High-profile Kidnappings Investigation

HPKI-2024-001

May 5, 2024

Hebron City/Digital Forensics Unit

Investigators:

OldGuard

WolfEyes

KingH

PineappleFlavor

21210006@htu.edu.jo

+962 778 656 985

Table of Contents

[Table of Figures 1](#_Toc168304655)

[1. Administration information 2](#_Toc168304656)

[2. The executive summary 3](#_Toc168304657)

[3. Investigation scope 5](#_Toc168304658)

[3.1. Acquisition and handling of the evidence 5](#_Toc168304659)

[3.2. Investigation environment 10](#_Toc168304660)

[3.3. Used Tools 10](#_Toc168304661)

[4. Analysis summary 11](#_Toc168304662)

[5. Analysis 11](#_Toc168304663)

[6. Conclusion 33](#_Toc168304664)

[7. Exhibits 34](#_Toc168304665)

[***COC (Chain of Custody)*** 34](#_Toc168304666)

[***Appendix 1*** 35](#_Toc168304667)

[***Appendix 2*** 36](#_Toc168304668)

[***Appendix 3*** 36](#_Toc168304669)

[8. Revision History 37](#_Toc168304670)

# Table of Figures

[Figure 1: Device, original image. 6](#_Toc166595063)

[Figure 2: USB, original image. 6](#_Toc166595064)

[Figure 3: Device, copy image from the original image. 7](#_Toc166595065)

[Figure 4: USB, COPY IMAGE FROM THE ORIGINAL IMAGE. 8](#_Toc166595066)

[Figure 5: Device, E01 copy image from the original image. 9](#_Toc166595067)

[Figure 6: USB, E01 copy image from the original image. 9](#_Toc166595068)

[Figure 7: The file content of the Device evidence image. 11](#_Toc166595069)

[Figure 8: The file content of the USB evidence image. 12](#_Toc166595070)

[Figure 9: The extracted files from the device image drive. 12](#_Toc166595071)

[Figure 10: The content of jump list files in the EaglesEye device. 13](#_Toc166595072)

[Figure 11: Automatic Link File content. 13](#_Toc166595073)

[Figure 12: QuickAccess link file content. 14](#_Toc166595074)

[Figure 13: Windows wordpad jump link file content. 15](#_Toc166595075)

[Figure 14: Photos Microsoft link file content. 15](#_Toc166595076)

[Figure 15: Microsoft edge link file content. 17](#_Toc166595077)

[Figure 16: Unknown name line file content. 19](#_Toc166595078)

[Figure 17: Windows Explorer link file content. 20](#_Toc166595079)

[Figure 18: Custom Link Files Content. 20](#_Toc166595080)

[Figure 19: The content of prefetch files in the EaglesEye device. 21](#_Toc166595081)

[Figure 20: viewing the prefetch files in the WinPrefetchView. 22](#_Toc166595082)

[Figure 21: prefetch files for specific volume. 22](#_Toc166595083)

[Figure 22: prefetch files for specific volume. 22](#_Toc166595084)

[Figure 23: google chrome prefetch files. 23](#_Toc166595085)

[Figure 24: google chrome prefetch file times stamps and target paths. 23](#_Toc166595086)

[Figure 25: the target googles chrome file path with time stamps. 24](#_Toc166595087)

[Figure 26: Recycle.Bin Folder Content. 24](#_Toc166595088)

[Figure 27: Library's Folder Content. 25](#_Toc166595089)

[Figure 28: Desktop Content. 26](#_Toc166595090)

[Figure 29: HT Folder Content. 26](#_Toc166595091)

[Figure 30: Self Study Folder Content. 27](#_Toc166595092)

[Figure 31: Content of the ZIP folder. 27](#_Toc166595093)

[Figure 32: Content of the ZIP Folder. 27](#_Toc166595094)

[Figure 33: Downloads Folder Content. 28](#_Toc166595095)

[Figure 34: Footer Signatures Searching Results. 29](#_Toc166595096)

[Figure 35: Extracted Docx File. 29](#_Toc166595097)

[Figure 36: Opened Docx. 30](#_Toc166595098)

[Figure 37: Docx After Coloring all the Content. 30](#_Toc166595099)

[Figure 38: USB MBR Entries Table. 31](#_Toc166595100)

[Figure 39: VBR Sector. 31](#_Toc166595101)

[Figure 40: Backup VBR in Last Sector. 32](#_Toc166595102)

[Figure 41: Pasting VBR. 33](#_Toc166595103)

[Figure 42: Recovered USB. 33](#_Toc166595104)

# 1. Administration information

Case number/case name: HPKI-2024-001 / High-profile Kidnappings Investigation

Department/organization requested the report: Metropolitan Police Department

Search warrants/authorization for the investigation of the evidence

On May 5, 2024, a search warrant (Warrant ID: DF-2024-105663) was issued by Honorable Osama AL-Risheq of the District Court for the jurisdiction of Metropolitan, authorizing the Digital Forensics Unit to conduct an investigation into the High-profile Kidnappings crime described in Case HPKI-2024-001. This warrant granted permission to seize and examine digital evidence related to the case, including but not limited to electronic devices, storage media, and any relevant documentation.

The search warrant was obtained based on probable cause of a recent series of high-profile kidnappings has put a pall over our capital city. It all started with the kidnapping of the CEO's daughter at our largest investment firm, which triggered a chain of events planned by the legendary criminal group known as BlackEagle. Their demand for a $1 million ransom for her release established a dangerous precedent, with other victims facing identical demands in exchange for their freedom. Despite law enforcement efforts, the BlackEagle's taunts and challenges simply became louder, implying even more daring acts in the future.

The Metropolitan Police Department caught an important part of the BlackEagle organisation and began interrogation procedures. However, initial interrogation revealed little about the schedule or location of their next operation. However, the suspect's device and USB drive were confiscated. Images of these things were extracted using the expertise of a digital forensics’ specialist, opening up new avenues of investigation.

Authorized personnel from the Digital Forensics Unit, including OldGuard, WolfEyes, KingH, and PineappleFlavor, were empowered to execute the search warrant in accordance with the law and departmental procedures. All actions conducted during the investigation were carried out in adherence to the terms outlined in the search warrant and applicable legal statutes.

The execution of the search warrant was documented and recorded in compliance with legal requirements, and the seized evidence was handled and preserved in accordance with chain of custody protocols to maintain its integrity for potential use in legal proceedings.

Investigators:

* OldGuard.
* WolfEyes.
* KingH.
* PineappleFlavor.

Victims: Not determined yet

Suspects: Black Eagle crime group

Interrogated or reviewed people: Eagle’s Eye (nickname, real name not yet determined)

# 2. The executive summary

The Digital Forensics Unit launched the investigation in response to an alarming increase in high-profile kidnappings in the capital city based on the asking of the capital city policy, all of which were linked to the known criminal group "BlackEagle." Given the complexity and challenges presented by situations like this, the investigation found a combination of barriers and alternatives.

The arrest of an important member of the Black Eagle group gave a critical opportunity for the police. The device gave investigators access to critical digital evidence that was previously unavailable to them. The recovered device and USB drive became a focus for digital forensic investigation, potentially revealing a wealth of information about the criminal group's inner workings and future goals.

This report provides a complete description of the findings obtained from the meticulous investigation of the confiscated digital assets. Its major goal is to find detailed facts that will shed light on the timing and location of the BlackEagle group's future crime activities.

Key findings:

* The identification of "BlackEagle" as the main criminal behind a number of high-profile kidnappings in the capital city is a significant step forward in the investigation.
* The Metropolitan Police successfully arrested a major member of the BlackEagle group, allowing access to important digital material critical to the case's progression.
* A thorough examination of the collected electronic equipment, including the suspect's device and USB drive, revealed a detailed trail of communication, time, and location that were directly related to the BlackEagle group's next crime activity.
* After initial challenges, the digital forensic investigation produced strong clues about the possible timing and location of BlackEagle's upcoming criminal activities, providing vital insights for law enforcement strategies and operational preparation.
* The forensic investigation of the digital evidence uncovered a wealth of incriminating information, including:
  + The location of the next crime which is KHBP (King Hussien Business Park).
  + The time for the next crime is Tuesday 11/06/2024 at 12 PM.

