FORENSICS
LAB SERIES

Lab 15: Steganography

Material in this Lab Aligns to the Following Certification Domains/Objectives
Computer Hacking Forensic Investigator (CHFI) Objectives
13: Steganography and Image File Forensics

Document Version: 2016-08-17

Contents

Introduction

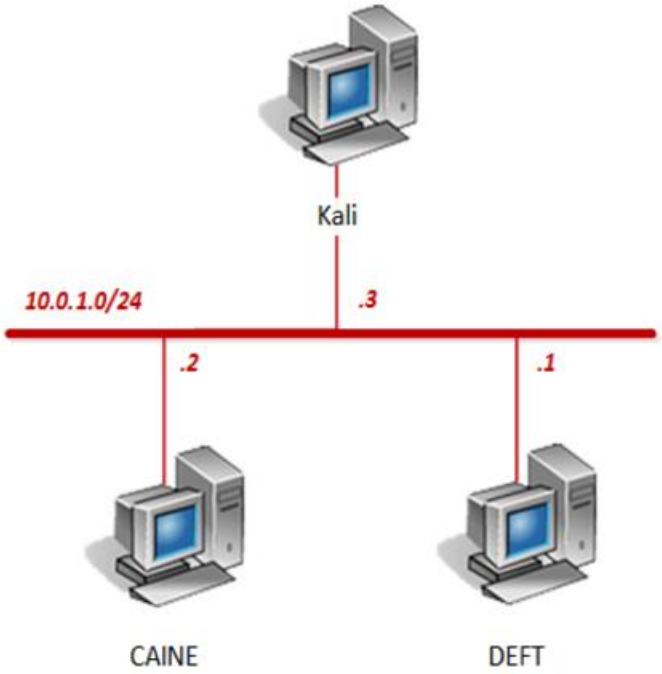
This lab will introduce steganography concepts. Steganography is the art of hiding messages or other information in various media. Various steganography techniques will be explored in this lab.

Objective

In this lab, you will be conducting forensic practices using various tools. You will be performing the following tasks:

1. Extracting Information from Image Files
2. Hiding Information in Image Files

Pod Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
DEFT	10.0.1.1	deft	password
CAINE	10.0.1.2	caine	
Kali	10.0.1.3	root	toor

1 Extracting Information from Image Files

1. Click on the **Kali** graphic on the *topology page* to open the VM.
2. Login using `root` as the *username* and `toor` as the *password*.
3. Open a new terminal by clicking on the **Terminal** icon located in the left tool pane.

4. Using the terminal, enter the command below to change to the **/root/Downloads/** directory.

```
cd Downloads
```

```
root@Kali2:~# cd Downloads
root@Kali2:~/Downloads#
```

5. Type the command below followed by pressing the **Enter** key to list only *JPG* files in the current directory.

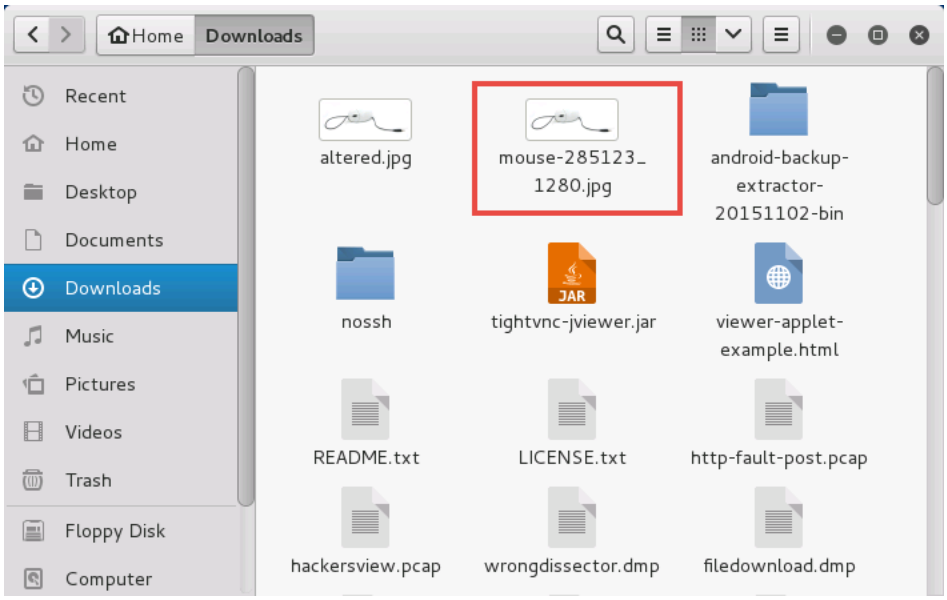
```
ls *.jpg
```

```
root@Kali2:~/Downloads# ls *.jpg
altered.jpg  mouse-285123_1280.jpg
root@Kali2:~/Downloads#
```

