Project 1: Case Study

-SPR400

Case Name: Industrial Espionage

Investigator Name: Syed Mujahid Hamid Ali

Student ID: 161202213

Email: shamid-ali@myseneca.ca

Table of Contents

Overview

This report is made as per the police's request. An investigation was done on an image of Larry's USB, who has been accused with Industrial Espionage. The investigation was done to check if there was any evidence that would prove that Larry was actually selling any data to other companies or not.

From the image we were able to find multiple files that were deleted, as they held important information. Regardless, we were able to extract those files alongside other files that showed that Larry was actually planning on selling an application source code to James, who was willing to pay $5000 more than the highest offer placed by other companies.

The report includes a detailed account of the investigation methodology, evidence collection and analysis, findings, recommendations, and conclusion.

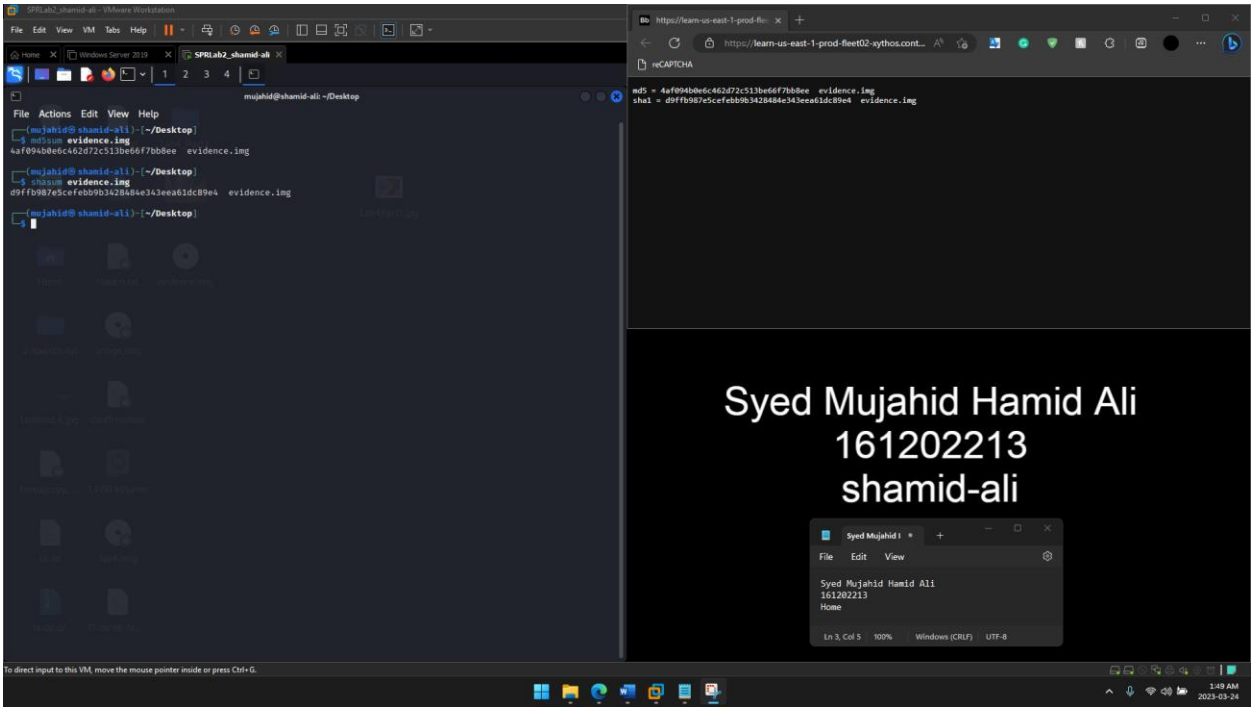
Evidence and Objectives

E1: One (1) image of Larry's USB

For this investigation, we were supposed to find the following:

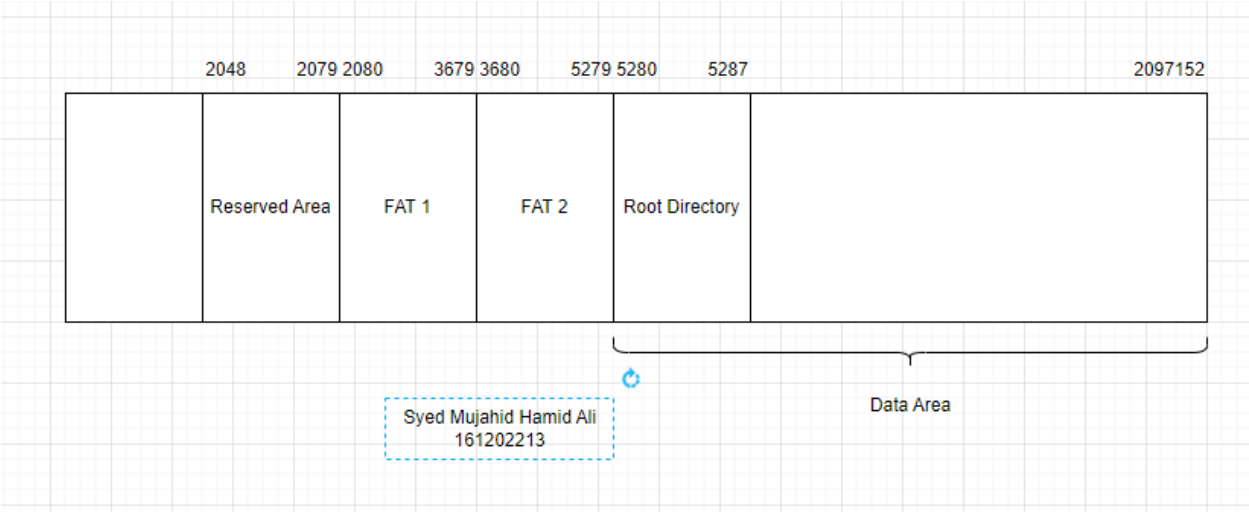
- The bidders for the application source code
- If there was any other data that Larry sold
- The processes taken by Larry to mask the files from public
- Other files that were recovered and if they are related to the investigation
- Steps taken by the investigator to examine the contents of all the files

We will prove that we are using the same image by checking the md5sum and sha1sum provided by in blackboard.



Forensic Analysis

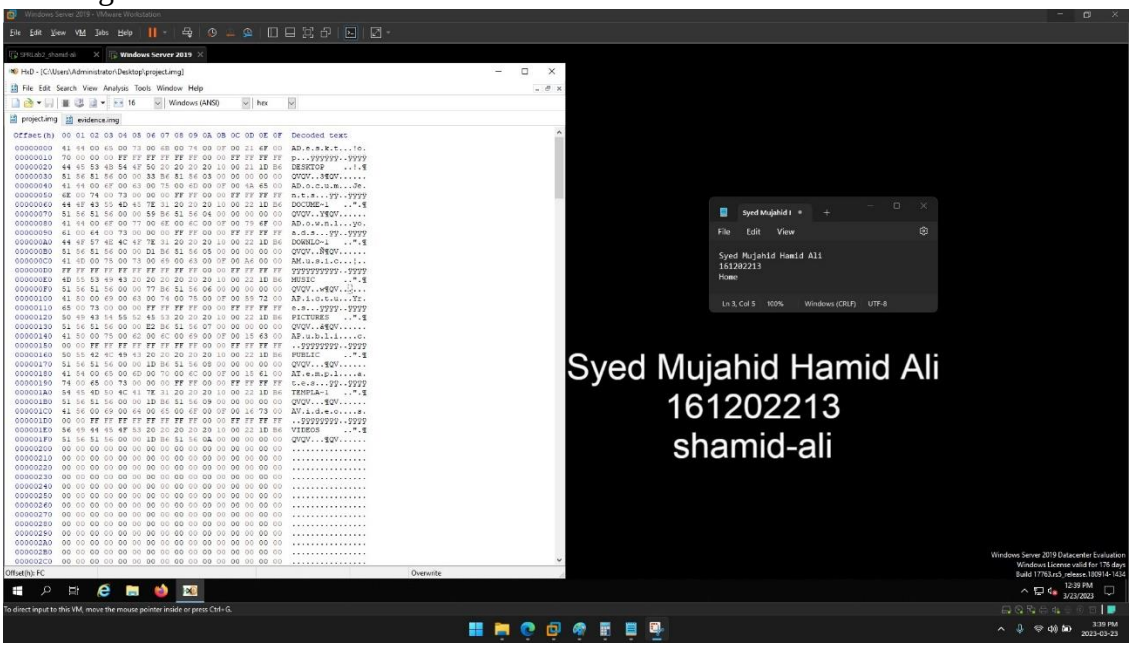
1) First, I made a diagram so that I would get the sector address for the image of the USB itself.



Now, we know that

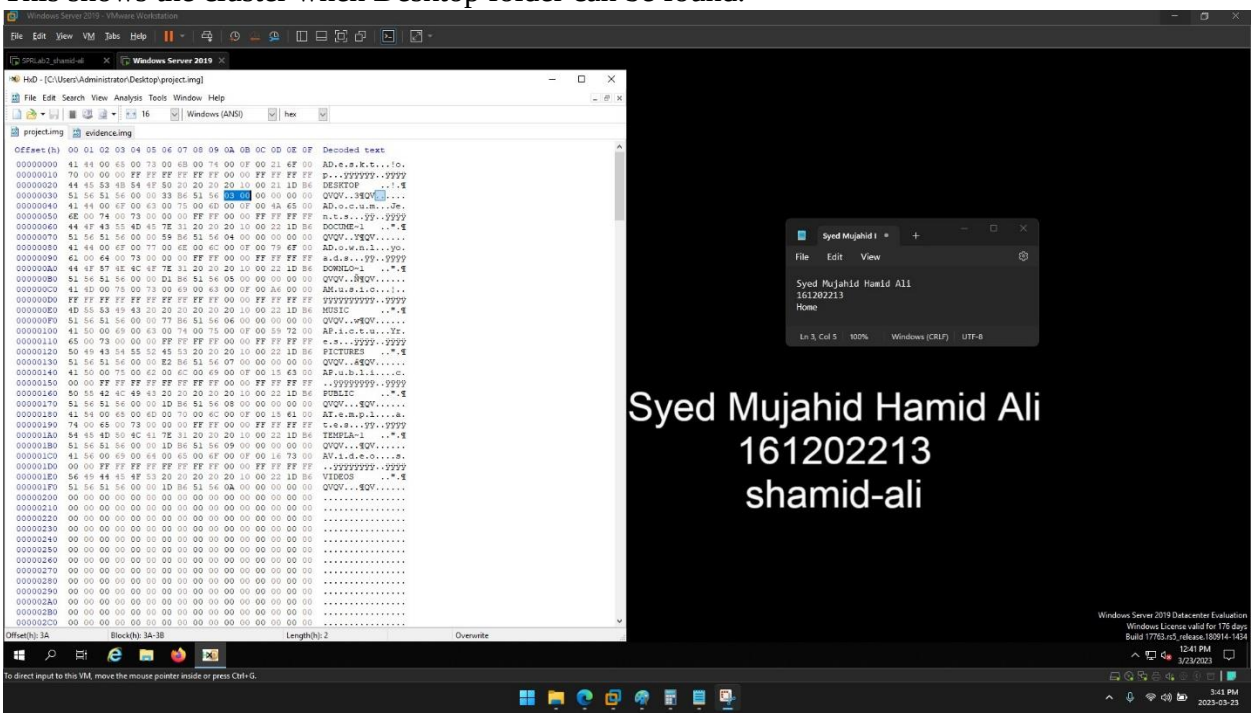
- This is a FAT32 file system.
- There are 512 bytes per sector.
- Reserved Area starts from sector 2048 and is of 32 sectors in size.
- There are two FAT tables, each of 1600 sectors in size.
- Root Directory is present right in the beginning of Data area and is of 8 sectors in size.
- Data area begins at sector 5280.
- Each cluster is of 8 sectors in size.

2) Next, I made a separate image for the Root Directory which will help in easier analysis of the image.

