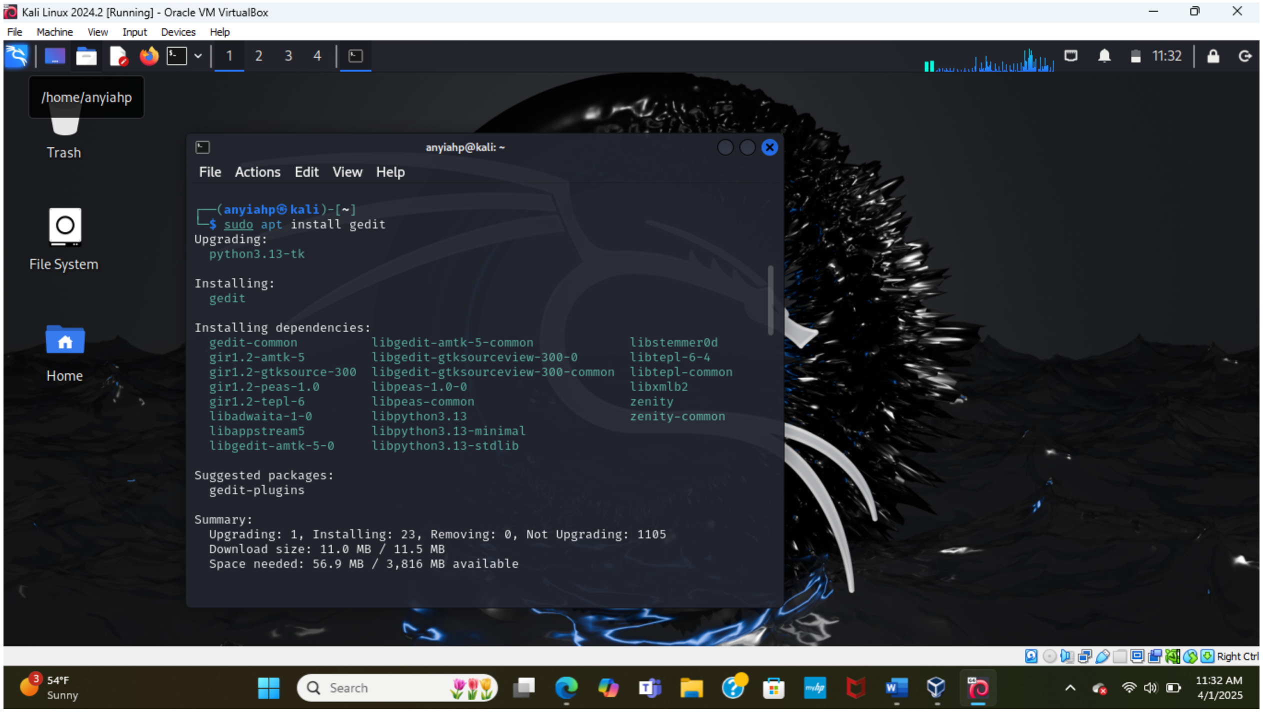
Old Dominion University
CYSE 450: Ethical Hacking and Penetration Testing

# Lab 4: Steganography using Steghide

**Handout Date**: March 27, 2025
**Due Date**: April 04, 2025, 11:59 pm
Total Points: 30

## Tasks

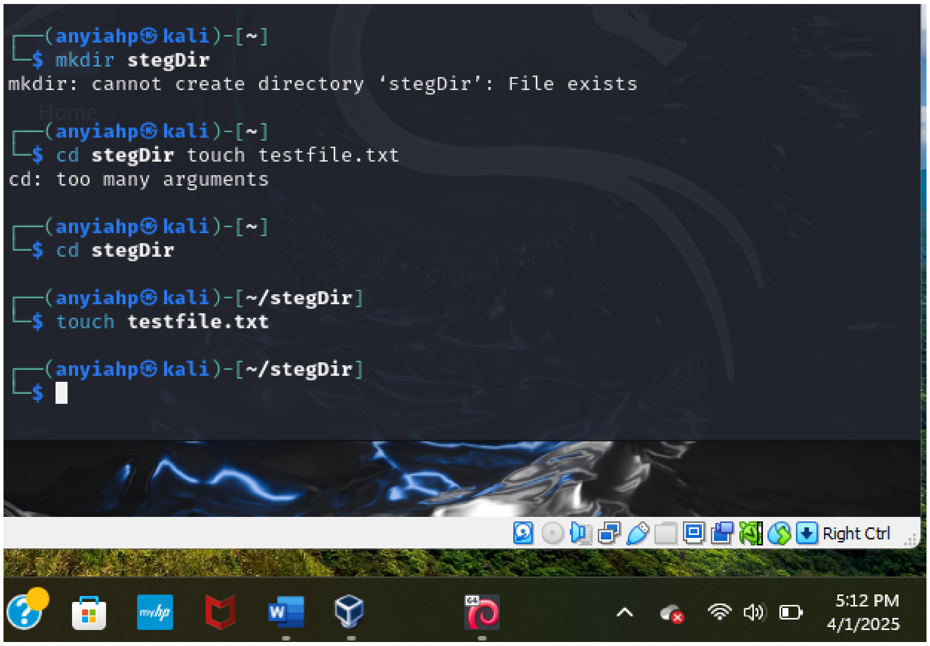
1. Open the terminal in Kali Linux and install ***gedit*** using the command: ***sudo apt install gedit***.



Kali Linux 2024.2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/home/anyiahp
Trash
File System
Home
anyiahp@kali: ~
File Actions Edit View Help

```
┌──(anyiahp㉿kali)-[~]
└─$ sudo apt install gedit
Upgrading:
  python3.13-tk

Installing:
  gedit

Installing dependencies:
  gedit-common          libgedit-amtk-5-common             libstemmer0d
  gir1.2-amtk-5         libgedit-gtksourceview-300-0       libtepl-6-4
  gir1.2-gtksource-300  libgedit-gtksourceview-300-common  libtepl-common
  gir1.2-peas-1.0       libpeas-1.0-0                      libxmlb2
  gir1.2-tepl-6         libpeas-common                     zenity
  libadwaita-1-0        libpython3.13                      zenity-common
  libappstream5         libpython3.13-minimal
  libgedit-amtk-5-0     libpython3.13-stdlib

Suggested packages:
  gedit-plugins

Summary:
  Upgrading: 1, Installing: 23, Removing: 0, Not Upgrading: 1105
  Download size: 11.0 MB / 11.5 MB
  Space needed: 56.9 MB / 3,816 MB available
```

