

**CY2002**

**Digital Forensics**

**Assignment 01**

**Assignment Title**

**Submitted by:** Mirza Humayun Masood

**Roll number:** i221749

**Date:** 20th October 2024

**Table of Contents**

[ **Introduction** 2](#_Toc180354107)

[ **Details and Steps** 2](#_Toc180354108)

[Q1 2](#_Toc180354109)

[Q2: 9](#_Toc180354110)

[Q3: 11](#_Toc180354111)

[ **Summary** 15](#_Toc180354112)

[ **References** 15](#_Toc180354113)

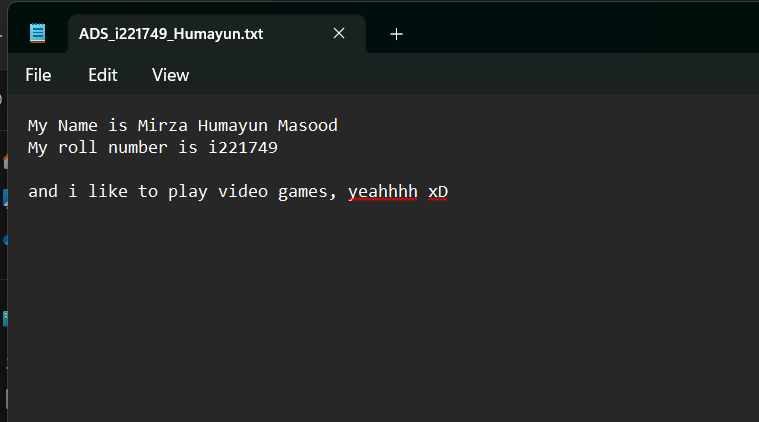
# **Introduction**

# **Details and Steps**

## Q1

In this Question we have to make Two files, one with EFS and one with ADS.

So for this questions a part, I made a txt file and entered following data in it.



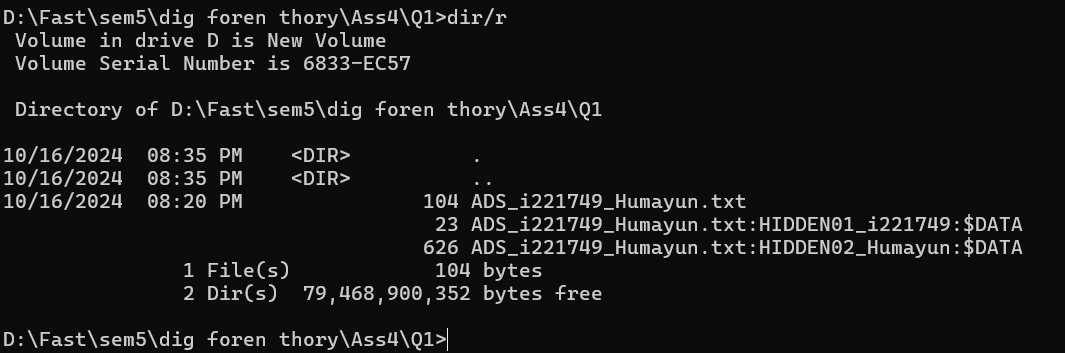
So after that, I wrote this command to attach a resident ADS with this file.

“echo Mirza Humayun Masood > ADS\_i221749\_Humayun.txt:HIDDEN01\_i221749”

And then I added another ADS file with non-resident data.

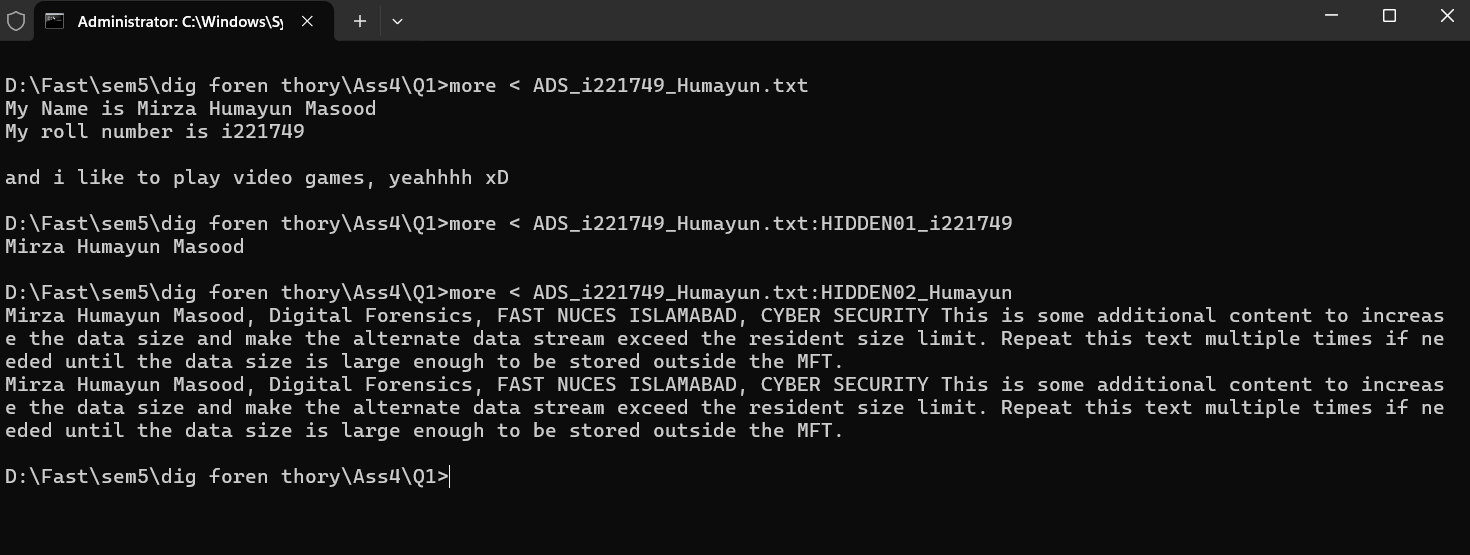
“echo Mirza Humayun Masood, Digital Forensics, FAST NUCES ISLAMABAD, CYBER SECURITY This is some additional content to increase the data size and make the alternate data stream exceed the resident size limit. Repeat this text multiple times if needed until the data size is large enough to be stored outside the MFT. Mirza Humayun Masood, Digital Forensics, FAST NUCES ISLAMABAD, CYBER SECURITY This is some additional content to increase the data size and make the alternate data stream exceed the resident size limit. Repeat this text multiple times if needed until the data size is large enough to be stored outside the MFT. > ADS\_i221749\_Humayun.txt:HIDDEN02\_Humayun”