Recommendations:

* Document all steps taken during the investigation and imaging process, including timestamps, personnel involved, and any observations made regarding the condition of the evidence. This documentation is essential for maintaining a clear chain of custody and ensuring the admissibility of the evidence in legal proceedings.
* Store the forensic images and original evidence in secure, controlled environments with restricted access to authorized personnel only. Implement robust security measures, such as encryption and access controls, to prevent unauthorized tampering or compromise of the evidence.
* After creating the forensic images, perform verification checks to ensure their integrity and accuracy. Utilize checksum algorithms or digital signatures to verify that the images are exact replicas of the original storage media, mitigating the risk of data corruption or alteration.
* Establish backup procedures for the forensic images to safeguard against potential data loss or corruption. Store redundant copies of the images in geographically dispersed locations or on secure cloud storage platforms to ensure their availability in the event of hardware failure or unforeseen emergencies.
* Preserve the digital evidence in its current state for further analysis or legal proceedings.
* Urgently create images of all drives and evidence we possess, as we remain uncertain whether the virus still persists or if it is concealed elsewhere.

# 3. Investigation scope

Resources to complete the investigation:

Physically:

* Device (24 GB)
* USB drive (200 MB).

## 3.1. Acquisition and handling of the evidence

The investigation team initiated an investigation upon receipt of a device and USB drive. The evidence, securely contained within a closed black one-time open policy box, was delivered to investigation team Labs at 9:11 a.m. (MST) on May 8, 2024, by a team of 10 policy officers.

The evidence package included a device and USB drive with corrupted USB unknown file system partition. The investigation team utilized FTKImager to create a raw DD image and E01 image of the evidence, ensuring the preservation of its integrity. Subsequent investigations and analysis were conducted solely on this working copy forensic image to maintain the original media's integrity.

The received device information:

|  |  |  |  |
| --- | --- | --- | --- |
| ***Device Model*** | ***Device Serial Number*** | ***Description*** | ***Capacity*** |
| “Kingston” flash drive | 0VSKP1808332 | Silver metal USB drive (flash) USB 3.0 | 200 MB |
| “Asus” Device with windows Operating System. | 85966314H5HSH | Black metal device Asus’s type | 24 GB |

The calculated hash of the original image device in Figure 1.

A screenshot of a computer

Description automatically generated

Figure 1: Device, original image.

The calculated hash of the original USB in Figure 2.

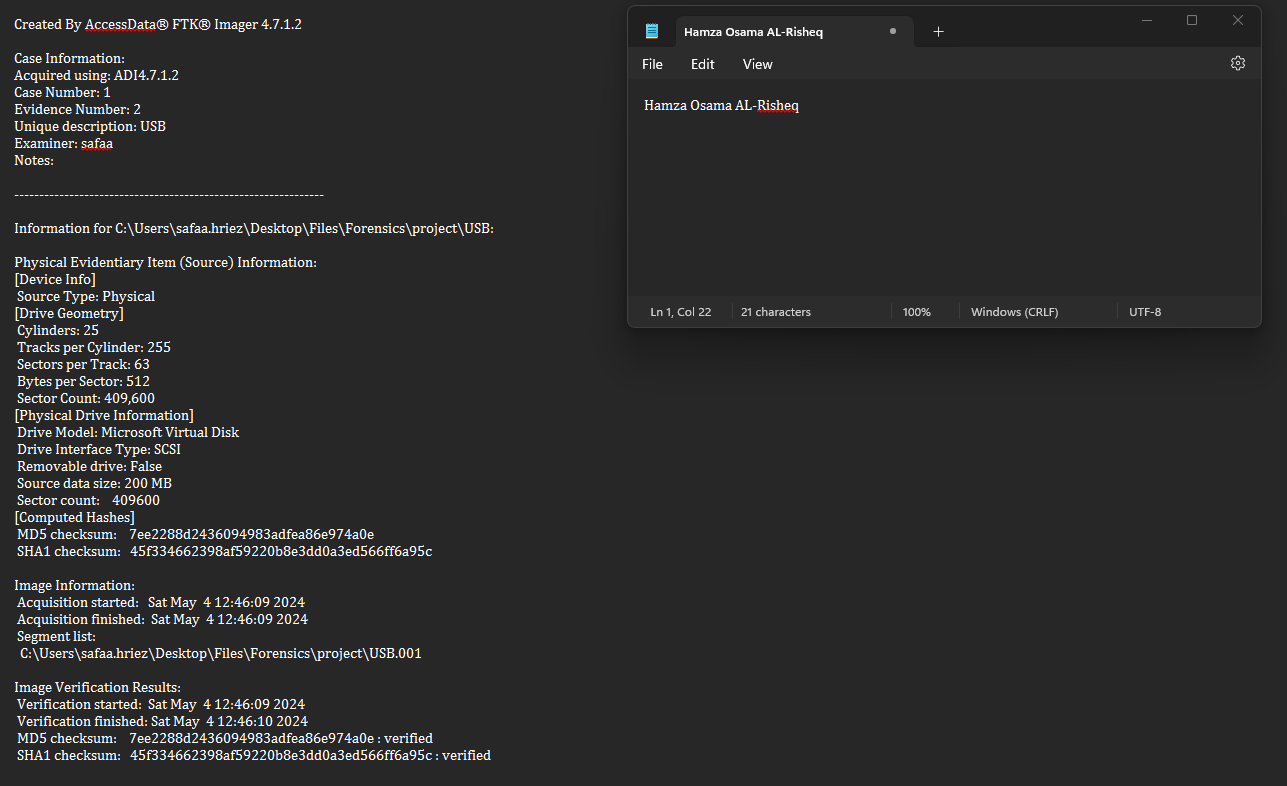


Figure 2: USB, original image.

Using the FTK Imager tool, I created a logical image (RAW DD) from the device and USB obtained. In Figure 3 and Figure 4, the metadata of the image is visible.

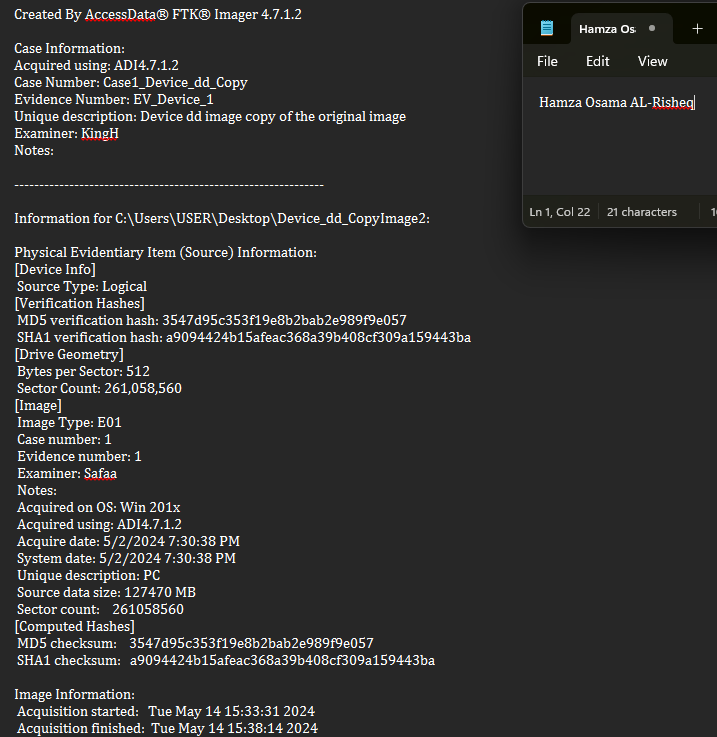


Figure 3: Device, copy image from the original image.

