48436/32309 Week 09 Disk Analysis Report

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

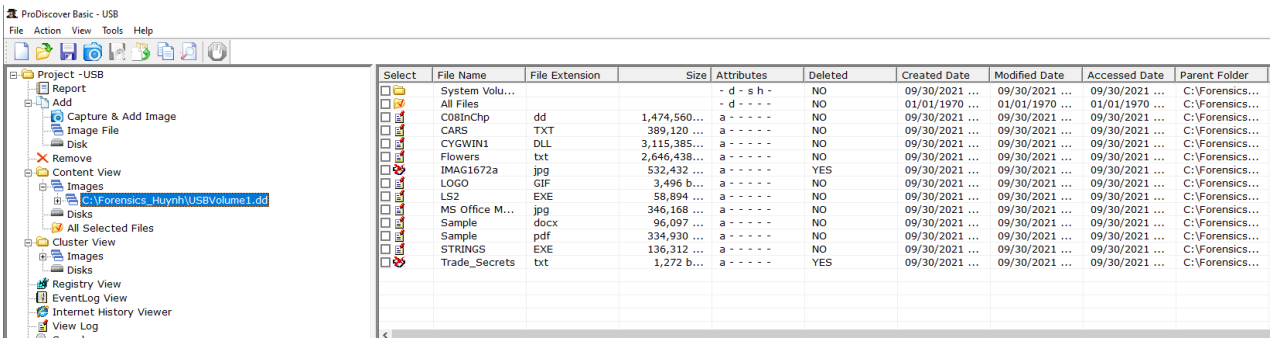
Acquire the Partition.

