CSEC 730 ADVANCED FORENSICS

Name : Shriram Karpoora Sundara Pandian (KP)

Title : Lab 1

Part 1

1.

Question 1 : How many partitions do your SIFT VM's */dev/sda* have? What is the offset of the starting sector for the "Linux" partition? Show the commands and screenshots.

Command : sudo fdisk -l /dev/sda

```
sansforensics@siftworkstation: ~
$ sudo fdisk -l /dev/sda
Disk /dev/sda: 488.29 GiB, 524288000000 bytes, 1024000000 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x60ccc656

Device     Boot   Start        End    Sectors   Size Id Type
/dev/sda1          2048    3999743    3997696   1.9G 82 Linux swap / Solaris
/dev/sda2  *    3999744 1023997951 1019998208 486.4G 83 Linux
```

It has two partitions (SDA1 and SDA2)

Offset of Linux is (3999744)

Question 2 : Which file system does this “Linux” partition use? What is the block size of this “Linux” partition? Show the commands and screenshots.

Command : sudo fsstat /dev/sda2 | less

-s = Display file information even the file is empty.

```
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: Ext4
Volume Name:
Volume ID: 4aa4140eb02fc785ce45cb0e9e329780

Last Written at: 2024-02-14 20:46:22 (UTC)
Last Checked at: 2021-06-24 20:58:25 (UTC)

Last Mounted at: 2024-02-14 20:46:27 (UTC)
Unmounted properly
Last mounted on: /

Source OS: Linux
Dynamic Structure
Compat Features: Journal, Ext Attributes, Resize Inode, Dir Index
InCompat Features: Filetype, Needs Recovery, Extents, 64bit, Flexible Block Gr
oups,
Read Only Compat Features: Sparse Super, Large File, Huge File, Extra Inode Si
ze
```

The file system the linux uses is ext4 filesystem.

Command : sudo dumpe2fs -h /dev/sda2

-h = human readable form

Below is the command to get superblock information.

```
sansforensics@siftworkstation: ~
$ sudo dumpe2fs -h /dev/sda2
dumpe2fs 1.45.5 (07-Jan-2020)
Filesystem volume name:   <none>
Last mounted on:          /
Filesystem UUID:          8097329e-0ecb-45ce-85c7-2fb00e14a44a
Filesystem magic number:  0xEF53
Filesystem revision #:    1 (dynamic)
Filesystem features:      has_journal ext_attr resize_inode dir_index filetype n
eeds_recovery extent 64bit flex_bg sparse_super large_file huge_file dir_nlink e
xtra_isize metadata_csum
Filesystem flags:         signed_directory_hash
Default mount options:    user_xattr acl
Filesystem state:         clean
Errors behavior:          Continue
Filesystem OS type:       Linux
Inode count:              31875072
Block count:              127499776
Reserved block count:     6374988
Free blocks:              123080421
Free inodes:              31627112
First block:              0
Block size:               4096
Fragment size:            4096
Group descriptor size:    64
Reserved GDT blocks:      1024
Blocks per group:         32768
Fragments per group:      32768
Inodes per group:         8192
Inode blocks per group:   512
Flex block group size:    16
Filesystem created:       Thu Jun 24 20:58:25 2021
Last mount time:          Thu Feb  8 17:56:19 2024
Last write time:          Thu Feb  8 17:56:11 2024
Mount count:              4
```

```
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ sudo dumpe2fs /dev/sda2 | grep -i 'block size'
dumpe2fs 1.45.5 (07-Jan-2020)
Block size:               4096
```

The block size of the sda2 which has linux is 4096.

2.

Question 3 : 1. The image “Linux_Financial_Case.001” contains one partition. In able to analyze this image, you have to first find the offset of the starting sector for the partition. What is the command along with the appropriate options you used?

Command : sudo fdisk -l Linux_Financial_Case.001

```
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ sudo fdisk -l Linux_Financial_Case.001
Disk Linux_Financial_Case.001: 961 MiB, 1007681536 bytes, 1968128 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x65529191

Device                     Boot Start     End Sectors  Size Id Type
Linux_Financial_Case.001p1       2048 1968127 1966080  960M 83 Linux
```

The offset for the starting sector is 2048.

3. Find the image's file system information (hint: you have to provide the offset you got from step 2.)

Question 4 : What is the command along with the appropriate options you used to find the file system?
Command : sudo fsstat -o 2048 Linux_Financial_Case.001

```
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ sudo fsstat -o 2048 Linux_Financial_Case.001
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: Ext2
Volume Name: ipar-usb
Volume ID: 2564987b4e5af88f454919f10de7fe42

Last Written at: 2015-11-06 17:49:09 (UTC)
Last Checked at: 2015-11-06 17:05:30 (UTC)

Last Mounted at: 2015-11-06 17:49:09 (UTC)
Unmounted Improperly
Last mounted on: /media/ipar/ipar-usb1

Source OS: Linux
Dynamic Structure
Compat Features: Ext Attributes, Resize Inode, Dir Index
InCompat Features: Filetype,
Read Only Compat Features: Sparse Super, Large File,

METADATA INFORMATION
--------------------------------------------
Inode Range: 1 - 61441
Root Directory: 2
Free Inodes: 61426

CONTENT INFORMATION
--------------------------------------------
Block Range: 0 - 245759
Block Size: 4096
Free Blocks: 241593

BLOCK GROUP INFORMATION
--------------------------------------------
Number of Block Groups: 8
Inodes per group: 7680
Blocks per group: 32768
```

Question 5. What type of file system is the image used?

The image is using ext2 file system type, from the above screenshot.

Question 6. In what scenarios, you do NOT have to use the offset option –o for a sleuthkit command?

The reason to not use the offset option :

- If the image has more than one partition.
- If the image offset starts with 0.
- If we are going to analyze the whole image instead of a particular portion.

Question 7. Provide the options of *mount* you will run to mount the Linux_Financial_Case.001 image's partition for forensics investigation? (Show a screenshot of the mounted filesystem)

-o - To pass (comma) based instructions.

Ro - read only

Loop - For mounting the image

Offset - To mention the partition information

```
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ sudo mount -o ro,loop,offset=$((512*2048)) Linux_Financial_Case.001 /mnt/evi
dence
```

```
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ cd /mnt/evidence
sansforensics@siftworkstation: /mnt/evidence
$ ls
Frank  Mark
```

Inside the Mark directory we can see the xls file with the following information.

```
sansforensics@siftworkstation: /mnt/evidence/Mark/Finance_Confidential
$ ls
Earning.xls
sansforensics@siftworkstation: /mnt/evidence/Mark/Finance_Confidential
$ cat Earning.xls


Financial Statement 2014-15

Kericu Inc.
```

4. Use *fls* to list the deleted files and directories, as a mactime body (-m), and save the file as *flsBody*.

Question 8. What is the command along with appropriate options you used?

Command : fls -o 2048 -d -m "/" lfc.dd>flsBody

-o = offset

-d = Only deleted files are listed

-m = Information based on mactime "/" mounting directory

```
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ fls -o 2048 -d -m "/" lfc.dd>flsBody
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ ls
flsBody  lfc.dd  Linux_Financial_Case.001  __MACOSX
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ cat flsBody
0|/Untitled Folder (deleted-realloc)|7681|d/drwxrwxr-x|2002|2002|4096|1447437530
|1446836360|1446836360|0
0|/Roger (deleted-realloc)|7681|d/drwxrwxr-x|2002|2002|4096|1447437530|144683636
0|1446836360|0
0|/.Trash-1000 (deleted)|38401|d/drwx------|1000|1000|0|1447436689|1447436851|14
47436851|0
0|/Untitled Folder 2 (deleted-realloc)|23041|d/drwxrwxr-x|1001|1001|4096|1447958
788|1446834161|1446835253|0
```

5. Use Sleuthkit's *mactime* to create a timeline of *flsBody*. Save the timeline in a file called *flsMactime* and examine the timeline.

Question 9. What is the command along with the appropriate options you used? Include a screenshot of a part of the content of *flsMactime.*

```
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ mactime -b flsBody -z EST5EDT -d   > flsMactime1
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ cat flsMactime1
Date,Size,Type,Mode,UID,GID,Meta,File Name
Xxx Xxx 00 0000 00:00:00,4096,...b,d/drwxrwxr-x,1001,1001,23041,"/Untitled Folde
r 2 (deleted-realloc)"
Xxx Xxx 00 0000 00:00:00,0,...b,d/drwx------,1000,1000,38401,"/.Trash-1000 (dele
ted)"
Xxx Xxx 00 0000 00:00:00,4096,...b,d/drwxrwxr-x,2002,2002,7681,"/Roger (deleted-
realloc)"
Xxx Xxx 00 0000 00:00:00,4096,...b,d/drwxrwxr-x,2002,2002,7681,"/Untitled Folder
 (deleted-realloc)"
Fri Nov 06 2015 13:22:41,4096,m...,d/drwxrwxr-x,1001,1001,23041,"/Untitled Folde
r 2 (deleted-realloc)"
Fri Nov 06 2015 13:40:53,4096,..c.,d/drwxrwxr-x,1001,1001,23041,"/Untitled Folde
r 2 (deleted-realloc)"
Fri Nov 06 2015 13:59:20,4096,m.c.,d/drwxrwxr-x,2002,2002,7681,"/Roger (deleted-
realloc)"
Fri Nov 06 2015 13:59:20,4096,m.c.,d/drwxrwxr-x,2002,2002,7681,"/Untitled Folder
 (deleted-realloc)"
Fri Nov 13 2015 12:44:49,0,.a..,d/drwx------,1000,1000,38401,"/.Trash-1000 (dele
ted)"
Fri Nov 13 2015 12:47:31,0,m.c.,d/drwx------,1000,1000,38401,"/.Trash-1000 (dele
ted)"
Fri Nov 13 2015 12:58:50,4096,.a..,d/drwxrwxr-x,2002,2002,7681,"/Roger (deleted-
realloc)"
Fri Nov 13 2015 12:58:50,4096,.a..,d/drwxrwxr-x,2002,2002,7681,"/Untitled Folder
 (deleted-realloc)"
Thu Nov 19 2015 13:46:28,4096,.a..,d/drwxrwxr-x,1001,1001,23041,"/Untitled Folde
r 2 (deleted-realloc)"
```

Command : mactime -b flsBody -z EST5EDT -d > flsMactime1

-b - To determine the file or body you want to have a mactime

-z - To determine the timezone

-d - Comma limited format for better readability.

6. Use *ils* to list the inode information for all deleted files, as a mactime body (-m), and save the file as *ilsBody*.

Question 10. What is the command along with the appropriate options you used?

Command : sudo ils -o 2048 -r -m Linux_Financial_Case.001 > ilsBody

-o - To mention offset of the file

-r - Only removed files

-m - Include mactime

```
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ sudo ils -o 2048 -r -m Linux_Financial_Case.001 > ilsBody
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ cat ilsBody
md5|file|st_ino|st_ls|st_uid|st_gid|st_size|st_atime|st_mtime|st_ctime|st_crtime
0|<Linux_Financial_Case.001-dead-11>|11|-/drwx------|0|0|0|1447436689|1447436836
|1447436836|0
0|<Linux_Financial_Case.001-dead-7683>|7683|-/lrwxrwxrwx|1000|1000|57|1447437474
|1447437469|1447437505|0
0|<Linux_Financial_Case.001-dead-15361>|15361|-/drwx------|1000|1000|0|144743668
9|1447436851|1447436851|0
0|<Linux_Financial_Case.001-dead-15362>|15362|-/rrw-r--r--|1000|1000|0|144682986
9|1447436851|1447436851|0
0|<Linux_Financial_Case.001-dead-15363>|15363|-/rrw-r--r--|1000|1000|0|144682986
9|1447436851|1447436851|0
0|<Linux_Financial_Case.001-dead-15364>|15364|-/rrw-r--r--|1000|1000|0|144682986
9|1447436851|1447436851|0
0|<Linux_Financial_Case.001-dead-15365>|15365|-/rrw-r--r--|1000|1000|0|144682986
9|1447436851|1447436851|0
0|<Linux_Financial_Case.001-dead-30721>|30721|-/drwx------|1000|1000|0|144743668
9|1447436851|1447436851|0
0|<Linux_Financial_Case.001-dead-30722>|30722|-/rrw-r--r--|1000|1000|0|144682986
5|1447436851|1447436851|0
0|<Linux_Financial_Case.001-dead-30723>|30723|-/rrw-r--r--|1000|1000|0|144682986
5|1447436851|1447436851|0
0|<Linux_Financial_Case.001-dead-30724>|30724|-/rrw-r--r--|1000|1000|0|144682986
5|1447436851|1447436851|0
0|<Linux_Financial_Case.001-dead-38401>|38401|-/drwx------|1000|1000|0|144743668
9|1447436851|1447436851|0
0|<Linux_Financial_Case.001-dead-38402>|38402|-/drwx------|1000|1000|0|144743668
9|1447436851|1447436851|0
0|<Linux_Financial_Case.001-dead-38403>|38403|-/drwx------|1000|1000|0|144743596
```

7. Use Sleuthkit's *mactime* to create a timeline of *ilsBody*. Save the timeline in a file called *ilsMactime* and examine the timeline.

