**CIS-387: Digital Forensics (4 credits)**

**With Dr. Jinhua Guo**

**Lab 8 – File Permissions Analysis for Financial Case**

**Demetrius Johnson**

**November 30, 2022**

# **INSTRUCTIONS**

## 1. Launch Autopsy from the Toolbox folder on the desktop.

## 2. Select > Create New Case

Graphical user interface, text, application, chat or text message

Description automatically generated

## 3. Name the case Financial Case.

## 4. Use the default Base Directory (Desktop) where Autopsy will store the Case data in Desktop\Financial Case.

Graphical user interface, text, application, email

Description automatically generated

## 5. Enter the Case Number as 001 and enter your name as Examiner.

## 6. Click Finish. You will see the "Add Data Source" window.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

## 7. Select Data source type. Choose Disk Image or VM File. Browse and select the path to the file Linux Financial Case.001.

Graphical user interface, application, Word

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

## 8. Select the Ingest Modules. Leave all modules checked. Click Next, then click Finish. NOTE: Ingest modules analyze the data in a data source. They perform all the analysis of the files and parse their contents.

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

## 9. You will see "Analyzing files from Financial Case.001" status at the lower right corner of the Autopsy Screen.

A picture containing chart

Description automatically generated

# **Explore image contents; answer case questions:**

## a) Browse through Data Sources>Linux Financial Case.001>vol2, what is the Inode number of Earning.xls? What is the data block number that contains Earning.xls file content? (Hint: click the File Metadata tab at the bottom-right pane.)

Graphical user interface, text, application

Description automatically generated

The Inode numbers is shown in the next screenshot:

Graphical user interface, text, application

Description automatically generated

Here is the block (group 6) where the data for the file is located; it has only a length of 1, meaning it is only 1 block long:

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

## b) When was Earning.xls last modified?

Graphical user interface, text, application

Description automatically generated

## c) What are the user and group IDs associated with Earning.xls in the directory 'Mark > Finance\_Confidential'?

Graphical user interface, text, application

Description automatically generated

## d) What are the user and group IDs associated with files in the 'Frank' directory? Is it different from the user and group ID for Earning.xls in Mark's directory?

Here is Frank’s directory meta data, notice that his directory contains 2 links, meaning the directory is linked to 2 different Inodes:

Text

Description automatically generated with low confidence

Here is the group number, and UID and GID for Mark’s financial document file:

Graphical user interface, text

Description automatically generated

As shown I the screenshots, the group IDs for **Earnings.xsl** file and **Frank** directory are not the same.

## e) What permissions do 'others' have for the Mark directory and Finance\_Confidential directory? Hint: click fold in the tree view, then click [current folder] in the Table view, look for the information from File Metadata.

Mark’s directory has the following permissions:

Graphical user interface, text, application

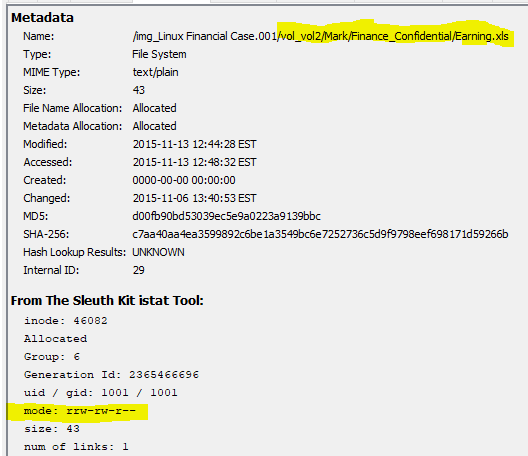
Description automatically generated

And Finance Confidential subdirectory under Mark’s directory has the following permissions:

Graphical user interface, text

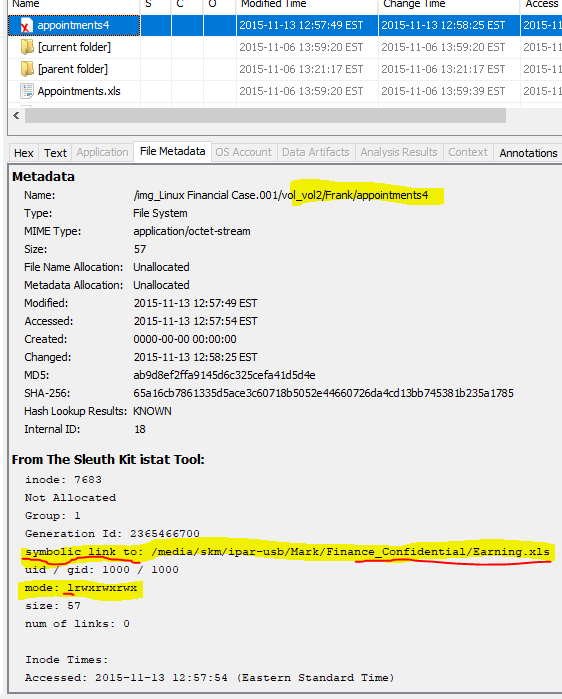
Description automatically generated

## f) What access permission do 'others' have for Earning.xls file? Does this mean that Frank could read this file?



So, since both the parent and subdirectories have the same file permissions: drwxrwx-x, then we know that for “others” user group has r-x permissions; so that means Frank could in fact (and any other user for that matter) read the data file, which has r-- permissions for others; so essentially, anyone can read the financial document.

## g) Do you see any deleted file in Frank’s directory that could be a soft link of Earning.xls? If yes, what is the file name of the soft link? Hint: The first character in the 'Mode' column will be 'l' and the deleted files are marked by a red cross.



As we can see in the screenshot above, Frank directory does contain a deleted softlink file that is linked to the Earnings.xls file inside of Mark🡪Finance\_Confidential directories; this softlink would only work if Frank has permission to read the file – and as discussed earlier, the file can be read by anyone according to the permissions of the file and all directories to which it belongs.

# Summary/Reflection

According to the analysis, Frank had in his directory a softlink file which points to the path where Mark’s confidential earnings file is held. The permissions are set such that anyone can read the file in Mark’s directory and subdirectories, and the directories allow for read access as well meaning that the softlink that Frank had would work for viewing the financial earnings. It can be reasonably inferred that at the very least Mark has potentially inappropriately set permissions on his files and directories and that Frank created a softlink to that file to the financial file to read it. It does not mean that this is definite because someone else in the IT administration with admin privileges could have changed the permissions and Frank potentially could have just been taking advantage of the fact that he had permission to read the file.

Overall, I got more familiar with file permissions in Linux (EXT-4). Also, recently I have been setting up my home network with things such as “remote desktop connection” and an NAS server and other network drives on my machines that require me to set the permissions appropriately. I am using windows, thus I am dealing with the NTFS file system and the built in permission syntax, which is very much similar in syntax and function as EXT4.