**Name: Huynh Lam Student ID: 13264763 Date: 10/10/2021 Activity No.: Cmp1/03**

In this week’s Lab we will use The Sleuth Kit (TSK) tools to gather disk information.

You may have to run apt-get update on your ubuntu before you install fsstat and fls

We will examine a USB with a FAT Partition and a NTFS Partition

We will delete some files and then try and recover them.

Reminder: To get the Thorough mark, you need to answer as a Forensics Investigator. (Week 1 module)

# Preparation 1 – Prepare the Evidence on the USB

Insert your small USB Flash Drive.

It will mount as a Drive letter, typically E:\Drive.

**Warning! We will ERASE ALL FILES!**

Set the volume size to 20 MB. Click next. Click next.

Select the FAT file system. Name the Volume Forensics F

Set the volume size to 20 MB. Click next. Click next.

Select the NTFS file system. Name the Volume Forensics N

Download and copy the Week 5 (Metadata) Sample files from UTS Online to each partition.

Delete the IMAG\* file in both partitions.

Also delete the Trade\_Secrets.txt file in both partitions.

Preparation 2 – Acquire the Image of the USB Volume

We use ProDiscover (week 2) to acquire images of the two Disk volumes (FAT 16 and NTFS).

If the ProDiscover Licence has expired, uninstall the program and install it again from the Week 2 download.

Do NOT acquire the whole disk.

Mount your USB with the two partitions, Forensics F and Forensics N.

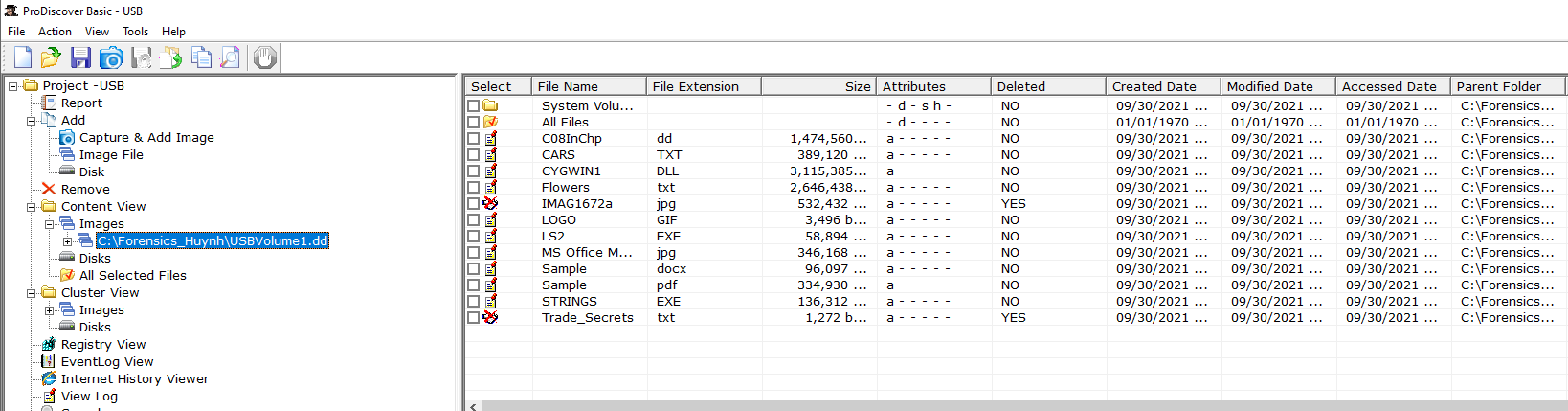
Run ProDiscover. Fill out the Project details. Call the project USB.