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

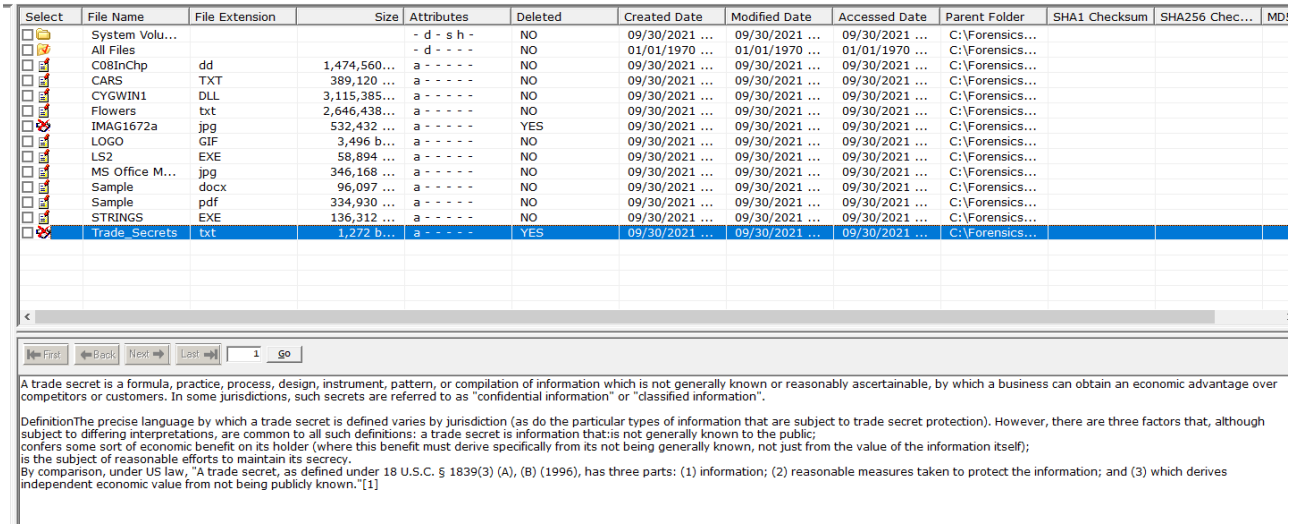
48436/32309

Week 09 Disk Analysis Report

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



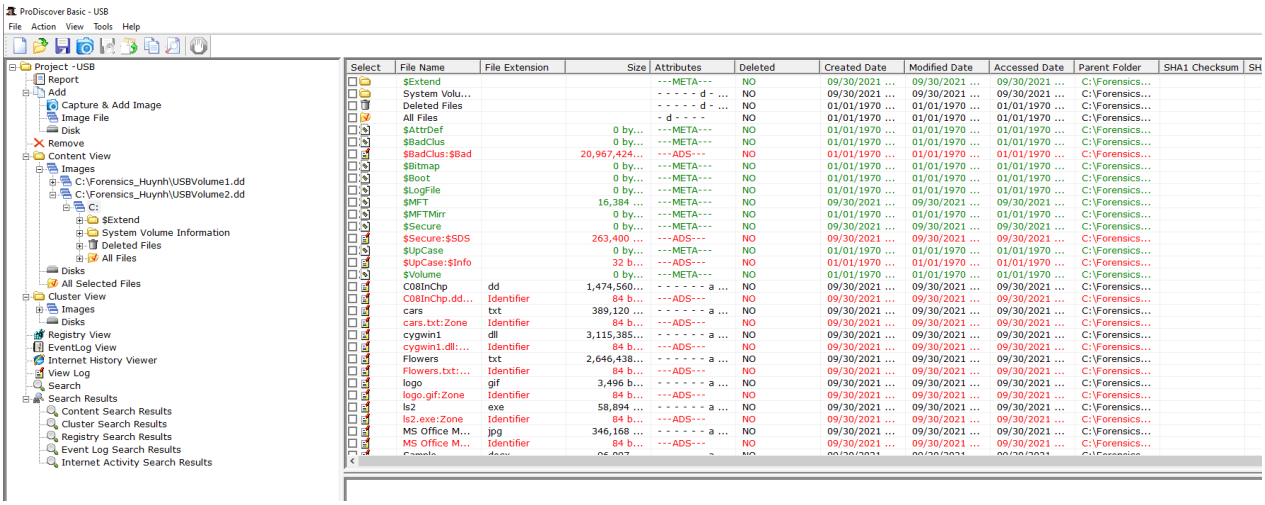
Select the deleted file Trade_Secrets.txt Confirm you can see the contents in the view pane. _ _



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

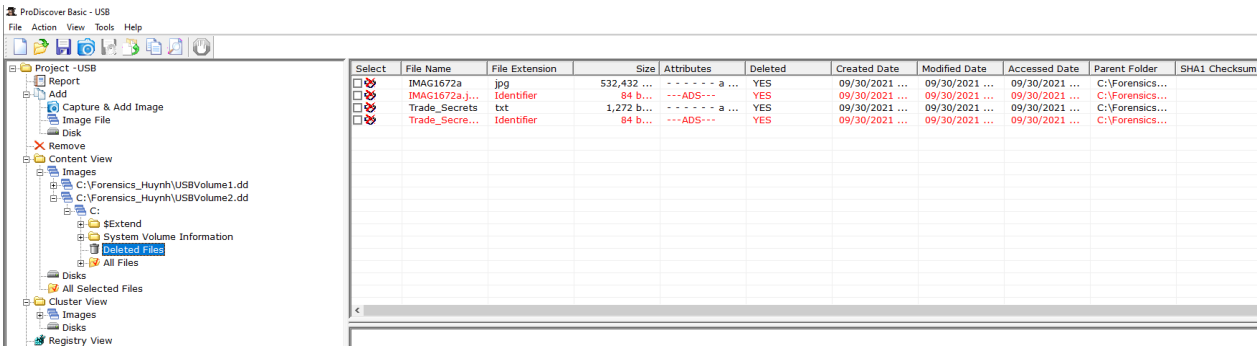
Now with NTFS you need to select the C:\Drive to see the files.

