

Name: _____ Student ID: _____

COS30015 Internet Security Lab6

You will need:
[RedHat Linux 7.3 \(VM\)](#)
A computer with internet access

In this lab you will perform a forensic analysis of a disk image using Autopsy/TSK

1. Start Virtual machine Loader, and download and launch the *RedHat Linux with local network* VM image.
2. After Linux finishes booting, log in as hacker (password warezwarez)
3. Start the x-windows server:
startx <Enter>
4. Maximise the VM window



5. Launch Mozilla (old name for Firefox)



6. Click New Case
7. Fill in the form.

Name: _____ Student ID: _____

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can only contain letters, numbers, and symbols.

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. b.

c. d.

e. f.

g. h.

i. j.

NEW CASE **CANCEL** **HELP**

8. ...and click New Case

You will get a feedback message and an OK button. If the button does not appear, go back in the browser and re-submit the form.

CASE GALLERY **HOST GALLERY** **HOST MANAGER**

Name	Description
<input checked="" type="radio"/> HITxx21_lab10	First autopsy case details

OK **NEW CASE** **MAIN MENU**
HELP

Note: many cases could appear here - select the one you have just created. (OK)

CASE GALLERY **HOST GALLERY** **HOST MANAGER**

No hosts have been added to case yet

ADD HOST **CLOSE CASE**
HELP

9. ...Click Add Host

10. Fill in the form. Note that the local time is GMT + 10, so enter 10 for timezone.

The data was collected during daylight saving time, so enter 3600 (1 hour in seconds) for the timeskew setting.

1. **Host Name:** The name of the computer being investigated. It can only have letters, numbers, and symbols.

2. **Description:** An optional one-line description or note about this computer.

3. **Timezone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

ADD HOST **CANCEL** **HELP**

Timeskew is (for this computer) 1h == 3600 seconds (in the past)

CASE GALLERY **HOST GALLERY** **HOST MANAGER**

Name	Description	
<input checked="" type="radio"/> sd-card01	KFC data breach investigation	details

Investigator (for reports only): None Provided

OK **ADD HOST** **CLOSE CASE**
HELP

11. Click on details to see data entered for this case:

HOST DETAILS

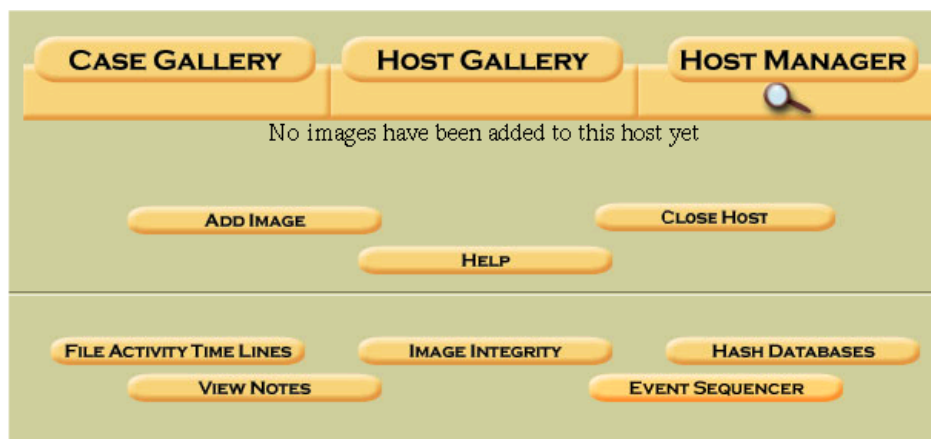
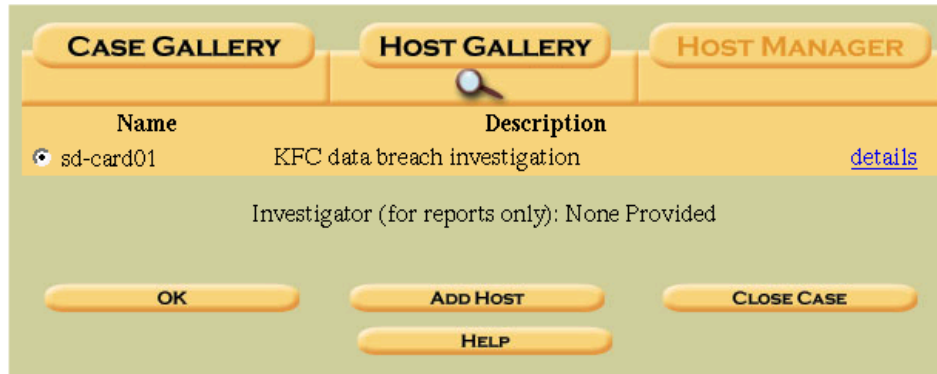
Name: sd-card01
Description: KFC data breach investigation
Timezone: 10
Timeskew: 3600