Select your Forensics \_yourname folder as the destination. Call the image file USBVolume1.dd

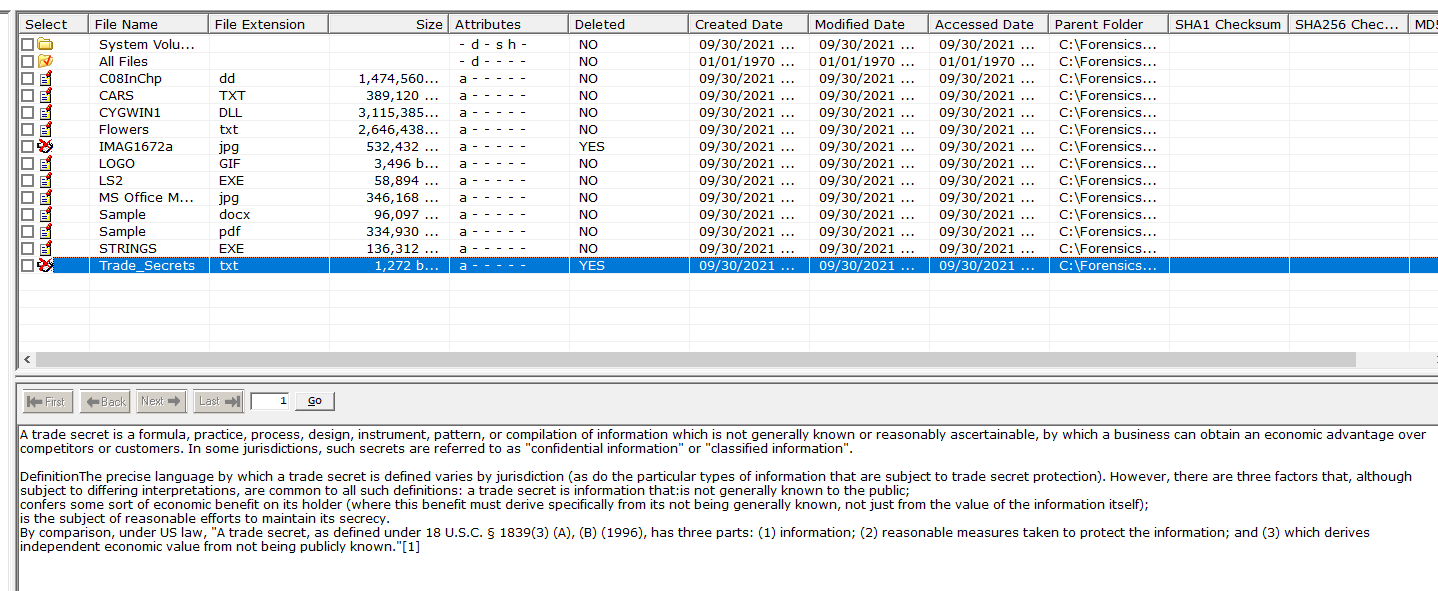
Acquire the Partition.

Confirm your image appears under Content View in the left panel.

Take a screen shot of the Project tree and list of files for your report.