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. _ __



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. _____

Week 09 Disk Analysis Report

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ xxd -l 512 USBPartition.dd
00000000: 33c0 8ed0 bc00 7cfb 5007 501f fcbe 1b7c  3.....|.P.P....|
00000010: bf1b 0650 57b9 e501 f3a4 cbbd be07 b104  ...PW...........
00000020: 386e 007c 0975 1383 c510 e2f4 cd18 8bf5  8n.|.u..........
00000030: 83c6 1049 7419 382c 74f6 a0b5 07b4 078b  ...It.8,t.......
00000040: f0ac 3c00 74fc bb07 00b4 0ecd 10eb f288  ..<.t...........
00000050: 4e10 e846 0073 2afe 4610 807e 040b 740b  N..F.s*.F..~..t.
00000060: 807e 040c 7405 a0b6 0775 d280 4602 0683  .~..t....u..F...
00000070: 4608 0683 560a 00e8 2100 7305 a0b6 07eb  F...V...!.s.....
00000080: bc81 3efe 7d55 aa74 0b80 7e10 0074 c8a0  ..>.}U.t..~..t..
00000090: b707 eba9 8bfc 1e57 8bf5 cbbf 0500 8a56  .......W.......V
000000a0: 00b4 08cd 1372 238a c124 3f98 8ade 8afc  .....r#..$?.....
000000b0: 43f7 e38b d186 d6b1 06d2 ee42 f7e2 3956  C..........B..9V
000000c0: 0a77 2372 0539 4608 731c b801 02bb 007c  .w#r.9F.s......|
000000d0: 8b4e 028b 5600 cd13 7351 4f74 4e32 e48a  .N..V...sQOtN2..
000000e0: 5600 cd13 ebe4 8a56 0060 bbaa 55b4 41cd  V......V.`..U.A.
000000f0: 1372 3681 fb55 aa75 30f6 c101 742b 6160  .r6..U.u0...t+a`
00000100: 6a00 6a00 ff76 0aff 7608 6a00 6800 7c6a  j.j..v..v.j.h.|j
00000110: 016a 10b4 428b f4cd 1361 6173 0e4f 740b  .j..B....aas.Ot.
00000120: 32e4 8a56 00cd 13eb d661 f9c3 496e 7661  2..V.....a..Inva
00000130: 6c69 6420 7061 7274 6974 696f 6e20 7461  lid partition ta
00000140: 626c 6500 4572 726f 7220 6c6f 6164 696e  ble.Error loadin
00000150: 6720 6f70 6572 6174 696e 6720 7379 7374  g operating syst
00000160: 656d 004d 6973 7369 6e67 206f 7065 7261  em.Missing opera
00000170: 7469 6e67 2073 7973 7465 6d00 0000 0000  ting system.....
00000180: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000190: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001b0: 0000 0000 002c 4463 9316 4336 0000 0020  .....,Dc..C6...
000001c0: 2100 0eac 2a02 0008 0000 00a0 0000 00ac  !...*...........
000001d0: 2b02 0739 3405 00a8 0000 00a0 0000 0000  +..94...........
000001e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001f0: 0000 0000 0000 0000 0000 0000 0000 55aa  ..............U.
```

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

- the last error message,

Week 09 Disk Analysis Report

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ xxd -l 512 USBPartition.dd
00000000: 33c0 8ed0 bc00 7cfb 5007 501f fcbe 1b7c  3.....|.P.P....|
00000010: bf1b 0650 57b9 e501 f3a4 cbbd be07 b104  ...PW...........
00000020: 386e 007c 0975 1383 c510 e2f4 cd18 8bf5  8n.|.u..........
00000030: 83c6 1049 7419 382c 74f6 a0b5 07b4 078b  ...It.8,t.......
00000040: f0ac 3c00 74fc bb07 00b4 0ecd 10eb f288  ..<.t...........
00000050: 4e10 e846 0073 2afe 4610 807e 040b 740b  N..F.s*.F..~..t.
00000060: 807e 040c 7405 a0b6 0775 d280 4602 0683  .~..t....u..F...
00000070: 4608 0683 560a 00e8 2100 7305 a0b6 07eb  F...V...!.s.....
00000080: bc81 3efe 7d55 aa74 0b80 7e10 0074 c8a0  ..>.}U.t..~..t..
00000090: b707 eba9 8bfc 1e57 8bf5 cbbf 0500 8a56  .......W.......V
000000a0: 00b4 08cd 1372 238a c124 3f98 8ade 8afc  .....r#..$?.....
000000b0: 43f7 e38b d186 d6b1 06d2 ee42 f7e2 3956  C..........B..9V
000000c0: 0a77 2372 0539 4608 731c b801 02bb 007c  .w#r.9F.s......|
000000d0: 8b4e 028b 5600 cd13 7351 4f74 4e32 e48a  .N..V...sQOtN2..
000000e0: 5600 cd13 ebe4 8a56 0060 bbaa 55b4 41cd  V......V.`..U.A.
000000f0: 1372 3681 fb55 aa75 30f6 c101 742b 6160  .r6..U.u0...t+a`
00000100: 6a00 6a00 ff76 0aff 7608 6a00 6800 7c6a  j.j..v..v.j.h.|j
00000110: 016a 10b4 428b f4cd 1361 6173 0e4f 740b  .j..B....aas.Ot.
00000120: 32e4 8a56 00cd 13eb d661 f9c3 496e 7661  2..V.....a..Inva
00000130: 6c69 6420 7061 7274 6974 696f 6e20 7461  lid partition ta
00000140: 626c 6500 4572 726f 7220 6c6f 6164 696e  ble.Error loadin
00000150: 6720 6f70 6572 6174 696e 6720 7379 7374  g operating syst
00000160: 656d 004d 6973 7369 6e67 206f 7065 7261  em.Missing opera
00000170: 7469 6e67 2073 7973 7465 6d00 0000 0000  ting system.....
00000180: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000190: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001b0: 0000 0000 002c 4463 9316 4336 0000 0020  .....,Dc..C6...
000001c0: 2100 0eac 2a02 0008 0000 00a0 0000 00ac  !...*...........
000001d0: 2b02 0739 3405 00a8 0000 00a0 0000 0000  +..94...........
000001e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001f0: 0000 0000 0000 0000 0000 0000 0000 55aa  ..............U.
```

