Name: _____ **Student ID:**_____

You will need:
RedHat Linux 7.3 (VM)
A computer with internet access

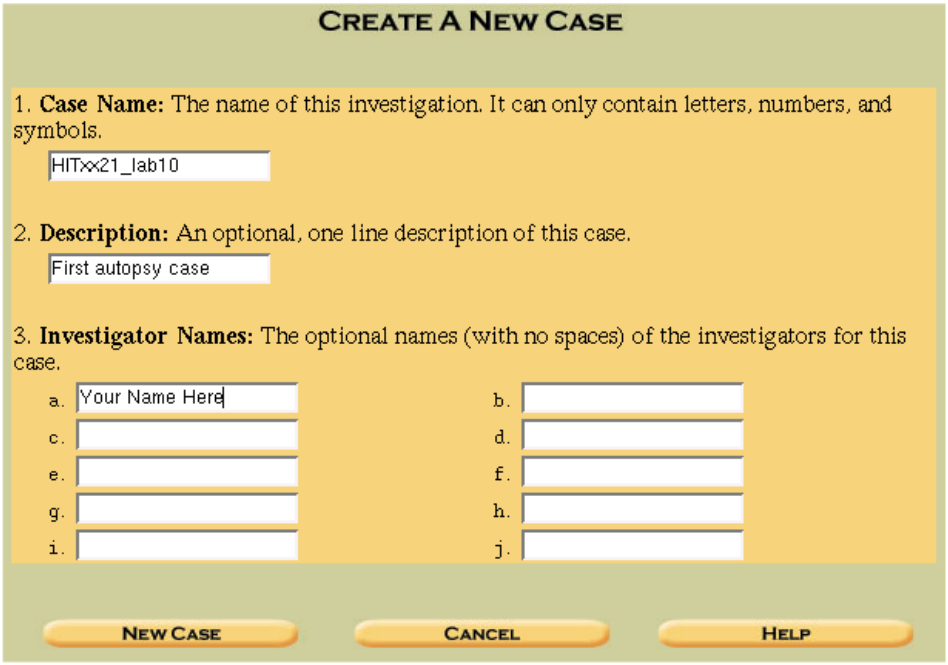
COS30015 Internet Security
Lab6

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.

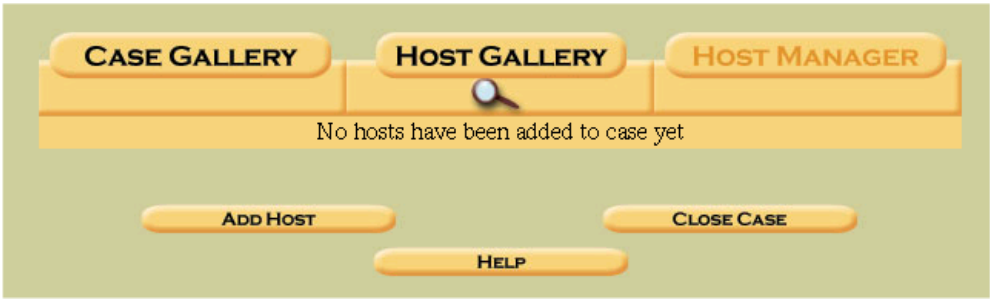
Name: _____ Student ID:_____



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.