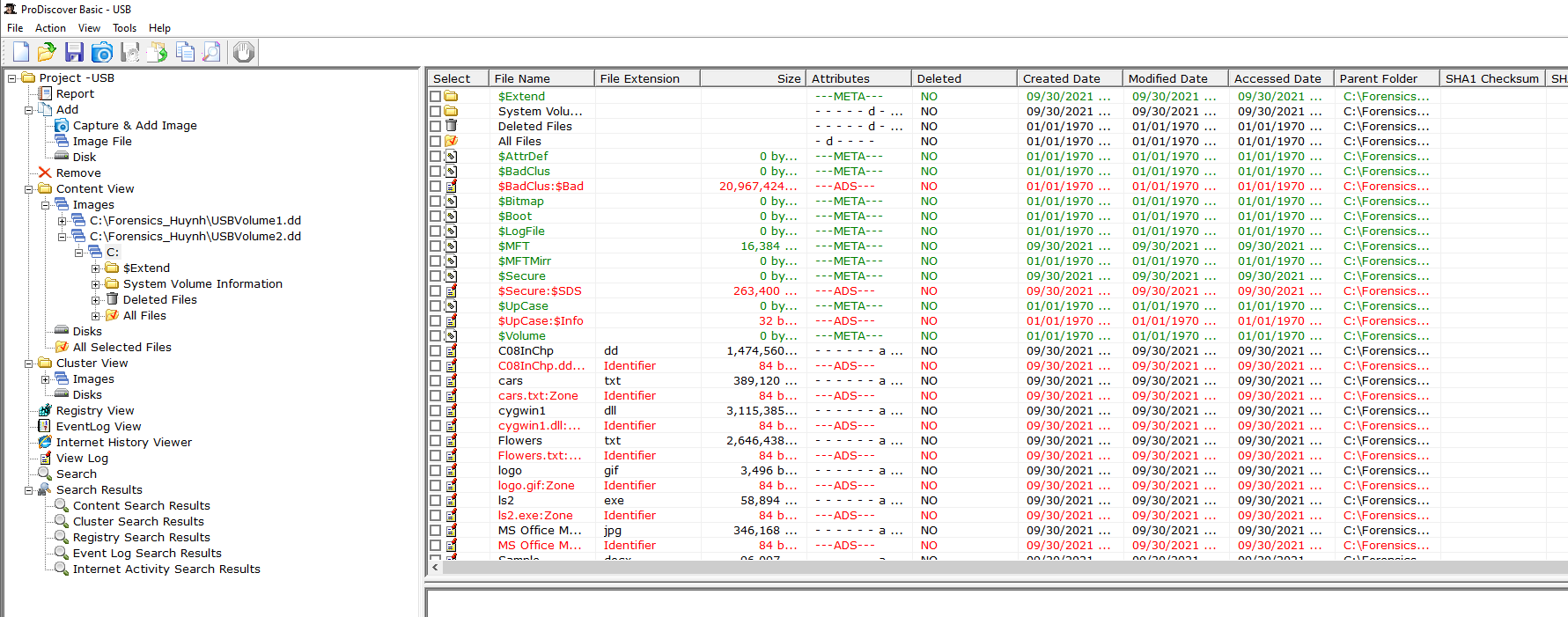
Select the deleted file Trade\_Secrets.txt Confirm you can see the contents in the view pane. \_ \_



Repeat to acquire your Forensics N Volume. Call it USBVolume2.dd

Now with NTFS you need to select the C:\Drive to see the files.

Take a screen shot of the Project tree and list of files for your report.



Also the deleted files have been moved to a separate folder.

Select the deleted file Trade\_Secrets.txt Confirm you can see the contents in the view pane. \_ \_\_

Text, application

Description automatically generated

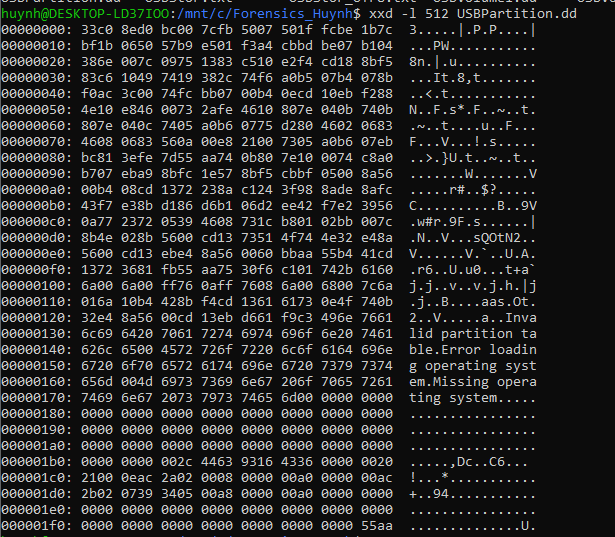
# Q1) MBR Partition Analysis of the USB

Download to your Forensics folder the USBPartition.dd file from Canvas.

Run ubuntu. Change to your Forensics folder.