so yeah it made two files. So when I dir/r in this directory, it shows.

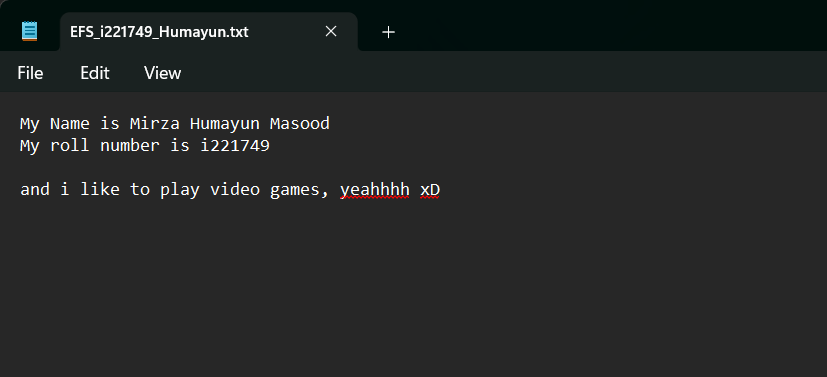


So as you can see it added two files, one with 23 bytes, and one with 626 bytes.

Now lets see the content of these files.

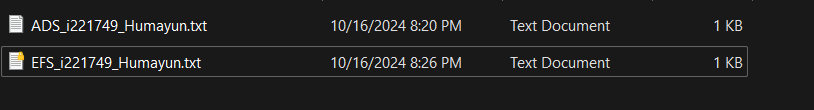


Now lets make a EFS file in the same directory.



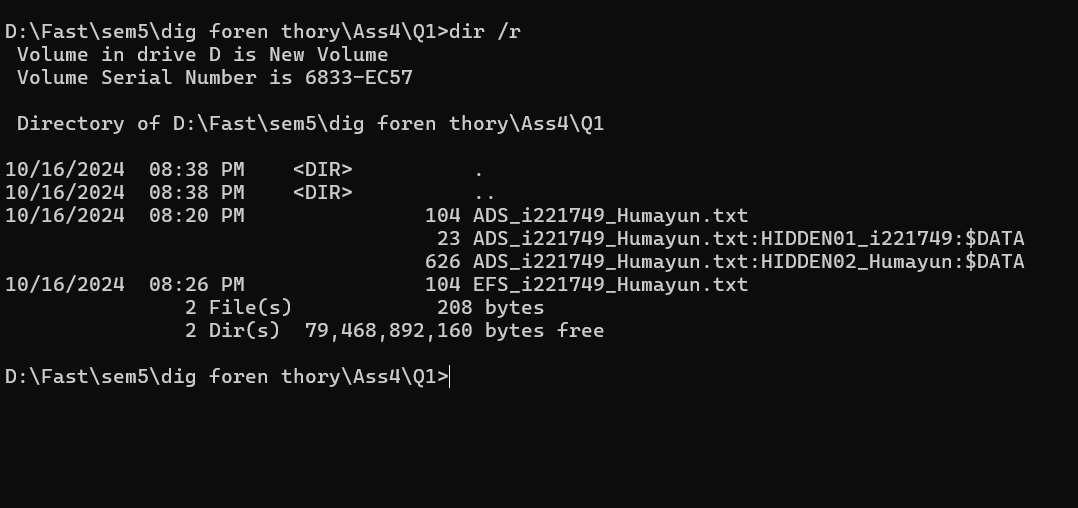
So I made the file with same content.

Now lets encrypt it.

