National University of Computer and Emerging Sciences
Islamabad Campus

CY2002

Digital Forensics

Assignment 01
Hands-On Projects

Submitted by: Mirza Humayun Masood
Roll number: I22-1749
Date: 16/9/2024

Table of Contents

Introduction

In this assignment we were given 6 hands on projects to investigate in autopsy so we can get a better understanding of the tool and basics of Digital Forensics.

Note: Table of content should be updated automatically. Just click on table of contents and click on update table.

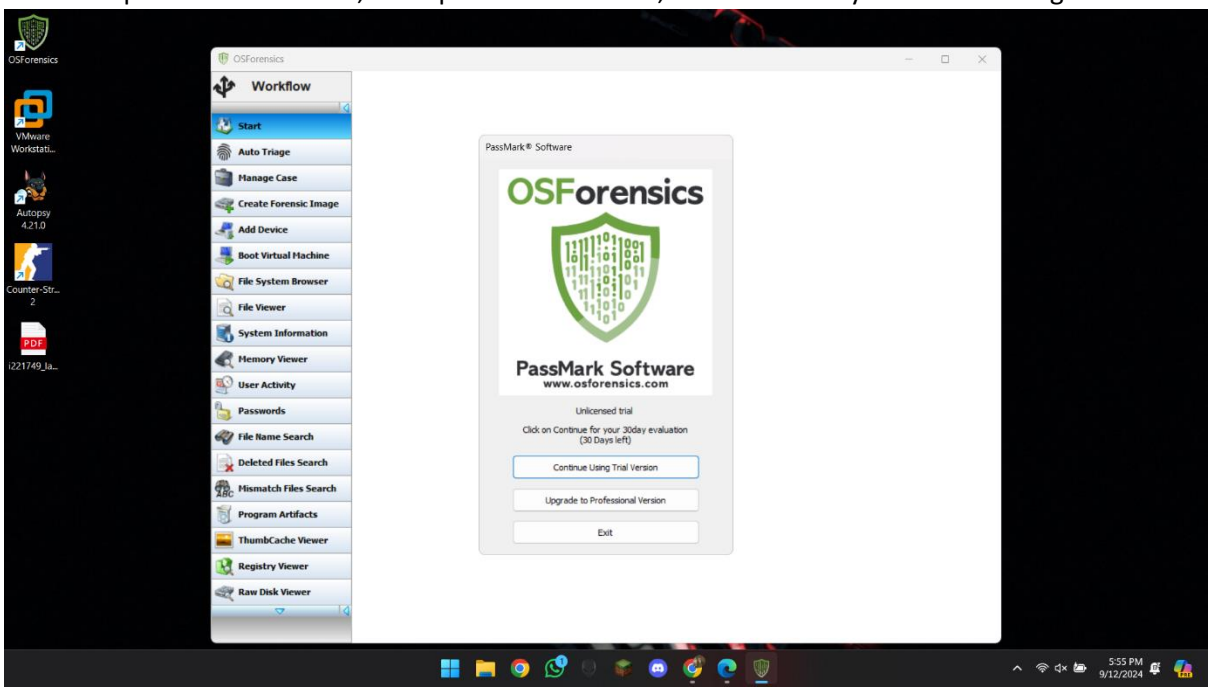
Details and Steps

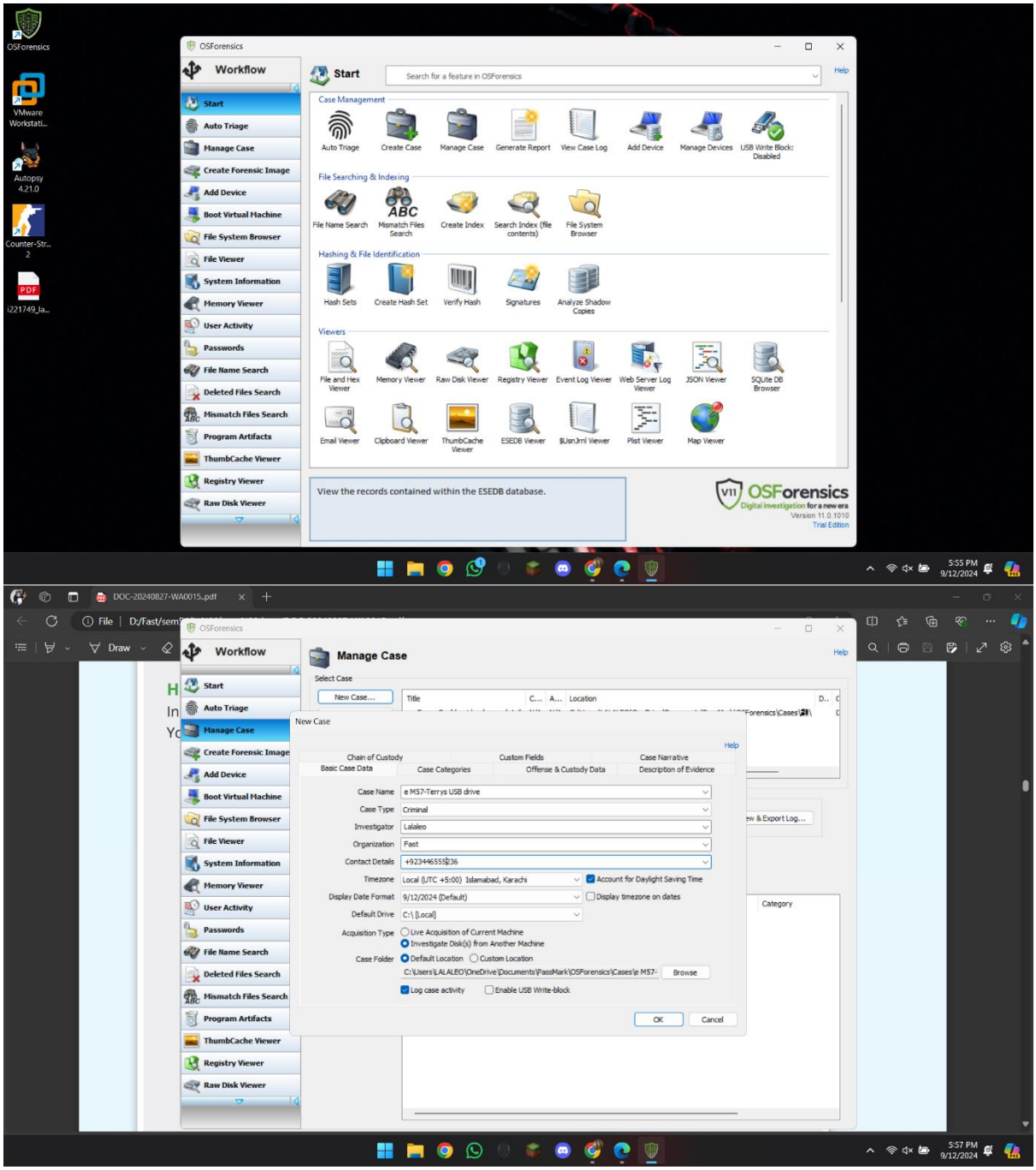
Hands-On Project 4-3

So in this Project, We had to use osforensics to tell if terry is involved with anything illicit.

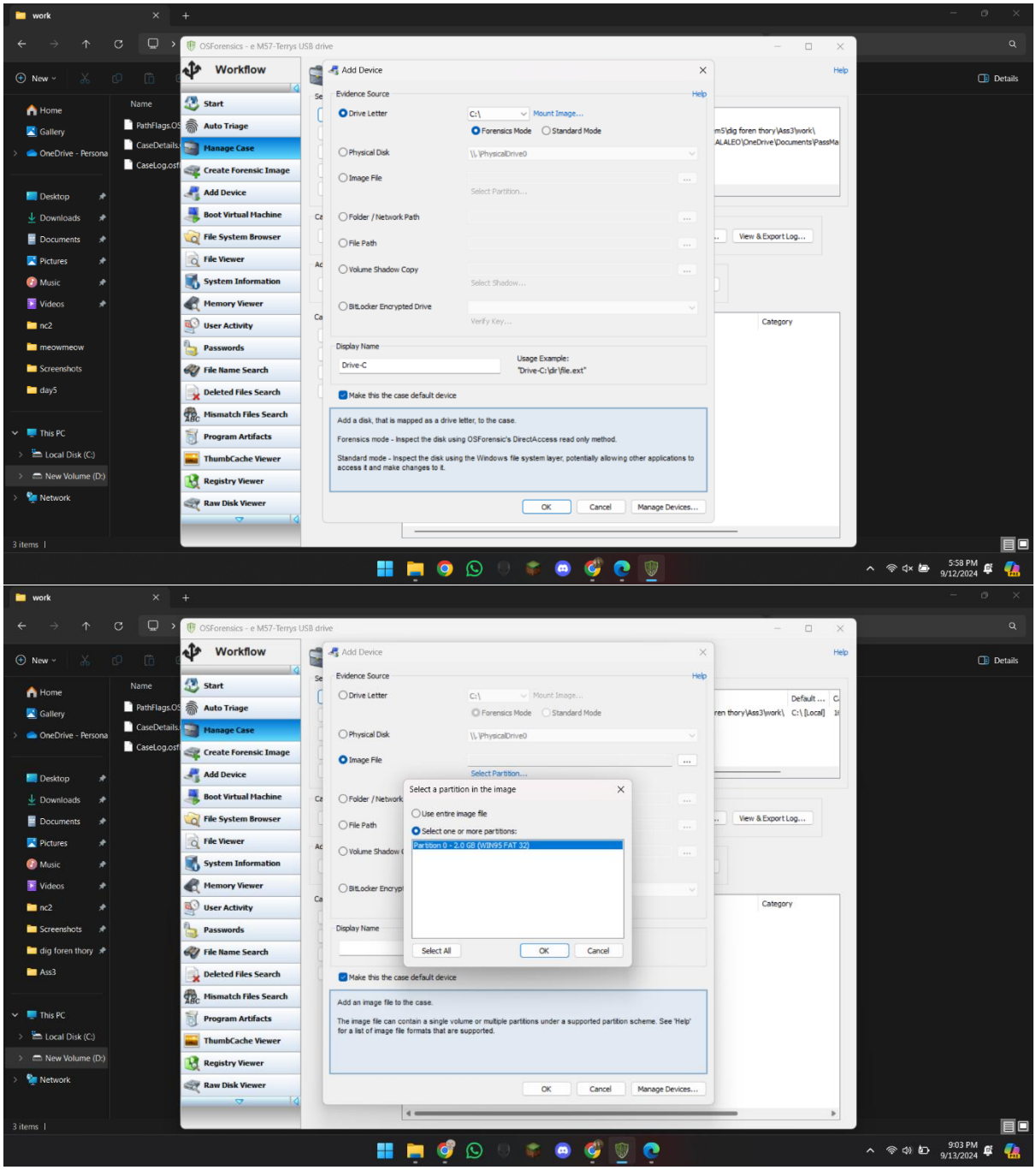
So first I opened the OSForensics software.