- the four partition types __ _____

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ xxd -l 512 USBPartition.dd
00000000: 33c0 8ed0 bc00 7cfb 5007 501f fcbe 1b7c  3.....|.P.P....|
00000010: bf1b 0650 57b9 e501 f3a4 cbbd be07 b104  ...PW...........
00000020: 386e 007c 0975 1383 c510 e2f4 cd18 8bf5  8n.|.u..........
00000030: 83c6 1049 7419 382c 74f6 a0b5 07b4 078b  ...It.8,t.......
00000040: f0ac 3c00 74fc bb07 00b4 0ecd 10eb f288  ..<.t...........
00000050: 4e10 e846 0073 2afe 4610 807e 040b 740b  N..F.s*.F..~..t.
00000060: 807e 040c 7405 a0b6 0775 d280 4602 0683  .~..t....u..F...
00000070: 4608 0683 560a 00e8 2100 7305 a0b6 07eb  F...V...!.s.....
00000080: bc81 3efe 7d55 aa74 0b80 7e10 0074 c8a0  ..>.}U.t..~..t..
00000090: b707 eba9 8bfc 1e57 8bf5 cbbf 0500 8a56  .......W.......V
000000a0: 00b4 08cd 1372 238a c124 3f98 8ade 8afc  .....r#..$?.....
000000b0: 43f7 e38b d186 d6b1 06d2 ee42 f7e2 3956  C..........B..9V
000000c0: 0a77 2372 0539 4608 731c b801 02bb 007c  .w#r.9F.s......|
000000d0: 8b4e 028b 5600 cd13 7351 4f74 4e32 e48a  .N..V...sQOtN2..
000000e0: 5600 cd13 ebe4 8a56 0060 bbaa 55b4 41cd  V......V.`..U.A.
000000f0: 1372 3681 fb55 aa75 30f6 c101 742b 6160  .r6..U.u0...t+a`
00000100: 6a00 6a00 ff76 0aff 7608 6a00 6800 7c6a  j.j..v..v.j.h.|j
00000110: 016a 10b4 428b f4cd 1361 6173 0e4f 740b  .j..B....aas.Ot.
00000120: 32e4 8a56 00cd 13eb d661 f9c3 496e 7661  2..V.....a..Inva
00000130: 6c69 6420 7061 7274 6974 696f 6e20 7461  lid partition ta
00000140: 626c 6500 4572 726f 7220 6c6f 6164 696e  ble.Error loadin
00000150: 6720 6f70 6572 6174 696e 6720 7379 7374  g operating syst
00000160: 656d 004d 6973 7369 6e67 206f 7065 7261  em.Missing opera
00000170: 7469 6e67 2073 7973 7465 6d00 0000 0000  ting system.....
00000180: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000190: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001b0: 0000 0000 002c 4463 9316 4336 0000 0020  .....,Dc..C6...
000001c0: 2100 0eac 2a02 0008 0000 00a0 0000 00ac  !...*...........
000001d0: 2b02 0739 3405 00a8 0000 00a0 0000 0000  +..94...........
000001e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001f0: 0000 0000 0000 0000 0000 0000 0000 55aa  ..............U.
```

- the four partitions boot status,