Directory: /home/hacker/evidence//HITxx21_lab10/sd-card01/

Alert Hash Database:
Exclude Hash Database:

OK

12. Click OK to load the *dd* file into the case:



13. Click Add Image

You will need the path to the disk image. To get this, open a console



window

14. And *cd* into the evidence directory:

```
[hacker@server hacker]$ ls
buffer  evidence JITXSS remoteshell trojan
energiser exploits jpeg.pl something.jpg
[hacker@server hacker]$ cd evidence
[hacker@server evidence]$ ls
autopsy.log HITx21_lab10 ictev image.dd reformatted.dd
[hacker@server evidence]$
```

The disk image is called *image.dd*

Note that the path is absolute – use *pwd* to get the path:

```
[hacker@server evidence]$ pwd
/home/hacker/evidence
[hacker@server evidence]$
```

1. **Location:** The full path (starting with /) to the raw file system image.
/home/hacker/evidence/image.dd

2. **Import Method:** The image can be imported into the Autopsy Evidence Locker from its current location by making a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
☒ Symlink ☐ Copy ☐ Move

3. **File System Type:** Specify the type of file system.
fat16

4. **Mount Point:** The directory or drive where the file system was mounted in the original suspect system (i.e. c:\ for Windows or /usr/ for UNIX). Not needed for swap or raw file system types.
E\ other:

5. **Data Integrity:** An MD5 hash can be used to verify the integrity of the file system image.
☒ A hash value has not been calculated yet, do it now.
☐ Do nothing about integrity checks for this image.
☐ The MD5 hash for this image is already known:
Verify MD5 After Importing?

ADD IMAGE CANCEL HELP

15. Fill in the form as above and click Add Image

Linking /home/hacker/evidence/image.dd to /home/hacker/evidence//HITox21_lab10/sd-card01//images/image.dd

Calculating MD5 of images/image.dd (this could take a while)
+ Current MD5: 9795FCF6ABA566FA03C08D0F9652392F

