

# 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: 0x60cccc656

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 Groups,
Read Only Compat Features: Sparse Super, Large File, Huge File, Extra Inode Size
```

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/evidence
```

```
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 Folder 2 (deleted-realloc)"
Xxx Xxx 00 0000 00:00:00,0,...b,d/drwx-----,1000,1000,38401,"/.Trash-1000 (deleted)"
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 Folder 2 (deleted-realloc)"
Fri Nov 06 2015 13:40:53,4096,...c.,d/drwxrwxr-x,1001,1001,23041,"/Untitled Folder 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 (deleted)"
Fri Nov 13 2015 12:47:31,0,m.c.,d/drwx-----,1000,1000,38401,"/.Trash-1000 (deleted)"
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 Folder 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_crttime
0|<Linux_Financial_Case.001-dead-11>|11|-/drwx-----|0|0|0|1447436689|1447436836
|1447436836|0
0|<Linux_Financial_Case.001-dead-7683>|7683|-/lrxwrxwx|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>"
```

The output continues with many more entries, each showing a timestamp, inode number, file mode, and a string representation of the file's metadata. The pattern repeats frequently, indicating many deleted files being reallocated.

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

**Question 12.** Do *ilsMactime* and *flsMactime* 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.

```
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ istat -o 2048 lfc.dd 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
```

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*.

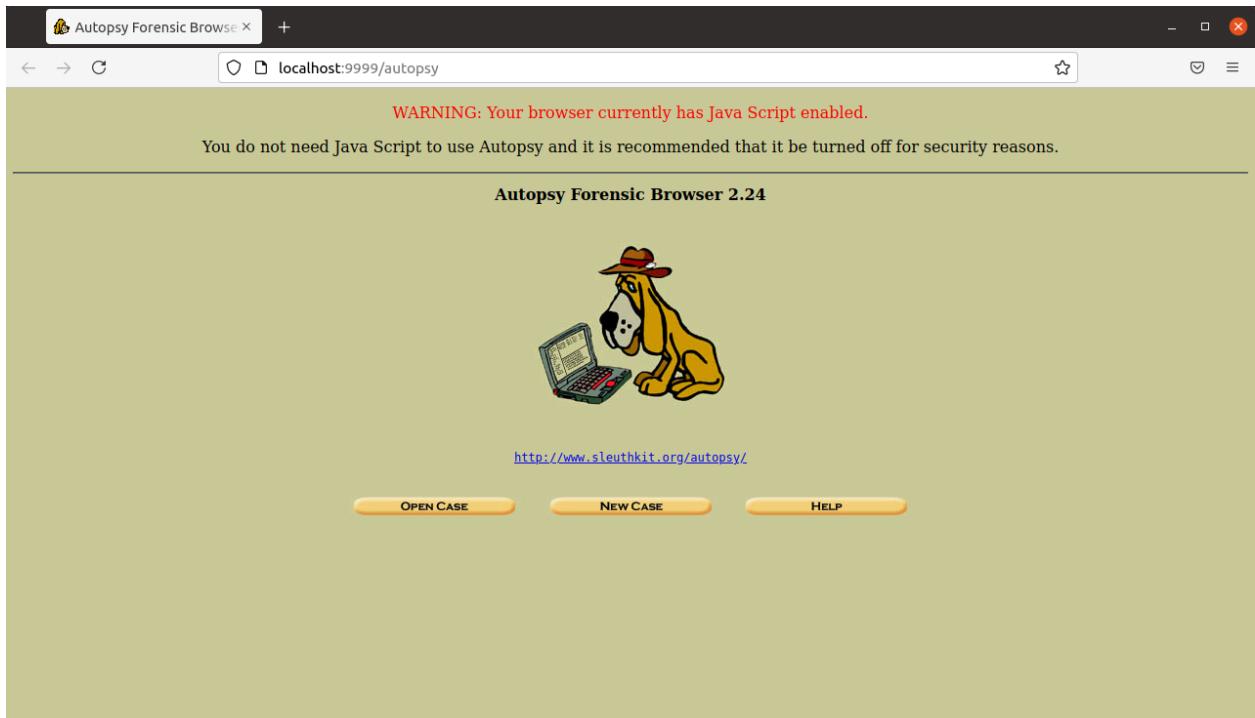
**Command : ifind -o 2048 -d 197122 Linux\_Financial\_Case.001**

-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

A screenshot of the Autopsy interface. It shows a yellow callout box with the following text:

**Local Name:** images/Linux\_Financial\_Case.001  
**Data Integrity:** An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)  
 Ignore the hash value for this image.  
 Calculate the hash value for this image.  
 Add the following MD5 hash value for this image:  
7b39de0ca146c89ad73d1d421c8f7a05  
 Verify hash after importing?