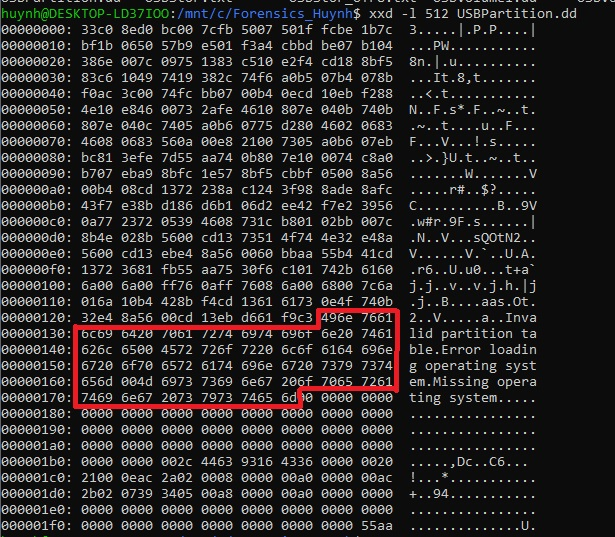
Run xxd -l 512 to view the partition file.

Confirm the result looks like the MBR in the Lecture slides. \_\_\_\_\_\_

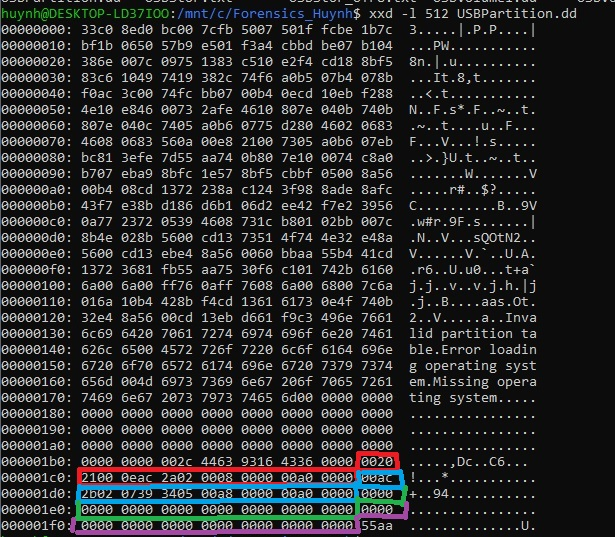


Take a screenshot of the MBR to upload. Identify the following:

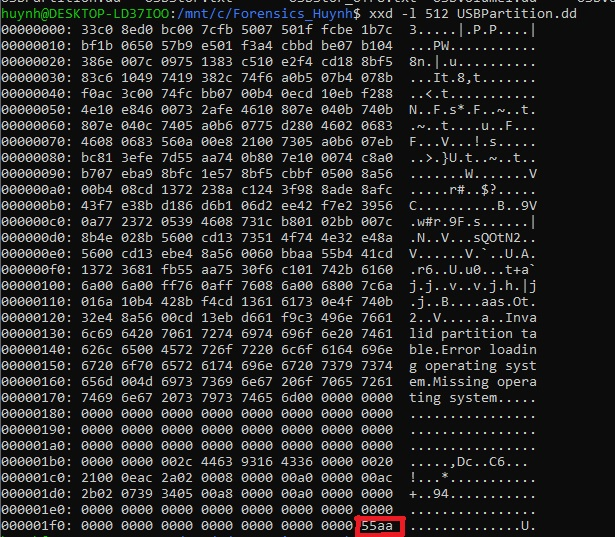
* the last error message,



* the four partition types \_\_ \_\_\_\_\_\_\_\_\_\_



* the four partitions boot status,
  + Boot status of these partitions are all 00 at the 0E column
* the MBR signature. \_\_\_\_\_\_\_\_\_



Indicate the location and the value for each. You can use Hex values or circle the item on the screen shot with a label. For the partition types, include the hex and the matching name from the lecture slide.

# Q2) GPT Partition Analysis of your Hard Drive

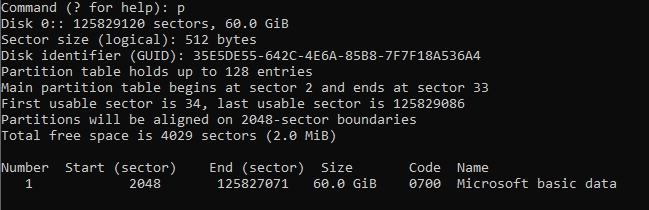
Download gdisk64.exe from Canvas into your Forensics Folder.

