National University of Computer and Emerging Sciences
Islamabad Campus

CY2002

Digital Forensics

Assignment 03

Hands-On Projects

Chapter 04: Processing Crime and Incident Scenes

Submitted by: Abdul Sami Qasim
Roll number: 22i-1725
Date: September 17, 2024

Table of Contents

Chapter 04: Processing Crime and Incident Scenes 0

- **Introduction** 2
- **Details and Steps** 2

Project 4-3 2

Project 4-4 10

Project 4-5 15

- **Summary** 17
- **References** 17

Introduction

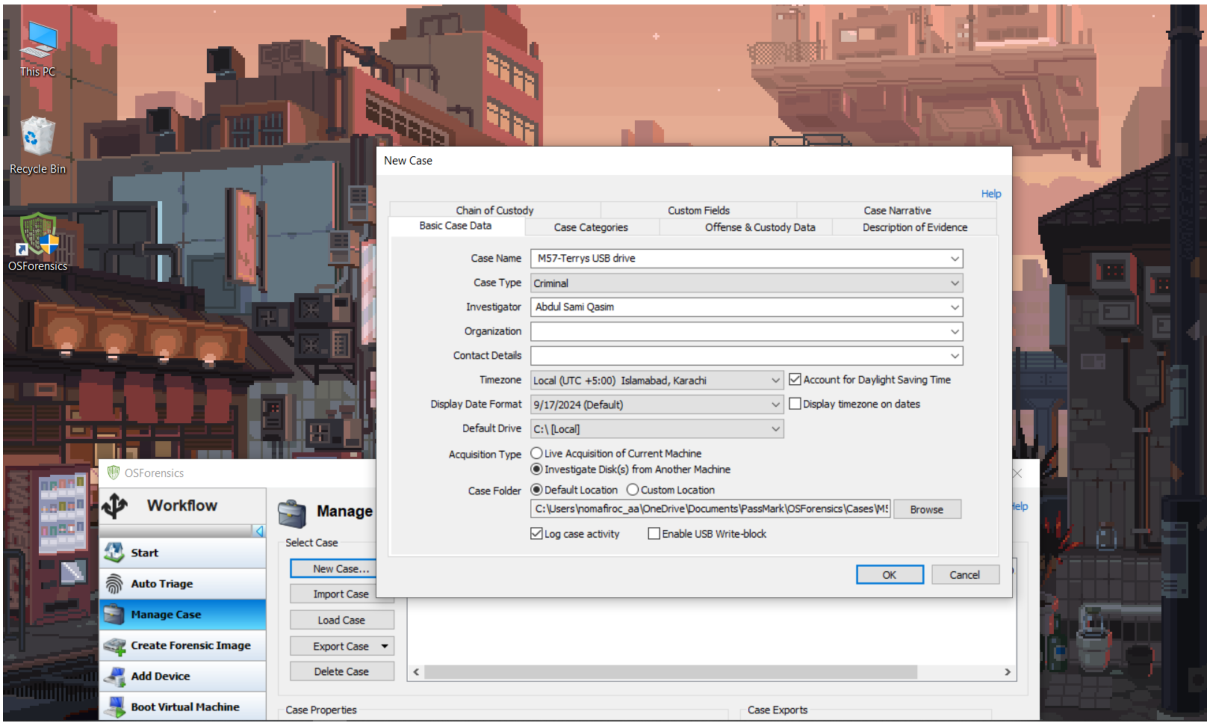
In this assignment we we’re told to complete Hands-on projects (4-3 to 4-5) from chapter 4 of the book “ Guide to Computer Forensics and Investigations, 6th ed.”

Details and Steps

Following are the steps taken to perform the assigned tasks.

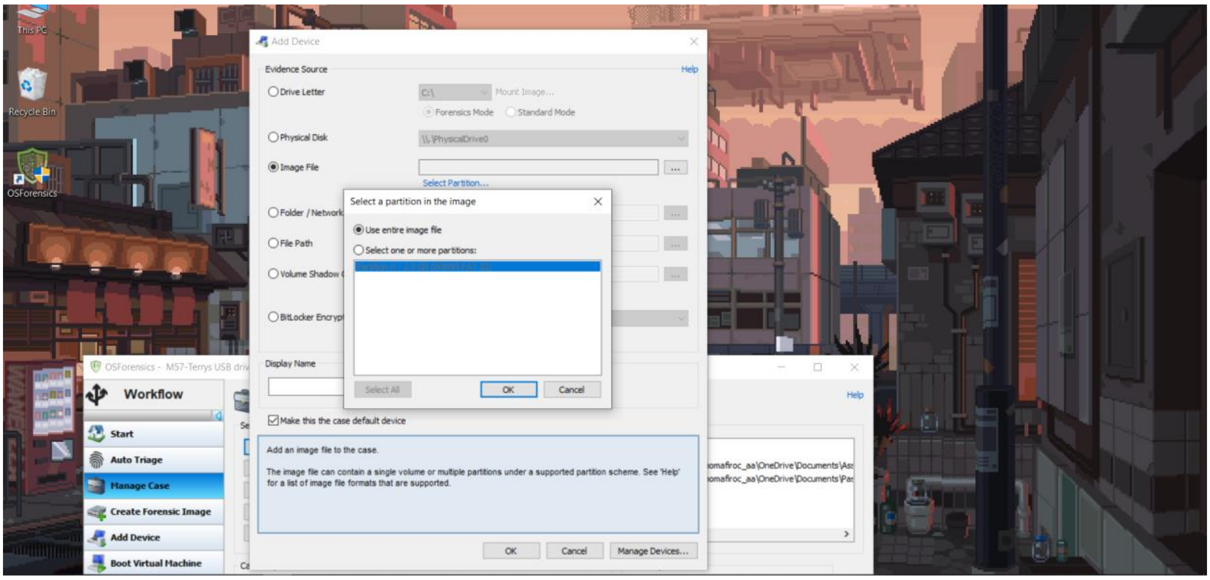
Project 4-3

This project requires us to analyze terry’s work USB for any signs of evidence related to the case. So, loading up the evidence to analyze it:



New Case

Case Name: M57-Terrys USB drive
Case Type: Criminal
Investigator: Abdul Sami Qasim
Organization:
Contact Details:
Timezone: Local (UTC +5:00) Islamabad, Karachi ☑ Account for Daylight Saving Time
Display Date Format: 9/17/2024 (Default) □ Display timezone on dates
Default Drive: C:\ [Local]
Acquisition Type: ○ Live Acquisition of Current Machine ● Investigate Disk(s) from Another Machine
Case Folder: ● Default Location ○ Custom Location
C:\Users\nomafiroc_aa\OneDrive\Documents\PassMark\OSForensics\Cases\M!
☑ Log case activity □ Enable USB Write-block



Add Device

Evidence Source

○ Drive Letter C:\ Mount Image...

○ Physical Disk \\.\PhysicalDrive0

● Image File

Select Partition...

○ Folder / Network

○ File Path

○ Volume Shadow

○ BitLocker Encrypt

Select a partition in the image

● Use entire image file

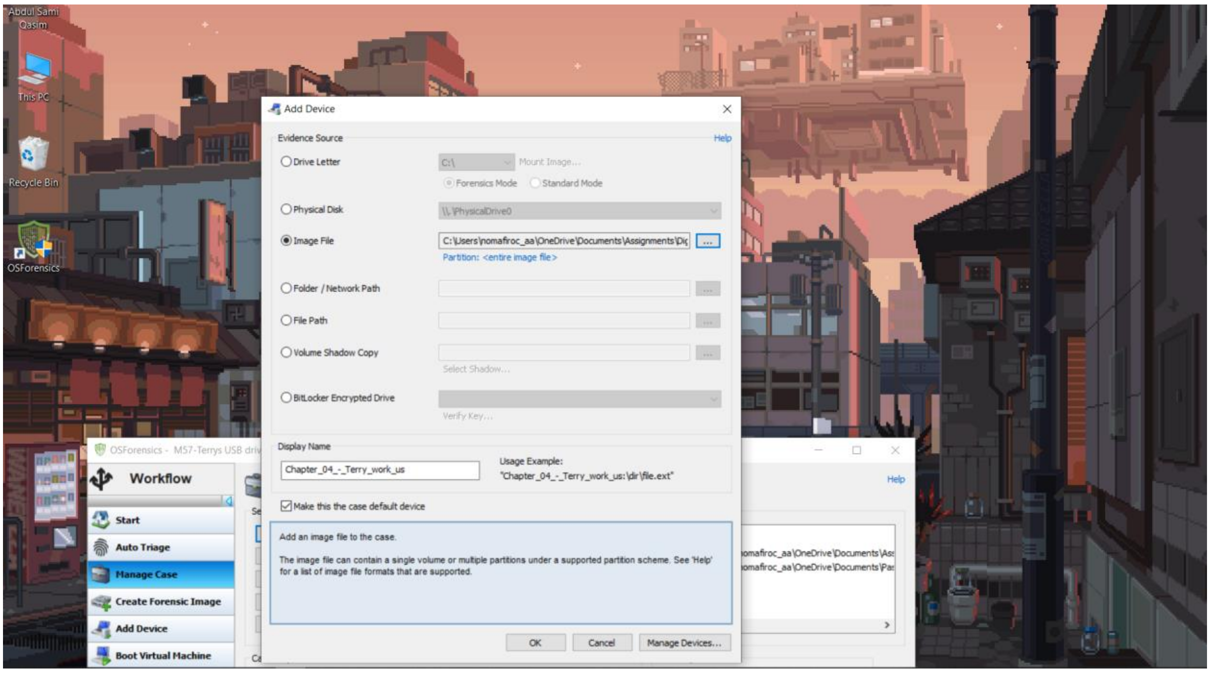
○ Select one or more partitions:

Display Name

☑ Make this the case default device

Add an image file to the case.

The image file can contain a single volume or multiple partitions under a supported partition scheme. See 'Help' for a list of image file formats that are supported.



Add Device

Evidence Source

○ Drive Letter C:\ Mount Image...

○ Physical Disk \\.\PhysicalDrive0

● Image File C:\Users\nomafiroc_aa\OneDrive\Documents\Assignments\Dig

Partition: <entire image file>

○ Folder / Network Path

○ File Path

○ Volume Shadow Copy

○ BitLocker Encrypted Drive

Display Name

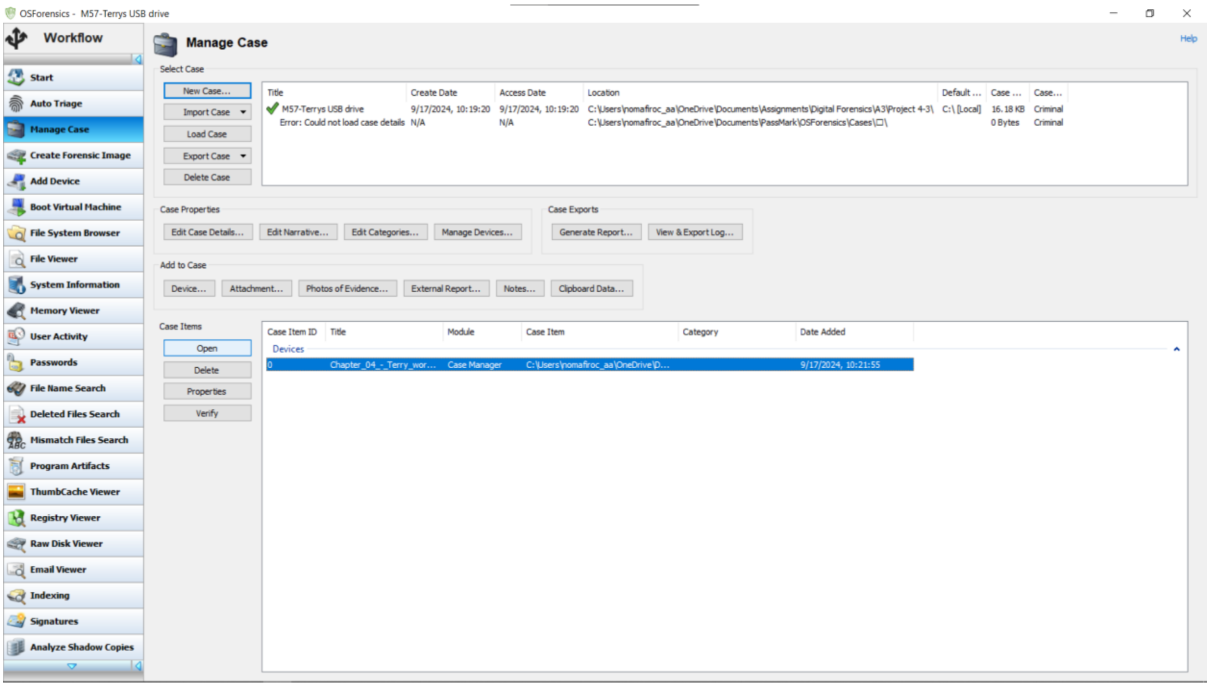
Chapter_04_-_Terry_work_us

Usage Example:
"Chapter_04_-_Terry_work_us:\dir\file.ext"

☑ Make this the case default device

Add an image file to the case.