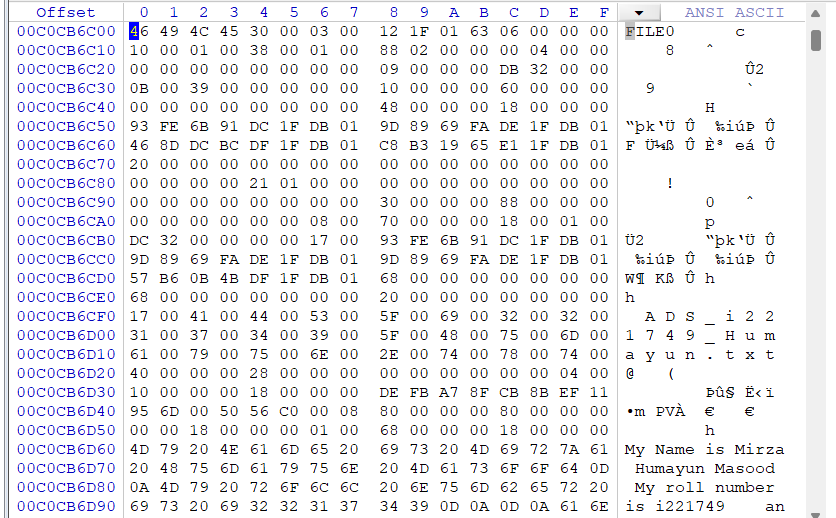


As you can see the lock on it.

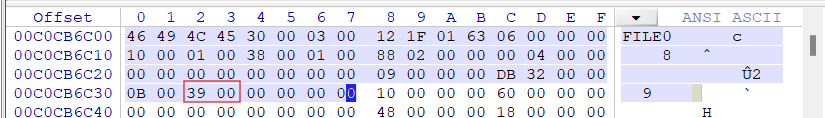
And



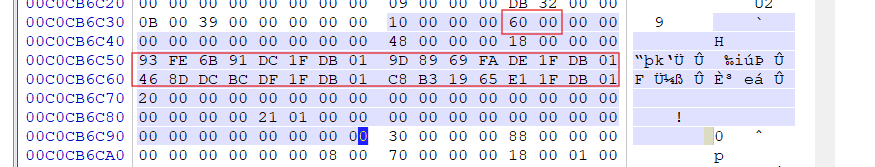
So when we open this file in Winhex, so its MFT Entry looks like



**Update Sequence Array**

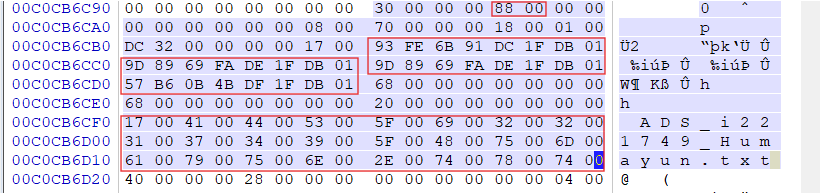


**Attribute 0x10 and its size**



And times are also highlighted.

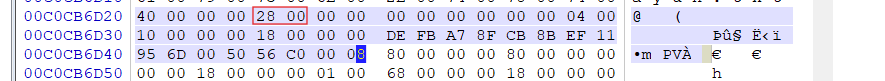
**Attribute 0x30 and its size**



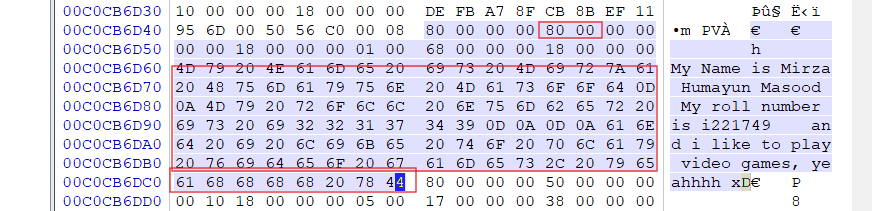


Also the times are highlited, and the name of the file aswell.

**Attribute 0x40 and its size**

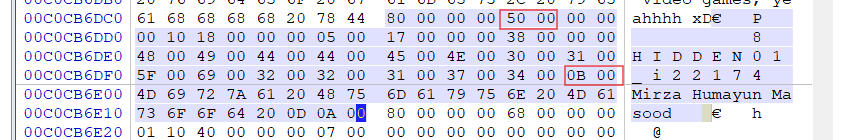
****

**Attribute 0x80 1**

****

It also has content in it, And its also resident.

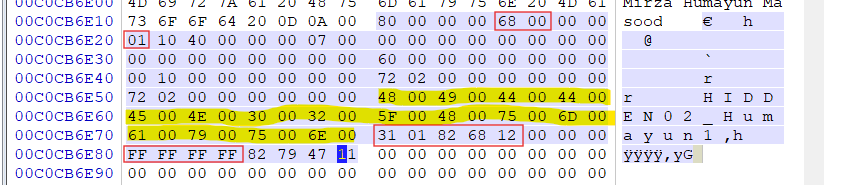
**Attribute 0x80 2**





It had the update sequence array replicable bytes, and the name of the ads, and also the content present in it. Its also Resident.