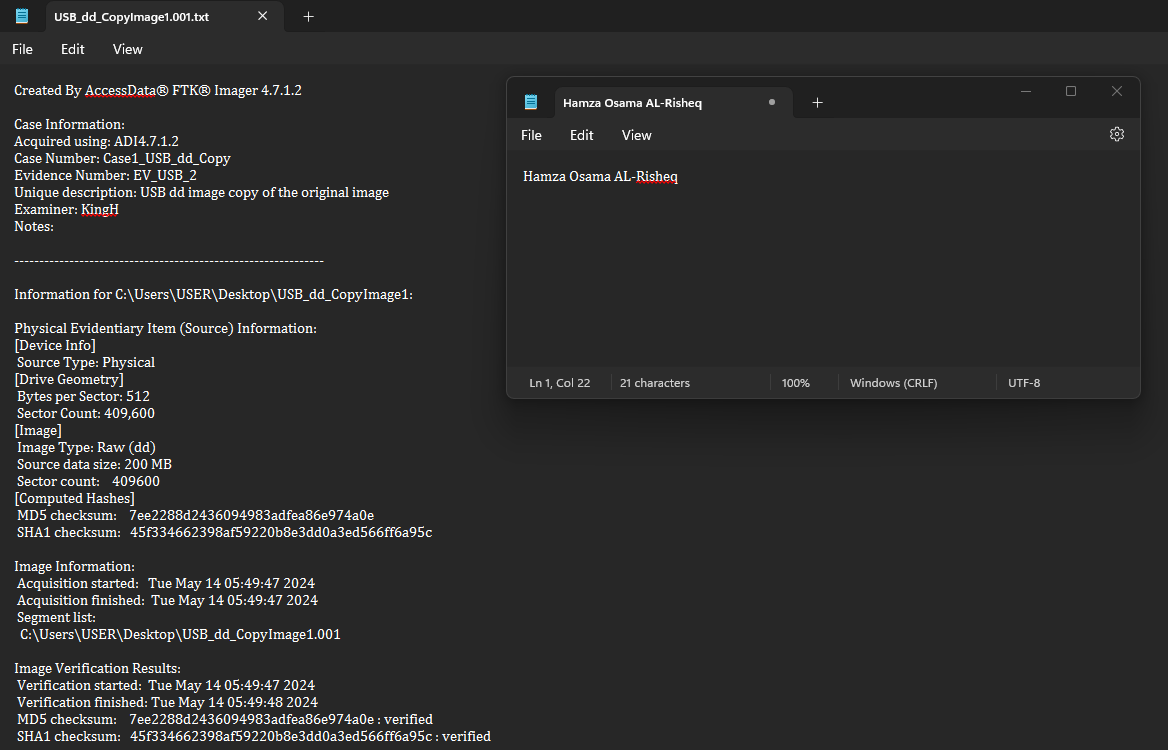


Figure 4: USB, COPY IMAGE FROM THE ORIGINAL IMAGE.

We will create another E01 image from the original image to conduct the investigation. This approach ensures that if any changes occur during the investigation, resulting in alterations to the image, we will have at least two copies of the evidence. Given that this case is highly confidential, we must apply the most secure techniques in the investigation to protect the integrity of the evidence. As we can in figures 5 and 6.

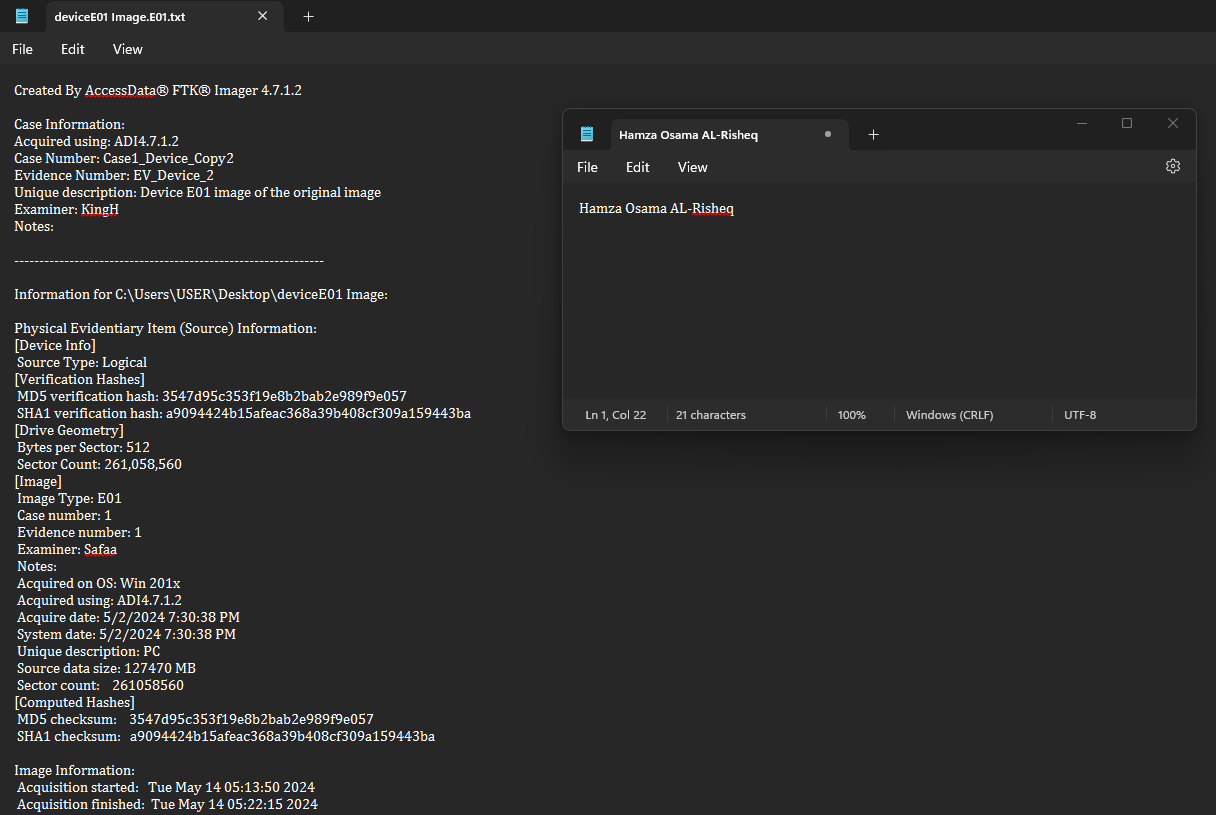


Figure 5: Device, E01 copy image from the original image.

**A screenshot of a computer

Description automatically generated**

Figure 6: USB, E01 copy image from the original image.

## 3.2. Investigation environment

The Digital Forensics Unit utilized specialized equipment and devices to conduct the investigation:

* Forensic Workstation (Laptop).
* Write-Blocked Hardware (Tableau TX1).
* External USB 1 TB Hard Drive for storing forensic images and case data.

## 3.3. Used Tools

The forensics tools employed in the performance of this in visitation were as follows:

* FTKImage – AccessData Version 4.7.1

FTK Imager is offering features like live imaging for creating forensic images without system shutdowns, extraction of volatile memory contents, imaging of network shares and remote devices, and selective extraction from forensic images. So, its main purpose is helping in doing acquisition.

* 010Editor – SweetScape 14.0.1

010 Editor is a widely recognized text and hex editor that provides experts with new ability to study and modify binary and files, as well as hard discs. With its different toolkit, which includes customizable templates and advanced scripting capabilities.

* HashMyFile – NirSofet 2.44

010 Editor is a widely recognized text and hex editor that provides experts with new ability to study and modify binary and files, as well as hard discs. With its different toolkit, which includes customizable templates and advanced scripting capabilities.

* WinPrefetchView - NirSofet 1.37

Provides insights into Windows Prefetch folder and file contents, helping in system analysis and forensic investigations.

* JumpListExplorer - Eric Zimmerman 2.0.0.0

Parses and analyzes Windows Jump Lists to reconstruct user activities and identify relevant artifacts.

* BrowsingHistoryView - NirSofet 2.57

Extracts and analyzes browsing history data from various web browsers, assisting in digital investigations.

# 4. Analysis summary

The investigation began by carefully examining the digital evidence retrieved from the confiscated device and USB drive and creating Raw(dd) copy image from each evidence. Our goal was to gather insights into the activities of the next BlackEagle group and uncover the location and time for their next crime. With several initial challenges, such as hidden files, our forensic analysis techniques enabled us to make substantial progress.