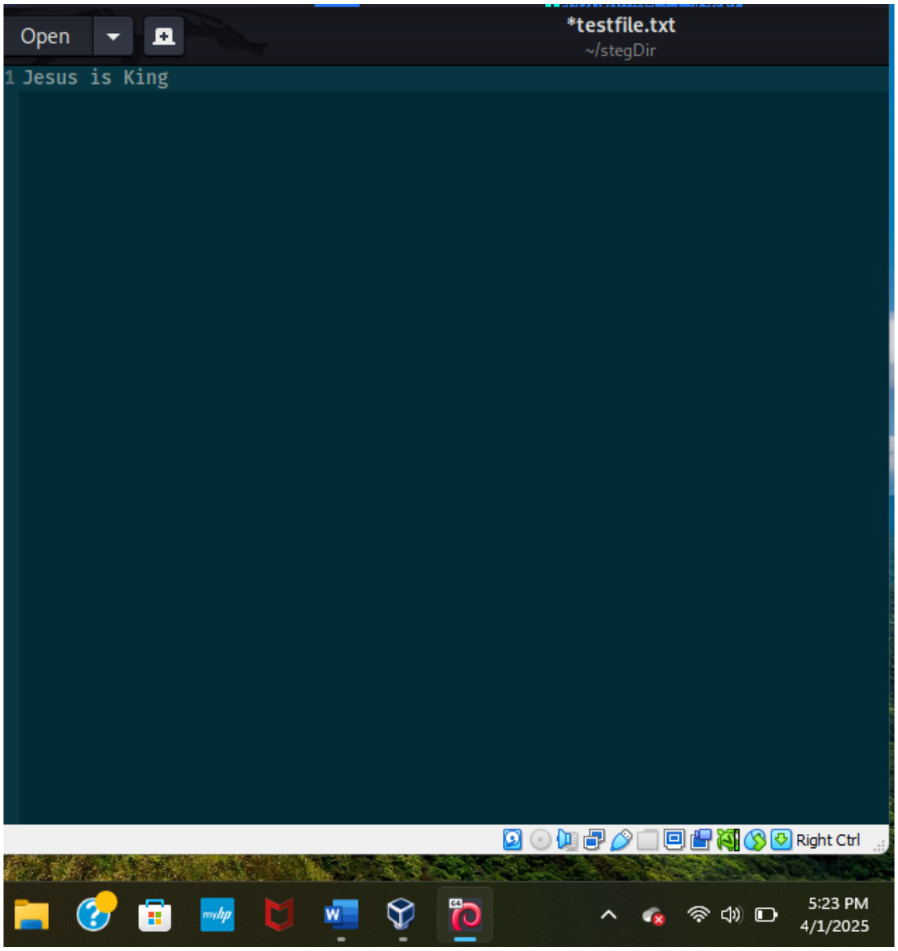
2. Create a new directory named ***stegDir*** using the ***mkdir*** command.



```
┌──(anyiahp㉿kali)-[~]
└─$ mkdir stegDir
mkdir: cannot create directory ‘stegDir’: File exists

┌──(anyiahp㉿kali)-[~]
└─$ cd stegDir touch testfile.txt
cd: too many arguments

┌──(anyiahp㉿kali)-[~]
└─$ cd stegDir

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ touch testfile.txt

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ 
```

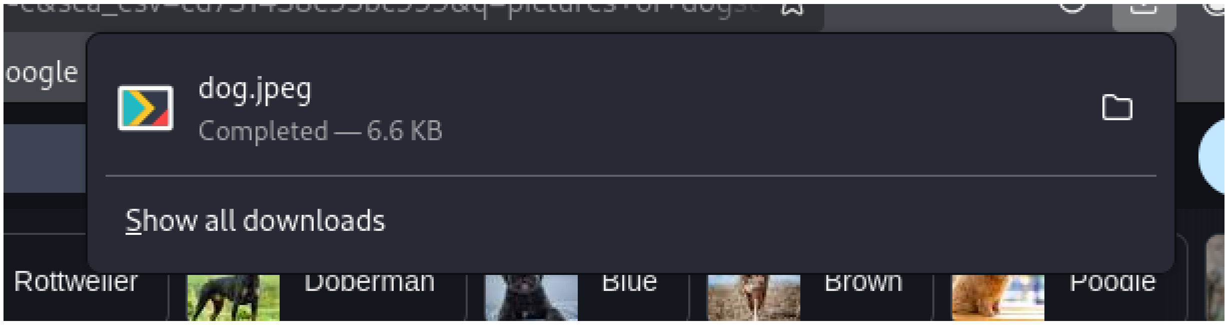
3. Go to the ***stegDir*** directory and create a new file named ***testfile.txt*** using the ***touch*** command.

4. Open the file ***testfile.txt*** using ***gedit*** and add some secret message there as the file content. Take a screenshot showing the secret message you added.



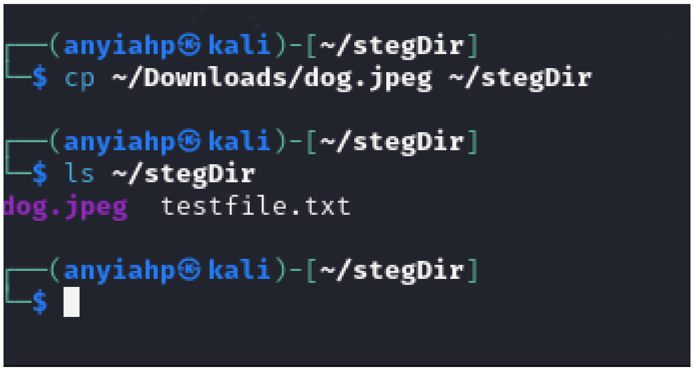
```
Jesus is King
```

5. Open Firefox (in Kali Linux) and download a random image of a dog. Name the downloaded file as ***dog.jpeg***. The image will be downloaded in the ***Downloads*** folder by default.