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.**

Analysis of the image file shows the following partitions:

Partition 1 (Type: Linux (0x83))

Sector Range: 2048 to 1968127

Mount Point:

File System Type:

For your reference, the `mmls` output was the following:

```
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors
```

Slot	Start	End	Length	Description
002:	000:000	0000002048	0001968127	0001966080 Linux (0x83)

**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.

```
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
$ mmls lfc.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

    Slot      Start      End      Length      Description
000: Meta    0000000000  0000000000  0000000001  Primary Table (#0)
001: -----  0000000000  0000002047  0000002048  Unallocated
002: 000:000  0000002048  0001968127  0001966080  Linux (0x83)
```

**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.

The screenshot shows the Autopsy Forensic Browser interface. At the top, there is a message box containing log information:

```
Calculating MD5 (this could take a while)
Current MD5: 7B39DE0CA146C89AD73D1D421C8F7A05
Integrity Check Passed
Testing partitions
Copying image(s) into evidence locker (this could take a little while)
Image file added with ID img1
Disk image (type dos) added with ID vol1
Volume image (2048 to 1968127 - ext - /1/) added with ID vol2
```

Below the message box are two buttons: "OK" and "ADD IMAGE".

The main window has a header with tabs: FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, and CLOSE. The FILE ANALYSIS tab is selected.

The left sidebar contains two sections:

- Directory Seek**: A text input field with the value "/1" and a "VIEW" button.
- File Name Search**: A text input field with the value "Perl" and a "SEARCH" button.
- ALL DELETED FILES**
- EXPAND DIRECTORIES**

The main content area displays a table of files found in the directory "/1". The table columns are:

DEL	Type	NAME	WRITTEN	ACCESSED	CHANGED	SIZE	UID	GID	META
	dir / in								
Error Parsing File (Invalid Characters?): V/V 61441: \$OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0									
	d / d	.l	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	.l	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	.Trash-1000/	2015-11-13 12:47:31 (EST)	2015-11-13 12:44:49 (EST)	2015-11-13 12:47:31 (EST)	0	1000	1000	38401
	d / d	Frank/	2015-11-06 13:59:20 (EST)	2015-11-13 12:58:50 (EST)	2015-11-06 13:59:20 (EST)	4096	2002	2002	7681
	d / d	Mark/	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	Roger/	2015-11-06 13:59:20 (EST)	2015-11-13 12:58:50 (EST)	2015-11-06 13:59:20 (EST)	4096	2002	2002	7681 (realloc)
✓	...	...	2015-11-06	2015-11-19	2015-11-06	1000	1001	1001	2001

At the bottom of the main content area, it says "File Browsing Mode".

<b>Inode Number:</b> <input type="text" value="23041"/>  <input type="button" value="VIEW"/>  <b>ALLOCATION LIST</b>	<div style="text-align: right; margin-bottom: 5px;"> <a href="#">◀ PREVIOUS</a> <a href="#">NEXT ▶</a> <a href="#">REPORT</a> <a href="#">VIEW CONTENTS</a> <a href="#">EXPORT CONTENTS</a> <a href="#">ADD NOTE</a> </div> <p><b>Pointed to by file:</b></p> <pre>/1/Mark /1/Mark/ /1/Mark/Finance_Confidential/.. /1/Mark/Transport/.. /1/Untitled Folder 2 (deleted)</pre> <p><b>File Type:</b> 370 XA sysV pure executable not stripped - 5.2 format</p> <p><b>MD5 of content:</b> 5cbb96051f65a6101le9caa7f5971abf -</p> <p><b>SHA-1 of content:</b> d4c3328da39ab28642cfcc99baf8d404eaf80666e -</p> <p><b>Details:</b></p> <pre>inode: 23041 Allocated Group: 3 Generation Id: 2365466695 uid / gid: 1001 / 1001 mode: drwxrwxr-x size: 4096 num of links: 4  Inode Times: Accessed: 2015-11-19 13:46:28 (EST) File Modified: 2015-11-06 13:22:41 (EST) Inode Modified: 2015-11-06 13:40:53 (EST)  Direct Blocks: <a href="#">98847</a></pre>
---	---

## ASCII ( display )

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	SIZE	UID	GID	META
	d / d	<a href="#">..l</a>	2015-11-06 13:22:41 (EST)	2015-11-19 13:46:28 (EST)	2015-11-06 13:40:53 (EST)	4096	1001	1001	<a href="#">23041</a>
	d / d	<a href="#">.l</a>	2015-11-13 12:44:31 (EST)	2015-11-19 13:46:42 (EST)	2015-11-06 13:40:53 (EST)	4096	1001	1001	<a href="#">46081</a>
✓	r / r	<a href="#">.~lock.Earning.xls#</a>	<a href="#">2015-11-13 12:44:31 (EST)</a>	<a href="#">2015-11-13 12:44:31 (EST)</a>	<a href="#">2015-11-13 12:44:31 (EST)</a>	0	1000	1000	<a href="#">46083</a>
	r / r	<a href="#">Earning.xls</a>	2015-11-13 12:44:28 (EST)	2015-11-13 12:48:32 (EST)	2015-11-06 13:40:53 (EST)	43	1001	1001	<a href="#">46082</a>

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

**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: d00fb9b0d53039ec5e9a0223a9139bbc
SHA-1 of file: 4b80ef9232ca59462f27511ed448e0e1ed00ae287