Question 11. What is the command along with appropriate options you used? Include a screenshot of a part of the content of *ilsMactime.*

Command : mactime -b ilsBody -z EST5EDT -d > ilsMactime1

-b - For passing the body

-z - For mentioning the timezone

-d - Comma format for better readability

```
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ mactime -b ilsBody -z EST5EDT -d   > ilsMactime1
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ cat ilsMactime1
```

```
Fri Nov 13 2015 12:32:46,0,.a..,-/drwx------,1000,1000,38403,"<Linux_Financial_Case.001-dead-38403>"
Fri Nov 13 2015 12:32:46,0,.a..,-/rrw-rw-r--,1000,1000,38405,"<Linux_Financial_Case.001-dead-38405>"
Fri Nov 13 2015 12:32:46,0,.a..,-/rrw-rw-r--,1000,1000,38406,"<Linux_Financial_Case.001-dead-38406>"
Fri Nov 13 2015 12:44:31,0,mac.,-/rrw-rw-r--,1000,1000,46083,"<Linux_Financial_Case.001-dead-46083>"
Fri Nov 13 2015 12:44:49,0,.a..,-/drwx------,0,0,11,"<Linux_Financial_Case.001-dead-11>"
Fri Nov 13 2015 12:44:49,0,.a..,-/drwx------,1000,1000,15361,"<Linux_Financial_Case.001-dead-15361>"
Fri Nov 13 2015 12:44:49,0,.a..,-/drwx------,1000,1000,30721,"<Linux_Financial_Case.001-dead-30721>"
Fri Nov 13 2015 12:44:49,0,.a..,-/drwx------,1000,1000,38401,"<Linux_Financial_Case.001-dead-38401>"
Fri Nov 13 2015 12:44:49,0,.a..,-/drwx------,1000,1000,38402,"<Linux_Financial_Case.001-dead-38402>"
Fri Nov 13 2015 12:47:16,0,m.c.,-/drwx------,0,0,11,"<Linux_Financial_Case.001-dead-11>"
Fri Nov 13 2015 12:47:31,0,m.c.,-/drwx------,1000,1000,15361,"<Linux_Financial_Case.001-dead-15361>"
Fri Nov 13 2015 12:47:31,0,m.c.,-/rrw-r--r--,1000,1000,15362,"<Linux_Financial_Case.001-dead-15362>"
Fri Nov 13 2015 12:47:31,0,m.c.,-/rrw-r--r--,1000,1000,15363,"<Linux_Financial_Case.001-dead-15363>"
Fri Nov 13 2015 12:47:31,0,m.c.,-/rrw-r--r--,1000,1000,15364,"<Linux_Financial_Case.001-dead-15364>"
Fri Nov 13 2015 12:47:31,0,m.c.,-/rrw-r--r--,1000,1000,15365,"<Linux_Financial_Case.001-dead-15365>"
Fri Nov 13 2015 12:47:31,0,m.c.,-/drwx------,1000,1000,30721,"<Linux_Financial_Case.001-dead-30721>"
Fri Nov 13 2015 12:47:31,0,m.c.,-/rrw-r--r--,1000,1000,30722,"<Linux_Financial_Case.001-dead-30722>"
Fri Nov 13 2015 12:47:31,0,m.c.,-/rrw-r--r--,1000,1000,30723,"<Linux_Financial_Case.001-dead-30723>"
Fri Nov 13 2015 12:47:31,0,m.c.,-/rrw-r--r--,1000,1000,30724,"<Linux_Financial_Case.001-dead-30724>"
Fri Nov 13 2015 12:47:31,0,m.c.,-/drwx------,1000,1000,38401,"<Linux_Financial_Case.001-dead-38401>"
Fri Nov 13 2015 12:47:31,0,m.c.,-/drwx------,1000,1000,38402,"<Linux_Financial_Case.001-dead-38402>"
Fri Nov 13 2015 12:47:31,0,m.c.,-/drwx------,1000,1000,38403,"<Linux_Financial_Case.001-dead-38403>"
Fri Nov 13 2015 12:47:31,0,m.c.,-/rrw-rw-r--,1000,1000,38405,"<Linux_Financial_Case.001-dead-38405>"
Fri Nov 13 2015 12:47:31,0,m.c.,-/rrw-rw-r--,1000,1000,38406,"<Linux_Financial_Case.001-dead-38406>"
Fri Nov 13 2015 12:57:49,57,m...,-/lrwxrwxrwx,1000,1000,7683,"<Linux_Financial_Case.001-dead-7683>"
Fri Nov 13 2015 12:57:54,57,.a..,-/lrwxrwxrwx,1000,1000,7683,"<Linux_Financial_Case.001-dead-7683>"
Fri Nov 13 2015 12:58:25,57,..c.,-/lrwxrwxrwx,1000,1000,7683,"<Linux_Financial_Case.001-dead-7683>"
```

8. Compare the number of entries from *ilsMactime* and from *flsMactime*.

Question 12. Do *ilsMactime* and *flsMactme* have the same number of entries? Explain your findings.

We can clearly see from the two screenshots above, one from ilsmactime and flsmactime, which shows ilsmactime has lot of entries and with full of inode information, whereas we can see the filenames and files which are deleted and most of them are reallocated, which shows along with the timeline of the files and inodes.

The main difference between them, we can clearly see that inode lists all the unallocated and allocated inodes, which i mean the inodes used for storing the blocks and inodes those are simply created. But in flsmactime, we can see only filenames and files that are human readable and created and accessed and deleted by human intervention, which makes the real difference.

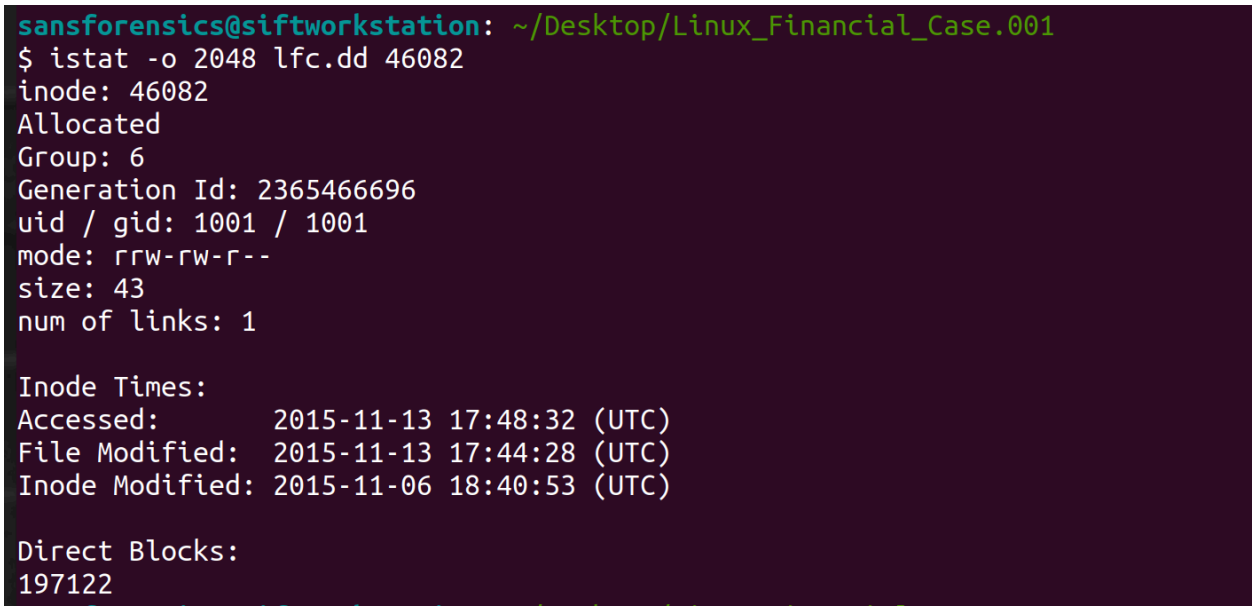
So in summary - ils lists all inodes which includes unnamed metadata/unused inodes, while fls just lists named file entries that were mapped to inodes.

9. use *istat* to view the details of the inode 46082.

Question 13. What is the command along with appropriate options you used? Include a screenshot.

Command : istat -o 2048 lfc.dd 46082

-o - defines the sector starting for making sure it is recording the proper file system.



10. use *icat* to dump out data from the inode 46082.

Question 14. What is the command along with appropriate options you used?

Command : icat -o 2048 Linux_Financial_Case.001 46082

```
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ icat -o 2048 Linux_Financial_Case.001 46082


Financial Statement 2014-15

Kericu Inc.
```

11. Use *ffind* to find the file's filename that has the inode 46082.

Question 15. What is the command along with appropriate options you used? Include a screenshot.

Command : ffind -o 2048 Linux_Financial_Case.001 46082

```
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ ffind -o 2048 Linux_Financial_Case.001 46082
/Mark/Finance_Confidential/Earning.xls
```

12. Use *blkcat* to dump out the data content of the datablock 197122

Question 16. What is the command along with the appropriate options you used?

Command : blkcat -o 2048 Linux_Financial_Case.001 197122 | more

```
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ blkcat -o 2048 Linux_Financial_Case.001 197122 | more


Financial Statement 2014-15

Kericu Inc.
```

Question 17. If a file with the inode 100 uses two block addresses, *block 1000* and *block 1001*, will “icat -f ext2 image 100” dump out the same content as the command “blkcat –f ext2 image 1000”? Explain your answer.

No, the information dumped by icat and blkcat are different because of their position in the image, what i mean is icat will show the information which is stored in the inode, for example, the inode 100 has two blocks in it which is 1000 and 1001, so it shows the content of block 1000 and 1001. Whereas, blkcat only shows information about the particular block, so here if you cat the block 1000 it will only show the information of the block 1000, not 1001 which is missed here. So the content of inode and the particular block will not be the same. There is a possibility that they could be the same, only when the inode has only one data block, then they will be the same.

13. Use *ifind* to find the inode number that one of its correspondent data blocks is 197122.

Question 18. What is the command along with appropriate options you used? Also provide a case scenario that shows the usefulness of *ifind*.

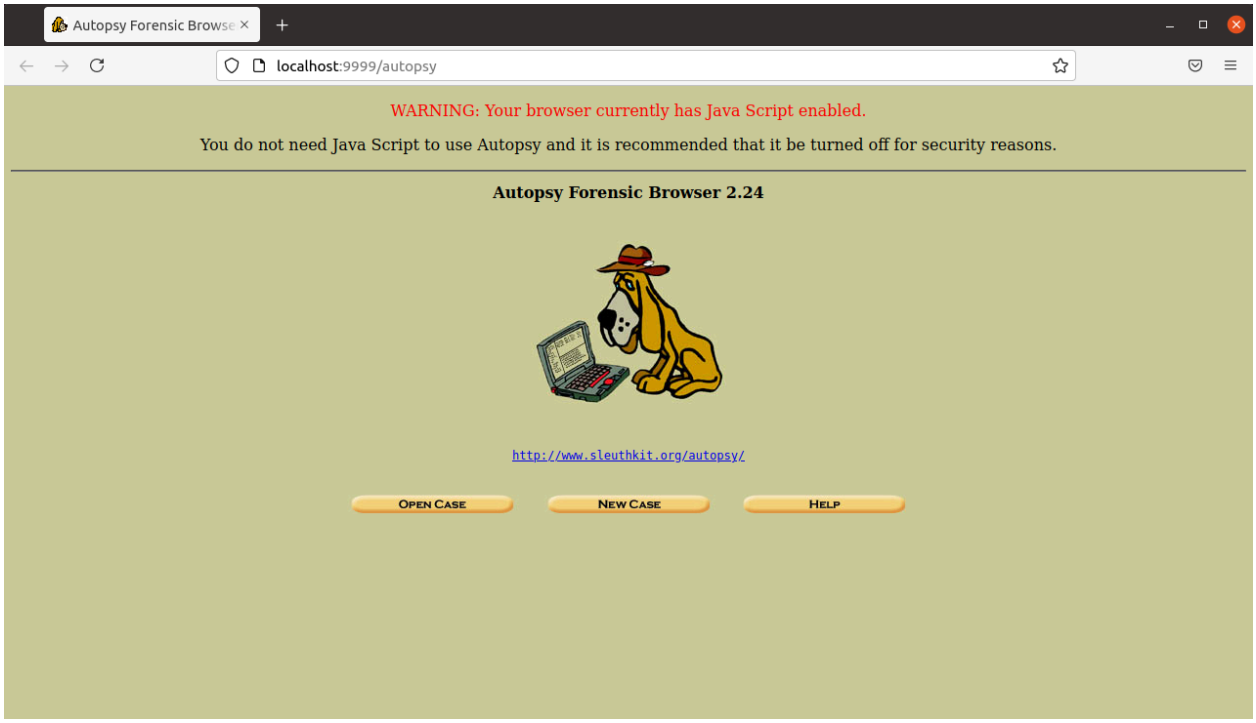
Command : ifind -o 2048 -d 197122 Linux_Financial_Case.001

-o - offset of the file

-d - Datablock number

```
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ ifind -o 2048 -d 197122 Linux_Financial_Case.001
46082
```

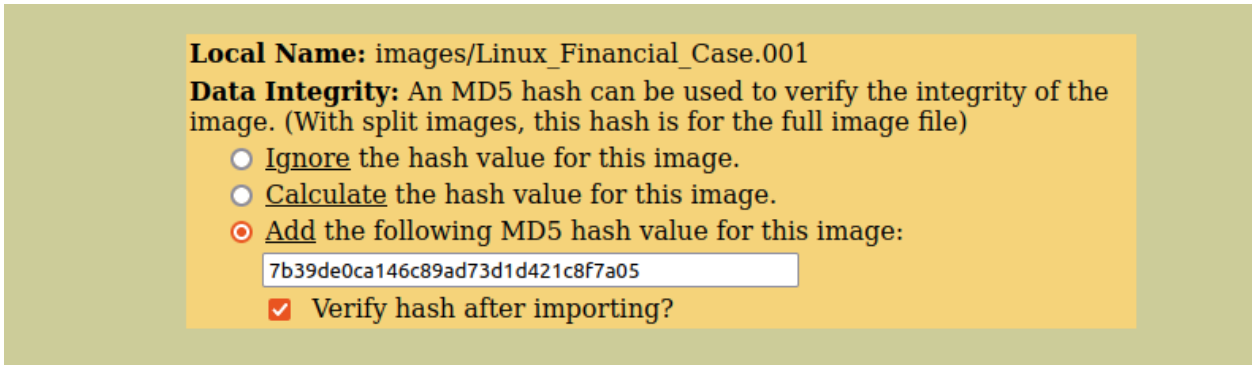
Part 2 : Autopsy



Question 1: Which option did you choose and why?

