PART 1. Practice the sleuthkit command line tools to analyze the image "*Linux_Financial_Case.001"*

Instructions:

1. Launch the SIFT Workstation 3. The default login username is **sansforensics**, and the default password is **forensics.**

2. 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.

Question 1. What is the command along with appropriate options you used?
⇒ mmls Linux_Financial_Case.001

3. Find the image's file system information. You have to provide the offset you got from step 2.

Question 2. What is the command along with appropriate options you used?
⇒ fsstat -o 2048 Linux_financial_Case.001

Question 3. What type of file system is the image used?
⇒ ext2

Question 4. In which scenarios, you do not have to use the offset option –o for a sleuthkit command?

⇒ The offset is used when you are carving out a specific piece of an image. If it is a primary partition beginning from slot 00, then stating a offset might not be necessary.

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

Question 5. What is the command along with appropriate options you used?
⇒ fls -o 2048 -f ext2 -m -d Linux_Financial_Case.001 > flsBody.txt

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

Question 6. What is the command along with appropriate options you used?
⇒ mactime -b flsBody.txt > flsMactime.txt

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

Question 7. What is the command along with appropriate options you used?
⇒ ils -o 2048 -f ext2 -m Linux_ Financial_Case.001

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

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

⇒ mactime -b ilsBody.txt > ilsMactime.txt

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

Question 9. Do *ilsMactime* and *flsMactme* have the same number of entries? Explain your findings.

No they do not. 'fls' traverses the directory and file name hierarchy and 'ils' traverses the metadata tables. **Mactime.txt ⇒ 7 ilsMactime.txt ⇒ 18**

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

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

⇒ istat -o 2048 -f ext2 Linux_Financial_Case.001 46082

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

Question 11. What is the command along with appropriate options you used?

⇒ icat -o 2048 -f ext2 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 12. What is the command along with appropriate options you used? Include a screenshot.
⇒ ffind -a -o 2048 -f ext2 Linux_Financial_Case.001 46082

Mark/Finance/Confidential/Earning.xls

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

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

⇒ blkcat -o 2048 -f ext2 Linux_Financial_Case.001 197122

financial statement 2014-15 **kericu inc.**

Question 14. 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.

⇒ **FALSE → this won't happen.** 'blkcat' displays the contents of a disk block [ex: blkcat imagefile.dd block_num] and 'icat' displays contents of blocks allocated to an inode [ex: icat imagefile.dd inode_num]. This won't happen possible, for example ..**[** blkcat -o 2048 Linux_Financial_Case.001 197122] & [icat -o 2048 Linux_Financial_Case.001 46082] both don't produce the same contents.

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

Question 15. What is the command along with appropriate options you used? Also provide a case scenario that shows the usefulness of *ifind*.

ifind -o 2048 -f ext2 Linux_Financial_Case.001 -d 197122 ⇒ **46082**

Case Scenario ⇒ Assuming the block number within the file system is known, 'ifind' can be ran on the block number to get the inode number of a file that may contain content you are searching for. Example, to prove that stolen credit card info matching a string search was contained in the file whos inode you could get by utilizing ifind.

PART 2. Use Autopsy to analyze "Linux_Financial_Case.001" case

---

Instructions:
Start a terminal (go to applications -> Accessories->Terminal) and type in
$ sudo autopsy
While this process is running, open a web browser point it to the URL indicated –
http://localhost:9999/autopsy

- Click on "New Case".
- Enter "linux_financial_case" as the case name, you may fill in other optional information, then click "New Case". Confirm the information and click "OK". (Names with spaces will not work.)
- Click "Add Host".
- Enter "Host1" under "Host Name" and "EST" under "Timezone" and click "Add Host".
- Confirm the information and click "ADD HOST".
- Click "Add Image".
- Click "ADD IMAGE FILE".
- Select "Disk" since this image contains a disk image (vs a partition).
- In "Location" type the path to the image file "Linux_Financial_Case.001".
- Explore the various "Import Methods".
- Review the options for checking / creating md5's and select the appropriate entry based on the information you currently have.

Question 1: Which option did you choose and why?
⇒ MD5: 7B39DE0CA146C89AD73D1D421C8F7A05
⇒ I chose to create an MD5 hash b/c this can be used for comparison against known good fingerprints

Question 2: Which Sleuthkit tool does Autopsy use to identify the partition?
⇒ **mmls [**Display the partition layout of a volume system (partition tables)]

Question 3: Which Sleuthkit tool does Autopsy use to determine the file system type of this partition?
⇒ **fsstat** [Display general details of a file system]

- Click "Add" to add the image to host 1.
- Confirm the information and click "OK".
- Now Autopsy should have mounted the partition.
- Select the partition, click "Analysis" and choose "FILE ANALYSIS" tab.
- In this mode, you can view file and directory metadata and file content.
- Click the inode of directory Mark, 23041, to see the detail information about Mark's directory.
- Go to Mark/Finance_Confidential directory, and click on Earning.xls file. In the information window at the bottom, explore the "display", "report", "export" links.