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

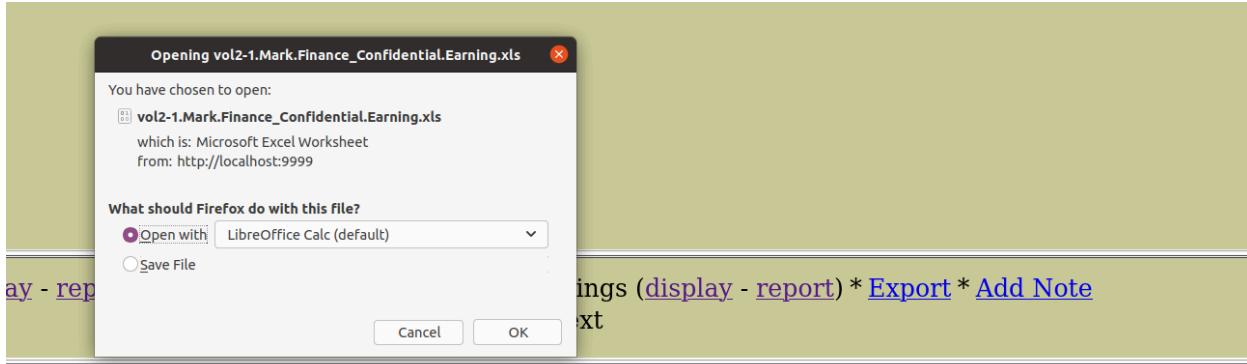
-----
CONTENT

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 0A 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	NAME	WRITTEN	ACCESSED	CHANGED	SIZE	UID	GID	META
d / d	dir / ln	..l	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
<input checked="" type="checkbox"/>	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.

<p>Sort Files by Type <a href="#">View Sorted Files</a></p>	<p>Analyzing "/var/lib/autopsy/linux_financial_case/host1/images/Linux_Financial_Case.001" Loading Allocated File Listing Processing 32 Allocated Files and Directories 100%</p> <p>All files have been saved to: /var/lib/autopsy/linux_financial_case/host1/output/sorter-vol2/ Output can be found by viewing: <a href="#">/var/lib/autopsy/linux_financial_case/host1/output/sorter-vol2/index.html</a></p> <hr/> <p style="text-align: center;"><b>Results Summary</b></p> <p><b>Images</b></p> <ul style="list-style-type: none"><li>• /var/lib/autopsy/linux_financial_case/host1/images/Linux_Financial_Case.001</li></ul> <p><b>Files (32)</b></p> <p><b>Files Skipped (28)</b></p> <ul style="list-style-type: none"><li>• Non-Files (28)</li><li>• Reallocated Name Files (2)</li><li>• 'ignore' category (0)</li></ul> <p><b>Extensions</b></p> <ul style="list-style-type: none"><li>• Extension Mismatches (1)</li></ul> <p><b>Categories (2)</b></p> <ul style="list-style-type: none"><li>• archive (0)</li><li>• audio (0)</li><li>• compress (0)</li><li>• crypto (0)</li><li>• data (0)</li><li>• disk (0)</li><li>• documents (1)</li><li>• exec (0)</li><li>• images (0)</li><li>• system (0)</li><li>• text (1)</li><li>• unknown (0)</li><li>• video (0)</li></ul>
---	---