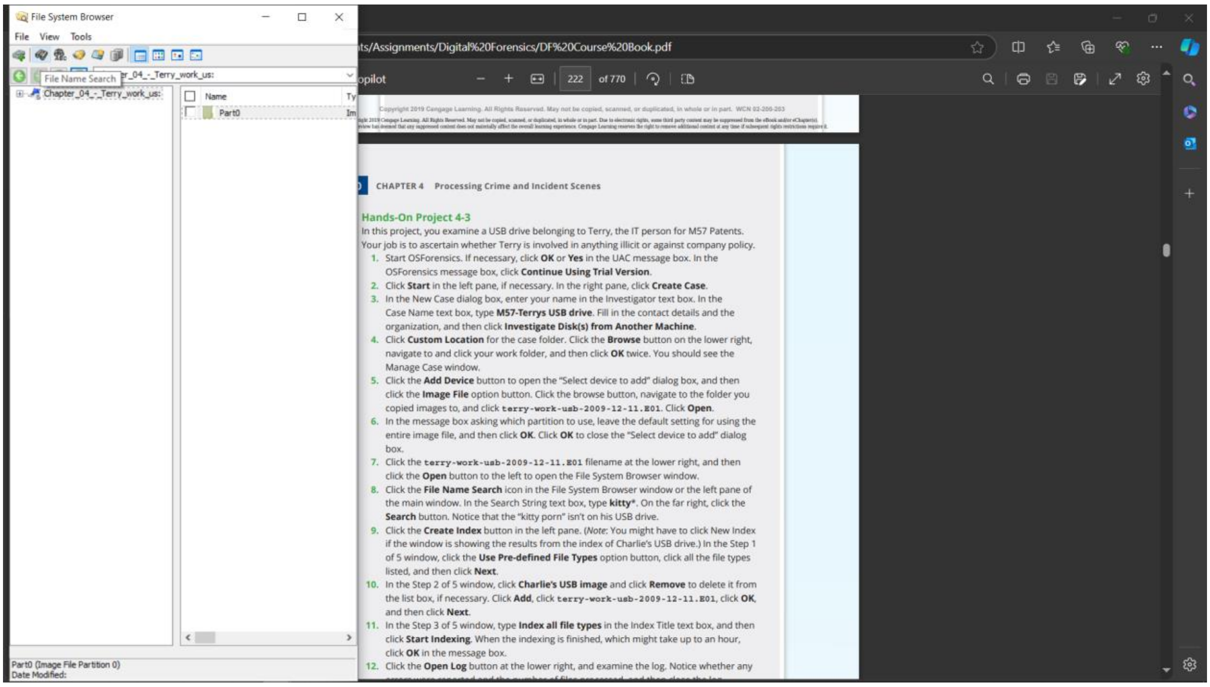
The image file can contain a single volume or multiple partitions under a supported partition scheme. See 'Help' for a list of image file formats that are supported.



Title	Create Date	Access Date	Location	Default ...	Case ...	Case...
✓ M57-Terrys USB drive	9/17/2024, 10:19:20	9/17/2024, 10:19:20	C:\Users\nomafiroc_aa\OneDrive\Documents\Assignments\Digital Forensics\A3\Project 4-3\	C:\ [Local]	16.18 KB	Criminal
Error: Could not load case details	N/A	N/A	C:\Users\nomafiroc_aa\OneDrive\Documents\PassMark\OSForensics\Cases\□\		0 Bytes	Criminal

Case Item ID	Title	Module	Case Item	Category	Date Added
Devices					
0	Chapter_04_-_Terry_wor...	Case Manager	C:\Users\nomafiroc_aa\OneDrive\D...		9/17/2024, 10:21:55

The evidence has been loaded successfully, now we have to search for the keyword "kitty"


File System Browser
File
View
Tools
File Name Search
r_04_-_Terry_work_us:
Chapter_04_-_Terry_work_us:
Name
Ty
Part0
Im
Part0 (Image File Partition 0)
Date Modified:
ts/Assignments/Digital%20Forensics/DF%20Course%20Book.pdf
opilot
222
of 770

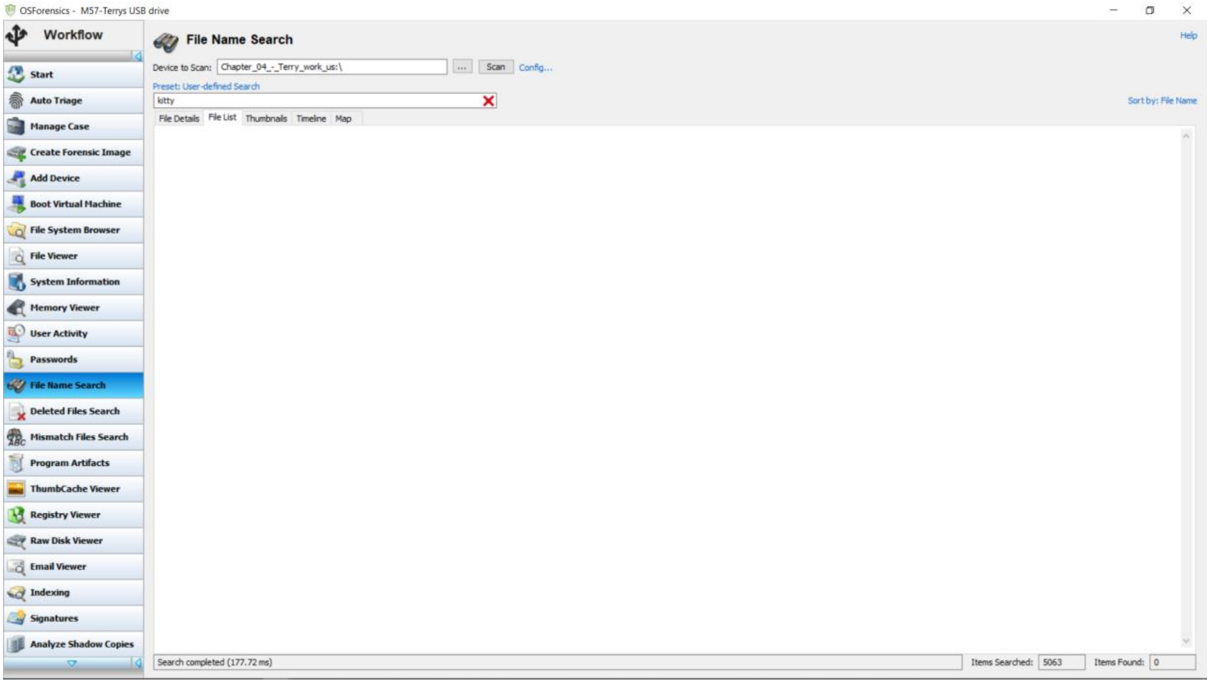
Copyright 2019 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. WCN 02-200-203

CHAPTER 4 Processing Crime and Incident Scenes

Hands-On Project 4-3

In this project, you examine a USB drive belonging to Terry, the IT person for M57 Patents. Your job is to ascertain whether Terry is involved in anything illicit or against company policy.

1. Start OSForensics. If necessary, click **OK** or **Yes** in the UAC message box. In the OSForensics message box, click **Continue Using Trial Version**.
2. Click **Start** in the left pane, if necessary. In the right pane, click **Create Case**.
3. In the New Case dialog box, enter your name in the Investigator text box. In the Case Name text box, type **M57-Terrys USB drive**. Fill in the contact details and the organization, and then click **Investigate Disk(s) from Another Machine**.
4. Click **Custom Location** for the case folder. Click the **Browse** button on the lower right, navigate to and click your work folder, and then click **OK** twice. You should see the Manage Case window.
5. Click the **Add Device** button to open the "Select device to add" dialog box, and then click the **Image File** option button. Click the browse button, navigate to the folder you copied images to, and click `terry-work-usb-2009-12-11.E01`. Click **Open**.
6. In the message box asking which partition to use, leave the default setting for using the entire image file, and then click **OK**. Click **OK** to close the "Select device to add" dialog box.
7. Click the `terry-work-usb-2009-12-11.E01` filename at the lower right, and then click the **Open** button to the left to open the File System Browser window.
8. Click the **File Name Search** icon in the File System Browser window or the left pane of the main window. In the Search String text box, type **kitty***. On the far right, click the **Search** button. Notice that the "kitty porn" isn't on his USB drive.
9. Click the **Create Index** button in the left pane. (*Note*: You might have to click New Index if the window is showing the results from the index of Charlie's USB drive.) In the Step 1 of 5 window, click the **Use Pre-defined File Types** option button, click all the file types listed, and then click **Next**.
10. In the Step 2 of 5 window, click **Charlie's USB image** and click **Remove** to delete it from the list box, if necessary. Click **Add**, click `terry-work-usb-2009-12-11.E01`, click **OK**, and then click **Next**.
11. In the Step 3 of 5 window, type **Index all file types** in the Index Title text box, and then click **Start Indexing**. When the indexing is finished, which might take up to an hour, click **OK** in the message box.
12. Click the **Open Log** button at the lower right, and examine the log. Notice whether any



Device to Scan: Chapter_04_-_Terry_work_us:\

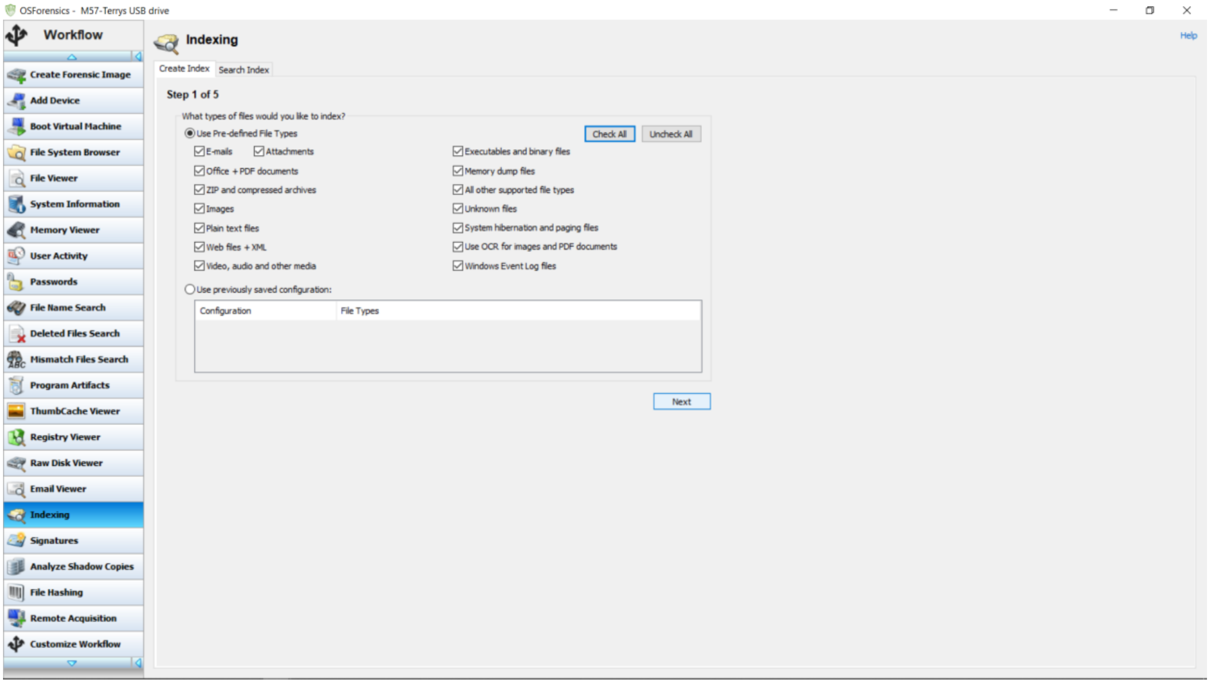
kitty

Search completed (177.72 ms)

Items Searched: 5063

Items Found: 0

Nothing related to the keyword was found on Terry's USB. Now starting the indexing process:



Step 1 of 5

What types of files would you like to index?