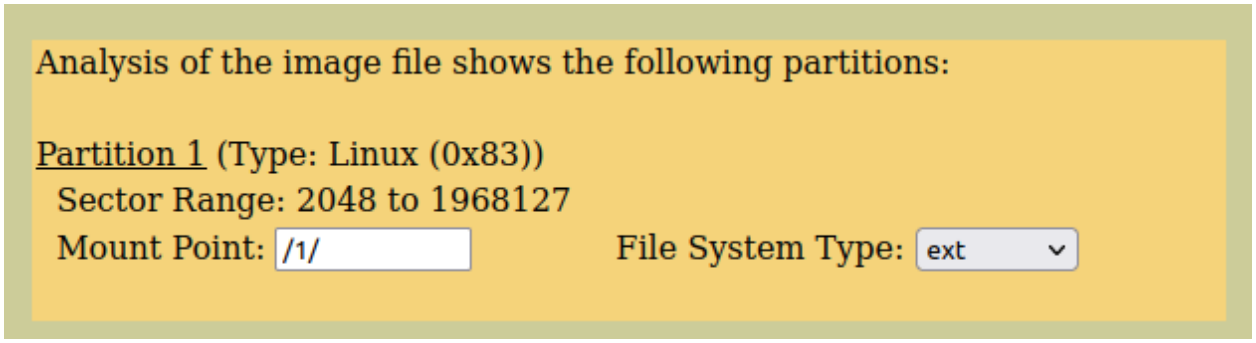
```
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ md5sum Linux_Financial_Case.001
7b39de0ca146c89ad73d1d421c8f7a05  Linux_Financial_Case.001
```

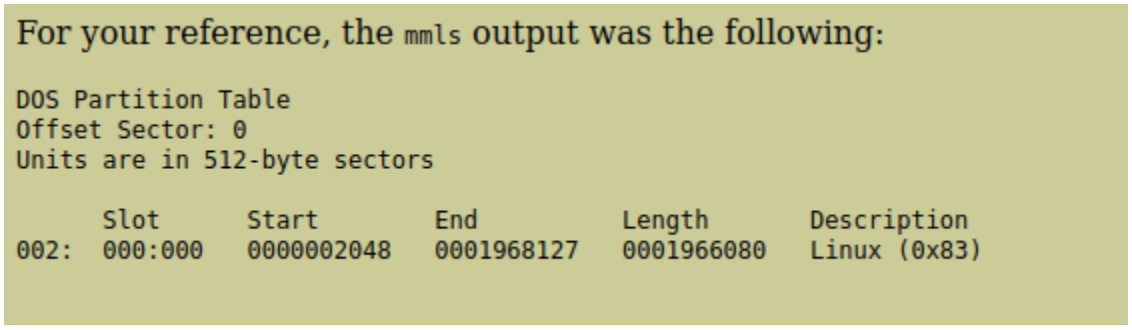
I first Calculated the md5hash of the .001 file



So I copied it here to verify after importing for ensuring that nothing changed in this image while importing.

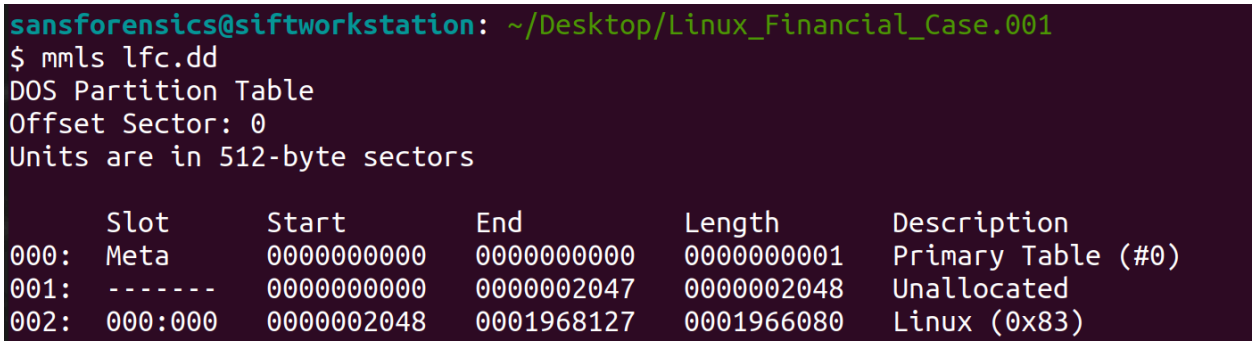
Autopsy identifies the partition and the file system type of this partition.





Question 2: Which Sleuthkit tool does Autopsy use to display the partition table information?

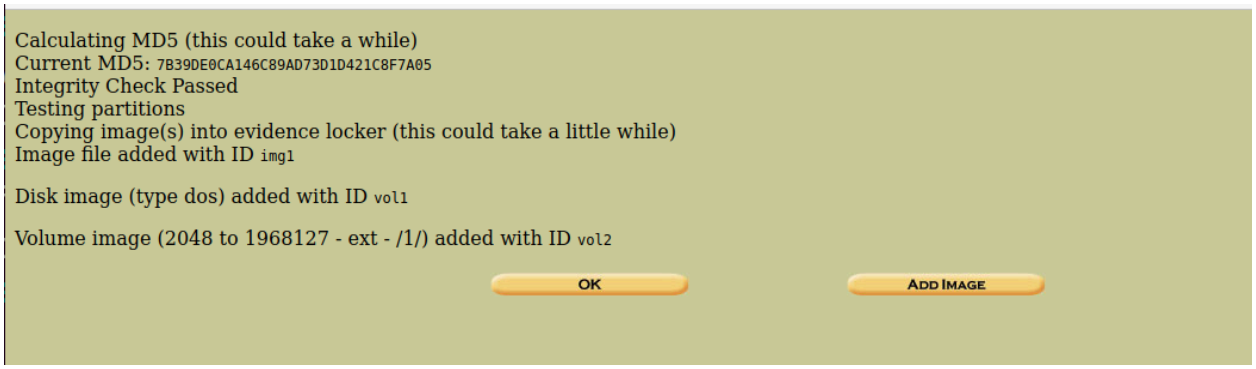
We can see that above table and below one are same. So it uses mmls to display the partition table information.

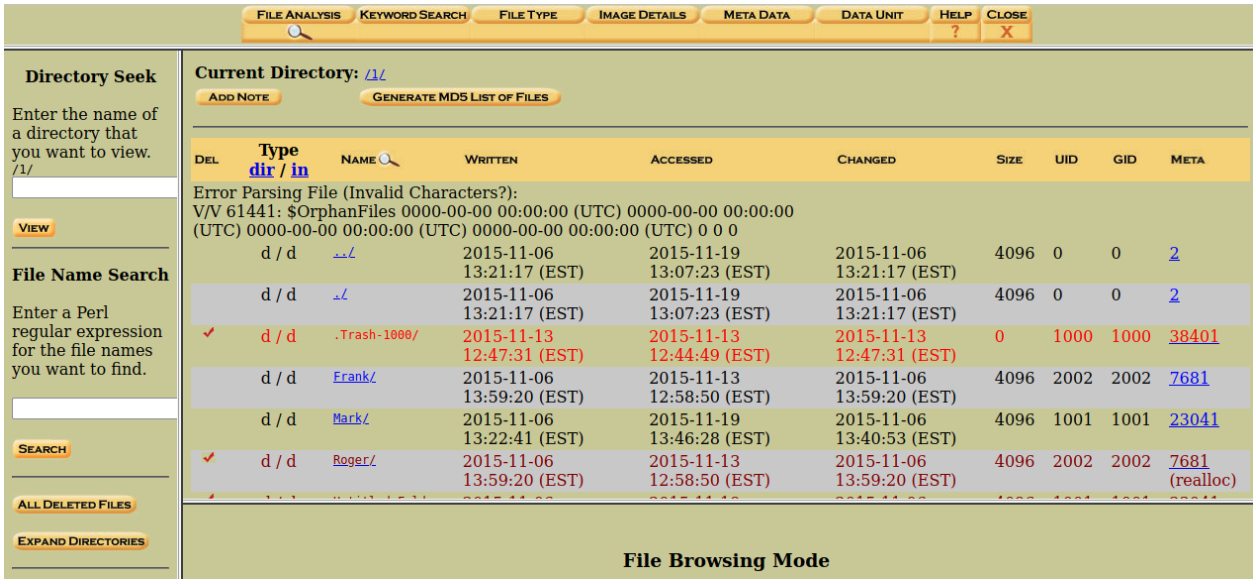


Question 3: Which Sleuthkit tool does Autopsy use to determine the file system type of this partition?

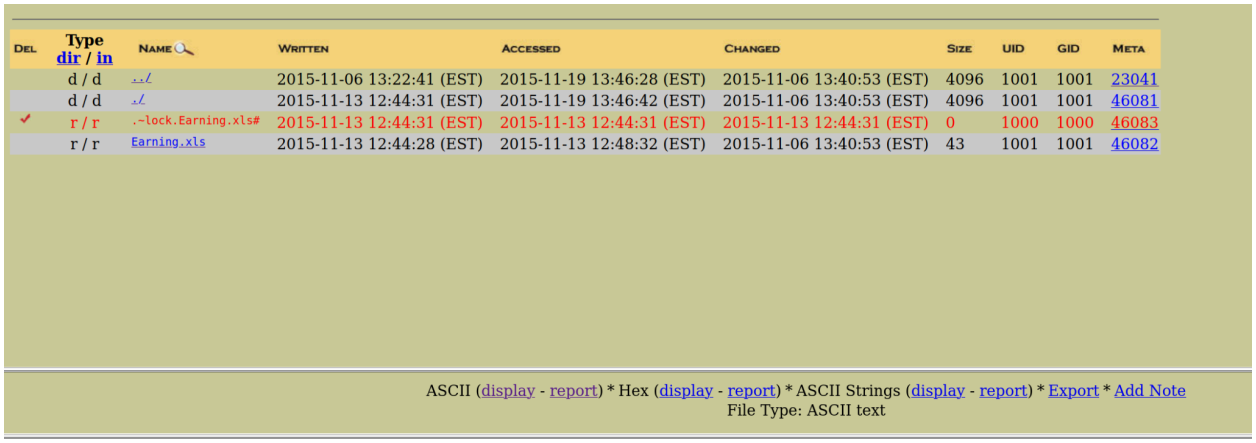
It will use the fsstat tool to deter the file system type which will show exactly what file system type the partition has.

Below are the step by step procedures I did to save up my work for future reference.





ASCII (display)



Del	Type dir / in	Name	Written	Accessed	Changed	Size	UID	GID	Meta
	d / d	../	2015-11-06 13:22:41 (EST)	2015-11-19 13:46:28 (EST)	2015-11-06 13:40:53 (EST)	4096	1001	1001	23041
	d / d	./	2015-11-13 12:44:31 (EST)	2015-11-19 13:46:42 (EST)	2015-11-06 13:40:53 (EST)	4096	1001	1001	46081
✔	r / r	.~lock.Earning.xls#	2015-11-13 12:44:31 (EST)	2015-11-13 12:44:31 (EST)	2015-11-13 12:44:31 (EST)	0	1000	1000	46083
	r / r	Earning.xls	2015-11-13 12:44:28 (EST)	2015-11-13 12:48:32 (EST)	2015-11-06 13:40:53 (EST)	43	1001	1001	46082

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note
File Type: ASCII text

Contents Of File: /1/Mark/Finance_Confidential/Earning.xls

Financial Statement 2014-15

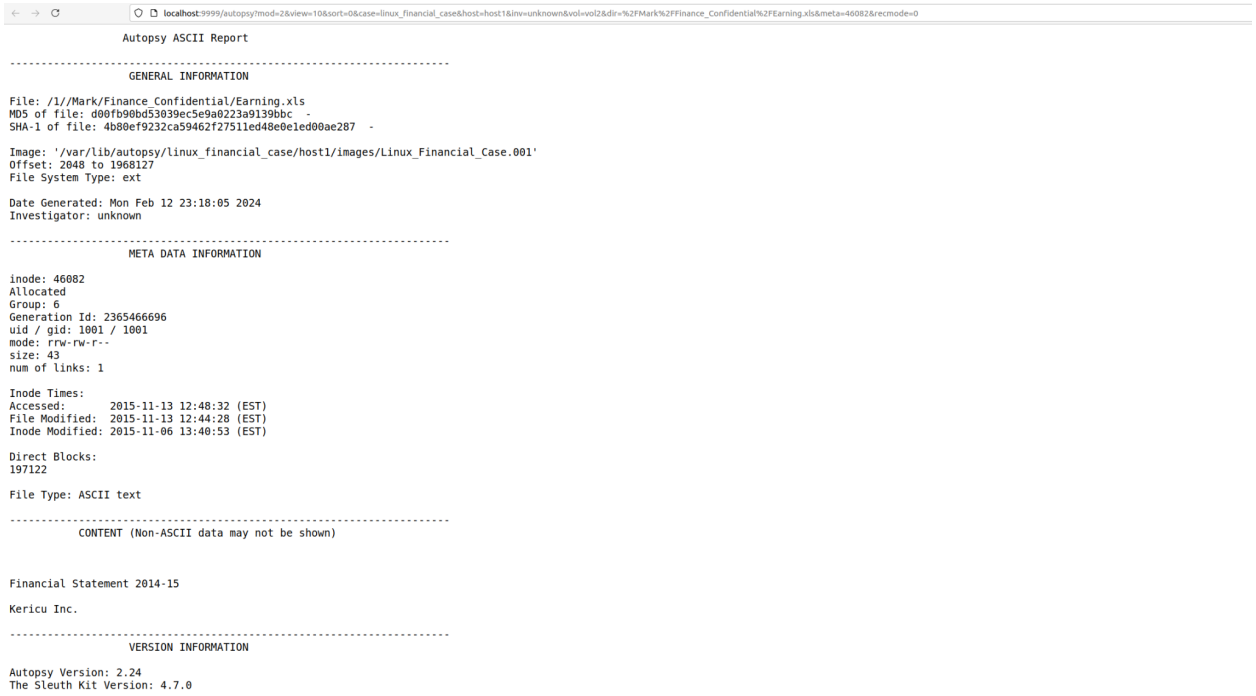
Kericu Inc.