**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
sansforensics@siftworkstation: ~/Desktop/Linux_Financial_Case.001
```

**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	
<b>FILE SYSTEM INFORMATION</b>	
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,
<b>METADATA INFORMATION</b>	
Inode Range:	1 - 61441
Root Directory:	2
Free Inodes:	61426
<b>CONTENT INFORMATION</b>	
Block Range:	0 - 245759
Block Size:	4096
Free Blocks:	241593
<b>BLOCK GROUP INFORMATION</b>	
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?

**FIs and iFs** 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/rw-rw---|2002|2002|0|1446836360|1446836360|1446836379|0
0|/1/Frank/Appointments3 (deleted-realloc)|7682|l/rw-rw---|2002|2002|0|1446836360|1446836360|1446836379|0
0|/1/Frank/Appointments4 -> /media/skm/ipmap-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/rw-r--|1000|1000|0|1447436671|1447436671|1447436671|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/rw-rw---|1001|1001|418022|1446834137|1446842440|1446842440|0
0|/1/Mark/Transport/Presentation.ppt|23043|r/rw-rw---|1001|1001|180224|1446834137|1446842440|1446842440|0
0|/1/Mark/stuff.doc (deleted-realloc)|23043|r/rw-rw---|1001|1001|180224|1446834137|1446842440|1446842440|0
0|/1/.Trash-1000 (deleted)|38401|d/drwxrwxr-x|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/$OrphanFiles|61441|V-V-----|0|0|0|0|0|0|0|0
0|/1/$OrphanFiles/OrphanFile-11 (deleted)|11|-drwxrwxr-x|0|0|0|1447436689|1447436836|1447436836|0
0|/1/$OrphanFiles/OrphanFile-15361 (deleted)|15361|-drwxrwxr-x|1000|1000|0|1447436689|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-15362 (deleted)|15362|-drwxrwxr-x|1000|1000|0|1446829869|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-15363 (deleted)|15363|-drwxrwxr-x|1000|1000|0|1446829869|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-15364 (deleted)|15364|-drwxrwxr-x|1000|1000|0|1446829869|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-15365 (deleted)|15365|-drwxrwxr-x|1000|1000|0|1446829869|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-30721 (deleted)|30721|-drwxrwxr-x|1000|1000|0|1447436689|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-30722 (deleted)|30722|-drwxrwxr-x|1000|1000|0|1446829865|144743685|1447436851|0
0|/1/$OrphanFiles/OrphanFile-30723 (deleted)|30723|-drwxrwxr-x|1000|1000|0|1446829865|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-30724 (deleted)|30724|-drwxrwxr-x|1000|1000|0|1446829865|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-38402 (deleted)|38402|-drwxrwxr-x|1000|1000|0|1447436689|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-38403 (deleted)|38403|-drwxrwxr-x|1000|1000|0|1447435966|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-38404 (deleted)|38404|-drwxrwxr-x|1000|1000|0|1446830721|1446830721|1446830721|0
0|/1/$OrphanFiles/OrphanFile-38405 (deleted)|38405|-drwxrwxr-x|1000|1000|0|1447435966|1447436851|1447436851|0
0|/1/$OrphanFiles/OrphanFile-38406 (deleted)|38406|-drwxrwxr-x|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.

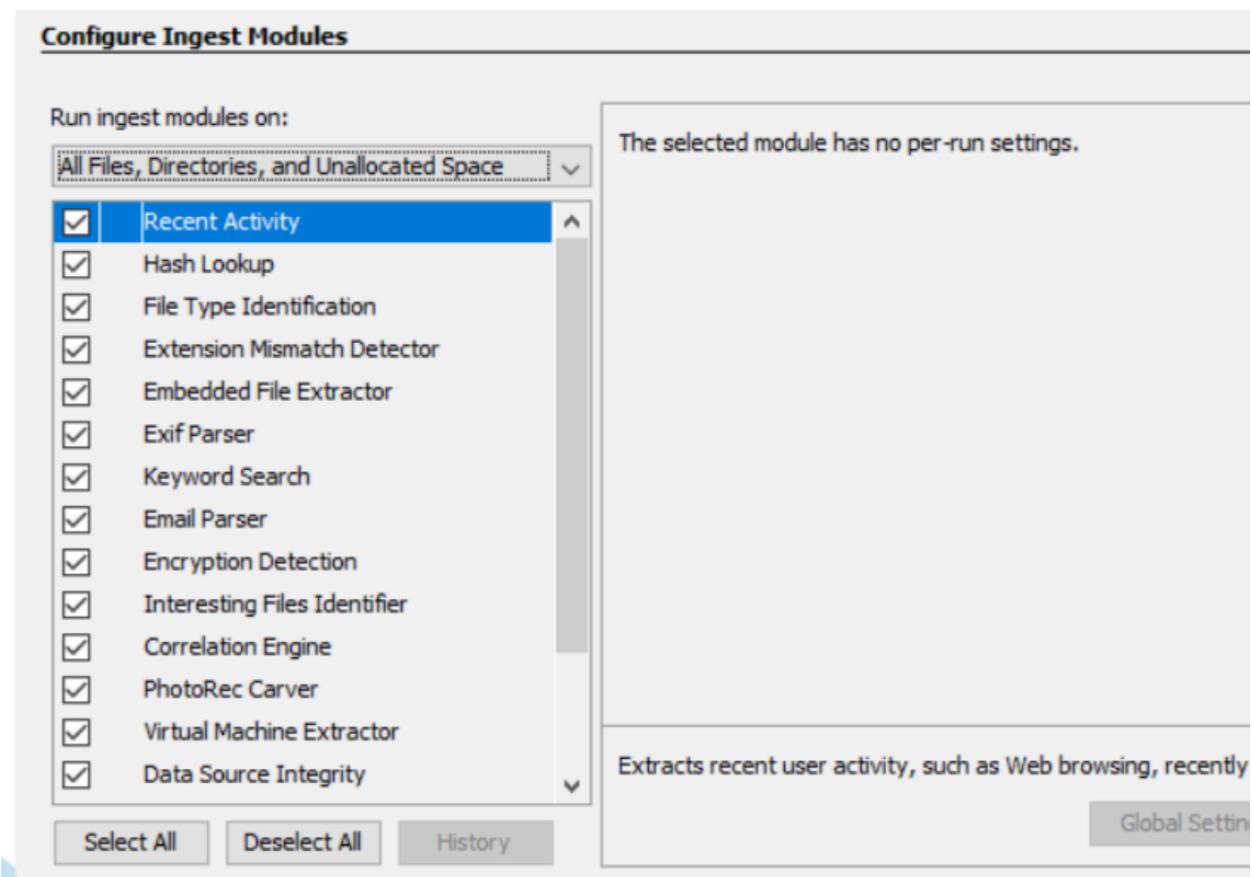
So having a timeline is a lot of information and considered as solid evidence.

Timeline View										
File System Events		File Details			File Data			File Path		
Date	Time	User	Type	Access	Size	Modif.	Atime	Block	inode	Path
<a href="#">CREATE DATA FILE</a> <a href="#">CREATE TIMELINE</a> <a href="#">VIEW TIMELINE</a> <a href="#">VIEW NOTES</a> <a href="#">HELP</a> <a href="#">CLOSE</a>										