● Use Pre-defined File Types

☑ E-mails ☑ Attachments

☑ Office + PDF documents

☑ ZIP and compressed archives

☑ Images

☑ Plain text files

☑ Web files + XML

☑ Video, audio and other media

☑ Executables and binary files

☑ Memory dump files

☑ All other supported file types

☑ Unknown files

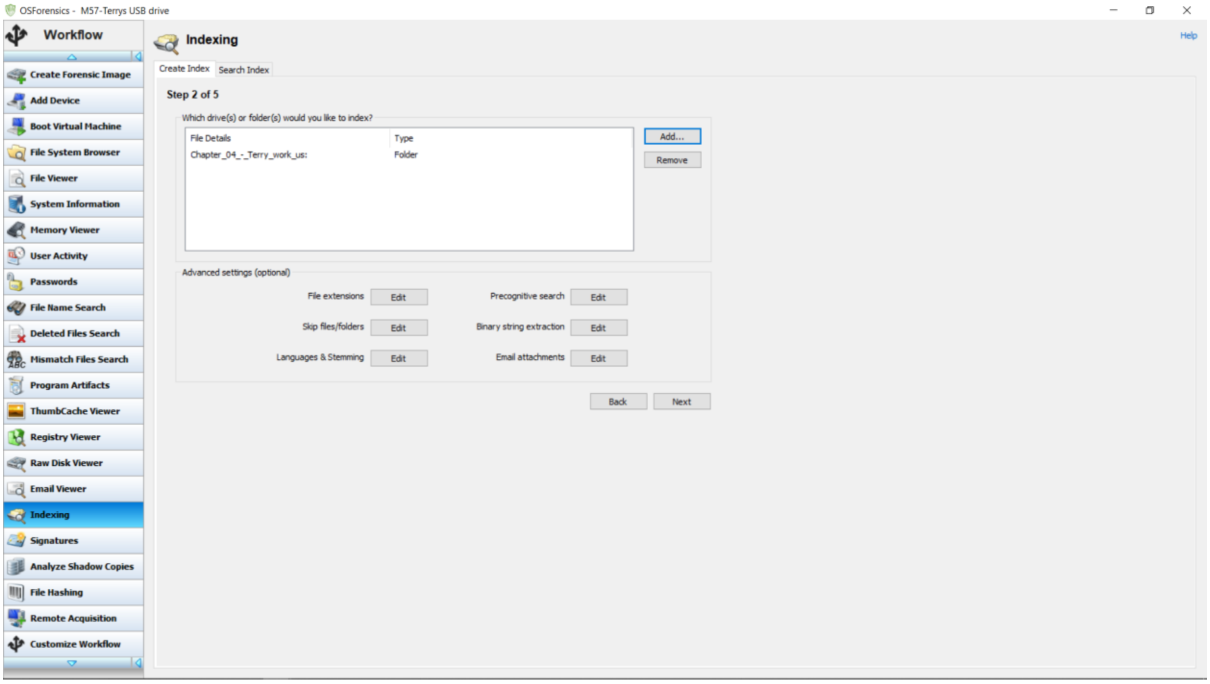
☑ System hibernation and paging files

☑ Use OCR for images and PDF documents

☑ Windows Event Log files

○ Use previously saved configuration:

Configuration	File Types



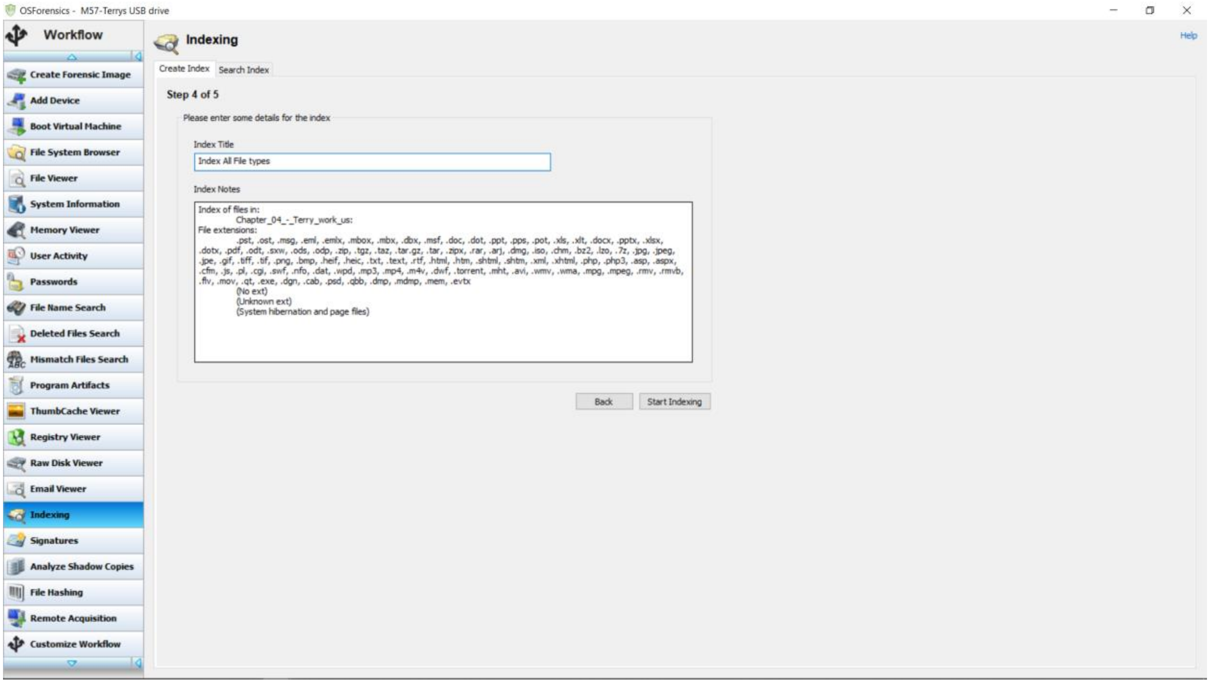
Indexing

Step 2 of 5

Which drive(s) or folder(s) would you like to index?

File Details	Type
Chapter_04_-_Terry_work_us:	Folder

Advanced settings (optional)



Indexing

Step 4 of 5

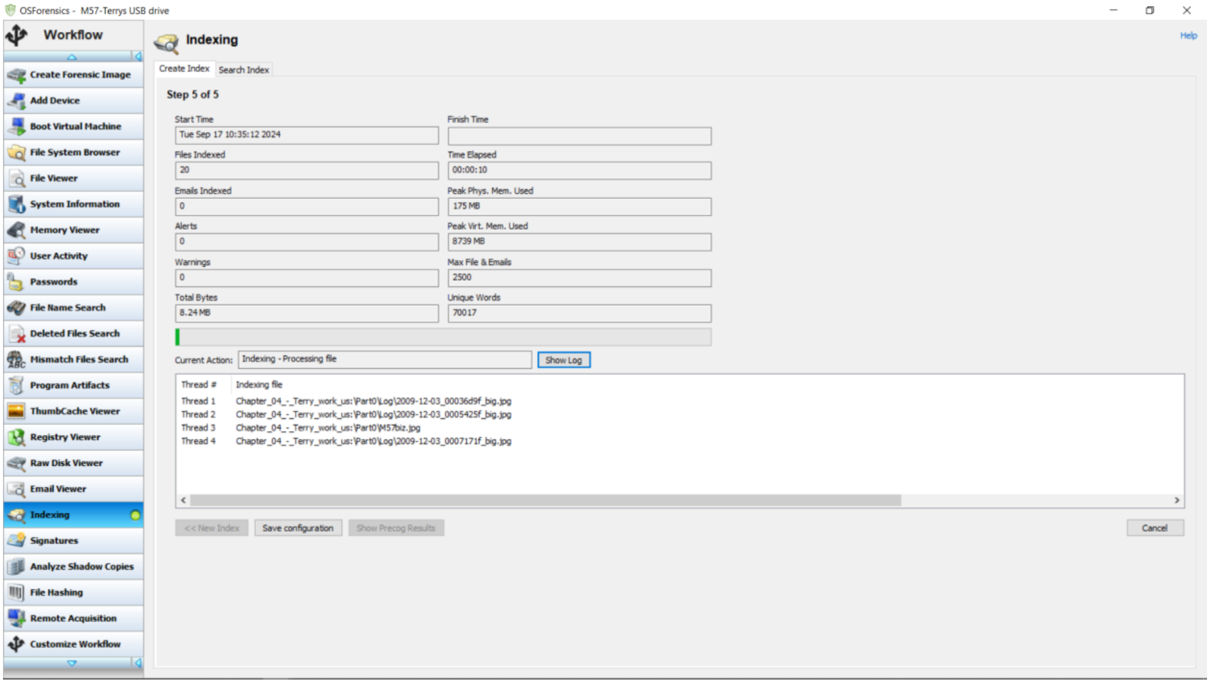
Please enter some details for the index

Index Title

Index All File types

Index Notes

```
Index of files in:
            Chapter_04_-_Terry_work_us:
File extensions:
            .pst, .ost, .msg, .eml, .emlx, .mbox, .mbx, .dbx, .msf, .doc, .dot, .ppt, .pps, .pot, .xls, .xlt, .docx, .pptx, .xlsx,
.dotx, .pdf, .odt, .sxw, .ods, .odp, .zip, .tgz, .taz, .tar.gz, .tar, .zipx, .rar, .arj, .dmg, .iso, .chm, .bz2, .lzo, .7z, .jpg, .jpeg,
.jpe, .gif, .tiff, .tif, .png, .bmp, .heif, .heic, .txt, .text, .rtf, .html, .htm, .shtml, .shtm, .xml, .xhtml, .php, .php3, .asp, .aspx,
.cfm, .js, .pl, .cgi, .swf, .nfo, .dat, .wpd, .mp3, .mp4, .m4v, .dwf, .torrent, .mht, .avi, .wmv, .wma, .mpg, .mpeg, .rmv, .rmvb,
.flv, .mov, .qt, .exe, .dgn, .cab, .psd, .qbb, .dmp, .mdmp, .mem, .evtx
            (No ext)
            (Unknown ext)
            (System hibernation and page files)
```



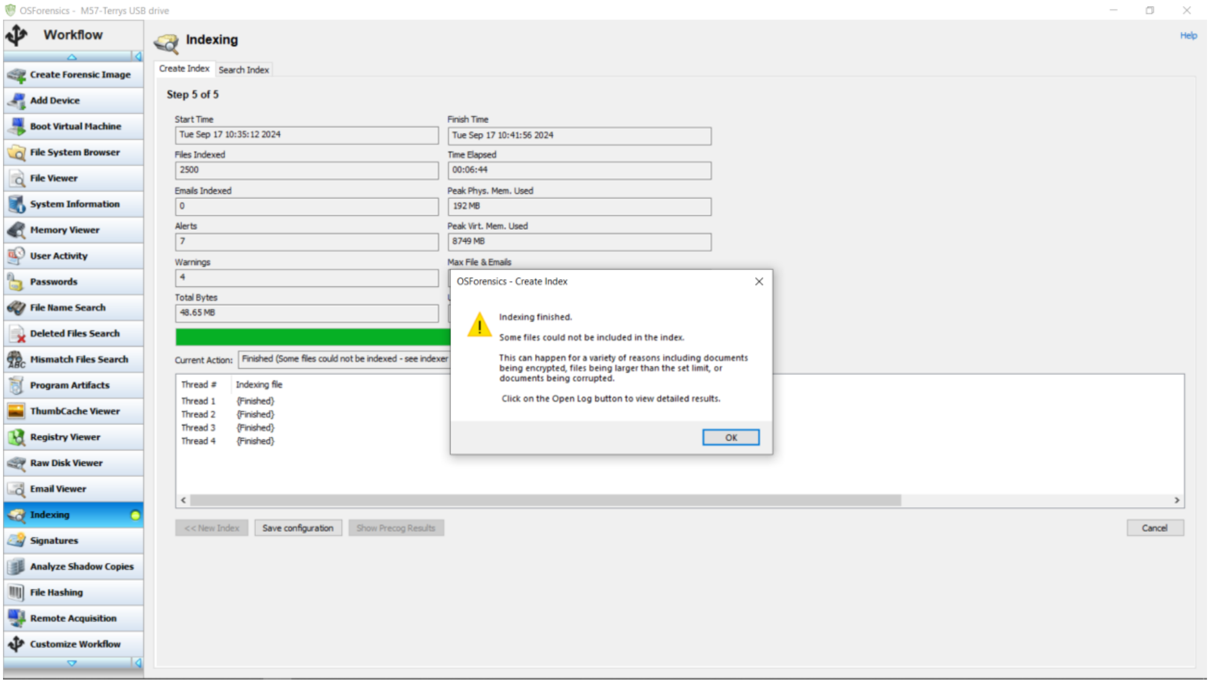
Indexing

Step 5 of 5

Start Time: Tue Sep 17 10:35:12 2024
Finish Time:
Files Indexed: 20
Time Elapsed: 00:00:10
Emails Indexed: 0
Peak Phys. Mem. Used: 175 MB
Alerts: 0
Peak Virt. Mem. Used: 8739 MB
Warnings: 0
Max File & Emails: 2500
Total Bytes: 8.24 MB
Unique Words: 70017

Current Action: Indexing - Processing file

```
Thread #   Indexing file
Thread 1   Chapter_04_-_Terry_work_us:\Part0\Log\2009-12-03_00036d9f_big.jpg
Thread 2   Chapter_04_-_Terry_work_us:\Part0\Log\2009-12-03_0005425f_big.jpg
Thread 3   Chapter_04_-_Terry_work_us:\Part0\M57biz.jpg
Thread 4   Chapter_04_-_Terry_work_us:\Part0\Log\2009-12-03_0007171f_big.jpg
```



