CIS-387: Digital Forensics (4 credits)

With Dr. Jinhua Guo

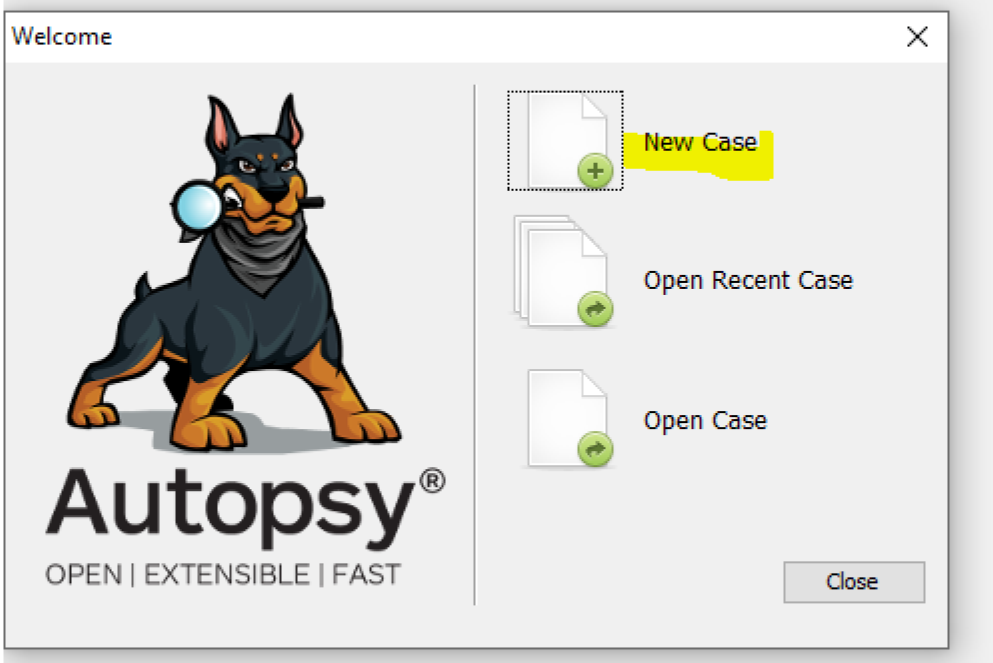
Lab 8 – File Permissions Analysis for Financial Case

Demetrius Johnson

November 30, 2022

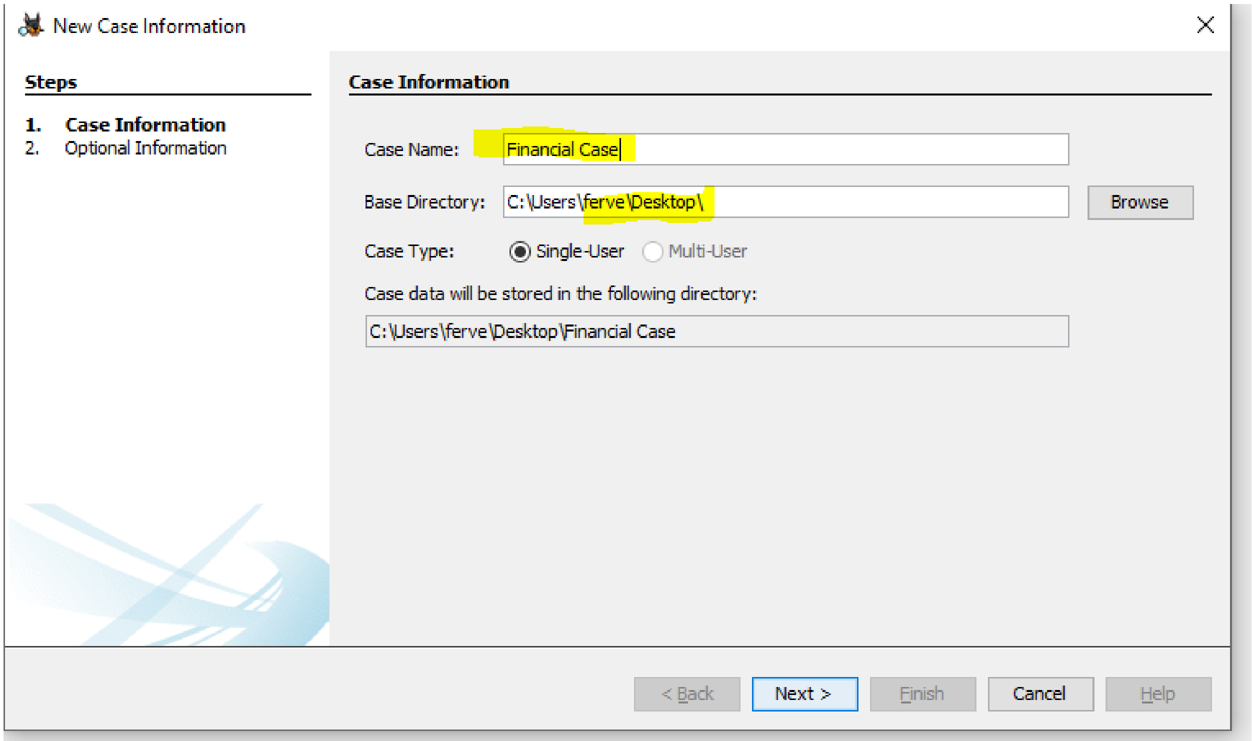
INSTRUCTIONS

1. Launch Autopsy from the Toolbox folder on the desktop.
2. Select > Create New Case



3. Name the case Financial Case.

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



Case Name: Financial Case

Base Directory: C:\Users\ferve\Desktop\

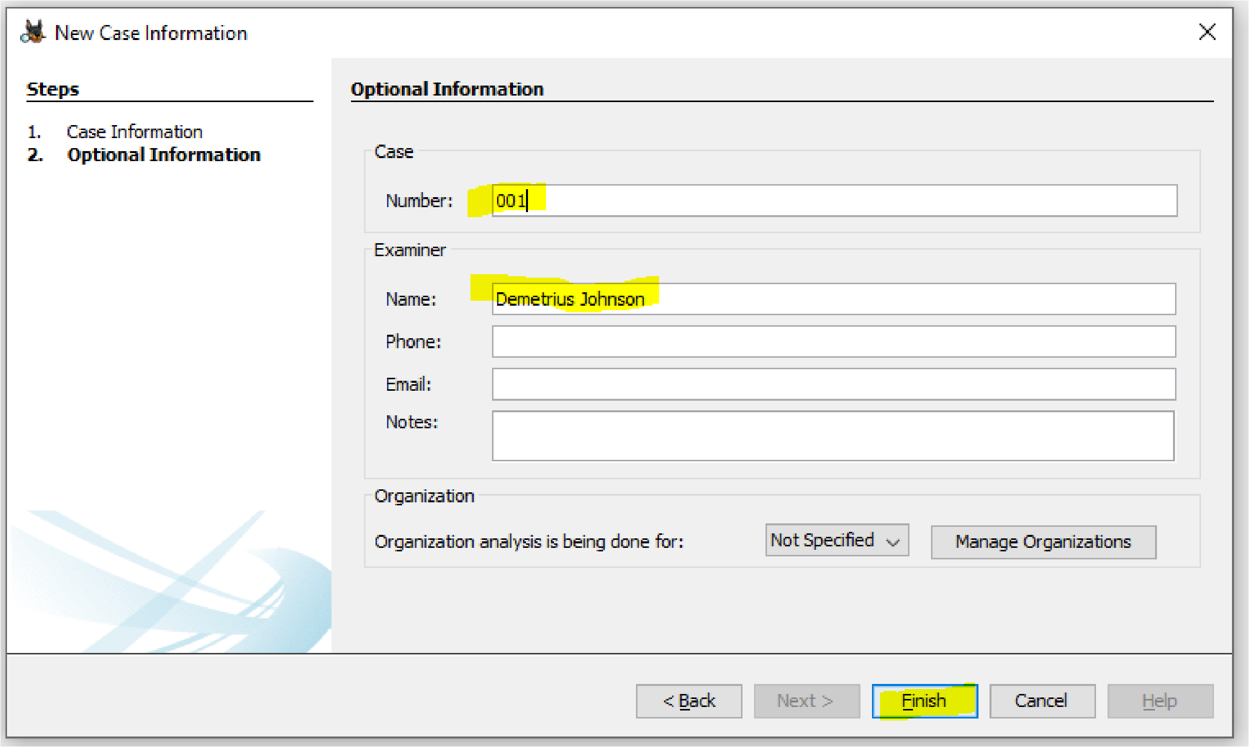
Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

C:\Users\ferve\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.