<a href="#">&lt;- Oct 2015</a> <a href="#">Summary</a> <a href="#">Dec 2015 -&gt;</a>										
<input type="button" value="Nov"/> <input type="button" value="2015"/> <input type="button" value="OK"/>										
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.

Linux\_Forensics\_Case - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case Keyword Lists Keyword Search

Data Sources Linux\_Financial\_Case.001\_1 Host Linux\_Financial\_Case.001 vol1 (Unallocated: 0-2047) vol2 (Linux (0x83): 2048-1968127) \$OrphanFiles (0) \$CarvedFiles (1) \$Unalloc (2) .Trash-1000 (0) Frank (5) Mark (5) Roger (0) Untitled Folder (0) Untitled Folder 2 (0)

File Views File Types Deleted Files MB File Size Data Artifacts Metadata (4) Analysis Results Keyword Hits (93) OS Accounts Tags Score Reports

Listing /img\_Linux\_Financial\_Case.001/vol\_vol2 Table Thumbnail Summary Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	File
\$OrphanFiles				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	All
\$CarvedFiles				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	All
\$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	All
.Trash-1000				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	All
Frank	(5)			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	All
Mark	(5)			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	All
Roger	(0)			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	0	Unallocated	Un
Untitled Folder	(0)			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	All
Untitled Folder 2	(0)			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	All

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

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.

linux\_financial\_case.001

vol1 (Unallocated: 0-2047) vol2 (Linux (0x83): 2048-1968127) \$OrphanFiles (0) \$CarvedFiles (1) \$Unalloc (2) .Trash-1000 (0) Frank (5) Mark (5) Roger (0) Untitled Folder (0) Untitled Folder 2 (0)

File Views File Types Deleted Files File System (9) All (40) MB File Size Data Artifacts Metadata (4) Analysis Results Keyword Hits (93) OS Accounts Tags

Name	S	C	O	Modified Time	Change Time	Access
appointments3				2015-11-06 13:59:20 EST	2015-11-06 13:59:39 EST	2015-1
appointments4				2015-11-13 12:57:49 EST	2015-11-13 12:58:25 EST	2015-1
Untitled Folder				2015-11-06 13:59:20 EST	2015-11-06 13:59:20 EST	2015-1
Roger				2015-11-06 13:59:20 EST	2015-11-06 13:59:20 EST	2015-1
~lock.Earning.xls#				2015-11-13 12:44:31 EST	2015-11-13 12:44:31 EST	2015-1
stuff.doc	1			2015-11-06 15:40:40 EST	2015-11-06 15:40:40 EST	2015-1
stuff.doc	1			2015-11-06 15:40:40 EST	2015-11-06 15:40:40 EST	2015-1
.Trash-1000				2015-11-13 12:47:31 EST	2015-11-13 12:47:31 EST	2015-1
Untitled Folder 2				2015-11-06 13:22:41 EST	2015-11-06 13:40:53 EST	2015-1
f0000000.ext	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-0
f000240.DS_Store	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-0
f000256.apple	1			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-0
f000264.rtf	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-0
f000272.DS_Store	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-0
f000288.apple	1			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-0

\* 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@rit.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	ixc9745@rit.edu	Engineering MF

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