Indexing

Step 5 of 5

Start Time: Tue Sep 17 10:35:12 2024
Finish Time: Tue Sep 17 10:41:56 2024
Files Indexed: 2500
Time Elapsed: 00:06:44
Emails Indexed: 0
Peak Phys. Mem. Used: 192 MB
Alerts: 7
Peak Virt. Mem. Used: 8749 MB
Warnings: 4
Max File & Emails
Total Bytes: 48.65 MB

Current Action: Finished (Some files could not be indexed - see indexer

```
Thread #   Indexing file
Thread 1   {Finished}
Thread 2   {Finished}
Thread 3   {Finished}
Thread 4   {Finished}
```

OSForensics - Create Index

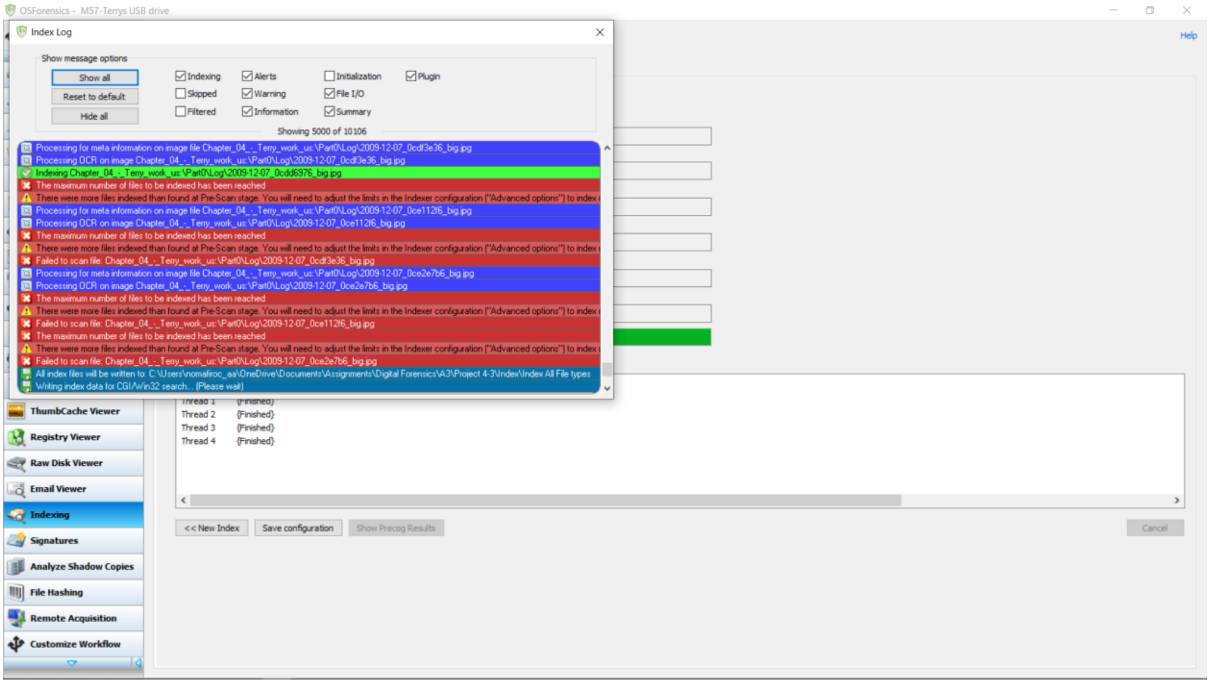
Indexing finished.

Some files could not be included in the index.

This can happen for a variety of reasons including documents being encrypted, files being larger than the set limit, or documents being corrupted.

Click on the Open Log button to view detailed results.

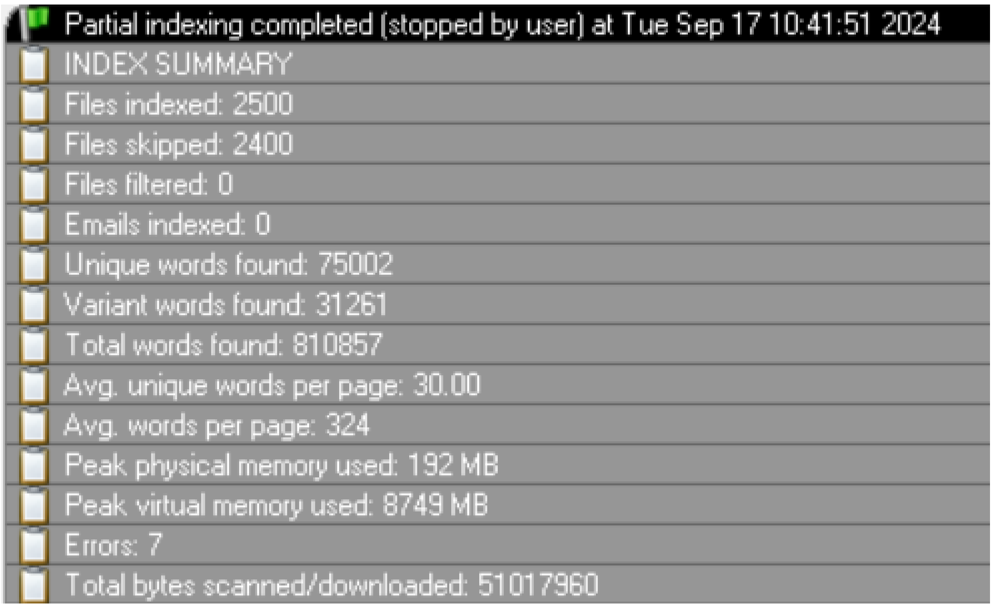
The following are the errors found in the indexing logs, there are a total of 7 errors.



```
Processing for meta information on image file Chapter_04_-_Terry_work_us:\Part0\Log\2009-12-07_0cdf3e36_big.jpg
Processing OCR on image Chapter_04_-_Terry_work_us:\Part0\Log\2009-12-07_0cdf3e36_big.jpg
Indexing Chapter_04_-_Terry_work_us:\Part0\Log\2009-12-07_0cdd6976_big.jpg
The maximum number of files to be indexed has been reached
There were more files indexed than found at Pre-Scan stage. You will need to adjust the limits in the Indexer configuration ("Advanced options") to index
Processing for meta information on image file Chapter_04_-_Terry_work_us:\Part0\Log\2009-12-07_0ce112f6_big.jpg
Processing OCR on image Chapter_04_-_Terry_work_us:\Part0\Log\2009-12-07_0ce112f6_big.jpg
The maximum number of files to be indexed has been reached
There were more files indexed than found at Pre-Scan stage. You will need to adjust the limits in the Indexer configuration ("Advanced options") to index
Failed to scan file: Chapter_04_-_Terry_work_us:\Part0\Log\2009-12-07_0cdf3e36_big.jpg
Processing for meta information on image file Chapter_04_-_Terry_work_us:\Part0\Log\2009-12-07_0ce2e7b6_big.jpg
Processing OCR on image Chapter_04_-_Terry_work_us:\Part0\Log\2009-12-07_0ce2e7b6_big.jpg
The maximum number of files to be indexed has been reached
There were more files indexed than found at Pre-Scan stage. You will need to adjust the limits in the Indexer configuration ("Advanced options") to index
Failed to scan file: Chapter_04_-_Terry_work_us:\Part0\Log\2009-12-07_0ce112f6_big.jpg
The maximum number of files to be indexed has been reached
There were more files indexed than found at Pre-Scan stage. You will need to adjust the limits in the Indexer configuration ("Advanced options") to index
Failed to scan file: Chapter_04_-_Terry_work_us:\Part0\Log\2009-12-07_0ce2e7b6_big.jpg
All index files will be written to: C:\Users\nomafiroc_aa\OneDrive\Documents\Assignments\Digital Forensics\A3\Project 4-3\Index\Index All File types
Writing index data for CGI/Win32 search... (Please wait)
```

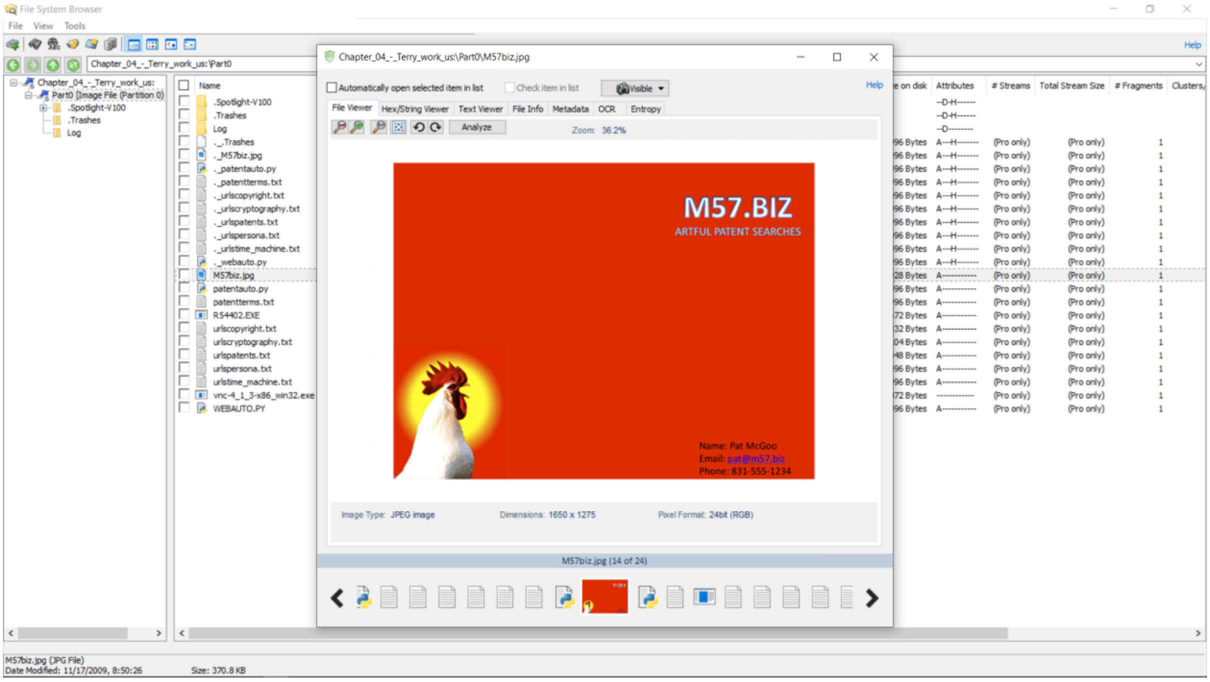
```
Thread 1    {Finished}
Thread 2    {Finished}
Thread 3    {Finished}
Thread 4    {Finished}
```

Summary of the indexing process:



```
Partial indexing completed (stopped by user) at Tue Sep 17 10:41:51 2024
INDEX SUMMARY
Files indexed: 2500
Files skipped: 2400
Files filtered: 0
Emails indexed: 0
Unique words found: 75002
Variant words found: 31261
Total words found: 810857
Avg. unique words per page: 30.00
Avg. words per page: 324
Peak physical memory used: 192 MB
Peak virtual memory used: 8749 MB
Errors: 7
Total bytes scanned/downloaded: 51017960
```

Afterwards, we’re told to look at some of the pictures and text files in the provided USB, here is a photo and a text file from it:

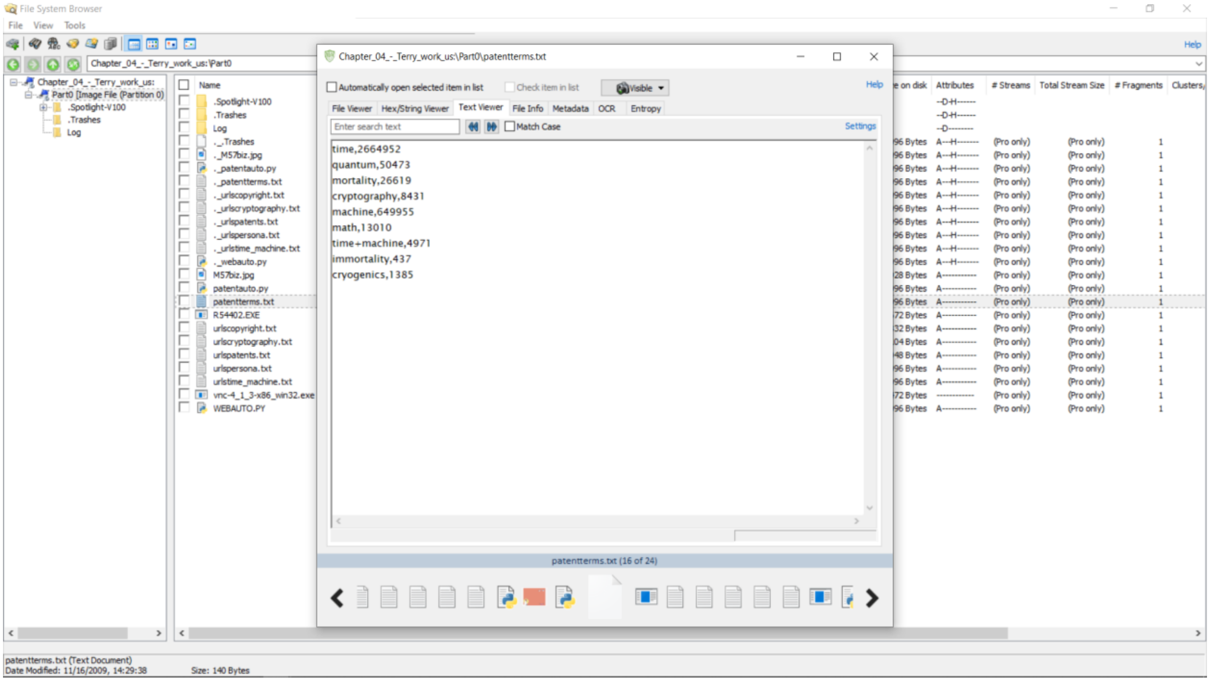


Chapter_04_-_Terry_work_us:
Part0 [Image File (Partition 0)]
.Spotlight-V100
.Trashes
Log