Question 4. What information do you get from “display” and “report”? What does “export” do?

We get a lot of information here. From below screenshots we get General information about the file and its metadata information which is very important for the analysis.

The export is simply exporting the information we needed as a .xls file that we are exporting below.

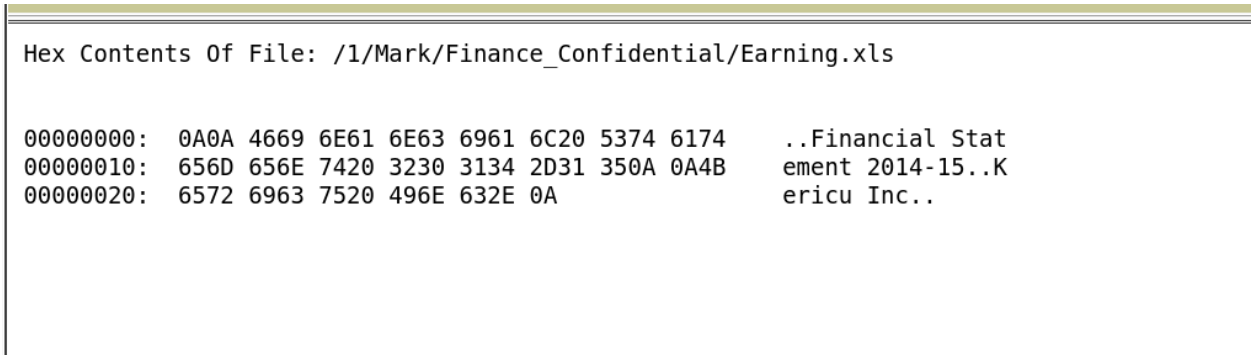
ASCII (Report)



localhost:9999/autopsy?mod=2&view=10&sort=0&case=linux_financial_case&host=host1&inv=unknown&vol=vol2&dir=%2FMark%2FFinance_Confidential%2FEarning.xls&meta=46082&recmode=0

```
                Autopsy ASCII Report

------------------------------------------------------------------
                  GENERAL INFORMATION

File: /1//Mark/Finance_Confidential/Earning.xls
MD5 of file: d00fb90bd53039ec5e9a0223a9139bbc  -
SHA-1 of file: 4b80ef9232ca59462f27511ed48e0e1ed00ae287  -

Image: '/var/lib/autopsy/linux_financial_case/host1/images/Linux_Financial_Case.001'
Offset: 2048 to 1968127
File System Type: ext

Date Generated: Mon Feb 12 23:18:05 2024
Investigator: unknown

------------------------------------------------------------------
                  META DATA INFORMATION

inode: 46082
Allocated
Group: 6
Generation Id: 2365466696
uid / gid: 1001 / 1001
mode: rrw-rw-r--
size: 43
num of links: 1

Inode Times:
Accessed:       2015-11-13 12:48:32 (EST)
File Modified:  2015-11-13 12:44:28 (EST)
Inode Modified: 2015-11-06 13:40:53 (EST)

Direct Blocks:
197122

File Type: ASCII text

------------------------------------------------------------------
          CONTENT (Non-ASCII data may not be shown)


Financial Statement 2014-15

Kericu Inc.

------------------------------------------------------------------
                  VERSION INFORMATION

Autopsy Version: 2.24
The Sleuth Kit Version: 4.7.0
```

Hex (Display)

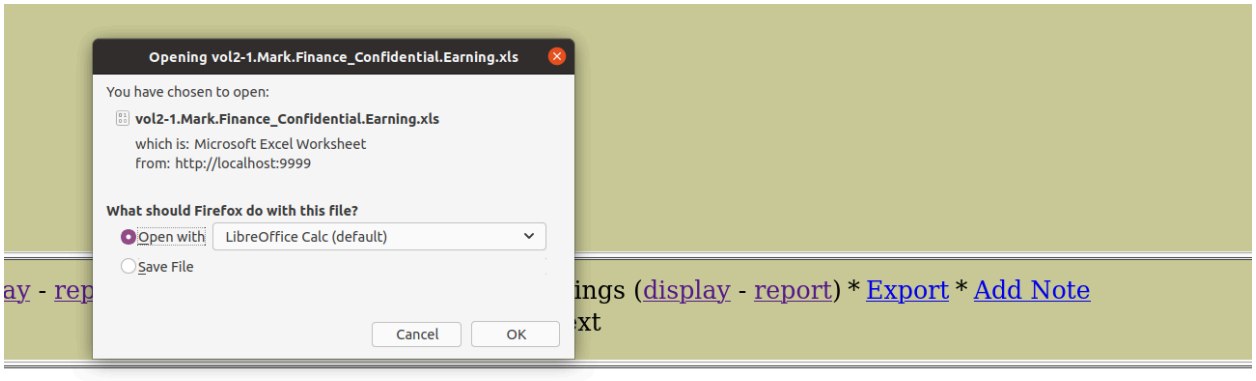


```
Hex Contents Of File: /1/Mark/Finance_Confidential/Earning.xls


00000000:  0A0A 4669 6E61 6E63 6961 6C20 5374 6174    ..Financial Stat
00000010:  656D 656E 7420 3230 3134 2D31 350A 0A4B    ement 2014-15..K
00000020:  6572 6963 7520 496E 632E 0A                ericu Inc..
```

Hex (Report)

```
                  Autopsy Hex Report

------------------------------------------------------------------
                   GENERAL INFORMATION

File: /1//Mark/Finance_Confidential/Earning.xls
MD5 of file: d00fb90bd53039ec5e9a0223a9139bbc  -
SHA-1 of file: 4b80ef9232ca59462f27511ed48e0e1ed00ae287  -

Image: '/var/lib/autopsy/linux_financial_case/host1/images/Linux_Financial_Case.001'
Offset: 2048 to 1968127
File System Type: ext

Date Generated: Mon Feb 12 23:20:49 2024
Investigator: unknown

------------------------------------------------------------------
                   META DATA INFORMATION

inode: 46082
Allocated
Group: 6
Generation Id: 2365466696
uid / gid: 1001 / 1001
mode: rrw-rw-r--
size: 43
num of links: 1

Inode Times:
Accessed:       2015-11-13 12:48:32 (EST)
File Modified:  2015-11-13 12:44:28 (EST)
Inode Modified: 2015-11-06 13:40:53 (EST)

Direct Blocks:
197122

File Type: ASCII text

------------------------------------------------------------------
                        CONTENT

00000000:  0A0A 4669 6E61 6E63 6961 6C20 5374 6174    ..Financial Stat
00000010:  656D 656E 7420 3230 3134 2D31 350A 0A4B    ement 2014-15..K
00000020:  6572 6963 7520 496E 632E 0A                ericu Inc..

------------------------------------------------------------------
                   VERSION INFORMATION

Autopsy Version: 2.24
The Sleuth Kit Version: 4.7.0
```

Export (Mode)



EXCEL data :

	A	B	C	D	E	F	G	H
1								
2								
3	Financial Statement 2014-15							
4								
5	Kericu Inc.							
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								

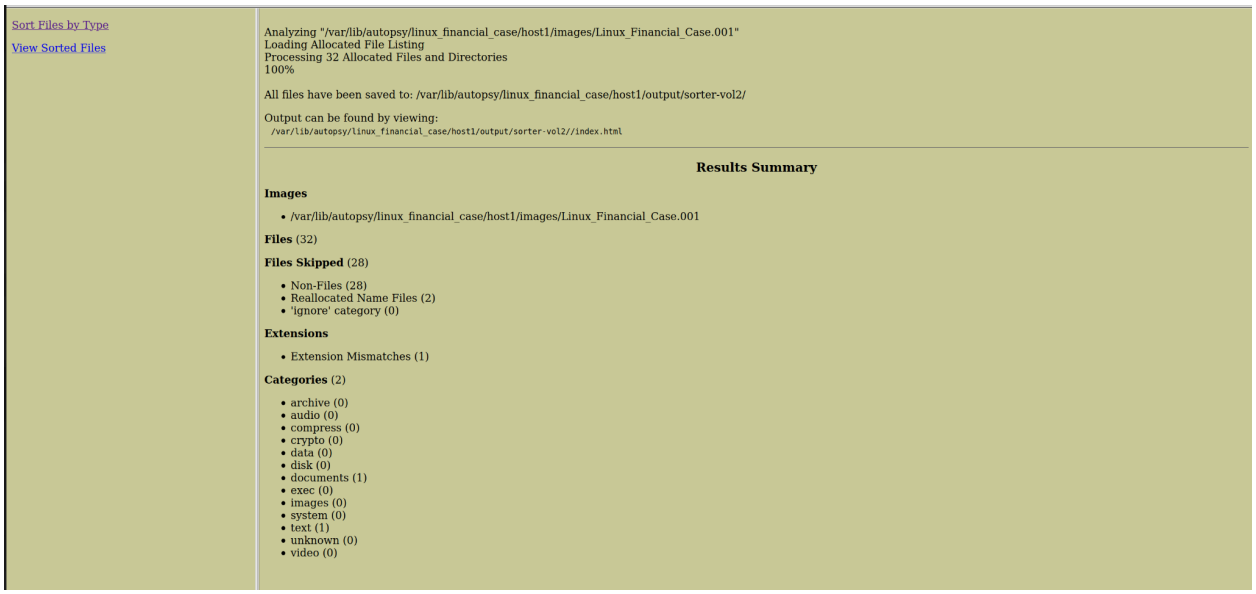
Question 5: How can you determine that a file has been deleted?

Del	Type dir / in	Name	Written	Accessed	Changed	Size	UID	GID	Meta
	d / d	../	2015-11-06 13:21:17 (EST)	2015-11-19 13:07:23 (EST)	2015-11-06 13:21:17 (EST)	4096	0	0	2
	d / d	./	2015-11-06 13:22:41 (EST)	2015-11-19 13:46:28 (EST)	2015-11-06 13:40:53 (EST)	4096	1001	1001	23041
	d / d	Finance_Confidential/	2015-11-13 12:44:31 (EST)	2015-11-19 13:46:42 (EST)	2015-11-06 13:40:53 (EST)	4096	1001	1001	46081
✔	r / r	stuff.doc	2015-11-06 15:40:40 (EST)	2015-11-06 13:22:17 (EST)	2015-11-06 15:40:40 (EST)	180224	1001	1001	23043 (realloc)
	d / d	Transport/	2015-11-06 14:02:22 (EST)	2015-11-06 14:02:27 (EST)	2015-11-06 14:02:22 (EST)	4096	1001	1001	23042

We can see here stuff.doc is deleted file. By seeing the tick on Del column.

Question 6: How is the “Sort Files by Type” formation useful in an investigation?

It is very useful because we can focus on a particular file type and start extracting a lot of information. For example, if I want to look into excel files only, I will start connecting the dots easily and analysis will be easier and more useful. Sorting always makes user to focus more and help view files better.



Sort Files by Type

View Sorted Files

Analyzing "/var/lib/autopsy/linux_financial_case/host1/images/Linux_Financial_Case.001"
Loading Allocated File Listing
Processing 32 Allocated Files and Directories
100%

All files have been saved to: /var/lib/autopsy/linux_financial_case/host1/output/sorter-vol2/

Output can be found by viewing:
/var/lib/autopsy/linux_financial_case/host1/output/sorter-vol2//index.html

Results Summary

Images

- /var/lib/autopsy/linux_financial_case/host1/images/Linux_Financial_Case.001

Files (32)

Files Skipped (28)

- Non-Files (28)
- Reallocated Name Files (2)
- 'ignore' category (0)

Extensions

- Extension Mismatches (1)

Categories (2)

- archive (0)
- audio (0)
- compress (0)
- crypto (0)
- data (0)
- disk (0)
- documents (1)
- exec (0)
- images (0)
- system (0)
- text (1)
- unknown (0)
- video (0)

Question 7: Knowing an inode number, which Sleuthkit tool does Autopsy use to determine the data blocks referenced by the inode?

Istat Tool can be used.

Command : Istat -o offset img inode_number

```
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ istat -o 2048 Linux_Financial_Case.001 46082
inode: 46082
Allocated
Group: 6
Generation Id: 2365466696
uid / gid: 1001 / 1001
mode: rrw-rw-r--
size: 43
num of links: 1

Inode Times:
Accessed:       2015-11-13 17:48:32 (UTC)
File Modified:  2015-11-13 17:44:28 (UTC)
Inode Modified: 2015-11-06 18:40:53 (UTC)

Direct Blocks:
197122
```

Question 8: What information can you get from this window? Where does Autopsy get this information from?

This is the same information we get from the **fsstat** command in the command line.

General File System Details

FILE SYSTEM INFORMATION

File System Type: Ext2
Volume Name: ipar-usb
Volume ID: 2564987b4e5af88f454919f10de7fe42

Last Written at: 2015-11-06 17:49:09 (UTC)
Last Checked at: 2015-11-06 17:05:30 (UTC)

Last Mounted at: 2015-11-06 17:49:09 (UTC)
Unmounted Improperly
Last mounted on: /media/ipar/ipar-usb1

Source OS: Linux
Dynamic Structure
Compat Features: Ext Attributes, Resize Inode, Dir Index
InCompat Features: Filetype,
Read Only Compat Features: Sparse Super, Large File,

METADATA INFORMATION

Inode Range: 1 - 61441
Root Directory: 2
Free Inodes: 61426

CONTENT INFORMATION

Block Range: 0 - 245759
Block Size: 4096
Free Blocks: 241593

BLOCK GROUP INFORMATION

Number of Block Groups: 8
Inodes per group: 7680
Blocks per group: 32768

Group: 0:
Inode Range: 1 - 7680
Block Range: 0 - 32767

We get all the information about the files, like type, Metadata, Group and Inode and block information.