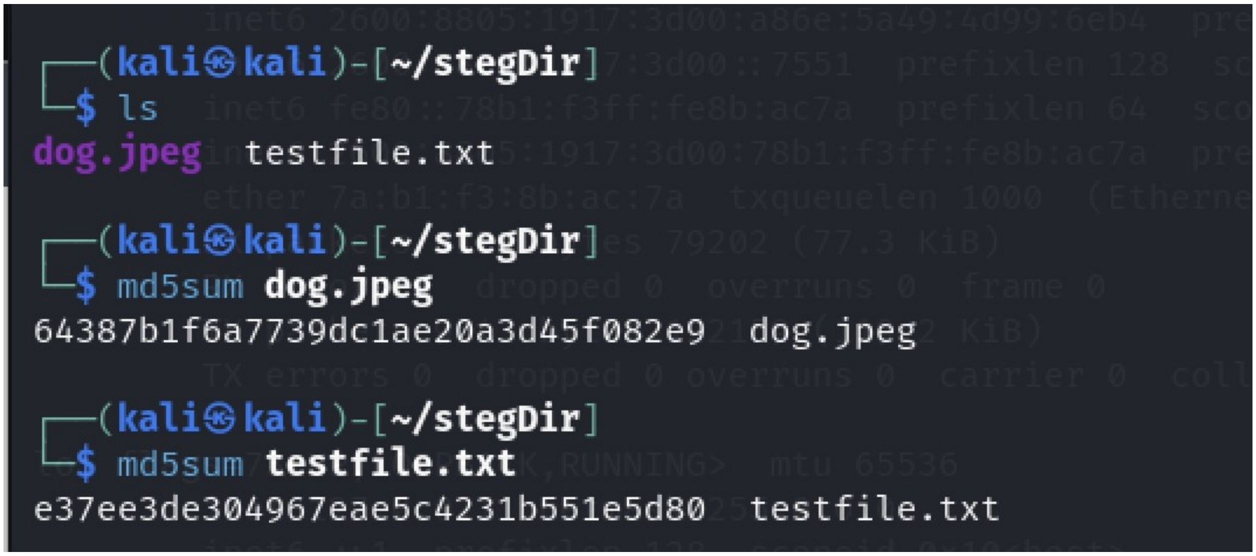
6. Copy the image from the ***Downloads*** directory to the ***stegDir*** directory using the ***cp*** command. The ***stegDir*** directory should have two files by now: *testfile.txt* and *dog.jpeg*.

Use ***ls*** command to show the contents of the ***stegDir*** directory and take a screenshot to attach it in your submission.



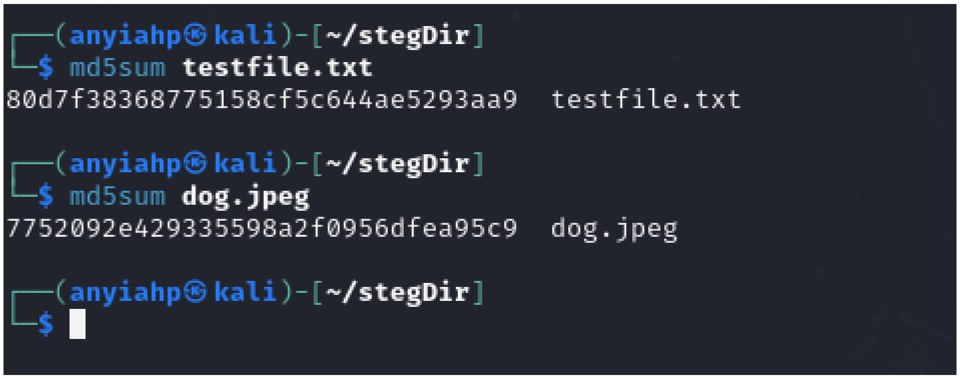
```
┌──(anyiahp㉿kali)-[~/stegDir]
└─$ cp ~/Downloads/dog.jpeg ~/stegDir

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ ls ~/stegDir
dog.jpeg   testfile.txt

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ 
```

7. Execute the ***md5sum*** command to check the checksums for both ***testfile.txt*** and ***dog.jpeg***. Learn about MD5 here: https://phoenixnap.com/kb/md5sum-linux). Take a screenshot similar to the following screenshot.



```
┌──(kali㉿kali)-[~/stegDir]
└─$ ls
dog.jpeg  testfile.txt

┌──(kali㉿kali)-[~/stegDir]
└─$ md5sum dog.jpeg
64387b1f6a7739dc1ae20a3d45f082e9  dog.jpeg

┌──(kali㉿kali)-[~/stegDir]
└─$ md5sum testfile.txt
e37ee3de304967eae5c4231b551e5d80  testfile.txt
```

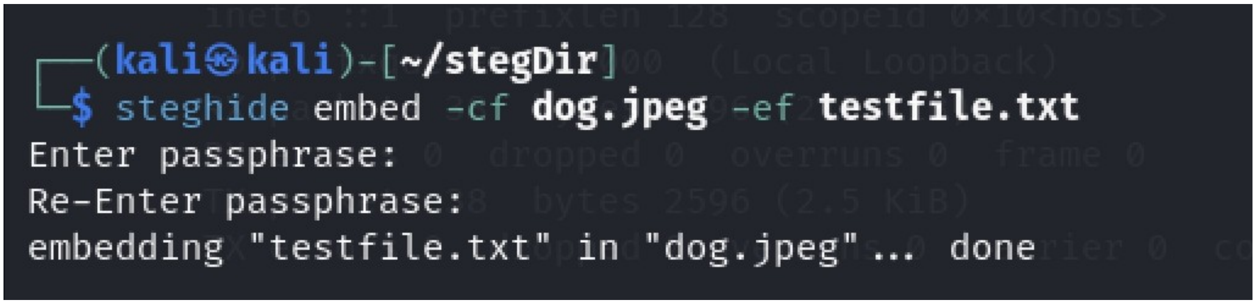
Student's image:



```
┌──(anyiahp㉿kali)-[~/stegDir]
└─$ md5sum testfile.txt
80d7f38368775158cf5c644ae5293aa9  testfile.txt

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ md5sum dog.jpeg
7752092e429335598a2f0956dfea95c9  dog.jpeg

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ 
```

8. Learn about ***steghide*** command here: https://manpages.ubuntu.com/manpages/trusty/man1/steghide.1.html.

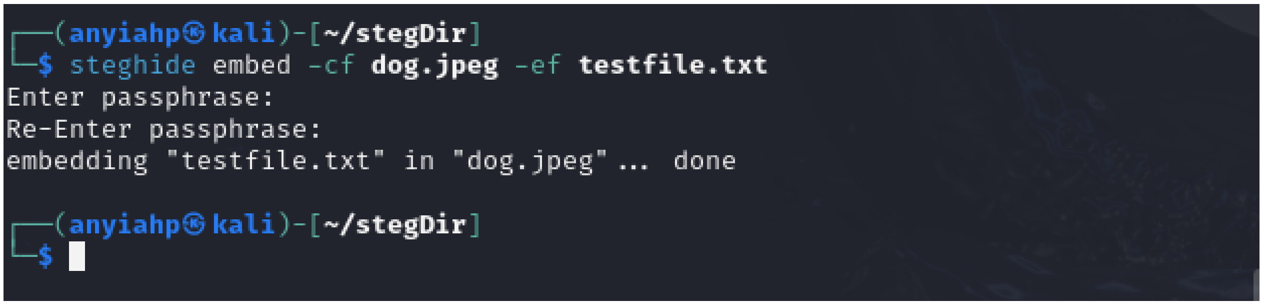
Use the ***steghide*** command to embed your ***testfile.txt*** (with secret message) into the image file **dog.jpeg** as shown in the following example screenshot (**note: *when prompted for the passphrase, you may type any password of your choice***).