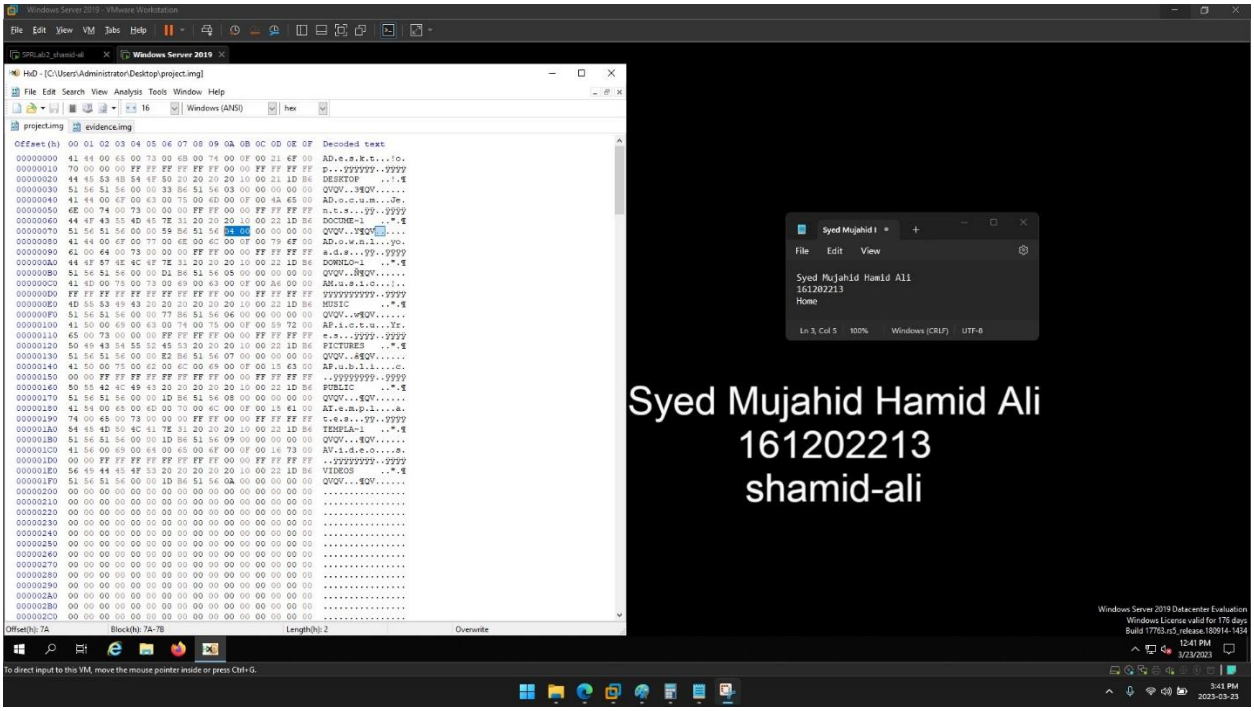


From this, we know that these are the folders present in the USB. We will get to know where the folders are present from the high 2 bytes and low 2 bytes, which would give the location of the files present in the specific directory.

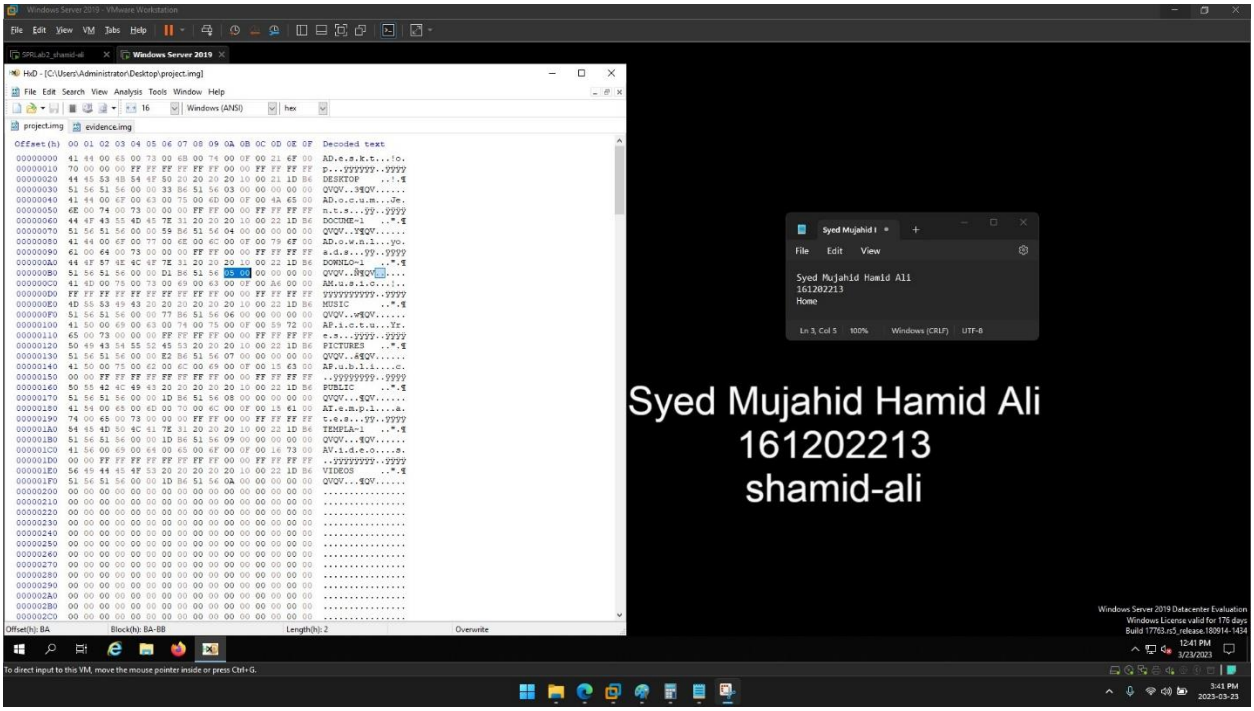
This shows the cluster when Desktop folder can be found.



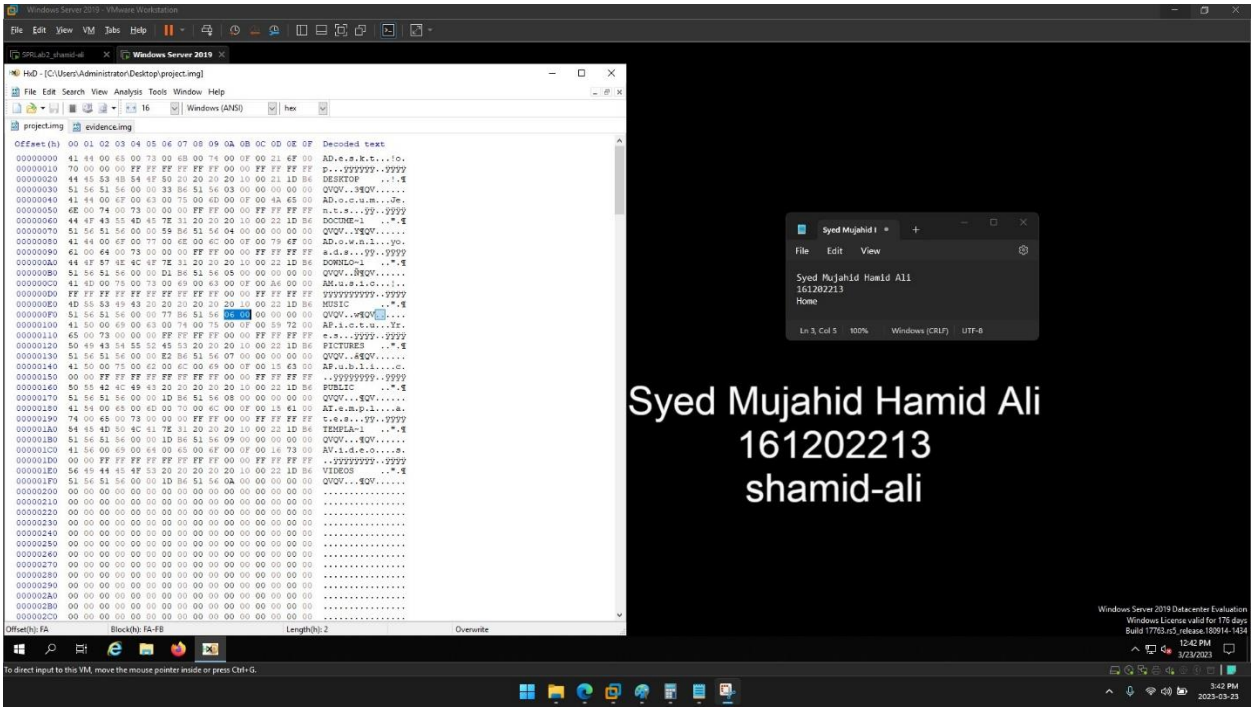
This is where Documents folder can be found.



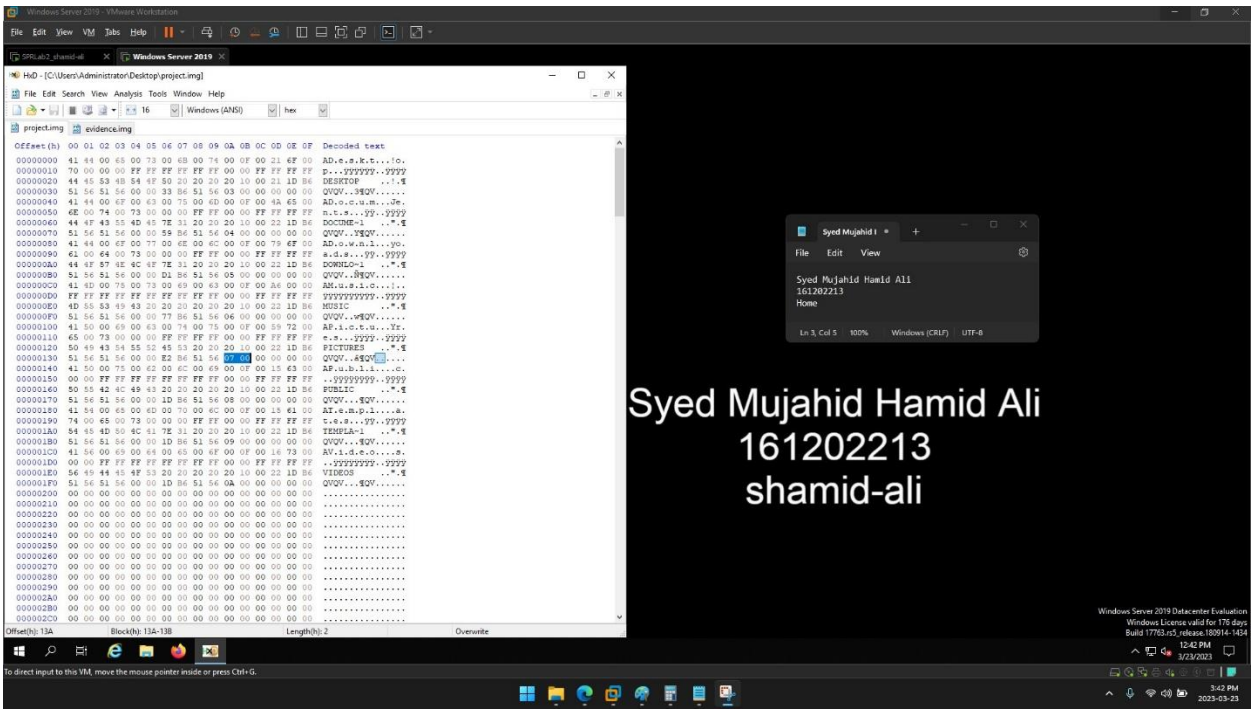
This shows where Downloads folder can be found.



