National University of Computer and Emerging Sciences
Islamabad Campus

CY2002

Digital Forensics

Assignment 04

ADS & EFS

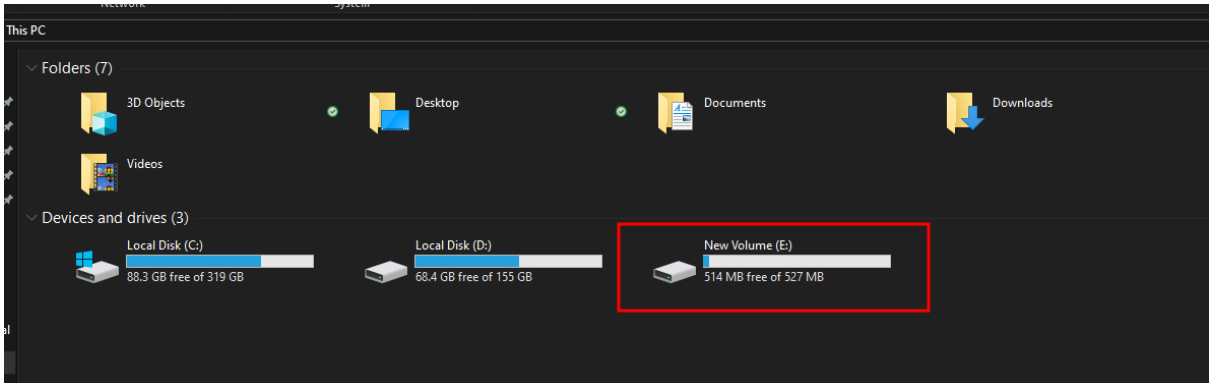
Submitted by: Ahmad Abdullah
Roll number: i22-1609
Date:

Table of Contents

Introduction

In this assignment, we analysed the $MFT file for certain scenarios. A file having two attached files, one which has resident data and another which has non-resident data. Another task was to analyse the EFS encrypted file.

For this assignment, I created another partition to other data does not create hinderance in my analysis.

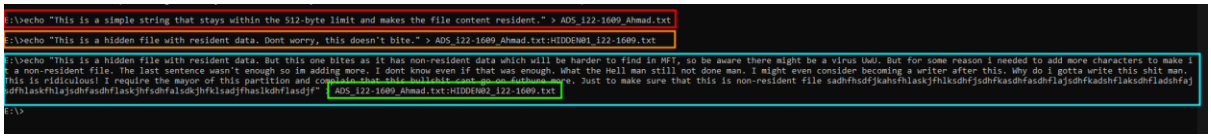


Details and Steps

I will be explaining all the steps for both types of files in different sections.