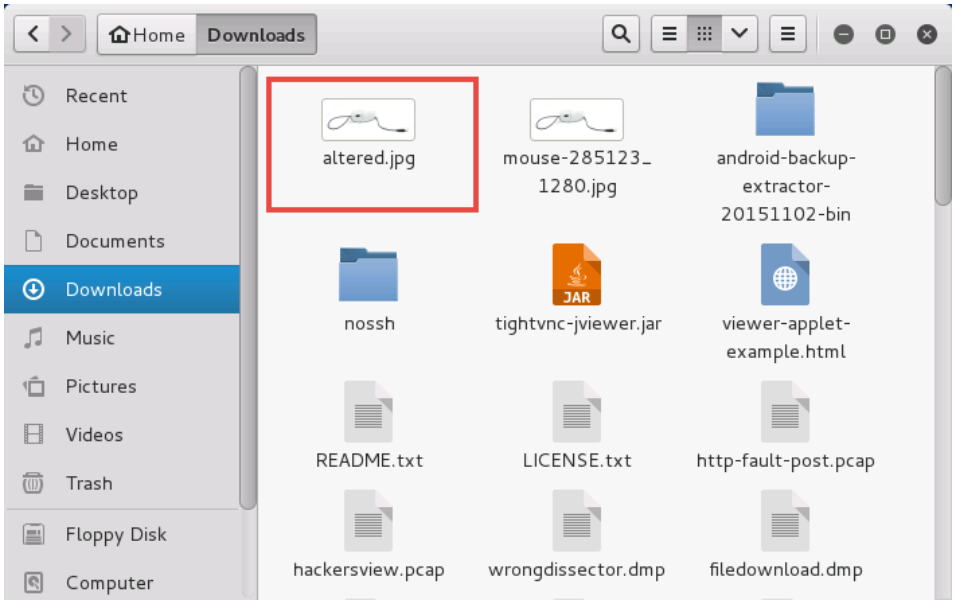
Notice the two *JPG* images.

6. Click on the **Files** icon located on the *Desktop* to open the file manager.

7. Using the file manager, navigate to **/root/Downloads/** and double-click on the **mouse-285123_1280.jpg** file to open it.



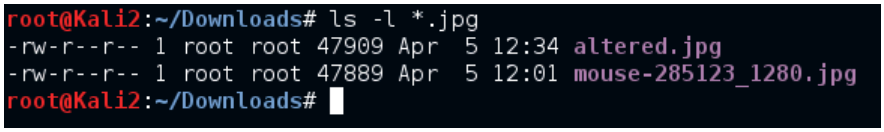
8. Notice a new file window appears showing an image of a mouse peripheral. Leave this window opened and change focus back to the **file manager**.
9. Using the file manager, double-click on the **altered.jpg** file to open it.



10. In the new file window, compare the image with the previously opened image. Notice that the images are visually the same. Close both **file windows**.
11. Change focus to the **terminal**.

12. Using the terminal, enter the command below to list the *JPG* files in a list view.

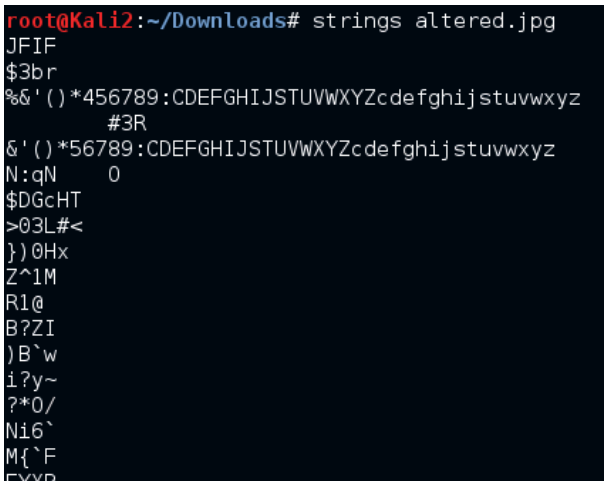
```
ls -l *.jpg
```



Notice the file sizes for both image files, one is different from the other even though they are visually the same image with the same file format.