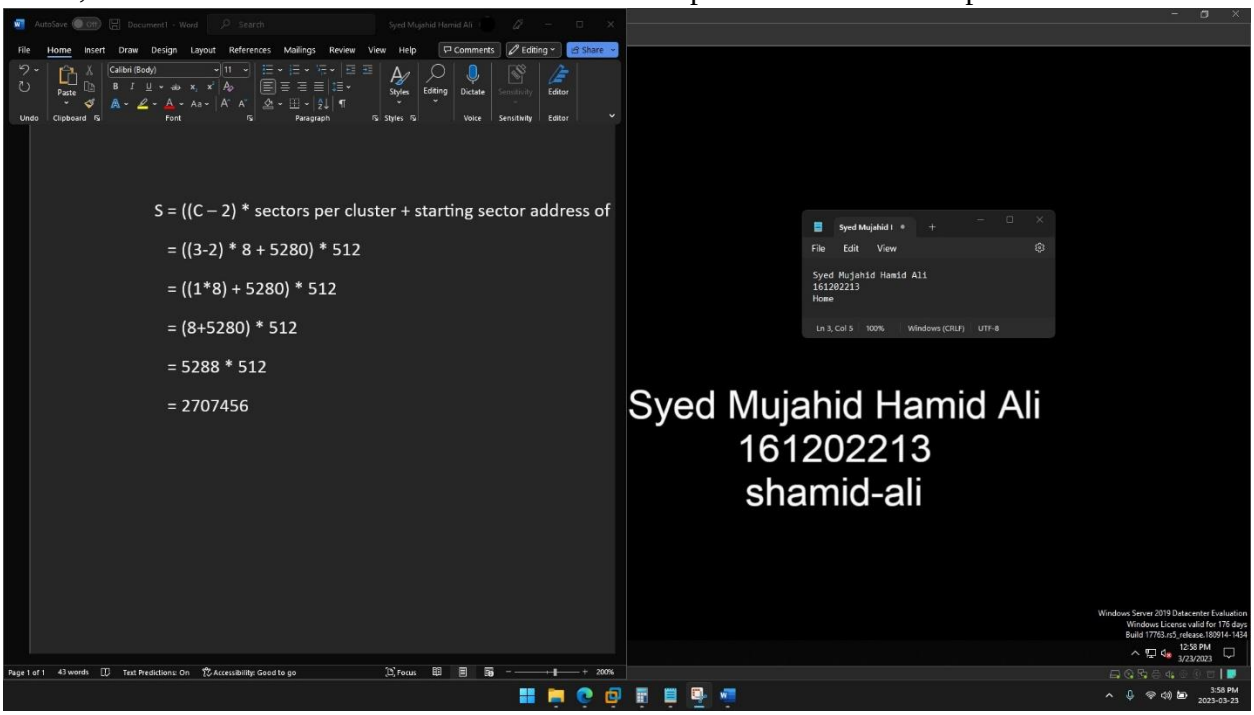
This is where Music folder can be found.

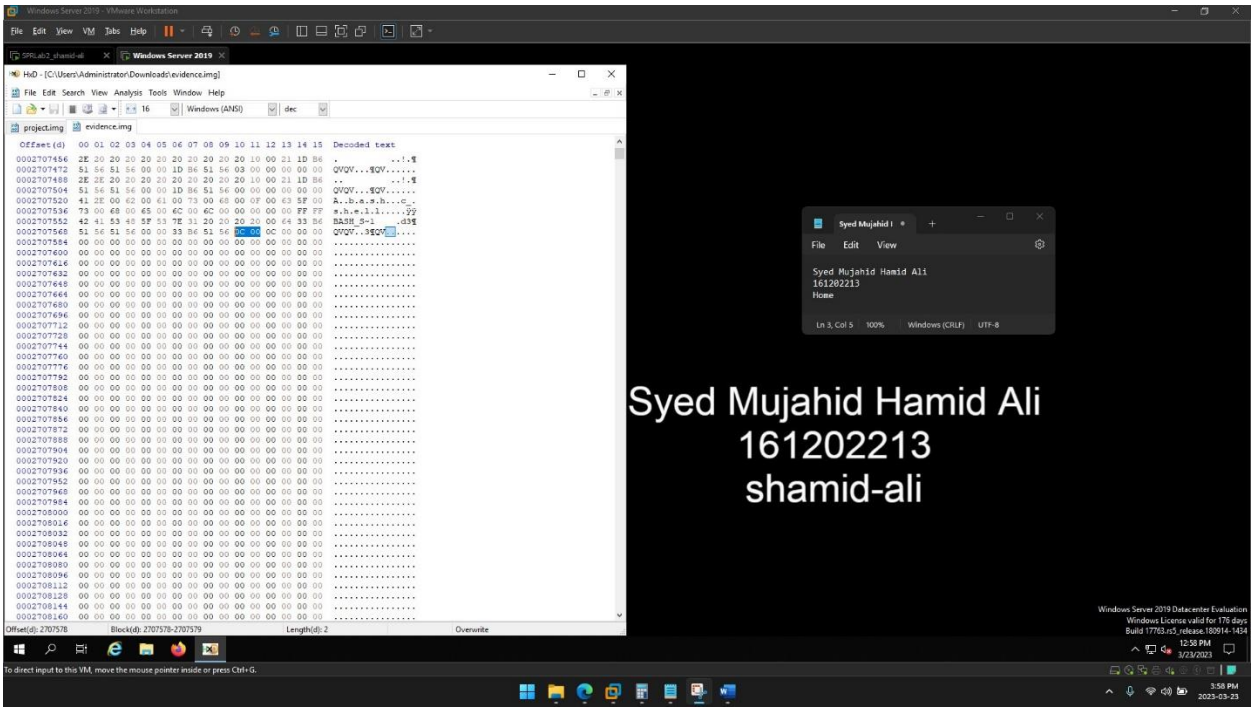


This is where Pictures folder can be found.

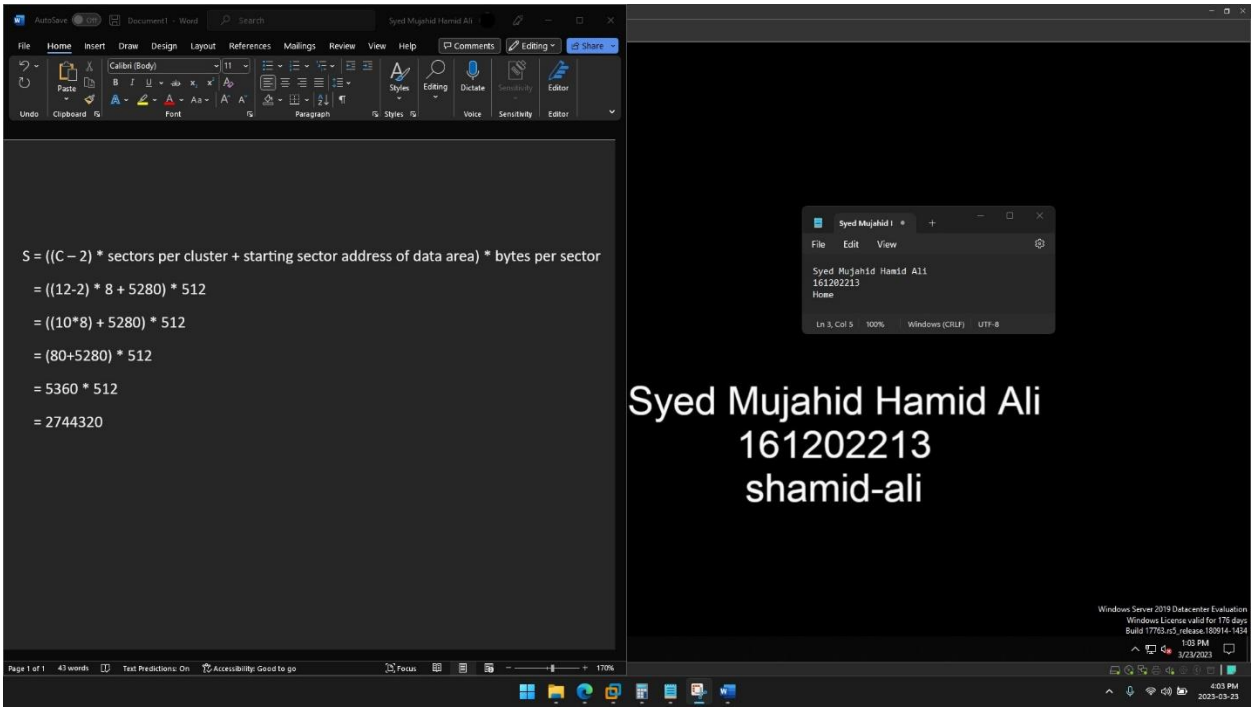


3) Now, lets analyze the Desktop folder. First we will find the root directory of the Desktop folder, which will contain information about the files present inside Desktop.

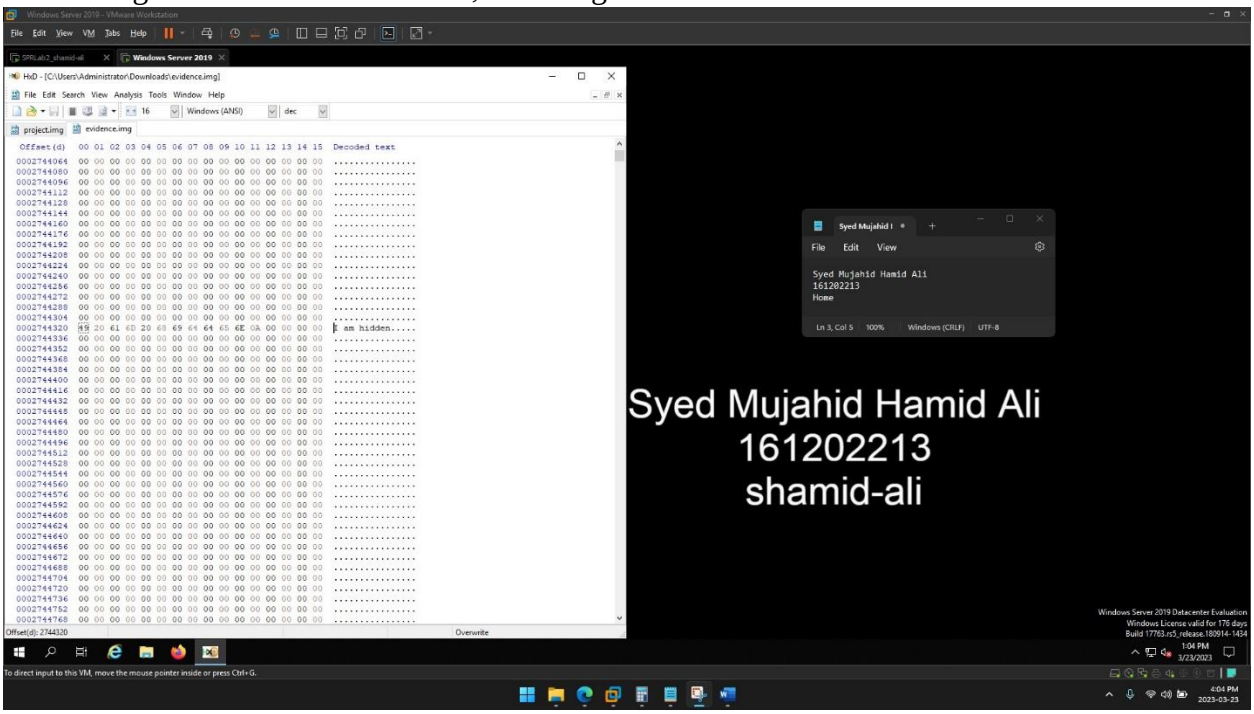




As we can see, only .bash_shell is present. We will follow the same process as above to find thee location of this file.