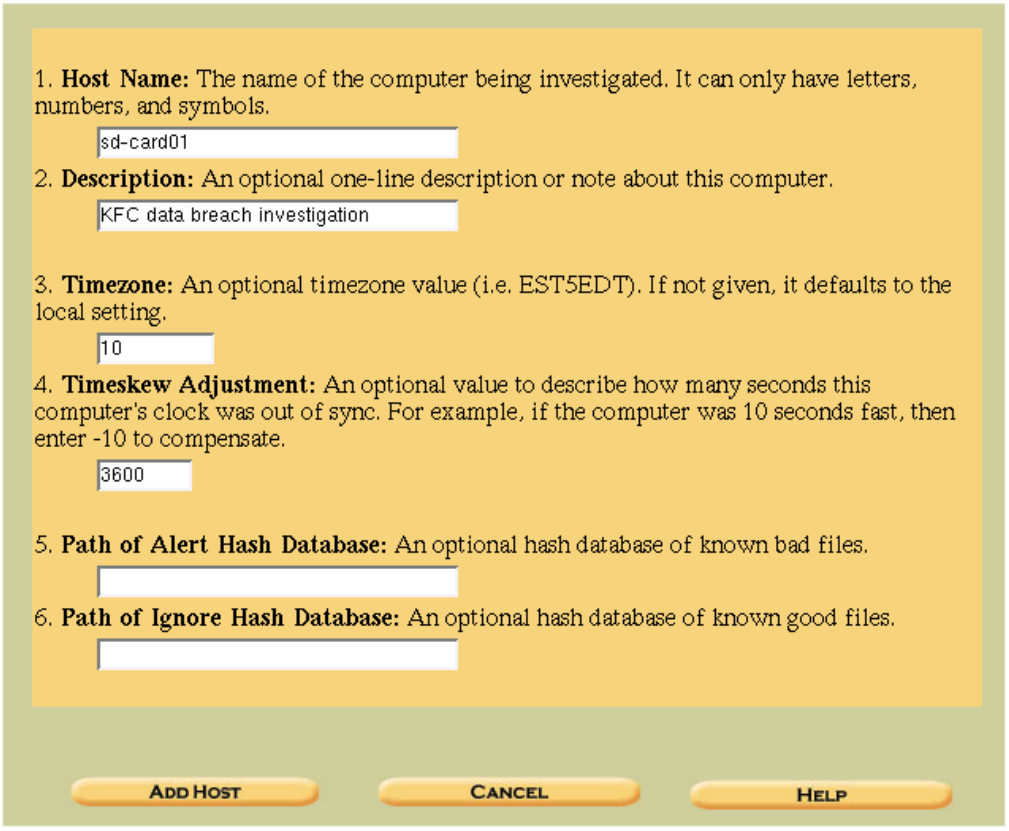
Note: many cases could appear here - select the one you have just created. (`OK`)