    - Boot status of these partitions are all 00 at the 0E column

- the MBR signature. _____

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ xxd -l 512 USBPartition.dd
00000000: 33c0 8ed0 bc00 7cfb 5007 501f fcbe 1b7c  3.....|.P.P....|
00000010: bf1b 0650 57b9 e501 f3a4 cbbd be07 b104  ...PW...........
00000020: 386e 007c 0975 1383 c510 e2f4 cd18 8bf5  8n.|.u..........
00000030: 83c6 1049 7419 382c 74f6 a0b5 07b4 078b  ...It.8,t.......
00000040: f0ac 3c00 74fc bb07 00b4 0ecd 10eb f288  ..<.t...........
00000050: 4e10 e846 0073 2afe 4610 807e 040b 740b  N..F.s*.F..~..t.
00000060: 807e 040c 7405 a0b6 0775 d280 4602 0683  .~..t....u..F...
00000070: 4608 0683 560a 00e8 2100 7305 a0b6 07eb  F...V...!.s.....
00000080: bc81 3efe 7d55 aa74 0b80 7e10 0074 c8a0  ..>.}U.t..~..t..
00000090: b707 eba9 8bfc 1e57 8bf5 cbbf 0500 8a56  .......W.......V
000000a0: 00b4 08cd 1372 238a c124 3f98 8ade 8afc  .....r#..$?.....
000000b0: 43f7 e38b d186 d6b1 06d2 ee42 f7e2 3956  C..........B..9V
000000c0: 0a77 2372 0539 4608 731c b801 02bb 007c  .w#r.9F.s......|
000000d0: 8b4e 028b 5600 cd13 7351 4f74 4e32 e48a  .N..V...sQOtN2..
000000e0: 5600 cd13 ebe4 8a56 0060 bbaa 55b4 41cd  V......V.`..U.A.
000000f0: 1372 3681 fb55 aa75 30f6 c101 742b 6160  .r6..U.u0...t+a`
00000100: 6a00 6a00 ff76 0aff 7608 6a00 6800 7c6a  j.j..v..v.j.h.|j
00000110: 016a 10b4 428b f4cd 1361 6173 0e4f 740b  .j..B....aas.Ot.
00000120: 32e4 8a56 00cd 13eb d661 f9c3 496e 7661  2..V.....a..Inva
00000130: 6c69 6420 7061 7274 6974 696f 6e20 7461  lid partition ta
00000140: 626c 6500 4572 726f 7220 6c6f 6164 696e  ble.Error loadin
00000150: 6720 6f70 6572 6174 696e 6720 7379 7374  g operating syst
00000160: 656d 004d 6973 7369 6e67 206f 7065 7261  em.Missing opera
00000170: 7469 6e67 2073 7973 7465 6d00 0000 0000  ting system.....
00000180: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000190: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001b0: 0000 0000 002c 4463 9316 4336 0000 0020  .....,Dc..C6...
000001c0: 2100 0eac 2a02 0008 0000 00a0 0000 00ac  !...*...........
000001d0: 2b02 0739 3405 00a8 0000 00a0 0000 0000  +..94...........
000001e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001f0: 0000 0000 0000 0000 0000 0000 0000 55aa  ..............U.
```

