Digital forensics

To find the partitions and mount them

-fdisk -l hdd.dd → This will give the hard disk informations

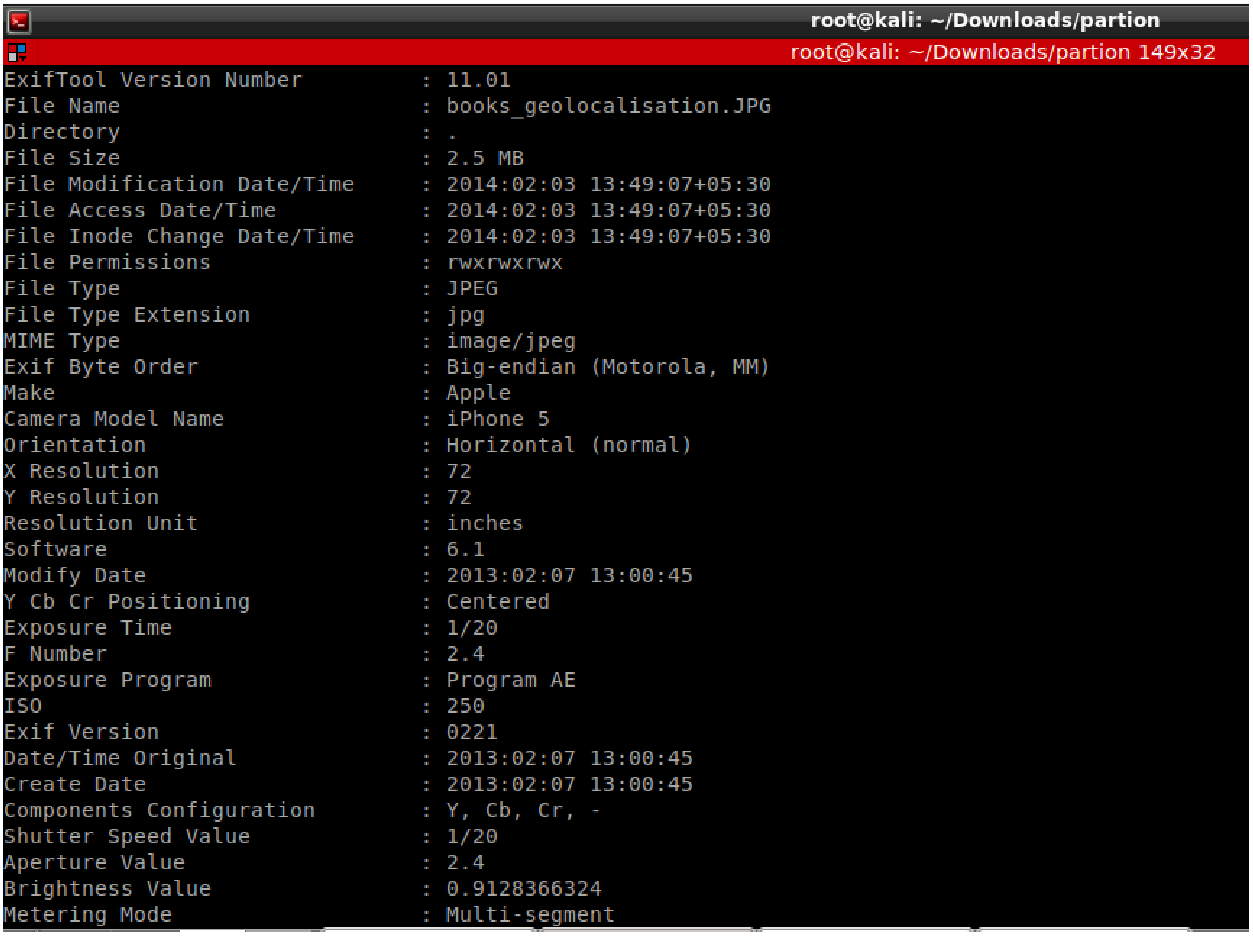
-mount -o ro,nonexec,loop,offset=$((sector*512)) hdd.dd(file_name) destination_directory

→ This is used to mount the hard disk.