To run gdisk type gdisk64.exe 0: (Run cmd.exe as Administrator)

To see the disk partition (GPT), type p (p is for print)

You should see a list of disk partitions.

Take a screen shot for upload.



What is the size and name of the first partition?

* Name is Microsoft basic data
* Size is 60 GB

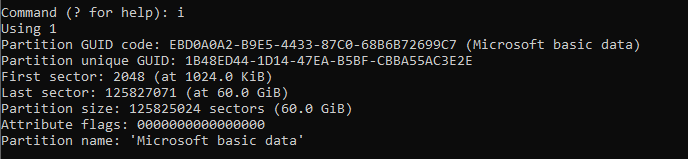
To see the first partition on this disk

type i (i is for information.)

Then type 1 (1 is the partition number )

Confirm you see partition GUID information \_\_\_.

Take a screen shot for upload.



Type q to quit gdisk.

# Q3) Identify the USB FAT file system using fsstat

Confirm you have the USBVolume1.dd file in your Forensics folder from Preparation 2 above.

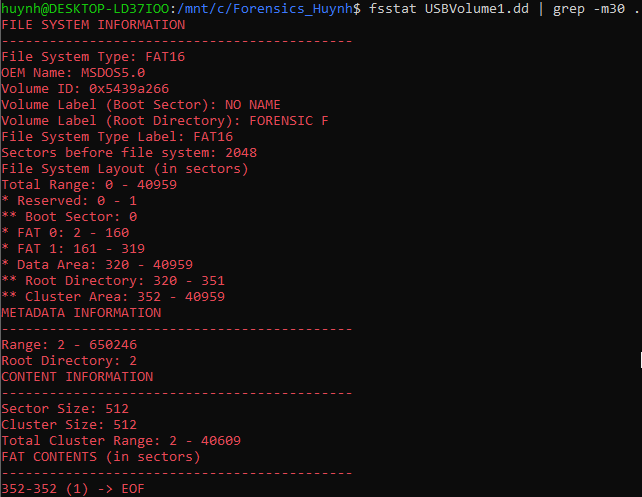
Run ubuntu. Change to your Forensics folder.

(You may have to install The Sleuth Kit using apt-get to run fsstat and fls.)

Type fsstat USBVolume1.dd | grep -m30 .

Note the trailing dot. Confirm you see the MBR details for the disk partition. \_ \_\_\_

Take a screen shot for the report. Yours may be different.



What is the OEM Name? MSDOS5.0

What is the Volume Root Directory Label? 320-351

First FAT size in sectors = (end – start ) = 2-160

Second FAT size in sectors = 161-319

Are the two FAT sizes the same? No

Why or why not? The smaller the partition, the smaller the cluster size and these partitions or FAT sizes goes up and so does the cluster size

# Q4) Identify the FAT files using fls

Confirm you have the USBVolume1.dd file in your Forensics folder.

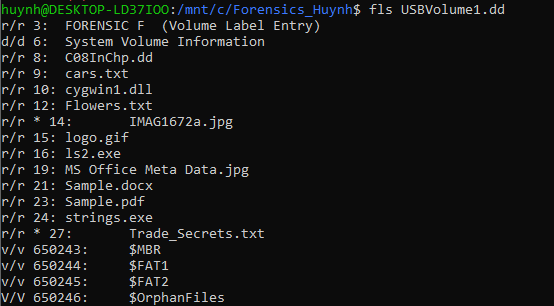
Run ubuntu. Change to your Forensics folder.

Type fls USBVolume1.dd | grep -m30 .

Confirm you see the files for the USB disk partition. \_ \_\_\_

(You may have to install The Sleuth Kit using apt-get to run fls).

Take a screenshot for your report.



What is the inode for ls2.exe? 16

Note \* indicates a deleted file.