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Page: 1 of 1	Page	← →	Go to Page: 1	Jump to Offset			Launch in HxD		
<hr/>									
0x00000000: 02 96 00 00 0C 00 01 02 2E 00 00 00 01 96 00 00 ..... 0x00000010: 0C 00 02 02 2E 2E 00 00 05 96 00 00 30 00 25 01 .....0.%. 0x00000020: 46 6F 72 65 6E 73 69 63 73 20 4C 61 62 73 20 61 Forensics Labs a 0x00000030: 6E 64 20 50 72 6F 6A 65 63 74 73 2E 74 72 61 73 nd Projects.tras 0x00000040: 68 69 6E 66 6F 00 00 00 06 96 00 00 B8 02 25 01 hinfo.....%. 0x00000050: 4C 61 62 20 61 6E 64 20 50 72 6F 6A 65 63 74 20 Lab and Project 0x00000060: 41 73 73 69 67 6E 6D 65 6E 74 73 2E 74 72 61 73 Assignments.tras 0x00000070: 68 69 6E 66 6F 2E 41 4D 06 96 00 00 88 0F 2C 01 hinfo.AM....., 0x00000080: 4C 61 62 20 61 6E 64 20 50 72 6F 6A 65 63 74 20 Lab and Project 0x00000090: 41 73 73 69 67 6E 6D 65 6E 74 73 2E 74 72 61 73 Assignments.tras 0x000000A0: 68 69 6E 66 6F 2E 4E 50 49 38 36 58 00 00 00 00 hinfo.NPI86X.... 0x000000B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....									

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	Mark			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

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

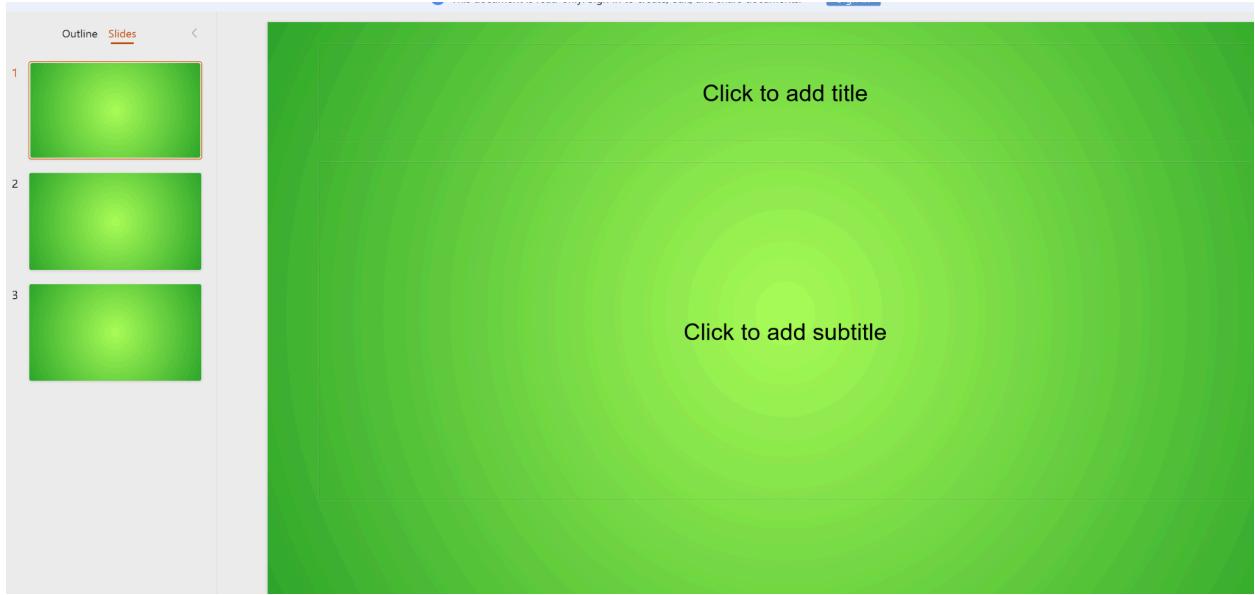
The screenshot shows a memory analysis interface. On the left, a tree view titled "Untitled Folder 2 (0)" lists various file types and their counts: Images (4), Videos (0), Audio (0), Archives (0), Databases (0), Documents, Executable, By Extension, By MIME Type, application (with subtypes like vnd.openxmlformats-officedocument.spreadsheetml.sheet, rtf, vnd.ms-powerpoint, octet-stream), image, multipart, and text. On the right, a main pane displays "Windows Memory Analysis Lab" with the question "Question: Why memory analysis is important for digital forensics." Below this, a section titled "METADATA" shows Content-Type: application/rft and X-Parsed-By: org.apache.tika.parser.DefaultParser.

Able to extract everything :

The screenshot shows a context menu for a file named "Presentation.ppt". The menu includes options like "View File in Directory", "View File in Timeline...", "View Item in New Window", "Open in External Viewer Ctrl+E", "Extract File(s)" (which is highlighted in blue), "Export Selected Rows to CSV", "Add File Tag", "Remove File Tag", "Add/Edit Central Repository Comment", "Add File to Hash Set", and "Properties". At the bottom, there is a hex dump of the file's contents.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
stuff.doc				2015-11-06 15:40:40 EST	2015-11-06 15:40:40 EST	2015-11-06 13:22:17 EST	0000-00-00 00:00:00	180224
Presentation.ppt				2015-11-06 15:40:40 EST	2015-11-06 15:40:40 EST	2015-11-06 13:22:17 EST	0000-00-00 00:00:00	180224
stuff.doc					2015-11-06 15:40:40 EST	2015-11-06 13:22:17 EST	0000-00-00 00:00:00	180224

This is Presentation.ppt



**We can view all the deleted files in single place :**



**Got email ID separately which is rich :**

The screenshot shows a digital forensic analysis interface. On the left, a search results pane displays a list of email addresses found in the system, filtered by a regular expression: `(\?)[a-zA-Z0-9%+\_]+(\,[a-zA-Z0-9%+\_+]*)*(\?)(\([a-zA-Z0-9](`. The results include numerous entries such as `aad7712@rit.edu (1)`, `ab5136@rit.edu (1)`, etc. On the right, a file analysis pane shows a table titled 'List Name' with columns 'List Name' and 'Files with Hits'. The table lists various email addresses from the search results, each appearing once. Below the panes are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, and Context.