New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: 001

Examiner

Name: Demetrius Johnson

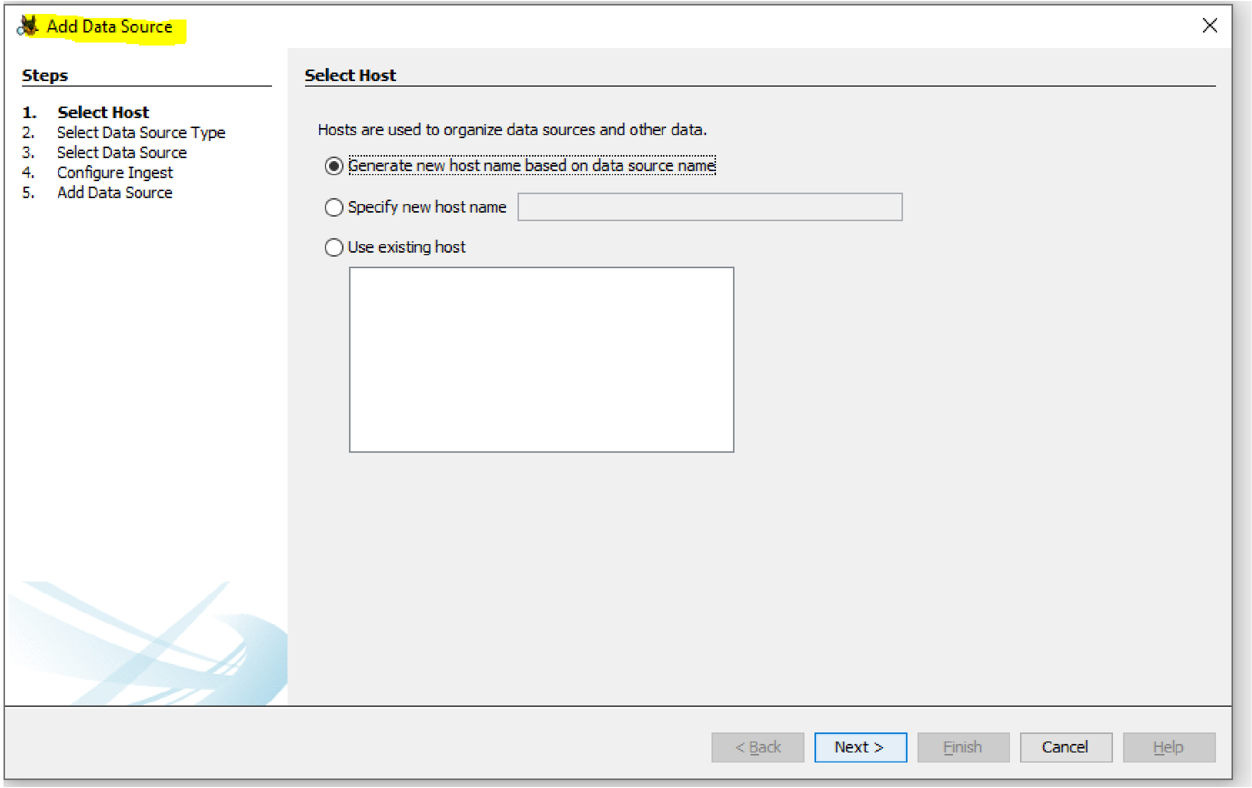
Phone:

Email:

Notes:

Organization

Organization analysis is being done for: Not Specified



Add Data Source

Steps

1. **Select Host**
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

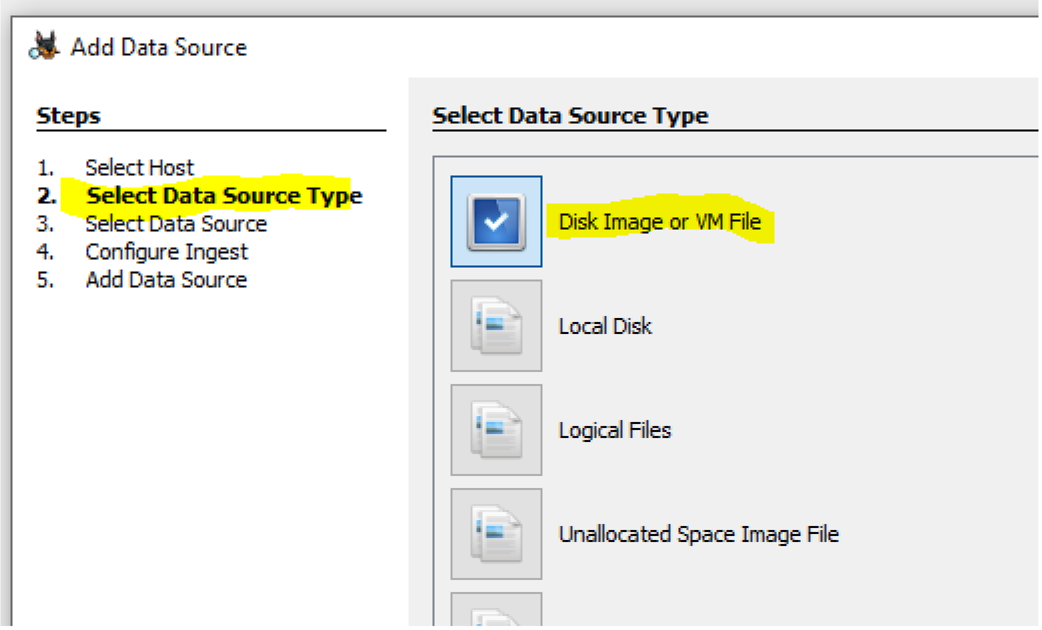
Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

○ Specify new host name

○ Use existing host

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



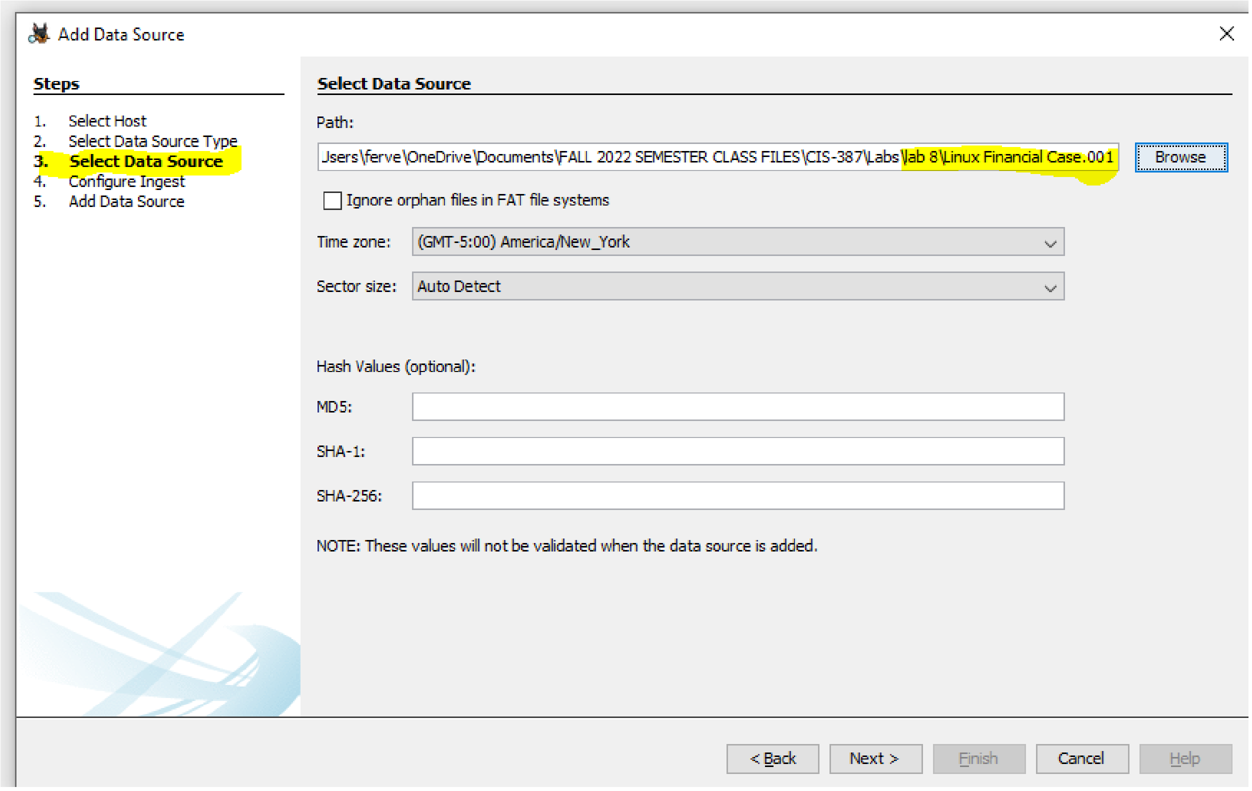
Add Data Source

Steps

1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source Type

☑ Disk Image or VM File



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path:

Jsers\ferve\OneDrive\Documents\FALL 2022 SEMESTER CLASS FILES\CIS-387\Labs\lab 8\Linux Financial Case.001

□ Ignore orphan files in FAT file systems

Time zone: (GMT-5:00) America/New_York

Sector size: Auto Detect

Hash Values (optional):