-umount hdd.dd →for unmounting the hard disk

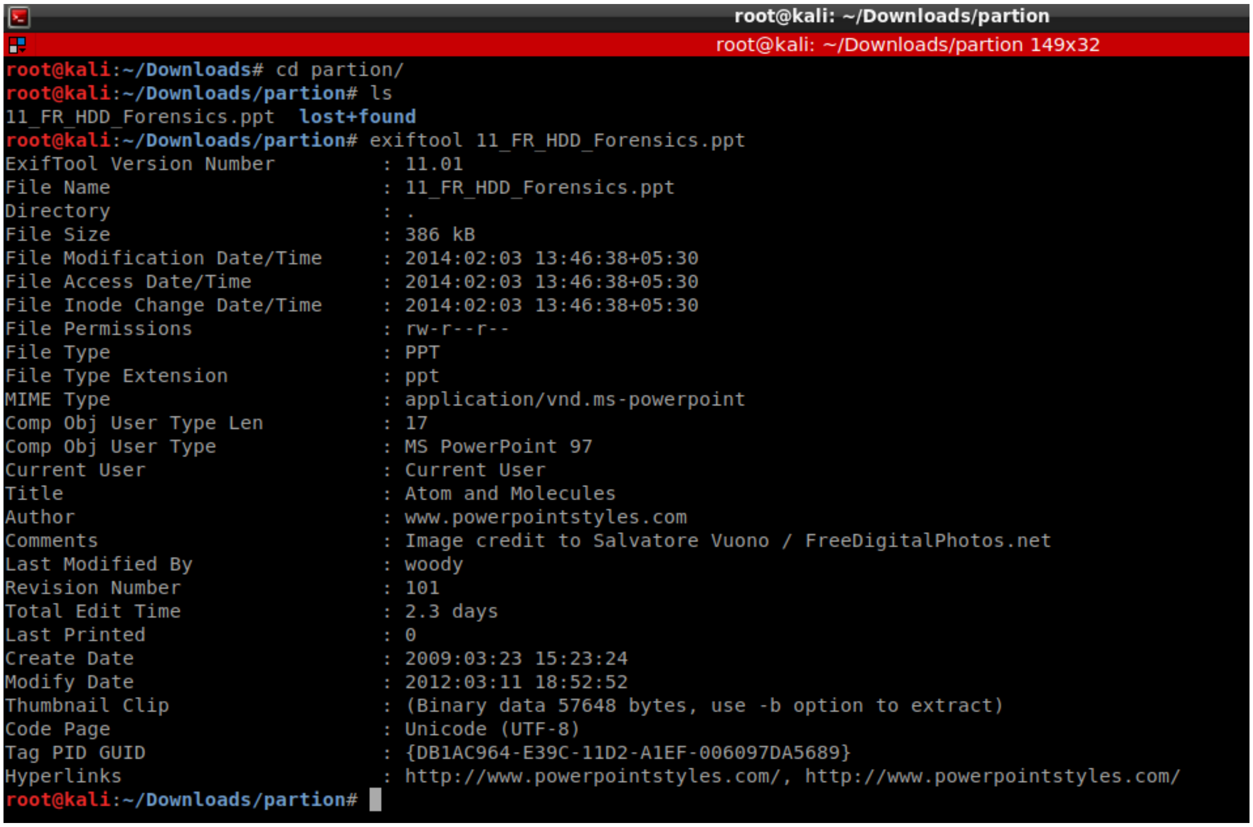
Metadata for picture and ppt

Metadata for both picture and ppt are been found by using the exiftool and Strings.


root@kali: ~/Downloads/partion
root@kali: ~/Downloads/partion 149x32

```
ExifTool Version Number         : 11.01
File Name                       : books_geolocalisation.JPG
Directory                       : .
File Size                       : 2.5 MB
File Modification Date/Time     : 2014:02:03 13:49:07+05:30
File Access Date/Time           : 2014:02:03 13:49:07+05:30
File Inode Change Date/Time     : 2014:02:03 13:49:07+05:30
File Permissions                : rwxrwxrwx
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : Apple
Camera Model Name               : iPhone 5
Orientation                     : Horizontal (normal)
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Software                        : 6.1
Modify Date                     : 2013:02:07 13:00:45
Y Cb Cr Positioning             : Centered
Exposure Time                   : 1/20
F Number                        : 2.4
Exposure Program                : Program AE
ISO                             : 250
Exif Version                    : 0221
Date/Time Original              : 2013:02:07 13:00:45
Create Date                     : 2013:02:07 13:00:45
Components Configuration        : Y, Cb, Cr, -
Shutter Speed Value             : 1/20
Aperture Value                  : 2.4
Brightness Value                : 0.9128366324
Metering Mode                   : Multi-segment
```

This tool gives the important information about the files like the time of creation, it's GPS, and so on.