List Name	Files with Hits
as8565@rit.edu (1)	1
ask3341@rit.edu (1)	1
at1641@rit.edu (1)	1
ati7382@g.rit.edu (1)	1
au3935@rit.edu (1)	1
axm9910@rit.edu (1)	1
bb5100@rit.edu (1)	1
bmt2224@rit.edu (1)	1
bx1842@rit.edu (1)	1
bxj9142@g.rit.edu (1)	1
cb3082@rit.edu (1)	1
cc4234@g.rit.edu (1)	1
chn2906@rit.edu (1)	1
cmd5778@g.rit.edu (1)	1
dk5396@rit.edu (1)	1
dmm8396@rit.edu (1)	1
dt1412@rit.edu (1)	1
dyr4315@rit.edu (1)	1
ek7710@g.rit.edu (1)	1
ggd5551@g.rit.edu (1)	1

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

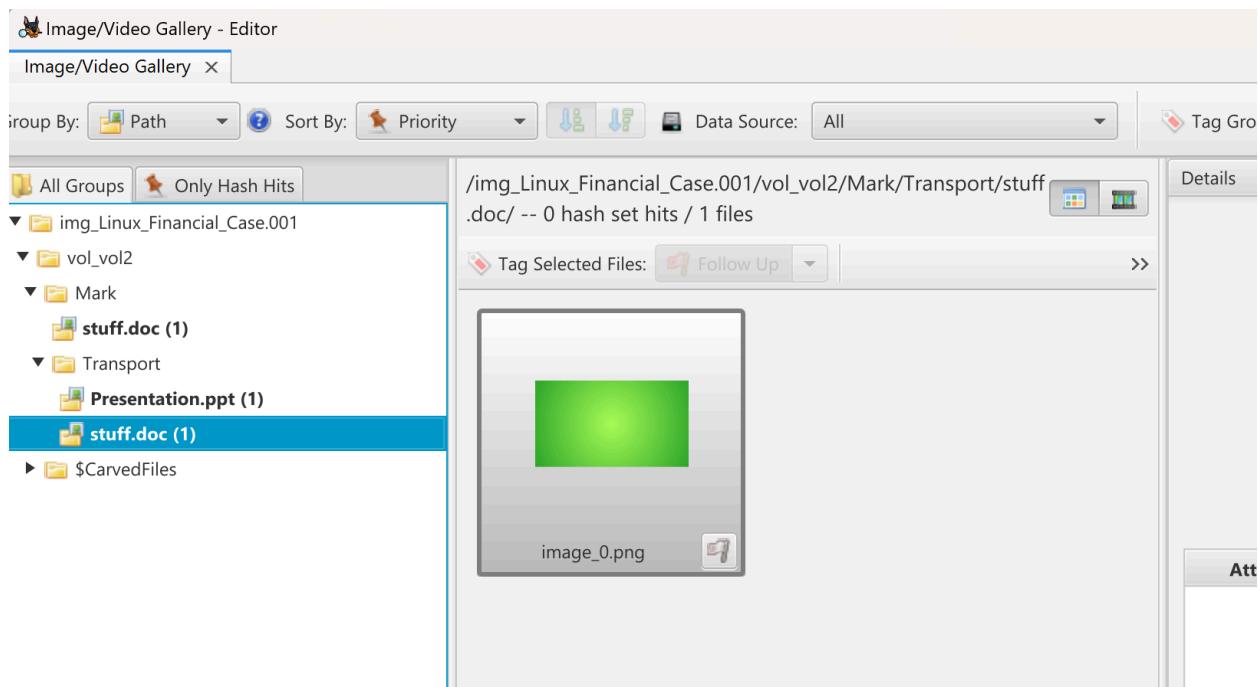
The screenshot shows a digital forensic analysis interface with a 'Keyword Lists' panel on the right containing a table of search filters. One filter, 'Credit Card Numbers', is selected. The main pane shows a table of search results with columns 'Name' and 'Keyword Preview'. The results list several files, including `f0000376.txt`, `f0001560.txt`, and `Unalloc_7_3276800_537919488`. Below the table are buttons for 'Save Table as CSV' and 'Modified Time'. At the bottom, there are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, Other Occurrences, and a search bar with 'Page: 2 of 127' and 'Text Source: Search Results'.

Name	Keyword Preview
f0000376.txt	eff7f7f7f7f7fffeff313131
f0001560.txt	3900ffffffffffff0063«b50000
Unalloc_7_3276800_537919488	eff7f7f7f7f7fffeff313131

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.

/img_Linux_Financial_Case.001/vol_vol2/Frank												5 Re
												Save Table as CS
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	K	
appointments4				2015-11-13 12:57:49 EST	2015-11-13 12:58:25 EST	2015-11-13 12:57:54 EST	0000-00-00 00:00:00	57	Unallocated	Unallocated	u	
[current 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	Allocated	Allocated	u	
[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	Allocated	u	
Appointments.xls				2015-11-06 13:59:20 EST	2015-11-06 13:59:39 EST	2015-11-06 13:59:20 EST	0000-00-00 00:00:00	0	Allocated	Allocated	u	
appointments3				2015-11-06 13:59:20 EST	2015-11-06 13:59:39 EST	2015-11-06 13:59:20 EST	0000-00-00 00:00:00	0	Unallocated	Allocated	u	

Data Content												
Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences			
Page: 1 of 1	Page	Go to Page:	1	Jump to Offset			Launch in HxD					
0x00000000: 02 00 00 00 0C 00 01 02 2E 00 00 00 02 00 00 00 .....												
0x00000010: 0C 00 02 02 2E 2E 00 00 01 1E 00 00 48 00 05 02 .....												
0x00000020: 46 72 61 6E 6B 66 6F 75 6E 64 00 00 01 1E 00 00 Frankfound.....												
0x00000030: 18 00 0F 02 55 6E 74 69 74 6C 65 64 20 46 6F 6C ....Untitled Fol												
0x00000040: 64 65 72 20 01 1E 00 00 1C 00 05 02 52 6F 67 65 der .....Roge												
0x00000050: 72 63 65 5F 43 6F 6E 66 69 64 65 6E 74 69 61 6C rce_Confidential												
0x00000060: 01 5A 00 00 A0 0F 04 02 4D 61 72 6B 72 6F 6A 65 .Z.....Markroje												
0x00000070: 63 74 73 00 01 96 00 00 8C 0F 0B 02 2E 54 72 61 cts.....Tra												
0x00000080: 73 68 2D 31 30 30 30 00 01 5A 00 00 78 0F 11 02 sh-1000..Z..x...												
0x00000090: 55 6E 74 69 74 6C 65 64 20 46 6F 6C 64 65 72 20 Untitled Folder												
0x000000a0: 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2.....												
0x000000b0: ..00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..												

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.**