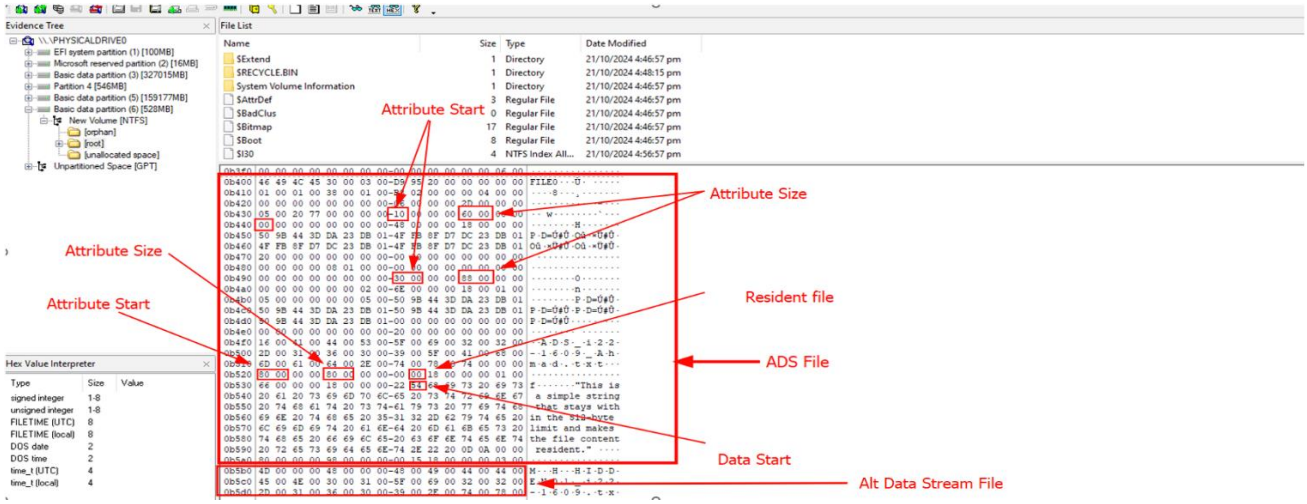
Alternate Data Stream

An Alternate Data Stream(ADS) is a kind of file that has one or more file attached to it which are also hidden. The first thing we needed to do was create such a file with 2 files attached to it.

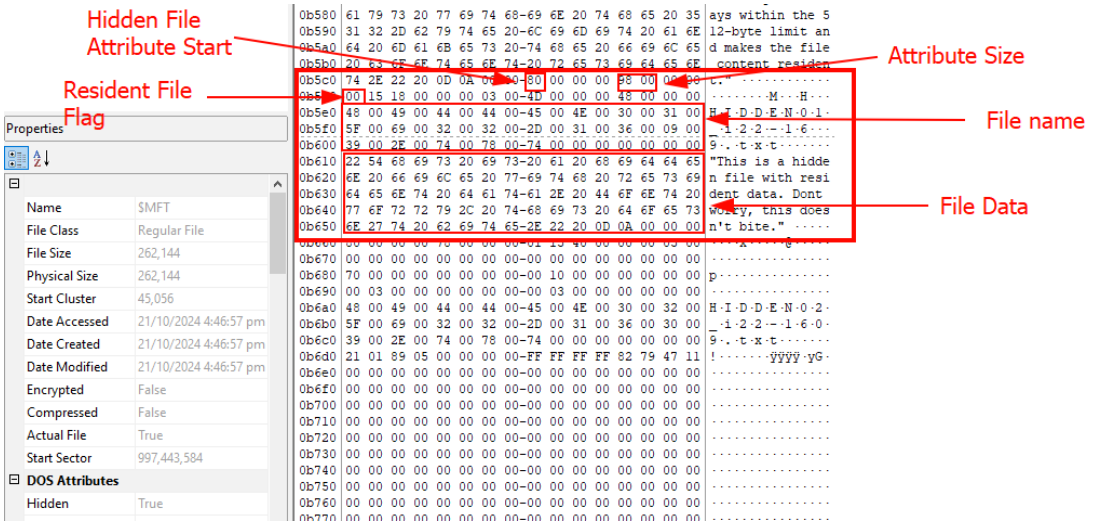


Question 1

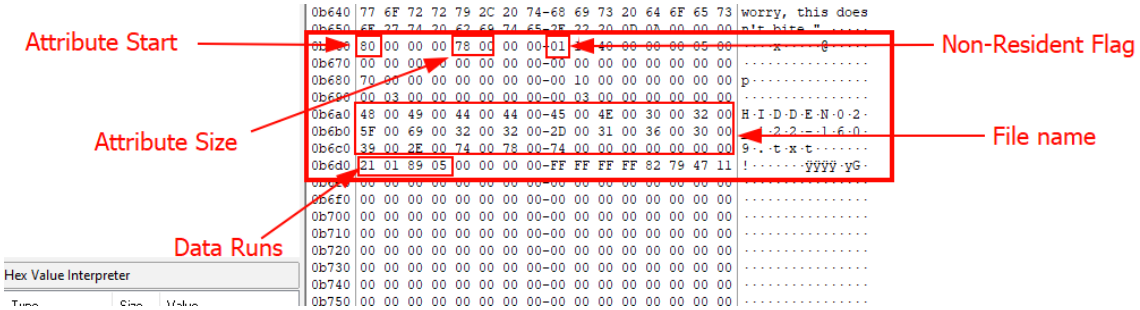
First, we located the file's entry in MFT to start the analysis which was quite easy to do.