13. Use the *strings* command on the *altered.jpg* file by typing the command below followed by pressing the **Enter** key. This command will pull all the *ASCII* strings out of the image.

```
strings altered.jpg
```

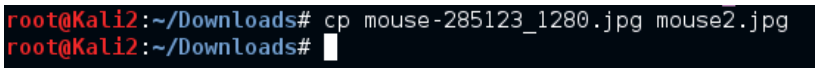


Notice at the very end of the string the word "*Hide*" is presented. This is one example of how text can be hidden in the hex values of an image.

2 Hiding Information in Image Files

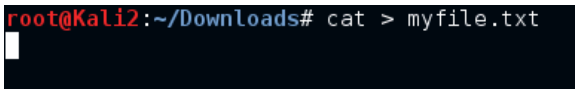
1. Using the terminal, make a copy of the **mouse-285123_1280.jpg** image file by entering the command below.

```
cp mouse-285123_1280.jpg mouse2.jpg
```



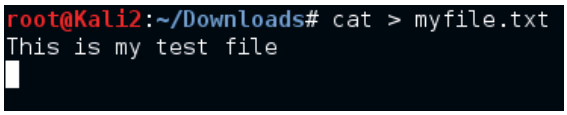
2. Begin to create a text file by entering the command below.

```
cat > myfile.txt
```

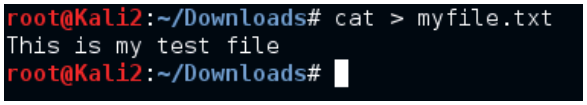


3. Continue to type in the terminal by typing the words below followed by pressing the **Enter** key.

```
This is my test file
```

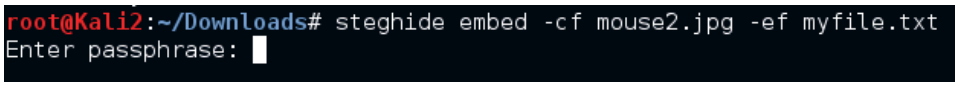


4. Press **CTRL+D** to save and exit the file.



5. Use the *Steghide* tool to hide text in an image file. Enter the command below to hide the **myfile.txt** file inside the **mouse2.jpg** file.

```
steghide embed -cf mouse2.jpg -ef myfile.txt
```



Command Breakdown:

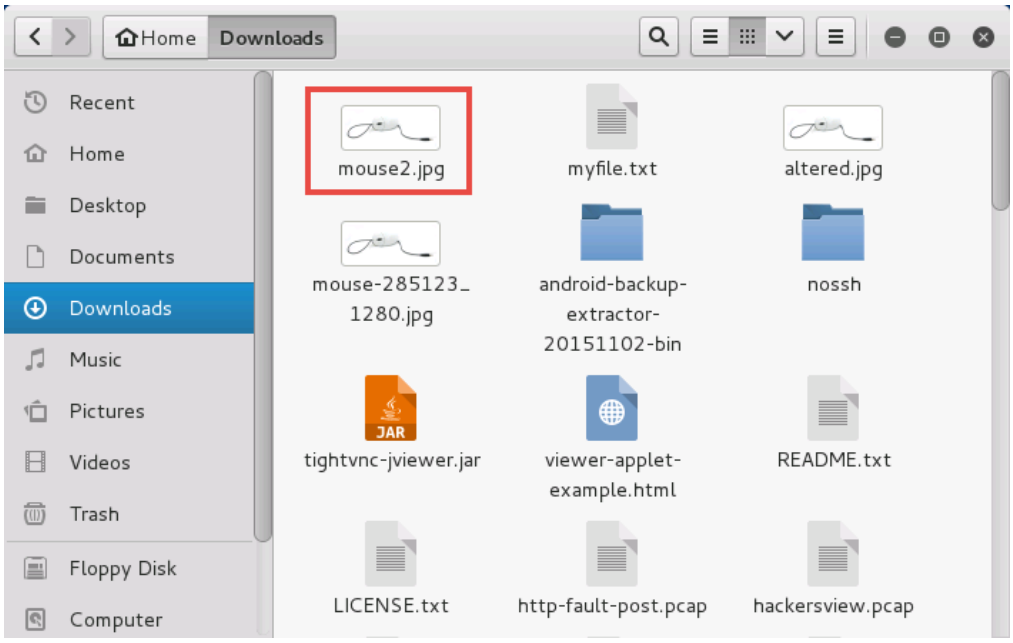
-cf = means to cover file
-ef = means to embed file

