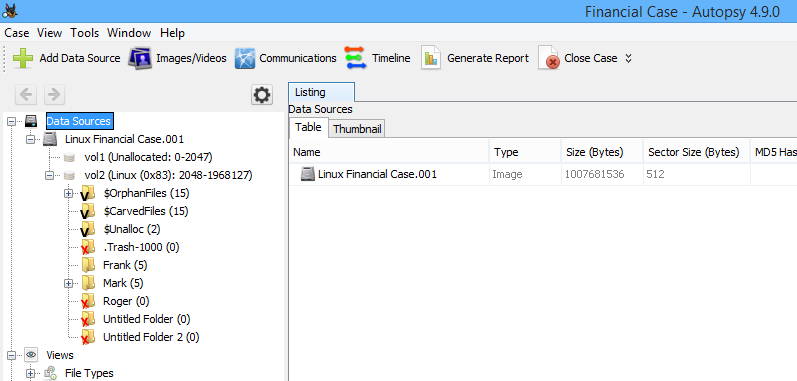
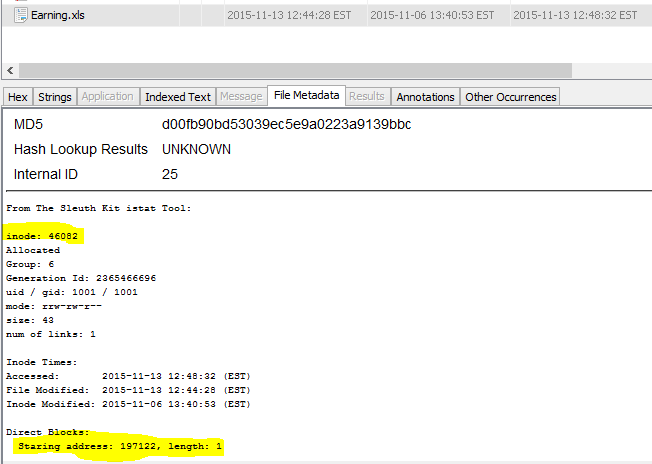
By : Marco Seman and Jason Lu

Lab 8 - Financial Case



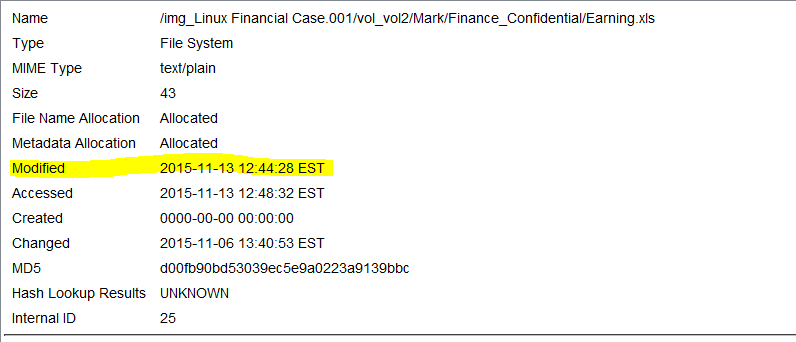
a) Browse through Data Sources>Linux Financial Case.001>vol2, what is the Inode number of Earning.xls? What is the data block number that contains Earning.xls file content? (Hint: click the File Metadata tab at the bottom-right pane.)

* The Inode number for earnings is 46082. The data block numbers starting address is 197122 at length one.



b) When was Earning.xls last modified?

Earnings was last modified on: 2015-11-13 12:44:28 EST

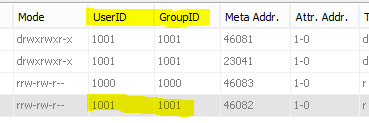


c) What are the user and group IDs associated with Earning.xls in the directory 'Mark >

Finance\_Confidential'? Hint: check the Table Viewer on the top right pane.

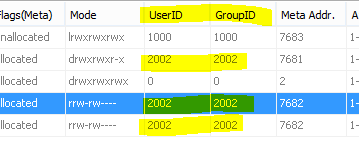
UserID: 1001

GroupID: 1001



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?

Franks: User and group ID are 2002 and 1000 compared to Mark’s whose IDs are 1001.