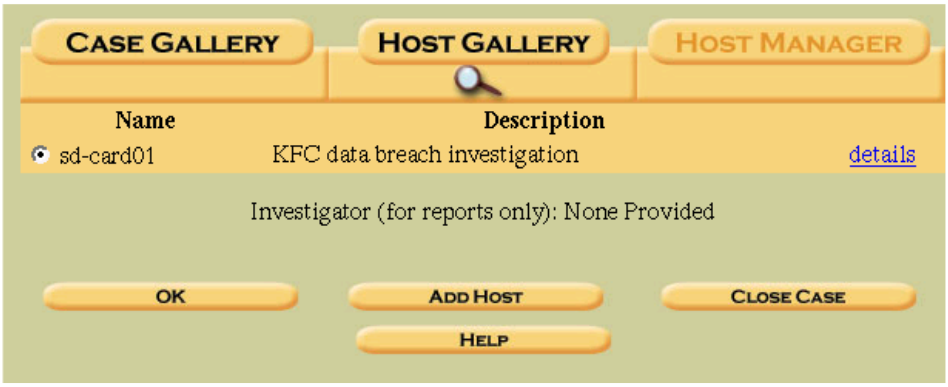
9. …Click `Add Host`

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

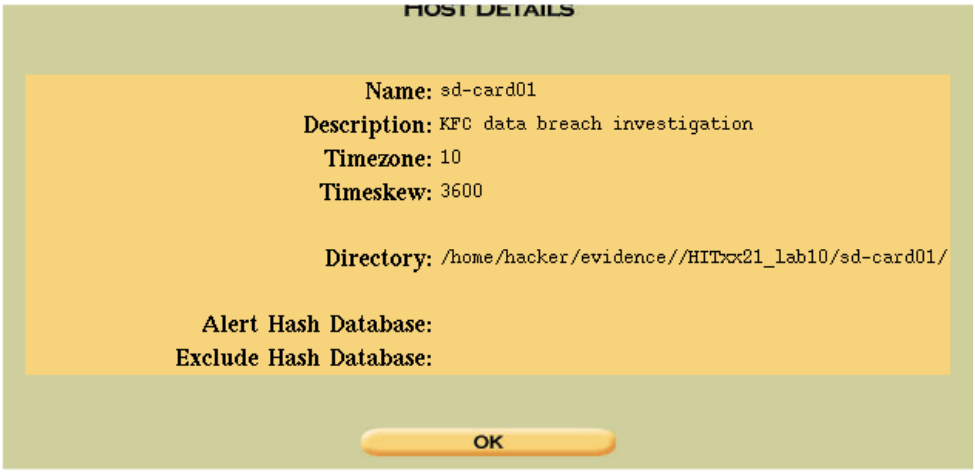
The data was collected during daylight saving time, so enter 3600 (1 hour in seconds) for the timeskew setting.



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



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

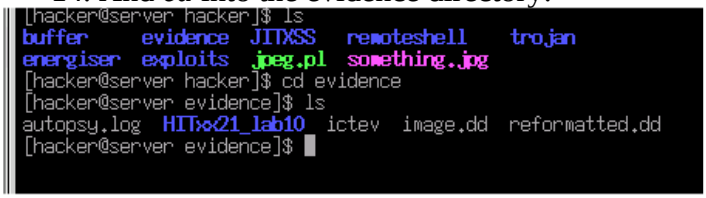


12. Click `OK` to load the *dd* file into the case:

13. Click `Add Image`

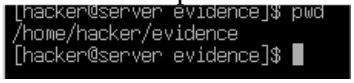
You will need the path to the disk image. To get this, open a console window 