Question 9: What Sleuthkit command line tool(s) was/were used to generate the body file?

Fls and **ils** to generate the body files.

/var/lib/autopsy/linux_financial_case/host1/output/body

```
0|/1/Frank|7681|d/drwxrwxr-x|2002|2002|4096|1447437530|1446836360|1446836360|0
0|/1/Frank/Appointments.xls|7682|r/rrw-rw----|2002|2002|0|1446836360|1446836360|1446836379|0
0|/1/Frank/appointments3 (deleted-realloc)|7682|l/rrw-rw----|2002|2002|0|1446836360|1446836360|1446836379|0
0|/1/Frank/appointments4 -> /media/skm/ipar-usb/Mark/Finance_Confidential/Earning.xls (deleted)|7683|l/lrwxrwxrwx|1000|1000|57|1447437474|1447437469|1447437505|0
0|/1/Untitled Folder (deleted-realloc)|7681|d/drwxrwxr-x|2002|2002|4096|1447437530|1446836360|1446836360|0
0|/1/Roger (deleted-realloc)|7681|d/drwxrwxr-x|2002|2002|4096|1447437530|1446836360|1446836360|0
0|/1/Mark|23041|d/drwxrwxr-x|1001|1001|4096|1447958788|1446834161|1446835253|0
0|/1/Mark/Finance_Confidential|46081|d/drwxrwxr-x|1001|1001|4096|1447958802|1447436671|1446835253|0
0|/1/Mark/Finance_Confidential/.~lock.Earning.xls# (deleted)|46083|r/rrw-rw-r--|1000|1000|0|1447436671|1447436671|1447436671|0
0|/1/Mark/Finance_Confidential/Earning.xls|46082|r/rrw-rw-r--|1001|1001|43|1447436912|1447436668|1446835253|0
0|/1/Mark/Transport|23042|d/drwxrwxr-x|1001|1001|4096|1446836547|1446836542|1446836542|0
0|/1/Mark/Transport/stuff.doc (deleted-realloc)|23043|r/rrw-rw----|1001|1001|180224|1446834137|1446842440|1446842440|0
0|/1/Mark/Transport/Presentation.ppt|23043|r/rrw-rw----|1001|1001|180224|1446834137|1446842440|1446842440|0
0|/1/Mark/stuff.doc (deleted-realloc)|23043|r/rrw-rw----|1001|1001|180224|1446834137|1446842440|1446842440|0
0|/1/.Trash-1000 (deleted)|38401|d/drwx------|1000|1000|0|1447436689|1447436851|1447436851|0
0|/1/Untitled Folder 2 (deleted-realloc)|23041|d/drwxrwxr-x|1001|1001|4096|1447958788|1446834161|1446835253|0
0|/1/$OrphanFiles|61441|V/V---------|0|0|0|0|0|0|0
0|/1/$OrphanFiles/OrphanFile-11 (deleted)|11|-/drwx------|0|0|0|1447436689|1447436836|1447436836|0
0|/1/$OrphanFiles/OrphanFile-15361 (deleted)|15361|-/drwx------|1000|1000|0|1447436689|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-15362 (deleted)|15362|-/rrw-r--r--|1000|1000|0|1446829869|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-15363 (deleted)|15363|-/rrw-r--r--|1000|1000|0|1446829869|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-15364 (deleted)|15364|-/rrw-r--r--|1000|1000|0|1446829869|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-15365 (deleted)|15365|-/rrw-r--r--|1000|1000|0|1446829869|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-30721 (deleted)|30721|-/drwx------|1000|1000|0|1447436689|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-30722 (deleted)|30722|-/rrw-r--r--|1000|1000|0|1446829865|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-30723 (deleted)|30723|-/rrw-r--r--|1000|1000|0|1446829865|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-30724 (deleted)|30724|-/rrw-r--r--|1000|1000|0|1446829865|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-38402 (deleted)|38402|-/drwx------|1000|1000|0|1447436689|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-38403 (deleted)|38403|-/drwx------|1000|1000|0|1447435966|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-38404 (deleted)|38404|-/rrw-rw-r--|1000|1000|0|1446830721|1446830721|1446830721|0
0|/1/$OrphanFiles/OrphanFile-38405 (deleted)|38405|-/rrw-rw-r--|1000|1000|0|1447435966|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-38406 (deleted)|38406|-/rrw-rw-r--|1000|1000|0|1447435966|1447436851|1447436851|0
```

Question 10: How might this timeline information be useful for forensic investigation

Having a timeline is crucial and very important for noting the particular execution of the file or deletion of the file or modification for the evidence purposes.

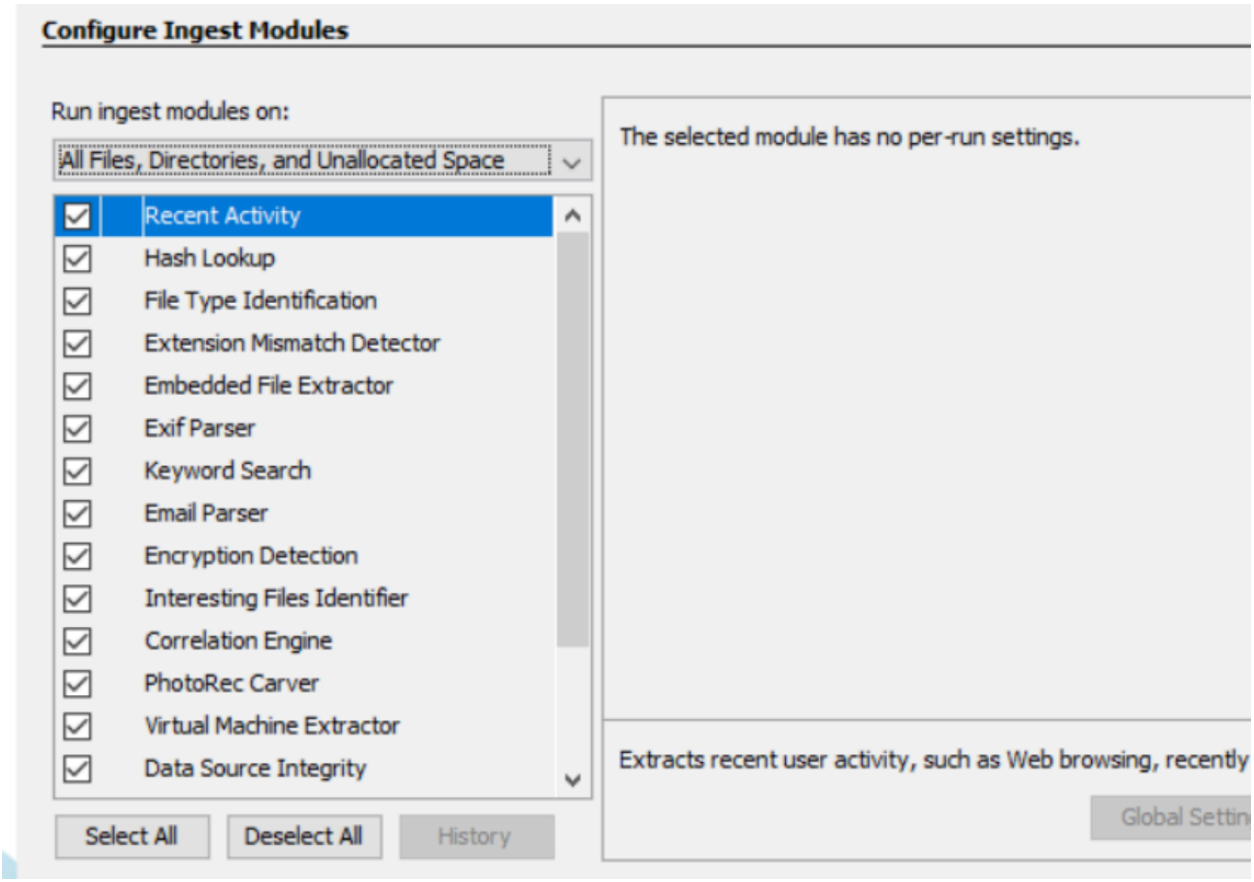
So having a timeline is a lot of information and considered as solid evidence.

Fri Nov 06 2015 12:11:05	0	.a..	-/rrw-r--r--	1000	1000	30722	/1/$OrphanFiles/OrphanFile-30722 (deleted)
	0	.a..	-/rrw-r--r--	1000	1000	30723	/1/$OrphanFiles/OrphanFile-30723 (deleted)
	0	.a..	-/rrw-r--r--	1000	1000	30724	/1/$OrphanFiles/OrphanFile-30724 (deleted)
Fri Nov 06 2015 12:11:09	0	.a..	-/rrw-r--r--	1000	1000	15362	/1/$OrphanFiles/OrphanFile-15362 (deleted)
	0	.a..	-/rrw-r--r--	1000	1000	15363	/1/$OrphanFiles/OrphanFile-15363 (deleted)
	0	.a..	-/rrw-r--r--	1000	1000	15364	/1/$OrphanFiles/OrphanFile-15364 (deleted)
	0	.a..	-/rrw-r--r--	1000	1000	15365	/1/$OrphanFiles/OrphanFile-15365 (deleted)
Fri Nov 06 2015 12:25:21	0	mac.	-/rrw-rw-r--	1000	1000	38404	/1/$OrphanFiles/OrphanFile-38404 (deleted)
Fri Nov 06 2015 13:22:17	180224	.a..	r/rrw-rw----	1001	1001	23043	/1/Mark/Transport/Presentation.ppt
	180224	.a..	r/rrw-rw----	1001	1001	23043	/1/Mark/Transport/stuff.doc (deleted-realloc)
	180224	.a..	r/rrw-rw----	1001	1001	23043	/1/Mark/stuff.doc (deleted-realloc)
Fri Nov 06 2015 13:22:41	4096	m...	d/drwxrwxr-x	1001	1001	23041	/1/Mark
	4096	m...	d/drwxrwxr-x	1001	1001	23041	/1/Untitled Folder 2 (deleted-realloc)
Fri Nov 06 2015 13:40:53	4096	..c.	d/drwxrwxr-x	1001	1001	23041	/1/Mark
	4096	..c.	d/drwxrwxr-x	1001	1001	23041	/1/Untitled Folder 2 (deleted-realloc)
	4096	..c.	d/drwxrwxr-x	1001	1001	46081	/1/Mark/Finance_Confidential
	43	..c.	r/rrw-rw-r--	1001	1001	46082	/1/Mark/Finance_Confidential /Earning.xls
Fri Nov 06 2015 13:59:20	4096	m.c.	d/drwxrwxr-x	2002	2002	7681	/1/Frank
	4096	m.c.	d/drwxrwxr-x	2002	2002	7681	/1/Roger (deleted-realloc)

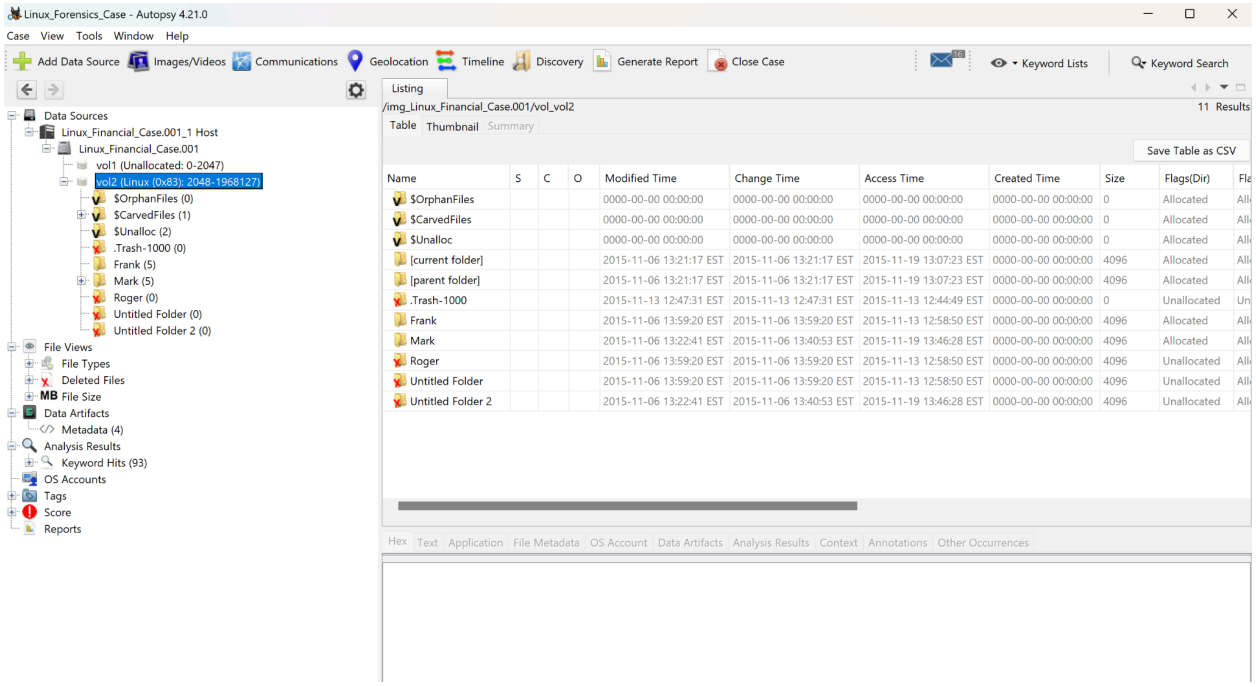
Part 3 : Windows Autopsy

1) List at least three features of Windows Autopsy with screenshots. (10 points)

Windows GUI is phenomenal because it does everything when we try to ingest the file into the system itself. For example, it does and shows everything by default in the following:



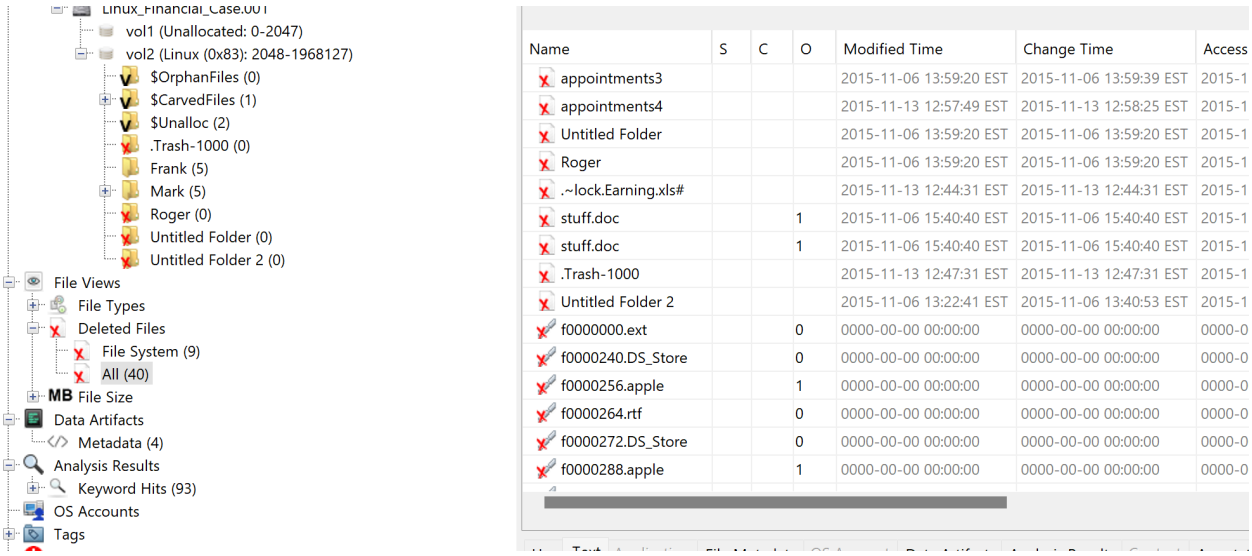
This is how it looks after ingestion of data and all the options pretty much everything is available.



Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol2 (Linux (0x83): 2048-1968127)	2	2048	1966080	Linux (0x83)	Allocated

*** We can see the partition here for Linux and its Starting sector.**

*** We can view all the deleted files and its content will be shown below in hex or text format, hex format is easy to view the content and sometimes, hex includes lot of details than text.**

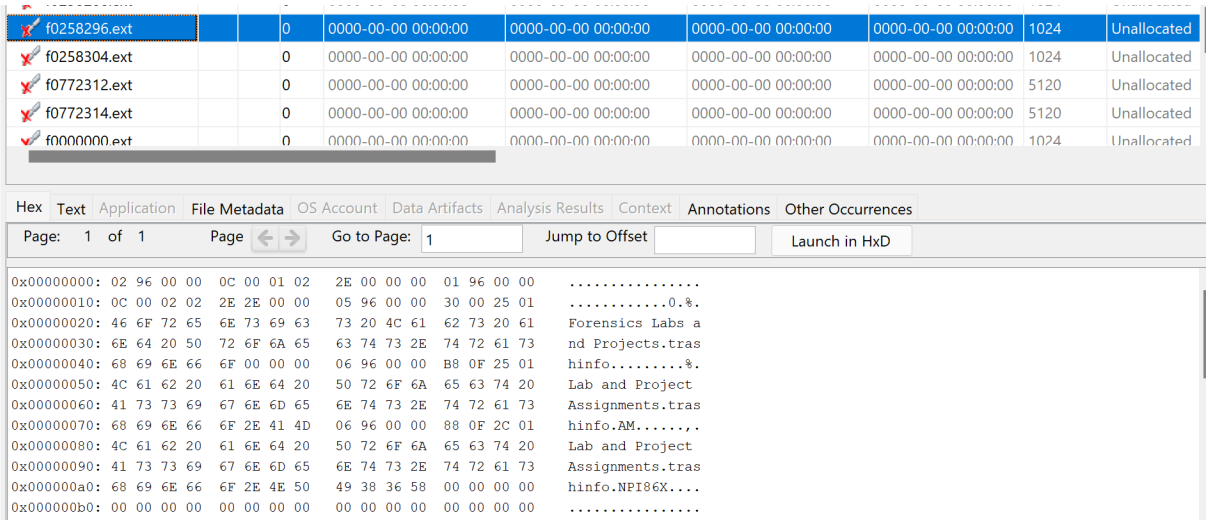


*** I found this non related data source but has email id and department and their names of the students which is a potential information**

Sheet1

Name	Email	Department	
mayuresh	mmk8578@rit.edu	Industrial	
Isaac	im5142@g.rit.edu	Telecom	
Pratith Kanagaraj	pxk5958@rit.edu	CS	
Yogeesh Seralathan	ys4815@rit.edu	CS	
Teija Mortvedt	tcm5264@rit.edu	ISE	
Rasika Kangutkar	rmk3541@rit.edu	CE	
ying-kai Huang	yh2075@grit.edu	CE	
Chun Yi Chu	cc4234@g.rit.edu	CE	
Juan Brito	jib7652@rit.edu	EE	
Anusha Balusu	ab5136@rit.edu	CS	
Pankhuri Roy	pr6538@rit.edu	CS	
S. M. Aftatul Aman	sa8331@rit.edu	Engineering, PhD	
Dhwanit Mehta	dmm8396@rit.edu	HCI	
John Chiu	jxc9745@rit.edu	Engineering, ME	

Got this from one of the files (Non related to this case anyways):

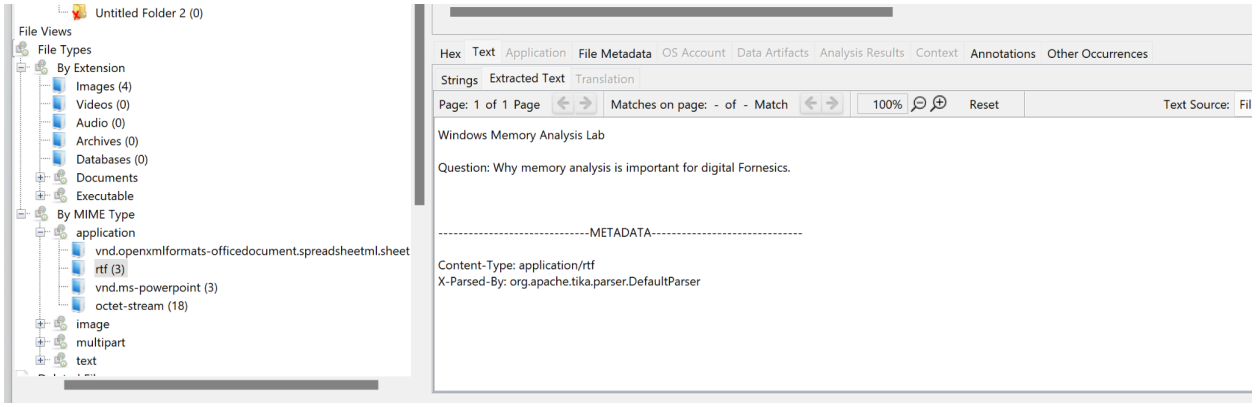


Three folders are deleted :

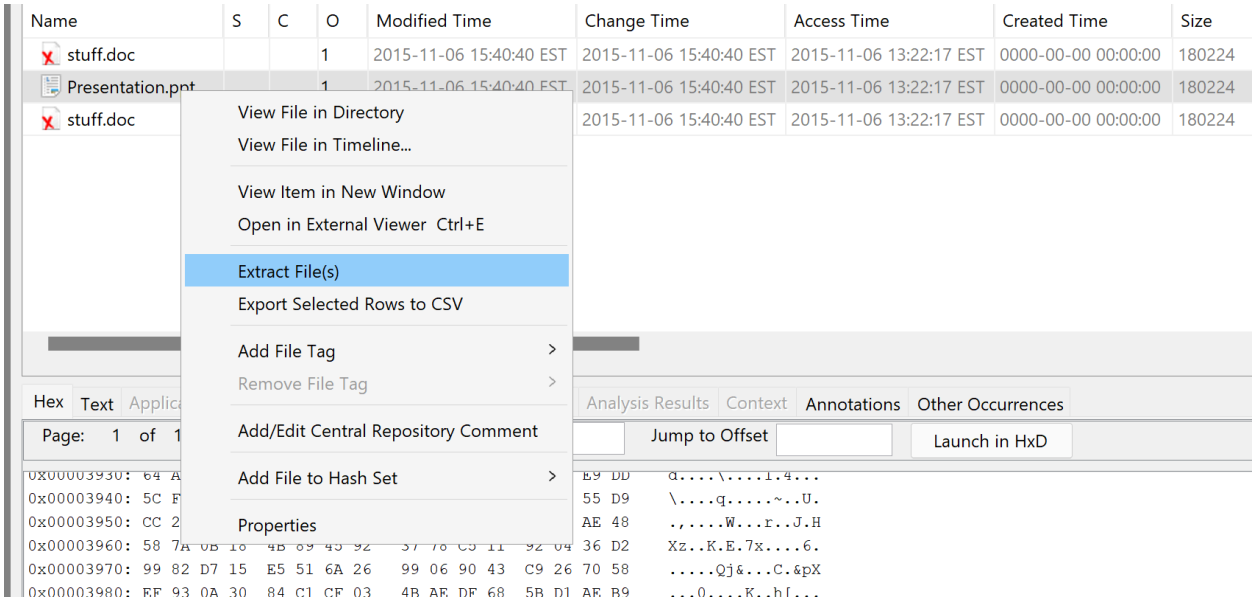
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
$Unalloc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated
[current folder]				2015-11-06 13:21:17 EST	2015-11-06 13:21:17 EST	2015-11-19 13:07:23 EST	0000-00-00 00:00:00	4096	Allocated
[parent folder]				2015-11-06 13:21:17 EST	2015-11-06 13:21:17 EST	2015-11-19 13:07:23 EST	0000-00-00 00:00:00	4096	Allocated
.Trash-1000				2015-11-13 12:47:31 EST	2015-11-13 12:47:31 EST	2015-11-13 12:44:49 EST	0000-00-00 00:00:00	0	Unallocated
Frank				2015-11-06 13:59:20 EST	2015-11-06 13:59:20 EST	2015-11-13 12:58:50 EST	0000-00-00 00:00:00	4096	Allocated
Mark				2015-11-06 13:22:41 EST	2015-11-06 13:40:53 EST	2015-11-19 13:46:28 EST	0000-00-00 00:00:00	4096	Allocated
Roger				2015-11-06 13:59:20 EST	2015-11-06 13:59:20 EST	2015-11-13 12:58:50 EST	0000-00-00 00:00:00	4096	Unallocated
Untitled Folder				2015-11-06 13:59:20 EST	2015-11-06 13:59:20 EST	2015-11-13 12:58:50 EST	0000-00-00 00:00:00	4096	Unallocated
Untitled Folder 2				2015-11-06 13:22:41 EST	2015-11-06 13:40:53 EST	2015-11-19 13:46:28 EST	0000-00-00 00:00:00	4096	Unallocated

Mark

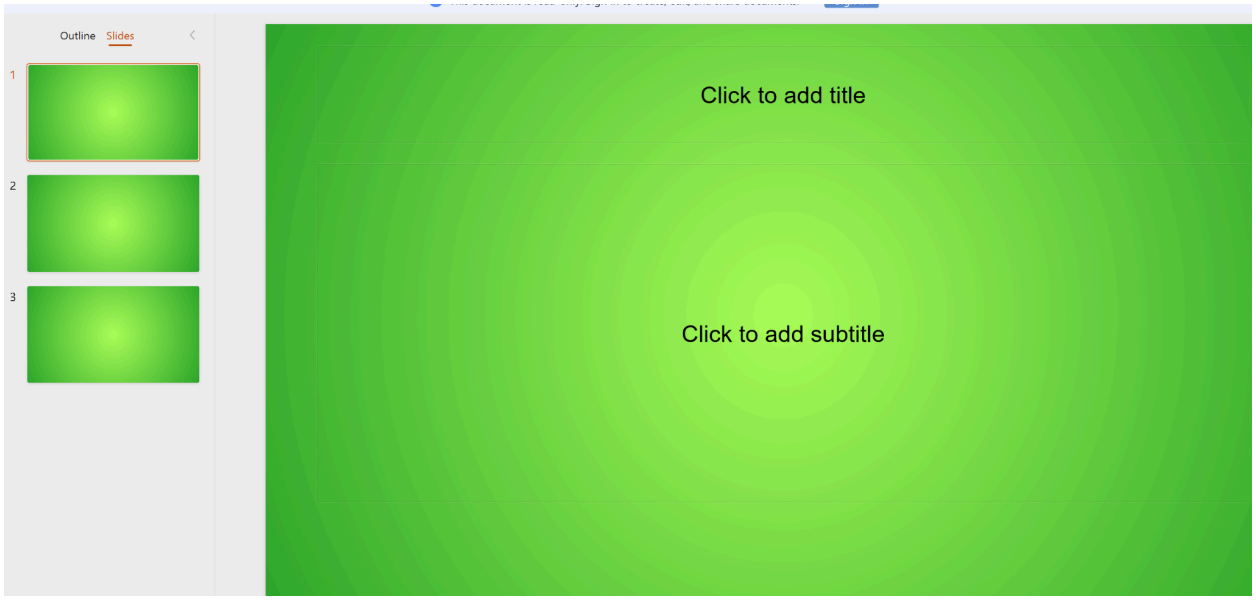
We can view different types of file types at a same place and very convenient to access



Able to extract everything :