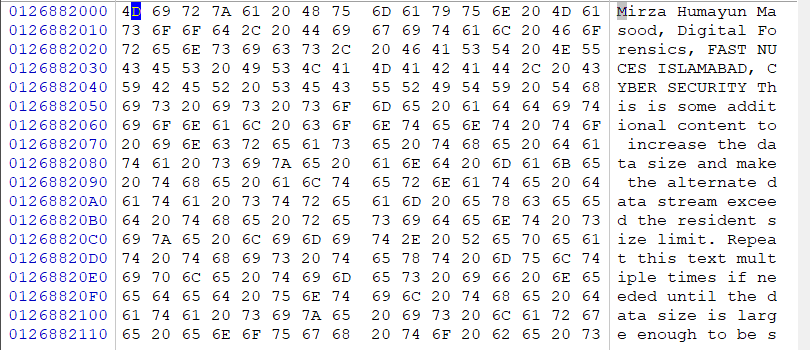
**Attribute 0x80 3**



As this is Resident, so we have to find its Data runs.

The Data run was 31 01 82 68 12

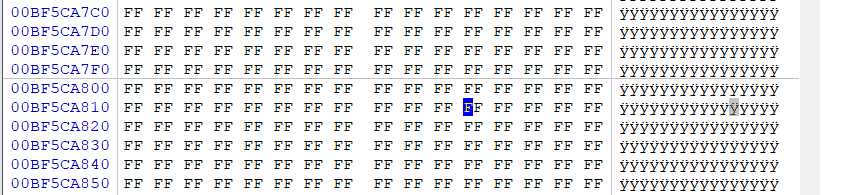
01 is the number of clusters assigned. 126882 is the cluster number in hex which become 1206402 in Decimal, and when we reach the Disk address we can see.



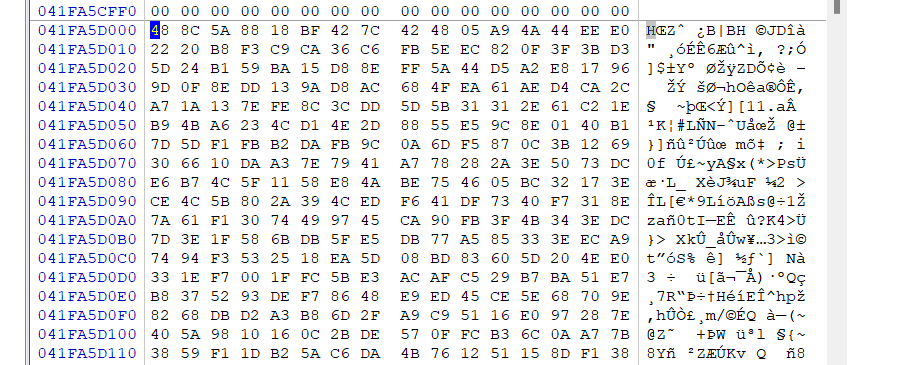
Now we see its entry in **bitmap**, that is it 1 or not.

Yeah, it is occupied

I actually divided 1206402 with 8 = 150800, and then added the 150800 bytes into starting address of Bitmap starting address.

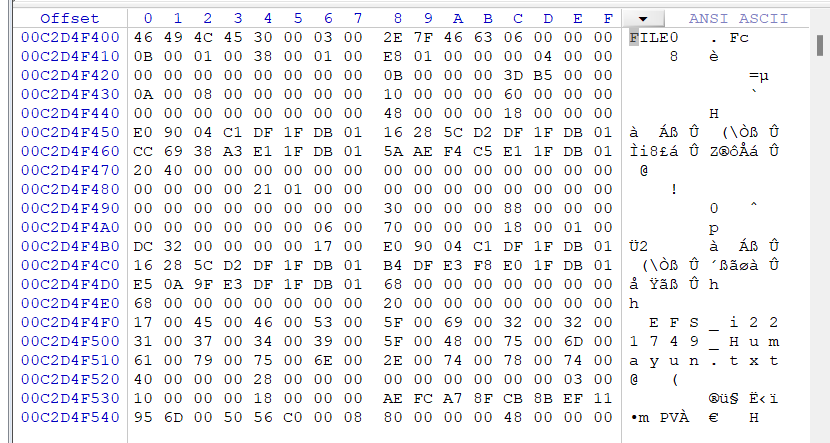


So, **for EFS file**



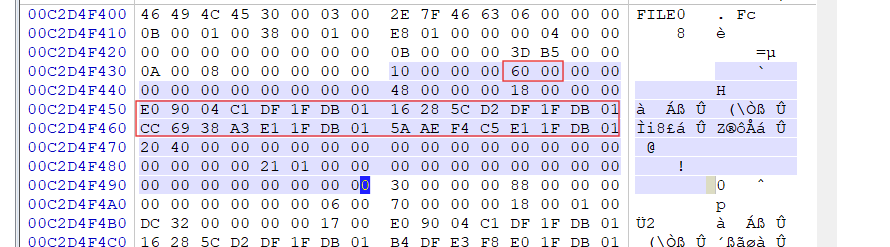
So, it is all encrypted.

But when we go to seek file record.

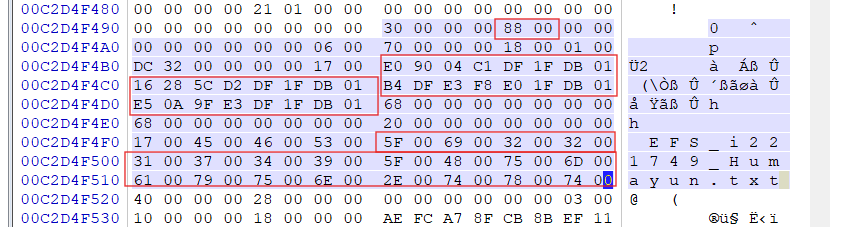


Now we see the attributes.