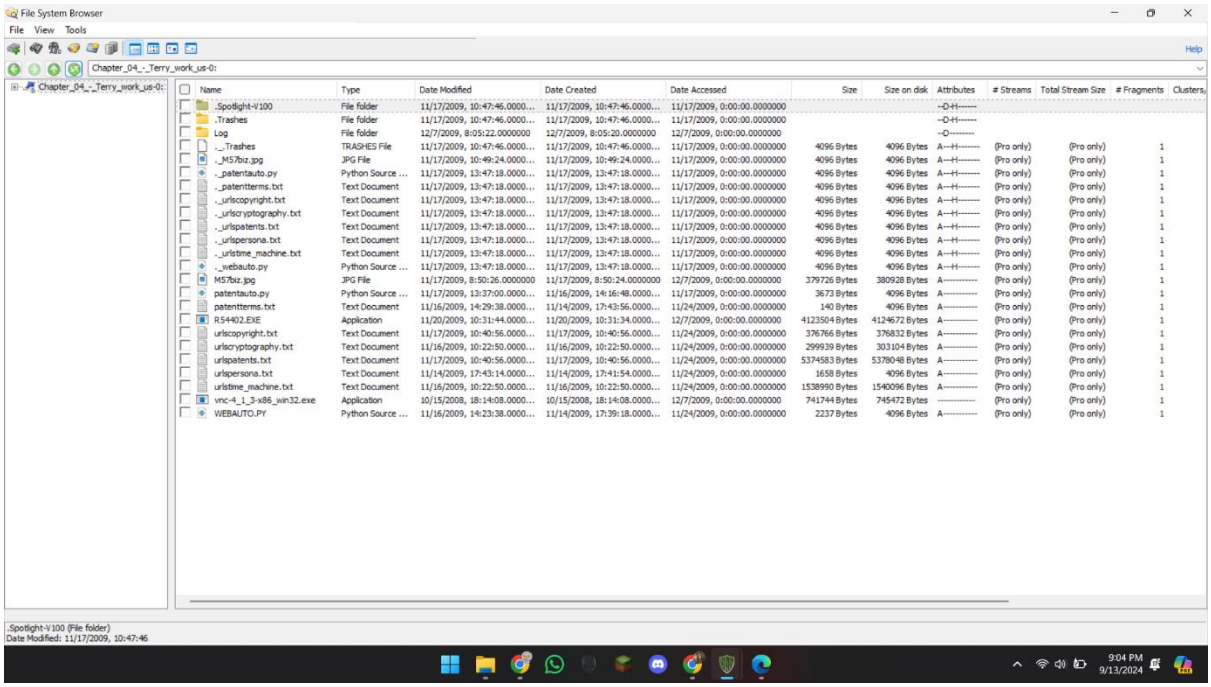
So first I opened the software, and opened a new case , and added terry's usb as an image file.



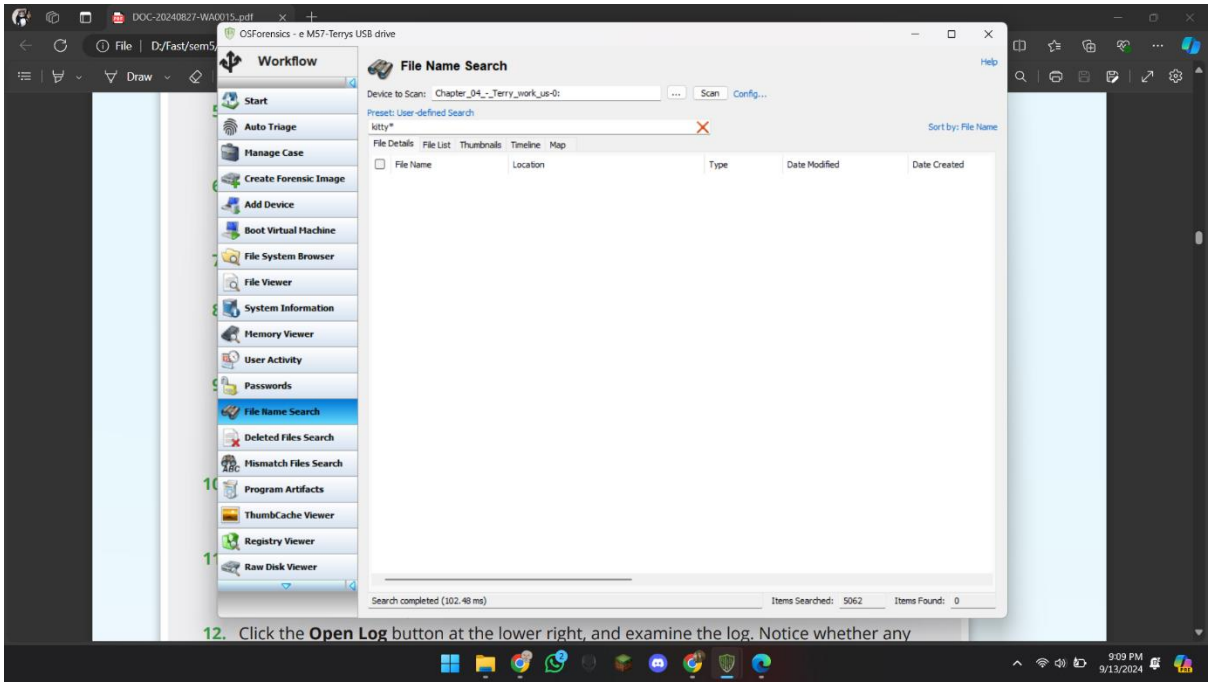

OSForensics
Workflow
Start
Auto Triage
Manage Case
Create Forensic Image
Add Device
Boot Virtual Machine
File System Browser
File Viewer
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted Files Search
Mismatch Files Search
Program Artifacts
ThumbCache Viewer
Registry Viewer
Raw Disk Viewer
Search for a feature in OSForensics
Case Management
Auto Triage
Create Case
Manage Case
Generate Report
View Case Log
Add Device
Manage Devices
USB Write Block: Disabled
File Searching & Indexing
File Name Search
Mismatch Files Search
Create Index
Search Index (file contents)
File System Browser
Hashing & File Identification
Hash Sets
Create Hash Set
Verify Hash
Signatures
Analyze Shadow Copies
Viewers
File and Hex Viewer
Memory Viewer
Raw Disk Viewer
Registry Viewer
Event Log Viewer
Web Server Log Viewer
JSON Viewer
SQLite DB Browser
Email Viewer
Clipboard Viewer
ThumbCache Viewer
ESEDB Viewer
$UsnJrnl Viewer
Plist Viewer
Map Viewer
View the records contained within the ESEDB database.
OSForensics
Digital investigation for a new era
Version 11.0.1010
Trial Edition
5:55 PM
9/12/2024

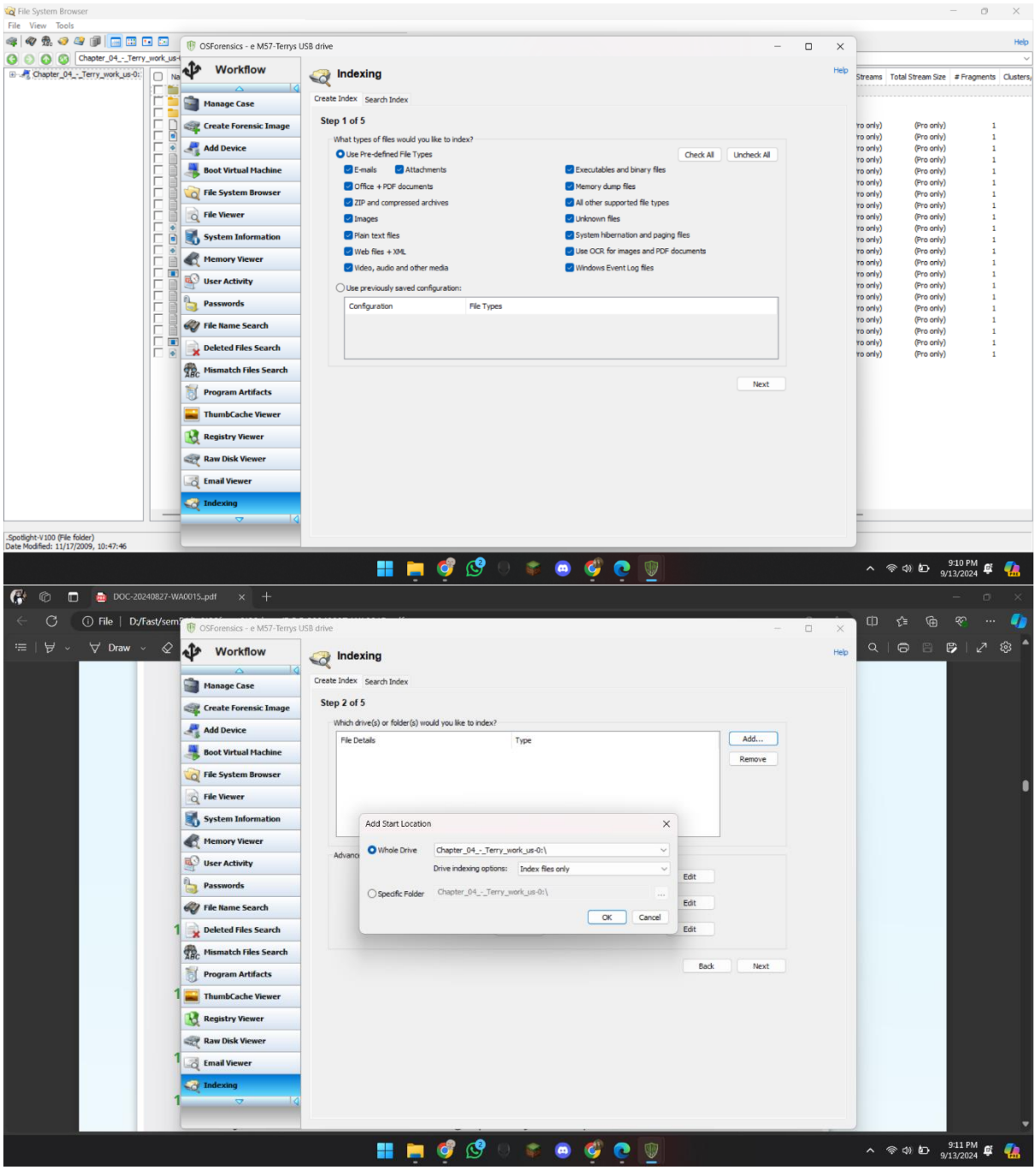
DOC-20240827-WA0015..pdf
Workflow
Manage Case
Select Case
New Case...
Title
Location
New Case
Chain of Custody
Custom Fields
Case Narrative
Basic Case Data
Case Categories
Offense & Custody Data
Description of Evidence
Case Name
e M57-Terrys USB drive
Case Type
Criminal
Investigator
Lalaleo
Organization
Fast
Contact Details
+923446555036
Timezone
Local (UTC +5:00) Islamabad, Karachi
Account for Daylight Saving Time
Display Date Format
9/12/2024 (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\LALALEO\OneDrive\Documents\PassMark\OSForensics\Cases\e M57-
Browse
Log case activity
Enable USB Write-block
OK
Cancel
Category
5:57 PM
9/12/2024

