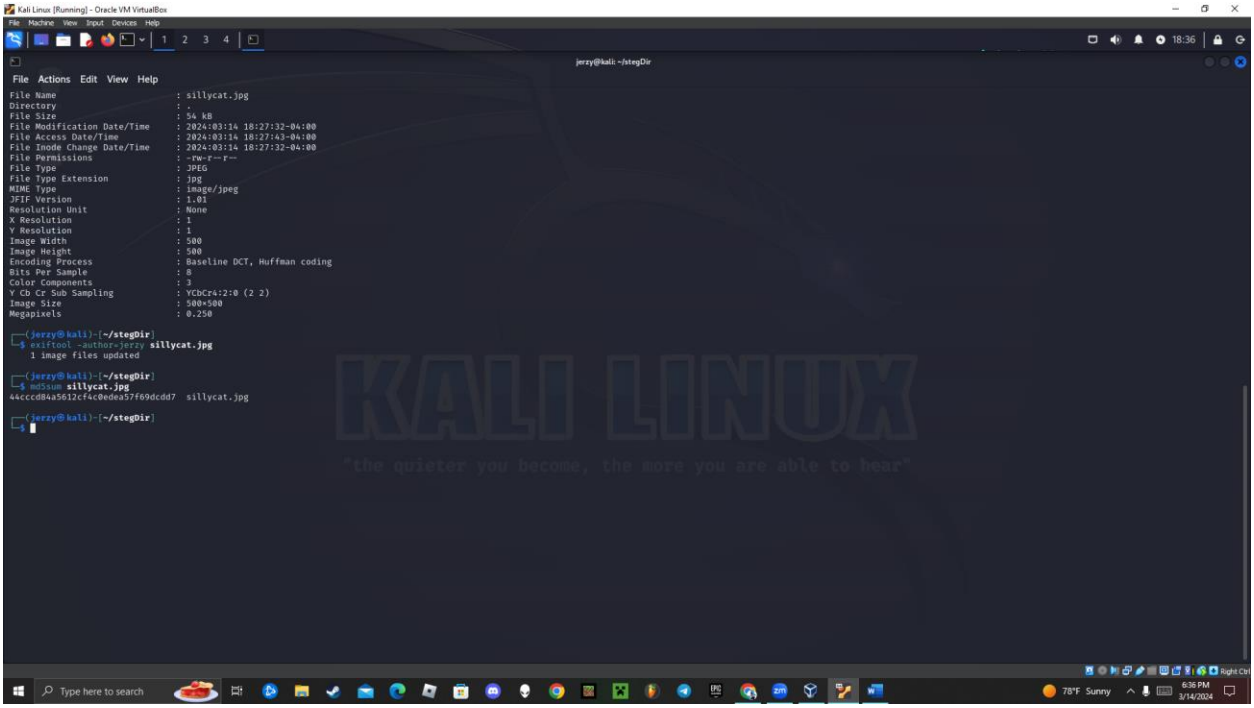
14. 
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
jerzy@kali: ~/stegDir
File Actions Edit View Help
└─$ cd stegDir
┌──(jerzy㉿kali)-[~/stegDir]
└─$ steghide --extract -sf sillycat.jpg
Enter passphrase:
wrote extracted data to "textfile.txt".
┌──(jerzy㉿kali)-[~/stegDir]
└─$ ls
sillycat.jpg textfile.txt
┌──(jerzy㉿kali)-[~/stegDir]
└─$ ls -la
total 68
drwxr-xr-x 2 jerzy jerzy 4096 Mar 14 18:32 .
drwx------ 17 jerzy jerzy 4096 Mar 14 18:32 ..
-rw-r--r-- 1 jerzy jerzy 54369 Mar 14 18:27 sillycat.jpg
-rw-r--r-- 1 jerzy jerzy 16 Mar 14 18:32 textfile.txt
┌──(jerzy㉿kali)-[~/stegDir]
└─$ cat textfile.txt
hello professor
┌──(jerzy㉿kali)-[~/stegDir]
└─$
KALI LINUX
"the quieter you become, the more you are able to hear"
Type here to search
Near record

15.

```
┌──(jerzy㉿kali)-[~/stegDir]
└─$ ls -la
total 68
drwxr-xr-x  2 jerzy jerzy  4096 Mar 14 18:32 .
drwx------ 17 jerzy jerzy  4096 Mar 14 18:32 ..
-rw-r--r--  1 jerzy jerzy 54369 Mar 14 18:27 sillycat.jpg
-rw-r--r--  1 jerzy jerzy    16 Mar 14 18:32 textfile.txt

┌──(jerzy㉿kali)-[~/stegDir]
└─$ cat textfile.txt
hello professor

┌──(jerzy㉿kali)-[~/stegDir]
└─$ exiftool sillycat.jpg
ExifTool Version Number         : 12.67
File Name                       : sillycat.jpg
Directory                       : .
File Size                       : 54 kB
File Modification Date/Time     : 2024:03:14 18:27:32-04:00
File Access Date/Time           : 2024:03:14 18:27:43-04:00
File Inode Change Date/Time     : 2024:03:14 18:27:32-04:00
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                     : 500
Image Height                    : 500
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                      : 500×500
Megapixels                      : 0.250

┌──(jerzy㉿kali)-[~/stegDir]
└─$
```

16.

```
File Name                       : sillycat.jpg
Directory                       : .
File Size                       : 54 kB
File Modification Date/Time     : 2024:03:14 18:27:32-04:00
File Access Date/Time           : 2024:03:14 18:27:43-04:00
File Inode Change Date/Time     : 2024:03:14 18:27:32-04:00
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                     : 500
Image Height                    : 500
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                      : 500×500
Megapixels                      : 0.250

┌──(jerzy㉿kali)-[~/stegDir]
└─$ exiftool -author=jerzy sillycat.jpg
    1 image files updated

┌──(jerzy㉿kali)-[~/stegDir]
└─$
```

17. 

Yes there is a difference the old md5 and new md5 do not match.