National University of Computer and Emerging Sciences
Islamabad Campus

CY2002

Digital Forensics

Assignment 04

ADS and EFS files

Submitted by: Abdul Sami Qasim
Roll number: 22i-1725
Date: October 25, 2024

Table of Contents

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

Question 1 2

Question 2 6

Question 3 9

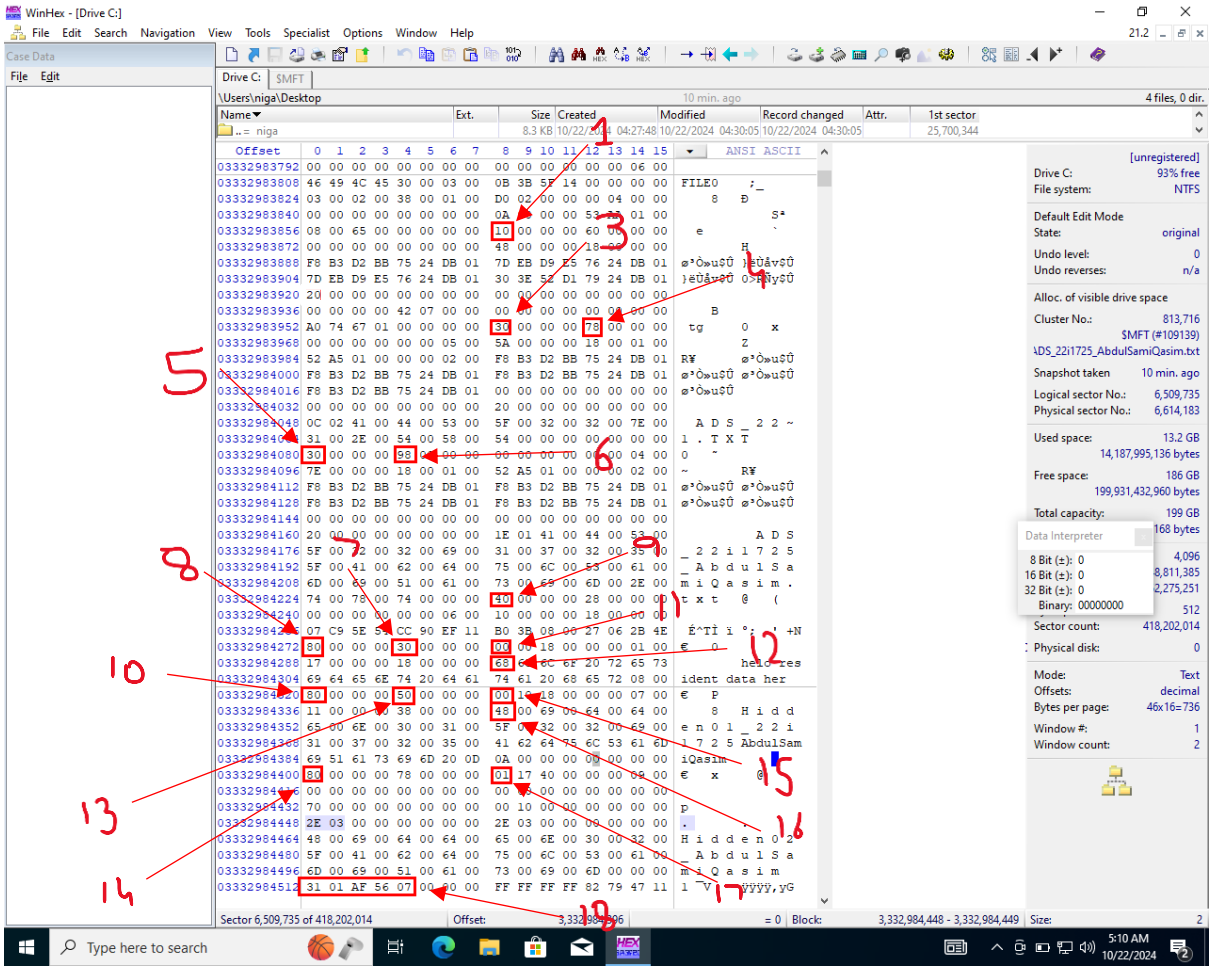
- **Summary** 11
- **References** 11

- # Introduction

  The assignment revolves around the use of winhex to read the MFT entries for ADS file streams and EFS encrypted files.