**Attribute 0x10**

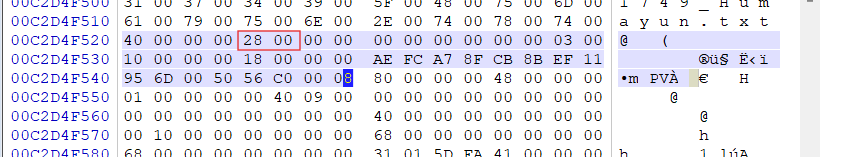


**Attribute 0x30**

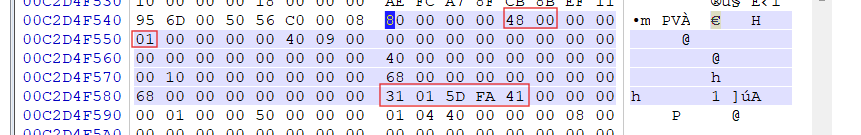


So its name is also highlighted.

**Attribute 0x40**

****

**Attribute 0x80**

****

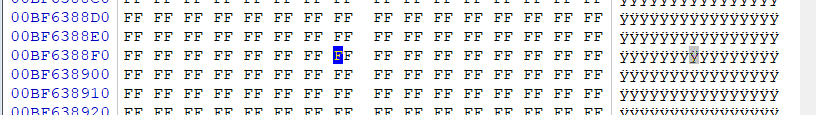
It is not resident as we have seen its place on disk which is all encrypted.

Its data run is, one cluster, and number is 41FA5D in hex, 4,323,933 in decimal.

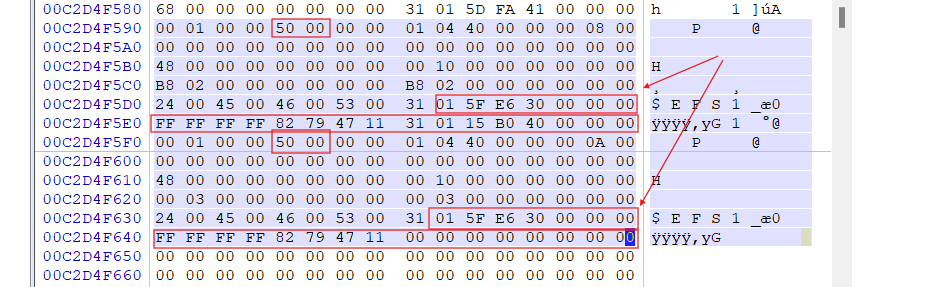
So if we see the bitmap for this.

4323933 with 8 = 540491

I added the value, and saw that the cluster was occupied.



**Attribute 0x100**

****

It had two 0x100 attributes, the highlighted part is FEKI, while it also have DDF offset and length and DDR offset and length.

So

DDF1: 00000008 (0)

DDF2: 0000000A (0)

DRF1: 00000000 (0)

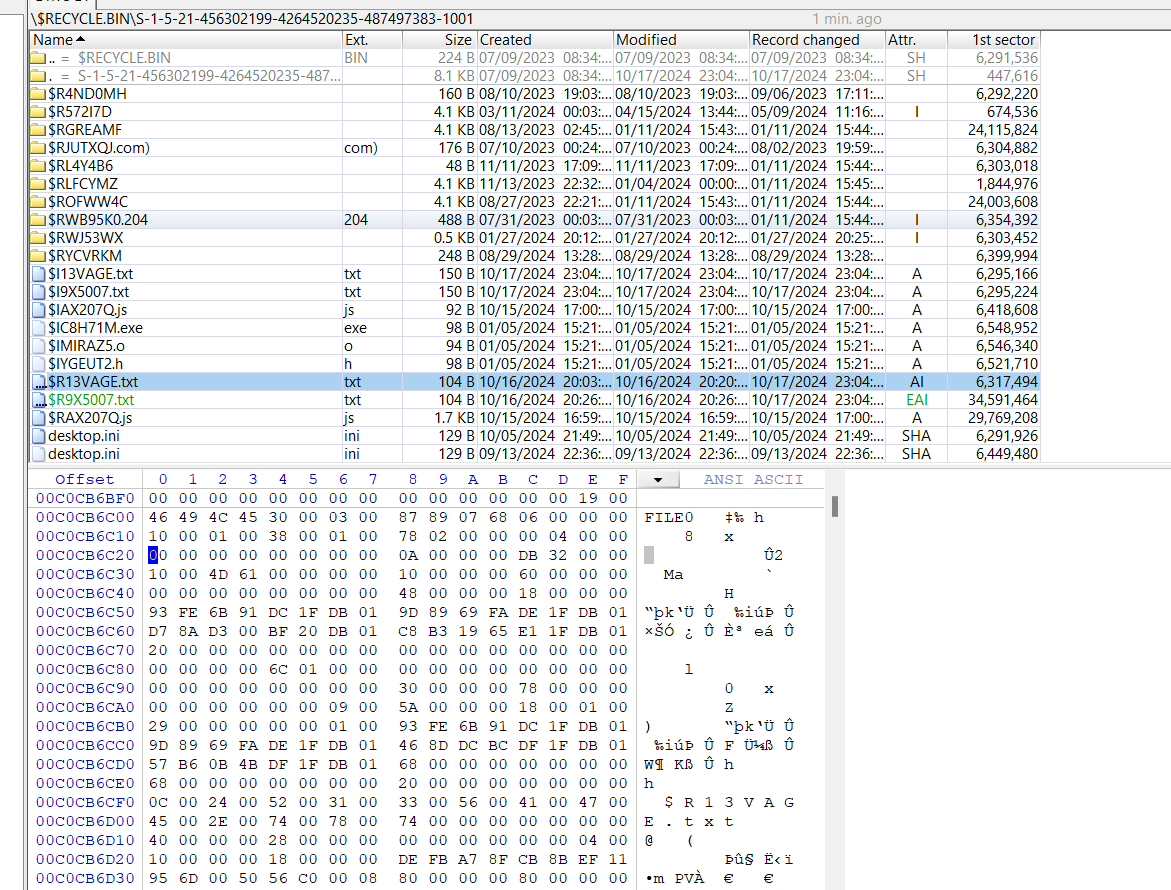
DRF2: 00000000 (0)