14. And *cd* into the evidence directory:

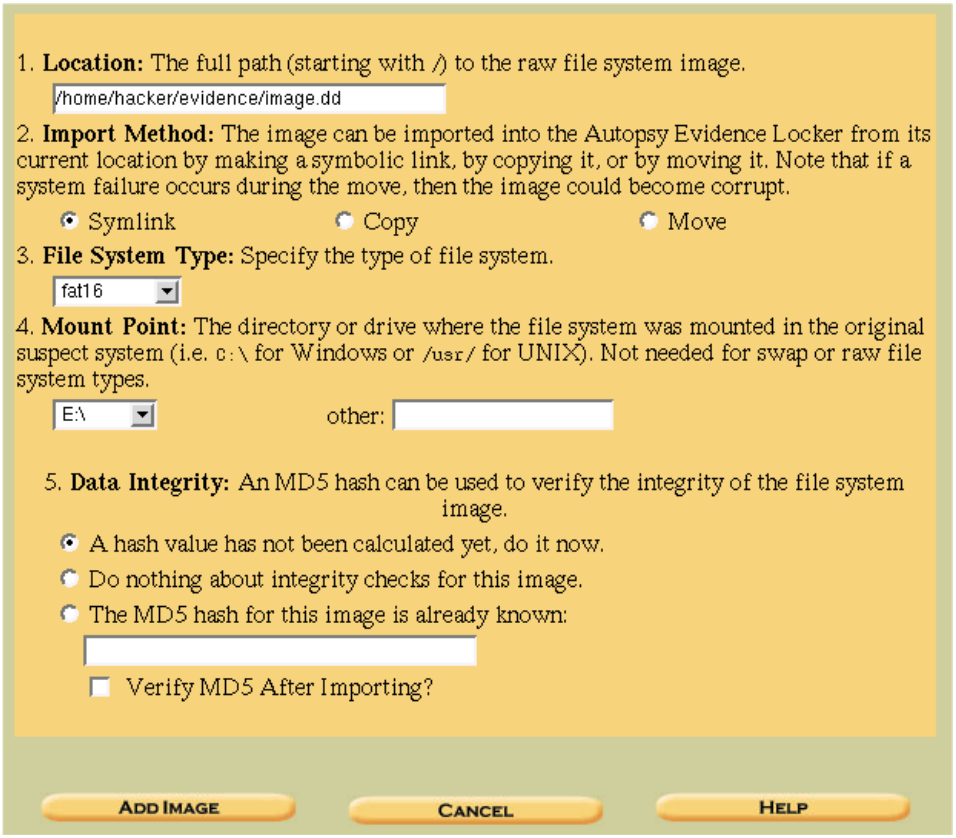


The disk image is called ***image.dd***

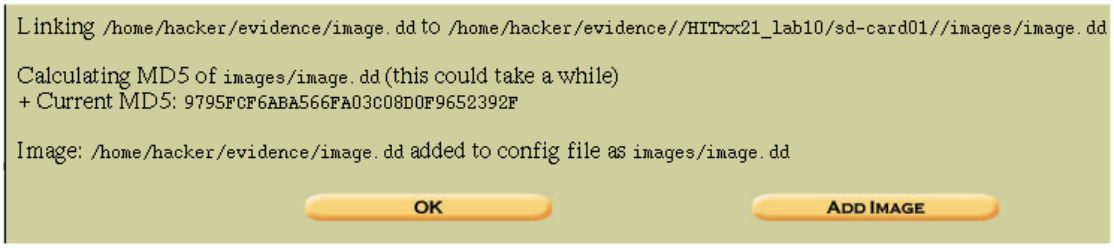
Note that the path is absolute – use *pwd* to get the path:



Name: _____ **Student ID:**_____



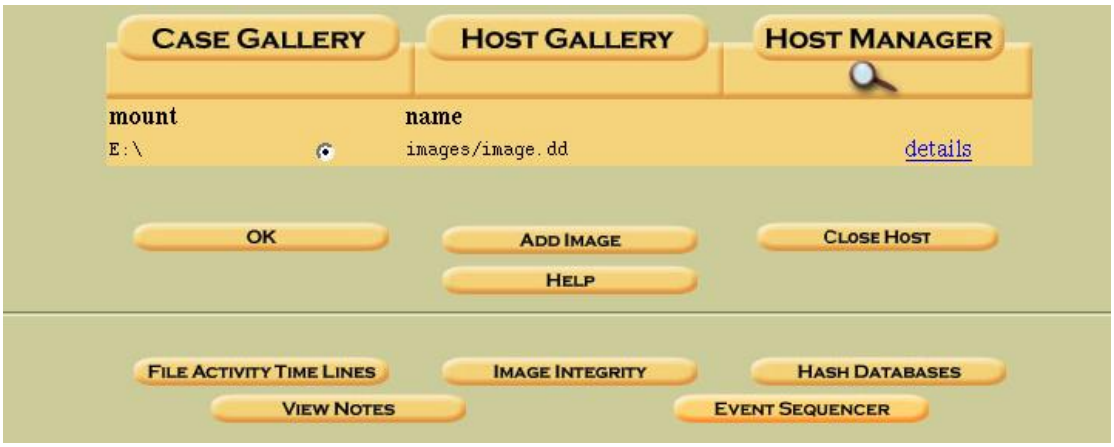
15. Fill in the form as above and click `Add Image`