Question 4. What information do you get from "display" and "report"? What does "export" do?
⇒ **Display** → Displays contents of the file: /1/Mark/Finance_Confidential/Earning.xls (if available)
⇒ **Report** → Generates a new tab with general info(files, hashes, offset,system type), Meta Data Information(inode, allocation, group, gen id, uid, num, size, links, MAC times, Direct Blocks)
⇒ **Export** → Saves the file locally [vol2-1.Mark.Finance_Confidential.Earning.xls]

Question 5: How can you determine that a file has been deleted?
⇒ Deleted files will be highlighted red in autopsy

Click "File Type". Then click "Sort Files by Type". Then click "OK".

Question 6: How is "Sort Files by Type" formation useful in an investigation?
Answer ⇒ Separation of images, executables, documents, text files etc. Depending on the type of investigation, the analyst can prioritize his/her work based on which file types are the best use of time. In addition, hash databases are utilized to flag files that are known to be bad and ignores files that are known to be good.

To view sorted file, click on "View Sorted Files" and copy/paste the URL into a browser.
Click on "Meta Data" and provide a valid inode number.

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

Click on the "Image Details" tab and read the information given.
Question 8: What information can you get from this window? Where does Autopsy get this information from?
⇒ File System Information / MetaData Information / Content Information / Block Group Information
⇒ Autopsy gets this information from the image & possibly the sleuth kit tool 'fsstat'

- Click the "Close" tab to close the "Analyze", and you will be back to the "Host Manager".
- Select the partition and click "File Activity Timelines"
- Click "Create Data File".
- Select the disk partition and click "OK", and confirm the information.

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

- Click "OK".
- Now we have the body file, we can sort the body file to generate a timeline.
- Autopsy this version has a bug for creating a timeline. To fix it, you will run "sudo cp /usr/bin/mactime /usr/bin/mactime-sleuthkit".

- In the “Create Timeline” window, you can select the starting and ending dates of file activity that you want to see, for example, from Jan. 2015 to Jan. 2016.
- Note the sorted information. Click the links at the top to look at other dates.

Question 10: How might this timeline information be useful for forensic investigations?
⇒ The timeline creates a sequential list of MAC times to determine when any image files where created, modified or accessed. This information can be a helpful tool for analysis, but more importantly for proving a sequence of events in court.

- Click “Close”.
- Back to “Host Manager”]
- Explore any other features of Autopsy & Sleuthkit you would like to.
- After you are done, close the case by clicking “Close Host” then “Close Case”. You can reopen the case to work on it later if you choose to.

Part 3. Report

- Now you are familiar with Autopsy/Sleuthkit features.
- Read the case scenario again, provide your statement and evidence that indicates Frank may have read Earning.xls. Why is Frank able to read a confidential document and how to change permissions, so that “Earning.xls” file will not be accessible by others?

Evidence: Below is a screenshot from Autopsy timeline.
⇒ On Nov 6 2015, activity by both Mark and Frank is normal.
⇒ On Nov 13 2015[the next time the Earning.xls file was accessed and modified], activity was abnormal.
⇒ The Earning.xls is being accessed from **Frank’s** server folder.

⇒ /l/Frank/appointments4 → /media/skm/lpar-usb/Mark/Finance_confidential/Earning.xls

Fri	Nov 13 2015 12:48:32	43	.a..	r/rrw-rw-r--	1001	1001	46082	/1/Mark/Finance_Confidential/Earning.xls
Fri	Nov 13 2015 12:57:49	57	m...	l/lrwxrwxrwx	1000	1000	7683	/1/Frank/appointments4 -> /media/skm/ipar-usb/Mark/Finance_Confidential/Earning.xls (deleted)
Fri	Nov 13 2015 12:57:54	57	.a..	l/lrwxrwxrwx	1000	1000	7683	/1/Frank/appointments4 -> /media/skm/ipar-usb/Mark/Finance_Confidential/Earning.xls (deleted)
Fri	Nov 13 2015 12:58:25	57	..c.	l/lrwxrwxrwx	1000	1000	7683	/1/Frank/appointments4 -> /media/skm/ipar-usb/Mark/Finance_Confidential/Earning.xls (deleted)
Fri	Nov 13 2015 12:58:50	4096	.a..	d/drwxrwxr-x	2002	2002	7681	/1/Frank

File Permissions:
With **lrwxrwxrwx**, ‘l’ stands for symbolic link. this is a special pointer allowing multiple filenames to point to the same Unix file. **rwxrwxrwx i**s a repeated set of permissions, **rwx** is the the maximum permissions allowed. According to this, Frank may have utilized these permissions to point to Mark’s confidential finance/earnings file in order to secretly read it. By removing the symbolic link ‘l’, Frank will lose these privileges and the file will be better protected. Additionally, this file can set to ‘read only’ privileges to avoid this happening in the future.