DRFs are zero that means there is no Data Recovery Field.

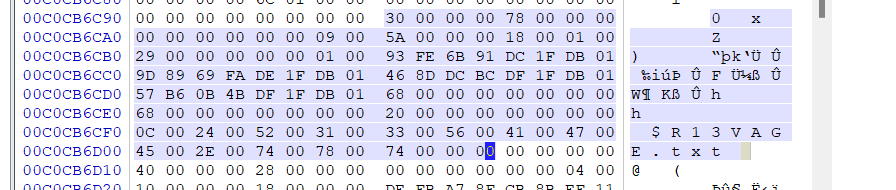
But Data decryption field is present in here.

## Q2:

So, lets just delete the files and see there MFT record entries.

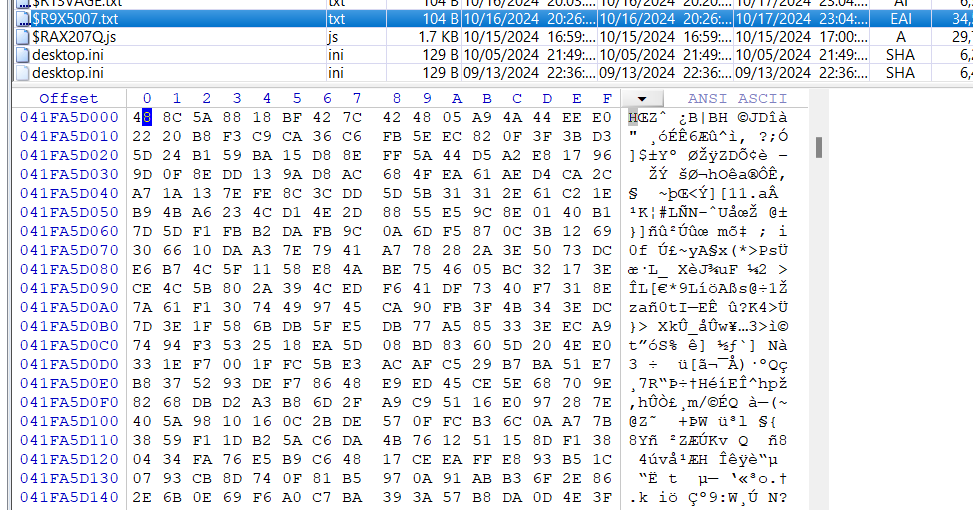


So when I opened the recycle bin, it had the files and the MFT record entry is still available in MFT.



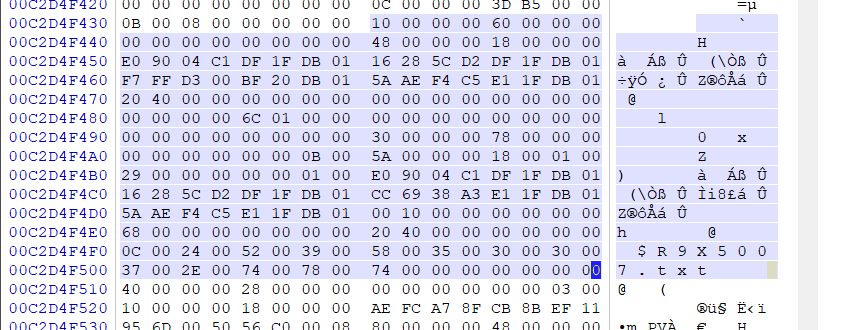
So the Name of the file is changed , and The last accessed time is also changed in attribute 10 and 30.

The rest is the same for ADS file, now look at EFS file.



After Deleting the content is still encrypted.

Now lets see the file record.