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:_____

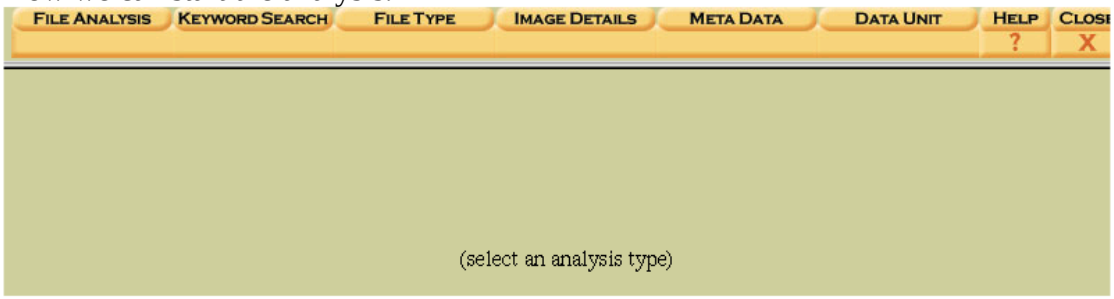


18. Click on `Details`

19. `Click "OK"` to return

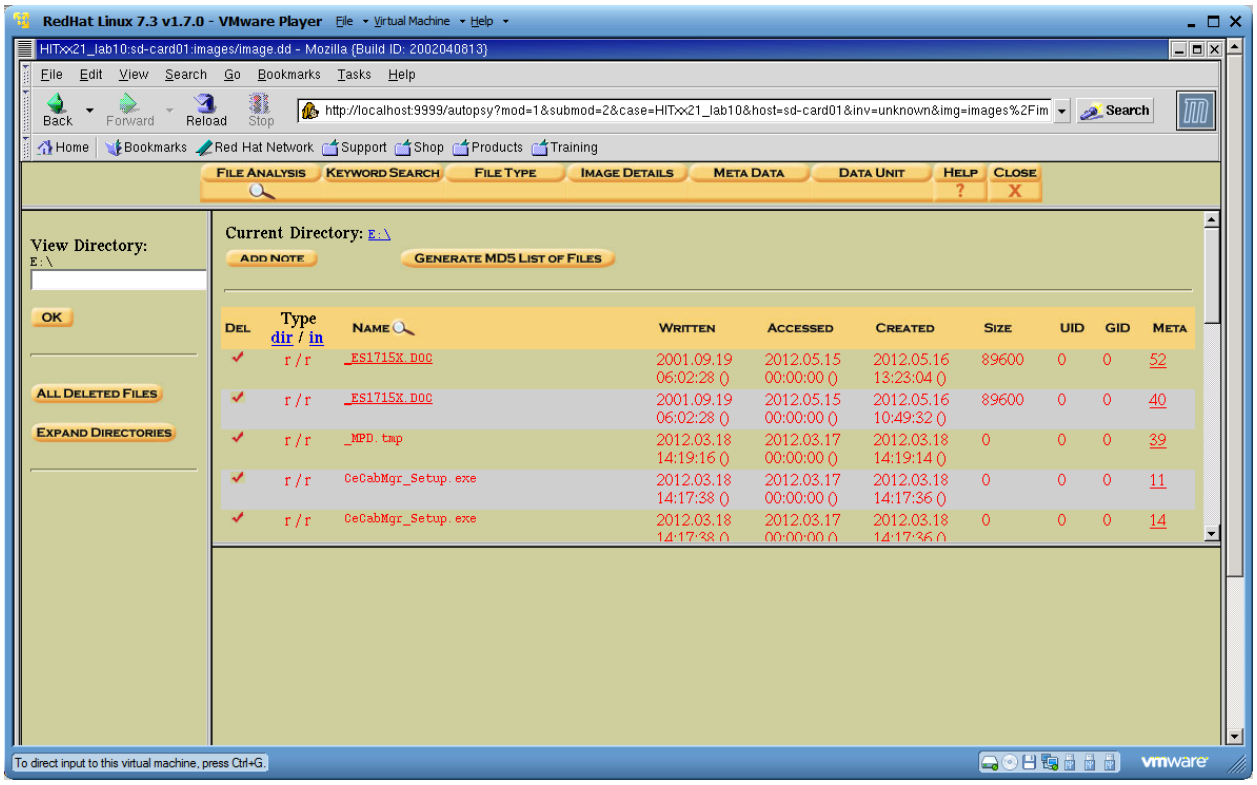
20. `Click "OK"` to continue…

Now we can start the analysis.