Name
.Spotlight-V100
.Trashes
Log
._.Trashes
._M57biz.jpg
._patentauto.py
._patentterms.txt
._urlscopyright.txt
._urlscryptography.txt
._urlspatents.txt
._urlspersona.txt
._urlstime_machine.txt
._webauto.py
M57biz.jpg
patentauto.py
patentterms.txt
R54402.EXE
urlscopyright.txt
urlscryptography.txt
urlspatents.txt
urlspersona.txt
urlstime_machine.txt
vnc-4_1_3-x86_win32.exe
WEBAUTO.PY

Image Type: JPEG image Dimensions: 1650 x 1275 Pixel Format: 24bit (RGB)

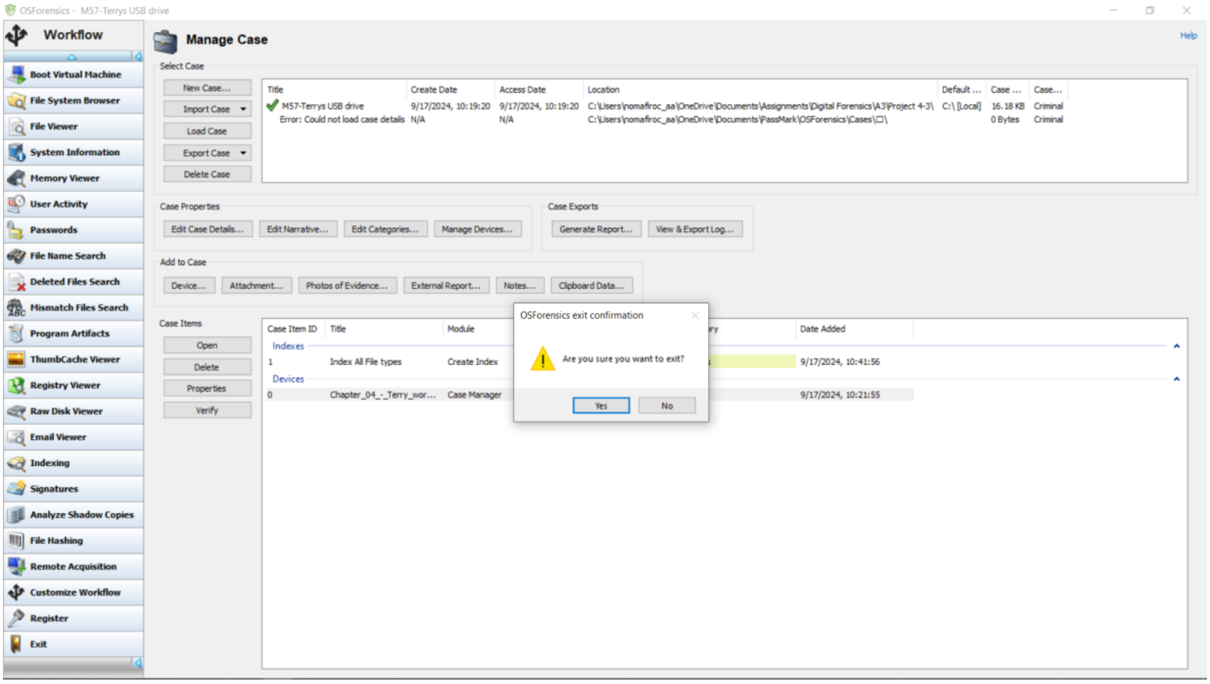
M57biz.jpg (JPG File)
Date Modified: 11/17/2009, 8:50:26 Size: 370.8 KB



```
time,2664952
quantum,50473
mortality,26619
cryptography,8431
machine,649955
math,13010
time+machine,4971
immortality,437
cryogenics,1385
```

patentterms.txt (Text Document)
Date Modified: 11/16/2009, 14:29:38 Size: 140 Bytes

Since we’re done with the analysis, exiting the case.



Title	Create Date	Access Date	Location	Default ...	Case ...	Case...
✓ M57-Terrys USB drive	9/17/2024, 10:19:20	9/17/2024, 10:19:20	C:\Users\nomafiroc_aa\OneDrive\Documents\Assignments\Digital Forensics\A3\Project 4-3\	C:\ [Local]	16.18 KB	Criminal
Error: Could not load case details	N/A	N/A	C:\Users\nomafiroc_aa\OneDrive\Documents\PassMark\OSForensics\Cases\□\		0 Bytes	Criminal

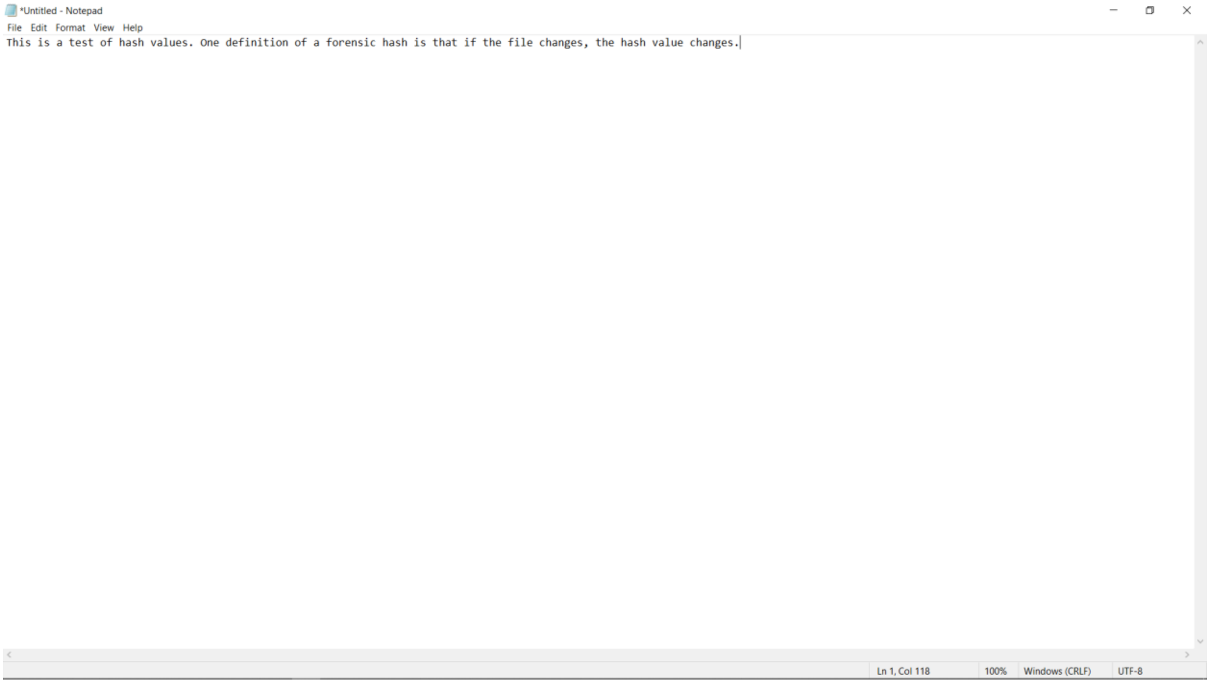
Case Item ID	Title	Module	...ry	Date Added
Indexes				
1	Index All File types	Create Index		9/17/2024, 10:41:56
Devices				
0	Chapter_04_-_Terry_wor...	Case Manager		9/17/2024, 10:21:55

OSForensics exit confirmation

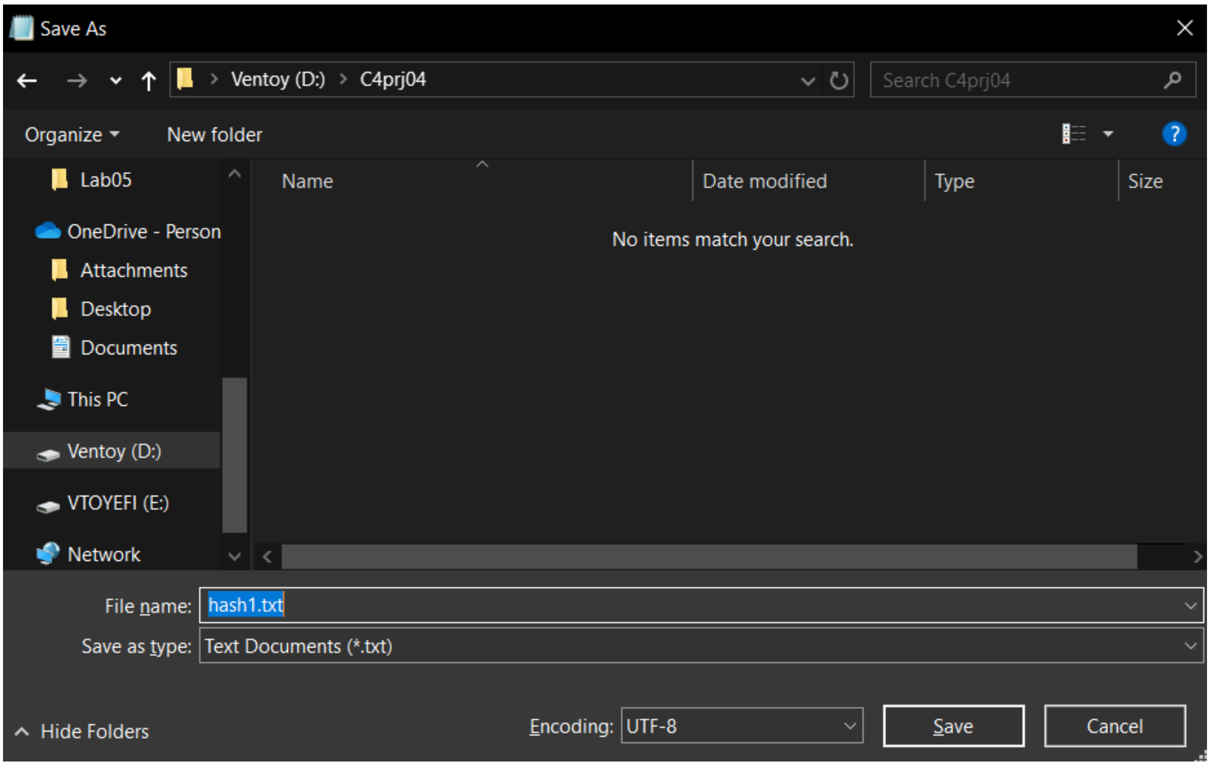
Are you sure you want to exit?