Image: /home/hacker/evidence/image.dd added to config file as images/image.dd

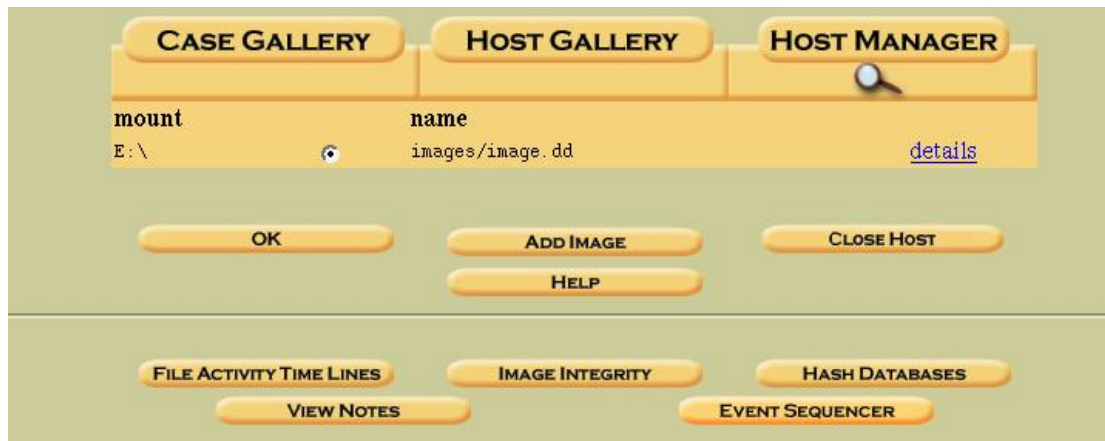
OK ADD IMAGE

16. Note the MD5 hash – you can use this later to confirm that your analysis has not altered the evidence.

What is the MD5 hash?

17. Click OK to continue

Name: _____ Student ID: _____



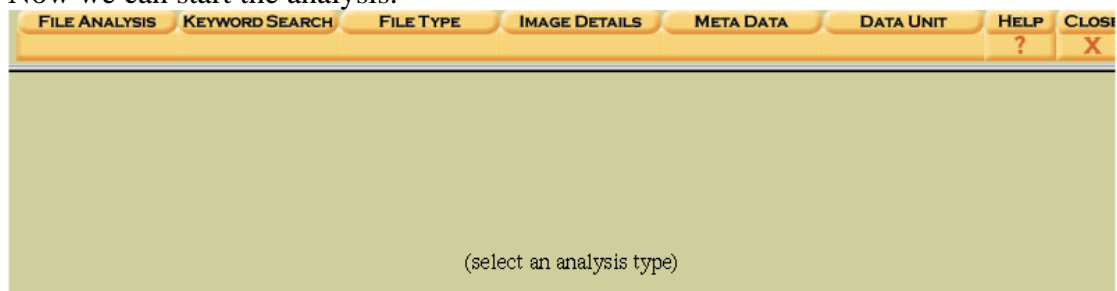
18. Click on Details



19. Click "OK" to return

20. Click "OK" to continue...

Now we can start the analysis.



21. Click on FileAnalysis



This is the file browser. You can select an underlined file (all of these have been deleted) and view its contents on the lower panel.

In the lower panel you can select the view (ASCII, Strings or Export). Export writes the file to the hard drive (/home/hacker/) where you can view it with an appropriate viewer.

22. Find the **Meta** value of *PgI71.png*.

There are two copies of the filesystem entry for *PgI71.png*. One is 54. 54 is actually the **iNode** number of this file.

To restore the file (and look at it) we need to do File Carving – Autopsy is not very good for this, so we'll use a Linux command from the console window:

Make sure that you are in the /home/hacker/evidence directory

23. Type:

```
icat image.dd 54 > picture.png
```

```
[hacker@server evidence]$ pwd
/home/hacker/evidence
[hacker@server evidence]$ ls
autopsy.log HITxx21_lab10 icatv image.dd reformatted.dd
[hacker@server evidence]$ icat image.dd 54 > picture.png
[hacker@server evidence]$
```

24. Now switch to the desktop and click on *picture.png* (if needed, click on the “hacker’s home” icon, click on the evidence directory)

But the image is corrupted!

Let's do a low-level recovery of the image.

Note that *reformatted.dd* is another copy of the disk image.