- # Details and Steps

Question 1

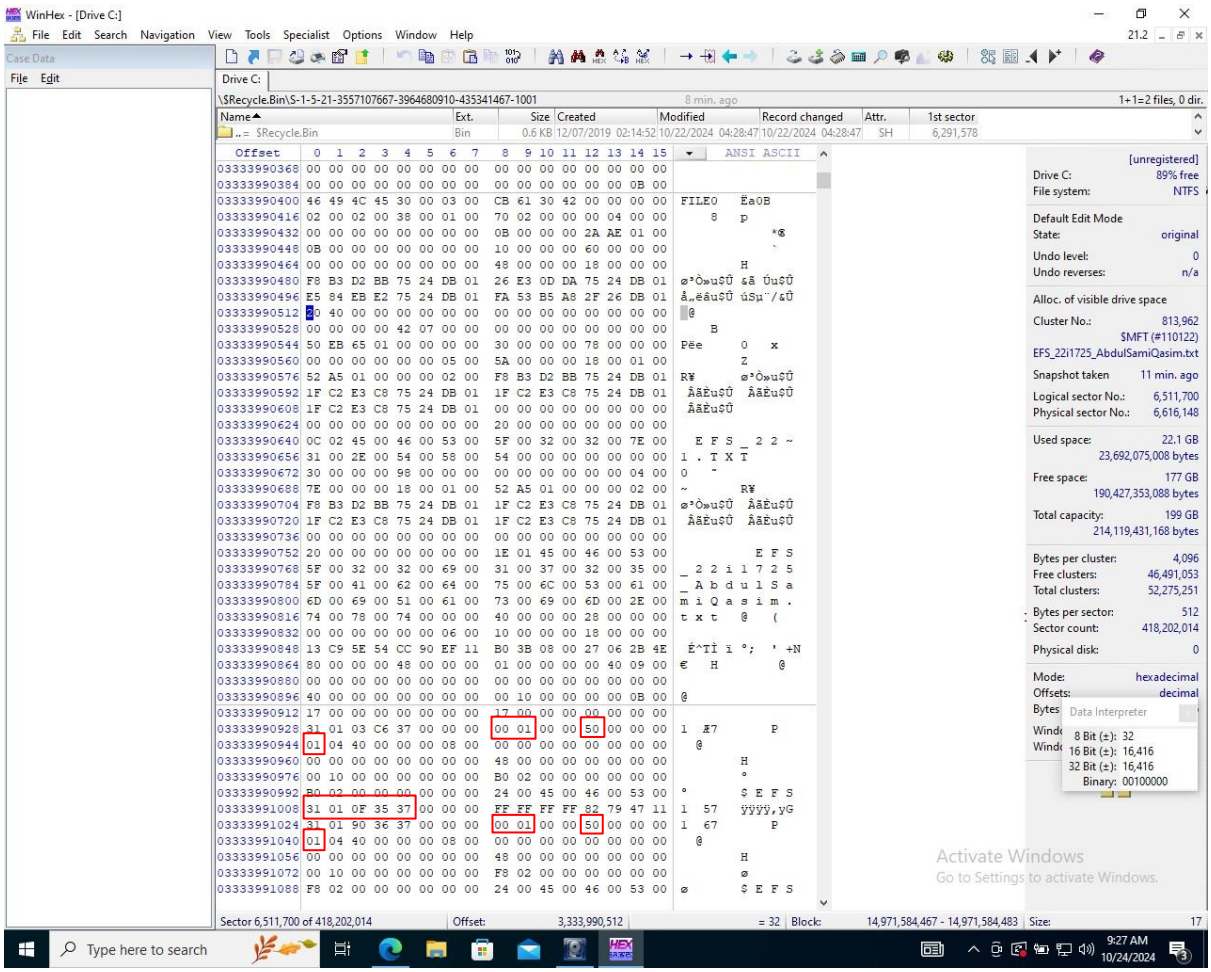


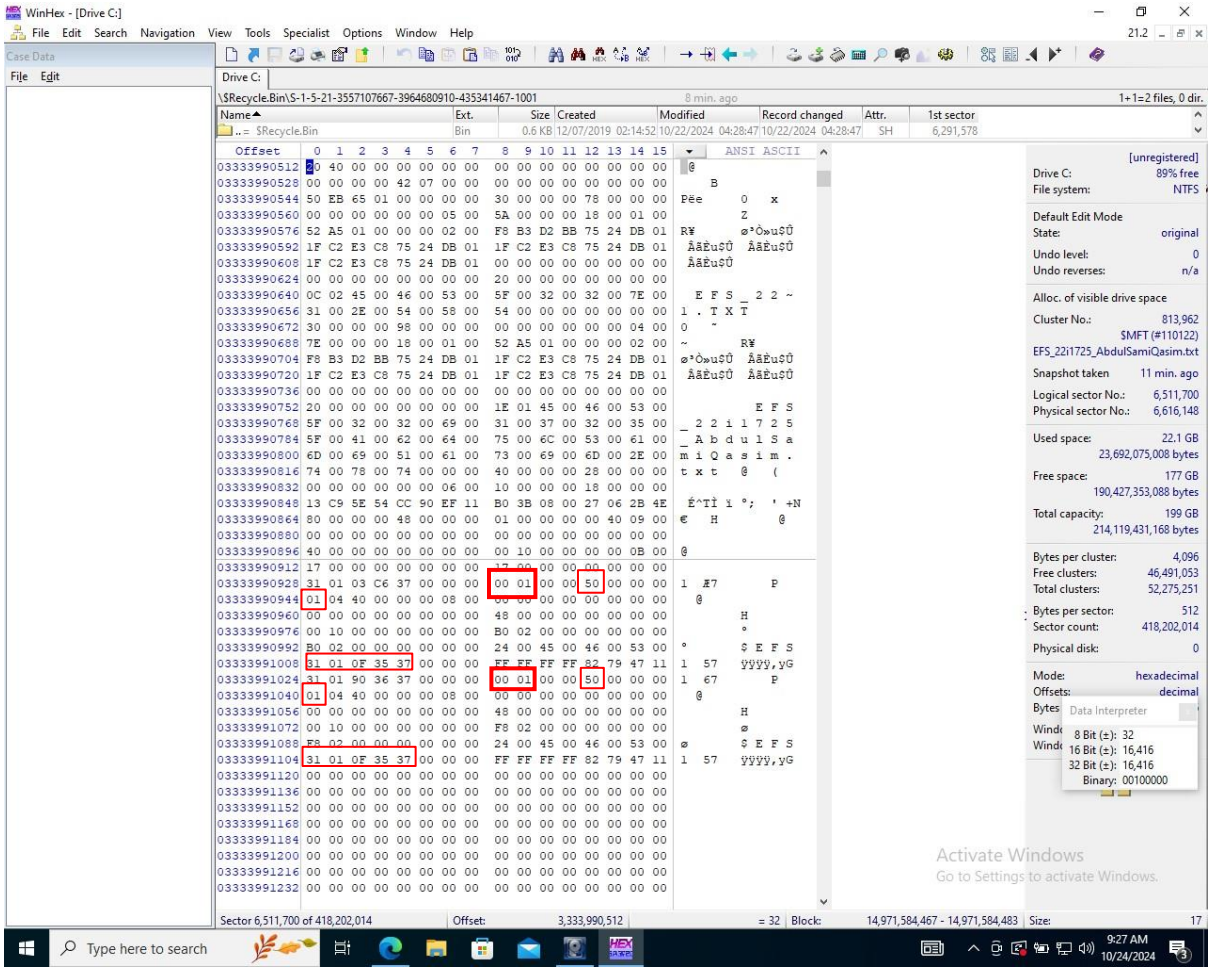
1. Attribute 0x10
2. -
3. Attribute 0x30
4. Size of 0x30 (0x78h bytes)
5. Attribute 0x30
6. Size of 0x30 (0x98h bytes)
7. Size of Attribute 0x80 (0x30h bytes)
8. Attribute 0x80
9. Attribute 0x40
10. Attribute 0x80
11. Flag for resident/non-resident (resident here as it is 00)
12. Start of data
13. Size of 0x80 attribute (0x50h bytes)

14. Attribute 0x80
15. Flag for resident/non-resident (resident as it is 00)
16. Start of data
17. Flag for resident/non-resident (non-resident as it is 01)
18. Datarun

