

Assignment# 3

Digital Forensics



September 17, 2024

Ahmad ABdullah i22-1609

Table of Contents

[Introduction 2](#_Toc177454242)

[Details and Steps 2](#_Toc177454243)

[Task 4-3 2](#_Toc177454244)

[Task# 4-4 7](#_Toc177454245)

[Task 4-5 11](#_Toc177454246)

[Summary 13](#_Toc177454247)

[References 13](#_Toc177454248)

# Introduction

In this assignment, we were tasked to do the hands-on project from the Book

“Guide to Computer Forensics and Investigations: Processing Digital Evidence”,

chapter 4. These tasks were done so that we would gain familiarity with some digital forensic software such as OS-Forensics and FTK Imager. Using resources provided alongside the book we carried out the task as the book guided. Below is the complete report of the tasks I performed.

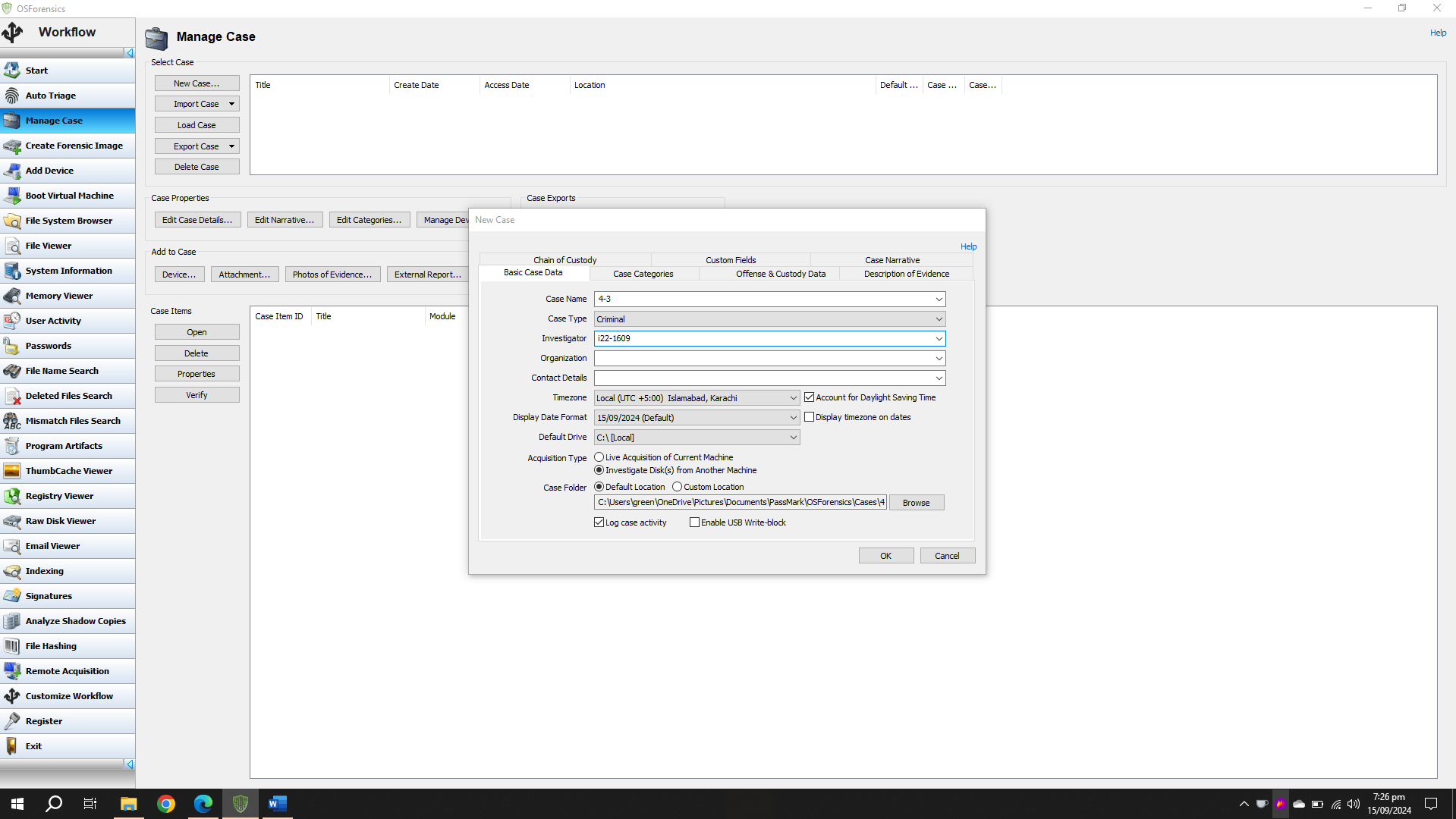
# Details and Steps

## Task 4-3

Initially, this project taught us how to load an image file in OS-Forensics. I loaded an image of a USB “terry-work-usb-2009-12-11.E01” for analysis purposes. After making the case, naming the case and then letting the OS-Forensics analyze the image, I tried to look for evidence that might suggest that a crime had been committed but we could not find any file or image that seemed suspicious in that regard.