1 ADS File



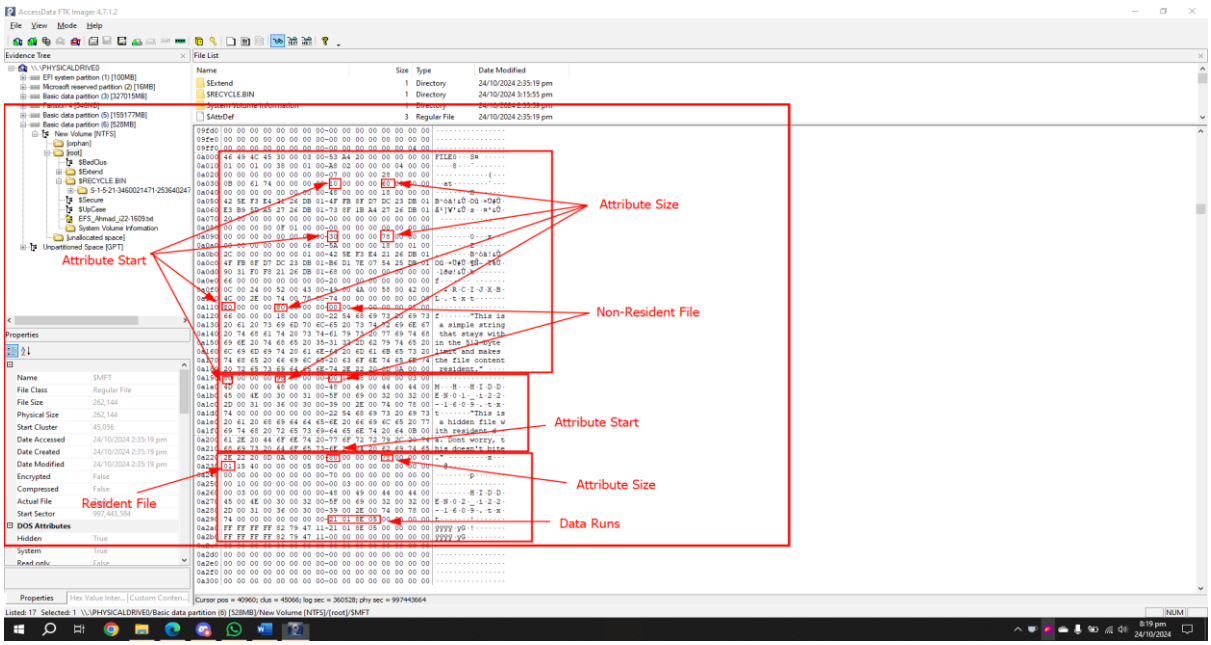
2 HIDDEN 1 FILE



3 HIDDEN 2 FILE

Question 2

In this question, we needed to delete the ADS file, the file which had two other file and then analyse the $MFT file again to see if there were any changes.