We discovered a wealth of information hidden within the digital artefacts, including hidden documents in other files containing vital information employed by the BlackEagle group. Furthermore, timestamps and location data encoded in the files gave useful context, allowing us to recreate the timeline of their operations and pinpoint possible targets.

Our investigation shed insight into the BlackEagle group's inner workings and gave significant intelligence to law enforcement. By uncovering hidden clues and decoding encrypted material, we obtained a better knowledge of their operations and took important actions to avoid future illegal activity.

# 5. Analysis

The initial step in the analysis process involved reading the image using FTK images to gain insight into the contents of the file system (the content of the drive device (the volume)) image of the device and USB to thoroughly understand its contents as in Figure 7 and Figure 8. (All the investigation procedures will be done on the E01 copied image).

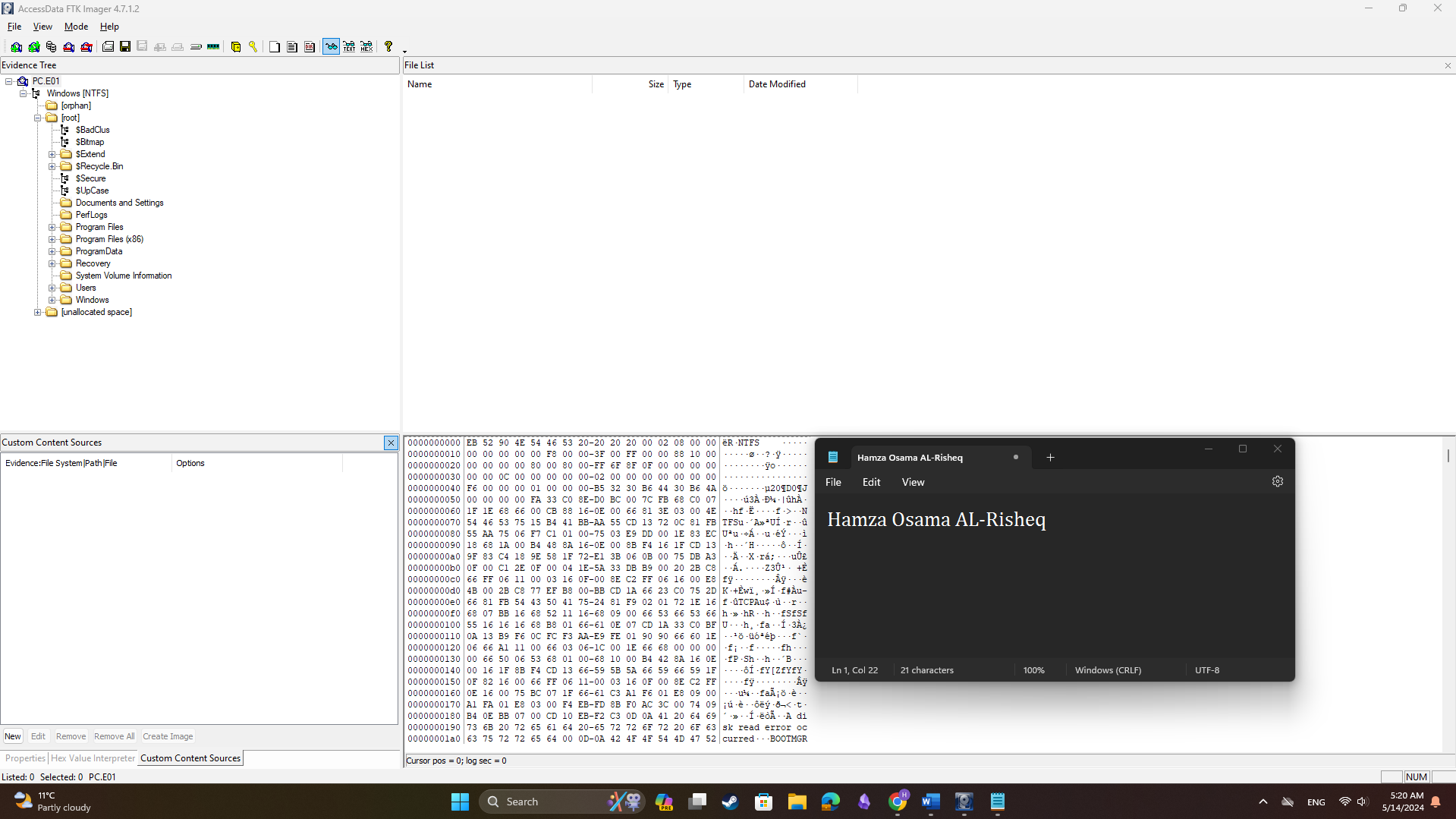


Figure 7: The file content of the Device evidence image.

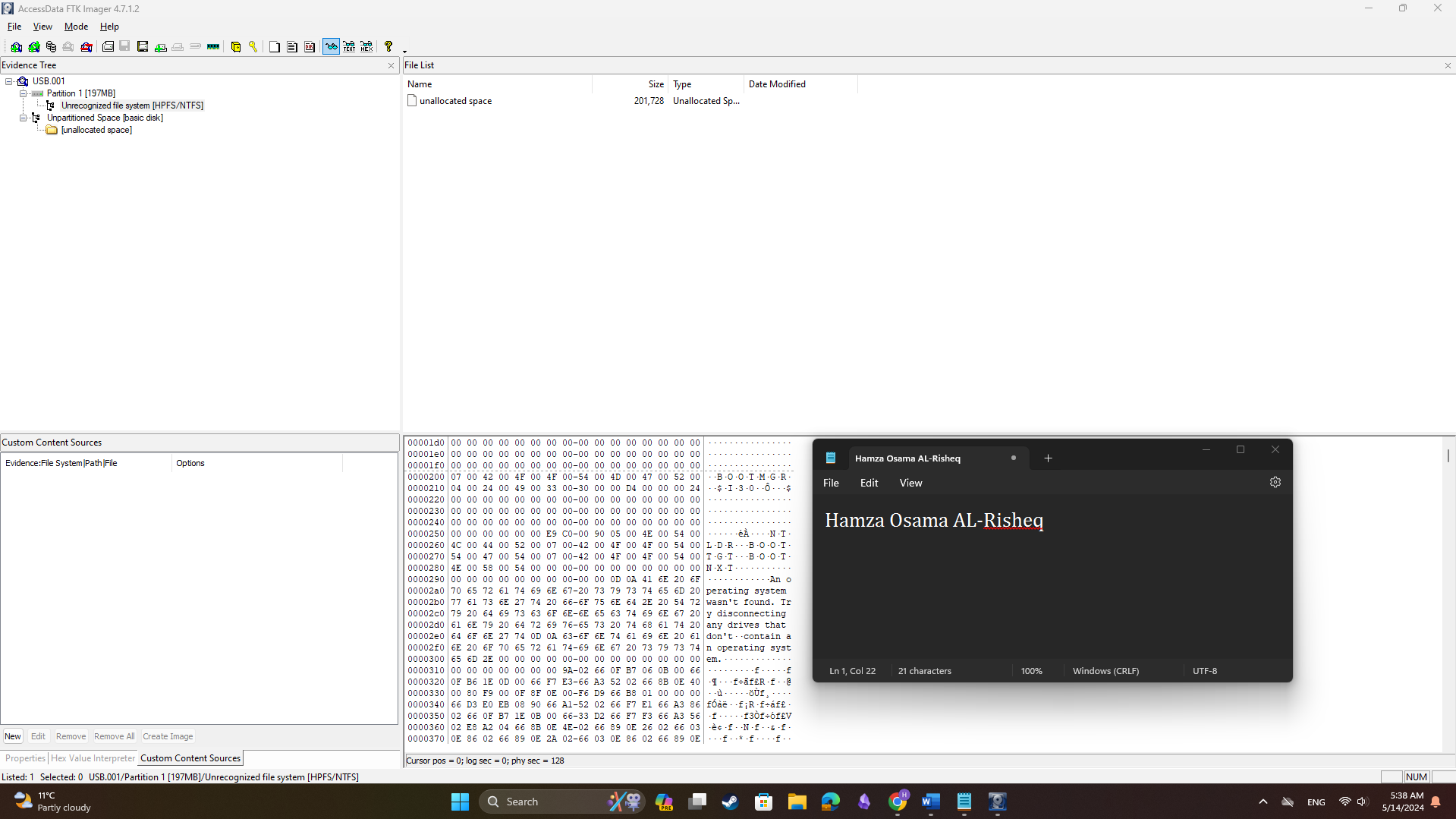
****

Figure 8: The file content of the USB evidence image.