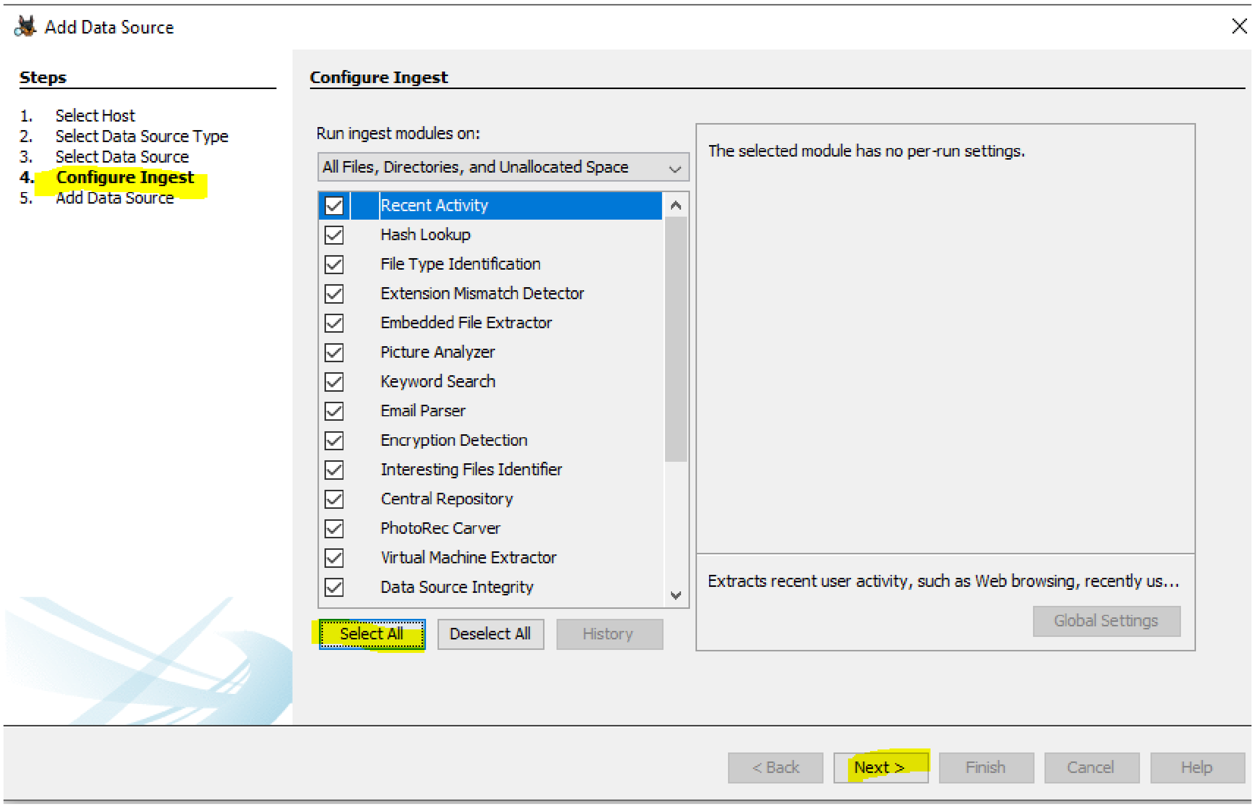
MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

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.



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

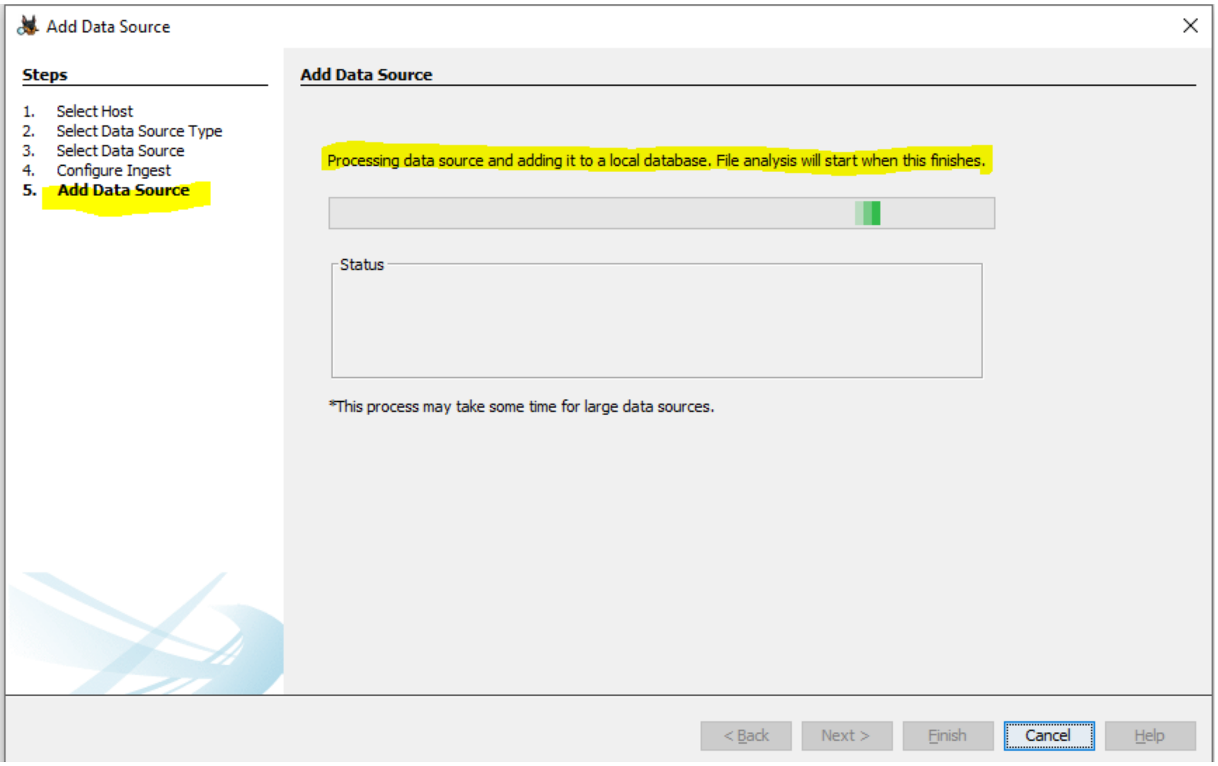
Configure Ingest

Run ingest modules on: All Files, Directories, and Unallocated Space

- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Extension Mismatch Detector
- ☑ Embedded File Extractor
- ☑ Picture Analyzer
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Encryption Detection
- ☑ Interesting Files Identifier
- ☑ Central Repository
- ☑ PhotoRec Carver
- ☑ Virtual Machine Extractor
- ☑ Data Source Integrity

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...



Add Data Source

Steps

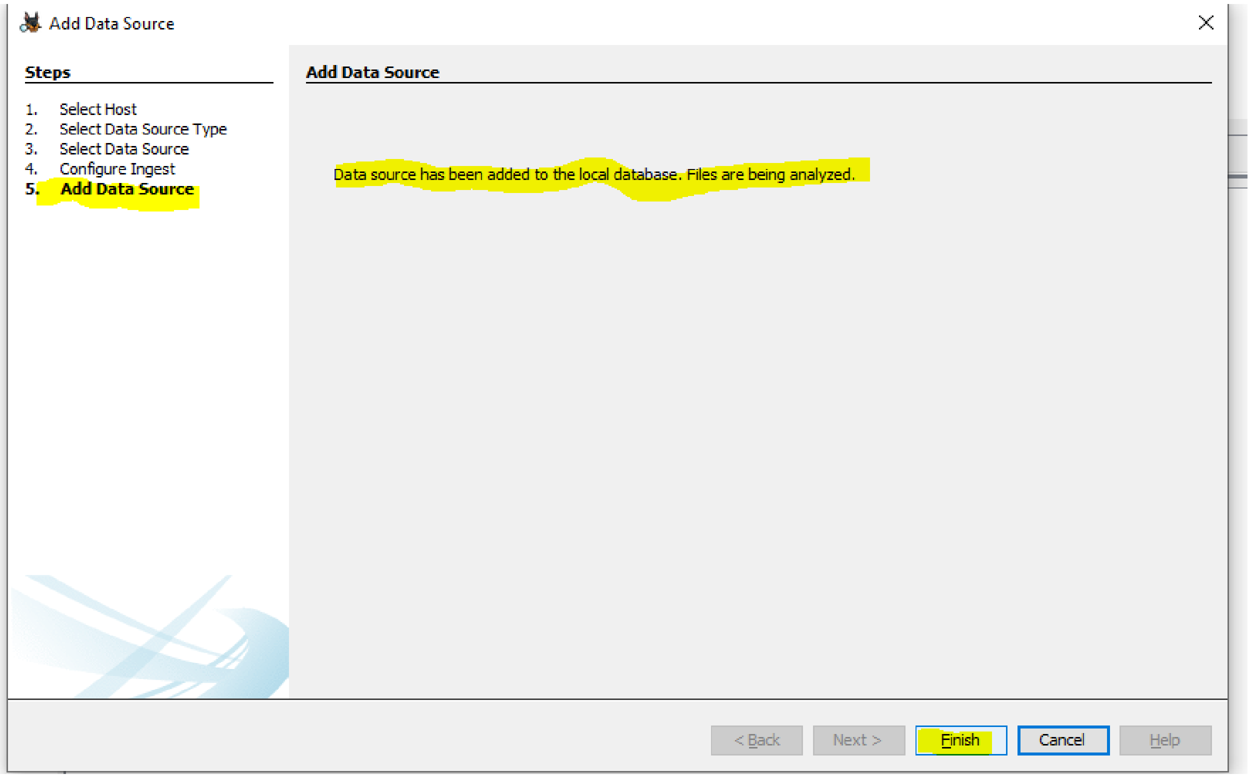
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. **Add Data Source**

Add Data Source

Processing data source and adding it to a local database. File analysis will start when this finishes.

Status

*This process may take some time for large data sources.



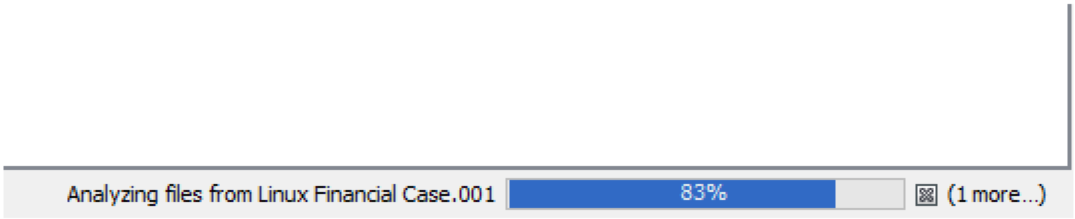
Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. **Add Data Source**

Add Data Source

Data source has been added to the local database. Files are being analyzed.