A screenshot of a computer

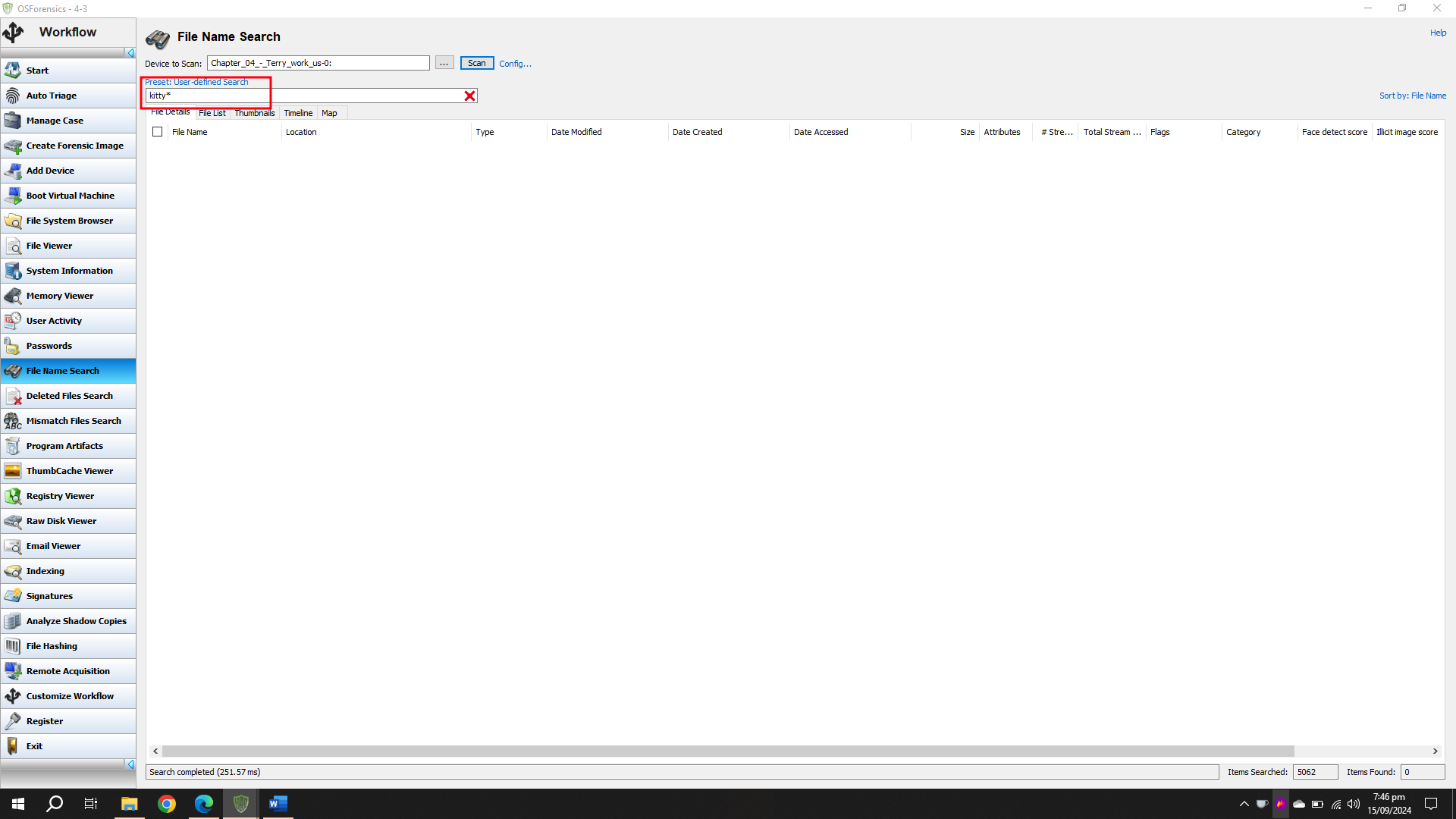
Description automatically generated

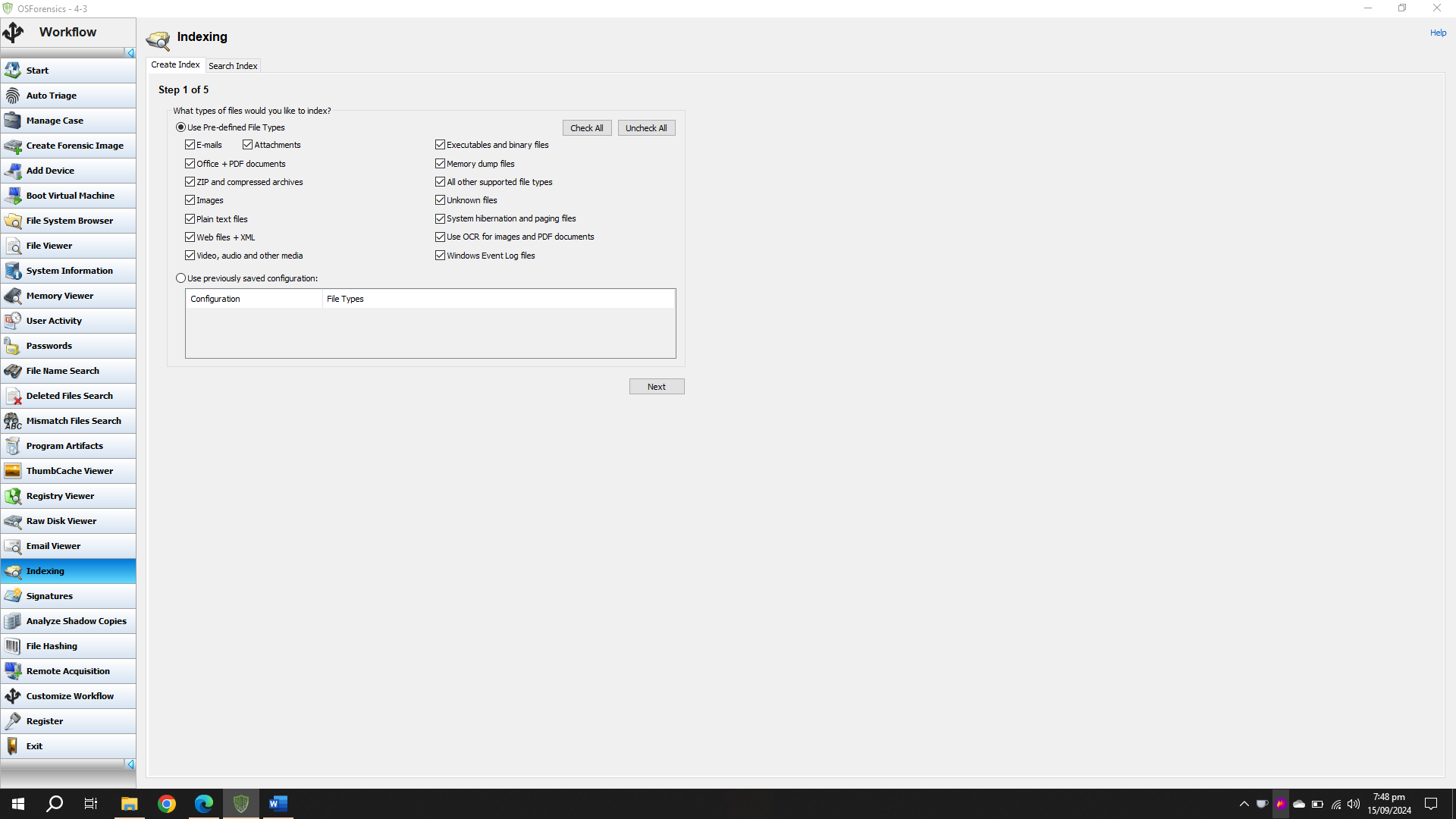