What are the inodes of the deleted flies.? 14 and 27

# Q5) Recover deleted files

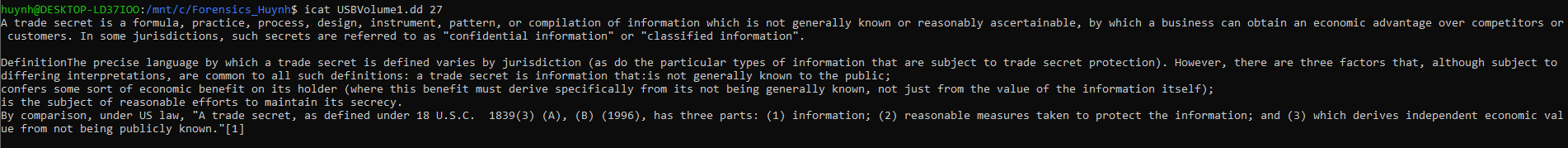
To recover the deleted file; we use icat on the inode.

Use icat with the inode for Trade\_Secrets.txt

Type icat <Image> <inode>

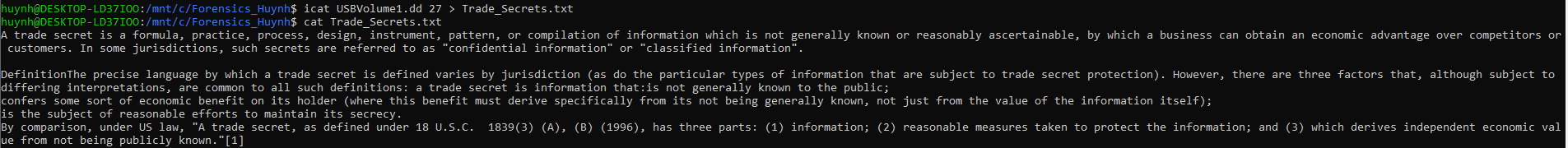
You should see the deleted file contents! (Your inode may be different.)

Take a screen shot of the command and the result.



We can now recover the deleted file. Type

icat <Image> <inode> > Trade\_Secrets.txt



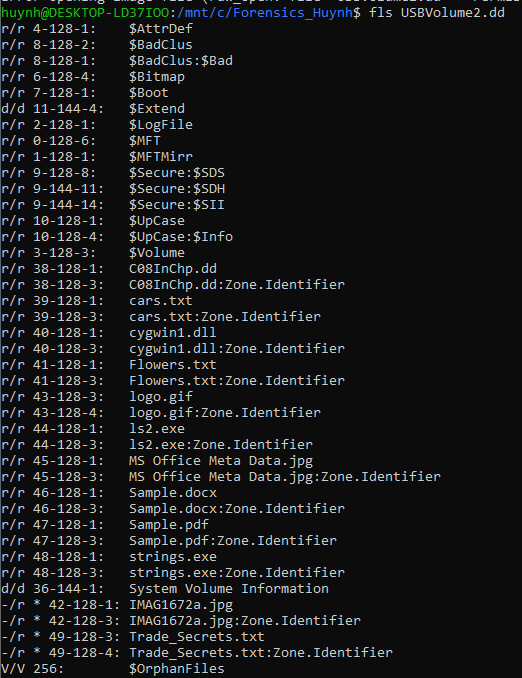
When will the technique fail to correctly recover a file?

The inode would have to be altered to fail to retrieve the file’s contents. There are also instances where the damage to the hard drive is so severe that data recovery is not possible.

Q6) NTFS analysis with The Sleuth Kit

We will repeat one of the steps we used for USB FAT32. However, NTFS is more complex so we will see a different result.

Type fls USBVolume2.dd Confirm you see the files for the disk partition.



Take a screenshot for your report.

Identify the ls2.exe inode 44-128-3 (44 is the inode)

Note the deleted files. inodes

42-128-1(42 is the inode) and 49-128-3 (49 is the inode) (yours will be different)

Which metadata items in the fls display may be of forensic interest? There are metadata files that start with $.

Explain why. These types of files could be of interest on how certain applications and system is running. As you can see there is a logfile which these files of interests can potentially give additional evidence to what the user was doing.

Close your cmd window and remove your USB stick when finished.