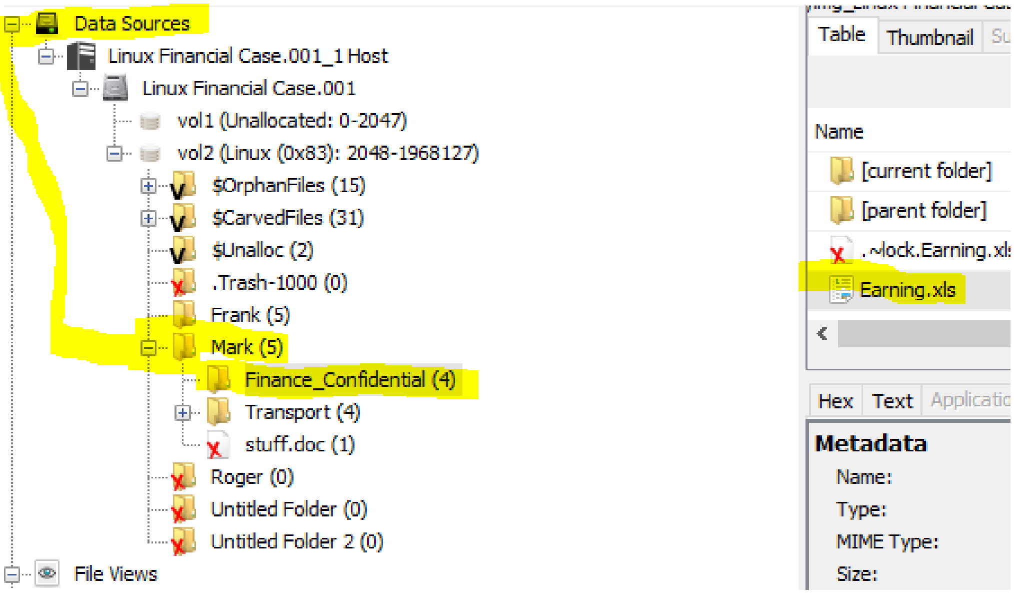
9. You will see "Analyzing files from Financial Case.001" status at the lower right corner of the Autopsy Screen.



Analyzing files from Linux Financial Case.001 83% (1 more...)

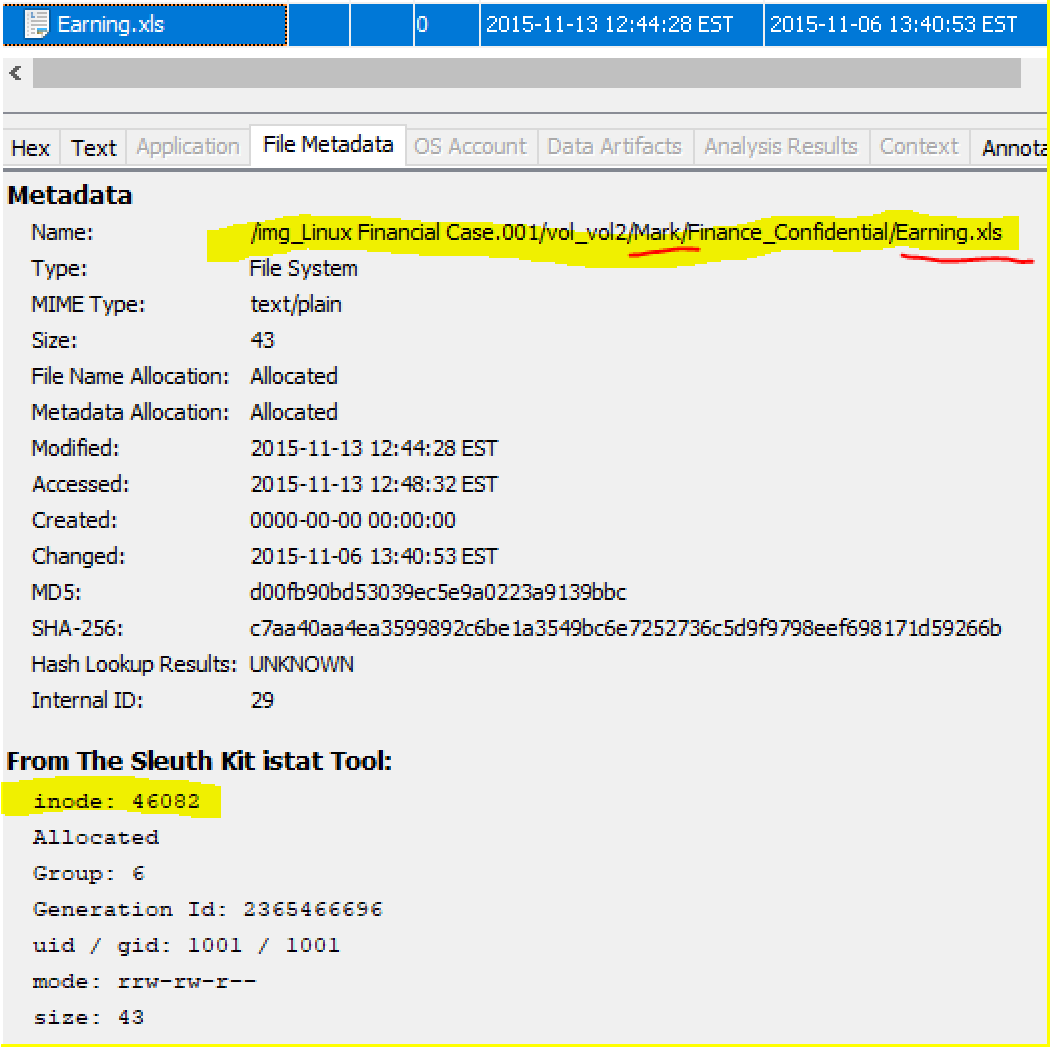
Explore image contents; answer case questions:

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.)



Data Sources
Linux Financial Case.001_1 Host
Linux Financial Case.001
vol1 (Unallocated: 0-2047)
vol2 (Linux (0x83): 2048-1968127)
$OrphanFiles (15)
$CarvedFiles (31)
$Unalloc (2)
.Trash-1000 (0)
Frank (5)
Mark (5)
Finance_Confidential (4)
Transport (4)
stuff.doc (1)
Roger (0)
Untitled Folder (0)
Untitled Folder 2 (0)
File Views

The Inode numbers is shown in the next screenshot:



Earning.xls			0	2015-11-13 12:44:28 EST	2015-11-06 13:40:53 EST

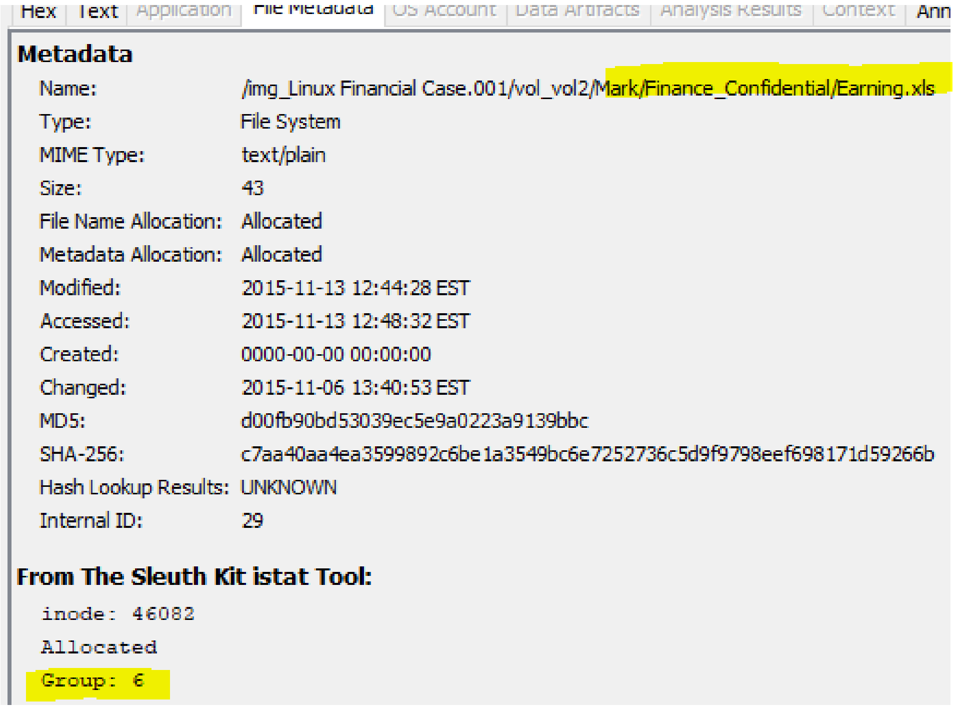
Metadata

Name:	/img_Linux Financial Case.001/vol_vol2/Mark/Finance_Confidential/Earning.xls
Type:	File System
MIME Type:	text/plain
Size:	43
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2015-11-13 12:44:28 EST
Accessed:	2015-11-13 12:48:32 EST
Created:	0000-00-00 00:00:00
Changed:	2015-11-06 13:40:53 EST
MD5:	d00fb90bd53039ec5e9a0223a9139bbc
SHA-256:	c7aa40aa4ea3599892c6be1a3549bc6e7252736c5d9f9798eef698171d59266b
Hash Lookup Results:	UNKNOWN
Internal ID:	29