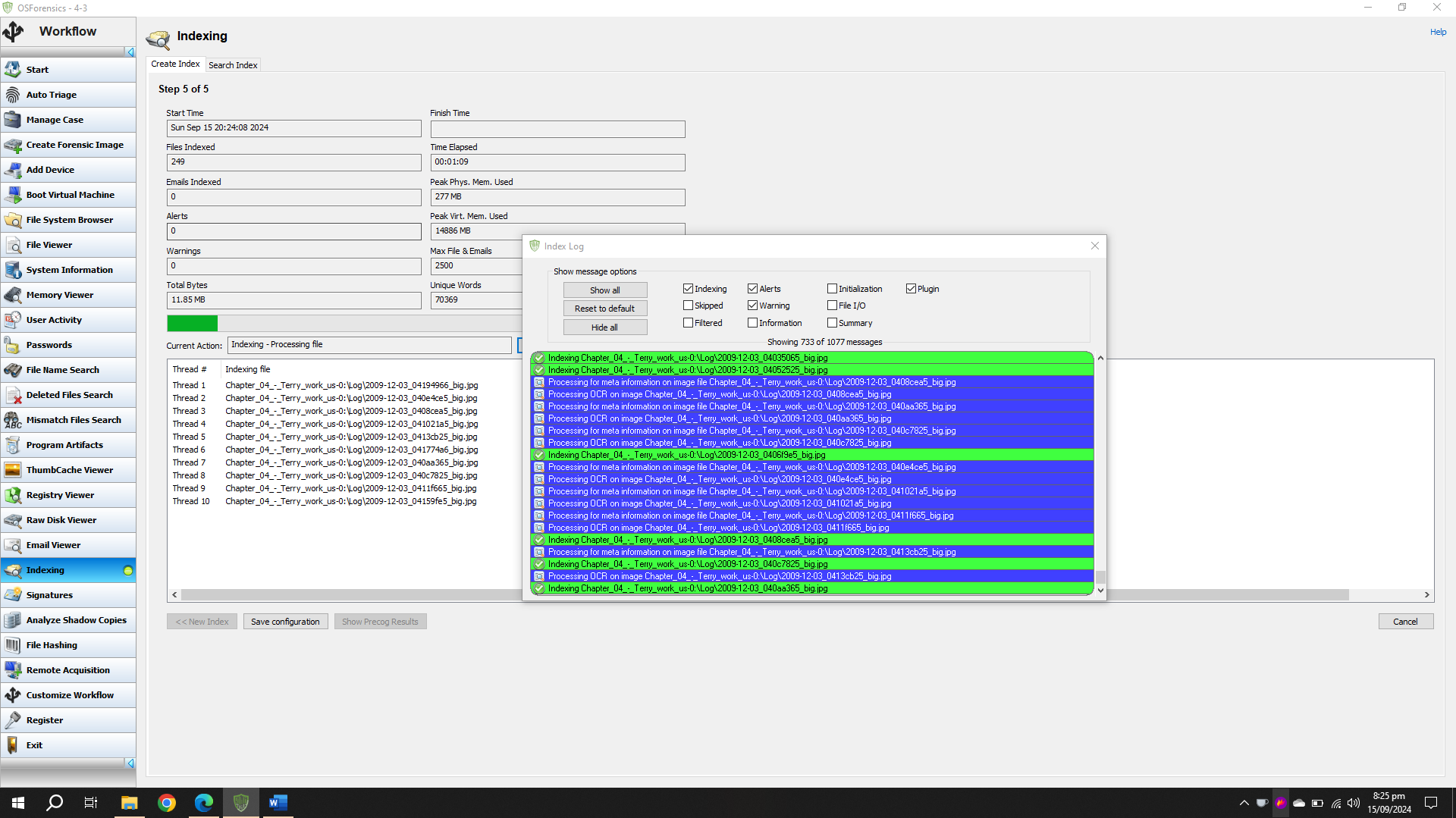
A screenshot of a computer

Description automatically generated

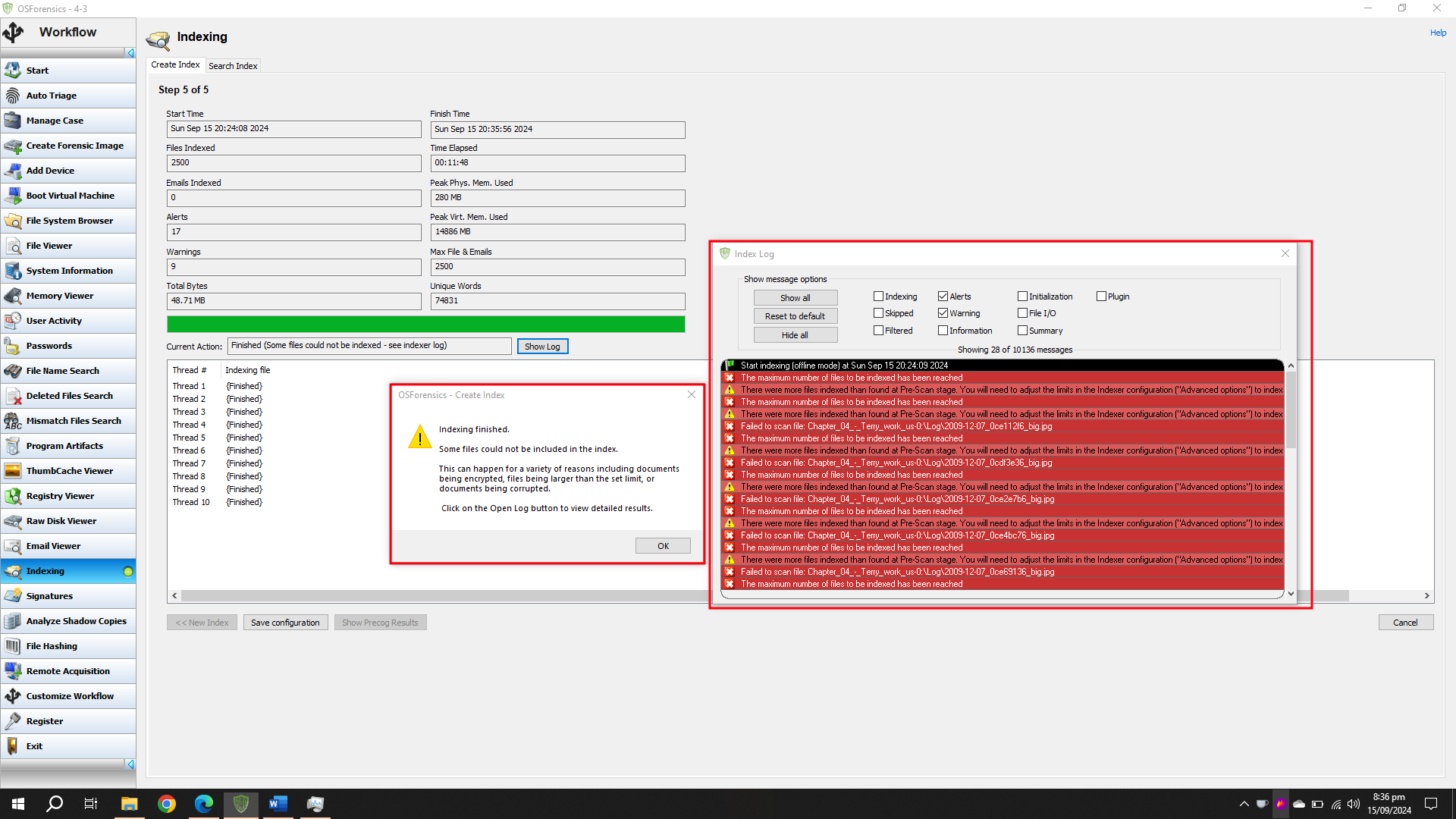
We were searching for a key word ‘Kitty Porn’ which the investigator has suspicion that the suspect had these files on his USB at some point, but we could not find any evidence related to such acquisitions.