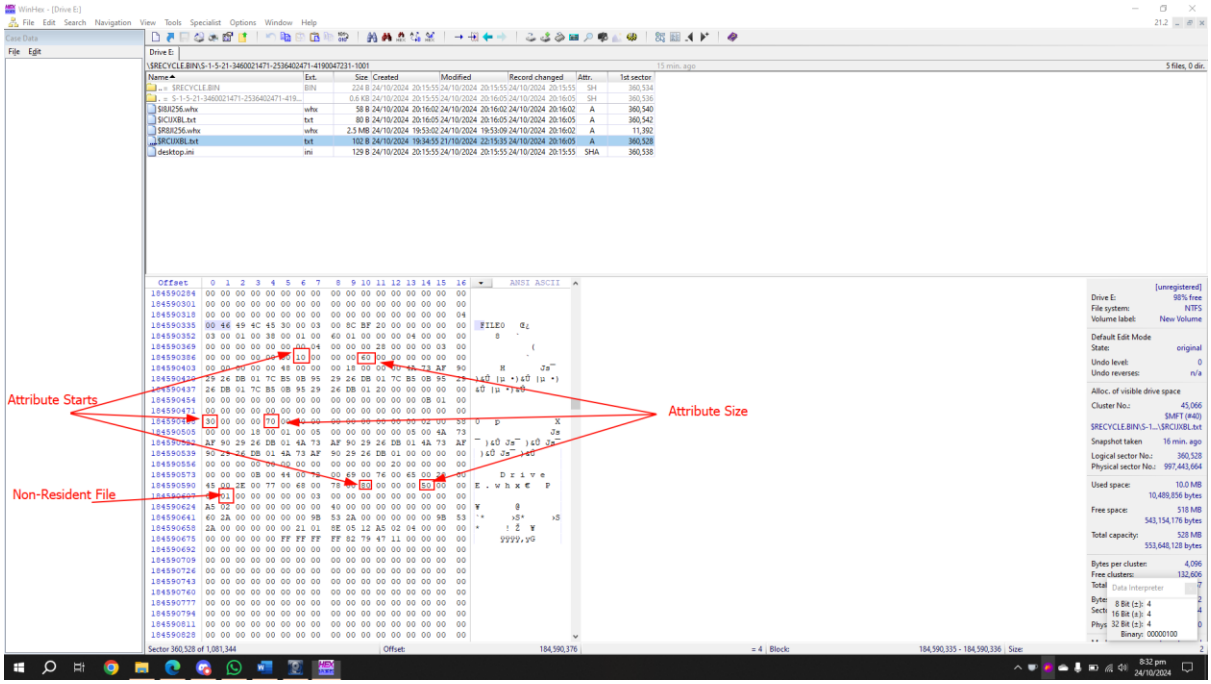


4 MFT Record after Deletion

Changes in MFT of ADS after Deletion

Question 3

In this question, we needed to delete the ADS from the Recycle Bin and then repeat the same procedure.



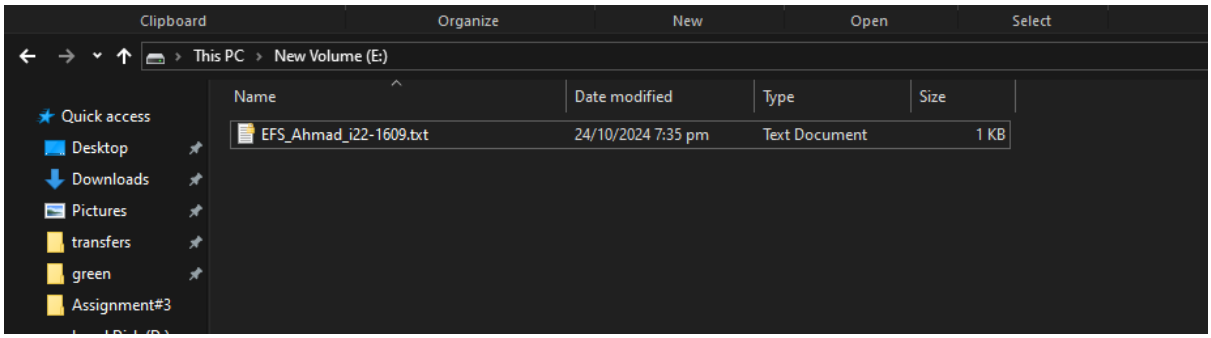
Changes in MFT of ADS after Deletion From Recycle Bin