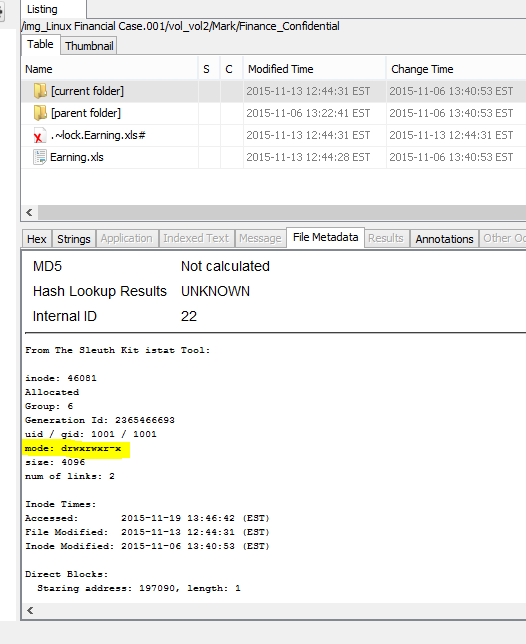


e) What permissions do 'others' have for the Mark directory and Finance\_Confidential directory?

Hint: click fold in the tree view, then click [current folder] in the Table view, look for the information from File Metadata.

The Permission for Finance\_Confidential file are: drwxrwxr-x meaning that all user can read the file (since all of them contain “r”), execute the file (since all of them contain “x”), and only the owner and its members are allowed to write to the directory (the first two contain “w” write access).

Others have Read and Execute Permissions for this directory.

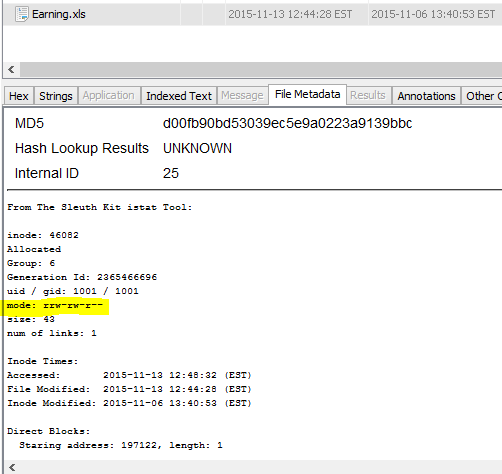


f) What access permission do 'others' have for Earning.xls file? Does this mean that Frank could read this file?

The access to the earnings file is: rrw-rw-r-- meaning that all users can read the file, only the owner and its members can write to the file, but nobody can execute the file.

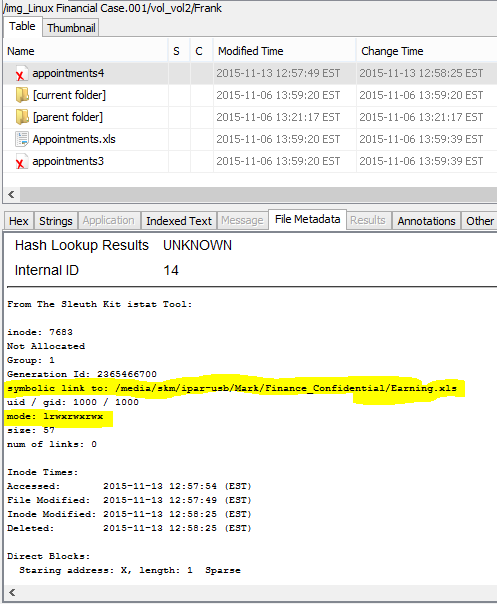
Others are only allowed to read the file.

Yes, Frank would be able to read the Earnings.xls 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.

Yes, appointments4 may has a soft link to the earnings.xls file since it contains a symbolic link to the earnings.xls. The file permissions for appointments4 is lrwxrwxrwx where l indicates a link to that file.



What we Learned:

In lab 8, we learned quite a bit on who has access to a certain file or folder using autopsy. When looking at the permissions, we learned that every file begins with a permissions string. For example, the letter d at the beginning of the file permissions means the file named is in the right most column in the directory. The letter l means that the file is a link to the file (like a windows shortcut, whereas it isn’t the actual file). After the first character, there are then 9 strings of letters that are followed. The first 3 characters indicate owner’s file permissions, the 4-7 characters indicate group permissions, and the last three characters indicate others file permissions. We also learned that r = read, w = write, and x = execute. If there is a “-” symbol, that user does not have access to that certain missing category.