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

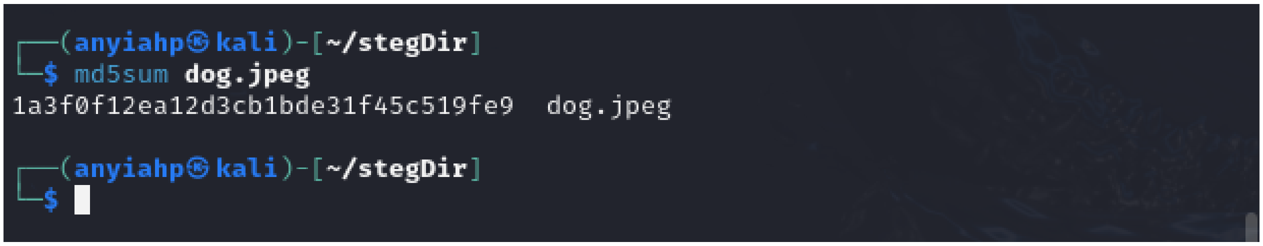
Take a screenshot showing the command and the relevant output from the terminal.

Student's image:



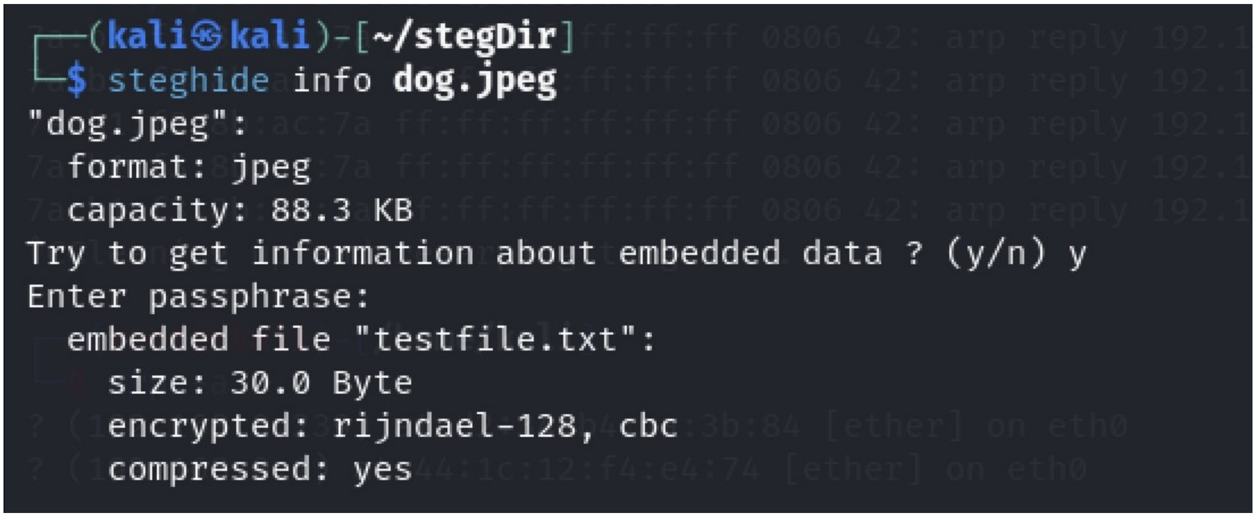
```
┌──(anyiahp㉿kali)-[~/stegDir]
└─$ steghide embed -cf dog.jpeg -ef testfile.txt
Enter passphrase:
Re-Enter passphrase:
embedding "testfile.txt" in "dog.jpeg"... done

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ 
```

9. Execute the command ***md5sum*** for ***dog.jpeg*** to check the hash for the image file. Do you see any difference? Student's answer: The output is different compared to my last output (step 7). Take a screenshot showing the command and the output hash.



```
┌──(anyiahp㉿kali)-[~/stegDir]
└─$ md5sum dog.jpeg
1a3f0f12ea12d3cb1bde31f45c519fe9  dog.jpeg

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ 
```

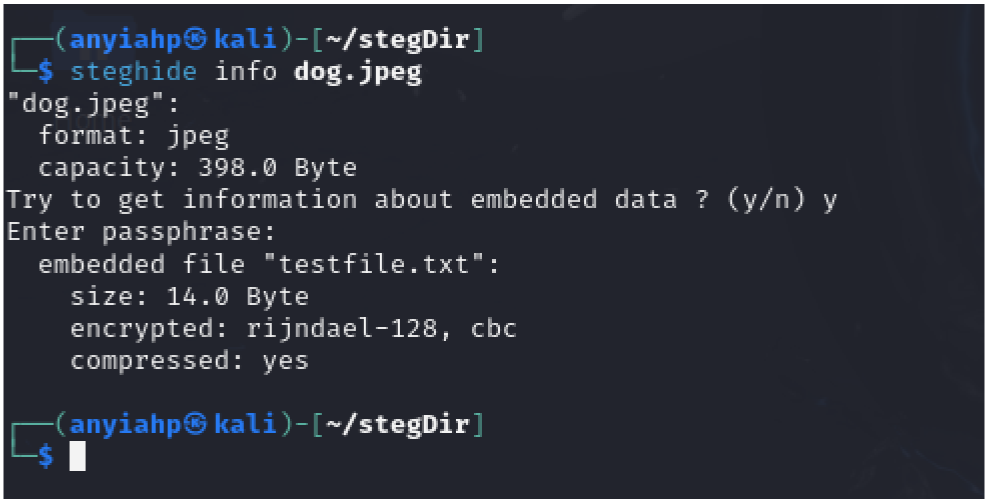
10. Execute the ***steghide*** command to get some information about ***dog.jpeg*** before extracting it, use the ***info*** command as shown in this following example screenshot:



```
┌──(kali㉿kali)-[~/stegDir]
└─$ steghide info dog.jpeg
"dog.jpeg":
  format: jpeg
  capacity: 88.3 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "testfile.txt":
    size: 30.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

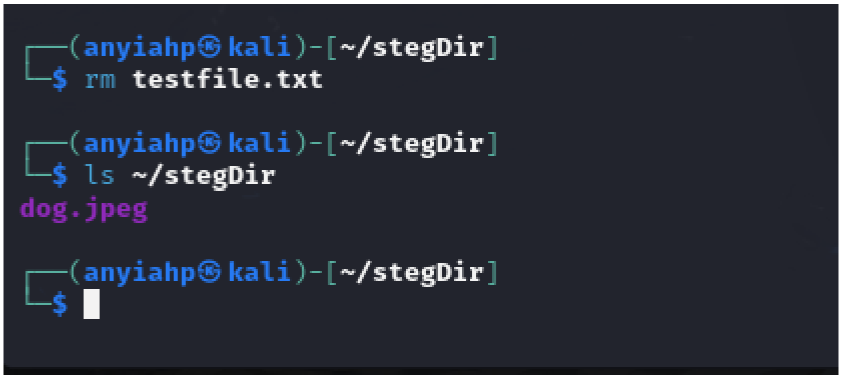
**Note that you will be asked to input the passphrase you set earlier when you embed the text file into the image**. Take a screenshot showing the command and the output.

Student's image:



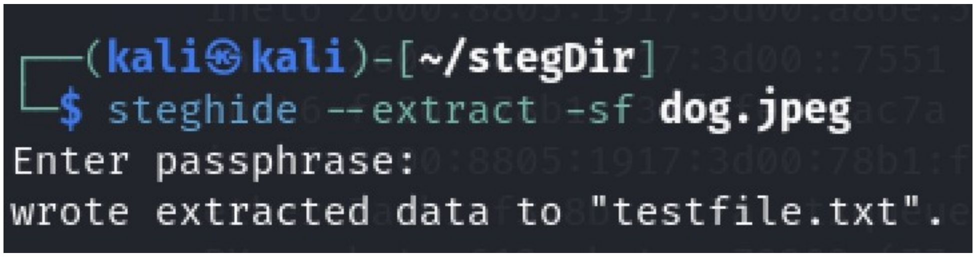
```
┌──(anyiahp㉿kali)-[~/stegDir]
└─$ steghide info dog.jpeg
"dog.jpeg":
  format: jpeg
  capacity: 398.0 Byte
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "testfile.txt":
    size: 14.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ 
```

11. Now, delete the file ***testfile.txt*** using the ***rm*** command. Use the ***ls*** command to show the contents of the ***stegDir*** directory and take a screenshot.



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

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ ls ~/stegDir
dog.jpeg

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ 
```