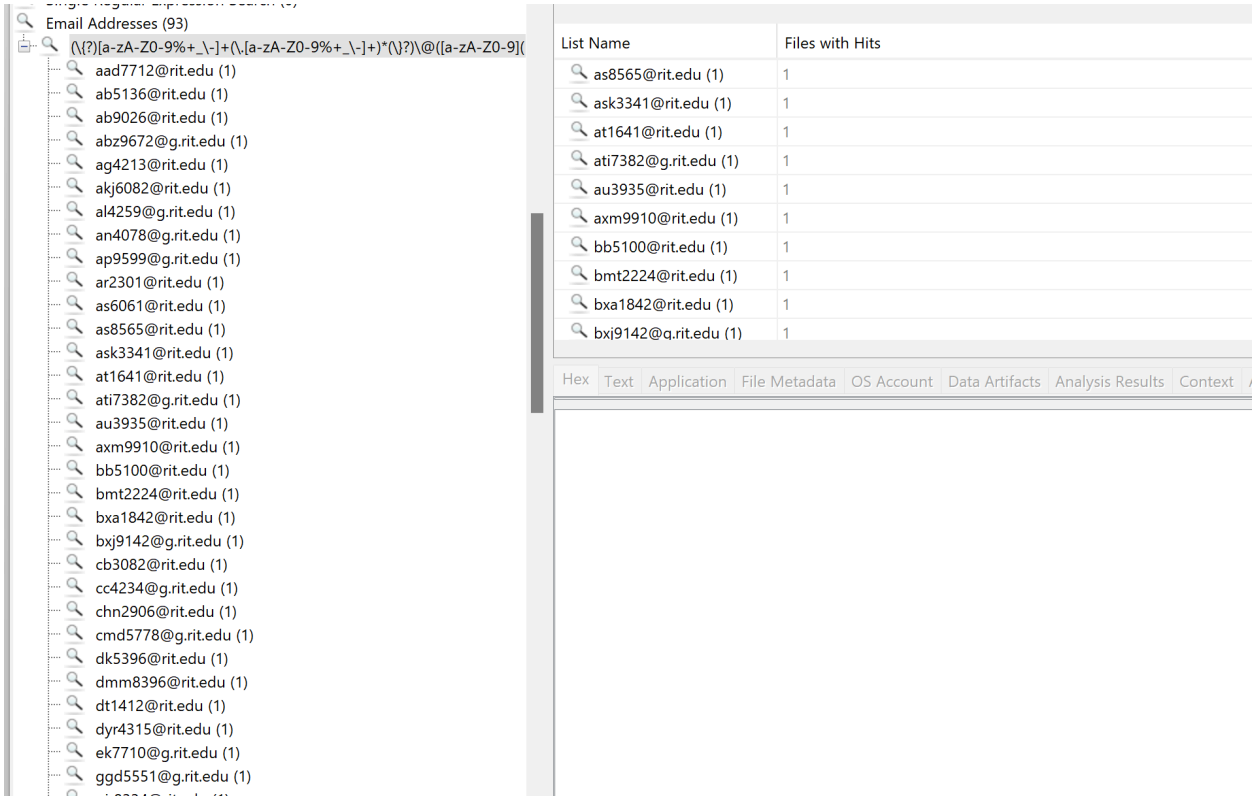


This is Presentation.ppt

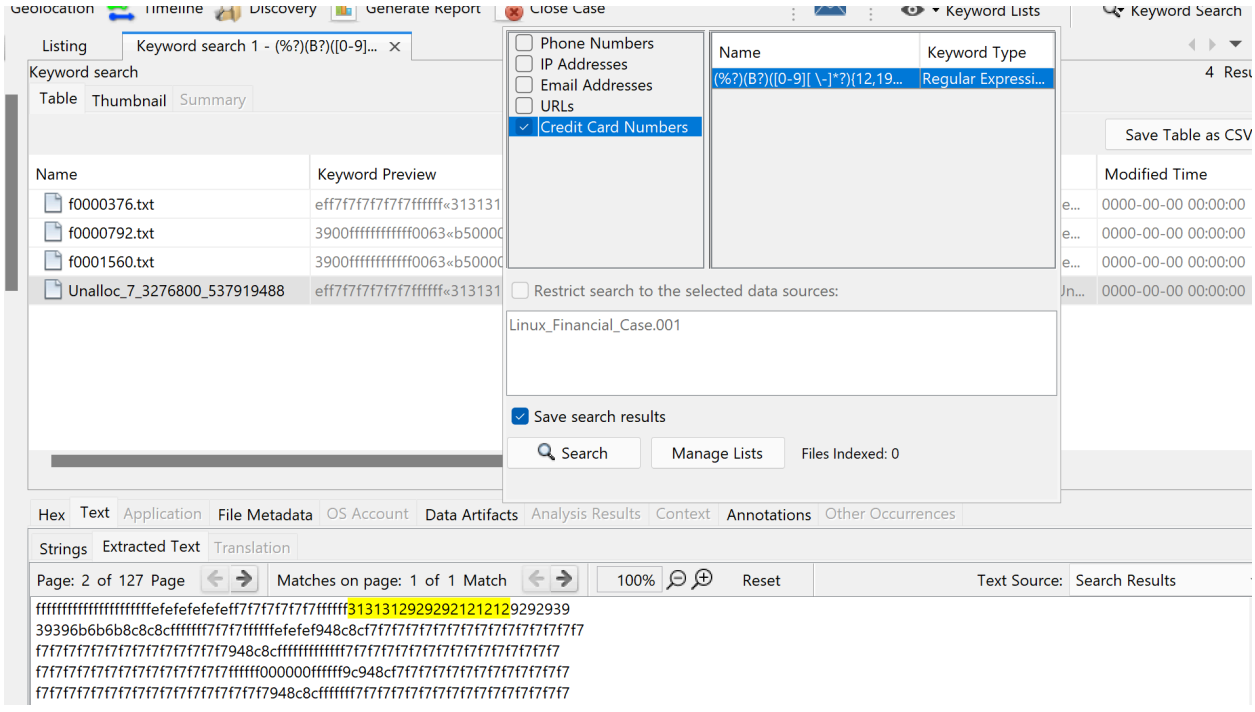


We can view all the deleted files in single place :

Got email ID separately which is rich :

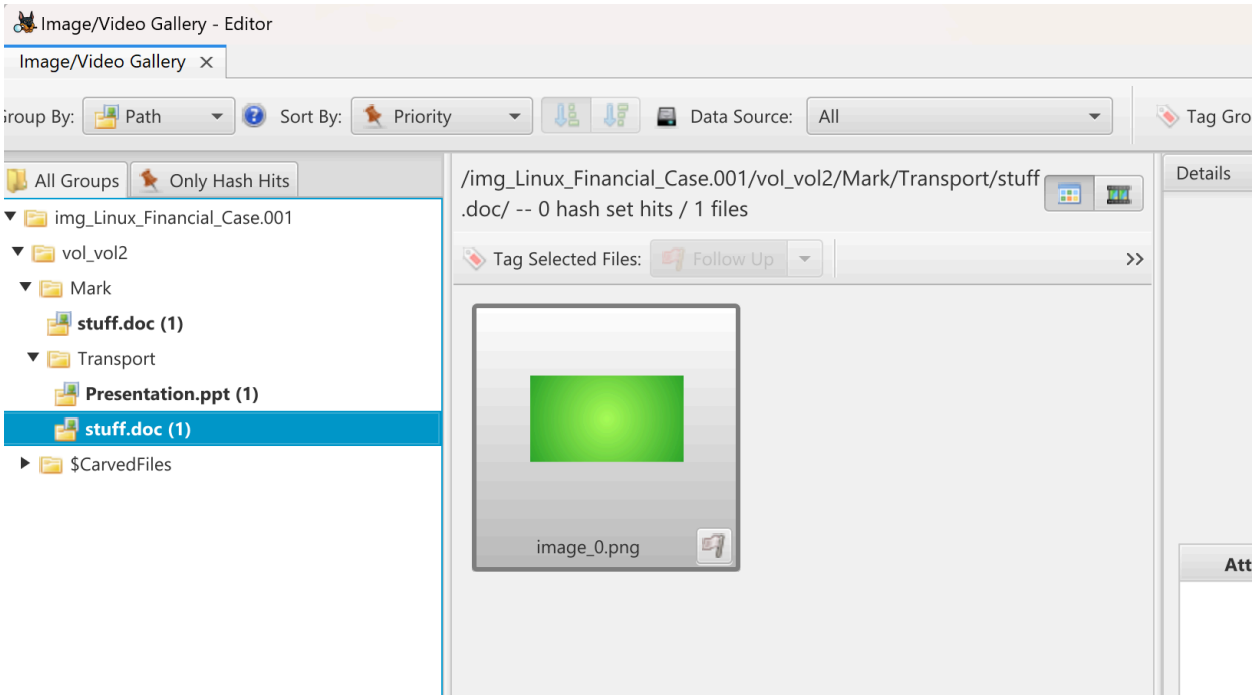


We can easily search using keywords filtration and got the credit card number below :



We can view details of the timelines, through visually appealing graphs :

*** We can view all the images separately :**



2) Compare the Windows Autopsy with the Linux Autopsy and provide your comments with two or three sentences. (6 points)

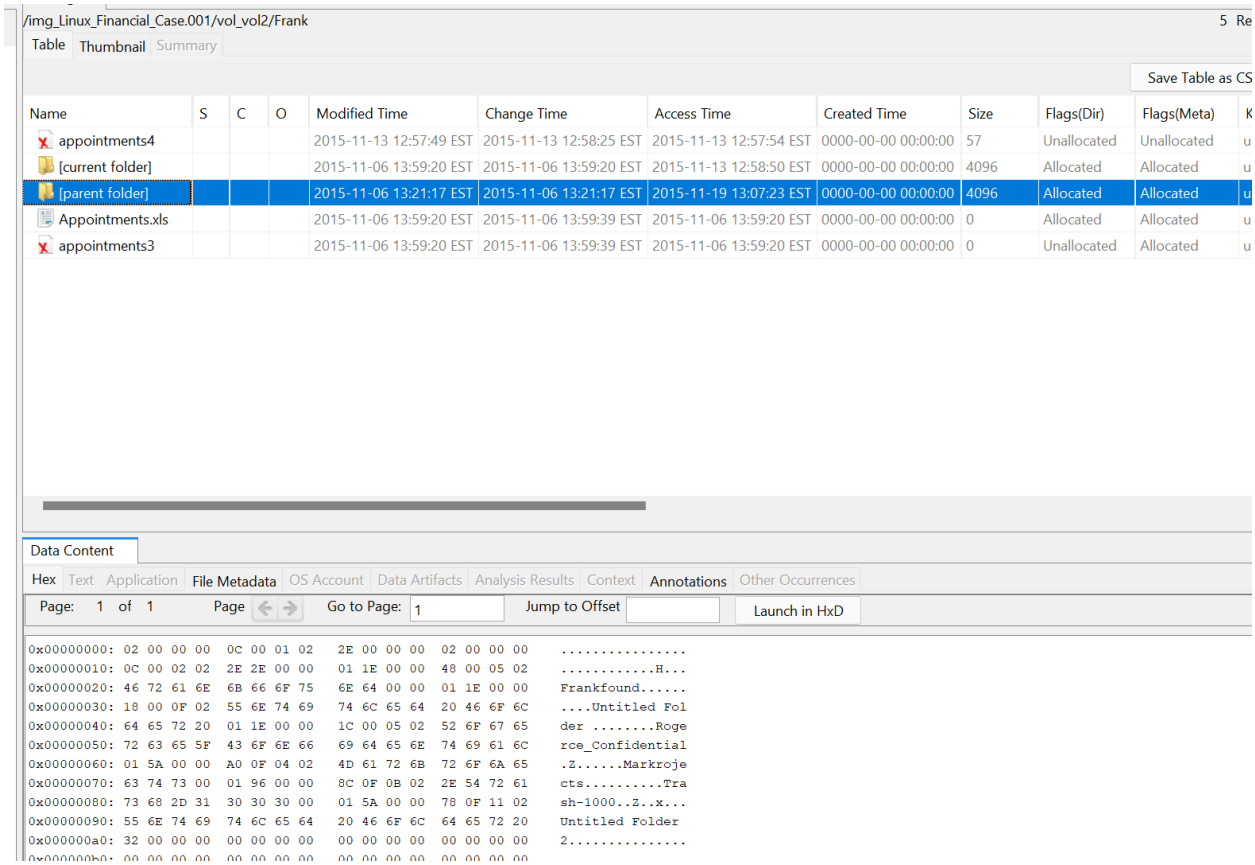
Autopsy is cool, but there is a day-and-night difference between the GUIs of Windows and Linux. Because I find the GUI of Linux autopsy to be more of a command-line GUI, there are not a lot of unique and customisable features, and we can't view everything in detail. We can say that the command line is working on all GUI clicks we make on the Linux autopsy, whereas the Windows autopsy is so rich and visually appealing and has good performance. The GUI is properly configured so that we can view all types of documents separately and do analysis based on our convenience, and it is much easier for the analysis of the investigation on the Windows autopsy. So in conclusion, the Windows Autopsy with a lot of features wins against the Linux Autopsy because of its rich, easy-to-customize options and the possibility of viewing the data in hex and text mode easily with a point of click.

Part 4. Report (14 points)

Read the case scenario again and provide a short report that includes:

1. **Your statement and evidence that indicates Frank may have read Earnings.xls. (8 points)**

To prove Frank may have read Earnings.xls, we can view it in his folder and we got the content below, indicating that Frank found the confidential information. Also, the timelines of his activities contradict Mark's folder and his files. These may be good evidence that Frank may have read the Earnings.xls file.



2. **Why is Frank able to read a confidential document? (3 points)**

This document had read permission for all and no encryption or permission was required to view it.