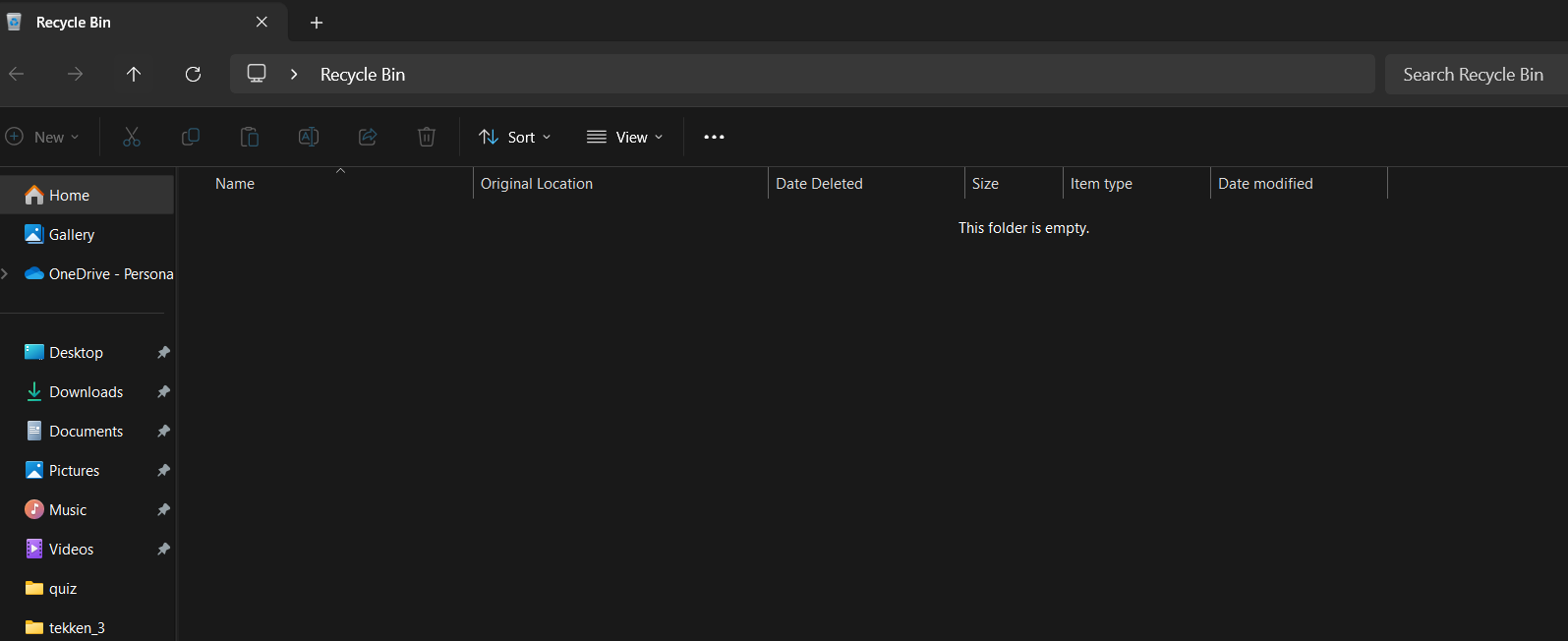
Name of the file and Accessed date in 10 and 30 is changed.

Rest is the same.

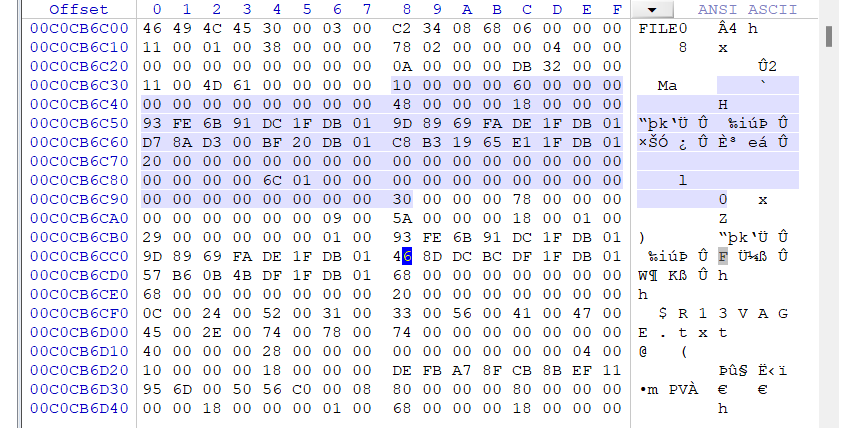
And the bitmap file is also the same.

## Q3:

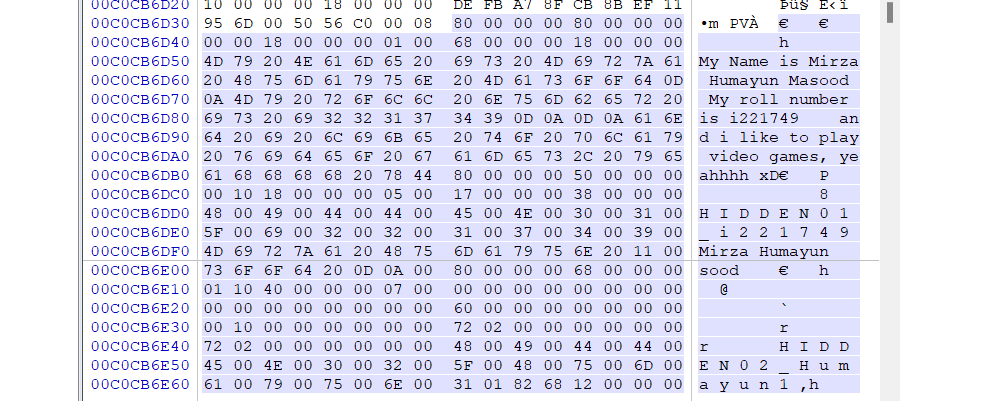
After Clearing the recycle bin.



