**Homework 3 Shruti Soni**

**Title: Explanation of Inode lab and computer forensic foremost technic lab**

Topics To focus: Inode , foremost, partition , track, sector, foremost commands.

First of all, How data stores (Read and Write) in computer hard disk when user create any file.

1. What is inode

inodes represent files. Each inode contains a lot of metadata about each file, such as file size, owner, permissions, create/modify/access time, and pointers to the data blocks in each file. Since a file can contain a large number of data blocks, inodes use trees of pointers to point to data blocks in large files. (JL, 2007)

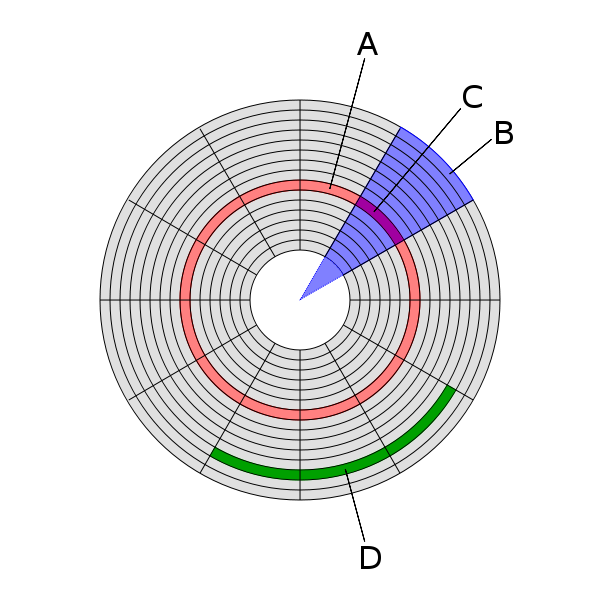
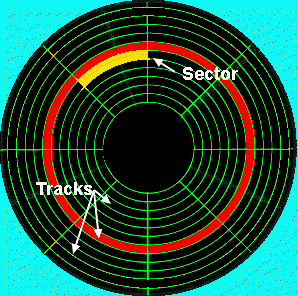
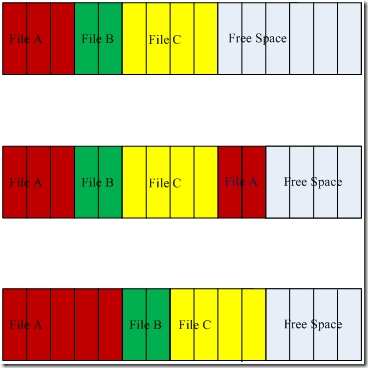
 

Figure 1: Disk structures:

1. Track
2. Geometrical sector
3. Track sector
4. [Cluster](https://en.wikipedia.org/wiki/Cluster_(file_system))

The platters inside a hard drive are structured to facilitate the storage and retrieval of data. Each platter is divided into concentric rings called “Tracks”. There are thousands of tracks on each platter. Each track is divided into sectors. A sector, as a rule, holds 512 bytes of data, this is usually the minimum quantity of information which is independently addressable for storage on a hard drive disk. Today, hard drive platters have thousands of sectors in a single track. (datarecoverylink, n.d.)



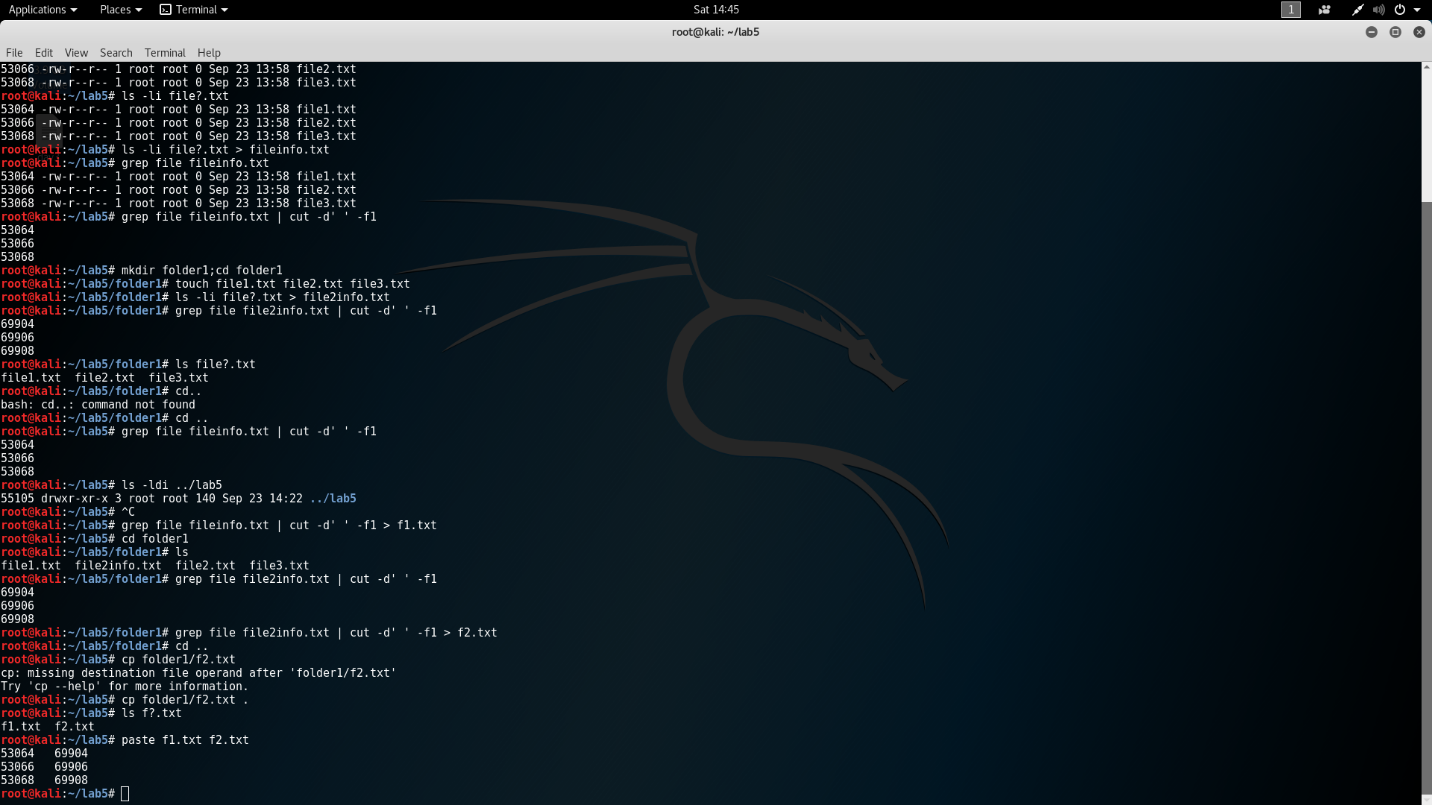
root@kali:~# whoami  
root  
root@kali:~# mkdir lab5;cd lab5 🡪 create directory , change directory and go on location of that folder