6. When prompted for a passphrase, type **`password`** following by pressing the **Enter** key.

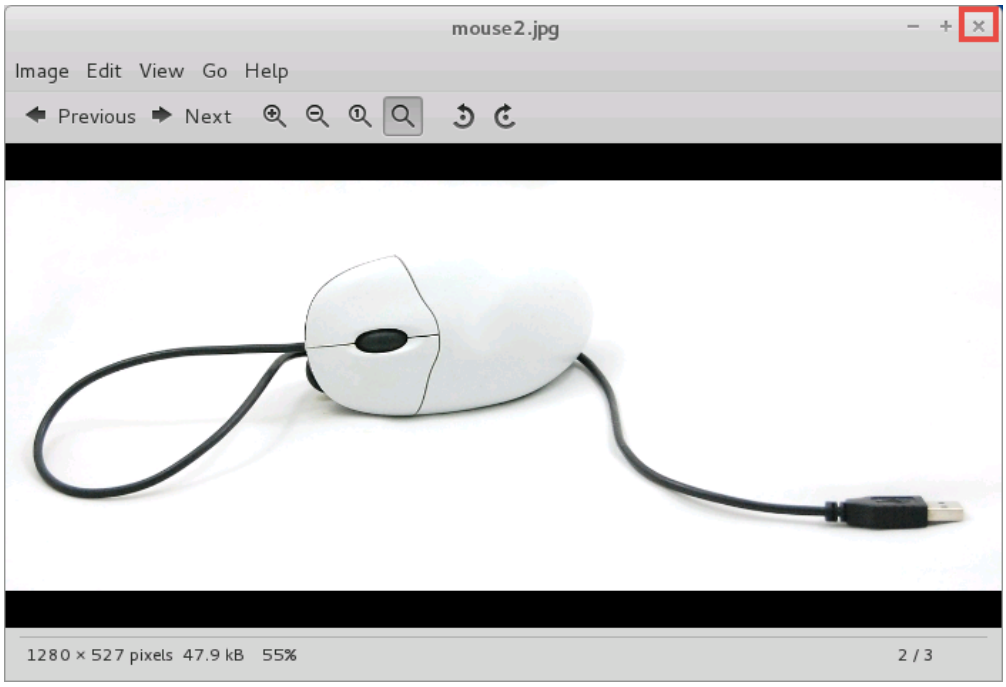
7. Type `password` once more. Press **Enter**.

```
root@Kali2:~/Downloads# steghide embed -cf mouse2.jpg -ef myfile.txt
Enter passphrase:
Re-Enter passphrase:
embedding "myfile.txt" in "mouse2.jpg"... done
root@Kali2:~/Downloads#
```

8. Change focus to the **file manager**.
9. Using the file manager, make sure to be viewing the **/root/Downloads/** directory and double-click on the **mouse2.jpg** file to open it.



10. In the new file window, notice again that there is no visual difference. Close the window.



11. Change focus back to the **terminal**.
12. Using the terminal, enter the command below to list the *JPG* files in a listed view.

```
ls -l *.jpg
```

```
root@Kali2:~/Downloads# ls -l *.jpg
-rw-r--r-- 1 root root 47909 Apr  5 12:34 altered.jpg
-rw-r--r-- 1 root root 47889 Apr  5 12:01 mouse-285123_1280.jpg
-rw-r--r-- 1 root root 47913 Aug  3 12:35 mouse2.jpg
root@Kali2:~/Downloads#
```

Notice the file size has changed from the original.

13. The *myfile.txt* file has been compressed and encrypted with *AES* by default. Use *Steghide* to extract the information by entering the command below.

```
steghide extract -sf mouse2.jpg
```

```
root@Kali2:~/Downloads# steghide extract -sf mouse2.jpg
Enter passphrase:
```

Command Breakdown:

-sf = means to source file

14. When prompted for a passphrase, type **`password`** followed by pressing **Enter**.

```
root@Kali2:~/Downloads# steghide extract -sf mouse2.jpg
Enter passphrase:
the file "myfile.txt" does already exist. overwrite ? (y/n)
```

15. When prompted to overwrite, press **`Y`** to confirm.

```
root@Kali2:~/Downloads# steghide extract -sf mouse2.jpg
Enter passphrase:
the file "myfile.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "myfile.txt".
root@Kali2:~/Downloads#
```

Notice the *myfile.txt* has been extracted from the image file which it was embedded to.

16. Confirm the integrity of the *myfile.txt* file by entering the command below.

```
cat myfile.txt
```

```
root@Kali2:~/Downloads# cat myfile.txt
This is my test file
root@Kali2:~/Downloads#
```

17. Close all **PC Viewers** and end the reservation to complete the lab.