For ADS file

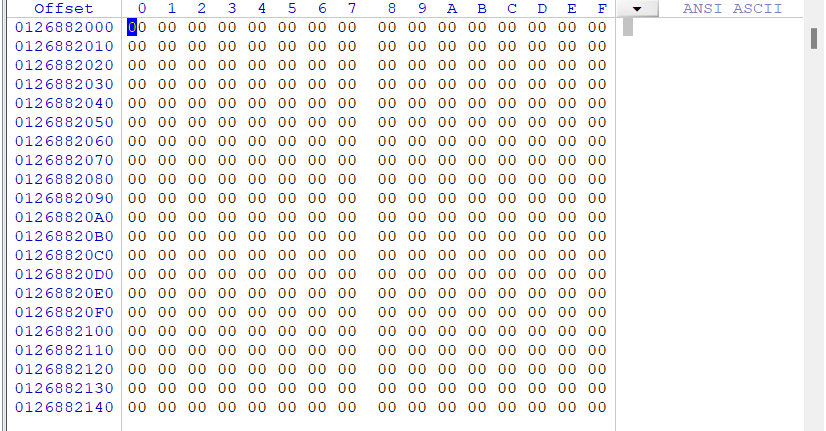


The record is still there.

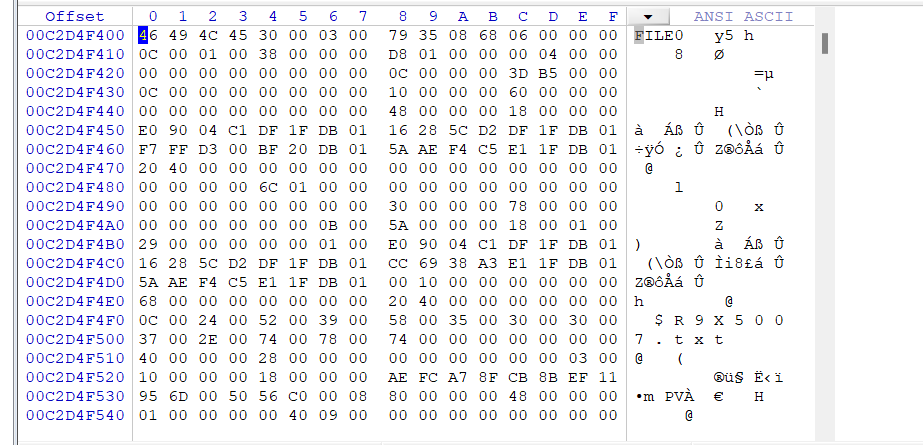


80 attributes still have the value.

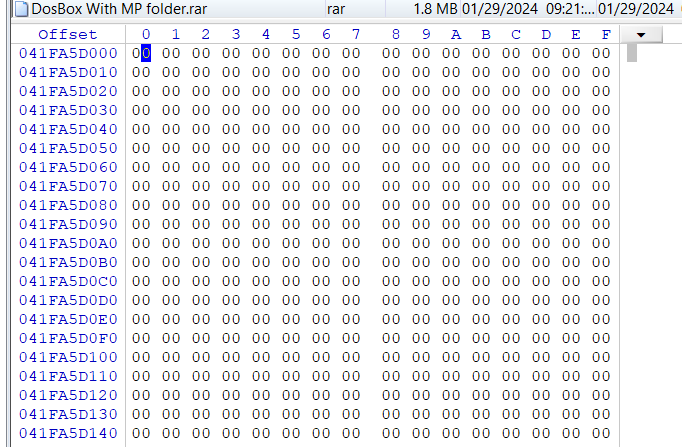
The cluster value is empty.



Now for EFS file.



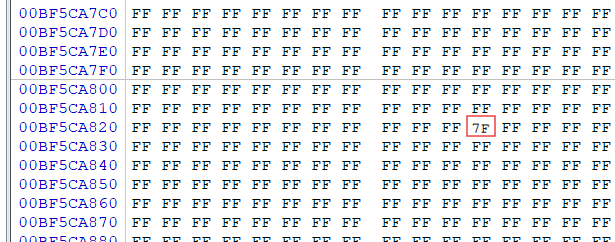
The file record looks the same.



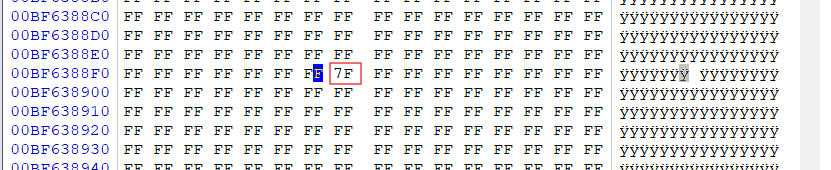
Cluster is empty aswell.

Now Bitmap file

For ADS



For EFS



So yeah it changed.

# **Summary**

In this assignment we were asked to Do analysis of MFT Record of ADS and EFS files where we looked at the clusters they reside on, By deleting, their attributes, and Bitmap file.

# **References**

Add at least 3 references to your assignment including course book.