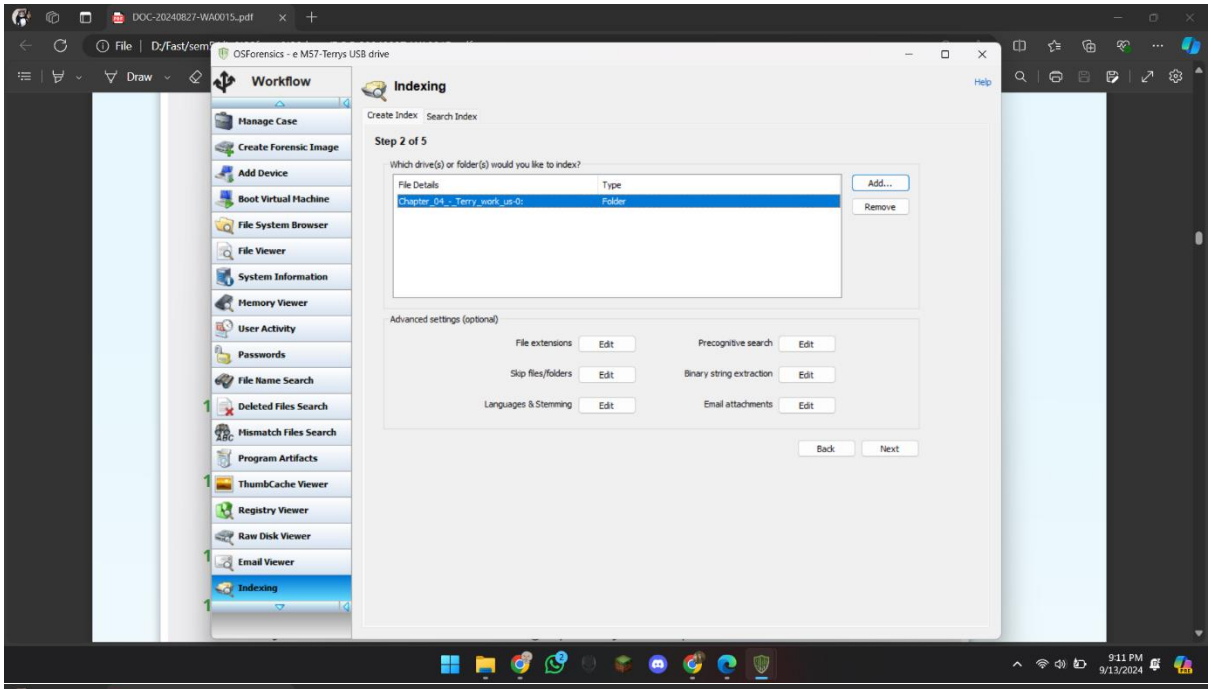

work
OSForensics - e M57-Terrys USB drive
Workflow
Start
Auto Triage
Manage Case
Create Forensic Image
Add Device
Boot Virtual Machine
File System Browser
File Viewer
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted Files Search
Mismatch Files Search
Program Artifacts
ThumbCache Viewer
Registry Viewer
Raw Disk Viewer
Add Device
Evidence Source
Drive Letter
Physical Disk
Image File
Folder / Network Path
File Path
Volume Shadow Copy
BitLocker Encrypted Drive
Display Name
Drive-C
Make this the case default device
Add a disk, that is mapped as a drive letter, to the case.
Forensics mode - Inspect the disk using OSForensic's DirectAccess read only method.
Standard mode - Inspect the disk using the Windows file system layer, potentially allowing other applications to access it and make changes to it.
OK
Cancel
Manage Devices...
Select a partition in the image
Use entire image file
Select one or more partitions:
Partition 0 - 2.0 GB (WIN95 FAT 32)
Select All
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.

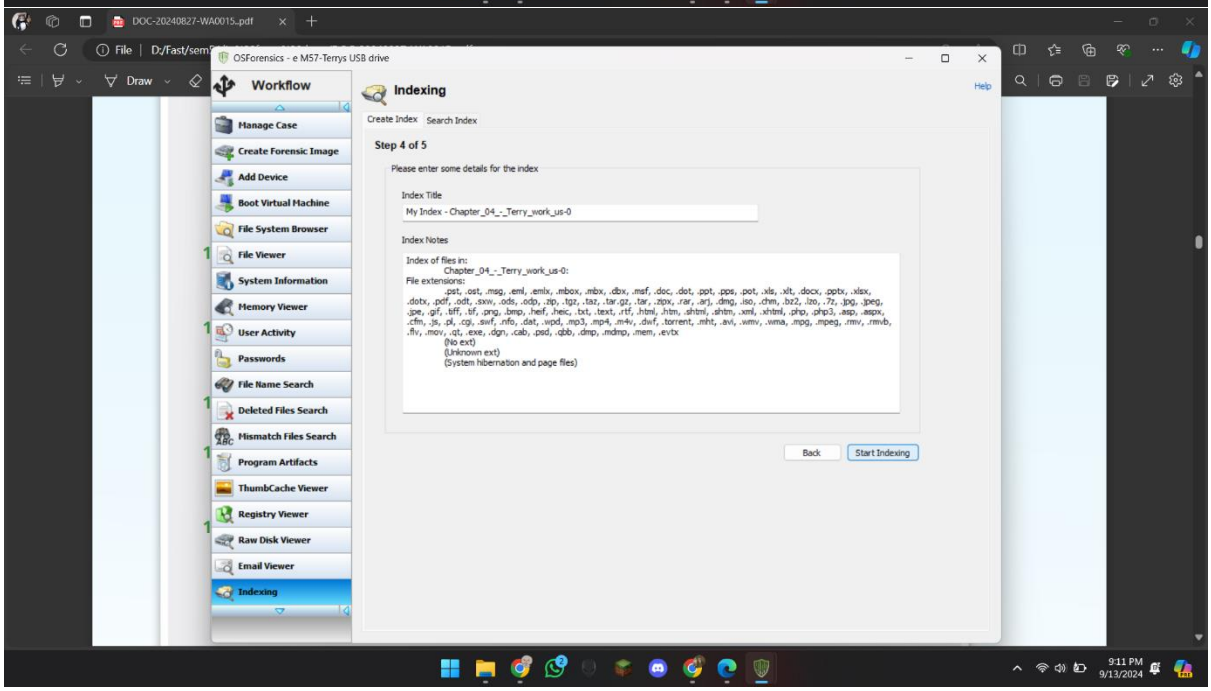


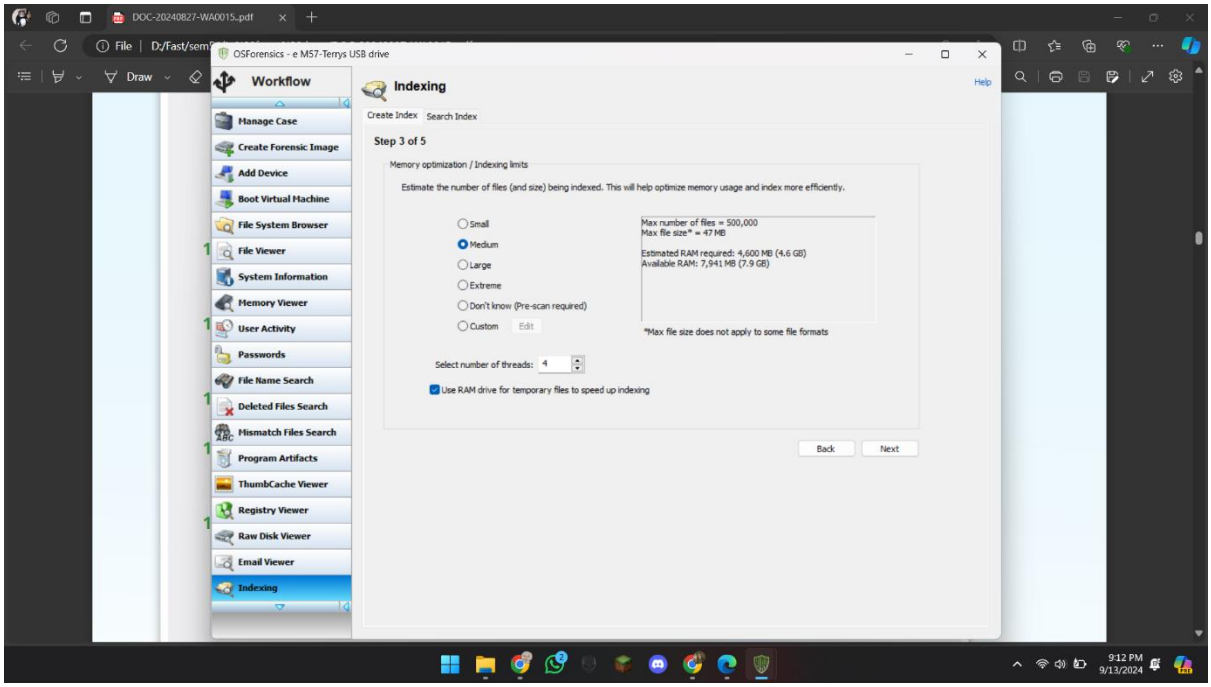
Here I went to File name search and wrote Kitty*, but could not found anything, Then I decided to create index, and filled out the requirements for that.