Based on Figures 7 and 8, we can ascertain that the device is not corrupted and is readable. We have investigated the device. However, the USB is corrupted, necessitating repairs to extract its contents. Nonetheless, we have initiated investigations on the device to discern the activities of its user, aiming to determine the location and timing of the next BlackEagle crime.

Now, we must start reading all the file contents of the device image to extract all the files that will be used in the investigation. This process will help us understand the user activities and how Eagle's Eye was hiding their information. See Figure 9.

A screenshot of a computer

Description automatically generated

Figure 9: The extracted files from the device image drive.

The extracted files were extracted based on the pre-investigation plan we already have built view Appendix 1 for the plan. To find the path for each extracted file you check [**Appendix 2**](#_Appendix_2).

Now to understand EaglesEye activities on the device we will start investigating the jump list files.

Jump List Files Analysis:

* Firstly, we must view the content of the jump list files in the EaglesEye device. See Figure 10.

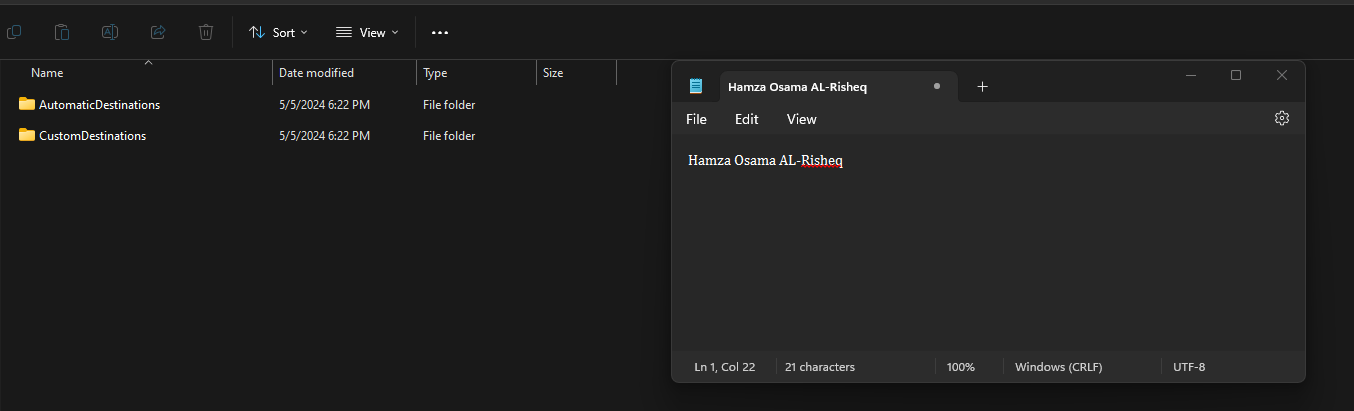


Figure 10: The content of jump list files in the EaglesEye device.

* Analyzing jump list files one by one using JumpListerExplorer tool:
* Automatic Link Files figure 11:

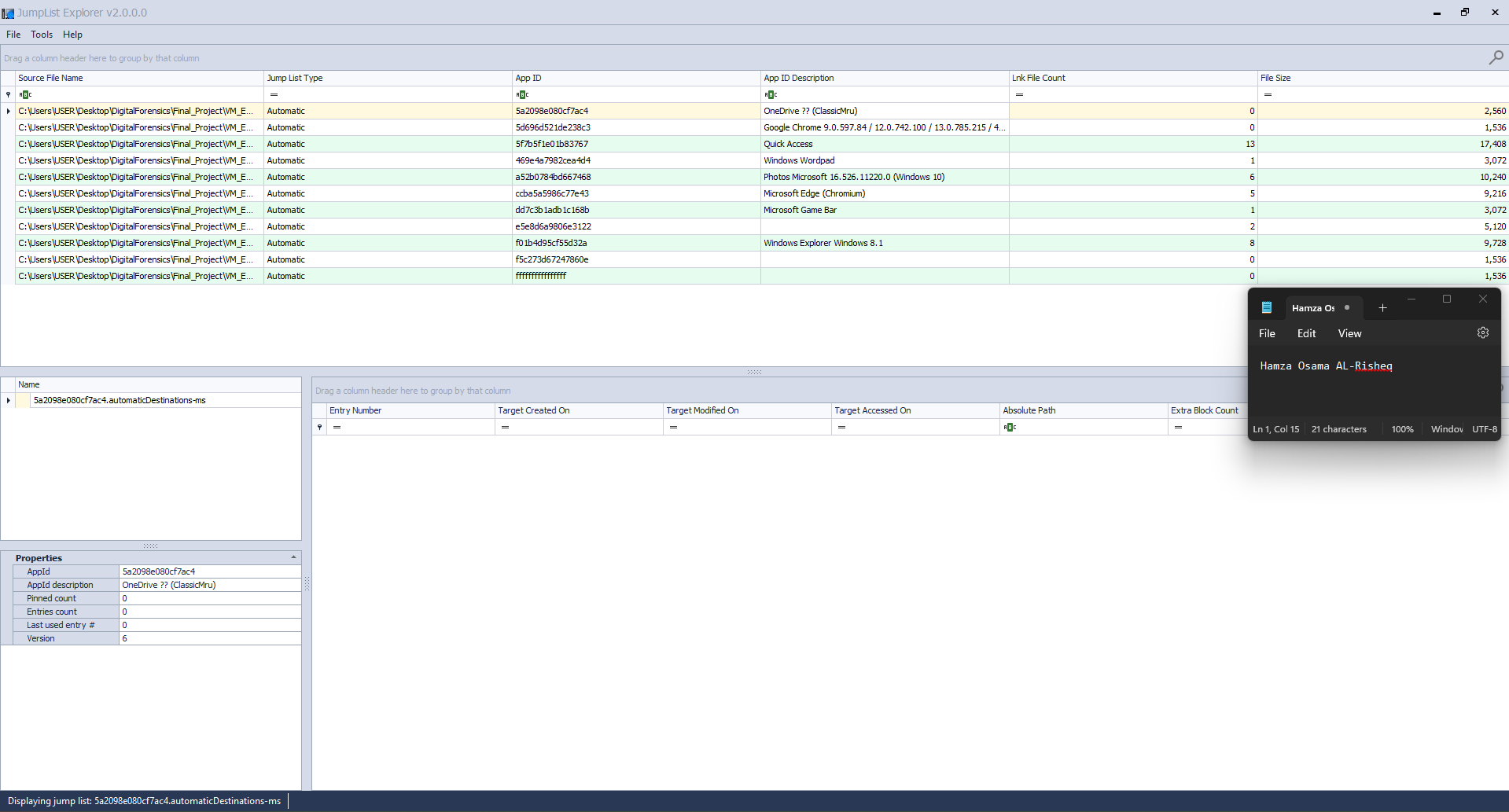


Figure 11: Automatic Link File content.

* + In the first two files, with appid (5a2098e080cf7ac4 and 5d696d521de283c3) there is no data, which means the user did not use or open them. I can evidence this when you click on them; you will not find any data, and the file count is 0.
  + The file with appid (5f7b5f1e01b83767) contains a lot of important information swhich they are the following:
    - The user accessed 13 files using the quickaccess feature in windows as we can see in figure 2.