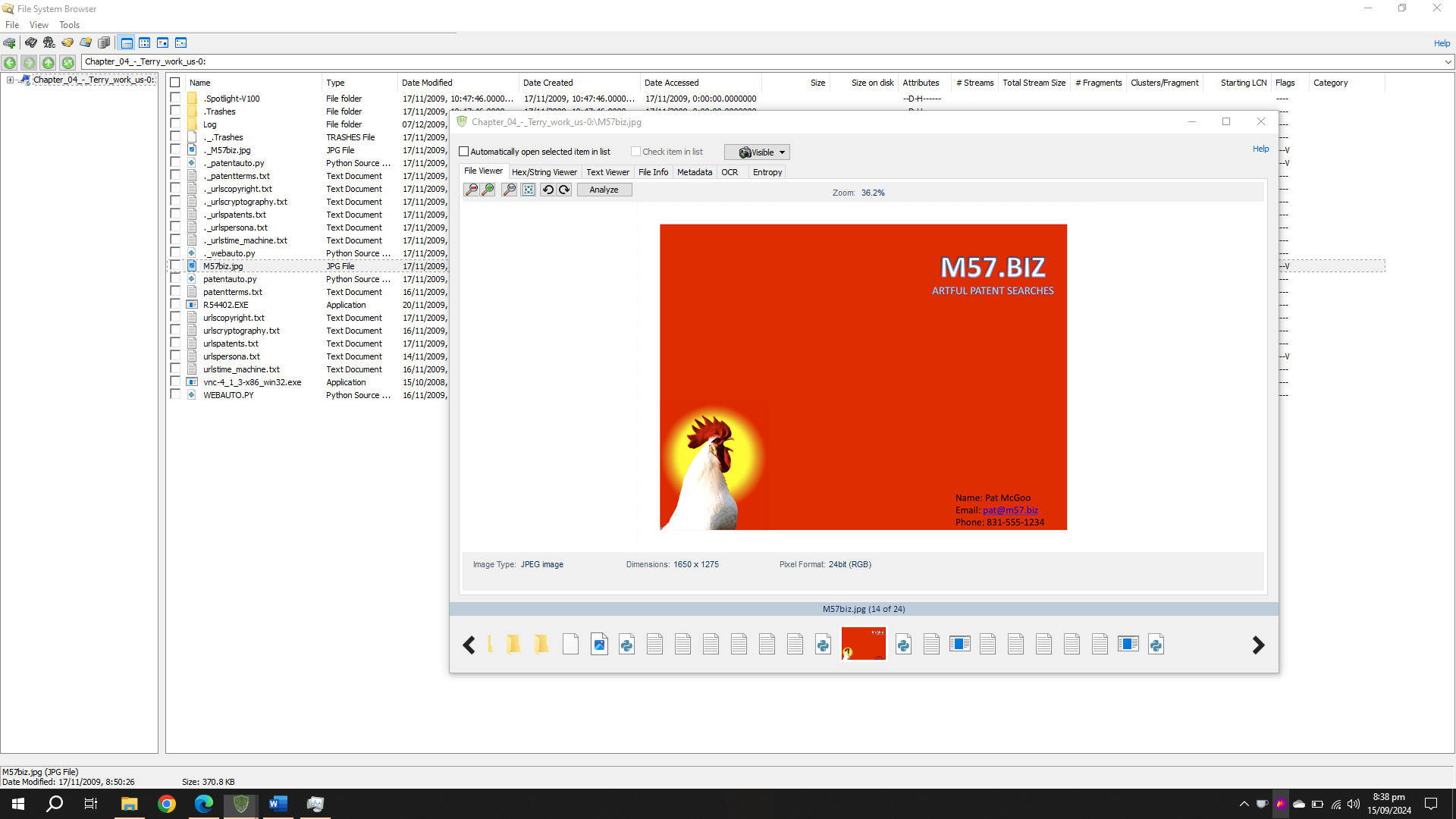


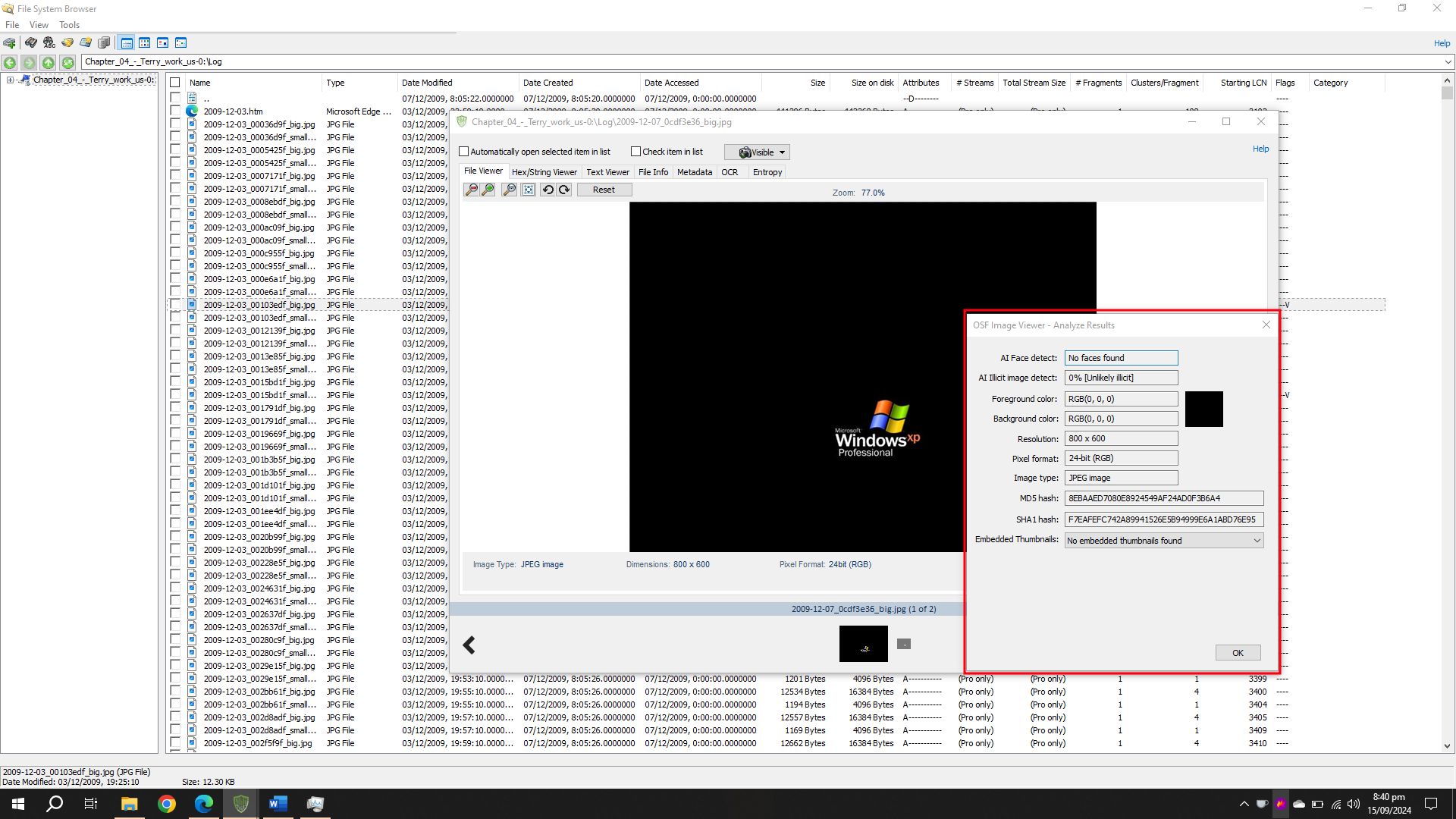


After indexing all the files we were greeted with some technical errors which said that the indexing it did was actually larger than it had assumed.