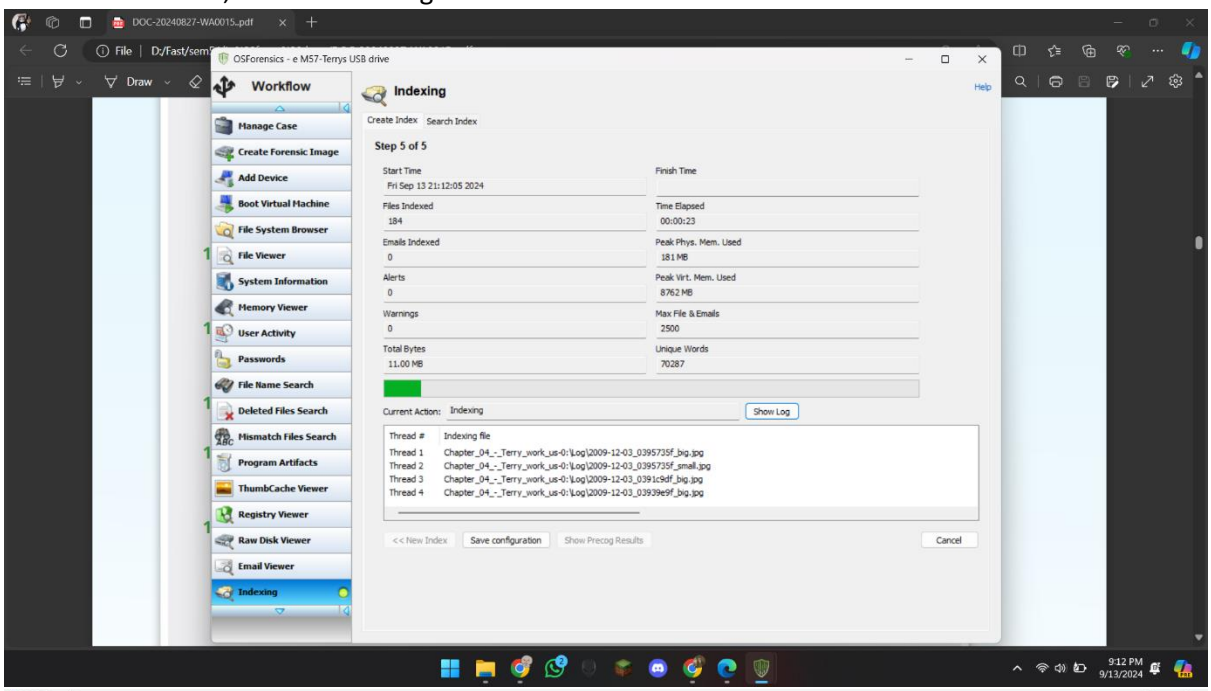

File System Browser
File View Tools
OSForensics - e M57-Terrys USB drive
Workflow
Manage Case
Create Forensic Image
Add Device
Boot Virtual Machine
File System Browser
File Viewer
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted Files Search
Mismatch Files Search
Program Artifacts
ThumbCache Viewer
Registry Viewer
Raw Disk Viewer
Email Viewer
Indexing
Indexing
Create Index
Search Index
Step 1 of 5
What types of files would you like to index?
Use Pre-defined File Types
Check All
Uncheck All
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
Next
Help
9:10 PM
9/13/2024
DOC-20240827-WA0015..pdf
Step 2 of 5
Which drive(s) or folder(s) would you like to index?
File Details
Type
Add...
Remove
Add Start Location
Whole Drive
Chapter_04_-_Terry_work_us-0:\
Drive indexing options:
Index files only
Specific Folder
OK
Cancel
Edit
Back
Next
9:11 PM
9/13/2024

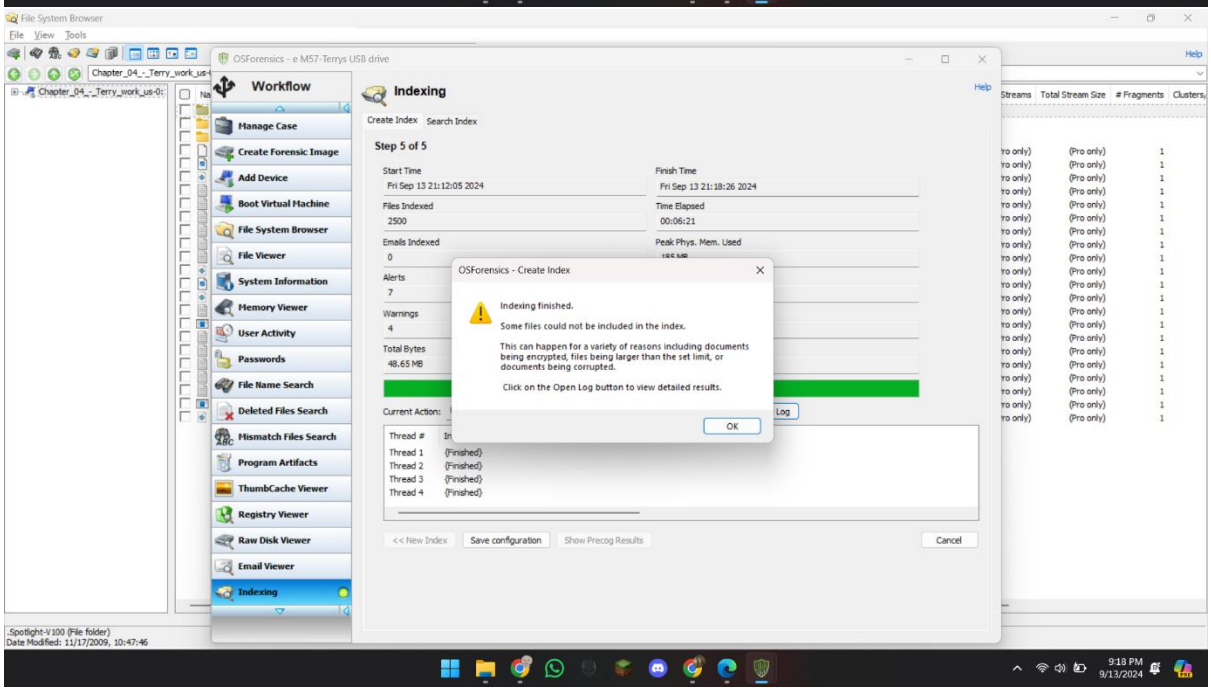

OSForensics - e M57-Terrys USB drive
Workflow
Manage Case
Create Forensic Image
Add Device
Boot Virtual Machine
File System Browser
File Viewer
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted Files Search
Mismatch Files Search
Program Artifacts
ThumbCache Viewer
Registry Viewer
Raw Disk Viewer
Email Viewer
Indexing
Indexing
Help
Create Index
Search Index
Step 2 of 5
Which drive(s) or folder(s) would you like to index?
File Details
Type
Chapter_04_-_Terry_work_us-0:
Folder
Add...
Remove
Advanced settings (optional)
File extensions
Edit
Precognitive search
Edit
Skip files/folders
Edit
Binary string extraction
Edit
Languages & Stemming
Edit
Email attachments
Edit
Back
Next


OSForensics - e M57-Terrys USB drive
Workflow
Indexing
Help
Create Index
Search Index
Step 4 of 5
Please enter some details for the index
Index Title
My Index - Chapter_04_-_Terry_work_us-0
Index Notes
Index of files in:
Chapter_04_-_Terry_work_us-0:
File extensions:
(No ext)
(Unknown ext)
(System hibernation and page files)
Back
Start Indexing

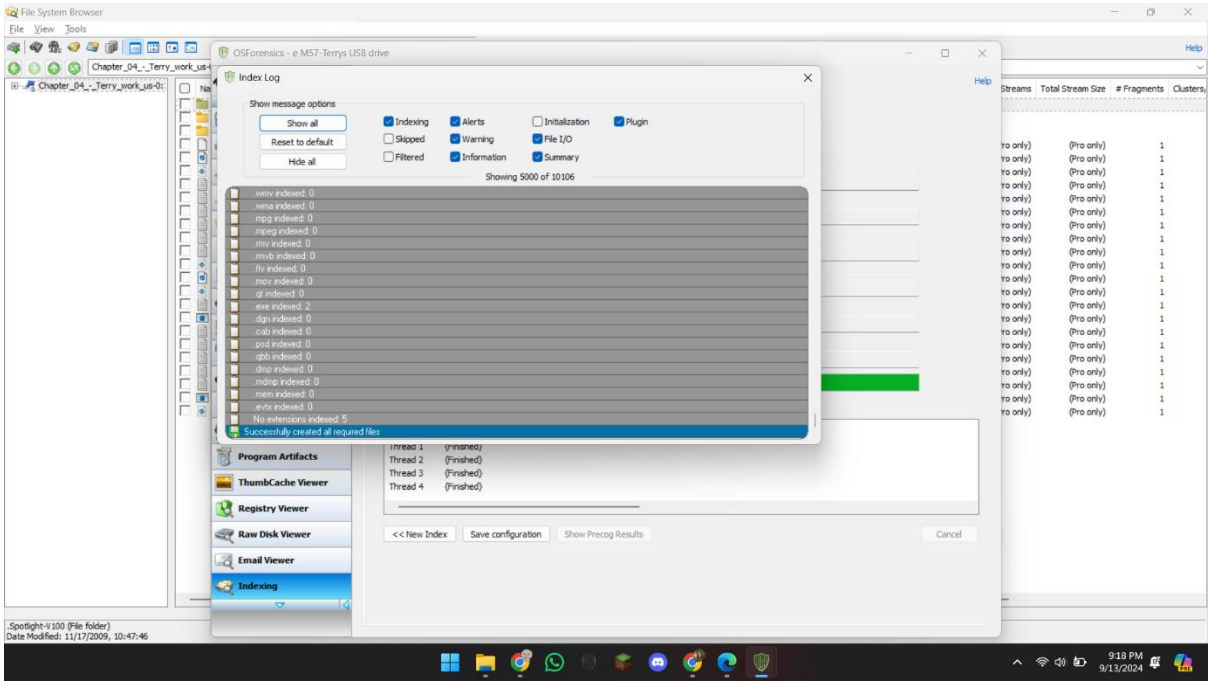

OSForensics - e M57-Terrys USB drive
Workflow
Manage Case
Create Forensic Image
Add Device
Boot Virtual Machine
File System Browser
File Viewer
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted Files Search
Mismatch Files Search
Program Artifacts
ThumbCache Viewer
Registry Viewer
Raw Disk Viewer
Email Viewer
Indexing
Indexing
Help
Create Index
Search Index
Step 3 of 5
Memory optimization / Indexing limits
Estimate the number of files (and size) being indexed. This will help optimize memory usage and index more efficiently.
Small
Medium
Large
Extreme
Don't know (Pre-scan required)
Custom
Edit
Max number of files = 500,000
Max file size* = 47 MB
Estimated RAM required: 4,600 MB (4.6 GB)
Available RAM: 7,941 MB (7.9 GB)
*Max file size does not apply to some file formats
Select number of threads: 4
Use RAM drive for temporary files to speed up indexing
Back
Next
9:12 PM
9/13/2024