root@kali: ~/Downloads/partion
root@kali: ~/Downloads/partion 149x32

```
root@kali:~/Downloads# cd partion/
root@kali:~/Downloads/partion# ls
11_FR_HDD_Forensics.ppt  lost+found
root@kali:~/Downloads/partion# exiftool 11_FR_HDD_Forensics.ppt
ExifTool Version Number         : 11.01
File Name                       : 11_FR_HDD_Forensics.ppt
Directory                       : .
File Size                       : 386 kB
File Modification Date/Time     : 2014:02:03 13:46:38+05:30
File Access Date/Time           : 2014:02:03 13:46:38+05:30
File Inode Change Date/Time     : 2014:02:03 13:46:38+05:30
File Permissions                : rw-r--r--
File Type                       : PPT
File Type Extension             : ppt
MIME Type                       : application/vnd.ms-powerpoint
Comp Obj User Type Len          : 17
Comp Obj User Type              : MS PowerPoint 97
Current User                    : Current User
Title                           : Atom and Molecules
Author                          : www.powerpointstyles.com
Comments                        : Image credit to Salvatore Vuono / FreeDigitalPhotos.net
Last Modified By                : woody
Revision Number                 : 101
Total Edit Time                 : 2.3 days
Last Printed                    : 0
Create Date                     : 2009:03:23 15:23:24
Modify Date                     : 2012:03:11 18:52:52
Thumbnail Clip                  : (Binary data 57648 bytes, use -b option to extract)
Code Page                       : Unicode (UTF-8)
Tag PID GUID                    : {DB1AC964-E39C-11D2-A1EF-006097DA5689}
Hyperlinks                      : http://www.powerpointstyles.com/, http://www.powerpointstyles.com/
root@kali:~/Downloads/partion#
```

Using the GPS information, the file can be located where it's been functioning.

Unknown deleted file

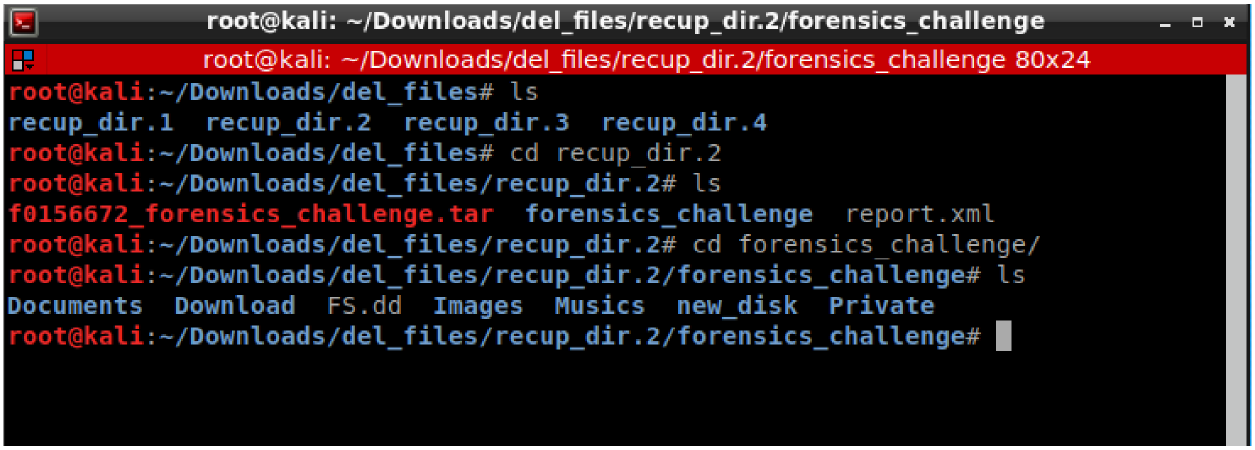
The unknown deleted files are being recovered using a photorec command. This is achieved by the following command:

Photorec /log /debug hdd.dd

-/log - Creates a log file.

-/debug – Adds debug Information

When this command is executed it takes to the photorec window where it will ask you to select the disk in which you have to find the lost files.



```
root@kali: ~/Downloads/del_files/recup_dir.2/forensics_challenge
root@kali: ~/Downloads/del_files/recup_dir.2/forensics_challenge 80x24
root@kali:~/Downloads/del_files# ls
recup_dir.1  recup_dir.2  recup_dir.3  recup_dir.4
root@kali:~/Downloads/del_files# cd recup_dir.2
root@kali:~/Downloads/del_files/recup_dir.2# ls
f0156672_forensics_challenge.tar  forensics_challenge  report.xml
root@kali:~/Downloads/del_files/recup_dir.2# cd forensics_challenge/
root@kali:~/Downloads/del_files/recup_dir.2/forensics_challenge# ls
Documents  Download  FS.dd  Images  Musics  new_disk  Private
root@kali:~/Downloads/del_files/recup_dir.2/forensics_challenge# 
```

Inside the photorec window the destination location(del_files) is fixed in which the lost files will be stored.

Files that are been discovered:

-Four Directories are been recovered.

-In which recup_dir.1 contains report.xml file.

-recup_dir.2 contains.tar.gz file when it’s unzipped forensics _challenge file was extracted.

-forensics_challenge contains:

-Documents - 03-icar-fractal.pdf, fractal.pdf, Fractal.pdf, fractales.pdf, fractals2.pdf, World_of_Fractal.pdf

-Download – trame.pcap

- FS.dd → when it’s passed to strings it gives a hash, google says it is for the flag for a challenge.
-Images - fractale.jpg, fractale2.jpg, fractale3.jpg, ………fractale11.jpg, jpg_NDH080408ak.jpg.
-Musics - miel-vie.mp3
-Private - priv.txt

//This every file has a hash which is used to clear a flag for a challenge.