# CIS/ECE 387 Fall 2018 Lab8

Due: **12/3/2018**

## ACTIVITY: CASE Study2 (Linux MAC Time and access control) with AUTOPSY

## IMAGE FILE

Download the image file, Linux Financial Case.001, on canvas under the Files->Labs->Lab8 folder.

## GOAL

In this exercise, you will practice the forensic tool Autopsy and use it to examine files' ownership and permissions given a device image.

## CASE SCENARIO

Mark Watson works as a Director of Finance at an advertising firm. He has been accused of illegally providing the annual financial report (*Earnings.xls*) to a contractor, Frank Lewis, to influence his next contract with the firm. Mark has denied sharing any document with Frank.

The IT administrator informed you that there is a Linux-based file server in the office where all employees save the official documents. Mark and Frank each have their own folders on this server.

You have been given the image of the hard drive, *Financial Case.001*, to find the evidence to prove that Frank has the permission to read the financial report *Earnings.xls*.

## INSTRUCTIONS

**Create the case**

1. Launch **Autopsy** from the Toolbox folder on the desktop.
2. Select > *Create New Case*
3. Name the case *Financial Case*.
4. Use the default Base Directory (Desktop) where Autopsy will store the Case data in *Desktop\Financial Case*.
5. Enter the Case Number as *001* and enter your name as *Examiner*.
6. Click *Finish*. You will see the "Add Data Source" window.

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

8. Select your local time zone and click *Next*. You will see Ingest (processing) modules window.
   NOTE: When you acquire a computer as evidence it is important to make note of the computer's time and time zone, especially if you need to correlate evidence from different time zones. You should never assume the time or time zone on a computer is correct.

9. 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 of the analysis of the files and parse their contents.

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

NOTE: Once you have the case created, you can reopen it at any time in Autopsy using *Open Existing Case*, then choose *Desktop\Financial Case\Financial Case.aut file*.

**Explore the image contents and answer questions about the case**

The Tree Viewer shows the discovered folders by the data sources they come from, as well as a list of files in the folders. It is located on the left side of the Autopsy screen. Each folder in the tree on the left shows how many items are contained within it in parenthesis after the directory name.

Explore the "Data Sources" tree on the left side of the Autopsy screen. When you select a directory in the tree, the files in that directory are shown in the Table Viewer located on the top right of the Autopsy screen. It displays the files and their corresponding attributes such as time, path, size, checksum, etc.

Use that information to answer the **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.)

b) When was Earning.xls last modified?

c) What are the user and group IDs associated with Earning.xls in the directory 'Mark > Finance_Confidential'? Hint: check the Table Viewer on the top right pane.

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?

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.

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

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

## Report

Your report should include the activity log (the steps you take or the commands you run) with some screenshots and/or outputs, and a brief reflection on what you learned (one or two paragraphs).

Please submit your lab report to Canvas under the "lab8" assignment folder. Each group just submits one report.