Project 4-4

In this project we're told to calculate hashes of a file before and after changes. So, first of all, making the original file :



```
This is a test of hash values. One definition of a forensic hash is that if the file changes, the hash value changes.
```



Save As

Ventoy (D:) > C4prj04

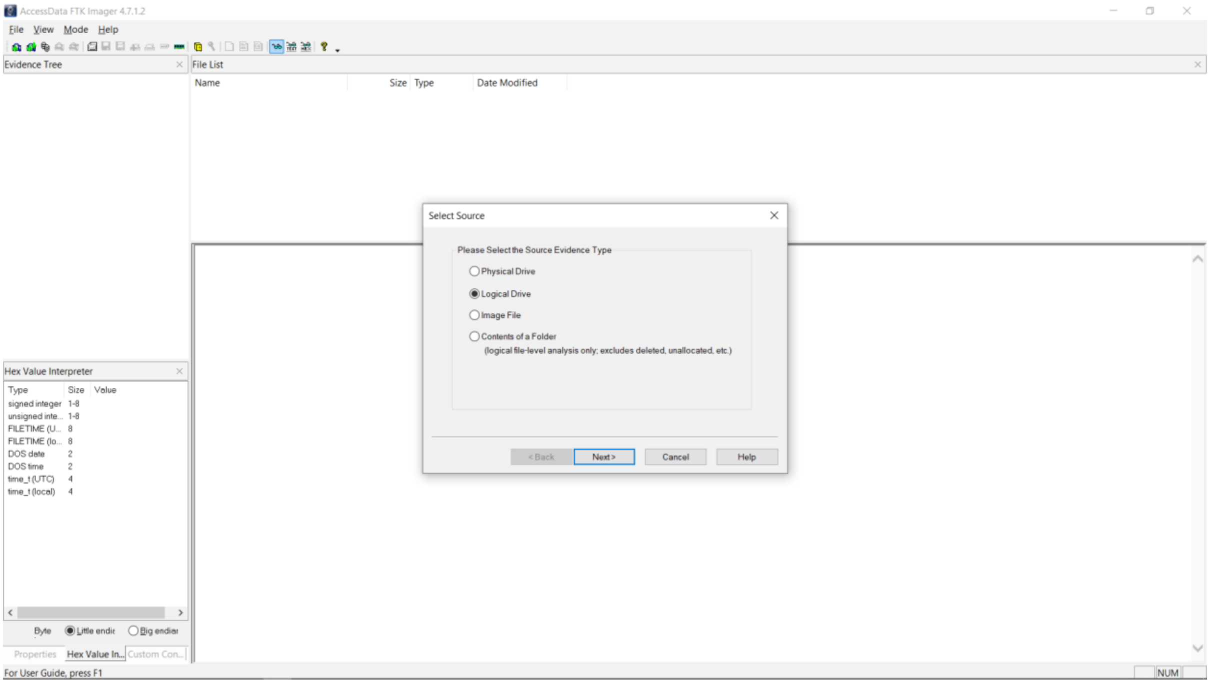
No items match your search.

File name: hash1.txt

Save as type: Text Documents (*.txt)

Encoding: UTF-8

Now we’re supposed to take the hash value using FTK Imager so for that, loading the USB drive into FTK Imager:



AccessData FTK Imager 4.7.1.2

Select Source

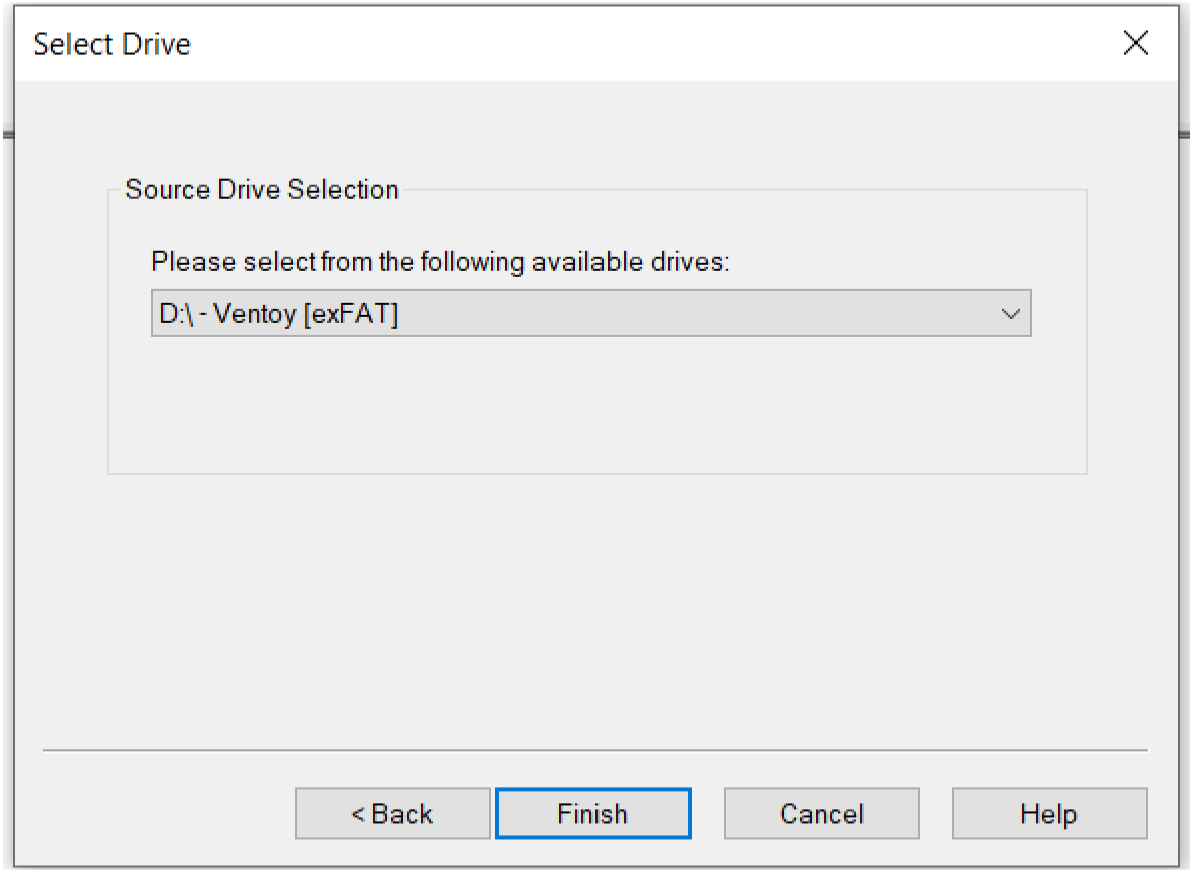
Please Select the Source Evidence Type

○ Physical Drive

● Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

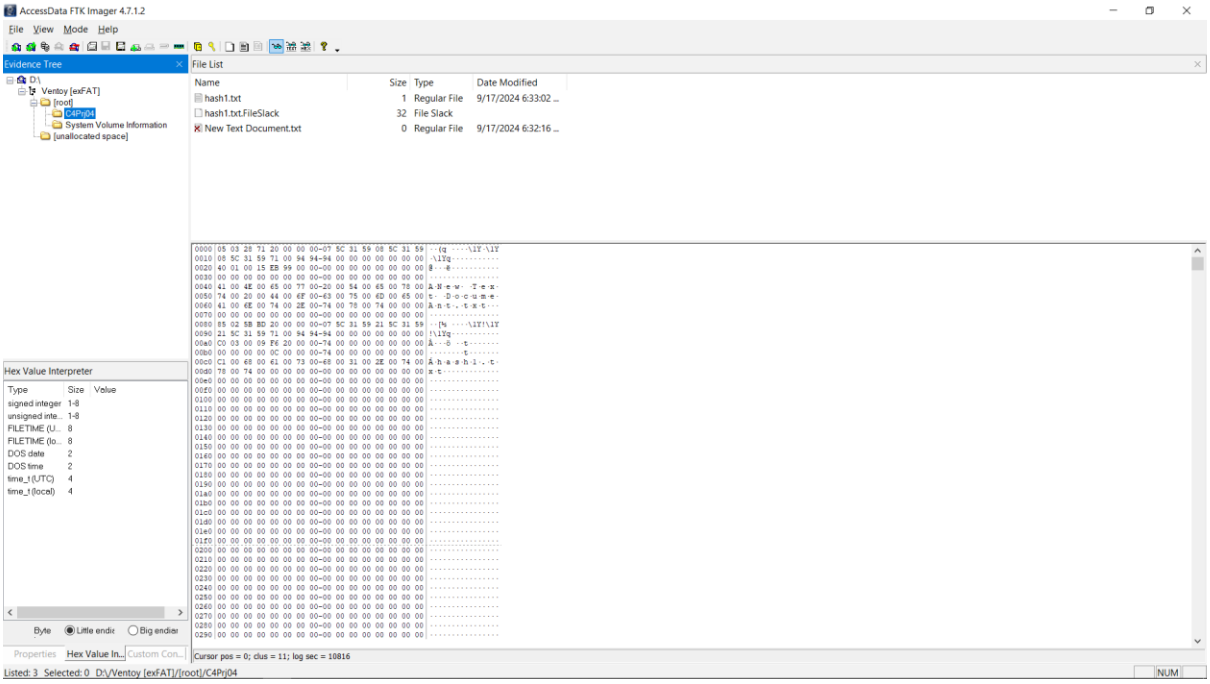


Select Drive

Source Drive Selection

Please select from the following available drives:

D:\ - Ventoy [exFAT]



AccessData FTK Imager 4.7.1.2

Evidence Tree:

```
D:\
  Ventoy [exFAT]
    [root]
      C4Prj04
      System Volume Information
    [unallocated space]
```

Name	Size	Type	Date Modified
hash1.txt	1	Regular File	9/17/2024 6:33:02 ...
hash1.txt.FileSlack	32	File Slack	
New Text Document.txt	0	Regular File	9/17/2024 6:32:16 ...

```
0000  05 03 28 71 20 00 00 00-07 5C 31 59 08 5C 31 59  ··(q ····\1Y·\1Y
0010  08 5C 31 59 71 00 94 94-94 00 00 00 00 00 00 00  ·\1Yq···········
0020  40 01 00 15 EB 99 00 00-00 00 00 00 00 00 00 00  @···ë···········
0030  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0040  41 00 4E 00 65 00 77 00-20 00 54 00 65 00 78 00  A·N·e·w· ·T·e·x·
0050  74 00 20 00 44 00 6F 00-63 00 75 00 6D 00 65 00  t· ·D·o·c·u·m·e·
0060  41 00 6E 00 74 00 2E 00-74 00 78 00 74 00 00 00  A·n·t·.·t·x·t···
0070  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0080  85 02 5B BD 20 00 00 00-07 5C 31 59 21 5C 31 59  ··[½ ····\1Y!\1Y
0090  21 5C 31 59 71 00 94 94-94 00 00 00 00 00 00 00  !\1Yq···········
00a0  C0 03 00 09 F6 20 00 00-74 00 00 00 00 00 00 00  À···ö ··t·······
00b0  00 00 00 00 0C 00 00 00-74 00 00 00 00 00 00 00  ········t·······
00c0  C1 00 68 00 61 00 73 00-68 00 31 00 2E 00 74 00  Á·h·a·s·h·1·.·t·
00d0  78 00 74 00 00 00 00 00-00 00 00 00 00 00 00 00  x·t·············
00e0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00f0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0100  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0110  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0120  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0130  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0140  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0150  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0160  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0170  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0180  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0190  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
01a0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
01b0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
01c0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
01d0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
01e0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
01f0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0200  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0210  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0220  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0230  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0240  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0250  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0260  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0270  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0280  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0290  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
```

Hex Value Interpreter

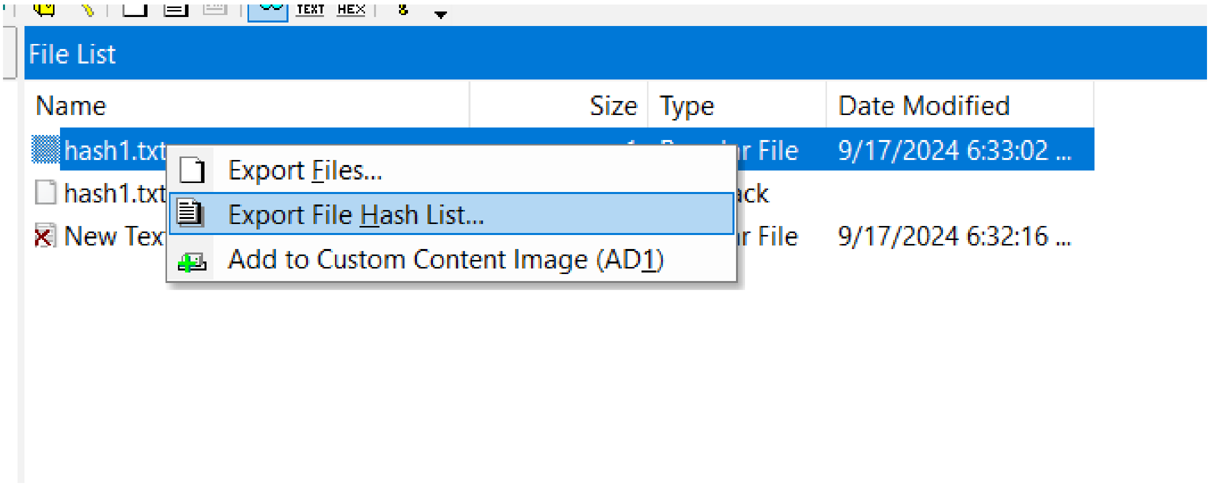
Type	Size	Value
signed integer	1-8	
unsigned inte...	1-8	
FILETIME (U...	8	
FILETIME (lo...	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