Here I waited a bit, as it was loading…

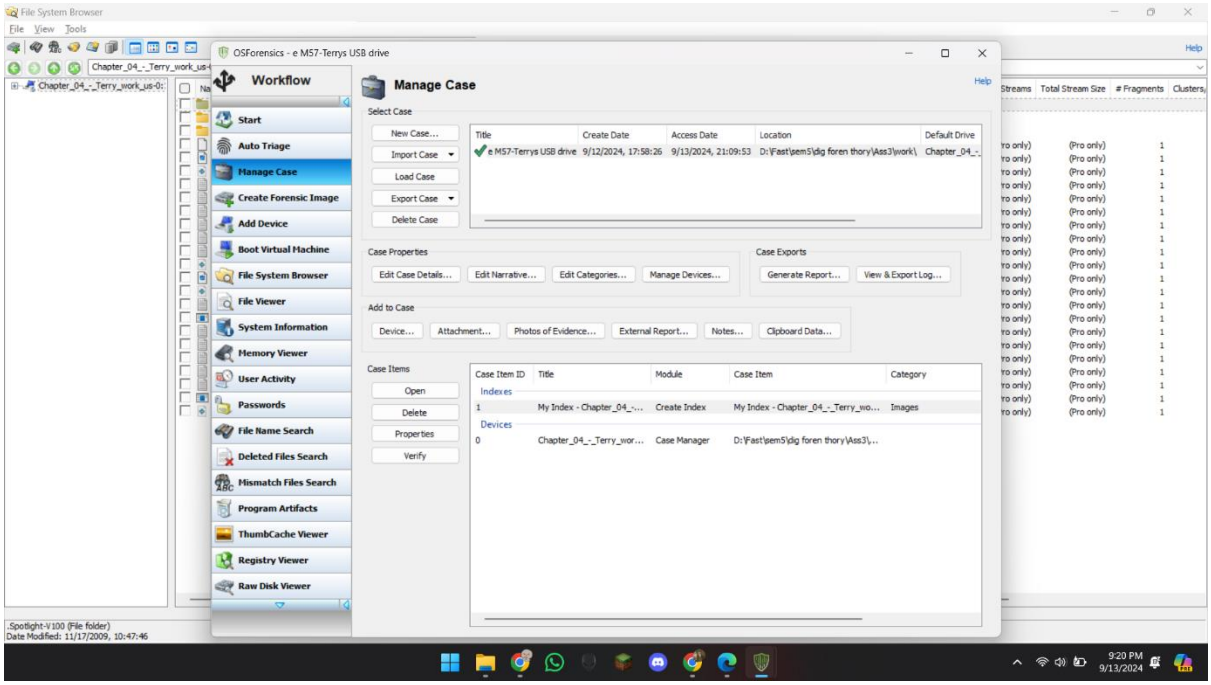


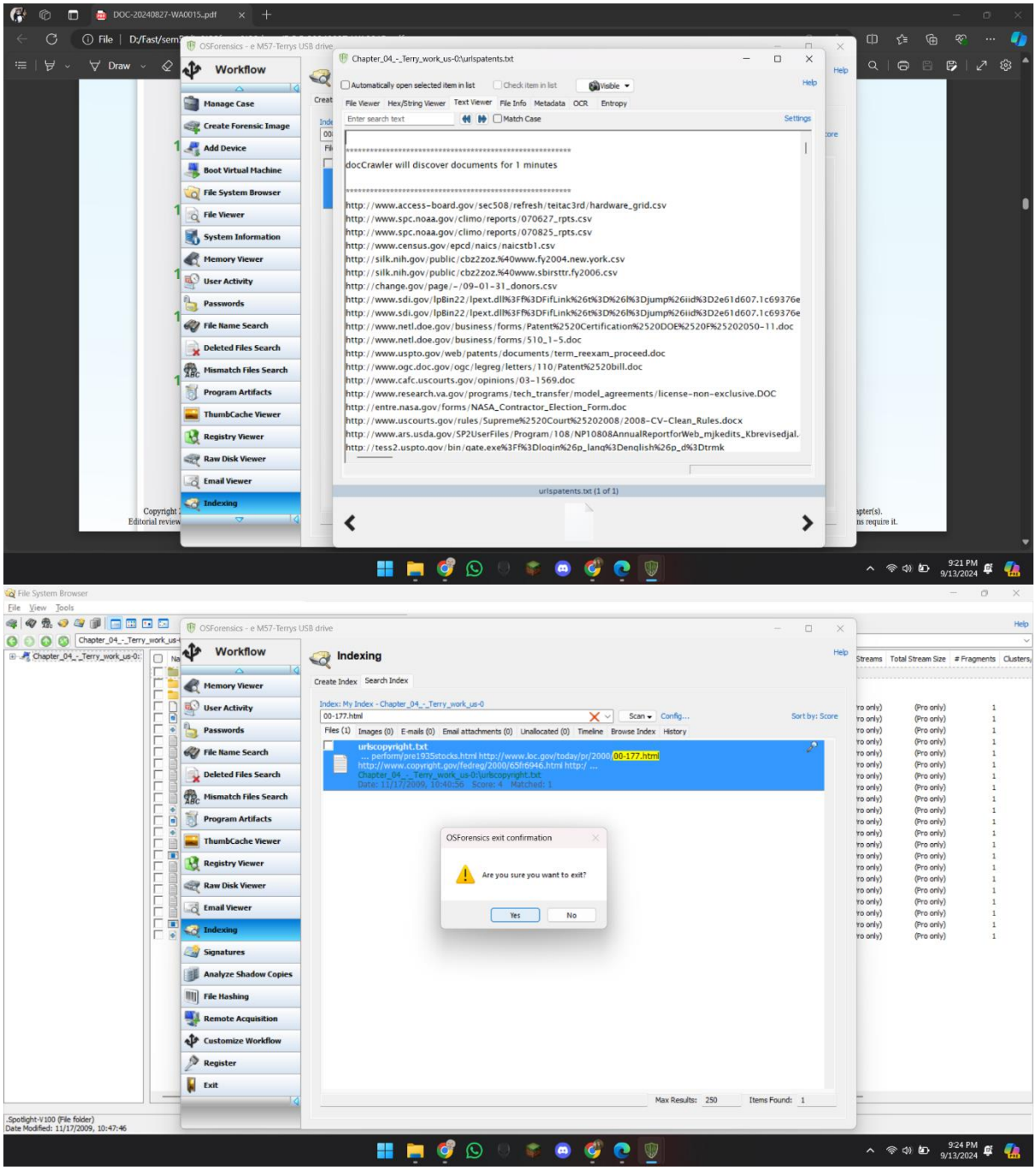


It completed and I saw the logs, and nothing went wrong.



I saw a file That contained some links, that looked somewhat illicit, so Here is the Screenshot of that.



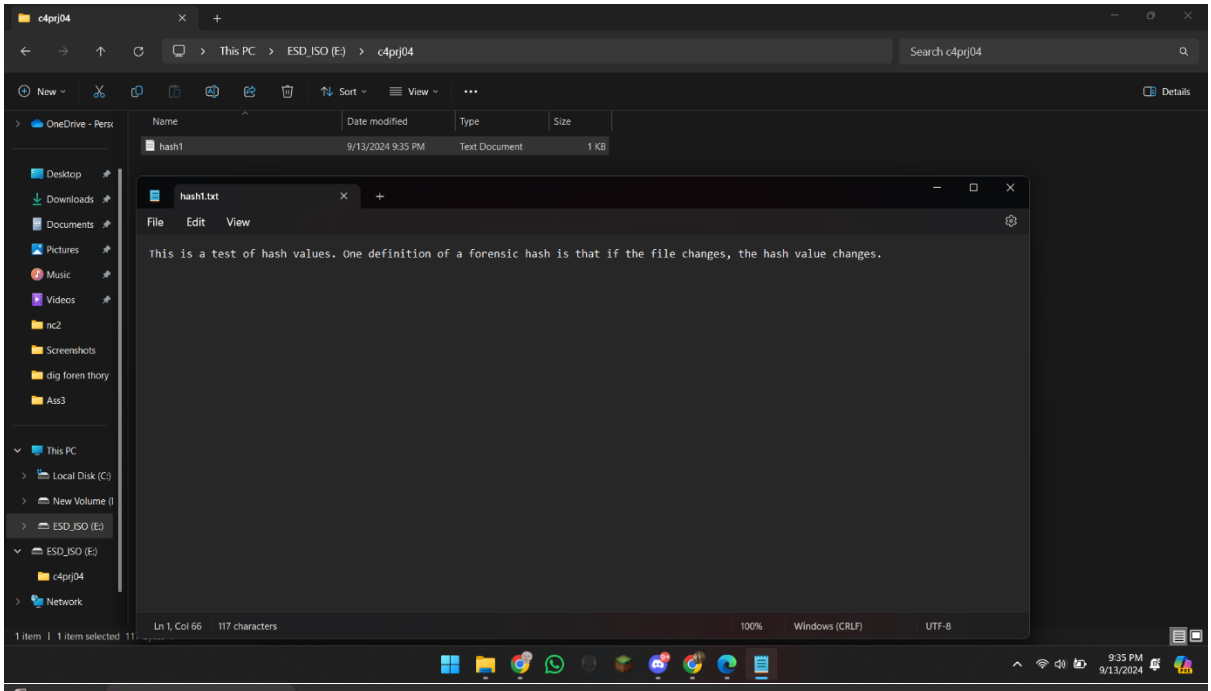


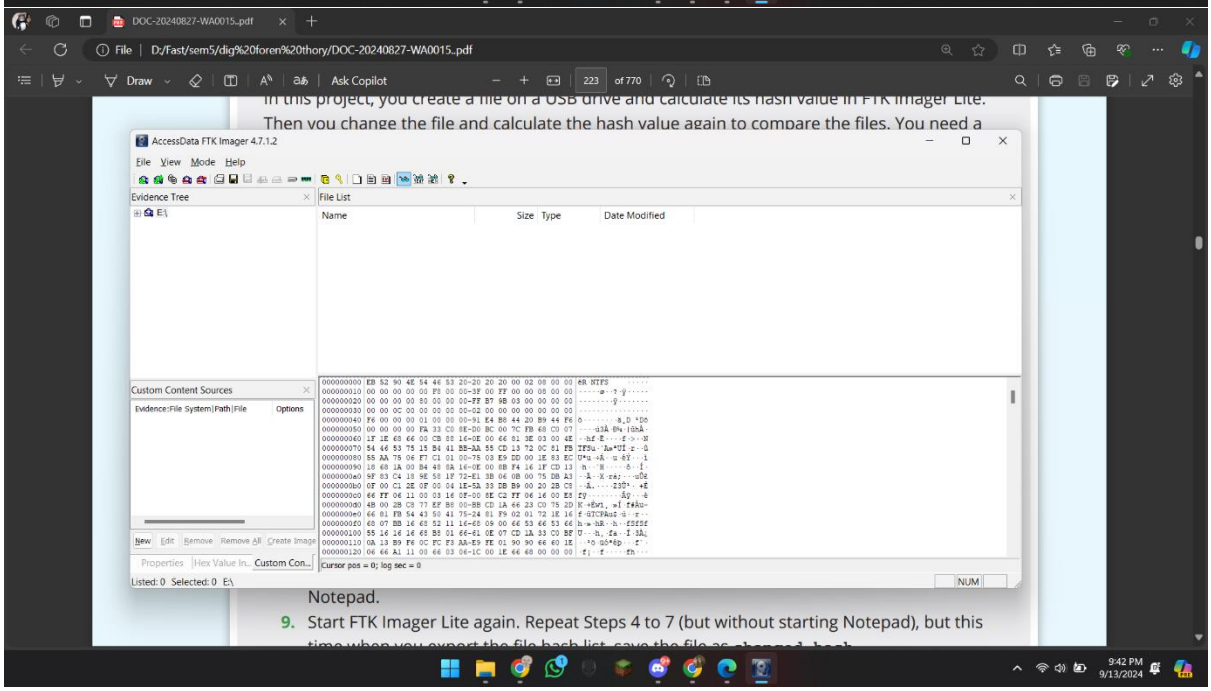
So the case was done.