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.

```
Command (? for help): p
Disk 0:: 125829120 sectors, 60.0 GiB
Sector size (logical): 512 bytes
Disk identifier (GUID): 35E5DE55-642C-4E6A-85B8-7F7F18A536A4
Partition table holds up to 128 entries
Main partition table begins at sector 2 and ends at sector 33
First usable sector is 34, last usable sector is 125829086
Partitions will be aligned on 2048-sector boundaries
Total free space is 4029 sectors (2.0 MiB)

Number  Start (sector)    End (sector)  Size       Code  Name
   1            2048       125827071   60.0 GiB    0700  Microsoft basic data
```

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.

```
Command (? for help): i
Using 1
Partition GUID code: EBD0A0A2-B9E5-4433-87C0-68B6B72699C7 (Microsoft basic data)
Partition unique GUID: 1B48ED44-1D14-47EA-B5BF-CBBA55AC3E2E
First sector: 2048 (at 1024.0 KiB)
Last sector: 125827071 (at 60.0 GiB)
Partition size: 125825024 sectors (60.0 GiB)
Attribute flags: 0000000000000000
Partition name: 'Microsoft basic data'
```

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.

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ fsstat USBVolume1.dd | grep -m30 .
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT16
OEM Name: MSDOS5.0
Volume ID: 0x5439a266
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory): FORENSIC F
File System Type Label: FAT16
Sectors before file system: 2048
File System Layout (in sectors)
Total Range: 0 - 40959
* Reserved: 0 - 1
** Boot Sector: 0
* FAT 0: 2 - 160
* FAT 1: 161 - 319
* Data Area: 320 - 40959
** Root Directory: 320 - 351
** Cluster Area: 352 - 40959
METADATA INFORMATION
--------------------------------------------
Range: 2 - 650246
Root Directory: 2
CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 2 - 40609
FAT CONTENTS (in sectors)
--------------------------------------------
352-352 (1) -> EOF
```

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.

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ fls USBVolume1.dd
r/r 3:  FORENSIC F  (Volume Label Entry)
d/d 6:  System Volume Information
r/r 8:  C08InChp.dd
r/r 9:  cars.txt
r/r 10: cygwin1.dll
r/r 12: Flowers.txt
r/r * 14:       IMAG1672a.jpg
r/r 15: logo.gif
r/r 16: ls2.exe
r/r 19: MS Office Meta Data.jpg
r/r 21: Sample.docx
r/r 23: Sample.pdf
r/r 24: strings.exe
r/r * 27:       Trade_Secrets.txt
v/v 650243:     $MBR
v/v 650244:     $FAT1
v/v 650245:     $FAT2
V/V 650246:     $OrphanFiles
```

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.)