From The Sleuth Kit istat Tool:

```
inode: 46082
Allocated
Group: 6
Generation Id: 2365466696
uid / gid: 1001 / 1001
mode: rrw-rw-r--
size: 43
```

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:

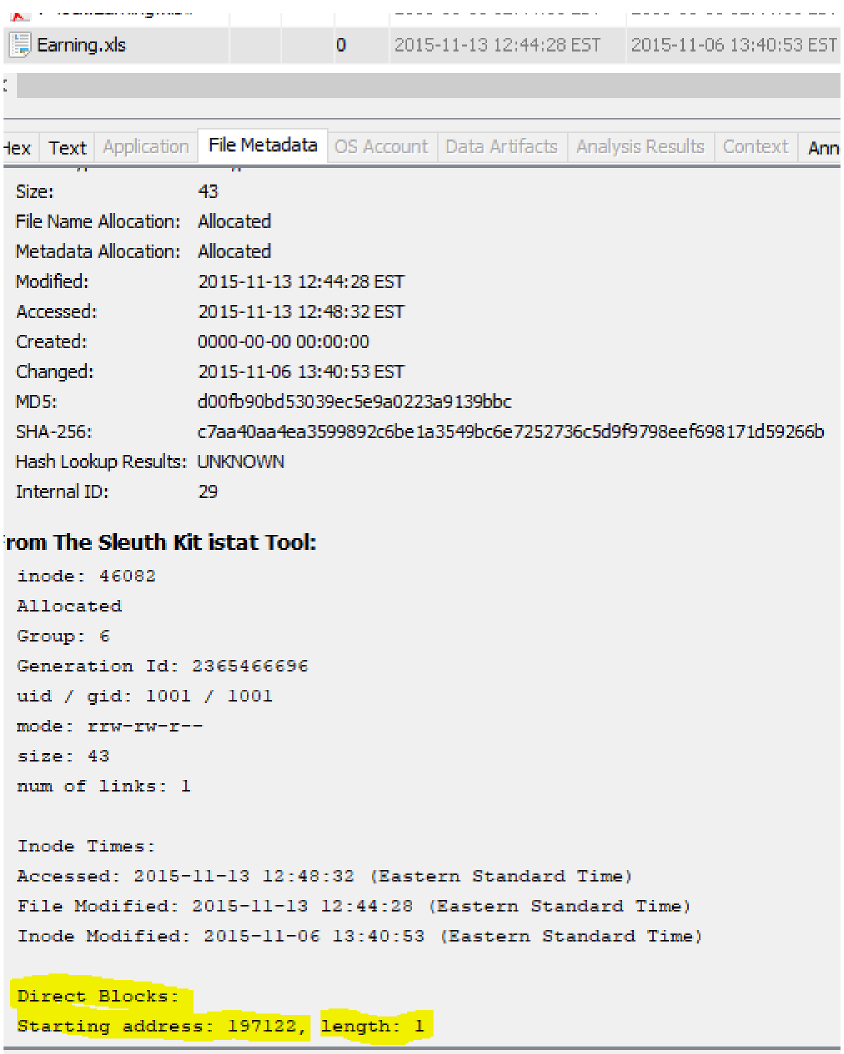


Metadata

```
Name:                   /img_Linux Financial Case.001/vol_vol2/Mark/Finance_Confidential/Earning.xls
Type:                   File System
MIME Type:              text/plain
Size:                   43
File Name Allocation:   Allocated
Metadata Allocation:    Allocated
Modified:               2015-11-13 12:44:28 EST
Accessed:               2015-11-13 12:48:32 EST
Created:                0000-00-00 00:00:00
Changed:                2015-11-06 13:40:53 EST
MD5:                    d00fb90bd53039ec5e9a0223a9139bbc
SHA-256:                c7aa40aa4ea3599892c6be1a3549bc6e7252736c5d9f9798eef698171d59266b
Hash Lookup Results:    UNKNOWN
Internal ID:            29
```

From The Sleuth Kit istat Tool:

```
inode: 46082
Allocated
Group: 6
```



Earning.xls 0 2015-11-13 12:44:28 EST 2015-11-06 13:40:53 EST

Size: 43
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2015-11-13 12:44:28 EST
Accessed: 2015-11-13 12:48:32 EST
Created: 0000-00-00 00:00:00
Changed: 2015-11-06 13:40:53 EST
MD5: d00fb90bd53039ec5e9a0223a9139bbc
SHA-256: c7aa40aa4ea3599892c6be1a3549bc6e7252736c5d9f9798eef698171d59266b
Hash Lookup Results: UNKNOWN
Internal ID: 29

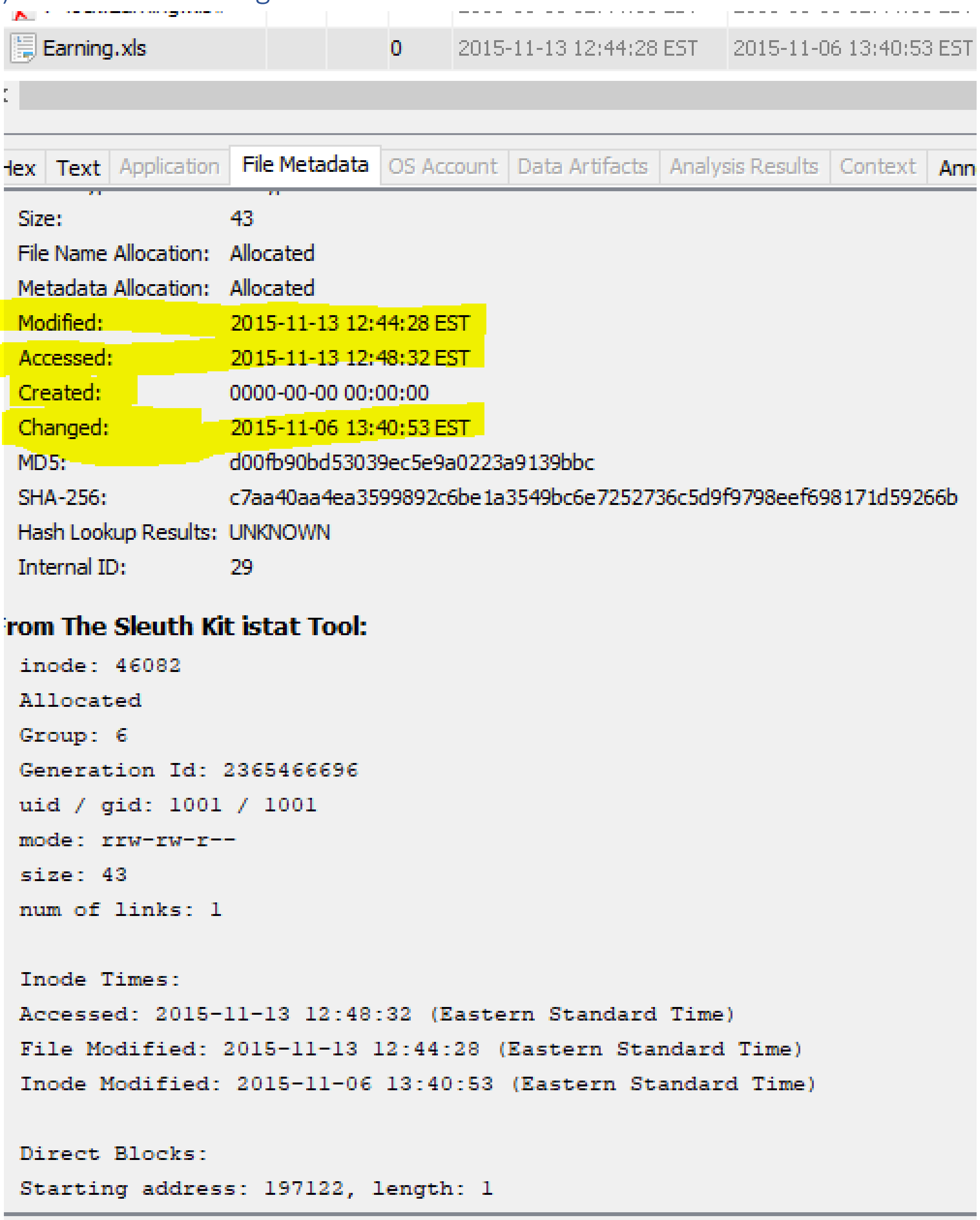
rom The Sleuth Kit istat Tool:

```
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 (Eastern Standard Time)
File Modified: 2015-11-13 12:44:28 (Eastern Standard Time)
Inode Modified: 2015-11-06 13:40:53 (Eastern Standard Time)

Direct Blocks:
Starting address: 197122, length: 1
```

b) When was Earning.xls last modified?