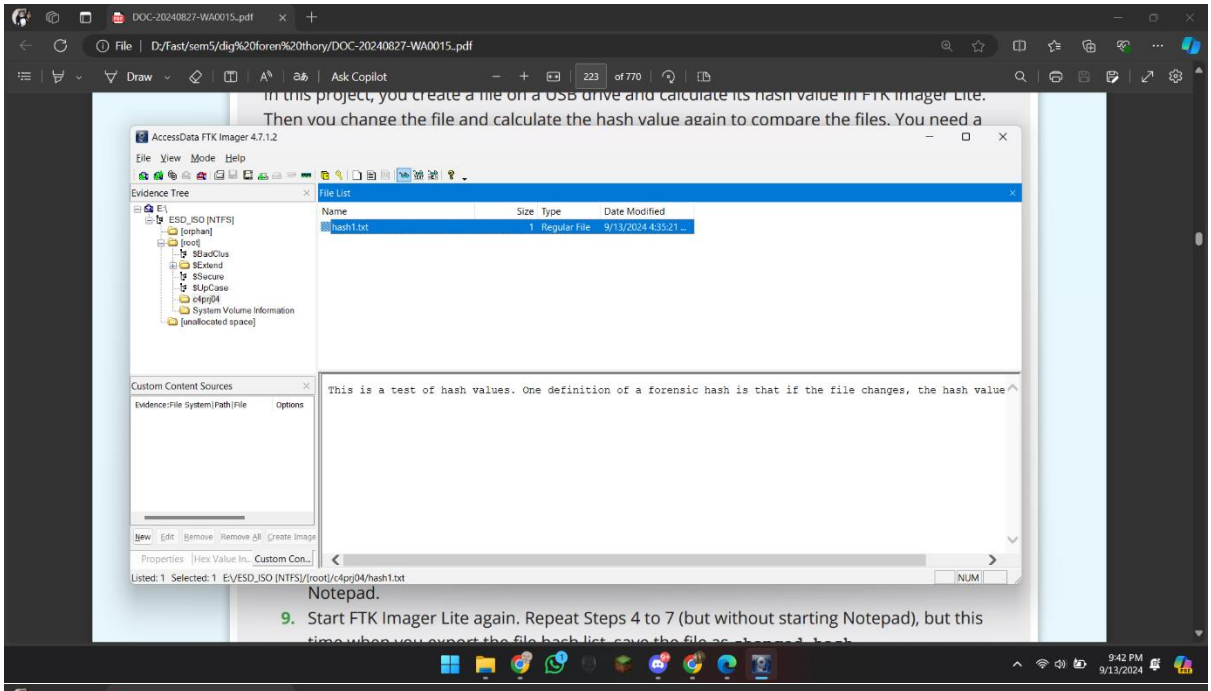
- Hands-On Project 4-4

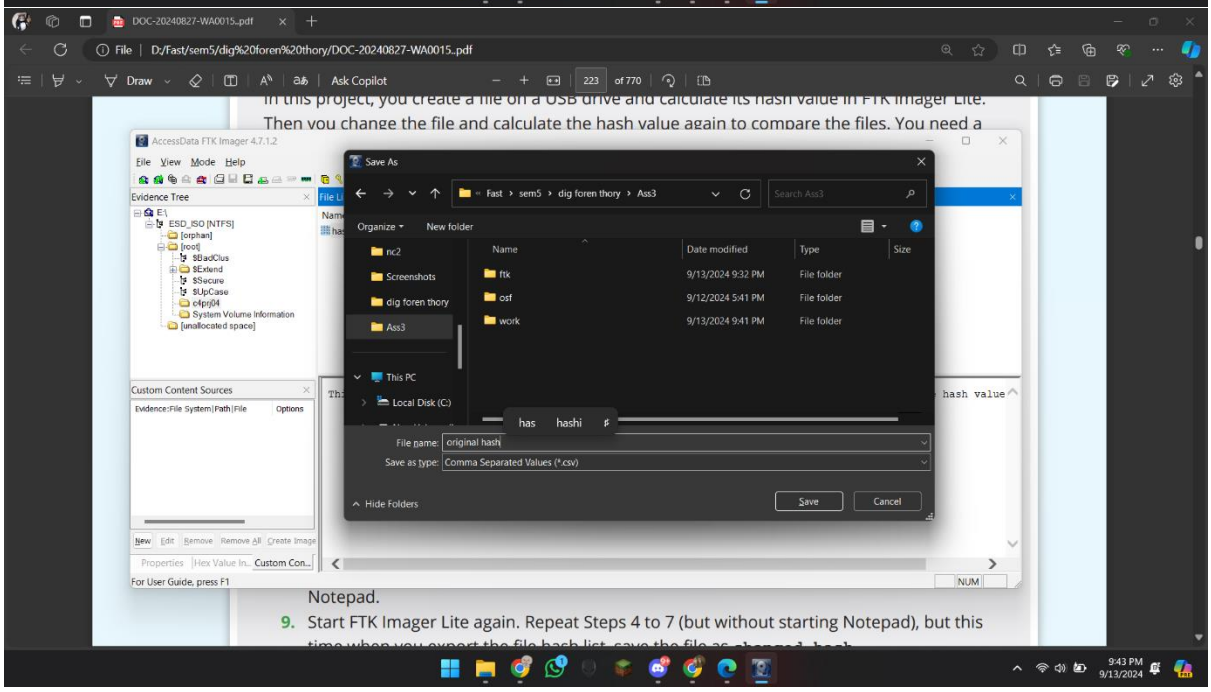
So this case was about We checked if we change something in the file , would the hash changes or not by using FTK imager.

So first I made a file name hash1.txt, and wrote smth in it, and opened the file in FTK imager, and exported the hashes of it.

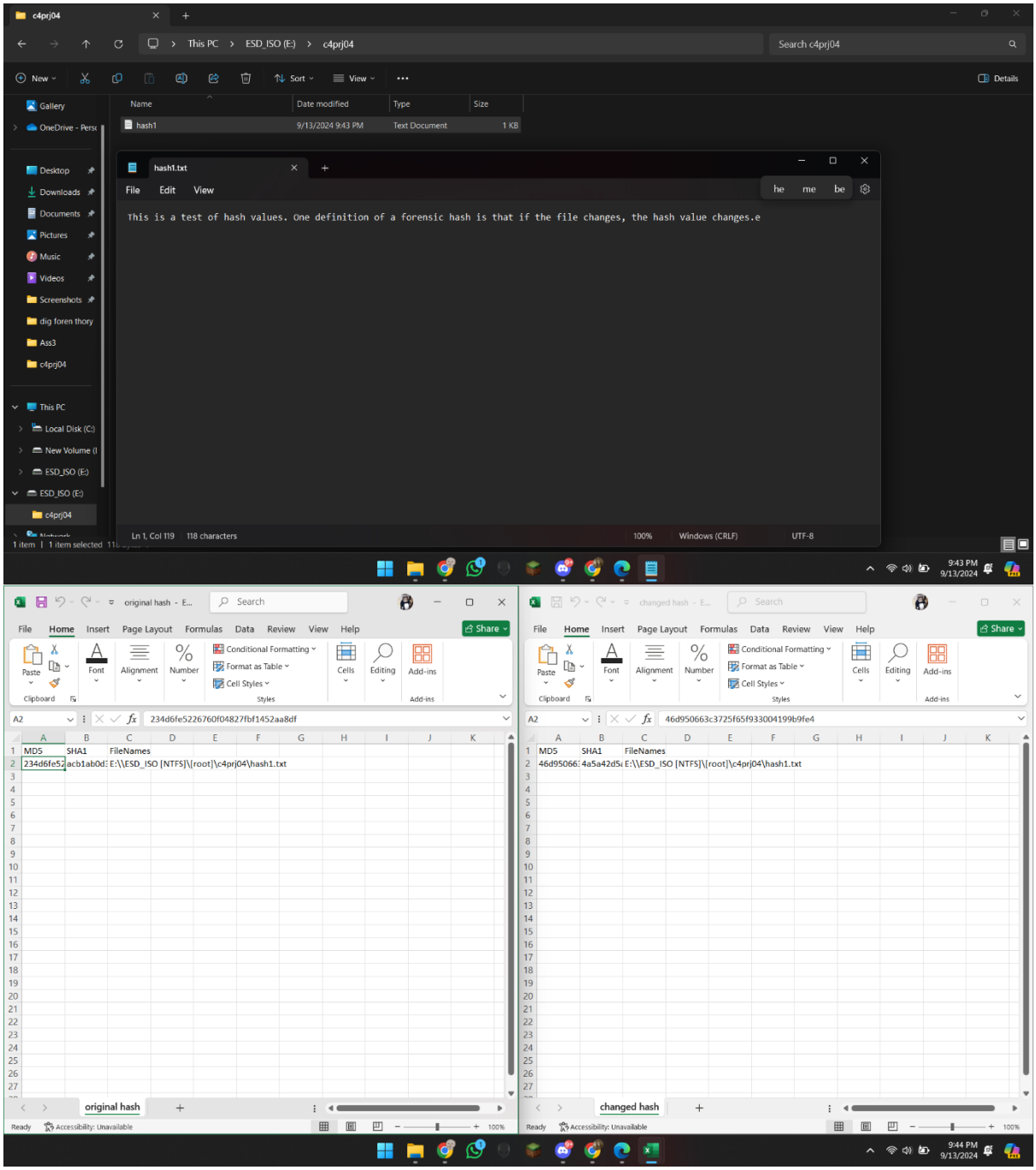

c4prj04
This PC › ESD_ISO (E:) › c4prj04
Search c4prj04
New
Sort
View
Details
Name
Date modified
Type
Size
hash1
9/13/2024 9:35 PM
Text Document
1 KB
hash1.txt
File Edit View
This is a test of hash values. One definition of a forensic hash is that if the file changes, the hash value changes.
Ln 1, Col 66
117 characters
100%
Windows (CRLF)
UTF-8
9:35 PM
9/13/2024