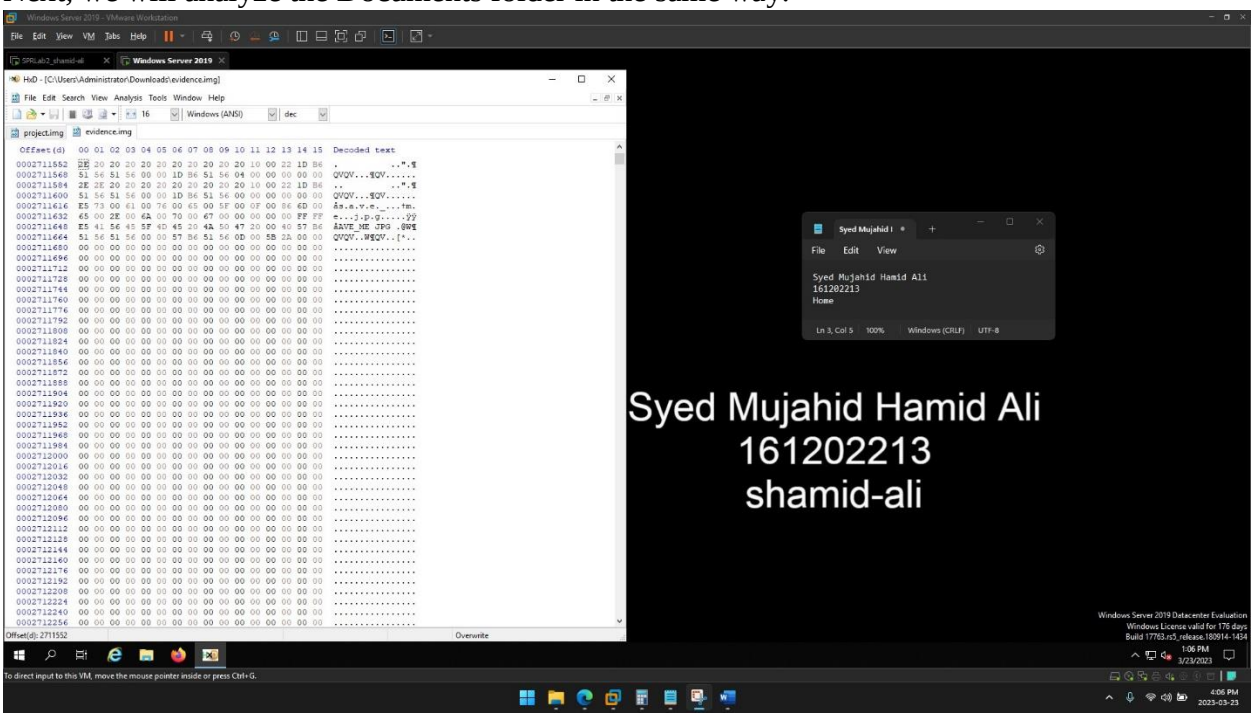
When we go to the mentioned sector, we will get the file.



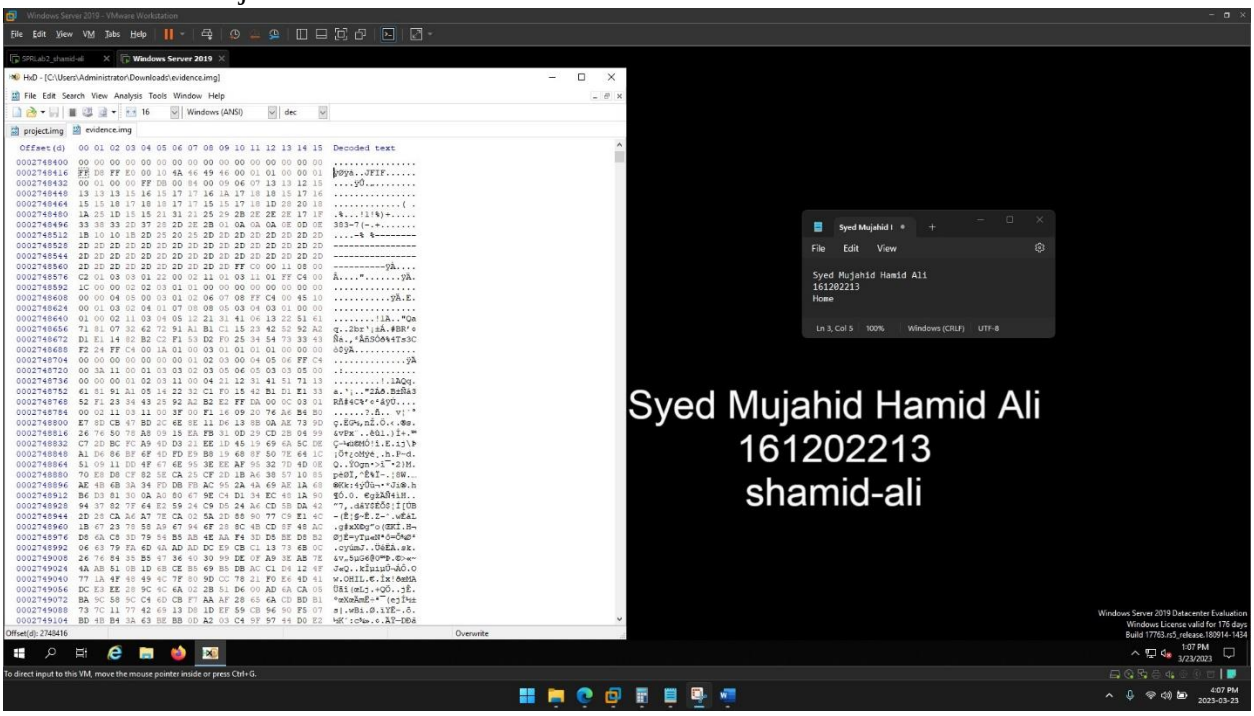
For other folders, this is a table that specifies the details that can be got from the root directory of all the files that are present in the USB.

File Name	Starting Sector	File Size (in sectors)	Ending Sector
save_me.jpg	2748416	10844	2759259
Message_from_Larry.docx	2826240	12801	2839040
Catch_me_if_you_can.docx	2760704	64728	2825431
Tulips.jpeg	2842624	2359351	5201974

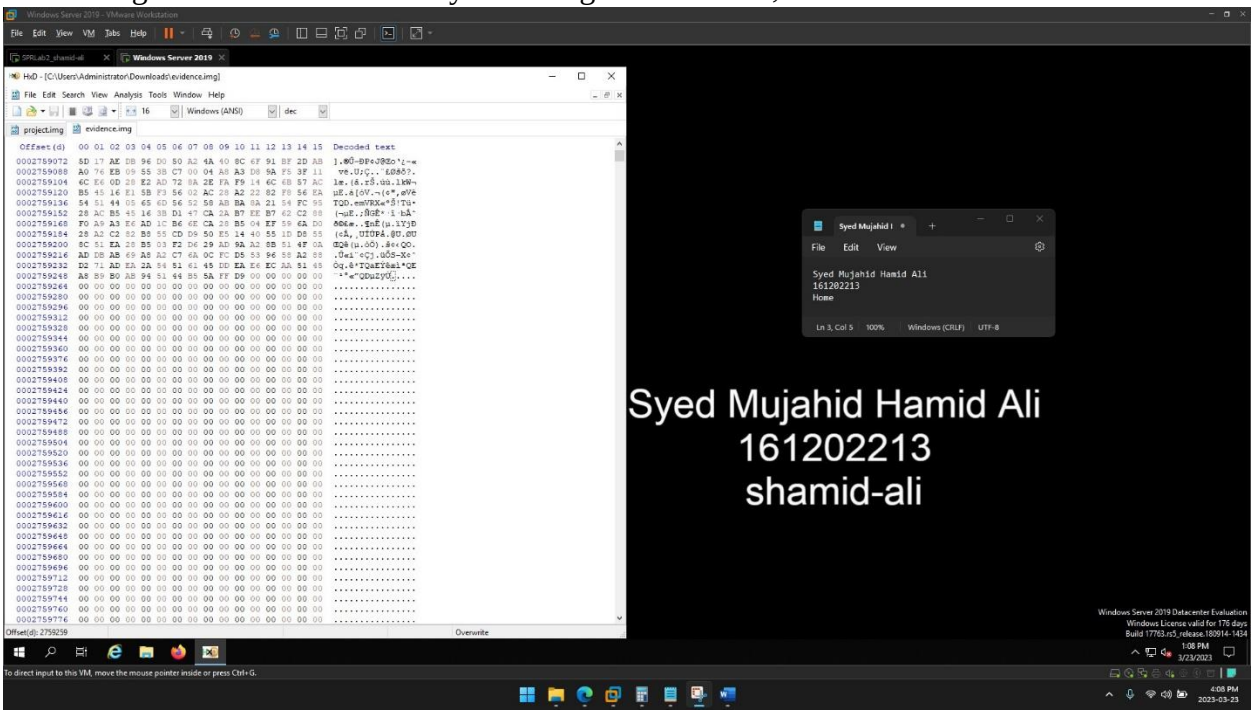
Next, we will analyze the Documents folder in the same way.



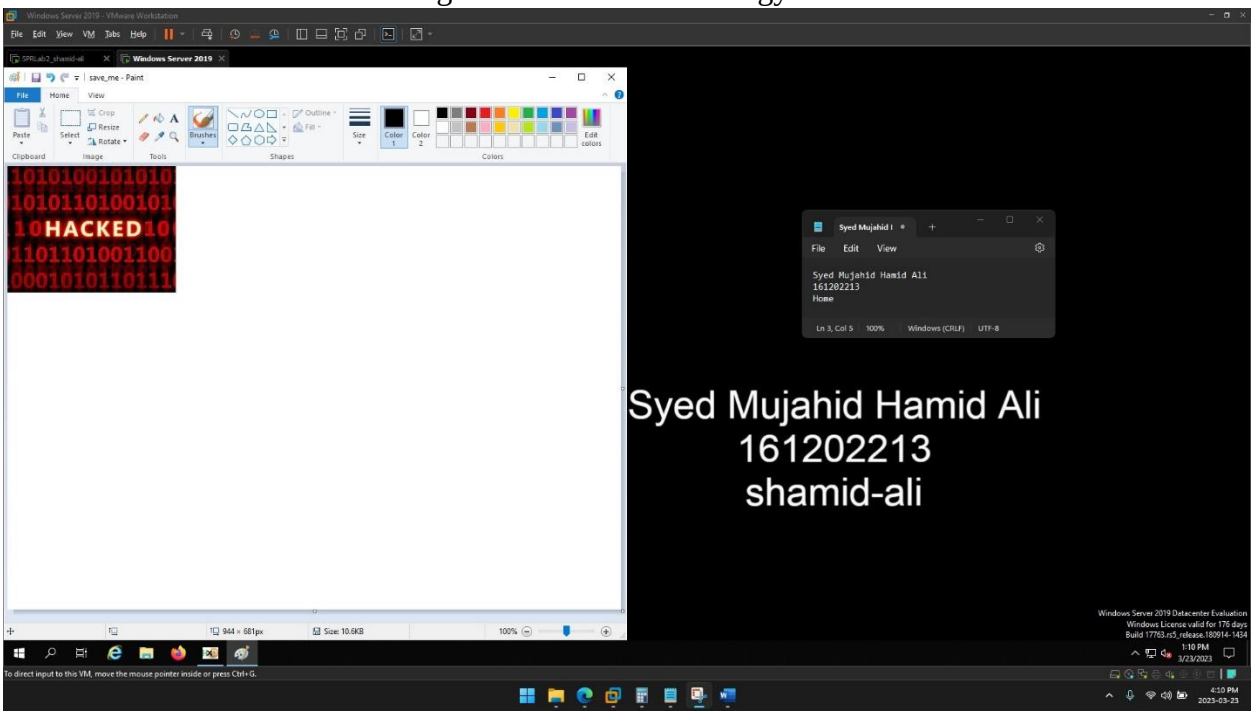
This shows that only ‘save_me.jpg’ is present. So now we can find the starting sector address of the file just like we did earlier.



The ending address can be found by searching for the trailer, which is FF D9 for this.