Earning.xls	0	2015-11-13 12:44:28 EST	2015-11-06 13:40:53 EST

Size:	43
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2015-11-13 12:44:28 EST
Accessed:	2015-11-13 12:48:32 EST
Created:	0000-00-00 00:00:00
Changed:	2015-11-06 13:40:53 EST
MD5:	d00fb90bd53039ec5e9a0223a9139bbc
SHA-256:	c7aa40aa4ea3599892c6be1a3549bc6e7252736c5d9f9798eef698171d59266b
Hash Lookup Results:	UNKNOWN
Internal ID:	29

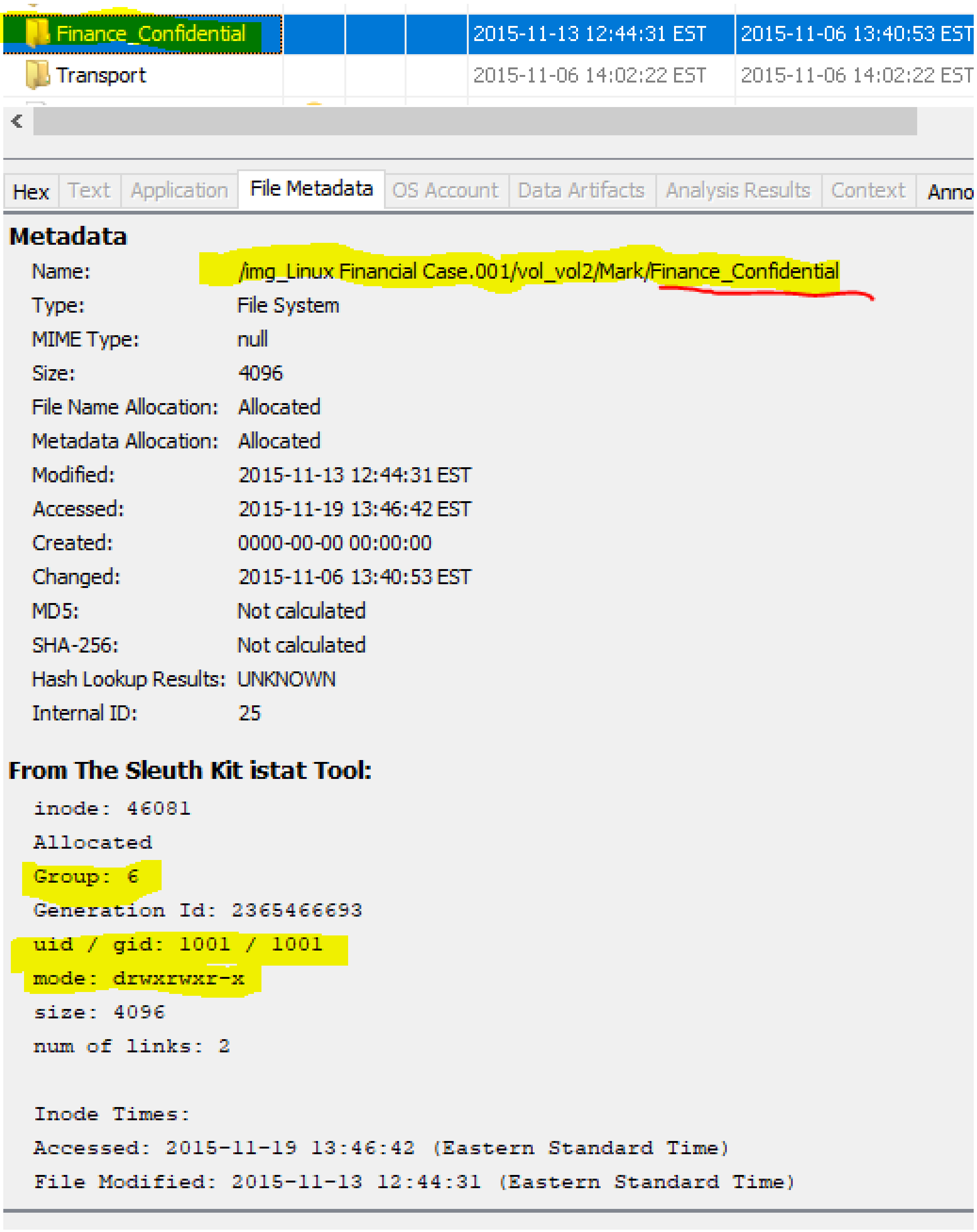
rom The Sleuth Kit istat Tool:

```
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 (Eastern Standard Time)
File Modified: 2015-11-13 12:44:28 (Eastern Standard Time)
Inode Modified: 2015-11-06 13:40:53 (Eastern Standard Time)

Direct Blocks:
Starting address: 197122, length: 1
```

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



Finance_Confidential			2015-11-13 12:44:31 EST	2015-11-06 13:40:53 EST
Transport			2015-11-06 14:02:22 EST	2015-11-06 14:02:22 EST

Metadata

Name:	/img_Linux Financial Case.001/vol_vol2/Mark/Finance_Confidential
Type:	File System
MIME Type:	null
Size:	4096
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2015-11-13 12:44:31 EST
Accessed:	2015-11-19 13:46:42 EST
Created:	0000-00-00 00:00:00
Changed:	2015-11-06 13:40:53 EST
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	25

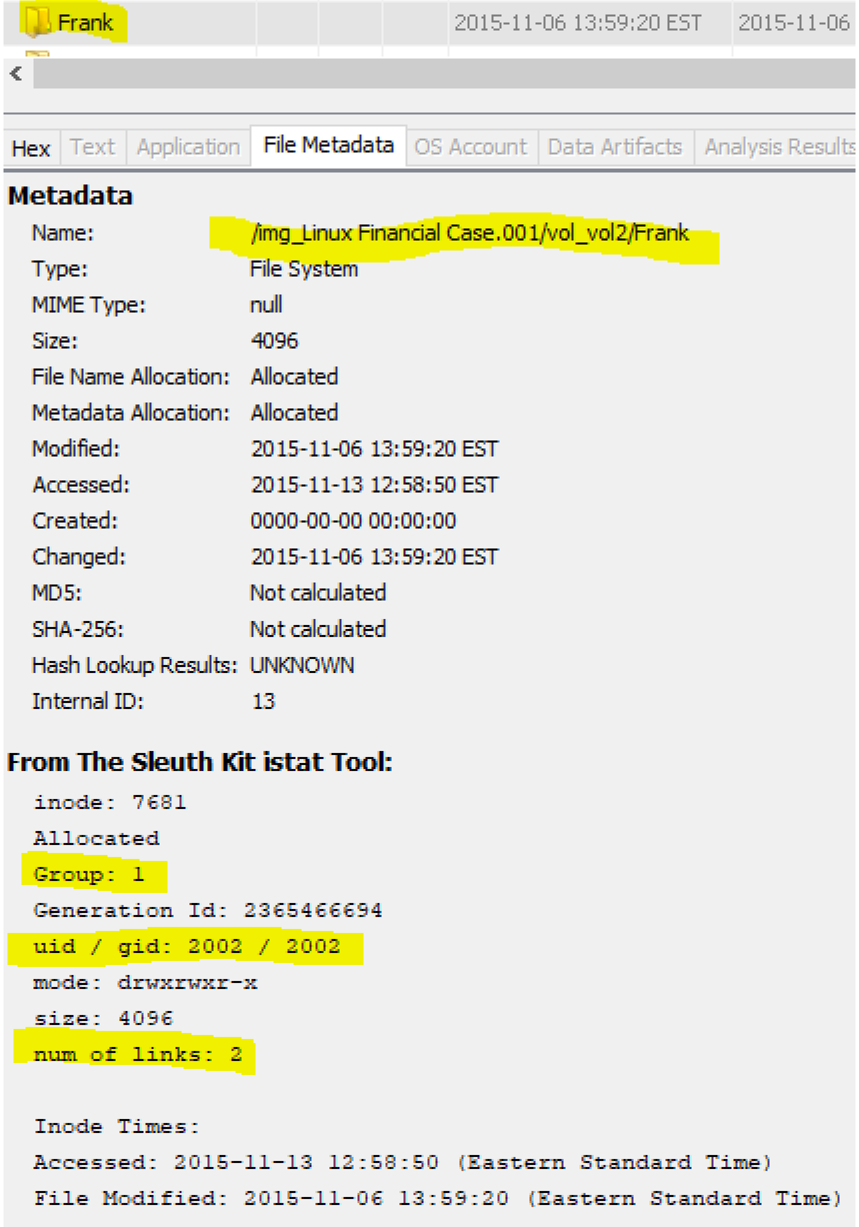
From The Sleuth Kit istat Tool:

```
inode: 46081
Allocated
Group: 6
Generation Id: 2365466693
uid / gid: 1001 / 1001
mode: drwxrwxr-x
size: 4096
num of links: 2

Inode Times:
Accessed: 2015-11-19 13:46:42 (Eastern Standard Time)
File Modified: 2015-11-13 12:44:31 (Eastern Standard Time)
```

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:



Metadata

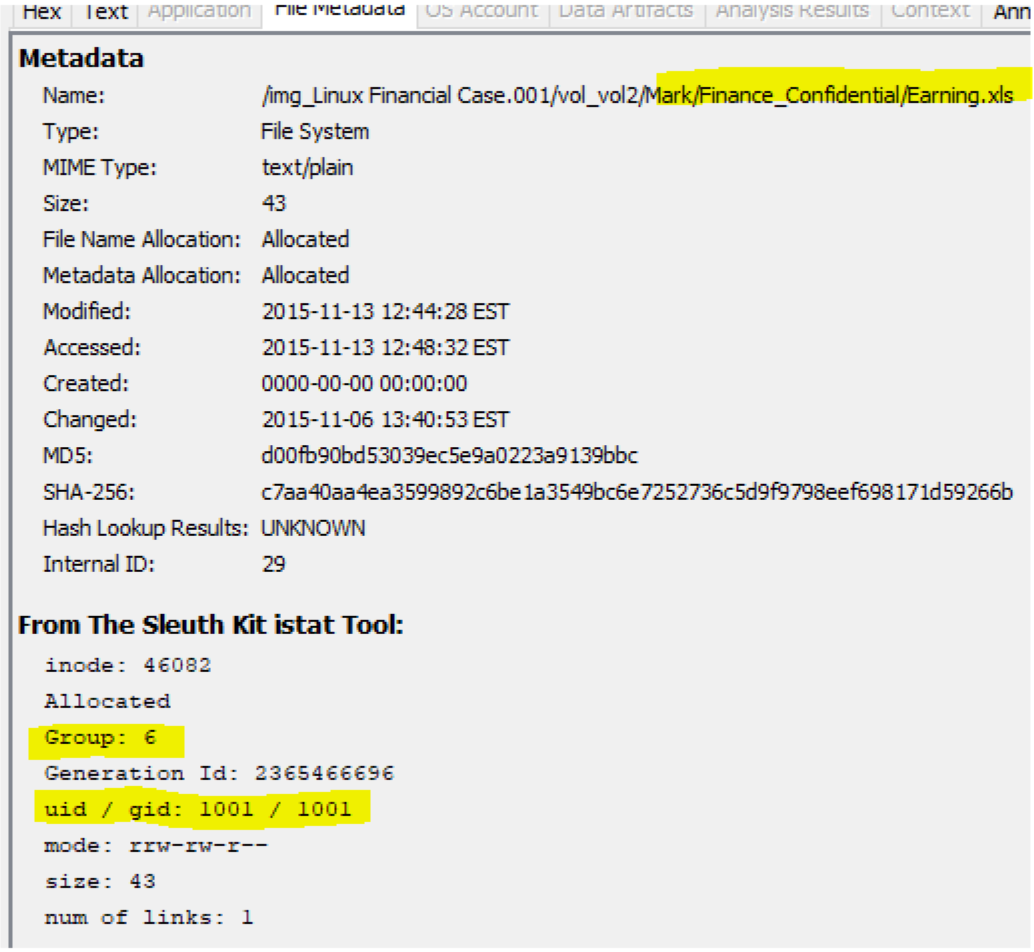
Name:	/img_Linux Financial Case.001/vol_vol2/Frank
Type:	File System
MIME Type:	null
Size:	4096
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2015-11-06 13:59:20 EST
Accessed:	2015-11-13 12:58:50 EST
Created:	0000-00-00 00:00:00
Changed:	2015-11-06 13:59:20 EST
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	13

From The Sleuth Kit istat Tool:

```
inode: 7681
Allocated
Group: 1
Generation Id: 2365466694
uid / gid: 2002 / 2002
mode: drwxrwxr-x
size: 4096
num of links: 2

Inode Times:
Accessed: 2015-11-13 12:58:50 (Eastern Standard Time)
File Modified: 2015-11-06 13:59:20 (Eastern Standard Time)
```

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



Metadata

Name:	/img_Linux Financial Case.001/vol_vol2/Mark/Finance_Confidential/Earning.xls
Type:	File System
MIME Type:	text/plain
Size:	43
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2015-11-13 12:44:28 EST
Accessed:	2015-11-13 12:48:32 EST
Created:	0000-00-00 00:00:00
Changed:	2015-11-06 13:40:53 EST
MD5:	d00fb90bd53039ec5e9a0223a9139bbc
SHA-256:	c7aa40aa4ea3599892c6be1a3549bc6e7252736c5d9f9798eef698171d59266b
Hash Lookup Results:	UNKNOWN
Internal ID:	29

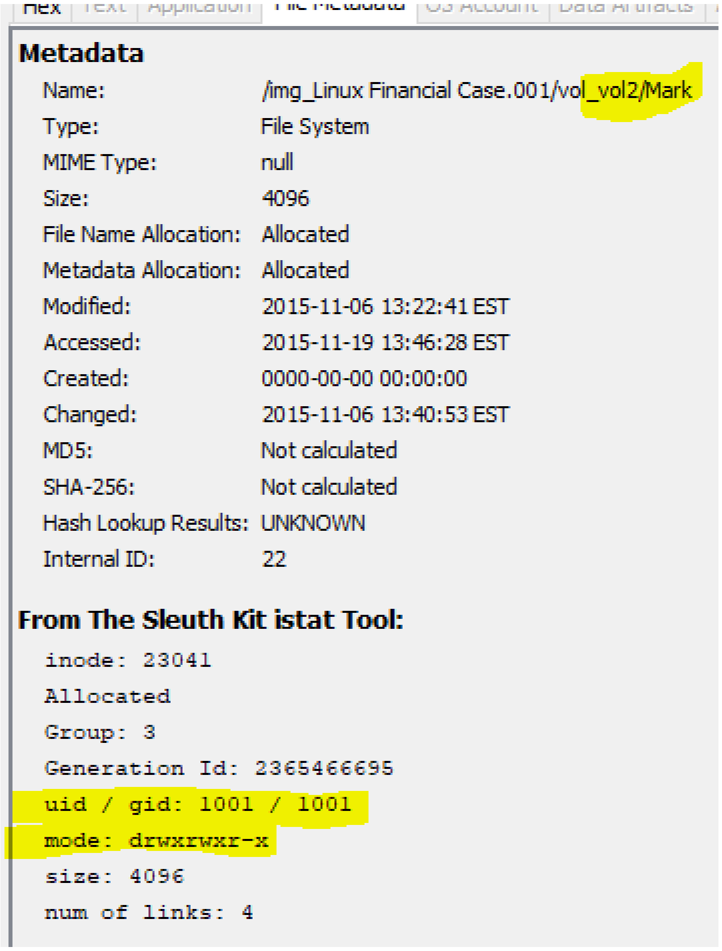
From The Sleuth Kit istat Tool:

```
inode: 46082
Allocated
Group: 6
Generation Id: 2365466696
uid / gid: 1001 / 1001
mode: rrw-rw-r--
size: 43
num of links: 1
```

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:



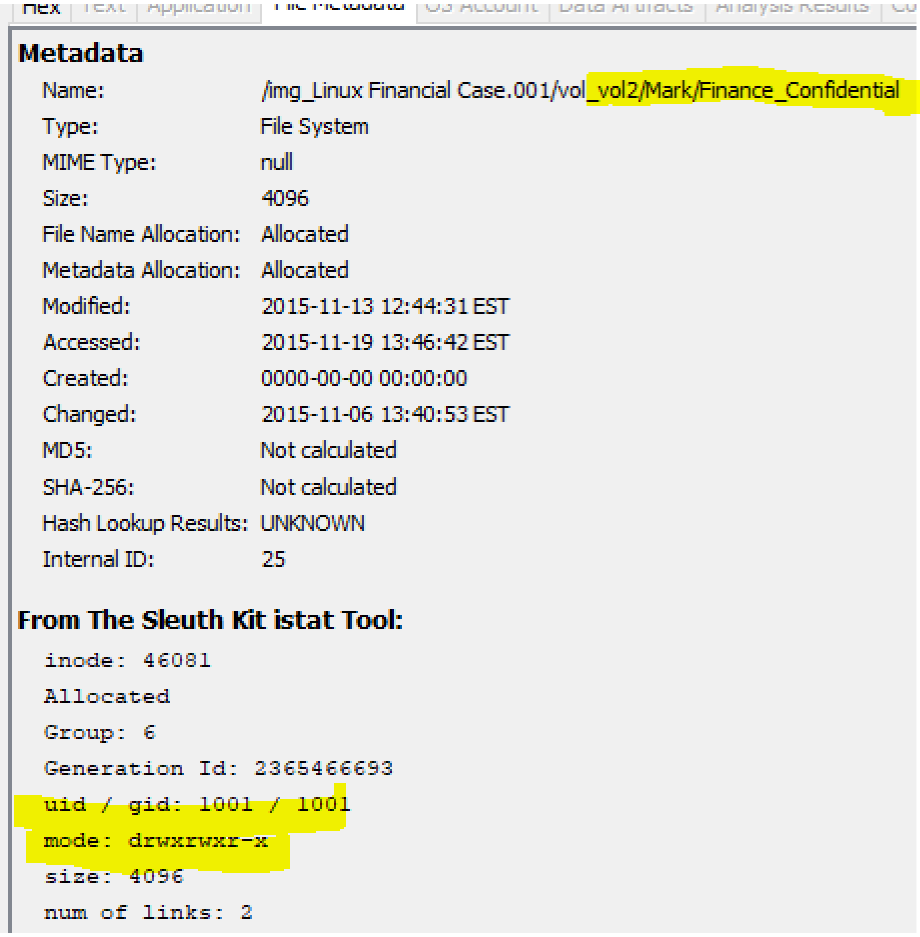
Metadata

Name:	/img_Linux Financial Case.001/vol_vol2/Mark
Type:	File System
MIME Type:	null
Size:	4096
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2015-11-06 13:22:41 EST
Accessed:	2015-11-19 13:46:28 EST
Created:	0000-00-00 00:00:00
Changed:	2015-11-06 13:40:53 EST
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	22

From The Sleuth Kit istat Tool:

```
inode: 23041
Allocated
Group: 3
Generation Id: 2365466695
uid / gid: 1001 / 1001
mode: drwxrwxr-x
size: 4096
num of links: 4
```