● Little endi ○ Big endiar

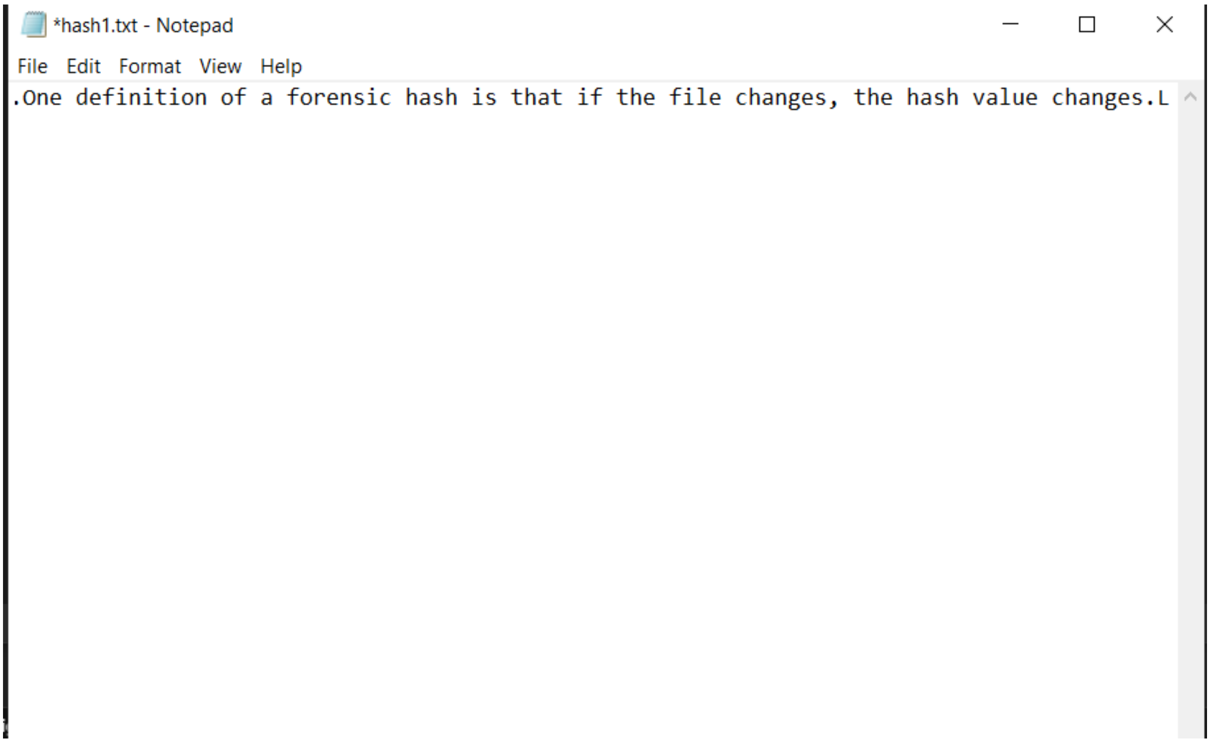
Cursor pos = 0; clus = 11; log sec = 10816

Listed: 3 Selected: 0 D:\/Ventoy [exFAT]/[root]/C4Prj04

Now, exporting the original hash value:



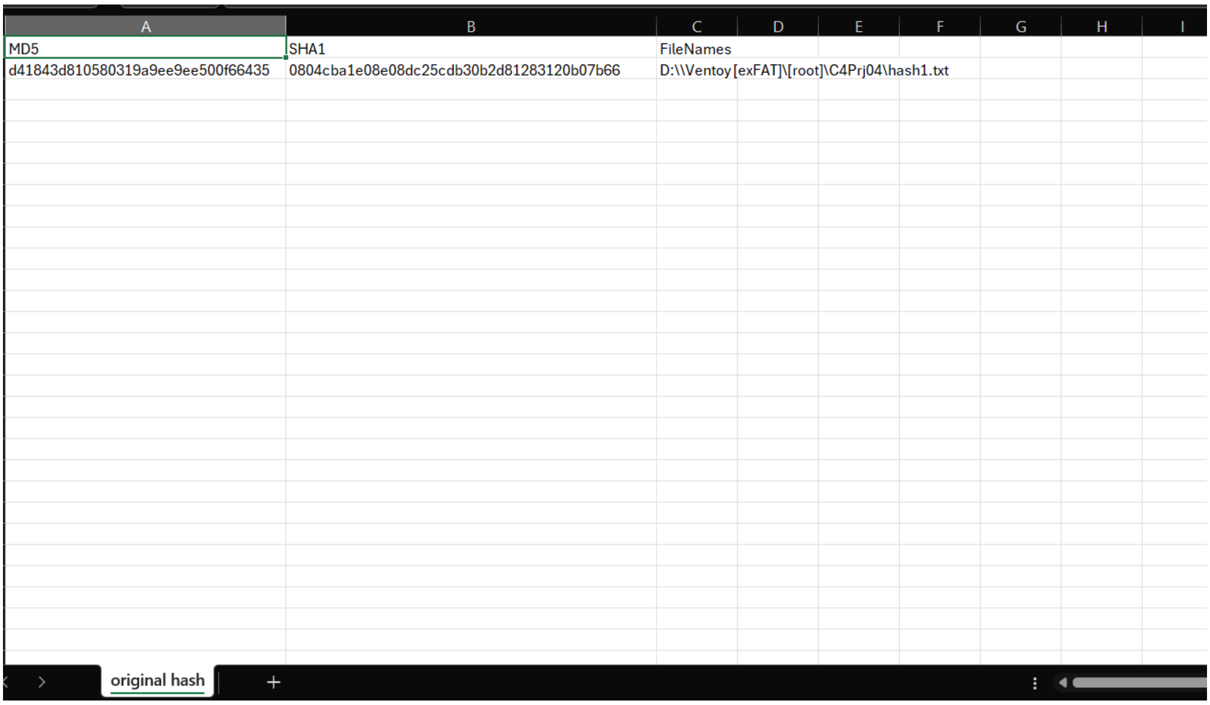
Since we have to check for the hash after making a change in the file, here I’m adding the character “L” at the end of the file to see what change it makes on the hash value.



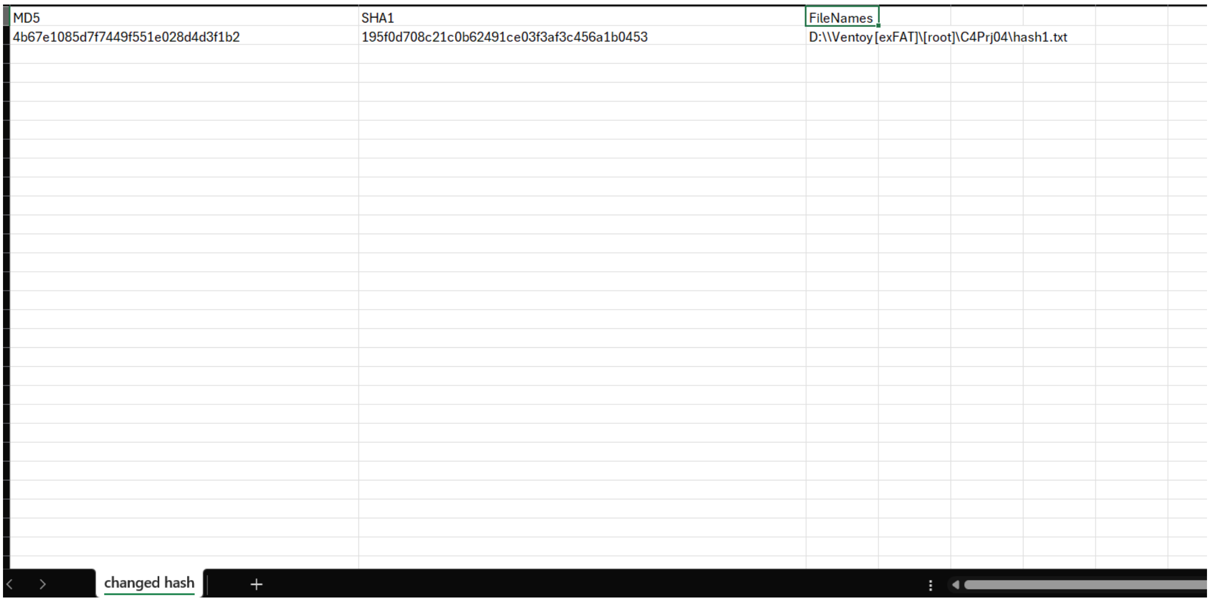
```
.One definition of a forensic hash is that if the file changes, the hash value changes.L
```

Now, we’re supposed to repeat the same steps as before to export the hash value form FTK Imager.

These are the original and changed file hashes respectively:



MD5	SHA1	FileNames
d41843d810580319a9ee9ee500f66435	0804cba1e08e08dc25cdb30b2d81283120b07b66	D:\\Ventoy [exFAT]\[root]\C4Prj04\hash1.txt



MD5	SHA1	FileNames
4b67e1085d7f7449f551e028d4d3f1b2	195f0d708c21c0b62491ce03f3af3c456a1b0453	D:\\Ventoy [exFAT]\[root]\C4Prj04\hash1.txt

Both hashes have clearly changed.

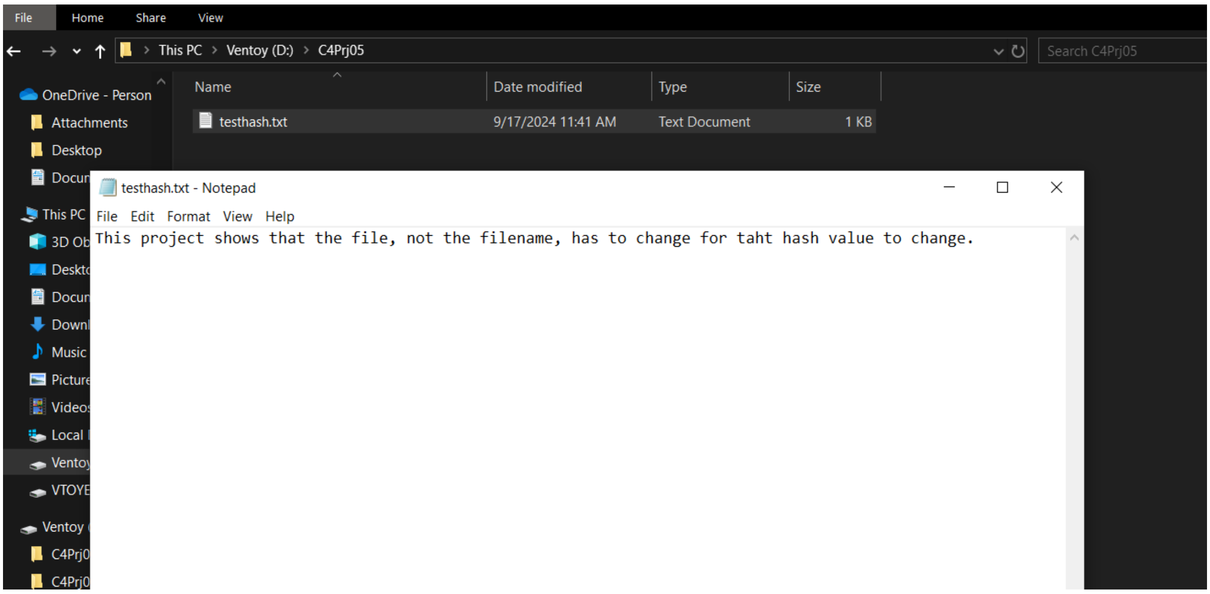
Original Hash : d41843d810580319a9ee9ee500f66435

Changed Hash : 4b67e1085d7f7449f551e028d4d3f1b2

Now we know that if there's even a slight change in the file contents, the hash value changes.

Project 4-5

In this project, we have to show that changing the extension of the file doesn't affect it's hash value, so first of all, making a text file.