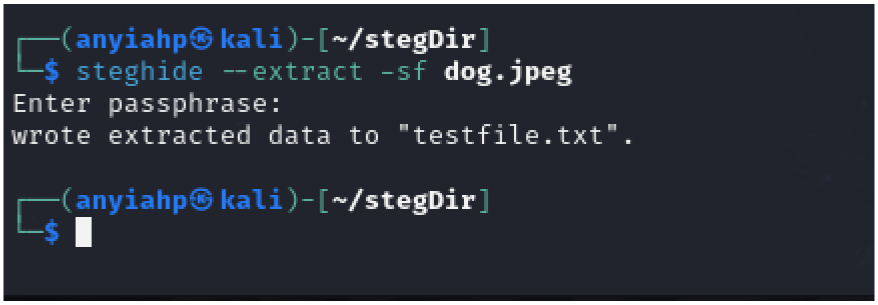
12. Extract the secret message by executing the ***steghide*** command with **- -** ***extract*** option as shown in the following example screenshot:



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

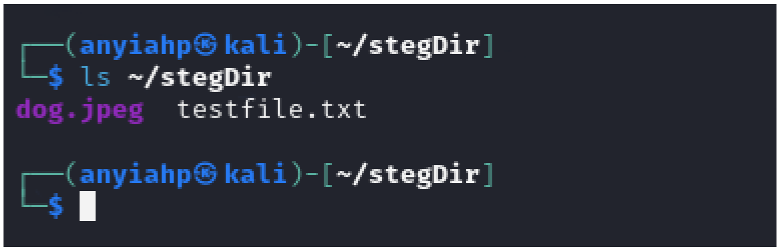
Take a screenshot showing the command and the output in the terminal.

Student's image:



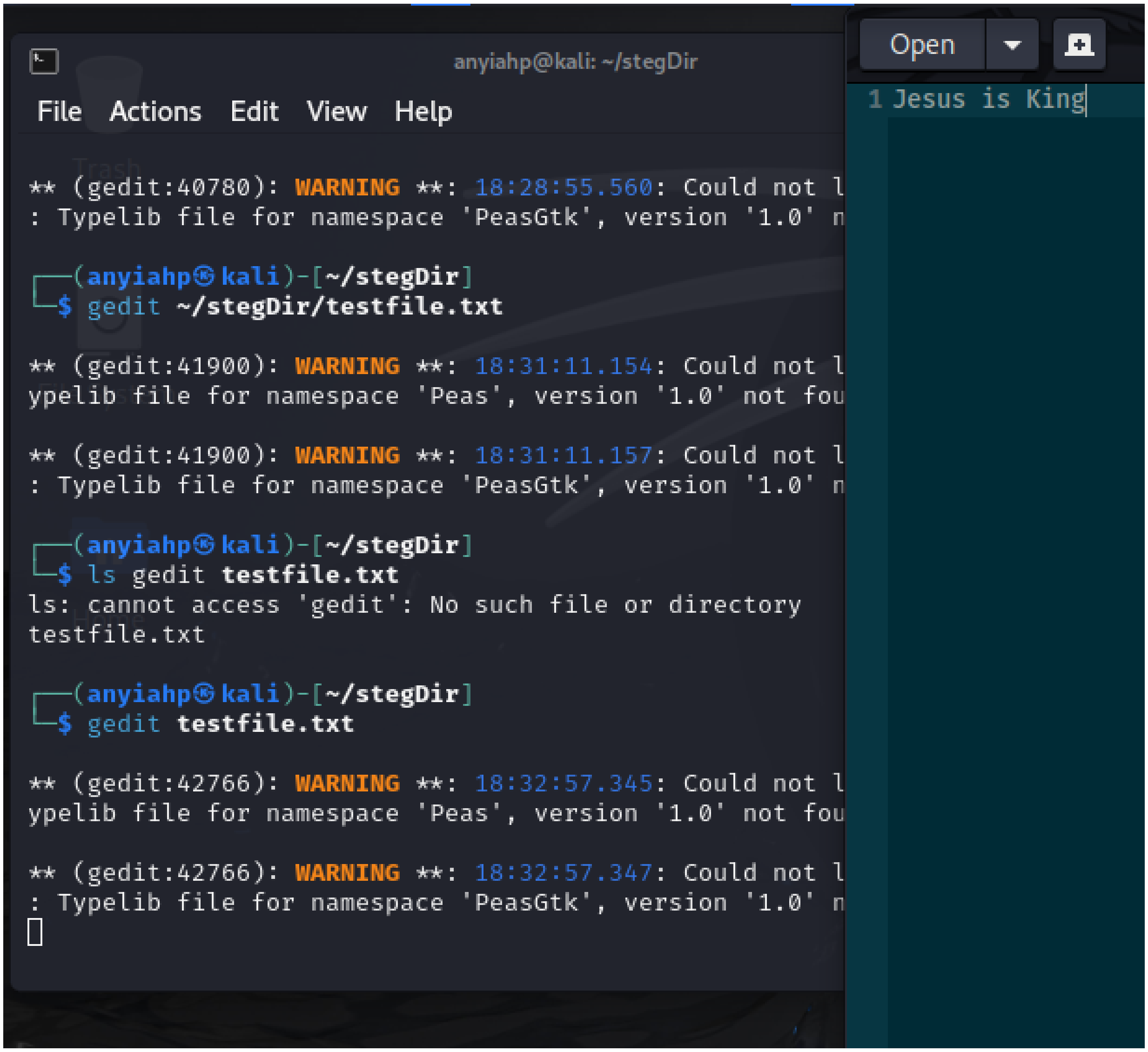
```
┌──(anyiahp㉿kali)-[~/stegDir]
└─$ steghide --extract -sf dog.jpeg
Enter passphrase:
wrote extracted data to "testfile.txt".

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ 
```