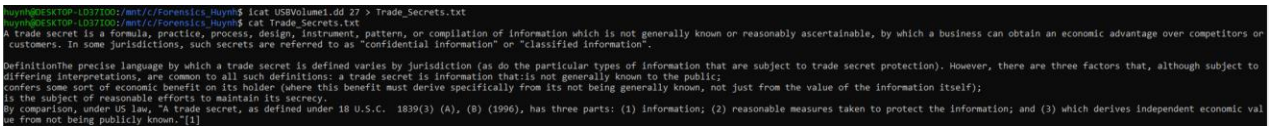
Take a screen shot of the command and the result.

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ icat USBVolume1.dd 27
A trade secret is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known or reasonably ascertainable, by which a business can obtain an economic advantage over competitors or
customers. In some jurisdictions, such secrets are referred to as "confidential information" or "classified information".

DefinitionThe precise language by which a trade secret is defined varies by jurisdiction (as do the particular types of information that are subject to trade secret protection). However, there are three factors that, although subject to
differing interpretations, are common to all such definitions: a trade secret is information that:is not generally known to the public;
confers some sort of economic benefit on its holder (where this benefit must derive specifically from its not being generally known, not just from the value of the information itself);
is the subject of reasonable efforts to maintain its secrecy.
By comparison, under US law, "A trade secret, as defined under 18 U.S.C.  1839(3) (A), (B) (1996), has three parts: (1) information; (2) reasonable measures taken to protect the information; and (3) which derives independent economic val
ue from not being publicly known."[1]
```

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.

```
huynh@DESKTOP-LD37IOO:/mnt/c/Forensics_Huynh$ fls USBVolume2.dd
r/r 4-128-1:    $AttrDef
r/r 8-128-2:    $BadClus
r/r 8-128-1:    $BadClus:$Bad
r/r 6-128-4:    $Bitmap
r/r 7-128-1:    $Boot
d/d 11-144-4:   $Extend
r/r 2-128-1:    $LogFile
r/r 0-128-6:    $MFT
r/r 1-128-1:    $MFTMirr
r/r 9-128-8:    $Secure:$SDS
r/r 9-144-11:   $Secure:$SDH
r/r 9-144-14:   $Secure:$SII
r/r 10-128-1:   $UpCase
r/r 10-128-4:   $UpCase:$Info
r/r 3-128-3:    $Volume
r/r 38-128-1:   C08InChp.dd
r/r 38-128-3:   C08InChp.dd:Zone.Identifier
r/r 39-128-1:   cars.txt
r/r 39-128-3:   cars.txt:Zone.Identifier
r/r 40-128-1:   cygwin1.dll
r/r 40-128-3:   cygwin1.dll:Zone.Identifier
r/r 41-128-1:   Flowers.txt
r/r 41-128-3:   Flowers.txt:Zone.Identifier
r/r 43-128-3:   logo.gif
r/r 43-128-4:   logo.gif:Zone.Identifier
r/r 44-128-1:   ls2.exe
r/r 44-128-3:   ls2.exe:Zone.Identifier
r/r 45-128-1:   MS Office Meta Data.jpg
r/r 45-128-3:   MS Office Meta Data.jpg:Zone.Identifier
r/r 46-128-1:   Sample.docx
r/r 46-128-3:   Sample.docx:Zone.Identifier
r/r 47-128-1:   Sample.pdf
r/r 47-128-3:   Sample.pdf:Zone.Identifier
r/r 48-128-1:   strings.exe
r/r 48-128-3:   strings.exe:Zone.Identifier
d/d 36-144-1:   System Volume Information
-/r * 42-128-1: IMAG1672a.jpg
-/r * 42-128-3: IMAG1672a.jpg:Zone.Identifier
-/r * 49-128-3: Trade_Secrets.txt
-/r * 49-128-4: Trade_Secrets.txt:Zone.Identifier
V/V 256:        $OrphanFiles
```

Take a screenshot for your report.

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

Note the deleted files. inodes

Week 09 Disk Analysis Report

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.