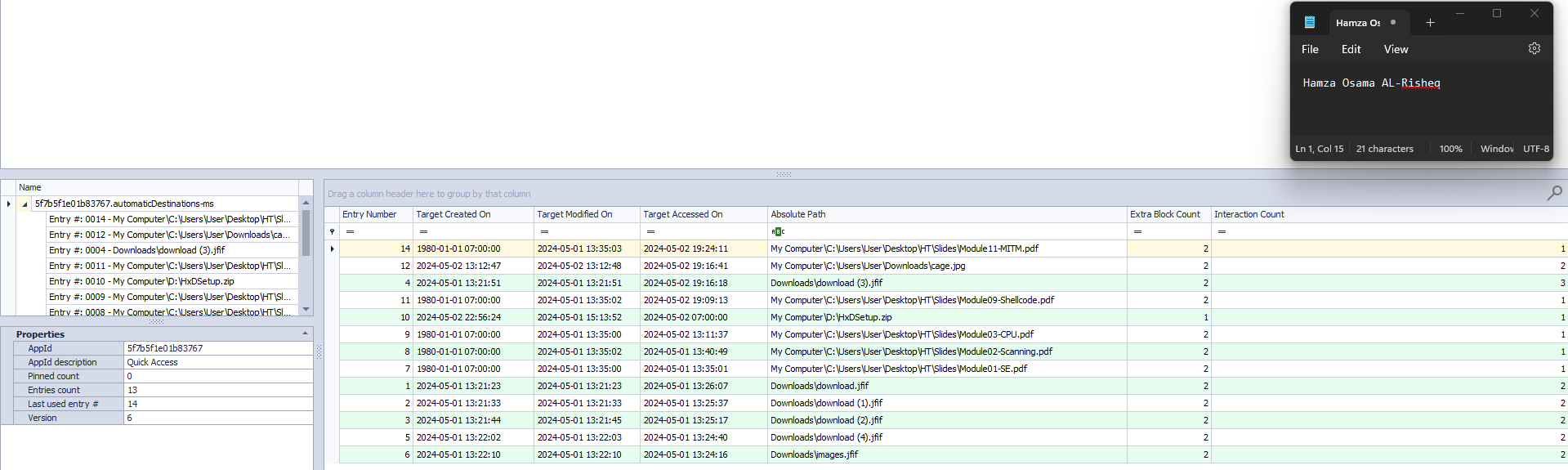


Figure 12: QuickAccess link file content.

* + - As we can see in Figure 12 that the user accessed the following files:
      * C:\Users\User\Desktop\HT\Slides\Module11-MITM.pdf
      * C:\Users\User\Desktop\HT\Slides\cage.jng
      * C:\Users\User\Downloads\download (3).jfif
      * C:\Users\User\Desktop\HT\Slides\Module09-Shellcode.pdf
      * D:\HxDSetup.zip
      * C:\Users\User\Desktop\HT\Slides\Module03-CPU.pdf
      * C:\Users\User\Desktop\HT\Slides\Module02-Scanning.pdf
      * C:\Users\User\Desktop\HT\Slides\Module01-SE.pdf
      * C:\Users\User\Downloads\download.jfif
      * C:\Users\User\Downloads\download (1).jfif
      * C:\Users\User\Downloads\download (2).jfif
      * C:\Users\User\Downloads\download (4).jfif
      * C:\Users\User\Downloads\images.jfif

We need to conduct further analysis on each file because we suspect that the user made alterations to these files. Additionally, we have observed that some file timestamps have been changed to the same creation time (1980-01-01 07:00:00), which requires deeper analysis. Moreover, the user accessed two drives, C: and D: indicating the possibility of an external drive such as a USB found at the crime scene, or another attached drive to the user's device.

By analyzing the Target accessed times on the app (5f7b5f1e01b83767), we can understand that the user activated their device at three specific times: from 2024-05-02 19:09:13 to 2024-05-02 19:24:11, the second time from 2024-05-01 13:24:16 to 2024-05-01 13:40:49, and the last time is 2024-05-02 07:00:00. The third time is very suspicious to me because it's not the usual time for the user, which means that it might have been changed or the user did something very suspicious on drive volume D:\.

* The file with appid (469e4a7892cea4d4) which is windows wordpad shows again suspicious activity as we can see in figure 13.

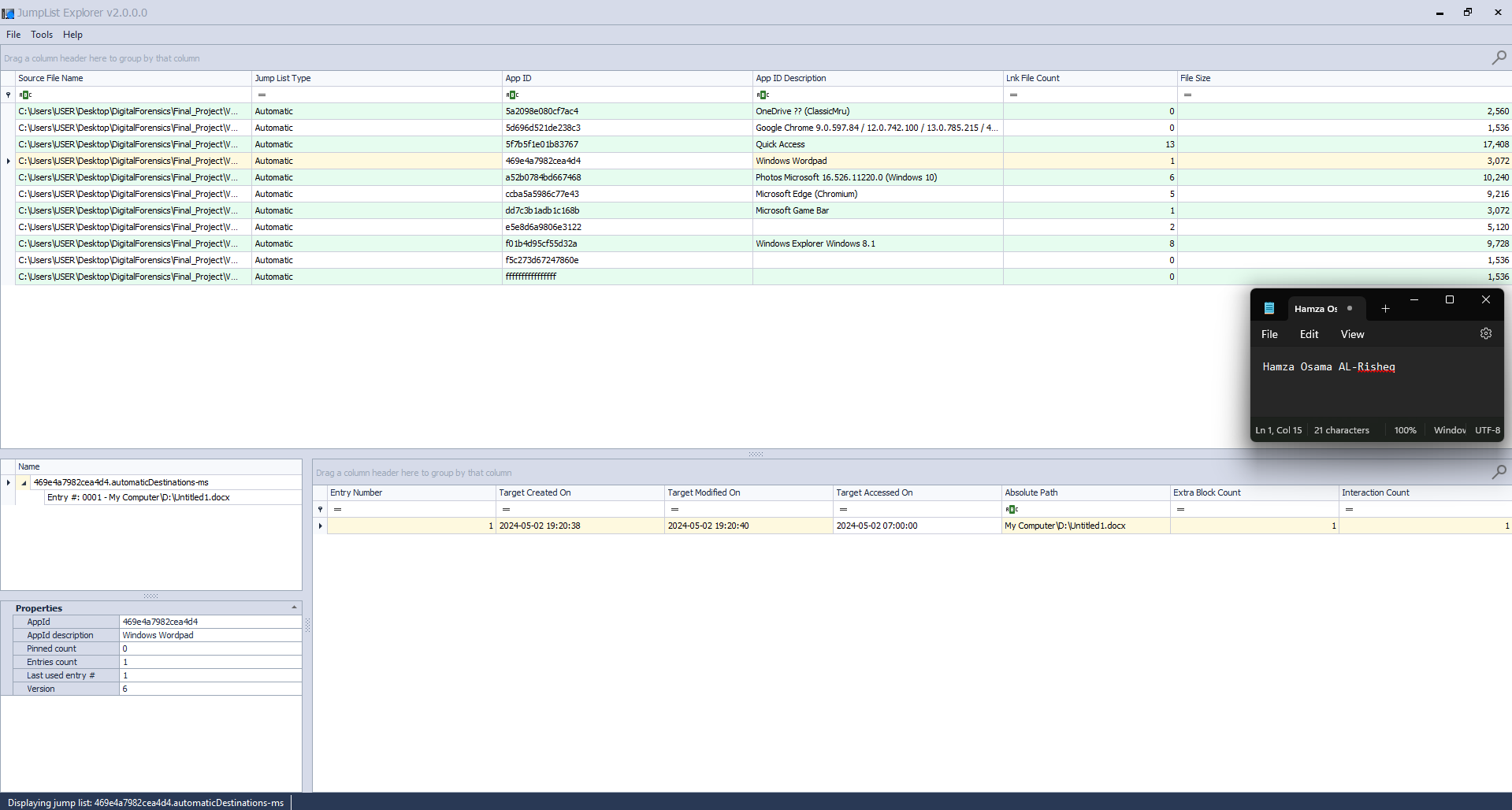


Figure 13: Windows wordpad jump link file content.

Its suspicious activity because it is evidence that the target time for Target accessed time is edited by the user and I can see that because the Target was created on 2024-05-02 19:20:38 and modified on 2024-05-02 19:20:40 but it accessed 2024-05-02 07:00:00. Which contains me that the accessed time is changed because the user accessed the file before its created also, we can find hour 7 am is mentioned again in more time which can lead us to something.

* Then analysis file with appid (a52b0784bd667468) is Photos Microsoft as we see in Figure 4.