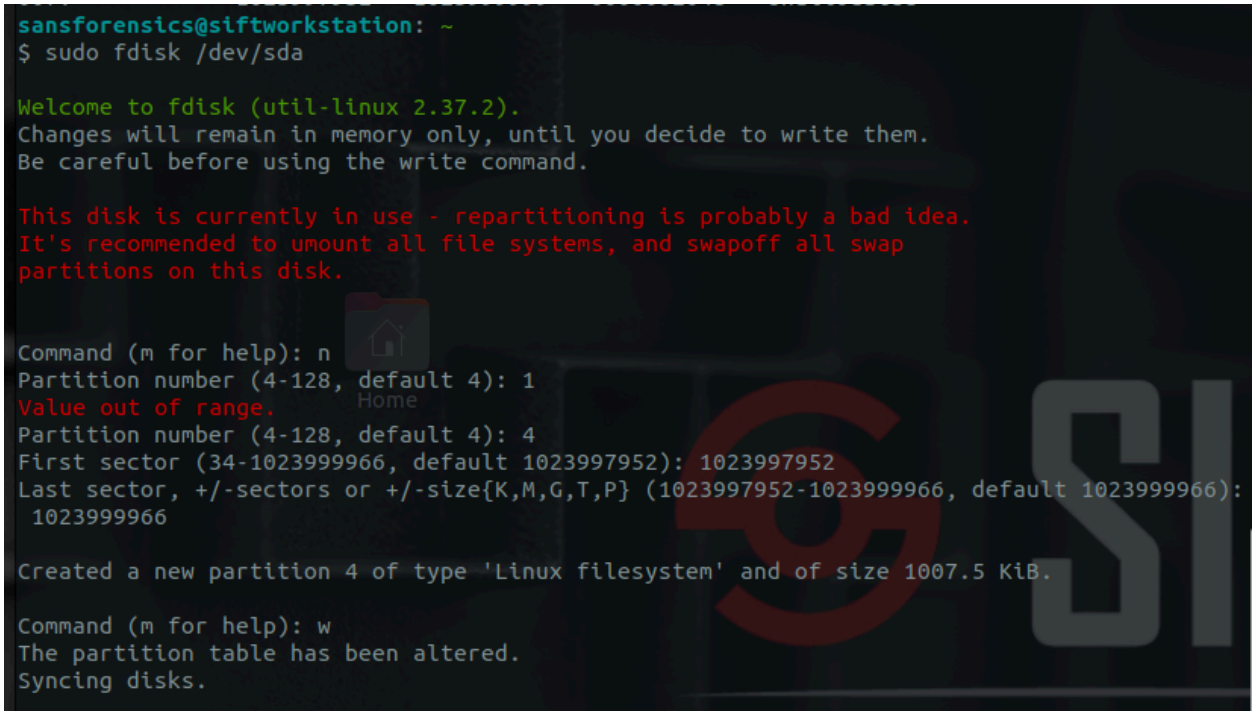
3. How do you change the permissions, so that the “Earning.xls” file will not be accessible by others? (3 points)

We can keep this file only accessible by root, or we can change the read and write permissions of this file by using the command "chmod." This command has a lot of variations, so different articles say different things, but I saw that “chmod 700 file” will remove read and write permission from others. After removing this permission, we should see the file type like this: “-rwx—---”. So now only the owner of the file can view this file.

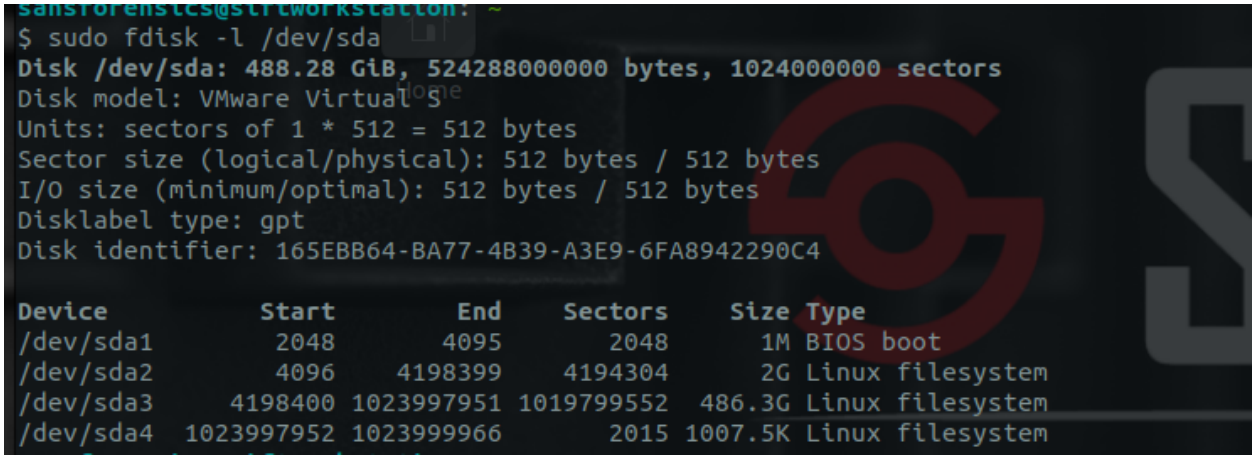
Part 5. Bonus (20 points)

Analyze deleted files in the ext4 filesystem.

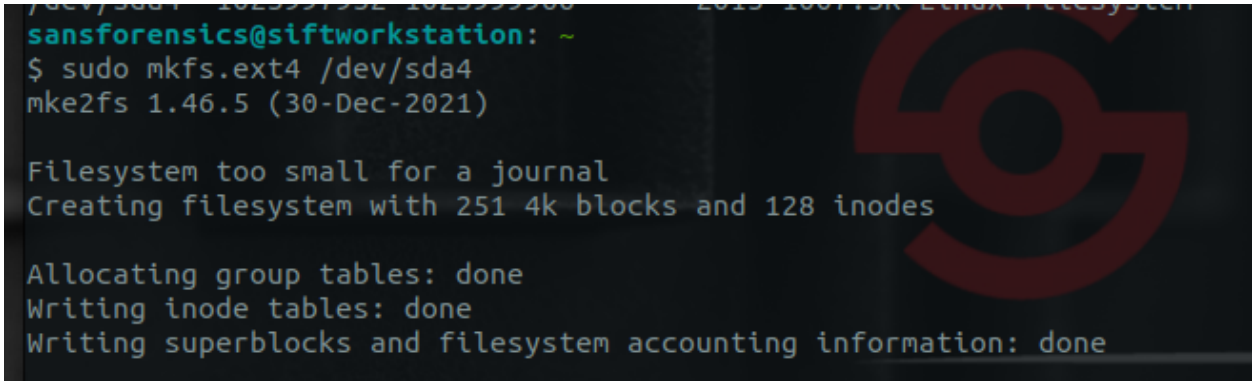
1.
Create a small ext4 partition on SIFT VM, create some files, a directory, and a couple of files in the directory, and delete some files.

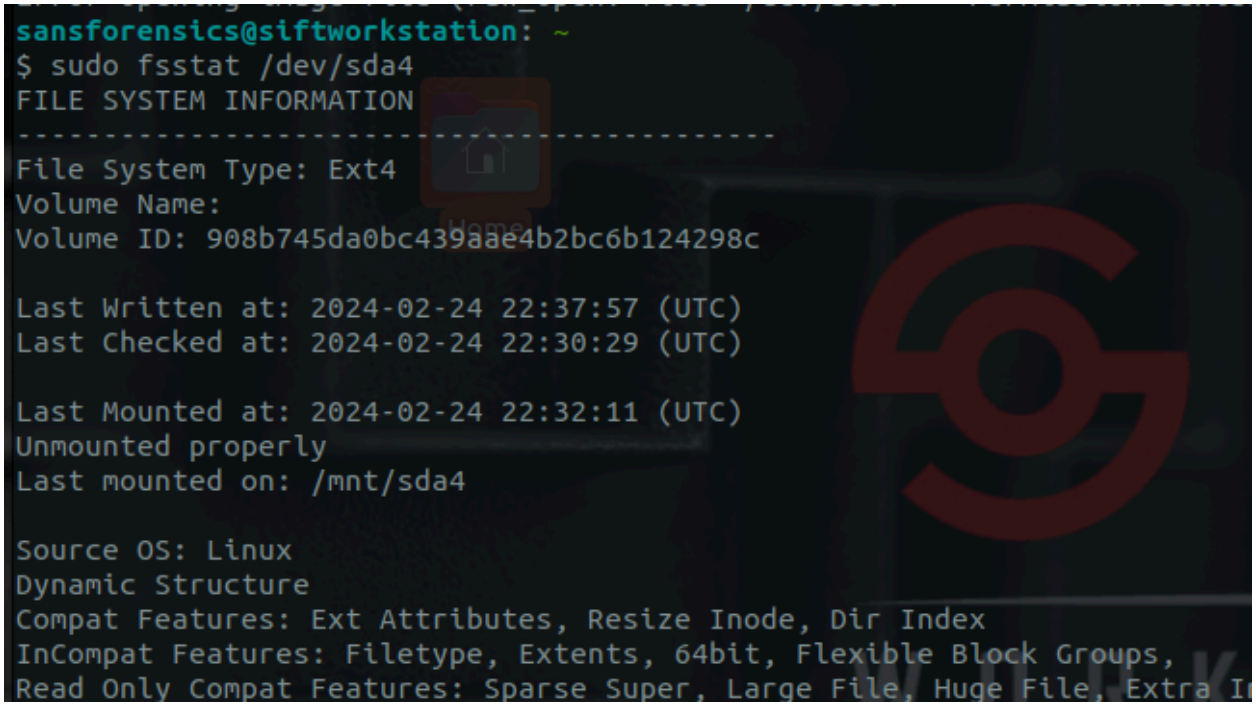


SDA4 has been created as a new partition :



Making SDA4 as ext4





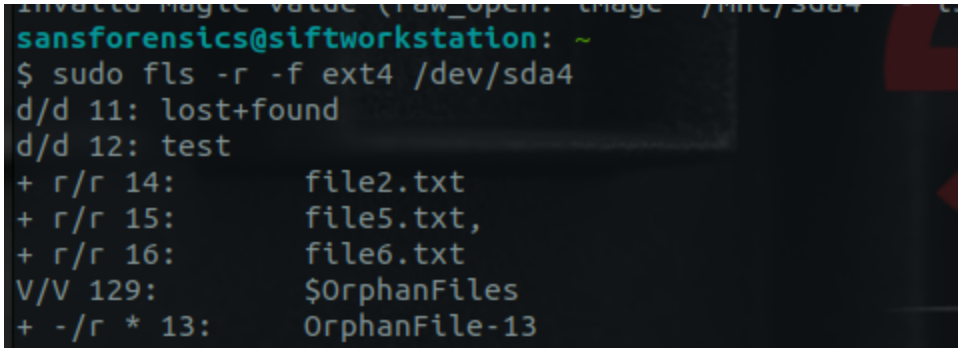
Creating and removing some files :

2.

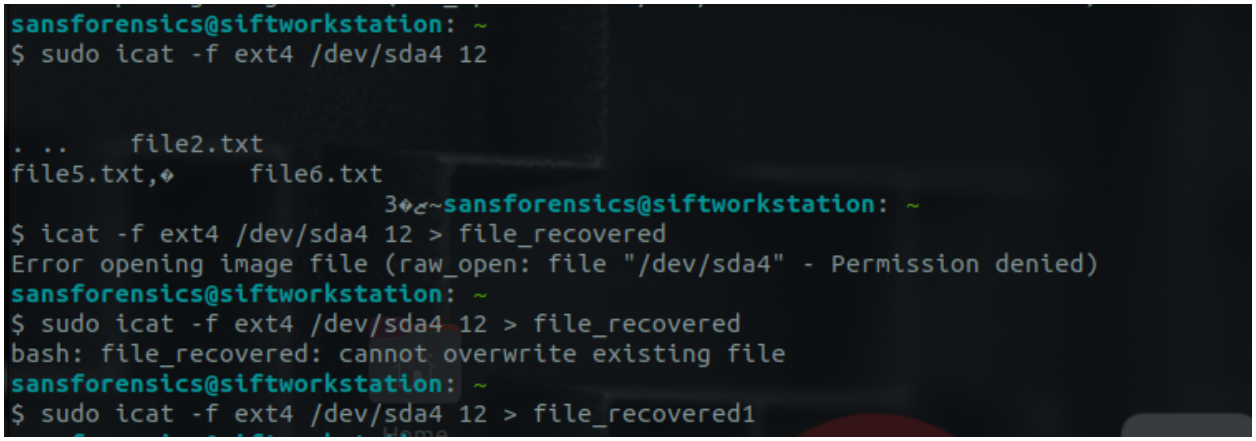
Use Sluethkit commands

Fls to list the inode of the deleted file. Show the inode content. Are you able to recover the content of the deleted files? Explain

List the deleted content (Test Folder)



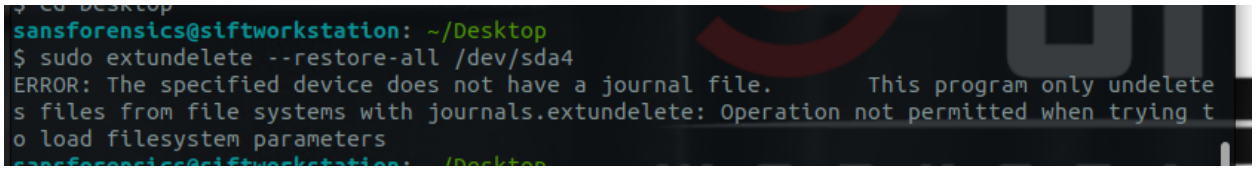
Trying to view the files through inode number and still the deleted inode is not reallocated so we can still recover the file, if it is overwritten or reallocated, it can't be recovered.



3.

Use extundelete to try to recover the deleted content (Note: undelete using extundelete is not guaranteed). Show your results and explain how extundelete attempts to undelete the content.

I tried using extundelete and got the error



I also checked about the journal file, I didn't get any proper values, but from the screenshot below Inode and data blocks are in use, but no recovery :