```
sansforensics@siftworkstation: ~
$ sudo fdisk /dev/sda

Welcome to fdisk (util-linux 2.37.2).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

This disk is currently in use - repartitioning is probably a bad idea.
It's recommended to umount all file systems, and swapoff all swap
partitions on this disk.

Command (m for help): n
Partition number (4-128, default 4): 1
Value out of range.
Partition number (4-128, default 4): 4
First sector (34-1023999966, default 1023997952): 1023997952
Last sector, +/-sectors or +/-size{K,M,G,T,P} (1023997952-1023999966, default 1023999966): 1023999966

Created a new partition 4 of type 'Linux filesystem' and of size 1007.5 KiB.

Command (m for help): w
The partition table has been altered.

Syncing disks.
```

**SDA4 has been created as a new partition :**

```
sansforensics@siftworkstation: ~
$ sudo fdisk -l /dev/sda
Disk /dev/sda: 488.28 GiB, 524288000000 bytes, 1024000000 sectors
Disk model: VMware Virtualhome
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: gpt
Disk identifier: 165EBB64-BA77-4B39-A3E9-6FA8942290C4

Device      Start      End    Sectors   Size Type
/dev/sda1     2048     4095      2048    1M  BIOS boot
/dev/sda2     4096  4198399     4194304    2G Linux filesystem
/dev/sda3  4198400 1023997951 1019799552 486.3G Linux filesystem
/dev/sda4  1023997952 1023999966        2015 1007.5K Linux filesystem
```

**Making SDA4 as ext4**

```
/dev/sda4: 1023997952 1023999966      2015 1007.5K Linux filesystem
sansforensics@siftworkstation: ~
$ sudo mkfs.ext4 /dev/sda4
mke2fs 1.46.5 (30-Dec-2021)

Filesystem too small for a journal
Creating filesystem with 251 4k blocks and 128 inodes

Allocating group tables: done
Writing inode tables: done
Writing superblocks and filesystem accounting information: done
```

```
sansforensics@siftworkstation: ~
$ sudo fsstat /dev/sda4
FILE SYSTEM INFORMATION
-----
File System Type: Ext4
Volume Name:
Volume ID: 908b745da0bc439aae4b2bc6b124298c
Last Written at: 2024-02-24 22:37:57 (UTC)
Last Checked at: 2024-02-24 22:30:29 (UTC)

Last Mounted at: 2024-02-24 22:32:11 (UTC)
Unmounted properly
Last mounted on: /mnt/sda4

Source OS: Linux
Dynamic Structure
Compat Features: Ext Attributes, Resize Inode, Dir Index
InCompat Features: Filetype, Extents, 64bit, Flexible Block Groups,
Read Only Compat Features: Sparse Super, Large File, Huge File, Extra I
```

#### Creating and removing some files :

```
rm: cannot remove 'file1.txt': Permission denied
sansforensics@siftworkstation: /mnt/sda4/test
$ sudo rm file1.txt
sansforensics@siftworkstation: /mnt/sda4/test
$ ls
file2.txt
sansforensics@siftworkstation: /mnt/sda4/test
$ sudo touch fil4.txt
sansforensics@siftworkstation: /mnt/sda4/test
$ sudo touch file5.txt, file6.txt
```

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 )

```
sansforensics@siftworkstation: ~
$ sudo fls -r -f ext4 /dev/sda4
d/d 11: lost+found
d/d 12: test
+ r/r 14:      file2.txt
+ r/r 15:      file5.txt,
+ r/r 16:      file6.txt
V/V 129:      $OrphanFiles
+ -/r * 13:    OrphanFile-13
```

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.

```
sansforensics@siftworkstation: ~
$ sudo icat -f ext4 /dev/sda4 12

...   file2.txt
file5.txt,♦   file6.txt
30c~sansforensics@siftworkstation: ~
$ icat -f ext4 /dev/sda4 12 > file_recovered
Error opening image file (raw_open: file "/dev/sda4" - Permission denied)
sansforensics@siftworkstation: ~
$ sudo icat -f ext4 /dev/sda4 12 > file_recovered
bash: file_recovered: cannot overwrite existing file
sansforensics@siftworkstation: ~
$ sudo icat -f ext4 /dev/sda4 12 > file_recovered1
```

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

```
~ cd Desktop
sansforensics@siftworkstation: ~/Desktop
$ sudo extundelete --restore-all /dev/sda4
ERROR: The specified device does not have a journal file.      This program only undelete
s files from file systems with journals.extundelete: Operation not permitted when trying t
o load filesystem parameters
sansforensics@siftworkstation: ~/Desktop
```

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 :

```
sansforensics@siftworkstation: ~
$ sudo tune2fs -l /dev/sda4
tune2fs 1.46.5 (30-Dec-2021)
Filesystem volume name: <none>
Last mounted on: /mnt/sda4
Filesystem UUID: 8c2924b1-c62b-4bae-9a43-bca05d748b90
Filesystem magic number: 0xEF53
Filesystem revision #: 1 (dynamic)
Filesystem features: ext_attr resize_inode dir_index filetype extent 64bit flex_bg sparse_super large_file huge_file dir_nlink extra_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: 128
Block count: 251
Reserved block count: 12
Overhead clusters: 12
Free blocks: 232
Free inodes: 113
First block: 0
Block size: 4096
Fragment size: 4096
Group descriptor size: 64
Blocks per group: 32768
Fragments per group: 32768
Inodes per group: 128
Inode blocks per group: 8
```