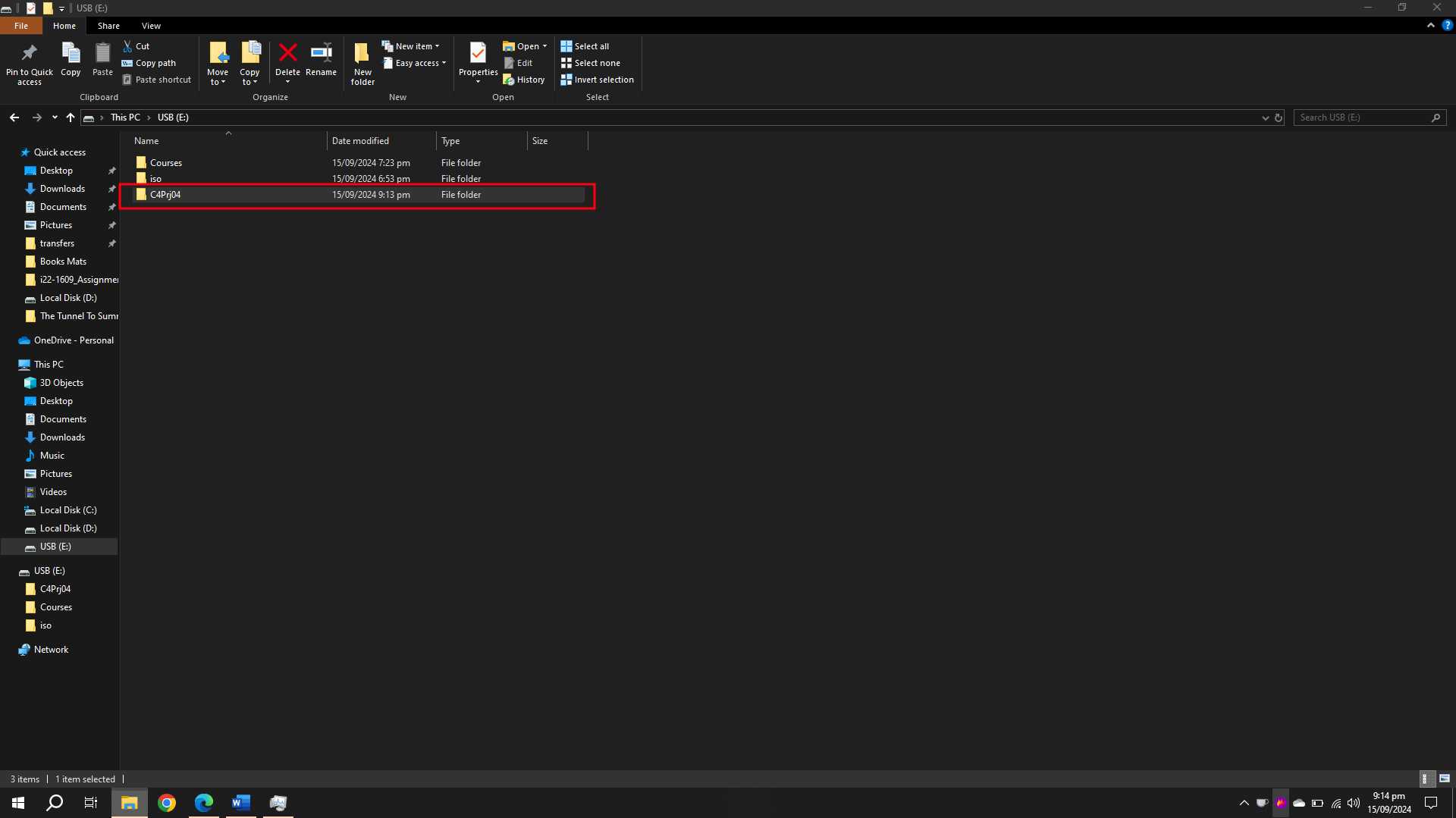
We were then asked to analyze some of the images but all I found was WindowsXP and some cocks.





## Task# 4-4

In this project, we essentially had to check how doing small changes to a file can change its hash quite a bit. Hash is a piece of string that is generated by some formula for any file which is used to check the integrity of a file. If the file has been modified than the next hash will be different than the original one.