13. Execute the ***ls*** command to list the contents in the ***stegDir*** directory. You should see ***testfile.txt*** there because it was hidden in the ***dog.jpeg*** image file and appeared after extracting the image file in the previous step (step-12). Take a screenshotn showing the contents of the ***stegDir*** directory.



```
┌──(anyiahp㉿kali)-[~/stegDir]
└─$ ls ~/stegDir
dog.jpeg  testfile.txt

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ 
```

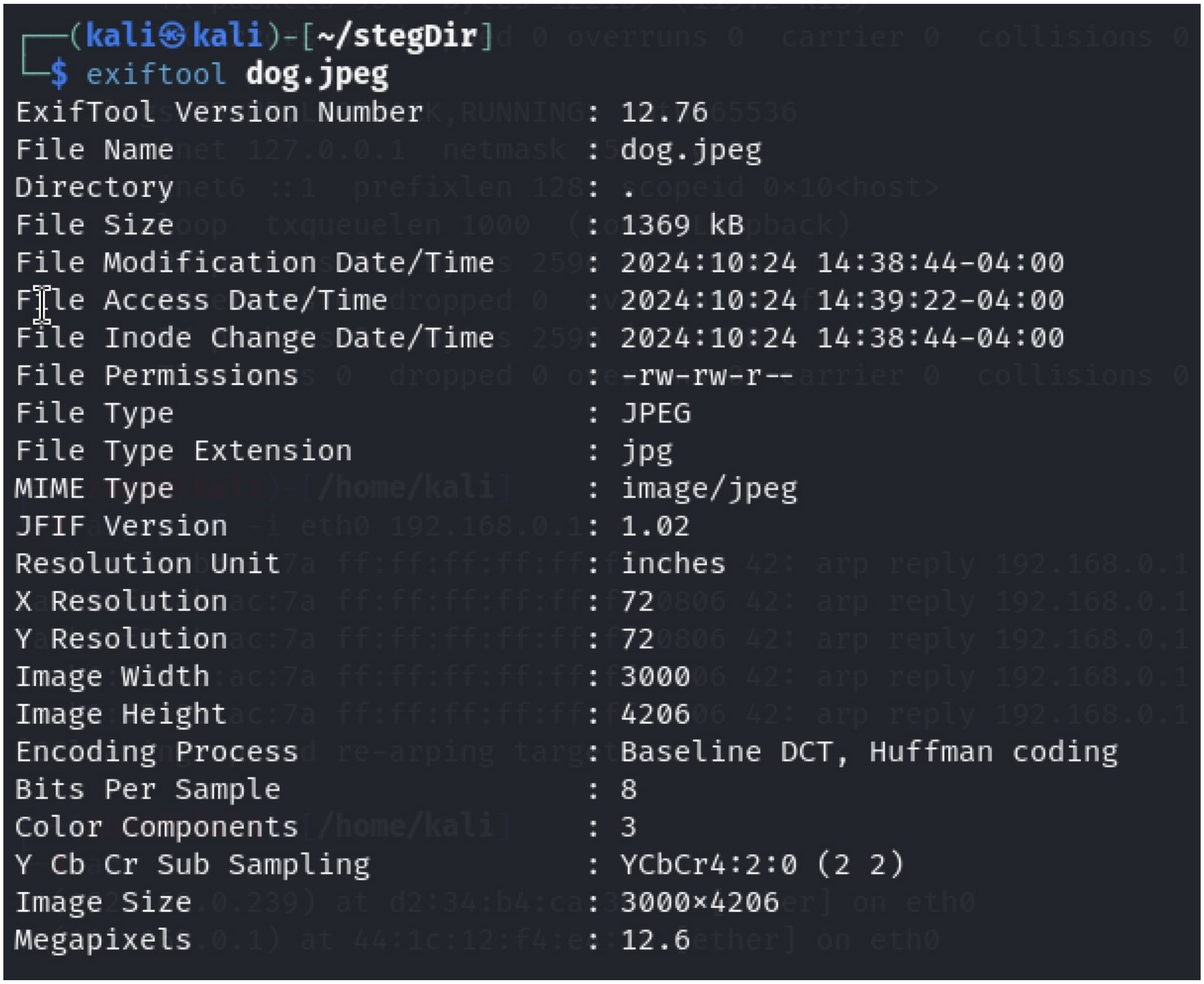
14. See the contents of the file ***testfile.txt*** using ***gedit***. Take a screenshot showing the contents.



```
** (gedit:40780): WARNING **: 18:28:55.560: Could not l
: Typelib file for namespace 'PeasGtk', version '1.0' n

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ gedit ~/stegDir/testfile.txt

** (gedit:41900): WARNING **: 18:31:11.154: Could not l
ypelib file for namespace 'Peas', version '1.0' not fou

** (gedit:41900): WARNING **: 18:31:11.157: Could not l
: Typelib file for namespace 'PeasGtk', version '1.0' n

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ ls gedit testfile.txt
ls: cannot access 'gedit': No such file or directory
testfile.txt

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ gedit testfile.txt

** (gedit:42766): WARNING **: 18:32:57.345: Could not l
ypelib file for namespace 'Peas', version '1.0' not fou

** (gedit:42766): WARNING **: 18:32:57.347: Could not l
: Typelib file for namespace 'PeasGtk', version '1.0' n
```