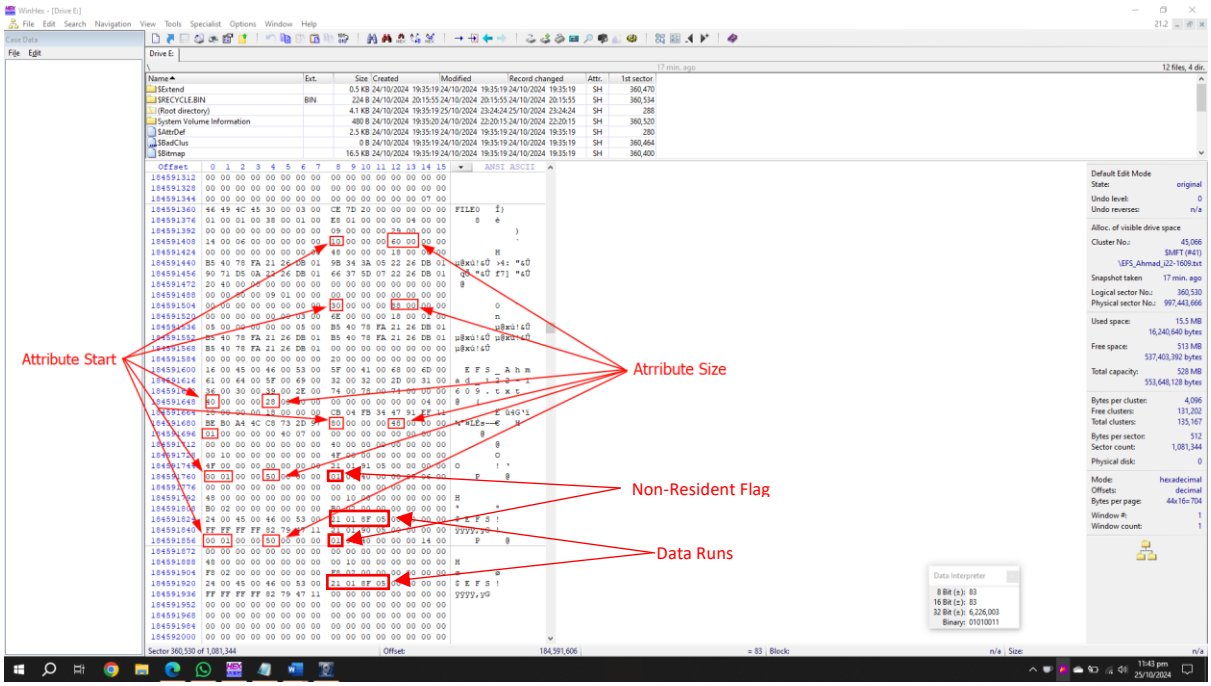
- 0x30 attribute is reduced further as the name of the file is shortened and the MFT modified time record was further changed.
- 0x80 attribute was shortened as well and the data was completely erased from the disk.
- 0x01 flag was added making it a non-resident file.

Encrypted File System

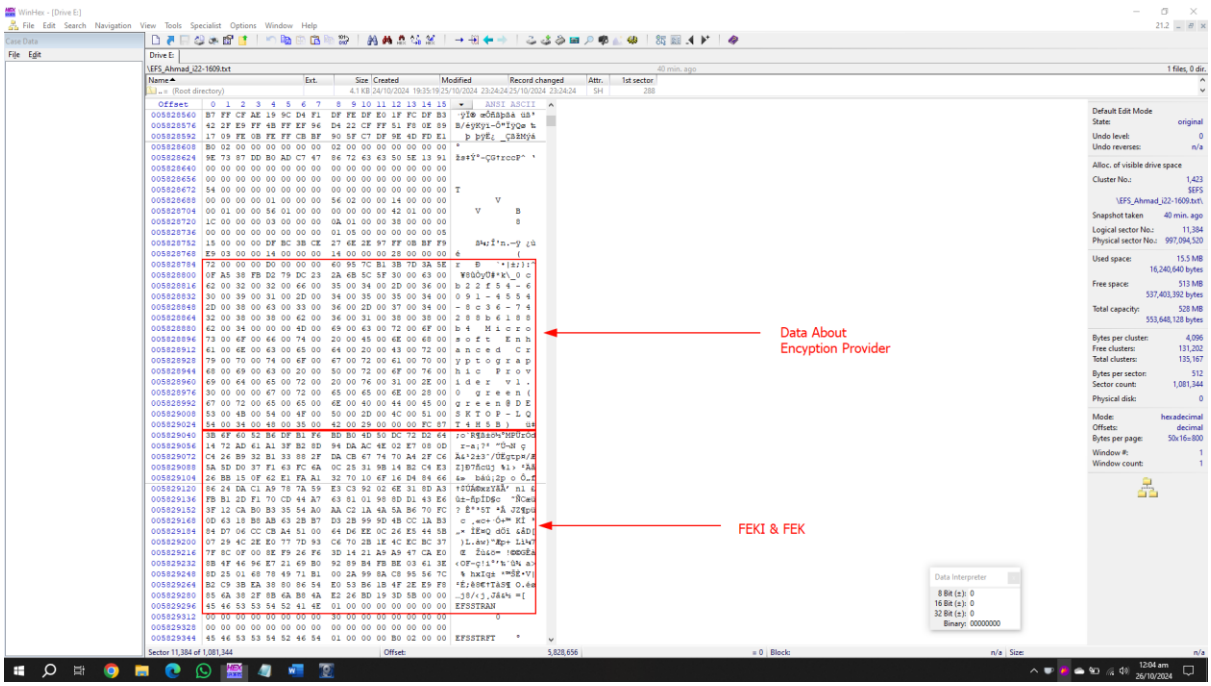
Encrypted File System (EFS) which, unlike BitLocker, allows a user to encrypt a single file rather than a full disk. This feature is only unlocked in the PRO version of Windows.