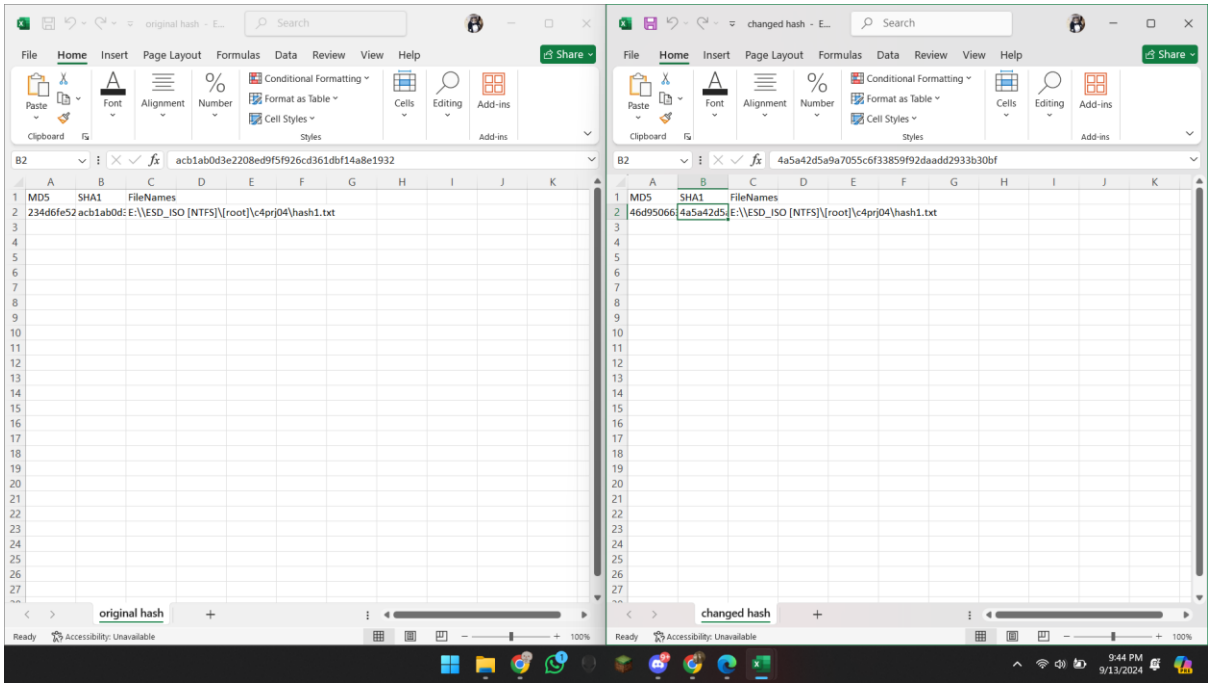

DOC-20240827-WA0015..pdf
File | D:/Fast/sem5/dig%20foren%20thory/DOC-20240827-WA0015..pdf
Draw
Ask Copilot
223
of 770
AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value In...
Custom Con...
Listed: 0 Selected: 0
Cursor pos = 0; log sec = 0
NUM
Notepad.
9. Start FTK Imager Lite again. Repeat Steps 4 to 7 (but without starting Notepad), but this
9:42 PM
9/13/2024





After exportig the csv, I added a letter in the file, and then did all the same work as above, and exported a csv file


c4prj04
This PC
ESD_ISO (E:)
c4prj04
Search c4prj04
New
Sort
View
Details
Gallery
OneDrive - Perso
Desktop
Downloads
Documents
Pictures
Music
Videos
Screenshots
dig foren thory
Ass3
c4prj04
This PC
Local Disk (C:)
New Volume (I
ESD_ISO (E:)
ESD_ISO (E:)
c4prj04
Name
Date modified
Type
Size
hash1
9/13/2024 9:43 PM
Text Document
1 KB
hash1.txt
File
Edit
View
This is a test of hash values. One definition of a forensic hash is that if the file changes, the hash value changes.e
Ln 1, Col 119
118 characters
100%
Windows (CRLF)
UTF-8
1 item | 1 item selected
9:43 PM
9/13/2024
original hash - E...
Search
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Help
Share
Paste
Font
Alignment
Number
Conditional Formatting
Format as Table
Cell Styles
Cells
Editing
Add-ins
Clipboard
Styles
Add-ins
A2
234d6fe5226760f04827fbf1452aa8df
MD5
SHA1
FileNames
234d6fe52
acb1ab0d
E:\\ESD_ISO [NTFS]\[root]\c4prj04\hash1.txt
original hash
Ready
Accessibility: Unavailable
changed hash - E...
Search
A2
46d950663c3725f65f933004199b9fe4
MD5
SHA1
FileNames
46d95066
4a5a42d5
E:\\ESD_ISO [NTFS]\[root]\c4prj04\hash1.txt
changed hash
Ready
Accessibility: Unavailable
9:44 PM
9/13/2024



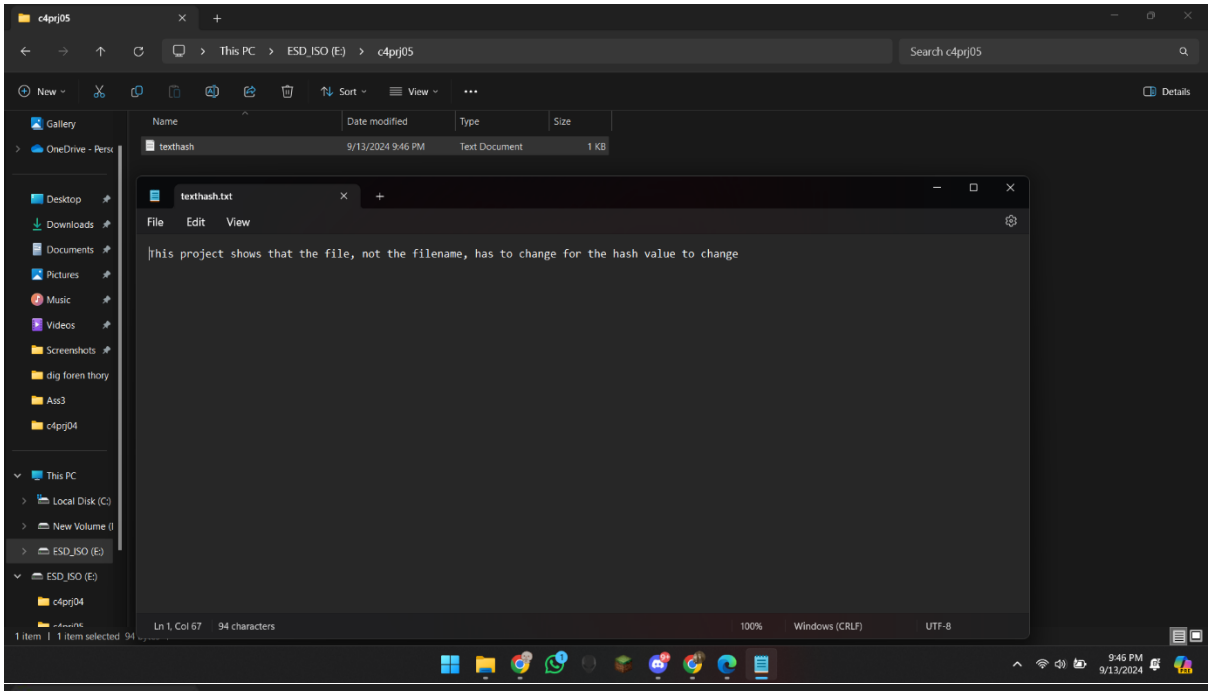
And here it was The results of Excel File showing that both the hashes have changed by adding a letter in the end.

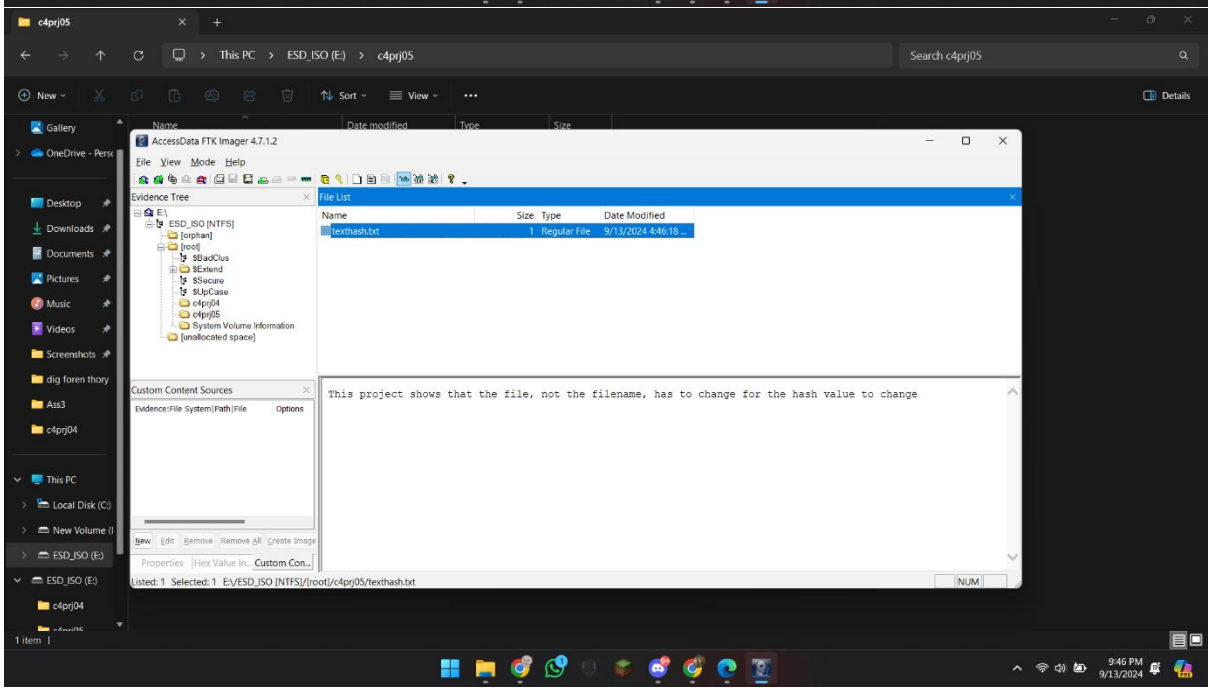
- ## Hands-On Project 4-5

  So this case was about We checked if we change name of the file , would the hash changes or not by using FTK imager.