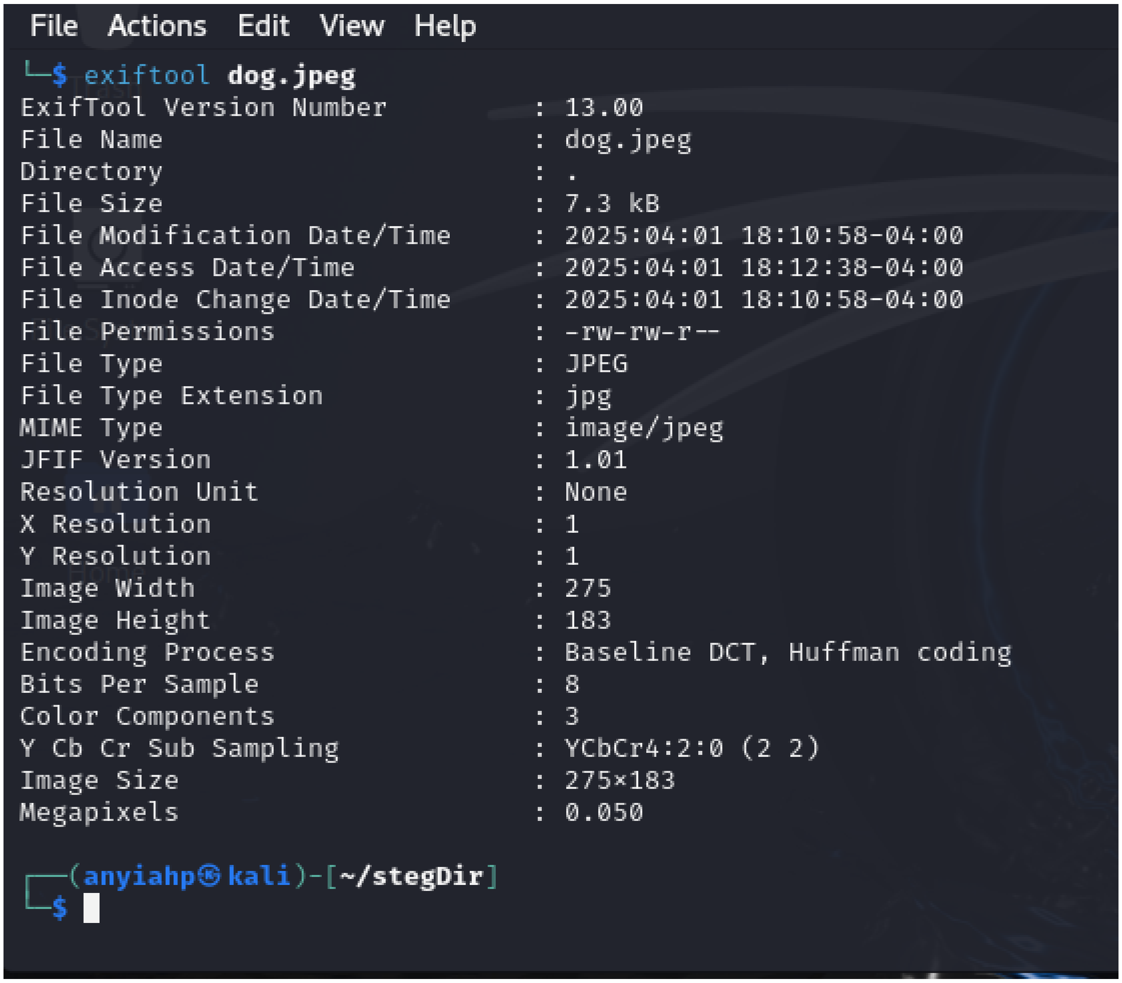
```
Jesus is King
```

15. See the metadata of the file ***dog.jpeg*** using the ***exiftool*** command as shown in the following example screenshot:



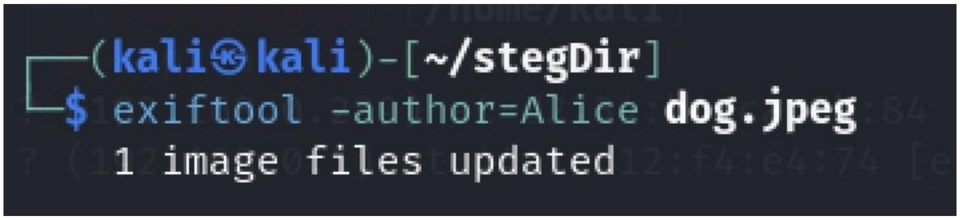
```
┌──(kali㉿kali)-[~/stegDir]
└─$ exiftool dog.jpeg
ExifTool Version Number         : 12.76
File Name                       : dog.jpeg
Directory                       : .
File Size                       : 1369 kB
File Modification Date/Time     : 2024:10:24 14:38:44-04:00
File Access Date/Time           : 2024:10:24 14:39:22-04:00
File Inode Change Date/Time     : 2024:10:24 14:38:44-04:00
File Permissions                : -rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.02
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Image Width                     : 3000
Image Height                    : 4206
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                      : 3000x4206
Megapixels                      : 12.6
```

Student’s image:



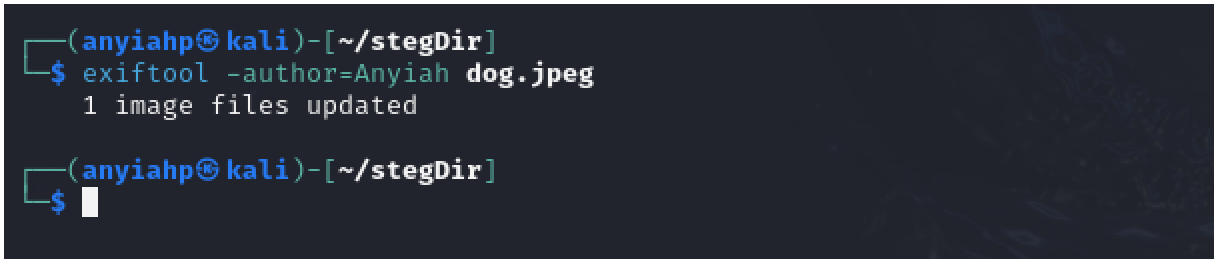
```
└─$ exiftool dog.jpeg
ExifTool Version Number         : 13.00
File Name                       : dog.jpeg
Directory                       : .
File Size                       : 7.3 kB
File Modification Date/Time     : 2025:04:01 18:10:58-04:00
File Access Date/Time           : 2025:04:01 18:12:38-04:00
File Inode Change Date/Time     : 2025:04:01 18:10:58-04:00
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
Image Width                     : 275
Image Height                    : 183
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                      : 275x183
Megapixels                      : 0.050

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ 
```

16. Change the author of the file ***dog.jpeg*** using the ***exiftool*** command as shown in the following example screenshot:



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

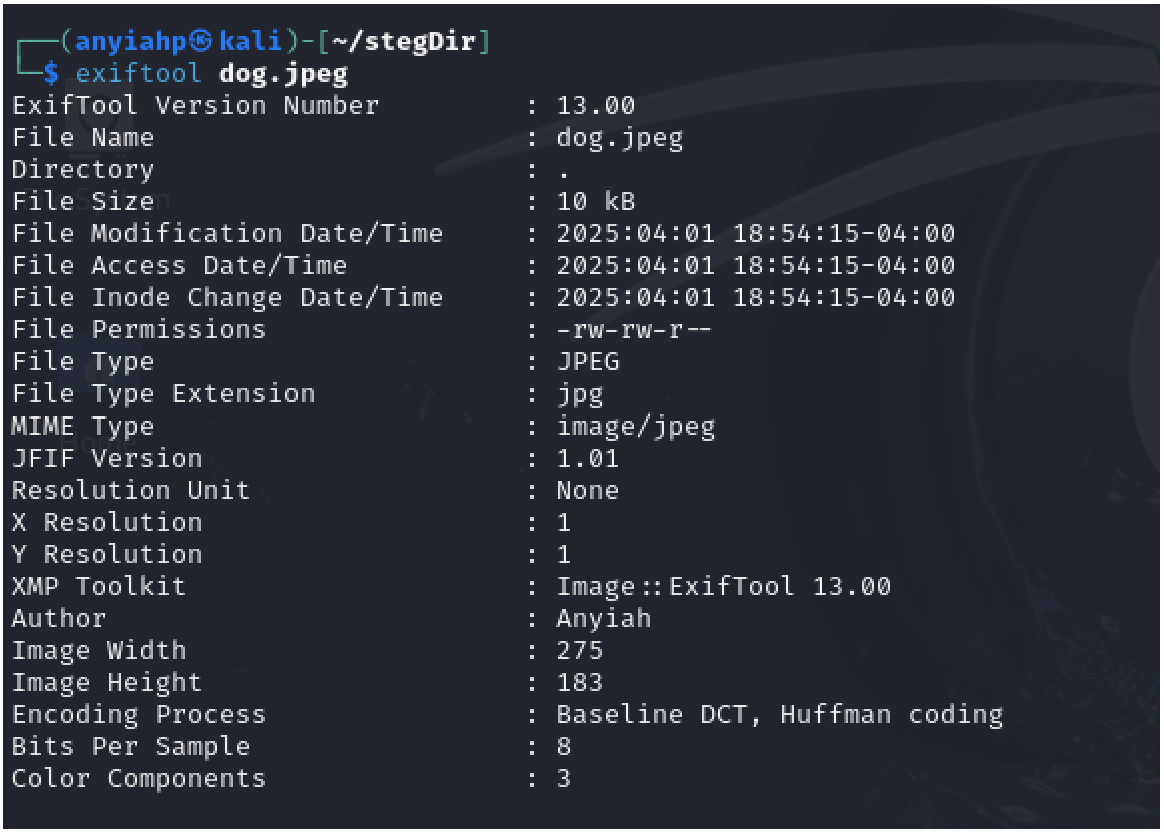
Student's image:



```
┌──(anyiahp㉿kali)-[~/stegDir]
└─$ exiftool -author=Anyiah dog.jpeg
    1 image files updated

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ 
```

**Note: when you enter the *exiftool* command in the terminal to update the author's name, make sure you replace "Alice" with your own name.**

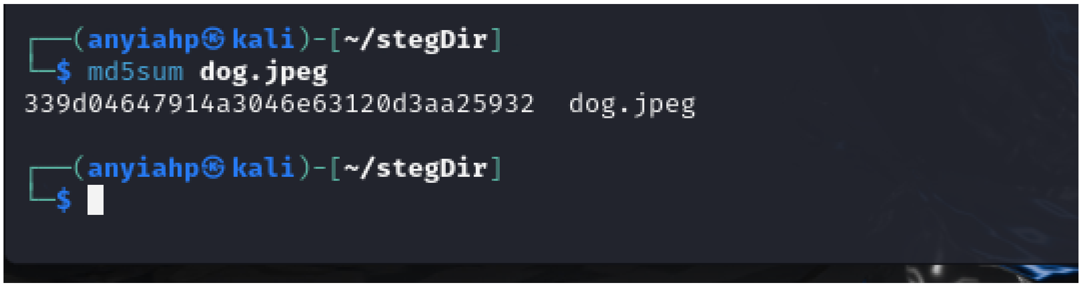
17. Repeat the step-15 and take a screenshot showing the updated metadata of the file ***dog.jpeg***. Highlight the author's name in the screenshot.



```
┌──(anyiahp㉿kali)-[~/stegDir]
└─$ exiftool dog.jpeg
ExifTool Version Number         : 13.00
File Name                       : dog.jpeg
Directory                       : .
File Size                       : 10 kB
File Modification Date/Time     : 2025:04:01 18:54:15-04:00
File Access Date/Time           : 2025:04:01 18:54:15-04:00
File Inode Change Date/Time     : 2025:04:01 18:54:15-04:00
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 13.00
Author                          : Anyiah
Image Width                     : 275
Image Height                    : 183
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
```

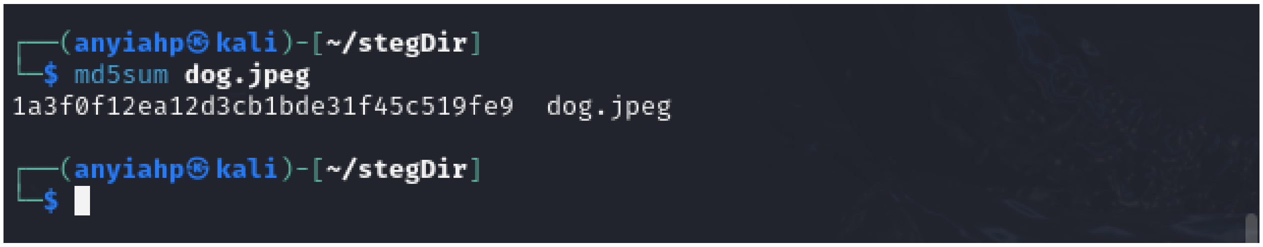
18. Execute the **md5sum** command for ***dog.jpeg***. Do you see any change in the hash value? Student's answer- The hash value for step 18 differs from the hash value in step 9. If yes, take a screenshot of the new hash and compare it with the previous hash you received in step-9.

**Step 18:**



```
┌──(anyiahp㉿kali)-[~/stegDir]
└─$ md5sum dog.jpeg
339d04647914a3046e63120d3aa25932  dog.jpeg

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ 
```

**Step 9:**



```
┌──(anyiahp㉿kali)-[~/stegDir]
└─$ md5sum dog.jpeg
1a3f0f12ea12d3cb1bde31f45c519fe9  dog.jpeg

┌──(anyiahp㉿kali)-[~/stegDir]
└─$ 
```

### Turn-in

- Attach all the screenshots in your submission.