This datarun has 3 components,

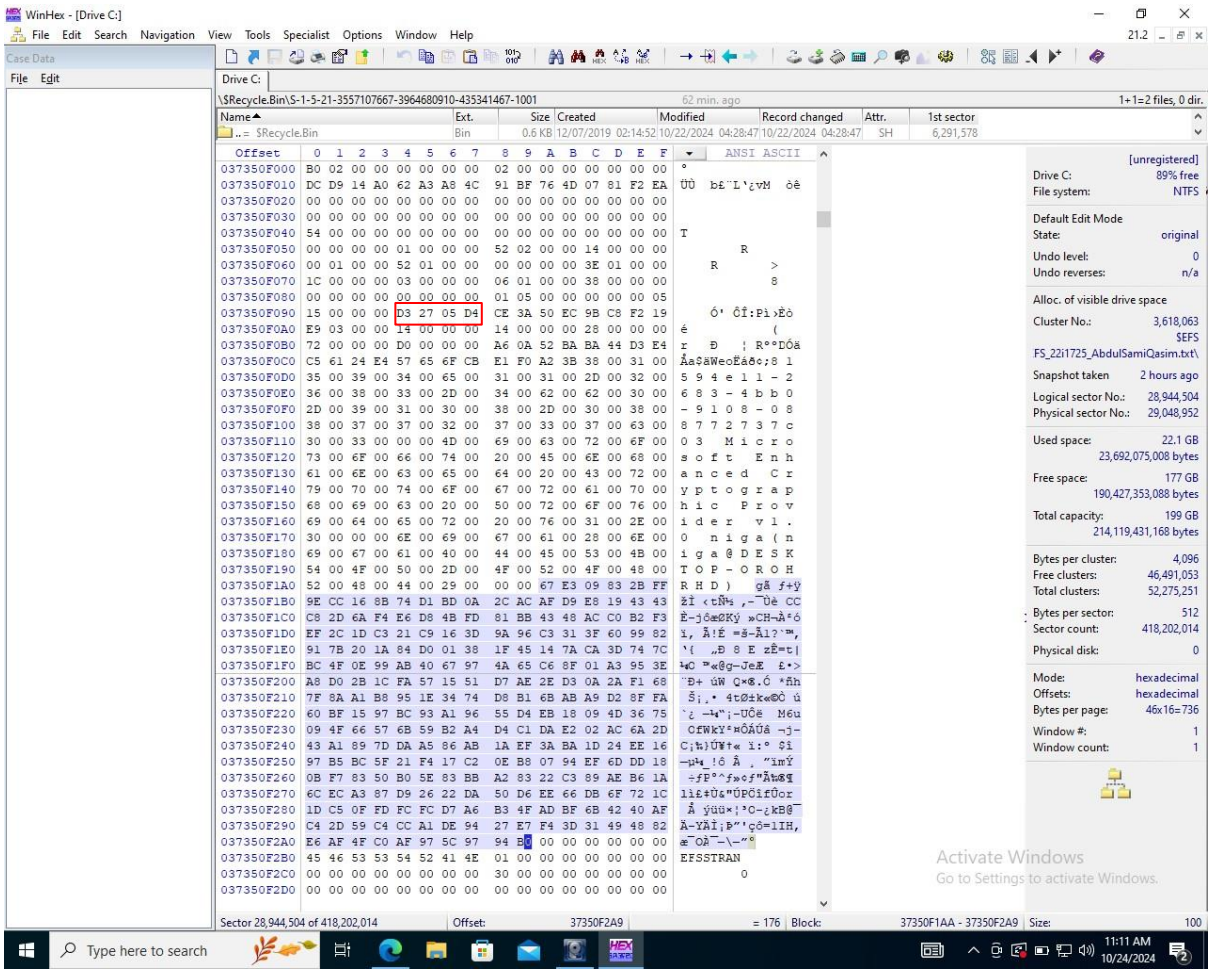
1. The first byte representing size of total datarun after that byte and individual sizes of second and third components.
2. The next component (size 01) represents the total cluster numbers
3. The last component (size 03) represents the LCN (logical cluster number) of the file content