21. Click on FileAnalysis

Name: _____ Student ID:_____



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  HITx21_lab10  ictev  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)

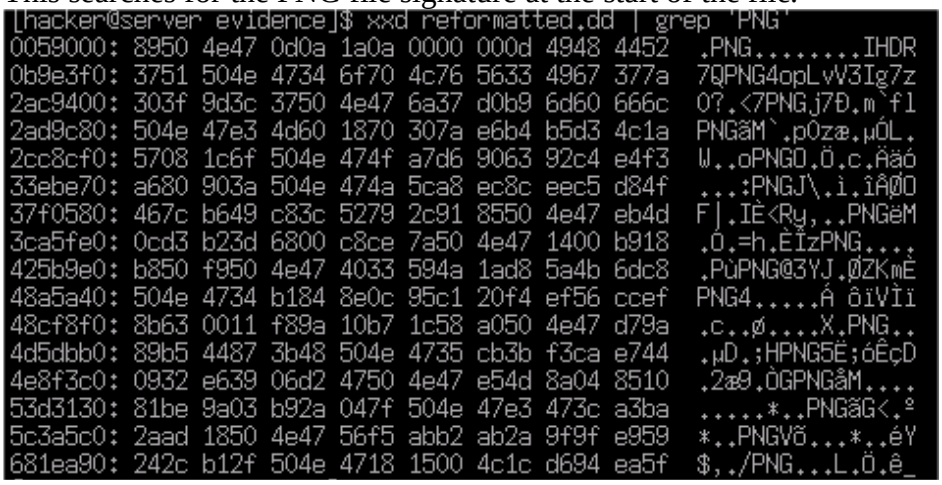
But the image is corrupted!

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.



Found at 0x0059000 = 364544 \\ (decimal)