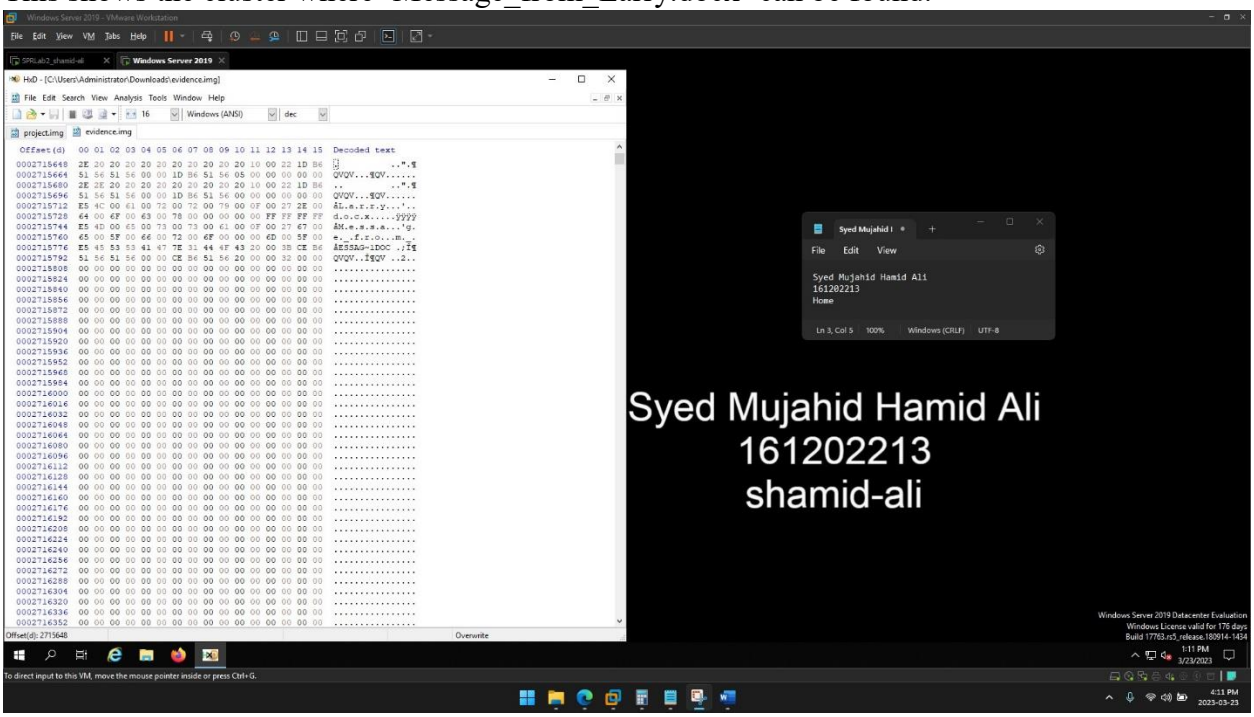
Then we can recover this file using the header-footer strategy.



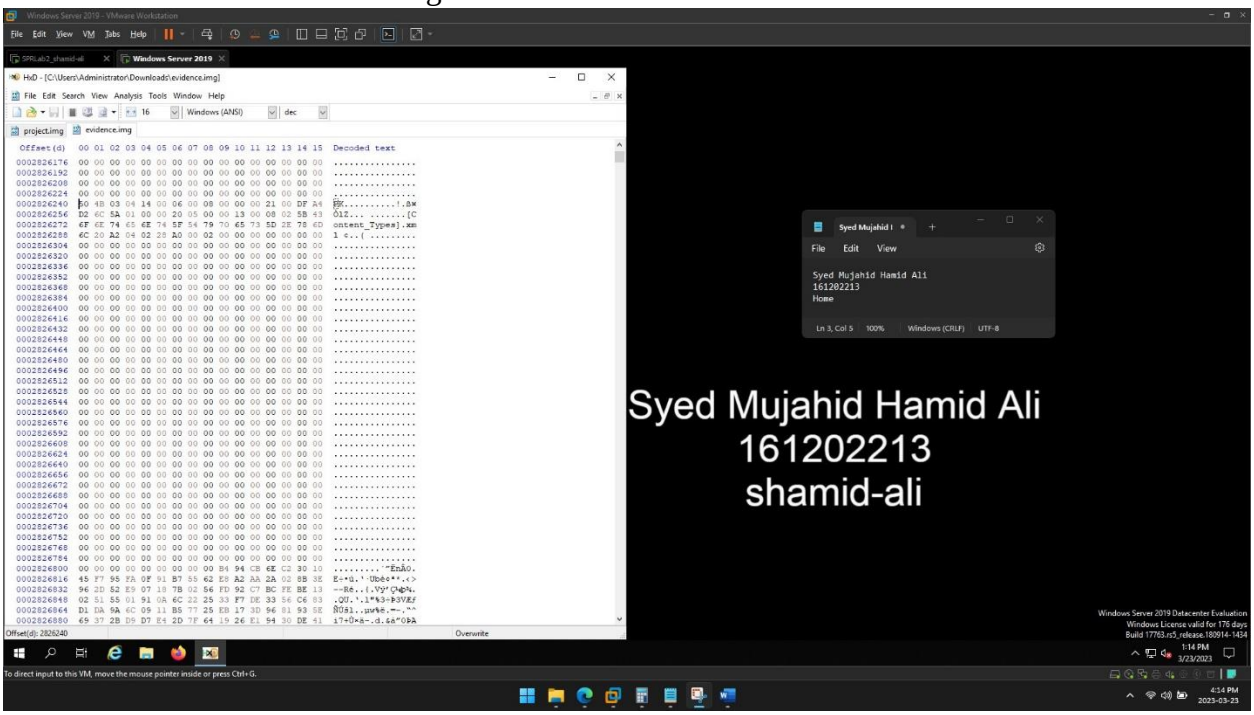
This shows the file recovered.

Next, we will analyze the Downloads folder. We can see that there is only one file present.

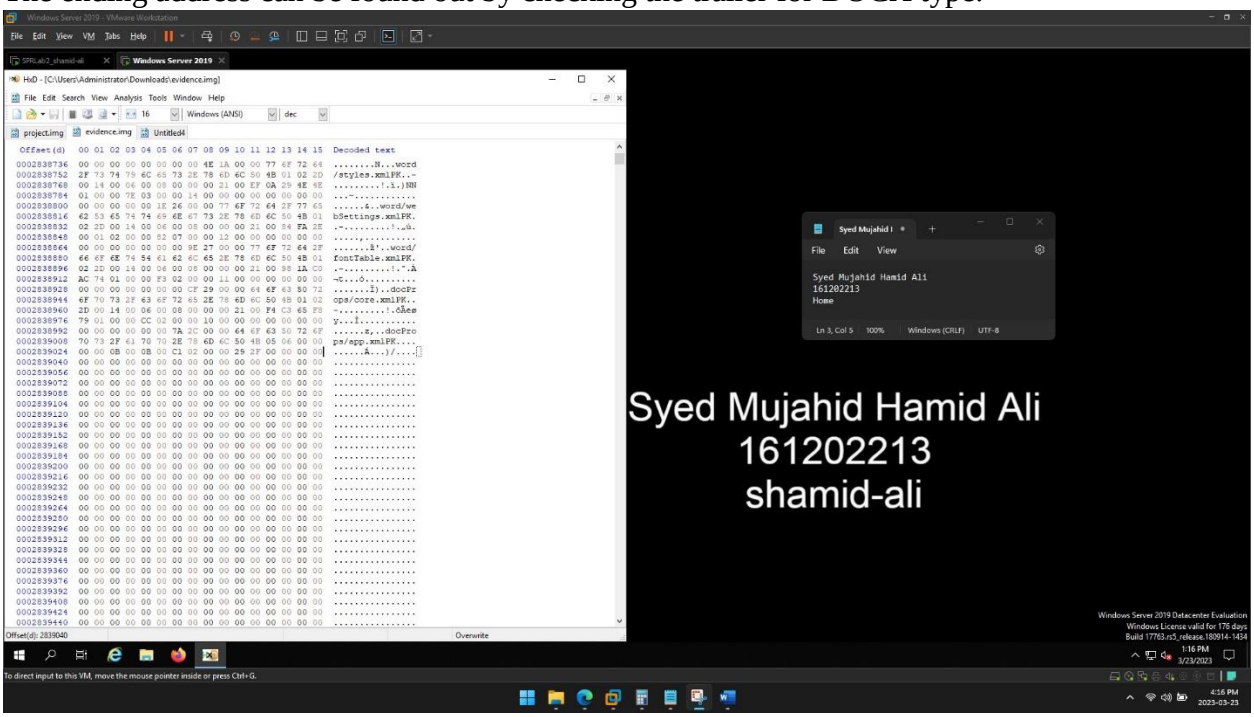
This shows the cluster where ‘Message_from_Larry.docx’ can be found.



This screenshot shows the starting sector address of the above file.

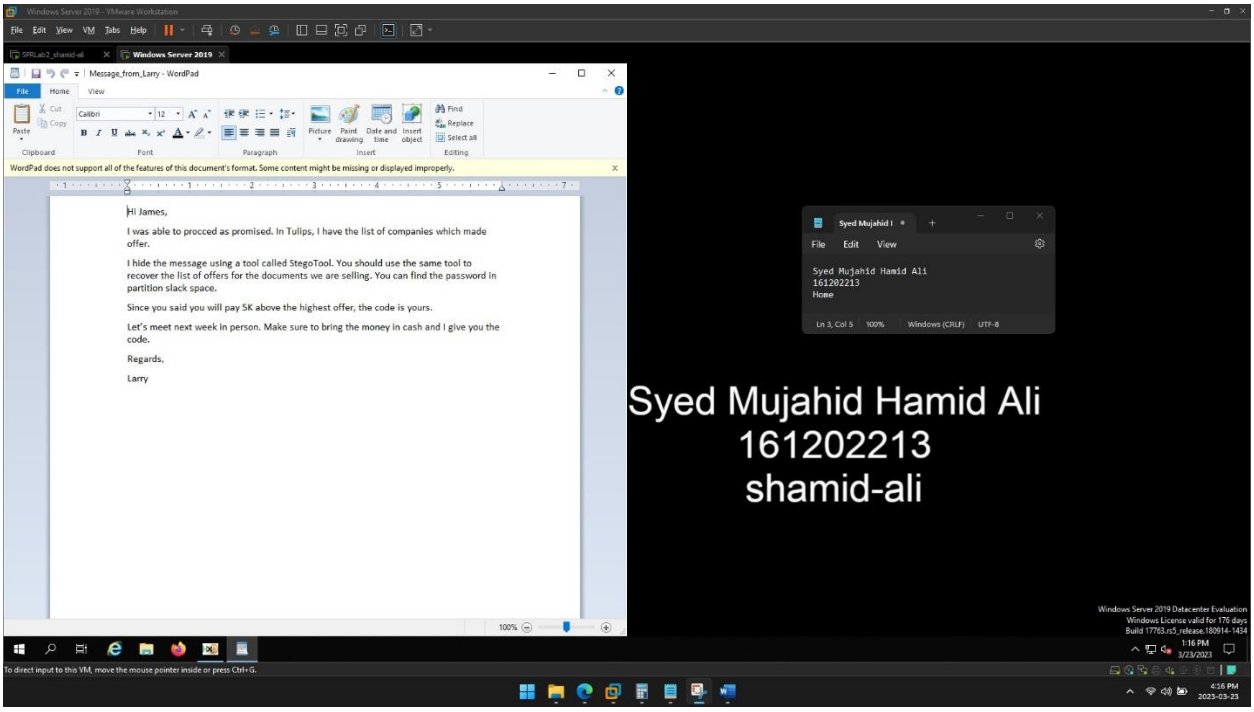


The ending address can be found out by checking the trailer for DOCX type.