root@kali:~/lab5# touch file1.txt file2.txt file3.txt 🡪 touch command use to create file and if exist then modify it   
root@kali:~/lab5# ls file?.txt 🡪 retrieve the existed files list of files I that folder  
file1.txt  file2.txt  file3.txt  
root@kali:~/lab5# ls -li file?.txt 🡪 Retrieve files with the file index number and modification date time and read write mode  
53064 -rw-r--r-- 1 root root 0 Sep 23 13:58 file1.txt  
53066 -rw-r--r-- 1 root root 0 Sep 23 13:58 file2.txt  
53068 -rw-r--r-- 1 root root 0 Sep 23 13:58 file3.txt

root@kali:~/lab5# ls -li file?.txt > fileinfo.txt 🡪 copy and paste all listed files info in fileinfo.txt file  
root@kali:~/lab5# grep file fileinfo.txt 🡪 search file with name fileinfo that is it exist or not   
53064 -rw-r--r-- 1 root root 0 Sep 23 13:58 file1.txt  
53066 -rw-r--r-- 1 root root 0 Sep 23 13:58 file2.txt  
53068 -rw-r--r-- 1 root root 0 Sep 23 13:58 file3.txt  
root@kali:~/lab5# grep file fileinfo.txt | cut -d' ' -f1 🡪use command to retrieve specific field information. Here we are retrieving field1 with indexes of files.  
53064  
53066  
53068

root@kali:~/lab5# mkdir folder1;cd folder1  
root@kali:~/lab5/folder1# touch file1.txt file2.txt file3.txt  
root@kali:~/lab5/folder1# ls -li file?.txt > file2info.txt  
root@kali:~/lab5/folder1# grep file file2info.txt | cut -d' ' -f1  
69904  
69906  
69908

Lab 5: Screenshot of commands In terminal of Kali Linux



Lab 6: Computer Forensic Foremost Lab

First if all what is foremost : [foremost](http://foremost.sourceforge.net/) is a forensics application to recover files based on their headers, footers, and internal data structures (Timme, n.d.).

Following is the step by step explanation how to recover deleted data using foremost functionality

Using Kali linux, there is a inbuilt application foremost. If there is not exist then install using following command

>>apt -get install foremost

>>ls /mnt/win

>> foremost -t png -i /dev/sda3

It will retrieve all the png from the usb which already deleted before.

Another way to do the same process :

Some important foremost command line arguments.

* -i  :- partition/image to recover
* -o :- location to store recovered files.
* -t  :- built in file filter options.  you can give multiple filters by separating using commas. (e.g: for jpg and pdf: -t jpg,pdf )
* -q :- quick mode (Aravinda, 2013).
  1. First make an empty writable directory to save recover files in a partition other than that you are going to recover. ( /recovery/data/ )
  2. Then run foremost.  I am going to recover my home partition ( /dev/sda3).
  3. To find out how is the sda3 (Borge, 2014) 🡪 apply command >>df -h

>> foremost -t jpg -i /dev/sda5 -o /recovery/data

# References

Aravinda, H. (2013, May 25). *Retriving data from daleted file*. Retrieved from http://tryitnw.blogspot.com/2013/05/recovering-your-deleted-files-using.html

Borge, A. (2014, May 23). Retrieved from https://alexandreborgesbrazil.files.wordpress.com/2014/05/recoveryourfilesforemost3.pdf

*datarecoverylink*. (n.d.). Retrieved from A Basic Understanding of Tracks & Sectors: http://www.datarecoverylink.com/understanding-tracks-and-sectors/

JL. (2007, Feb 28). Retrieved from http://cseweb.ucsd.edu/~j2lau/cs120/week8.html

Timme, F. (n.d.). *howtoforge*. Retrieved from https://www.howtoforge.com/recover-deleted-files-with-foremost

Extra Source :

<http://linuxcommand.org/lc3_man_pages/ls1.html>