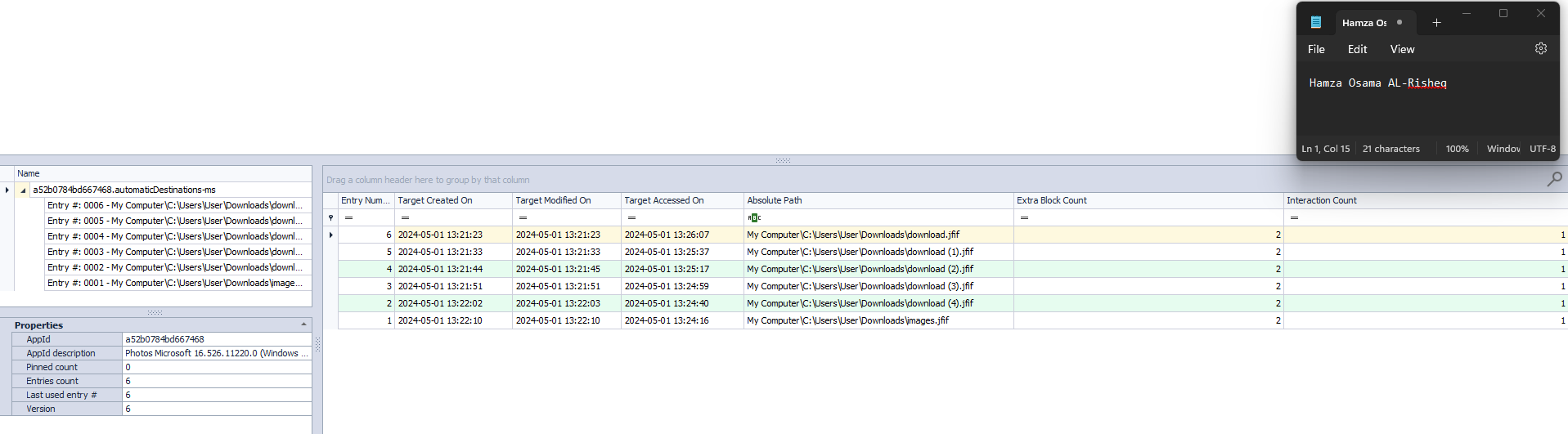


Figure 14: Photos Microsoft link file content.

Comparing the times of the same files in QucikAccess and Photos Microsoft

**Table 1: Comparing timestamps for specific link file in QucikAccess and Photos Microsoft**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| App Name | File Path | Created time | Modified Time | Accessed Time |
| Quick Access | C:\Users\User\Downloads\download.jfif | 2024-05-01 13:21:23 | 2024-05-01 13:21:23 | 2024-05-01 13:26:07 |
| Photos Microsoft | C:\Users\User\Downloads\download.jfif | 2024-05-01 13:21:23 | 2024-05-01 13:21:23 | 2024-05-01 13:26:07 |
| Quick Access | C:\Users\User\Downloads\download (1).jfif | 2024-05-01 13:21:33 | 2024-05-01 13:21:33 | 2024-05-01 13:25:37 |
| Photos Microsoft | C:\Users\User\Downloads\download (1).jfif | 2024-05-01 13:21:33 | 2024-05-01 13:21:33 | 2024-05-01 13:25:37 |
| Quick Access | C:\Users\User\Downloads\download (2).jfif | 2024-05-01 13:21:44 | 2024-05-01 13:21:45 | 2024-05-01 13:25:17 |
| Photos Microsoft | C:\Users\User\Downloads\download (2).jfif | 2024-05-01 13:21:44 | 2024-05-01 13:21:45 | 2024-05-01 13:25:17 |
| Quick Access | C:\Users\User\Downloads\download (4).jfif | 2024-05-01 13:22:02 | 2024-05-01 13:22:03 | 2024-05-01 13:24:40 |
| Photos Microsoft | C:\Users\User\Downloads\download (4).jfif | 2024-05-01 13:22:02 | 2024-05-01 13:22:03 | 2024-05-01 13:24:40 |
| Quick Access | C:\Users\User\Downloads\images.jfif | 2024-05-01 13:22:10 | 2024-05-01 13:22:10 | 2024-05-01 13:24:16 |
| Photos Microsoft | C:\Users\User\Downloads\images.jfif | 2024-05-01 13:22:10 | 2024-05-01 13:22:10 | 2024-05-01 13:24:16 |
| **Quick Access** | **C:\Users\User\Downloads\download (3).jfif** | **2024-05-01 13:21:51** | **2024-05-01 13:21:51** | **2024-05-02 19:16:18** |
| **Photos Microsoft** | **C:\Users\User\Downloads\download (3).jfif** | **2024-05-01 13:21:51** | **2024-05-01 13:21:51** | **2024-05-01 13:24:59** |

Based on the comparison in Table 1 we can find out that the target with C:\Users\User\Downloads\download (3).jfif path has accessed two different times which leads us to understand that maybe we will find something in this jfif file hidden files or something in the image structure.

* The appid (ccba5a5986c77e43) which Microsoft Edge has 5 specific target files that the user opens using the Microsoft Edge (when you open a pdf file you will use a browser) here the user used Microsoft Edge as we can see in figure 5.

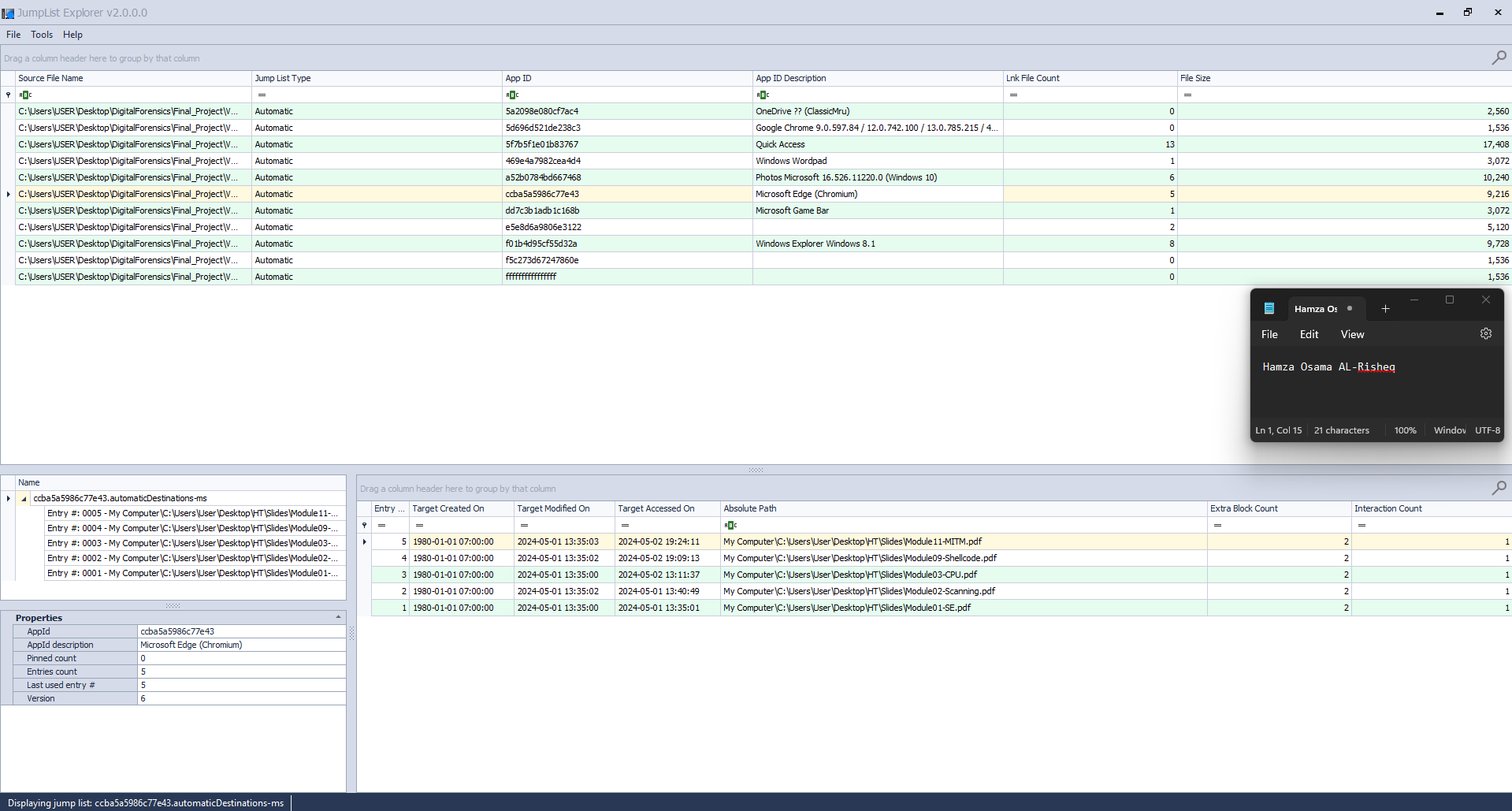


Figure 15: Microsoft edge link file content.