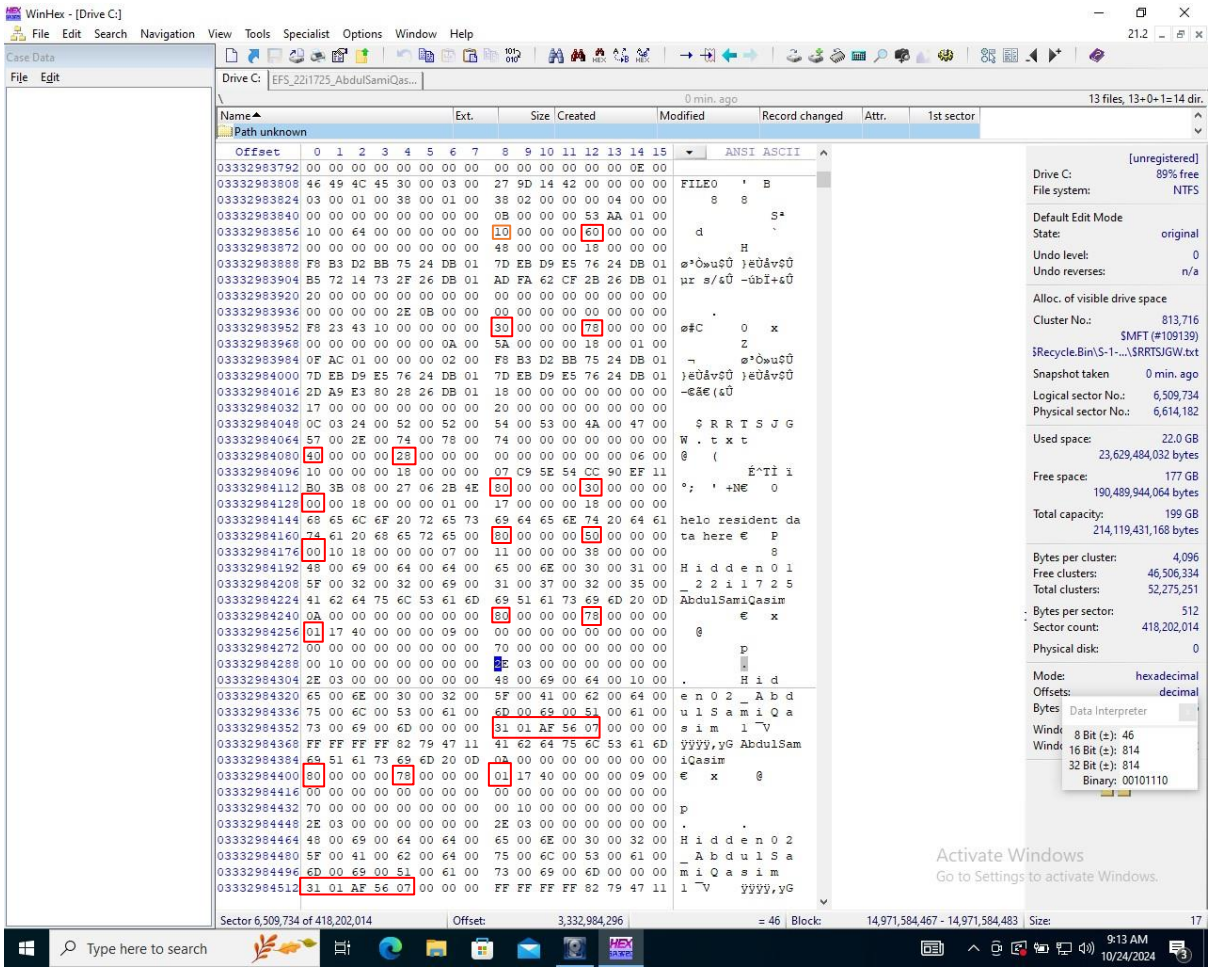
There are two 0x100 attributes, one is the DDF (Data Decryption Field) and the other is the DRF (Data Recovery Field). The FEK and FEKI both are non-resident, as suggested by the 01 flag on the 8th offset byte from the start of the attribute.