We created an EFS encrypted file enabled EFS on it and then analyzed it in MFT using WinHex software.

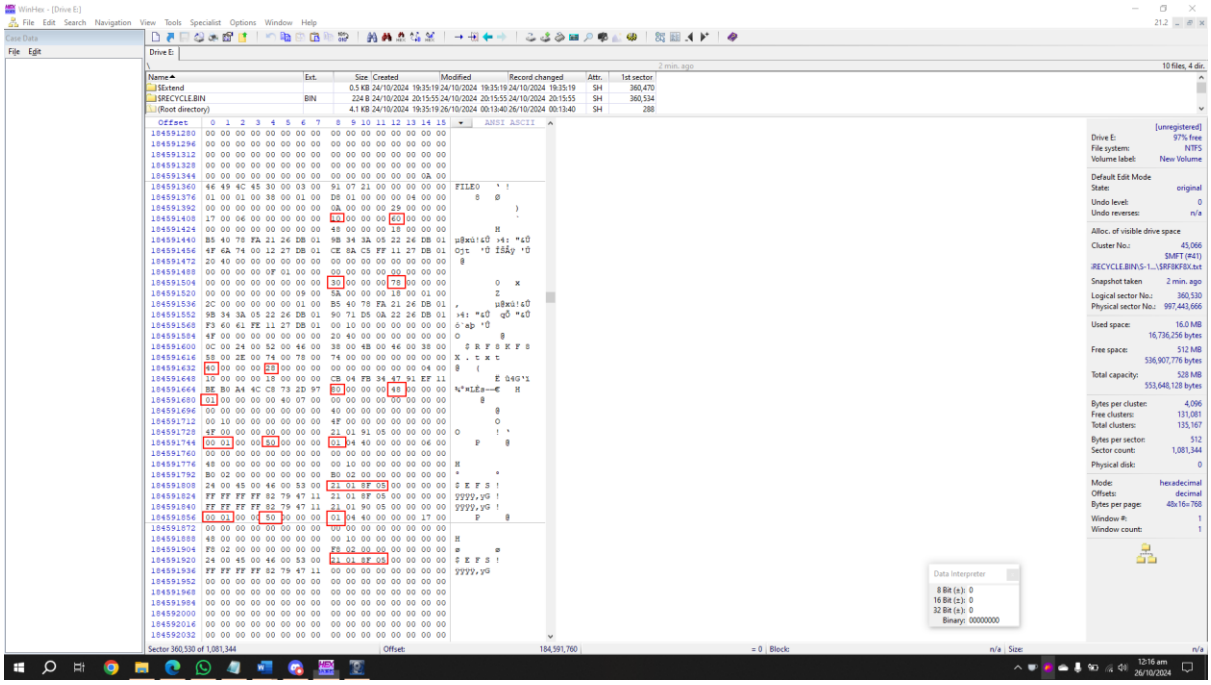




There are two 0x100 attributes one for DDF(Data Decryption Field) and the other for DRF(Data Recovery Field). The FEKI and FEK are stored in an external file with their data runs given.