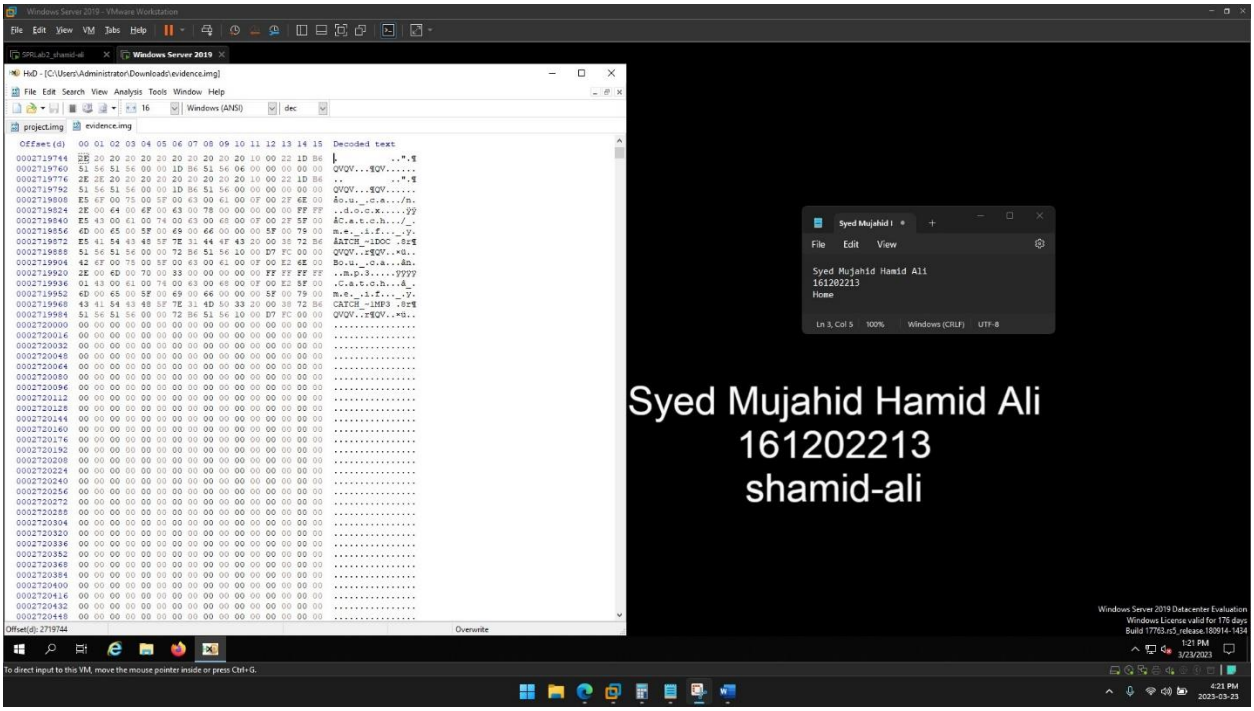


Using the header-trailer strategy, we will be able to recover the file.

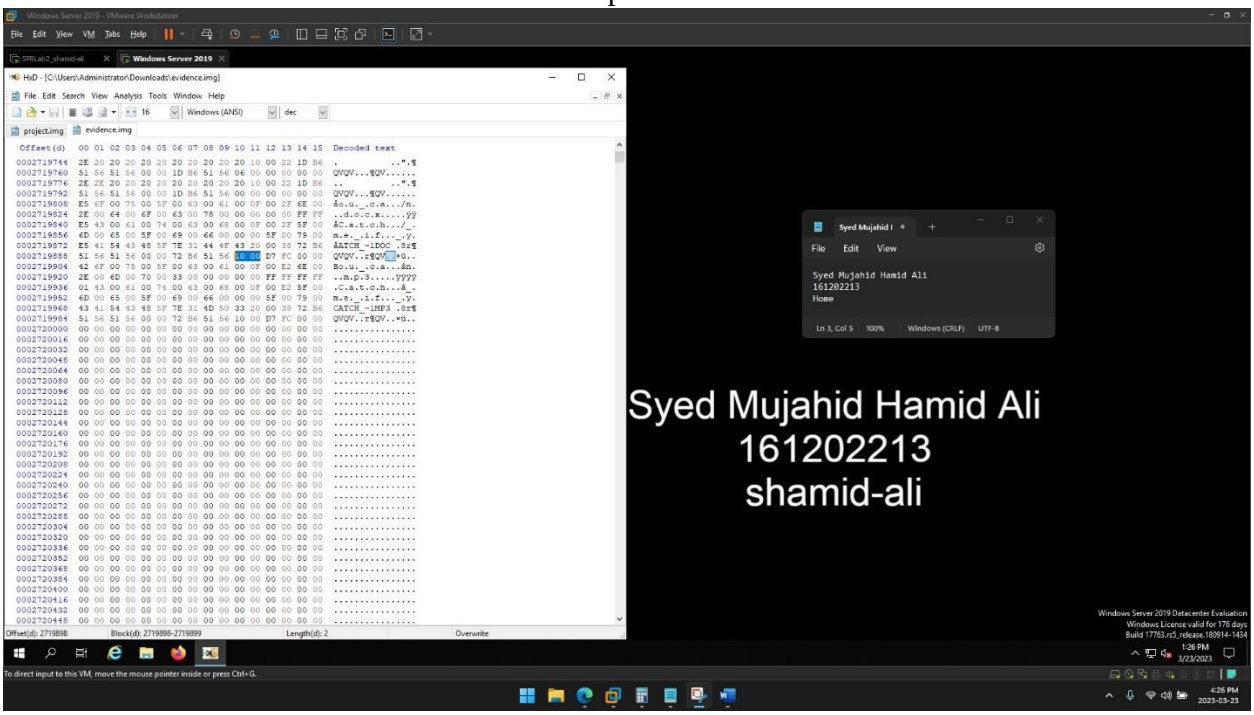
This shows the file recovered.



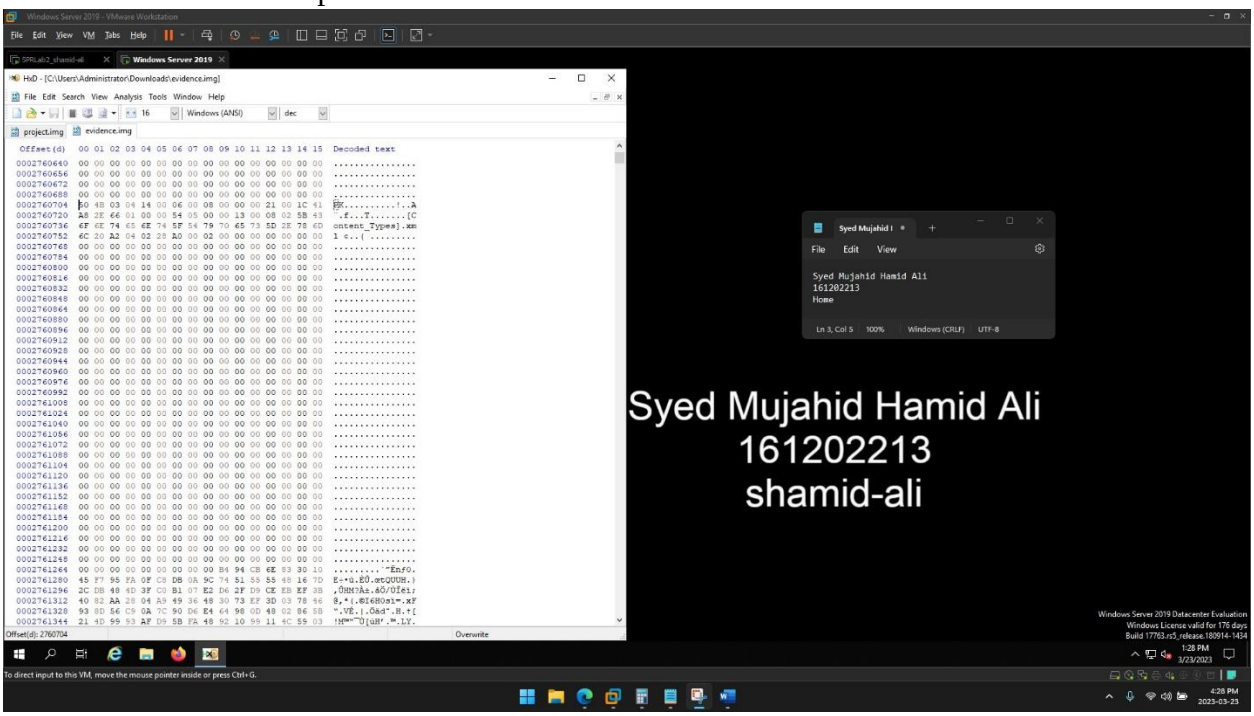
Next folder that we will analyze is Music. This shows the number of files present in the directory. We can see that there are two files present, one DOCX and one MP3 file. But if we examine closely, we see that both files point to the same sector address, saying that the file is obfuscated twice. This also means that we have only file that we can recover from this folder.



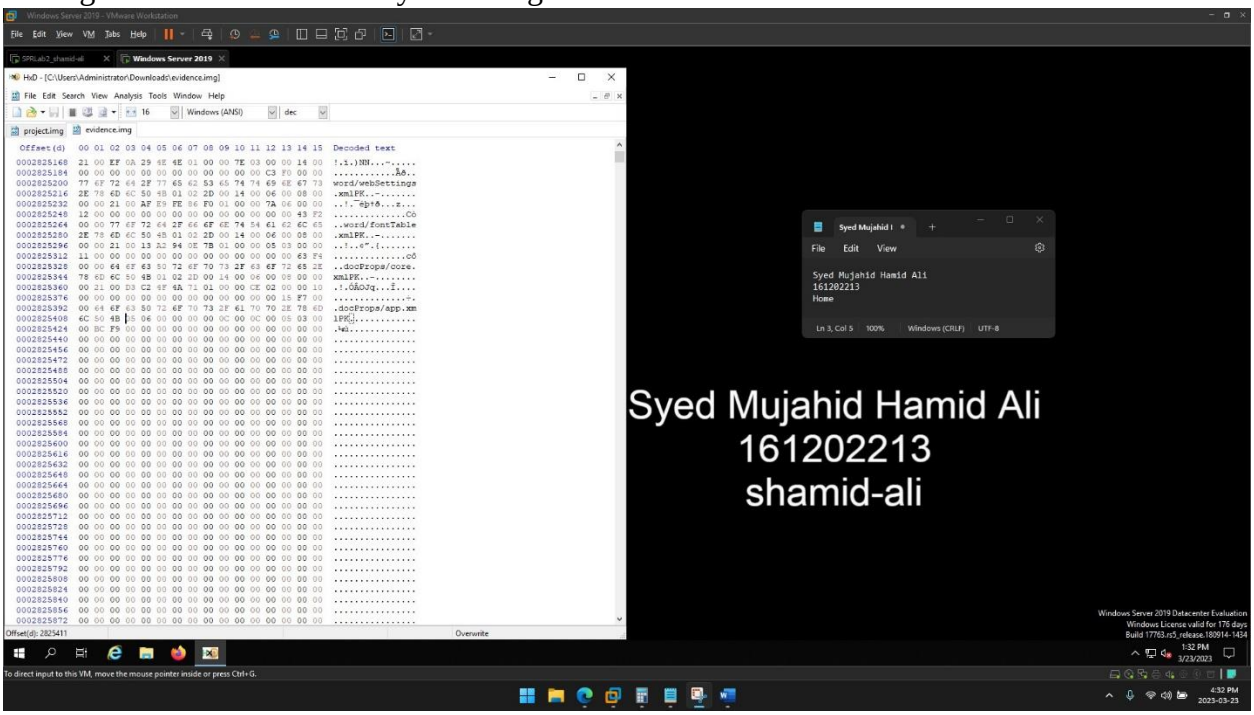
This shows the cluster where the DOCX file is present.