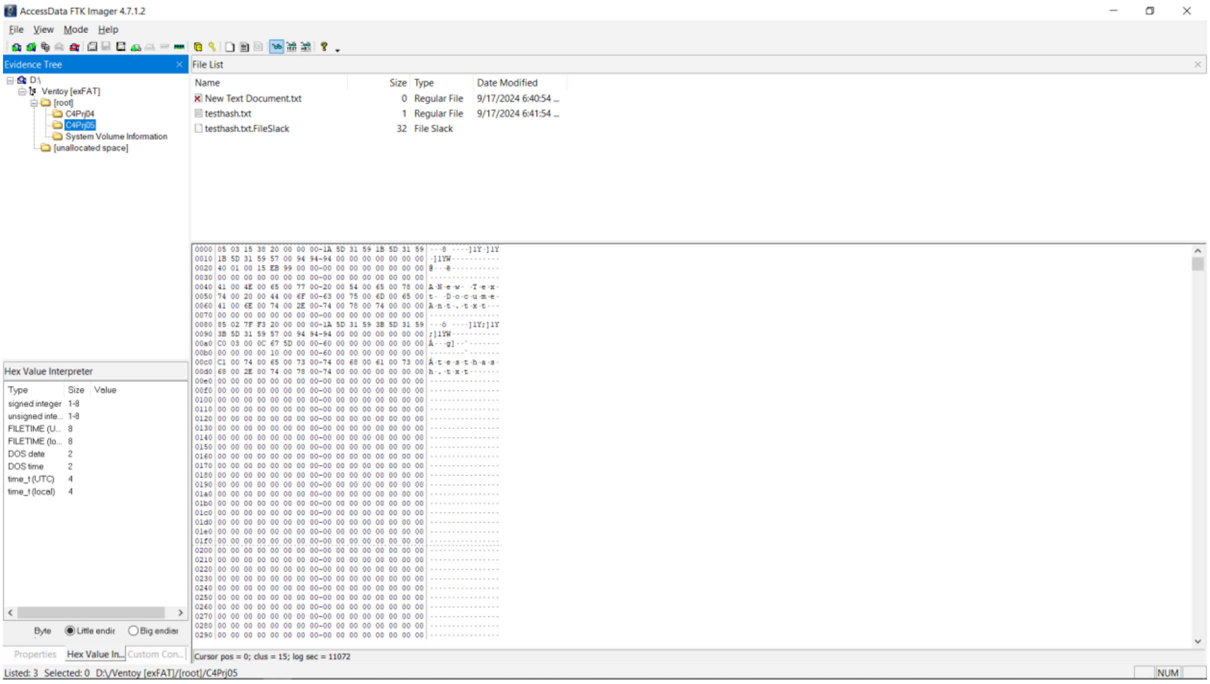
This PC > Ventoy (D:) > C4Prj05

Name	Date modified	Type	Size
testhash.txt	9/17/2024 11:41 AM	Text Document	1 KB

testhash.txt - Notepad

```
This project shows that the file, not the filename, has to change for taht hash value to change.
```

Loaded the USB drive into FTK Imager to export the original hash value:



AccessData FTK Imager 4.7.1.2

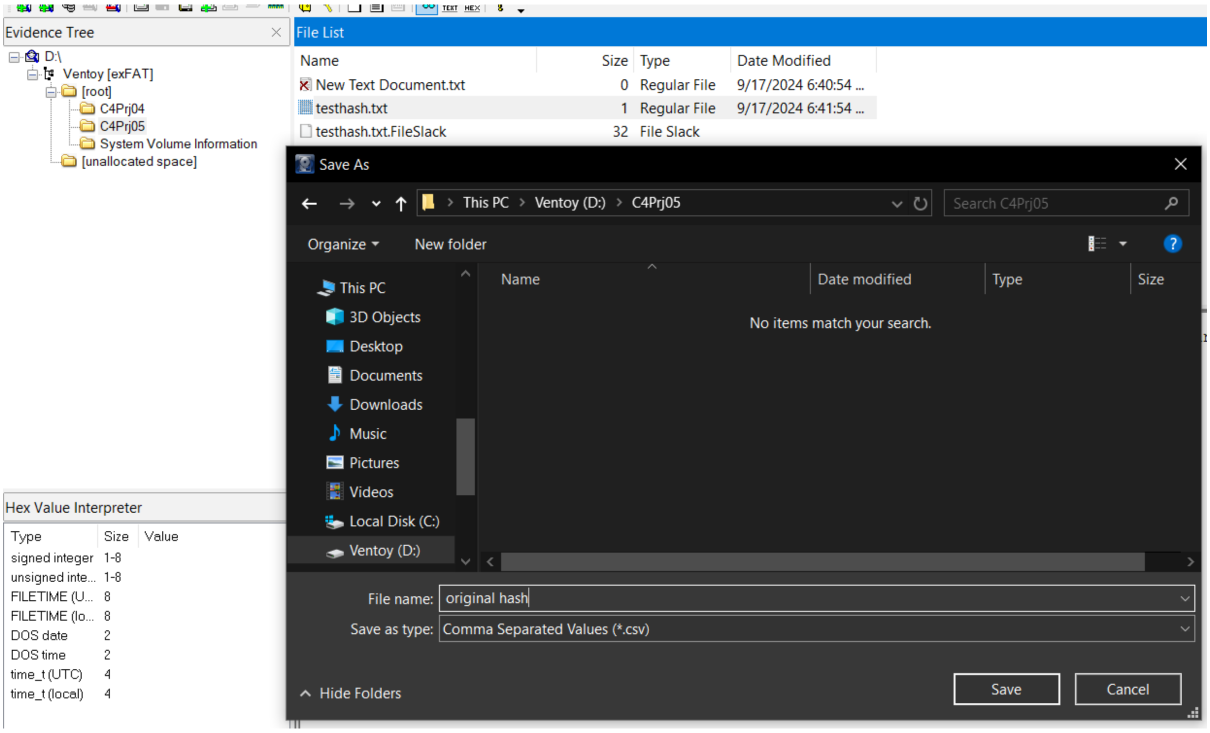
Name	Size	Type	Date Modified
New Text Document.txt	0	Regular File	9/17/2024 6:40:54 ...
testhash.txt	1	Regular File	9/17/2024 6:41:54 ...
testhash.txt.FileSlack	32	File Slack	

```
0000 05 03 15 38 20 00 00 00-1A 5D 31 59 1B 5D 31 59  ···8 ····]1Y·]1Y
0010 1B 5D 31 59 57 00 94 94-94 00 00 00 00 00 00 00  ·]1YW···········
0020 40 01 00 15 EB 99 00 00-00 00 00 00 00 00 00 00  @···ë···········
0030 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0040 41 00 4E 00 65 00 77 00-20 00 54 00 65 00 78 00  A·N·e·w· ·T·e·x·
0050 74 00 20 00 44 00 6F 00-63 00 75 00 6D 00 65 00  t· ·D·o·c·u·m·e·
0060 41 00 6E 00 74 00 2E 00-74 00 78 00 74 00 00 00  A·n·t·.·t·x·t···
0070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0080 85 02 7F F3 20 00 00 00-1A 5D 31 59 3B 5D 31 59  ···ó ····]1Y;]1Y
0090 3B 5D 31 59 57 00 94 94-94 00 00 00 00 00 00 00  ;]1YW···········
00a0 C0 03 00 0C 67 5D 00 00-60 00 00 00 00 00 00 00  À···g]··`·······
00b0 00 00 00 00 10 00 00 00-60 00 00 00 00 00 00 00  ········`·······
00c0 C1 00 74 00 65 00 73 00-74 00 68 00 61 00 73 00  Á·t·e·s·t·h·a·s·
00d0 68 00 2E 00 74 00 78 00-74 00 00 00 00 00 00 00  h·.·t·x·t·······
00e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0120 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0130 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0140 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0150 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0160 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0170 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0180 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0190 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
01a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
01b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
01c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
01d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
01e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
01f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0200 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0210 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0220 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0230 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0240 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0250 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0260 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0270 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0280 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0290 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
```

Type	Size	Value
signed integer	1-8	
unsigned inte...	1-8	
FILETIME (U...	8	
FILETIME (lo...	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

Cursor pos = 0; clus = 15; log sec = 11072

Listed: 3 Selected: 0 D:\Ventoy [exFAT]/[root]/C4Prj05



Evidence Tree

- D:\
  - Ventoy [exFAT]
    - [root]
      - C4Prj04
      - C4Prj05
      - System Volume Information
    - [unallocated space]

File List

Name	Size	Type	Date Modified
New Text Document.txt	0	Regular File	9/17/2024 6:40:54 ...
testhash.txt	1	Regular File	9/17/2024 6:41:54 ...
testhash.txt.FileSlack	32	File Slack	

Hex Value Interpreter

Type	Size	Value
signed integer	1-8	
unsigned inte...	1-8	
FILETIME (U...	8	
FILETIME (lo...	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

Save As

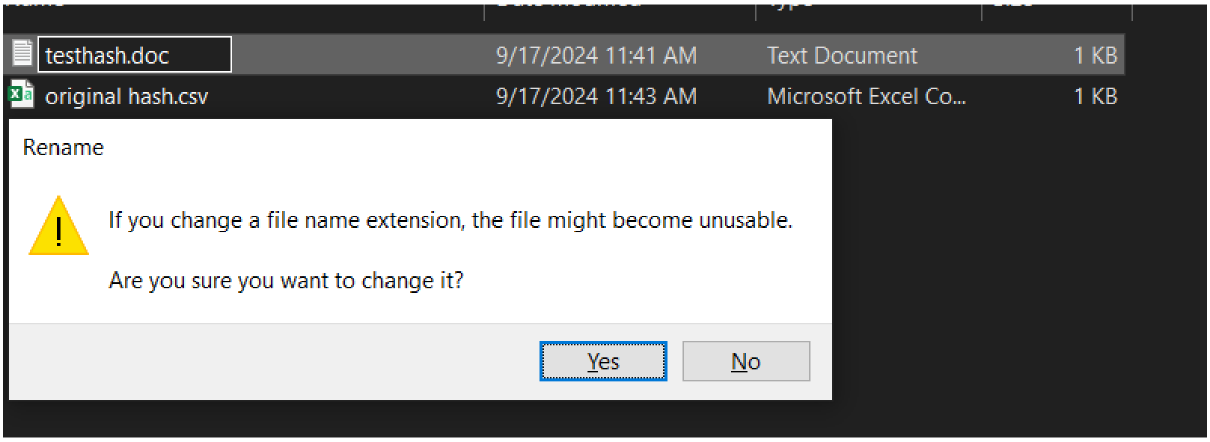
This PC > Ventoy (D:) > C4Prj05

No items match your search.

File name: original hash

Save as type: Comma Separated Values (*.csv)

Now to check if the hash changes, changing the extension of the text file to .doc



testhash.doc	9/17/2024 11:41 AM	Text Document	1 KB
original hash.csv	9/17/2024 11:43 AM	Microsoft Excel Co...	1 KB

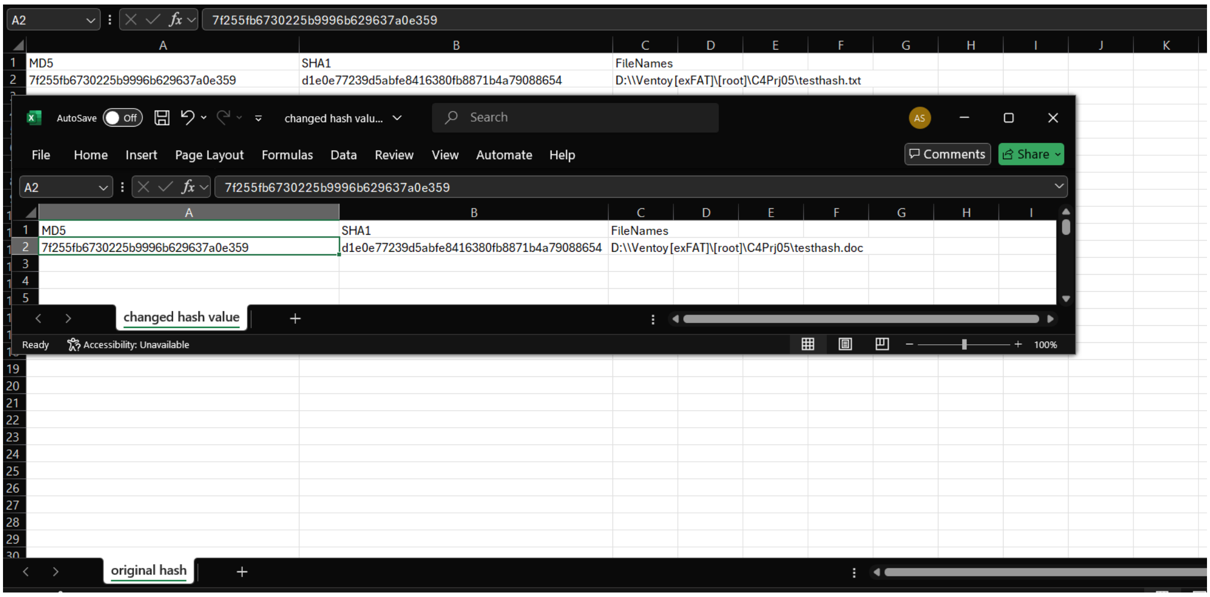
Rename

If you change a file name extension, the file might become unusable.

Are you sure you want to change it?

Afterwards, we calculate the hash of the file again to see if the hash changes or not.

The following are the hashes obtained:



A2 7f255fb6730225b9996b629637a0e359

	A	B	C
1	MD5	SHA1	FileNames
2	7f255fb6730225b9996b629637a0e359	d1e0e77239d5abfe8416380fb8871b4a79088654	D:\\Ventoy [exFAT]\[root]\C4Prj05\testhash.txt

original hash

A2 7f255fb6730225b9996b629637a0e359

	A	B	C
1	MD5	SHA1	FileNames
2	7f255fb6730225b9996b629637a0e359	d1e0e77239d5abfe8416380fb8871b4a79088654	D:\\Ventoy [exFAT]\[root]\C4Prj05\testhash.doc

changed hash value

The hashes are the same.

Original Hash : 7f255fb6730225b9996b629637a0e359

Changed Hash : 7f255fb6730225b9996b629637a0e359

Now we know that changing the extension of the files doesn't affect the hash value.

- ## Summary

Throughout these projects, we have received hands on practice of the two tools OSForensics and FTK Imager along with crucial information on how and what affects file hashes.

- ## References

Nelson, B., Philips, A., & Steuart, C. (n.d.). *Guide to Computer Forensics and Investigations.*