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***.

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

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.

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.

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
```

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.

9. Execute the command ***md5sum*** for ***dog.jpeg*** to check the hash for the image file. Do you see any difference? Take a screenshot showing the command and the output hash.

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.

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.

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

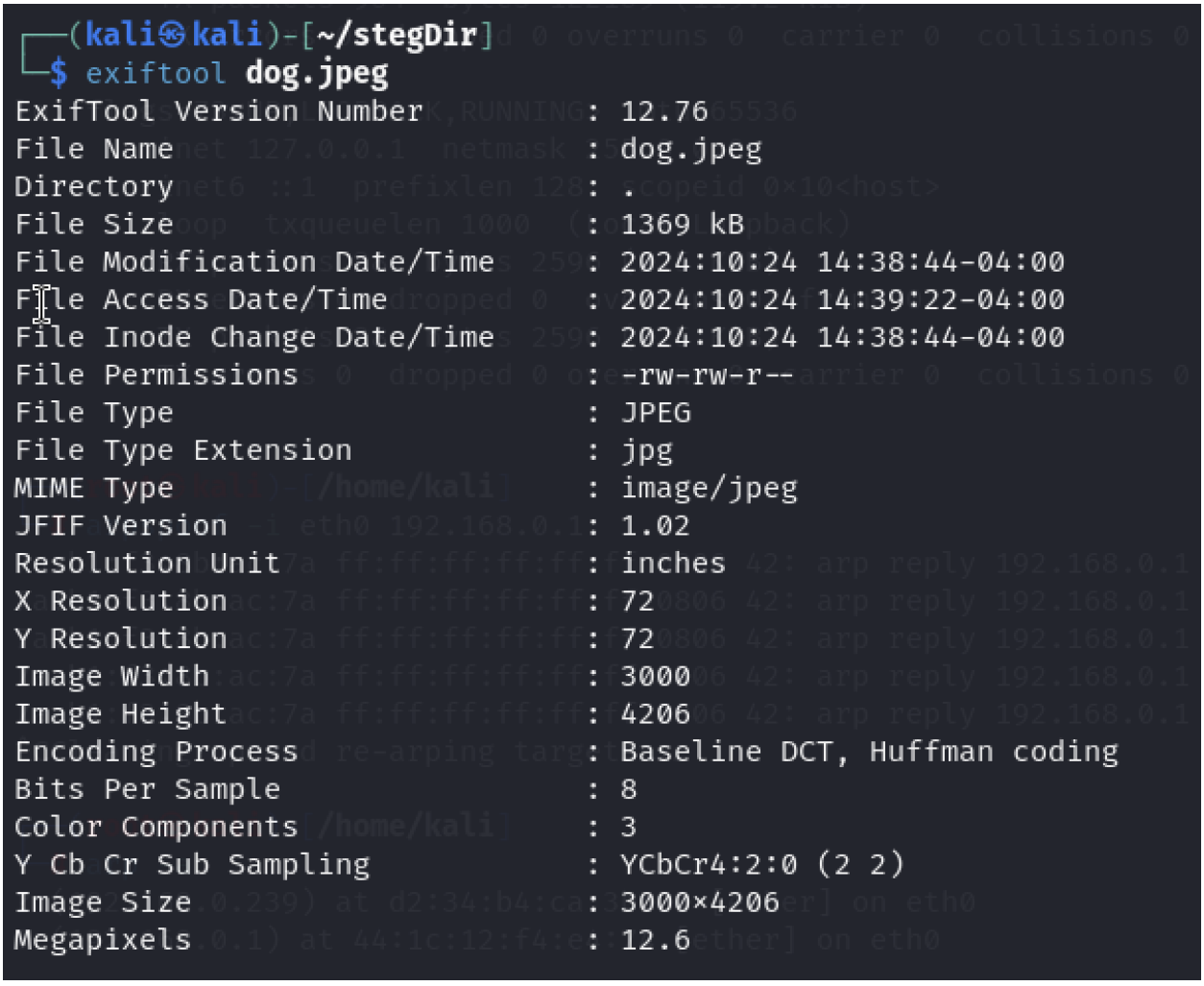
```
┌──(kali㉿kali)-[~/stegDir]
└─$ steghide --extract -sf dog.jpeg
Enter passphrase:
wrote extracted data to "testfile.txt".
```

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

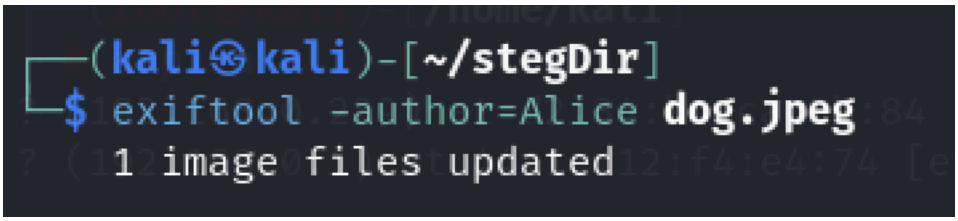
13. Execute the ***ls*** command to list the contents in the ***stegDir*** directory. You should see ***testfile.txt*** there because it was hidden in the ***dog.jpeg*** image file and appeared after extracting the image file in the previous step (step-12). Take a screenshotn showing the contents of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

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

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



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



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.

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

Turn-in

- Attach all the screenshots in your submission.