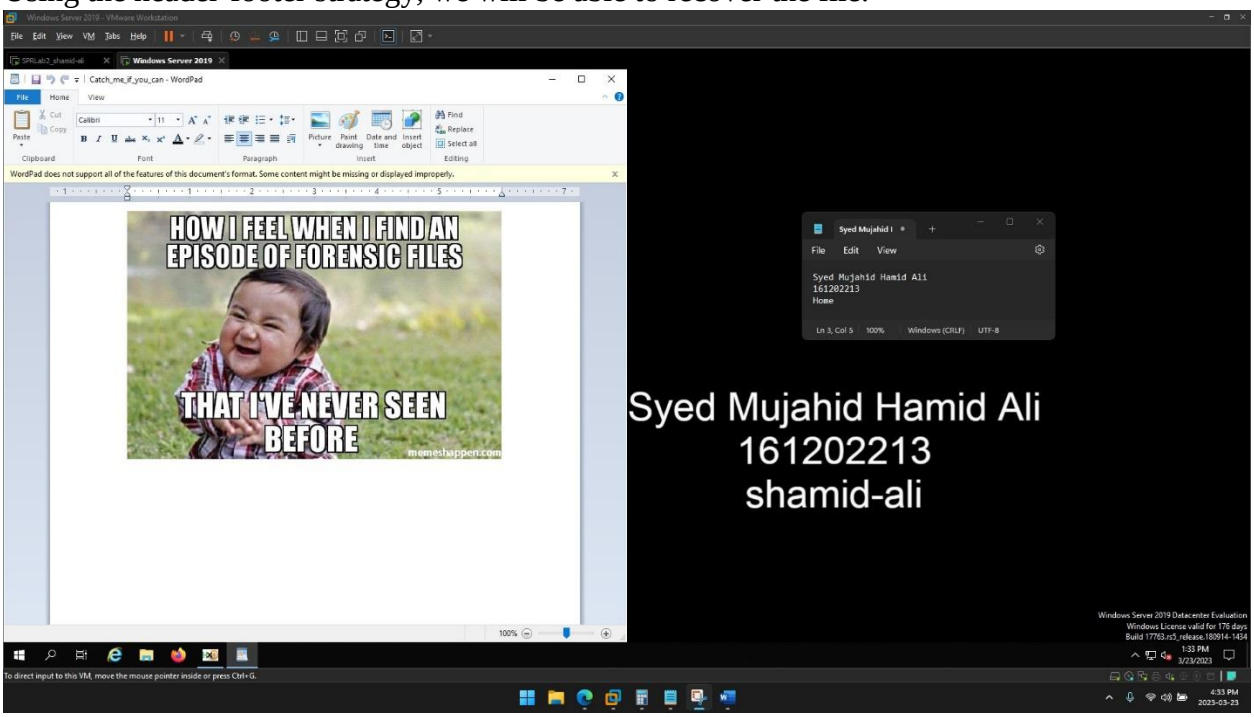
From this we will be able to get the starting address similar to the calculations done to get for the first file in this report.



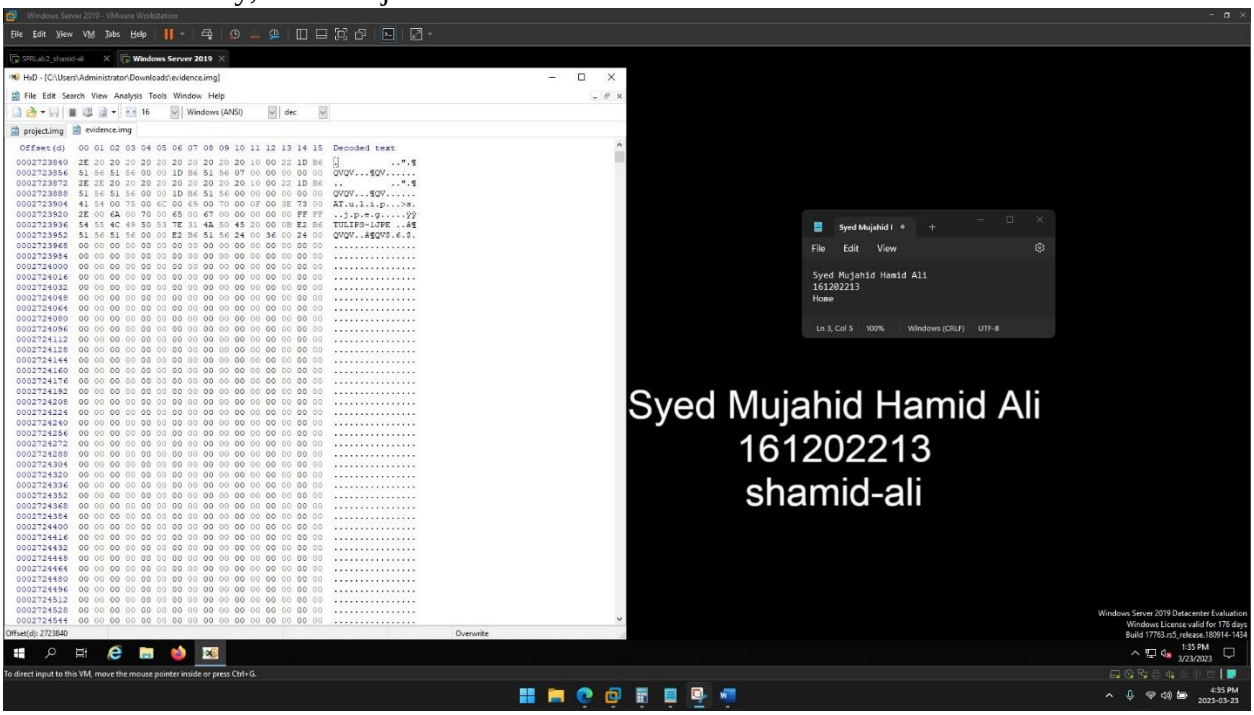
Ending address can be found by searching for the trailer of DOCX file.



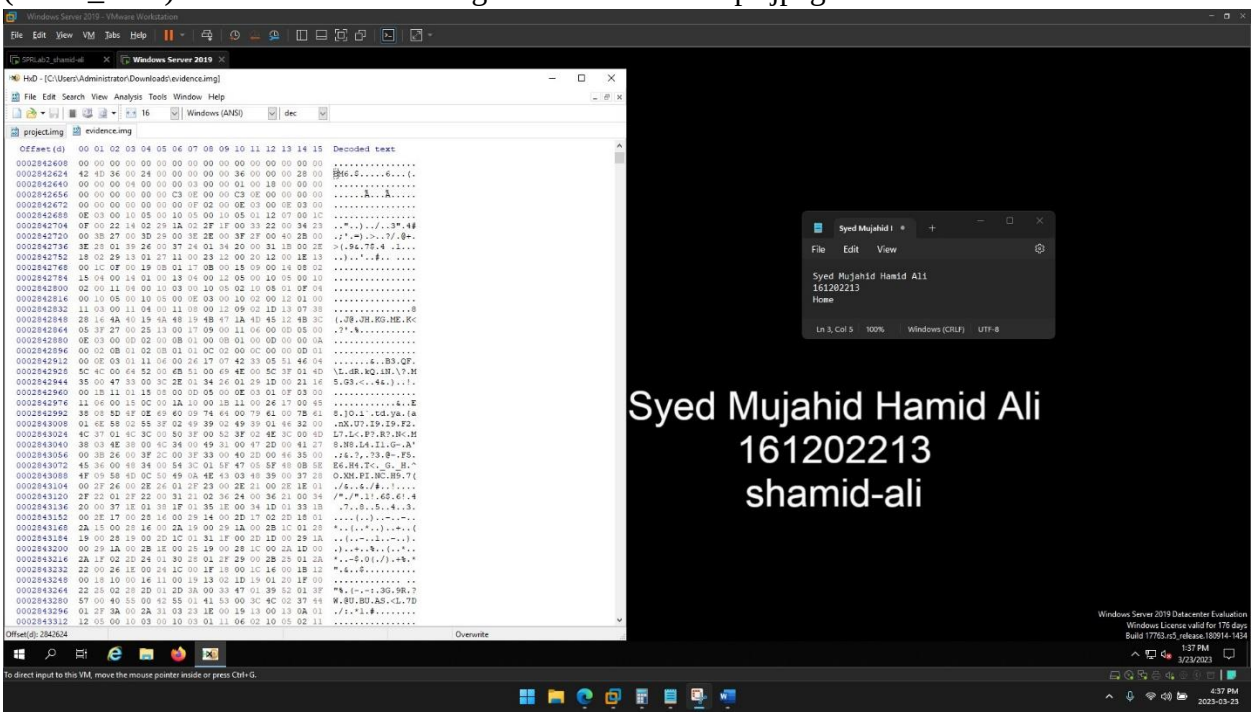
Using the header-footer strategy, we will be able to recover the file.



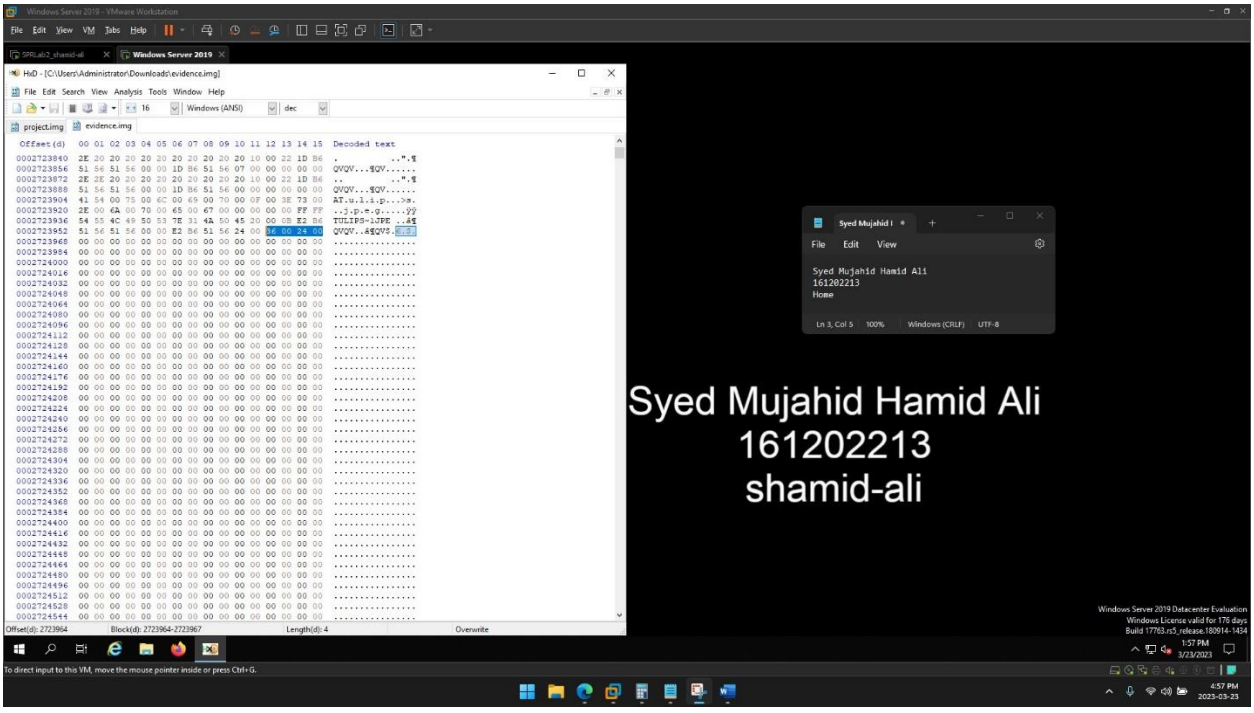
The last folder is the Pictures folder. This screenshot shows the number of files present inside the directory, which is just one.



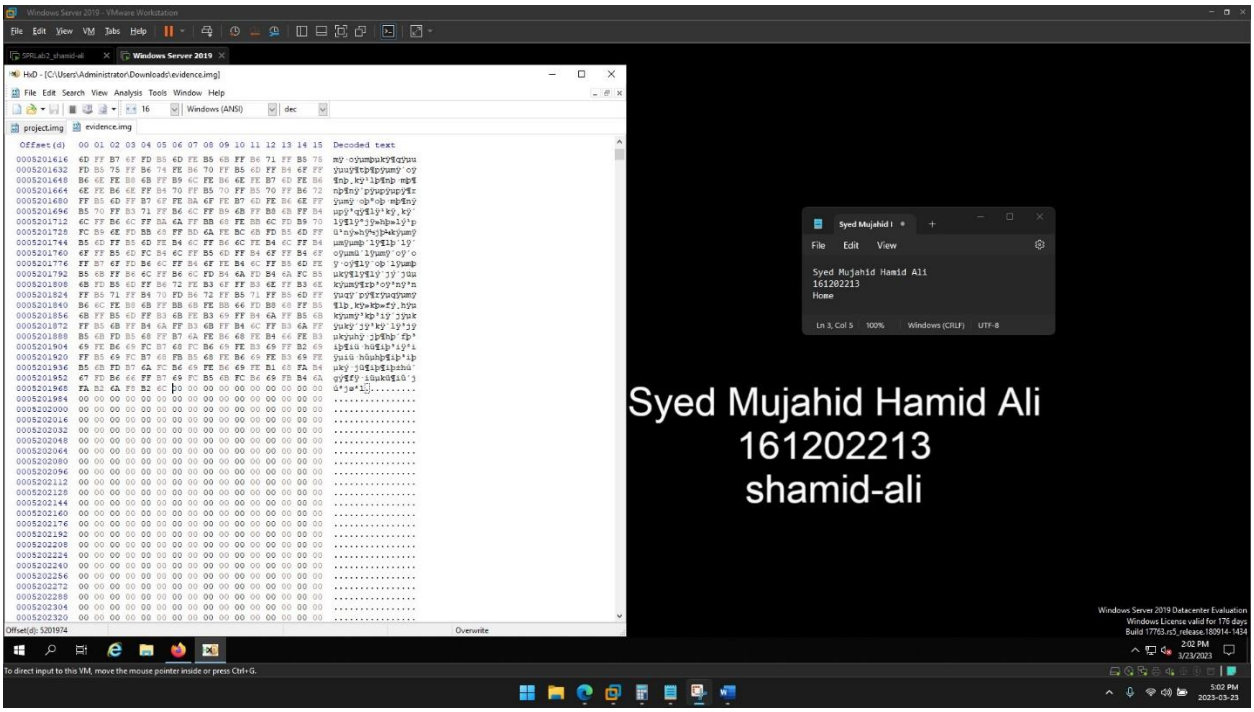
To get the starting address, we can do a similar calculation as we did for the first file (.bash_shell). This shows the starting address of the Tulips.jpeg.