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



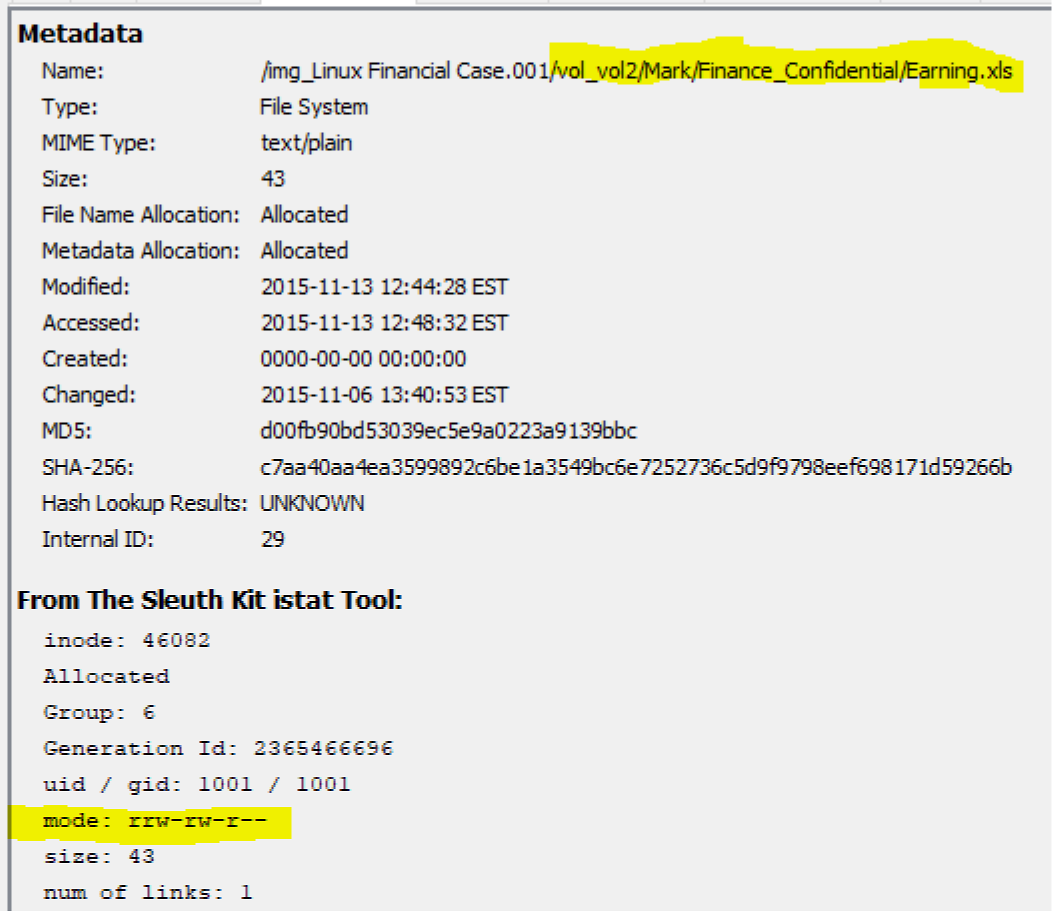
Metadata

Name:	/img_Linux Financial Case.001/vol_vol2/Mark/Finance_Confidential
Type:	File System
MIME Type:	null
Size:	4096
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2015-11-13 12:44:31 EST
Accessed:	2015-11-19 13:46:42 EST
Created:	0000-00-00 00:00:00
Changed:	2015-11-06 13:40:53 EST
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	25

From The Sleuth Kit istat Tool:

```
inode: 46081
Allocated
Group: 6
Generation Id: 2365466693
uid / gid: 1001 / 1001
mode: drwxrwxr-x
size: 4096
num of links: 2
```

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



Metadata

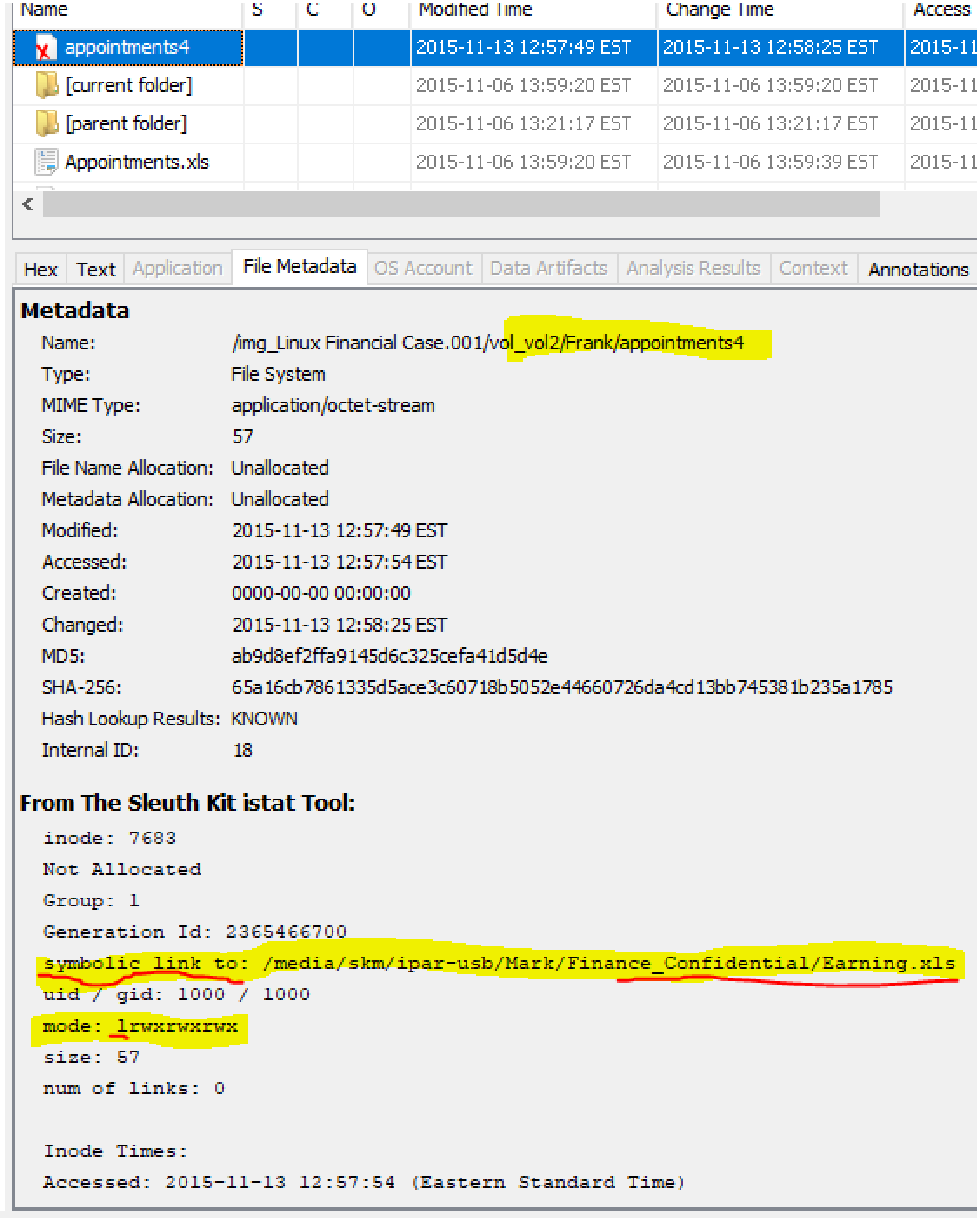
```
Name:                   /img_Linux Financial Case.001/vol_vol2/Mark/Finance_Confidential/Earning.xls
Type:                   File System
MIME Type:              text/plain
Size:                   43
File Name Allocation:   Allocated
Metadata Allocation:    Allocated
Modified:               2015-11-13 12:44:28 EST
Accessed:               2015-11-13 12:48:32 EST
Created:                0000-00-00 00:00:00
Changed:                2015-11-06 13:40:53 EST
MD5:                    d00fb90bd53039ec5e9a0223a9139bbc
SHA-256:                c7aa40aa4ea3599892c6be1a3549bc6e7252736c5d9f9798eef698171d59266b
Hash Lookup Results:    UNKNOWN
Internal ID:            29
```

From The Sleuth Kit istat Tool:

```
inode: 46082
Allocated
Group: 6
Generation Id: 2365466696
uid / gid: 1001 / 1001
mode: rrw-rw-r--
size: 43
num of links: 1
```

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.



Name	S	C	O	Modified Time	Change Time	Access
appointments4				2015-11-13 12:57:49 EST	2015-11-13 12:58:25 EST	2015-11
[current folder]				2015-11-06 13:59:20 EST	2015-11-06 13:59:20 EST	2015-11
[parent folder]				2015-11-06 13:21:17 EST	2015-11-06 13:21:17 EST	2015-11
Appointments.xls				2015-11-06 13:59:20 EST	2015-11-06 13:59:39 EST	2015-11

Metadata

Name:	/img_Linux Financial Case.001/vol_vol2/Frank/appointments4
Type:	File System
MIME Type:	application/octet-stream
Size:	57
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2015-11-13 12:57:49 EST
Accessed:	2015-11-13 12:57:54 EST
Created:	0000-00-00 00:00:00
Changed:	2015-11-13 12:58:25 EST
MD5:	ab9d8ef2ffa9145d6c325cefa41d5d4e
SHA-256:	65a16cb7861335d5ace3c60718b5052e44660726da4cd13bb745381b235a1785
Hash Lookup Results:	KNOWN
Internal ID:	18

From The Sleuth Kit istat Tool:

```
inode: 7683
Not Allocated
Group: 1
Generation Id: 2365466700
symbolic link to: /media/skm/ipar-usb/Mark/Finance_Confidential/Earning.xls
uid / gid: 1000 / 1000
mode: lrwxrwxrwx
size: 57
num of links: 0

Inode Times:
Accessed: 2015-11-13 12:57:54 (Eastern Standard Time)
```

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.