THE FEK is located here (highlighted in light blue is the FEK):



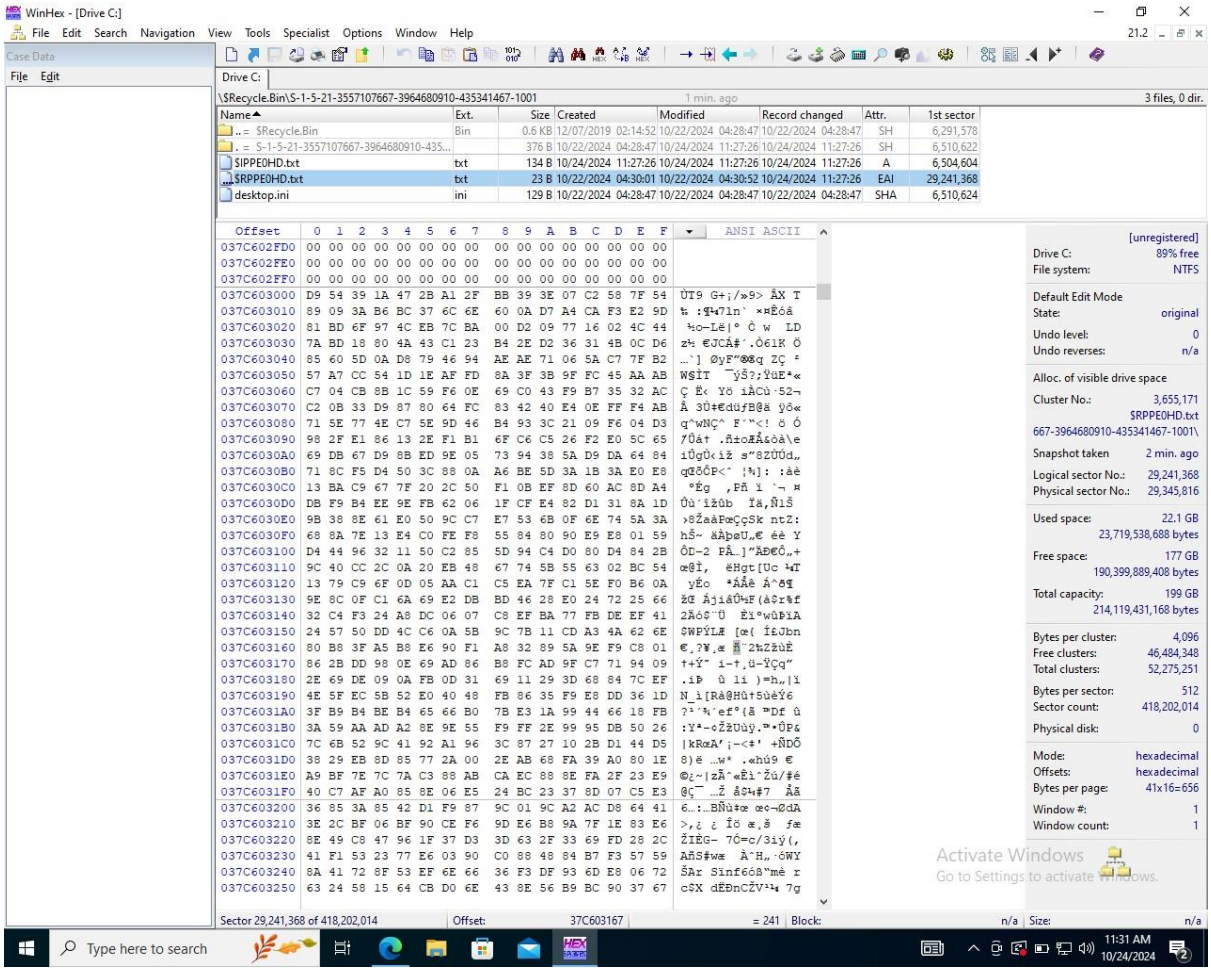
The hexes highlighted in red mark the start of the FEKI which goes on till the beginning of the FEK (the block highlighted in blue)