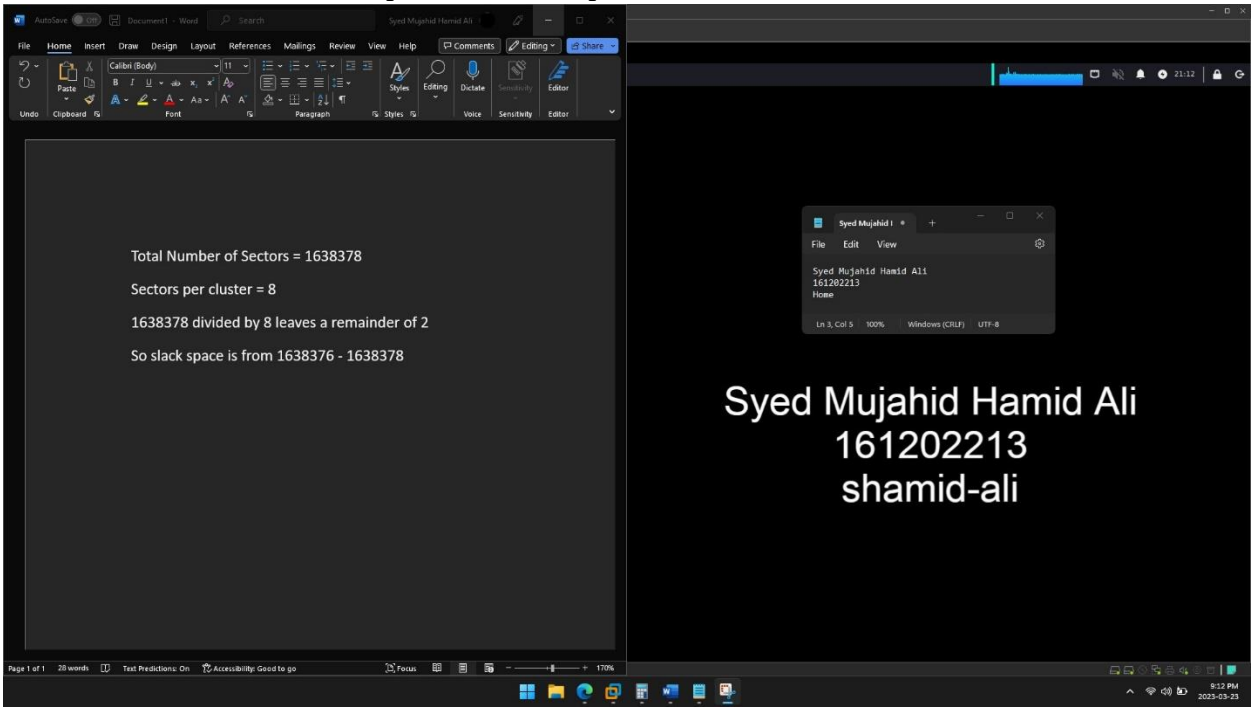
From this we can see that the file is actually a bitmap (BMP) image as the header matches for that format. But there is no specific trailer. For this, we need to find the size first.



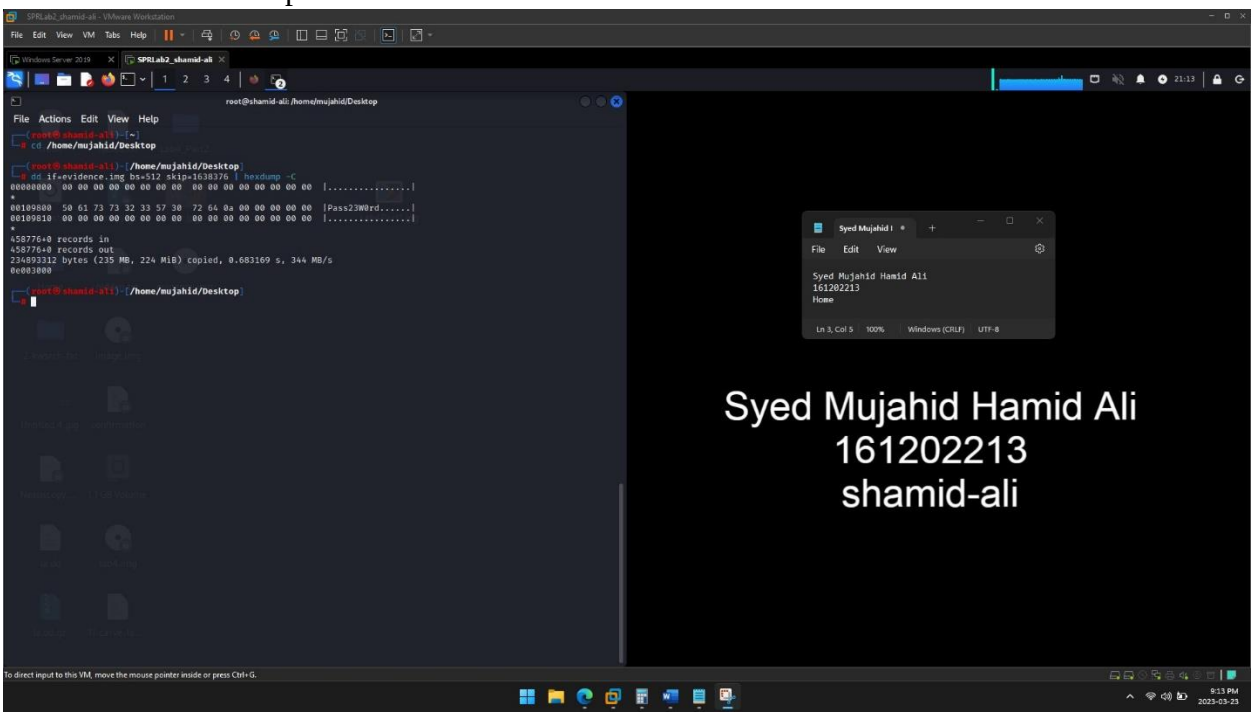
Then we will add the size to the starting address and subtract 1 from it to get the ending sector address.



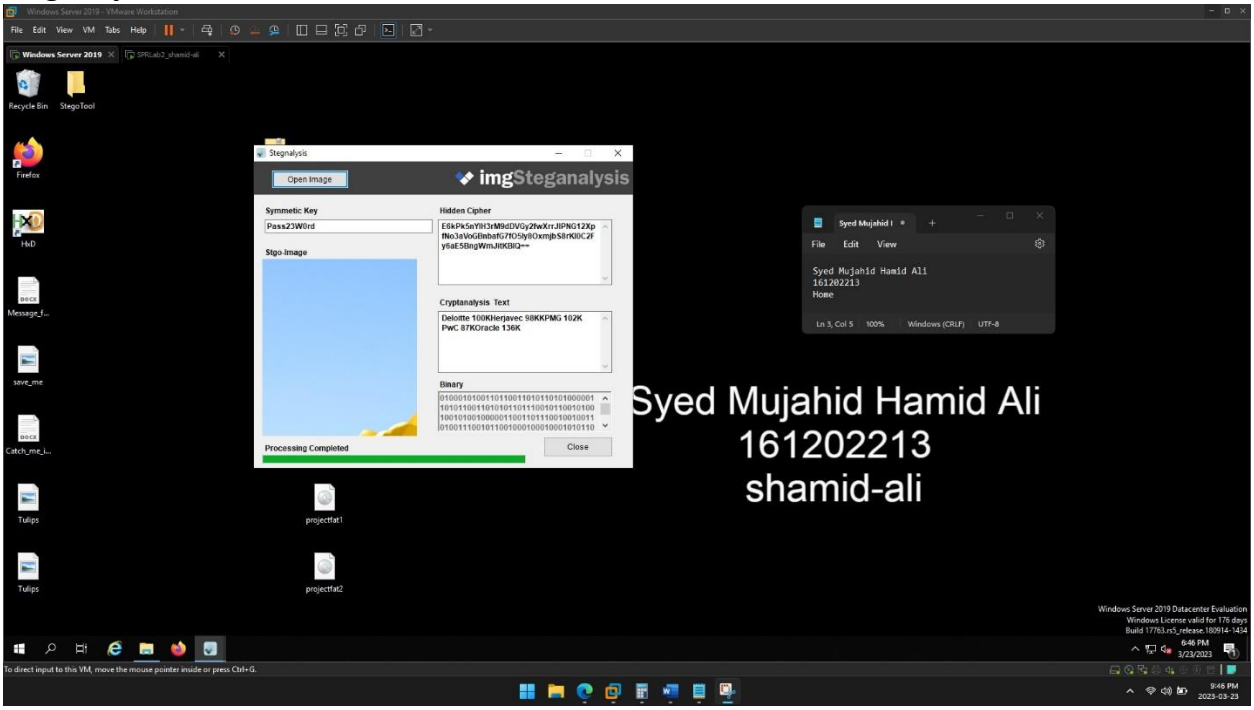
But we also know from ‘ Message_from_Larry.docx’ that this file contains a hidden message, for which we need a password that can be found in the partition slack space. This shows the calculation of partition slack space.



When we ‘dd’ the image and skip the total clusters subtracted by 2, we will get the contents of the slack space.



Then we will use ‘StegoTool’, we can get the hidden text from the image from Steganalysis.



Relevant Findings

These are all the findings that could be discovered from the above evidences.

- The other bidders and the offers that they put forward are:
  1. Deloitte 100K
  2. Herjavec 98K
  3. KPMG 102K
  4. PwC 87K
  5. Oracle 136K

- Larry sold only the application source code, as we can see that he tells James about the source code itself as he wills to pay more money.

- The first file was not masked at all. Rest all files were deleted, and in the last file a text message was hidden which told about the offers made by other companies.

- The only files that was related to the actual investigation were 'Message_from_Larry.docx' and 'Tulips.jpeg' as they told about the offer made by James and the second file showed the offers made by the other companies. Rest all files were pointless when talking about the investigation, as 'save_me.jpg' is just a generic image, 'Catch_me_if_you_can.docx' was a meme.

- As the investigator, I mainly used header-trailer carving techniques for retrieval of files. I also had to use StegoTool to find the message that was hidden in the 'Tulips.jpeg' file. Apart from that, the actual sector addresses were got from the tables giving in the textbook (namely 10.1 – 10.5).

Conclusion

We can conclude that Larry has been charged with Industrial Espionage, as he planned to sell an application source code made for his company to someone else for a price. We also know that the code was intended to be sold to James at a price of 141,000 (which is 5,000 more than what was offered by Oracle). We also know that only the application source code was sold.

Timestamps

19-03-2023

22:40 started working on the project

20-03-2023

00:40 found two jpg files and called it a day

22-03-2023

23:00 Restarted on the project

23-03-2023

01:17 Found one image and one document, called it a day

12:30 Started working on it again

22:00 Found all files and started on report making

24-03-2023

02:40 Finished the report and submitted