25. First we use the console to issue the command:

```
xxd reformatted.dd | grep 'PNG'
```

This searches for the PNG file signature at the start of the file.

```
[hacker@server evidence]$ xxd reformatted.dd | grep 'PNG'
0059000: 8950 4e47 0d0a 1a0a 0000 000d 4948 4452 .PNG.....IHDR
0b9e3f0: 3751 504e 4734 6f70 4c76 5633 4967 377a 7QPNG4opLvV3Ig7z
2ac9400: 303f 9d3c 3750 4e47 6a37 d0b9 6d60 666c 0?,<7PNGj7D,m`f1
2ad9c80: 504e 47e3 4d60 1870 307a e6b4 b5d3 4c1a PNG&M`.p0zæ,µÓL.
2cc8cf0: 5708 1c6f 504e 474f a7d6 9063 92c4 e4f3 W..oPNGO.Ö.c.Ääó
33ebe70: a680 903a 504e 474a 5ca8 ec8c eec5 d84f ...:PNGJ\,i,iÂ00
37f0580: 467c b649 c83c 5279 2c91 8550 4e47 eb4d F|.IÉ<Ry,..PNGeM
3ca5fe0: 0cd3 b23d 6800 c8ce 7a50 4e47 1400 b918 .D.=h.ÈIzPNG....
425b9e0: b850 f950 4e47 4033 594a 1ad8 5a4b 6dc8 .PùPNG@3YJ.ØZKmÈ
48a5a40: 504e 4734 b184 8e0c 95c1 20f4 ef56 ccef PNG4.....Á ôiVïi
48cf8f0: 8b63 0011 f89a 10b7 1c58 a050 4e47 d79a .c.,ø,...X.PNG..
4d5dbb0: 89b5 4487 3b48 504e 4735 cb3b f3ca e744 .µD.;HPNG5É;óÊçD
4e8f3c0: 0932 e639 06d2 4750 4e47 e54d 8a04 8510 .2æø.òGPNG&M....
53d3130: 81be 9a03 b92a 047f 504e 47e3 473c a3ba .....*..PNG&G<.,°
5c3a5c0: 2aad 1850 4e47 56f5 abb2 ab2a 9f9f e959 *.PNGVö...*,.éY
681ea90: 242c b12f 504e 4718 1500 4c1c d694 ea5f $,./PNG...L.Ö.ê_
```

Found at **0x0059000 = 364544** \\ (decimal)