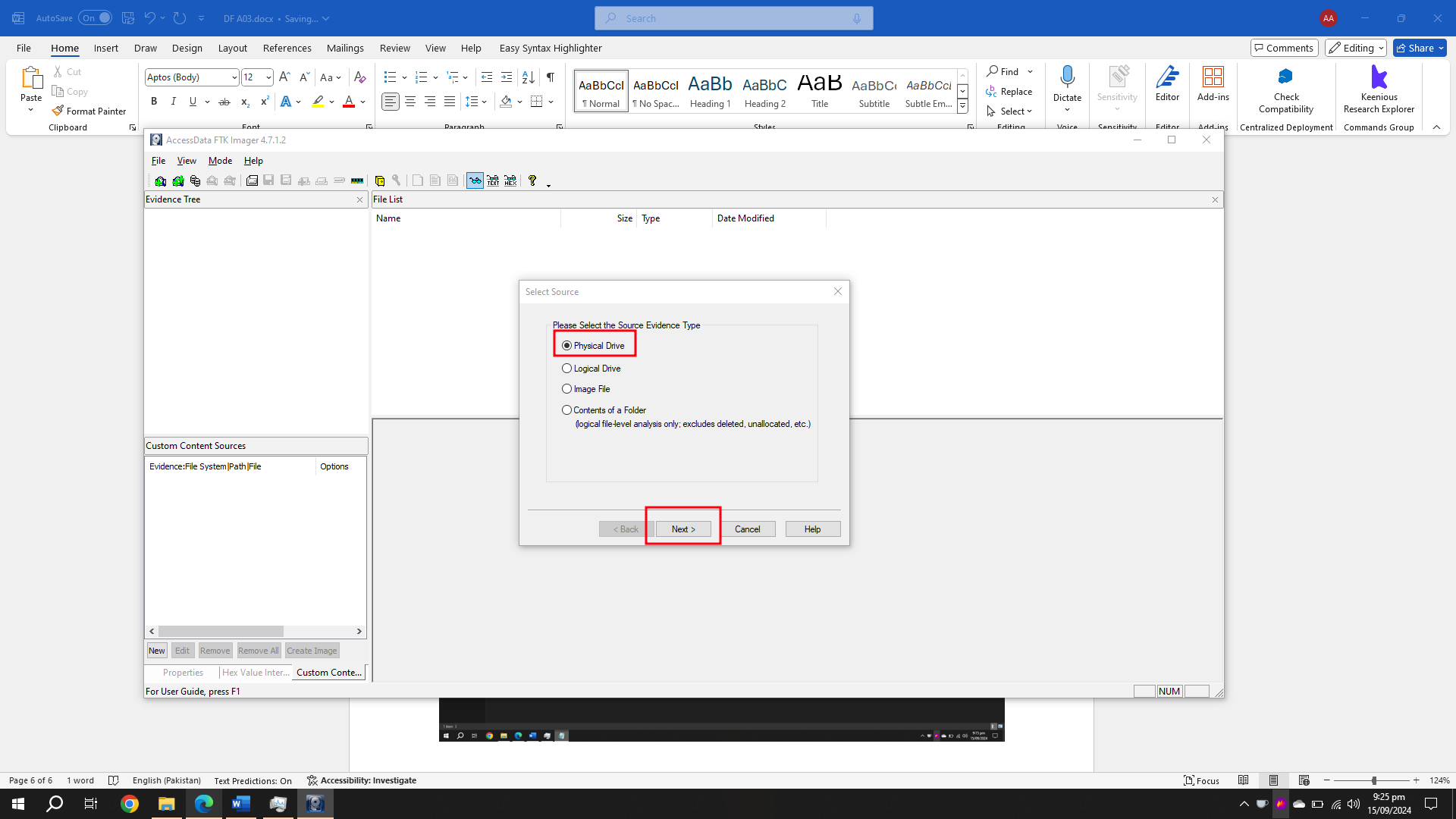


We start by creating a folder ‘C4Prj04’ in a USB drive and then making a txt file and write the string given in the book.

A screenshot of a computer

Description automatically generated

After creating the txt file we then use FTK Imager to load the USB for analysis.



A screenshot of a computer

Description automatically generated

We locate the file in FTK Imager and Export its Hash value in a csv file.