Question 2

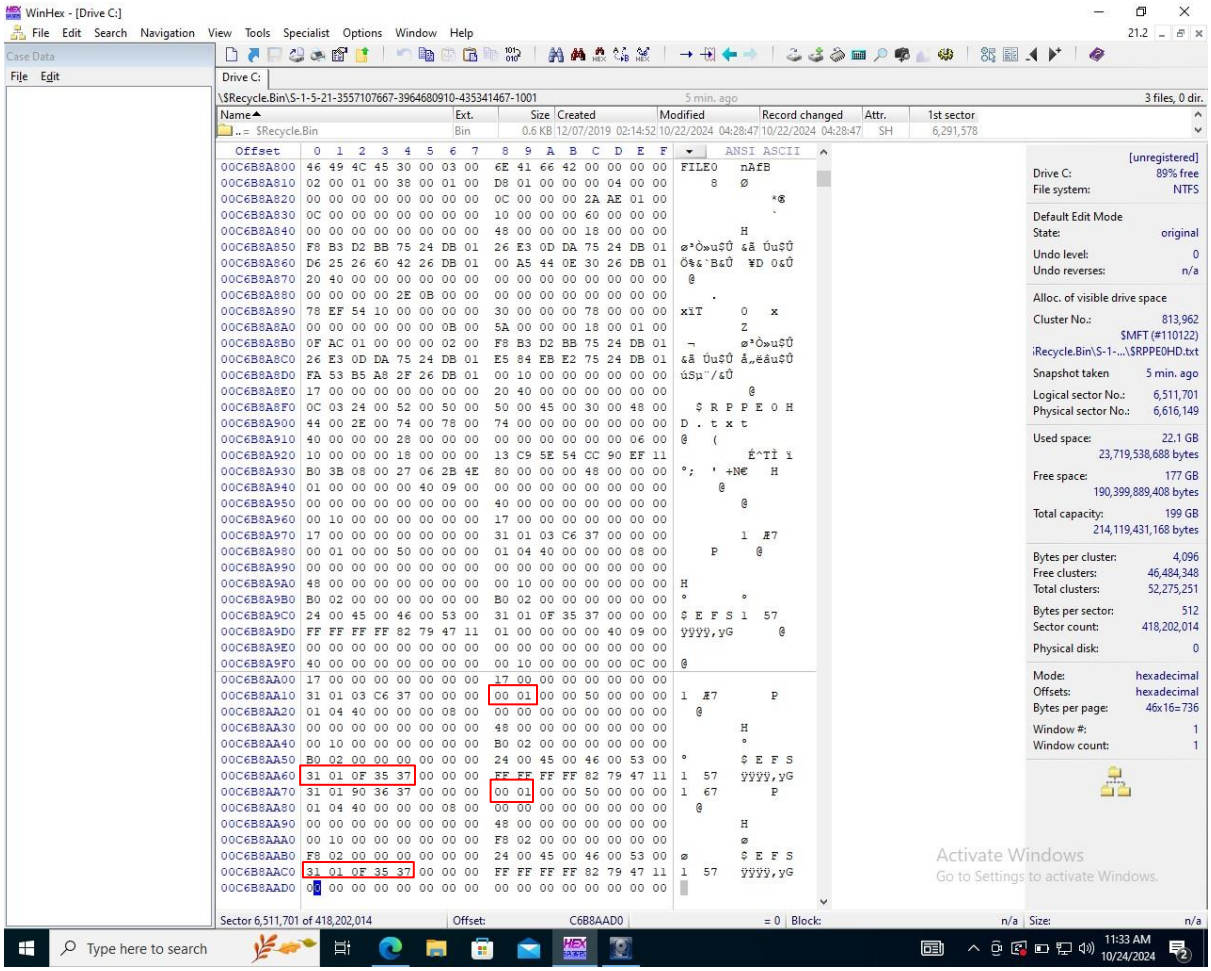


Changes:

1. Second 0x30 attribute is removed
2. Name of the .txt changed
3. Resident data remained the same and the hidden files are still intact
4. There are two same 0x80 attributes



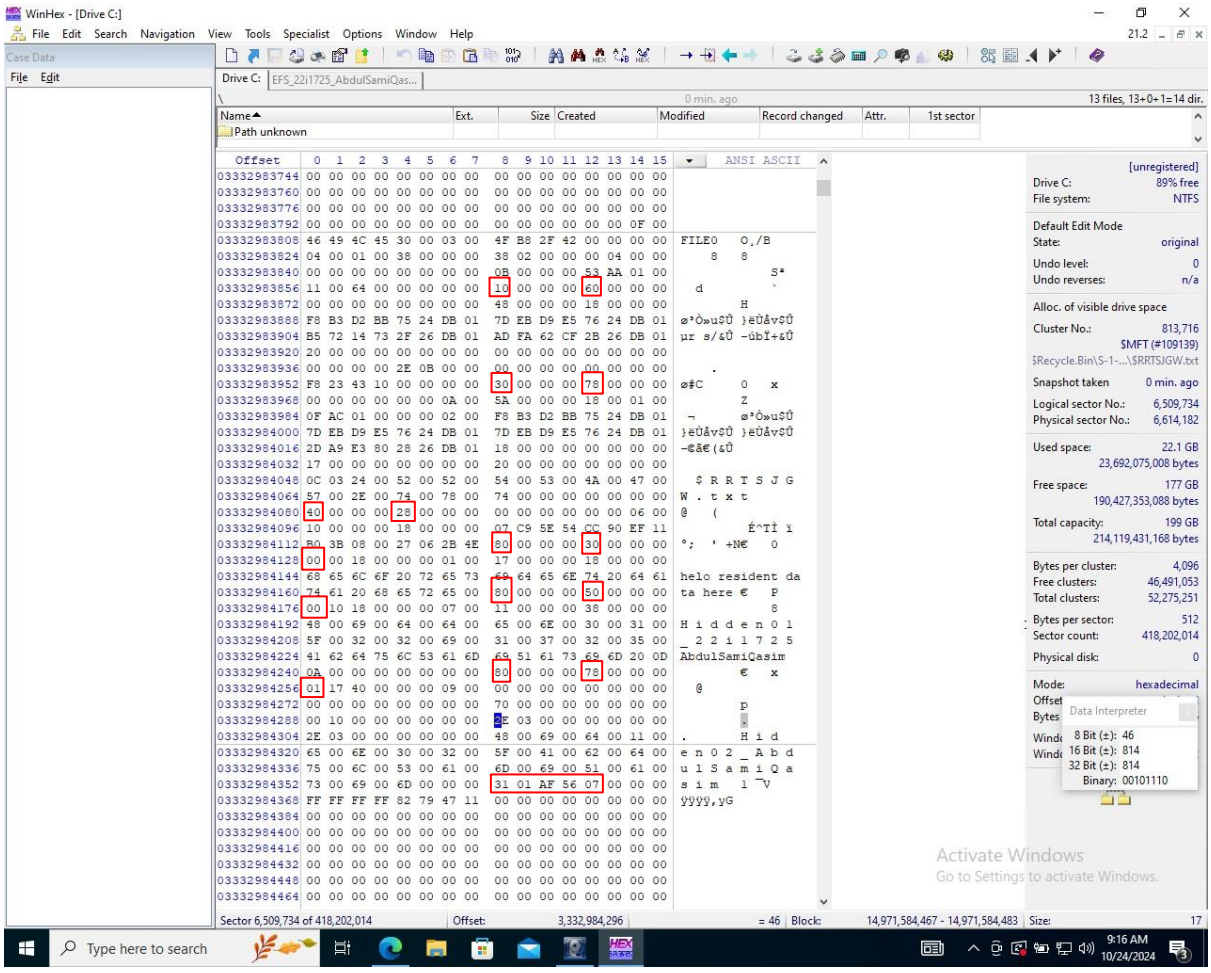
Data remains encrypted even after deletion.