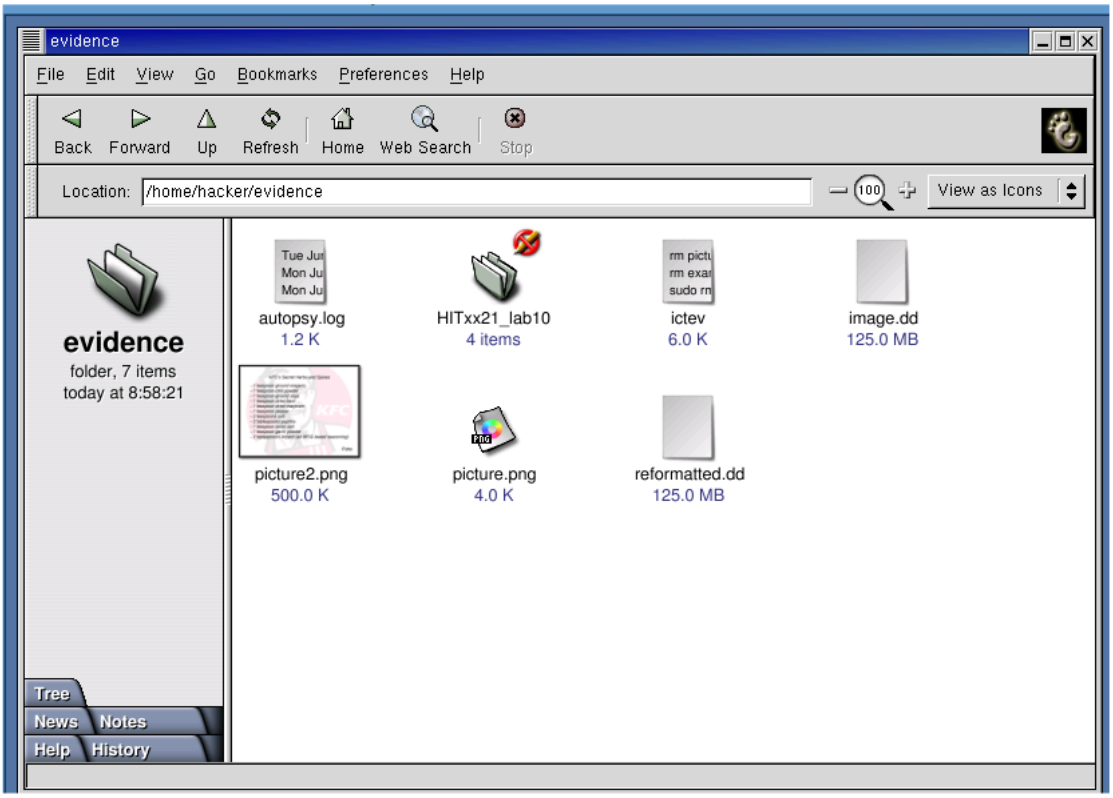
divide by 512 = 712 sectors

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

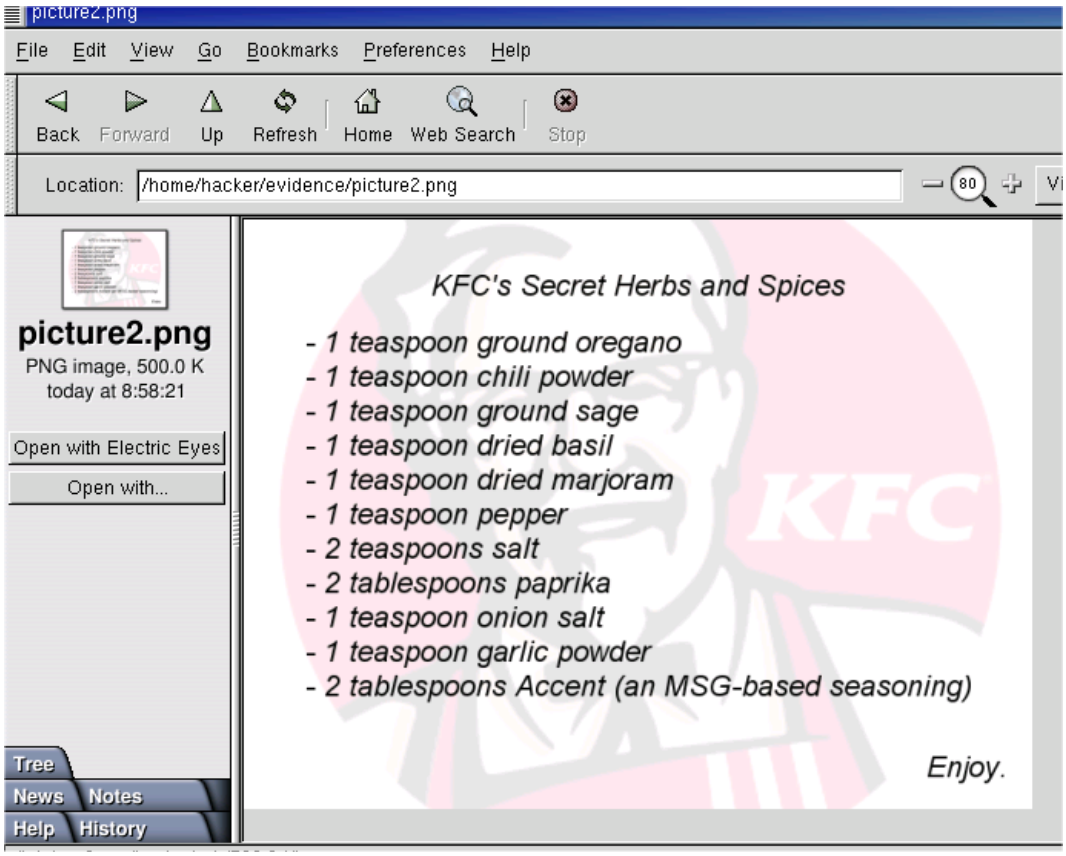
```
dd if=reformatted.dd of=picture2.png skip=712 bs=512
count=1000
```

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

Name: _____ Student ID:_____



Congratulations!



Name: _____ Student ID:_____

Have fun!

End of lab.