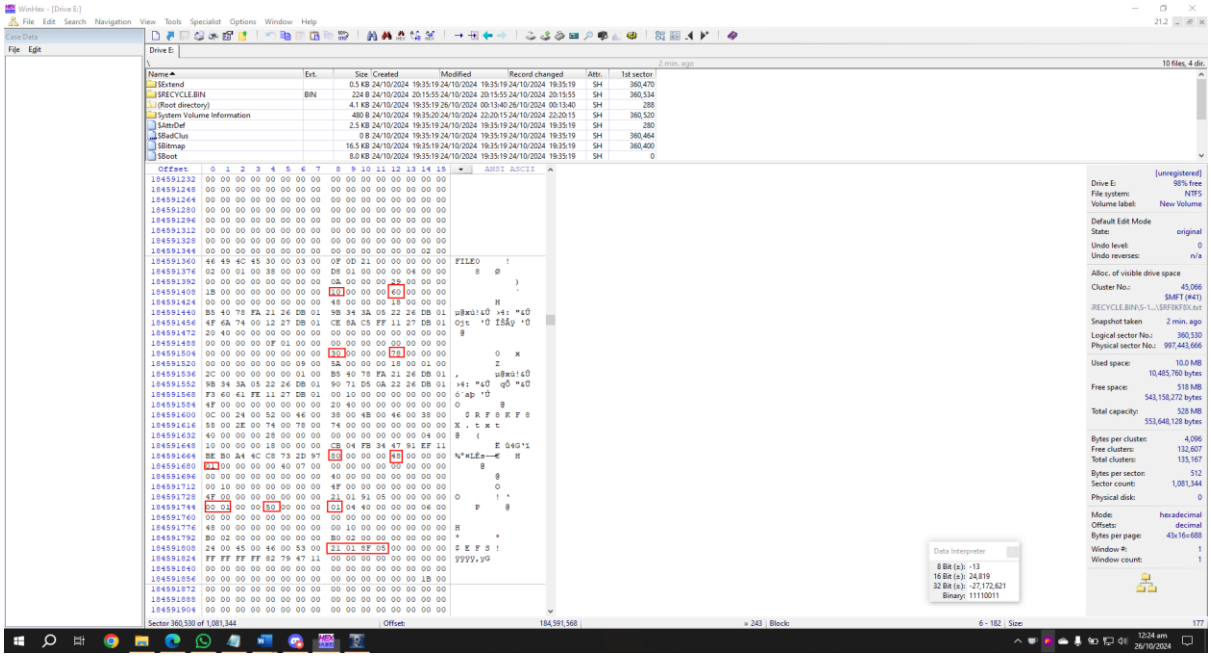
Question 2



The only thing that was changed was 0x30 attribute length which changed the name of the file and the MFT modified date and time. EFS remained the same even with the file in recycle bin.

Question 3

In this, same as ADS, we also needed to delete the file from Recycle Bin and analyse the MFT record again.



Changes in MFT of ADS after Deletion From Recycle Bin

- One EFS(0x100) entry was removed most probably DDF.

Summary

To summarise this assignment, we found some interesting things such as how MFT records are changed when a file is deleted temporarily and permanently in both cases as normal and encrypted file.

References

attribute-encrypted-files. (n.d.). Retrieved from ntfs.com: https://ntfs.com/attribute-encrypted files.htm logged_utility_stream.html. (n.d.).

Retrieved from flatcap.github.io: https://flatcap.github.io/linux ntfs/ntfs/attributes/logged_utility_stream.html Maningo, J. (2015). efs-protecting-files-at-rest.

Retrieved from quickstart.com: https://www.quickstart.com/data-science/efs-protecting-files-at-rest/ Nelson, B., Philips, A., & Steuart, C. (2019). Guide to Computer Forensics and Investigations 6th ed. Cengage.