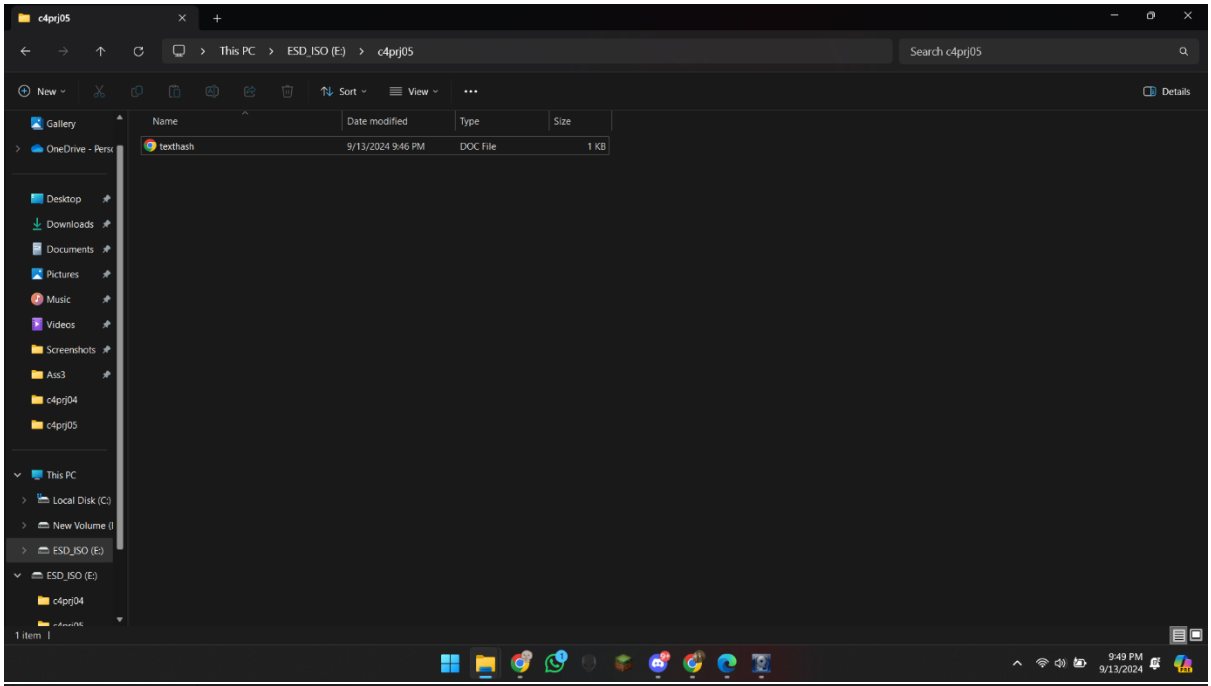
  So I made a new folder in the usb and then made a file with test hash, and then did the same thing as above project.

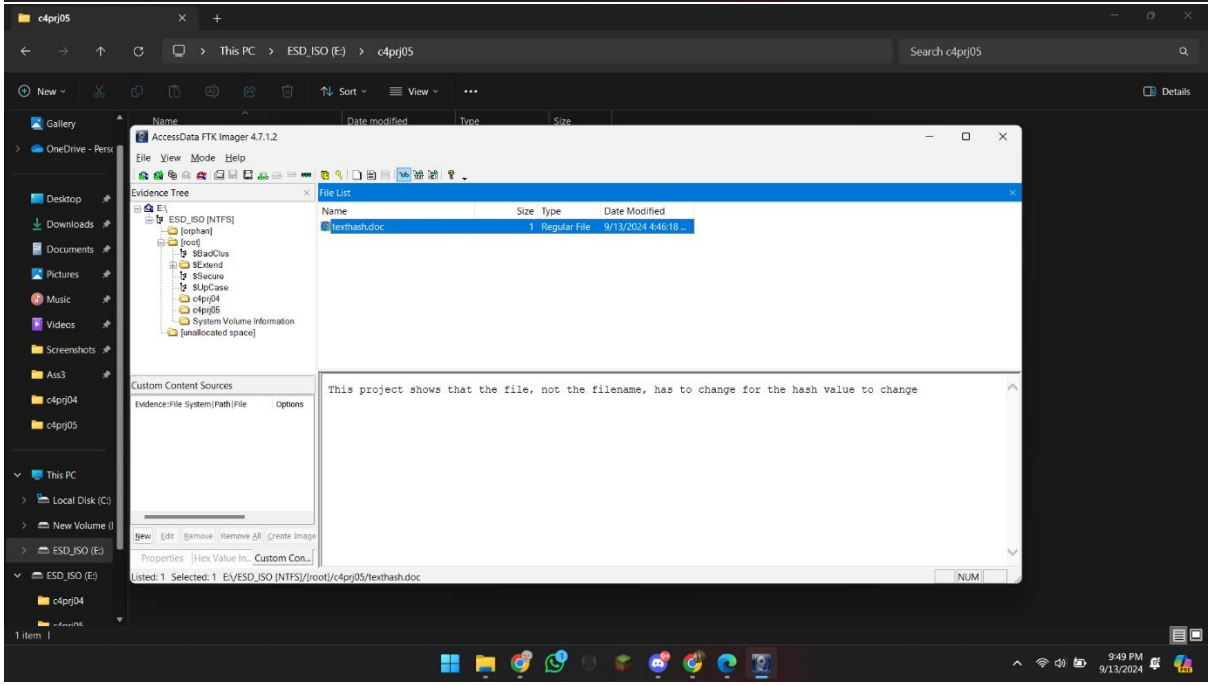
As you can see I made a file, opened the usb in FTK imager, and exported the hash csv.

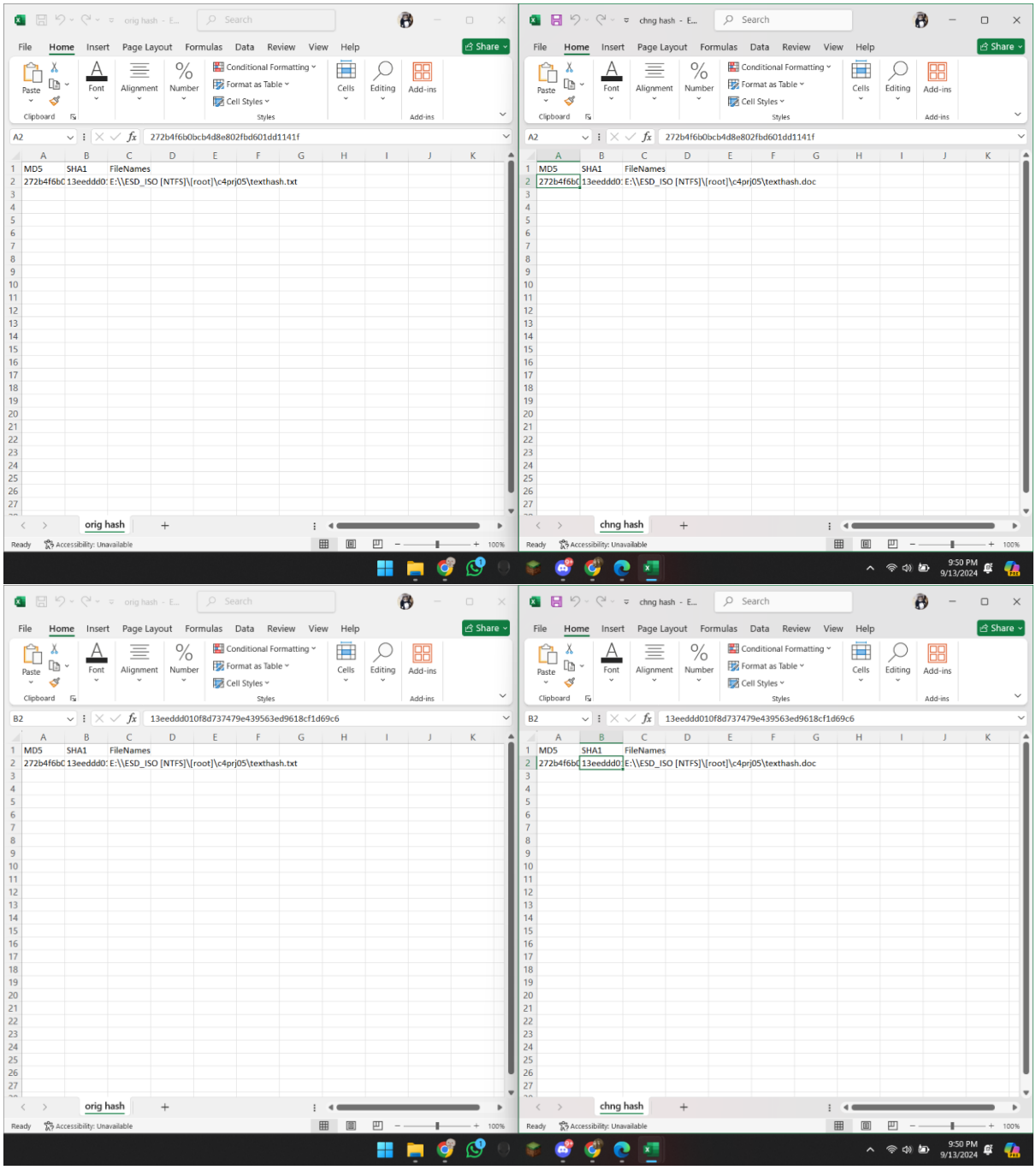

c4prj05
This PC
ESD_ISO (E:)
c4prj05
Search c4prj05
New
Sort
View
Details
Gallery
OneDrive - Perso
Name
Date modified
Type
Size
texthash
9/13/2024 9:46 PM
Text Document
1 KB
Desktop
Downloads
Documents
Pictures
Music
Videos
Screenshots
dig foren thory
Ass3
c4prj04
This PC
Local Disk (C:)
New Volume (I
ESD_ISO (E:)
ESD_ISO (E:)
c4prj04
texthash.txt
File
Edit
View
This project shows that the file, not the filename, has to change for the hash value to change
Ln 1, Col 67
94 characters
100%
Windows (CRLF)
UTF-8
1 item | 1 item selected
9:46 PM
9/13/2024


c4prj05
This PC
ESD_ISO (E:)
c4prj05
Search c4prj05
New
Sort
View
Details
AccessData FTK Imager 4.7.1.2
File
View
Mode
Help
Evidence Tree
File List
Name
Size
Type
Date Modified
texthash.txt
1
Regular File
9/13/2024 4:46:18 ...
ESD_ISO [NTFS]
[orphan]
[root]
$BadClus
$Extend
$Secure
$UpCase
c4prj04
c4prj05
System Volume Information
[unallocated space]
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value In...
Custom Con...
This project shows that the file, not the filename, has to change for the hash value to change
Listed: 1
Selected: 1
E:\ESD_ISO [NTFS]\[root]\c4prj05\texthash.txt
NUM
1 item
9:46 PM
9/13/2024

Then changed the extension of the file, and then did the same thing as above, and exported the csv.







So per the results of excel files, Both the hashes were equal, so that shows that Hashes doesn't change if we change the name of the file.

• Summary

In summary, We learned how to use OSForensics tool, and FTK imager, and also learnt that if we change something inside a file, the hash would change, but if we change the name of the file, Hashes does not change.

References

- Nelson, B., Phillips, A., & Steuart, C. (2003). *Guide to Computer Forensics and Investigations.*