A screenshot of a computer

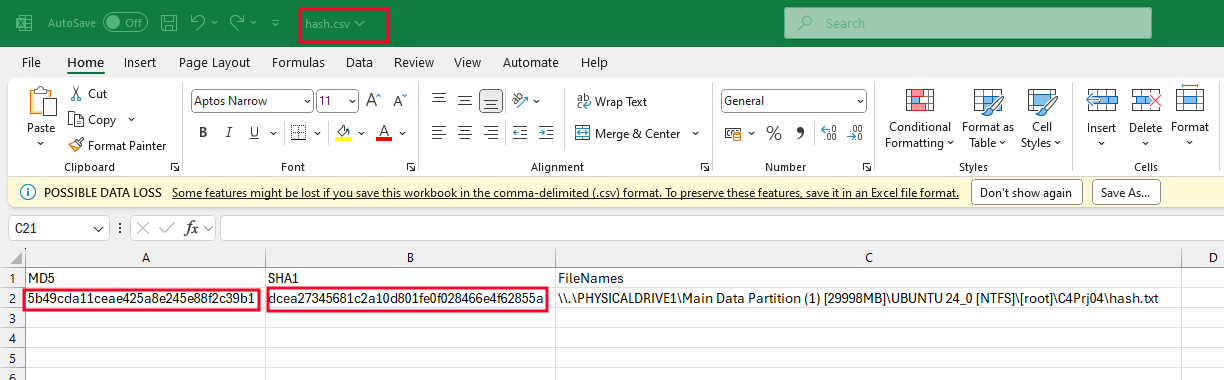
Description automatically generated

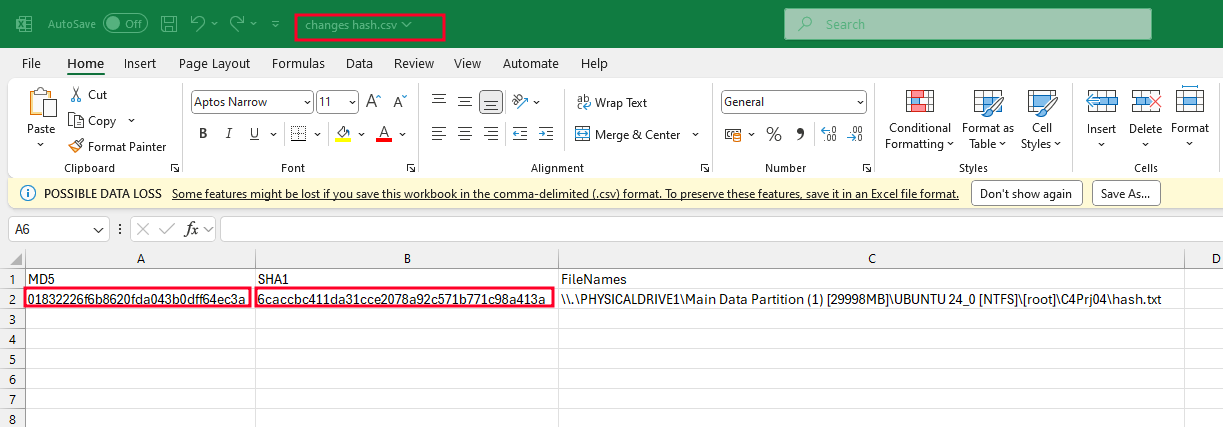
Next, we add some changes in the text file and repeat the process again.

A screenshot of a computer

Description automatically generated

Upon analysing both hash values we quickly see the difference in the hash values before and after doing some changes on the file.





## Task 4-5

In this project, we were tasked with the same type but this time we had to change the extension of the file and see if the hash of the file changes or not.

A screenshot of a computer

Description automatically generated

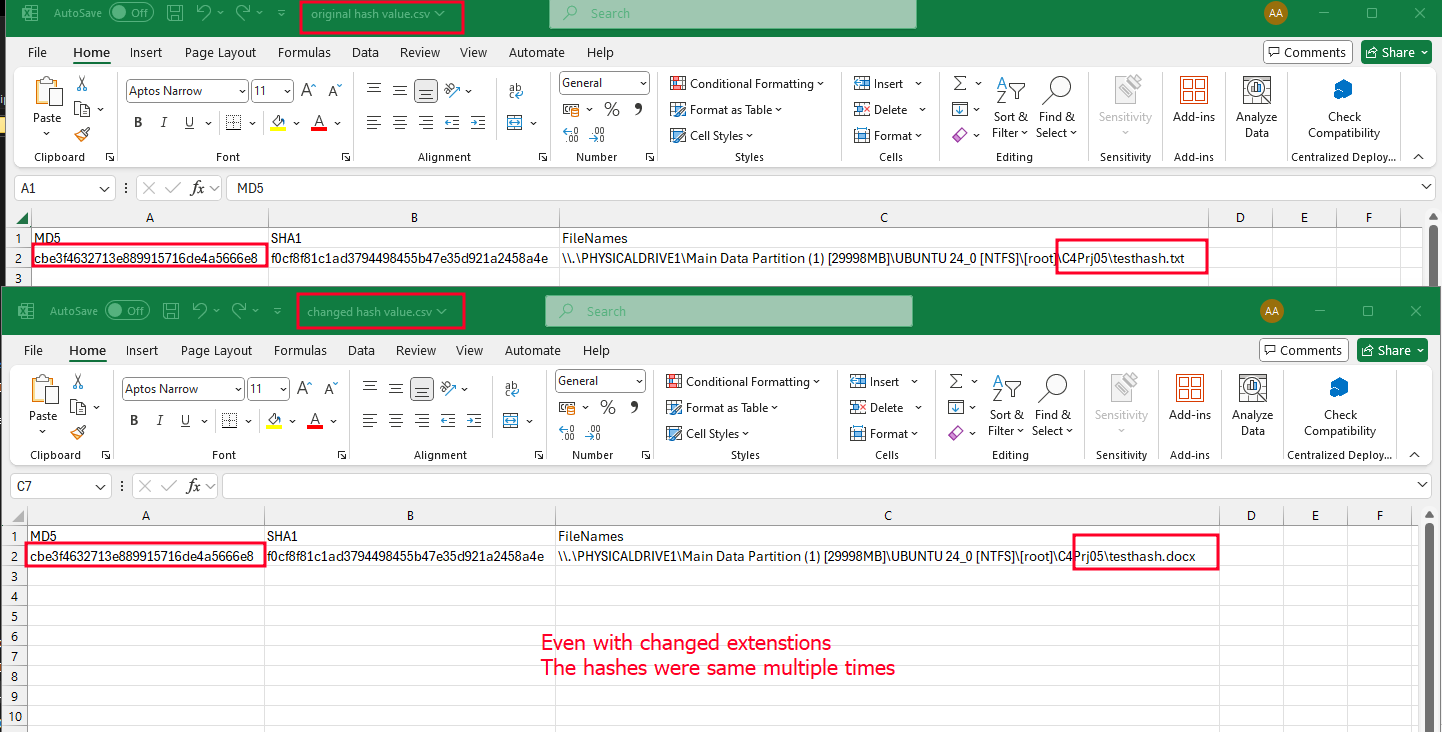
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Carrying out the same process we see that both the hashes are the same even after changing the file extension. This is due to the reason that even if we change the file extension by renaming it, it does not change the hex value of the value of the file which contains information about the real extension of the file.



# Summary

These tasks were given to us to get familiar with how this software works and can a Digital Forensic Investigator can use this software to gather information about a disk image. OS-Forensics provides extensive tools to analyse an image of a file while FTK Imager can be used to make an image as well as analyse it on the spot as well.

# References

Book -“Guide to Computer Forensics and Investigations: Processing Digital Evidence”