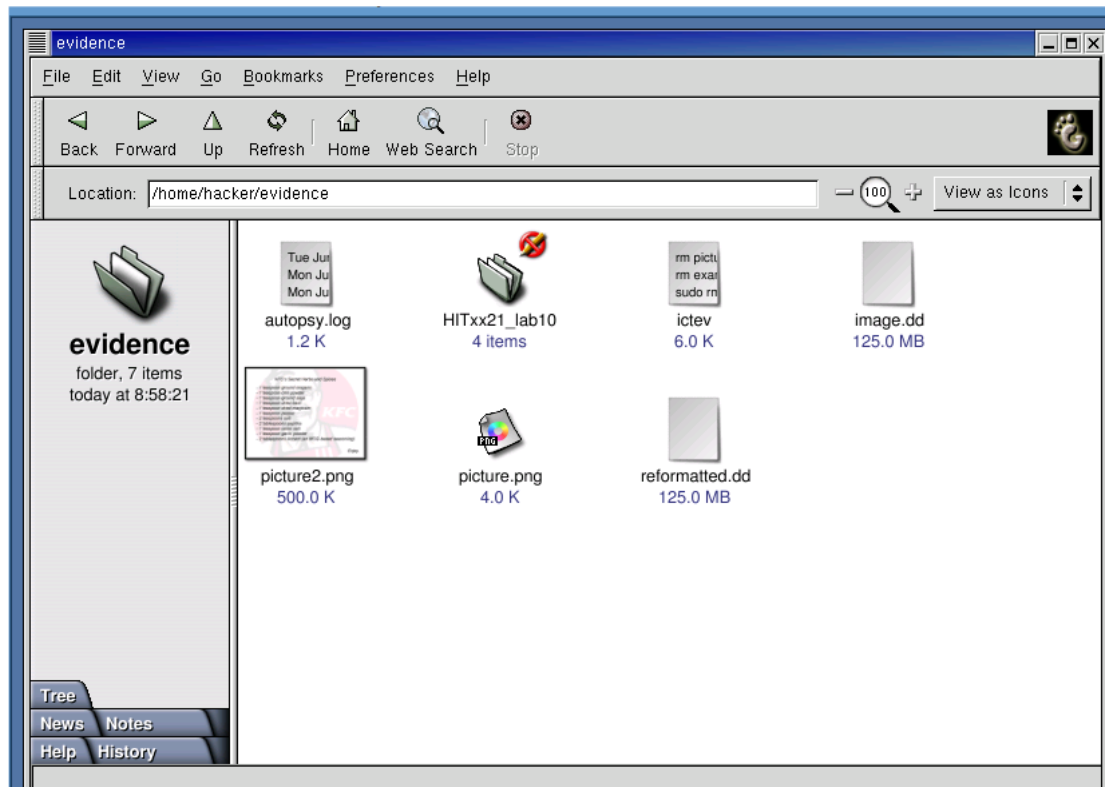
divide by 512 = 712 sectors

26. Then we use *dd* to recover the file:

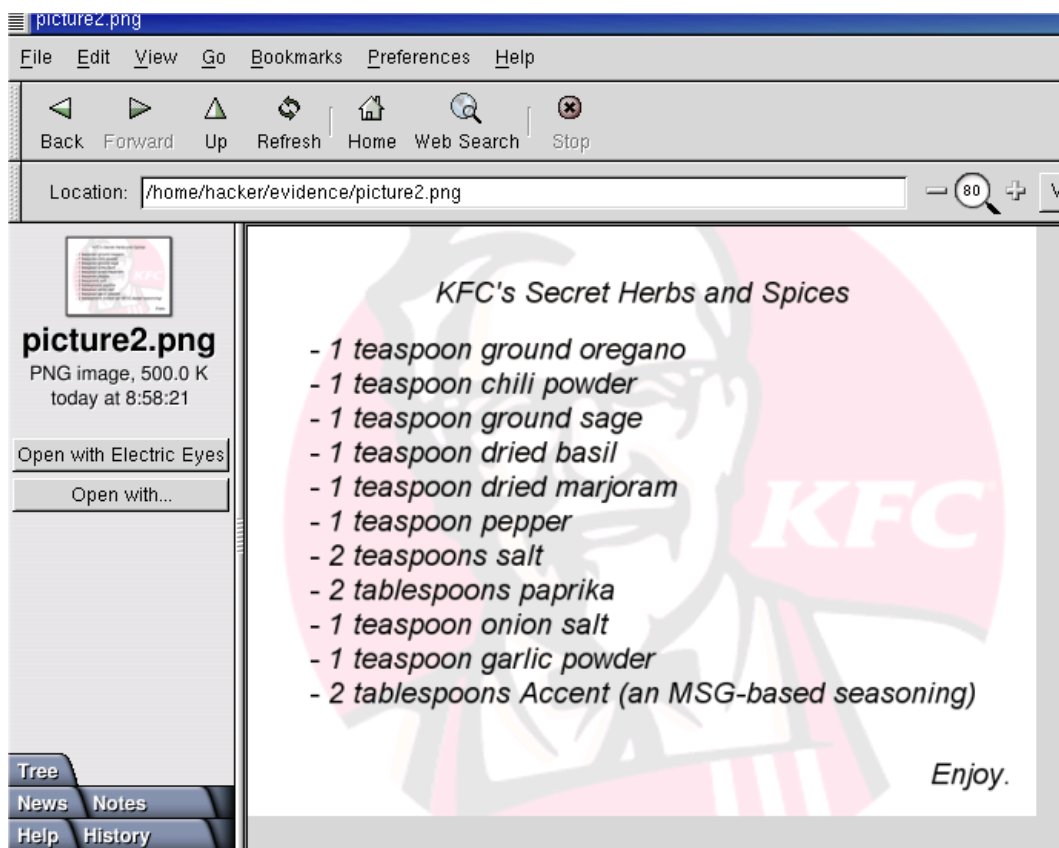
```
dd if=reformatted.dd of=picture2.png skip=712 bs=512 count=1000
```

```
[hacker@server evidence]$ dd if=reformatted.dd of=picture2.png skip=712 bs=512 count=1000
1000+0 records in
1000+0 records out
[hacker@server evidence]$ █
```

27. Now switch to the desktop and click on *picture2.png*



Congratulations!



Name: _____ **Student ID:** _____

Have fun!

End of lab.