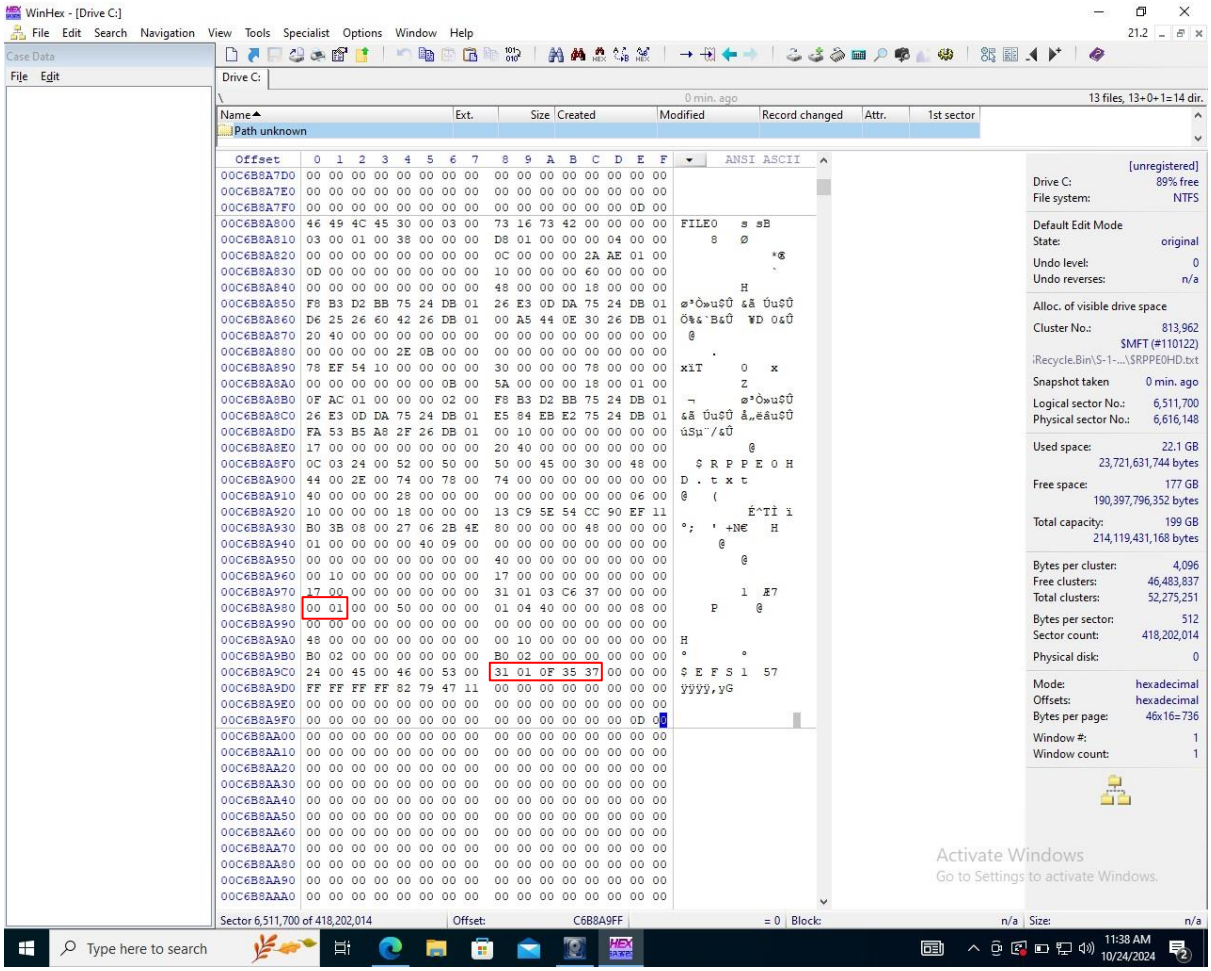
Changes:

1. One 0x30 attribute got deleted
2. Name changed

Question 3



Everything is the same except for the second 0x80 attribute.



One 0x100 attribute got deleted.

• Summary

To summarize the assignment, we've manually seen how to find the data in a file, how to locate dataruns and we saw how to find information about an EFS 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.