**Table 2: Comparing timestamps for specific link file in QucikAccess and Microsoft edge.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| App Name | File Path | Created time | Modified Time | Accessed Time |
| Quick Access | C:\Users\User\Desktop\HT\Slides\Module01-SE.pdf | 1980-01-01 07:00:00 | 2024-05-01 13:35:00 | 2024-05-01 13:35:01 |
| Microsoft edge | C:\Users\User\Desktop\HT\Slides\Module01-SE.pdf | 1980-01-01 07:00:00 | 2024-05-01 13:35:00 | 2024-05-01 13:35:01 |
| Quick Access | C:\Users\User\Desktop\HT\Slides\Module02-Scanning.pdf | 1980-01-01 07:00:00 | 2024-05-01 13:35:02 | 2024-05-01 13:40:49 |
| Microsoft edge | C:\Users\User\Desktop\HT\Slides\Module02-Scanning.pdf | 1980-01-01 07:00:00 | 2024-05-01 13:35:02 | 2024-05-01 13:40:49 |
| Quick Access | C:\Users\User\Desktop\HT\Slides\Module03-CPU.pdf | 1980-01-01 07:00:00 | 2024-05-01 13:35:00 | 2024-05-02 13:11:37 |
| Microsoft edge | C:\Users\User\Desktop\HT\Slides\Module03-CPU.pdf | 1980-01-01 07:00:00 | 2024-05-01 13:35:00 | 2024-05-02 13:11:37 |
| Quick Access | C:\Users\User\Desktop\HT\Slides\Module09-Shellcode.pdf | 1980-01-01 07:00:00 | 2024-05-01 13:35:02 | 2024-05-02 19:09:13 |
| Microsoft edge | C:\Users\User\Desktop\HT\Slides\Module09-Shellcode.pdf | 1980-01-01 07:00:00 | 2024-05-01 13:35:02 | 2024-05-02 19:09:13 |
| Quick Access | C:\Users\User\Desktop\HT\Slides\Module11-MITM.pdf | 1980-01-01 07:00:00 | 2024-05-01 13:35:03 | 2024-05-02 19:24:11 |
| Microsoft edge | C:\Users\User\Desktop\HT\Slides\Module11-MITM.pdf | 1980-01-01 07:00:00 | 2024-05-01 13:35:03 | 2024-05-02 19:24:11 |

***Table 2 results:***

* There are more than two files that are in Microsoft Edge jump link file content, that have the same modified time which means that the user edited both of them at the same time which is lead that the user changed their modified time. They are:
  1. C:\Users\User\Desktop\HT\Slides\Module01-SE.pdf with C:\Users\User\Desktop\HT\Slides\Module03-CPU.pdf.
  2. C:\Users\User\Desktop\HT\Slides\Module02-Scanning.pdf with C:\Users\User\Desktop\HT\Slides\Module09-Shellcode.pdf.
* Because the times between the Quick Access and Microsoft Edge times are the same even if they are changed, I can understand that the user used the Quick Access feature to open these PDF files and when using the Microsoft Edge browser to open, view, and edit them.
* The file with appid (e5e8d6a9806e3122) has two files' content as we can see in Figure 6.

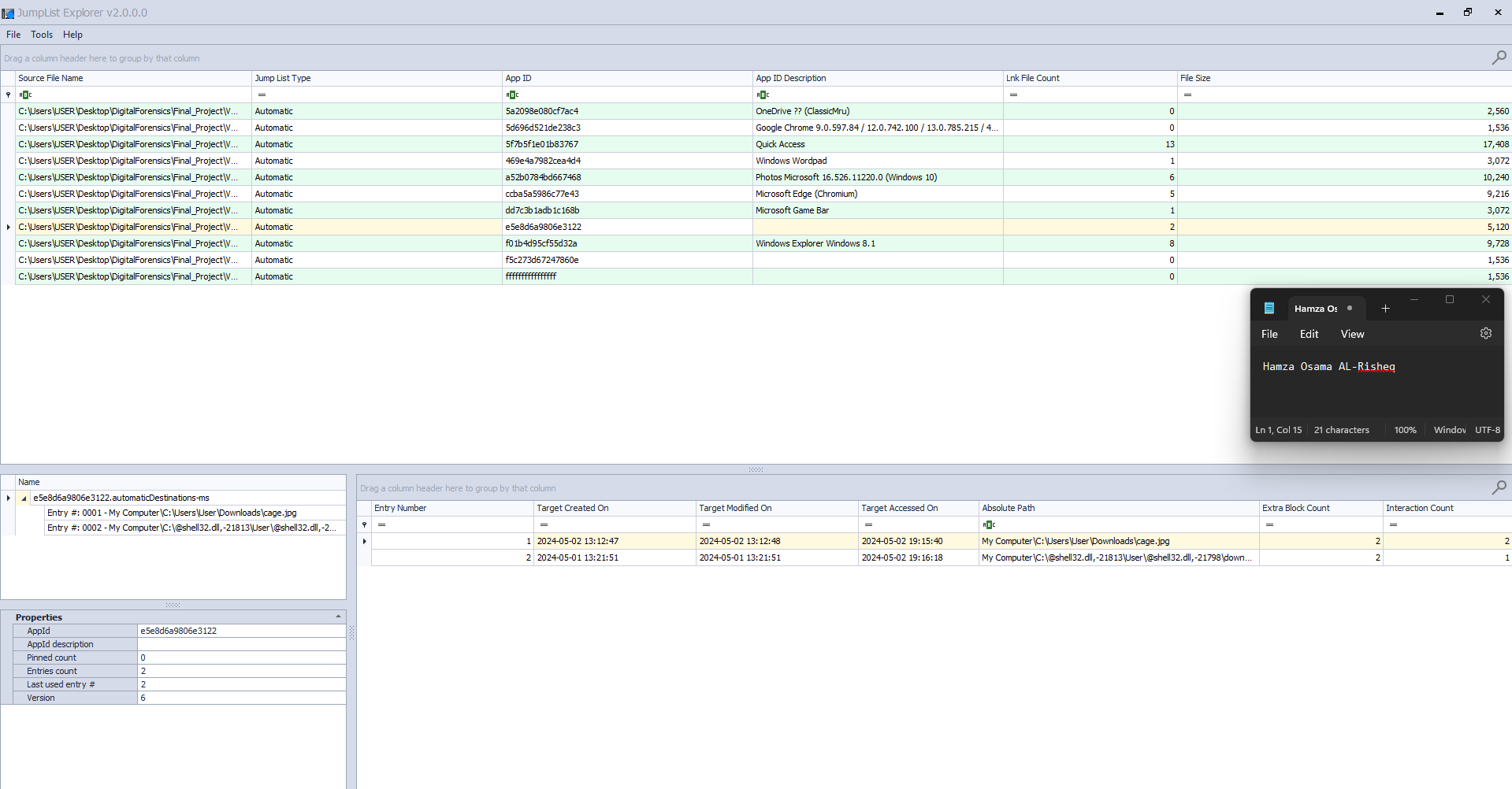


Figure 16: Unknown name line file content.

Because the app is without a name which may be an application that used to do something suspicious, and the jump link files of that application contain two image paths because they are images that suspect this process, or this app used to do something so we will do more investigation on these two images.

* The file with appid (f01b4d95cf55d32a) is Windows Explorer content can be seen in Figure 7.

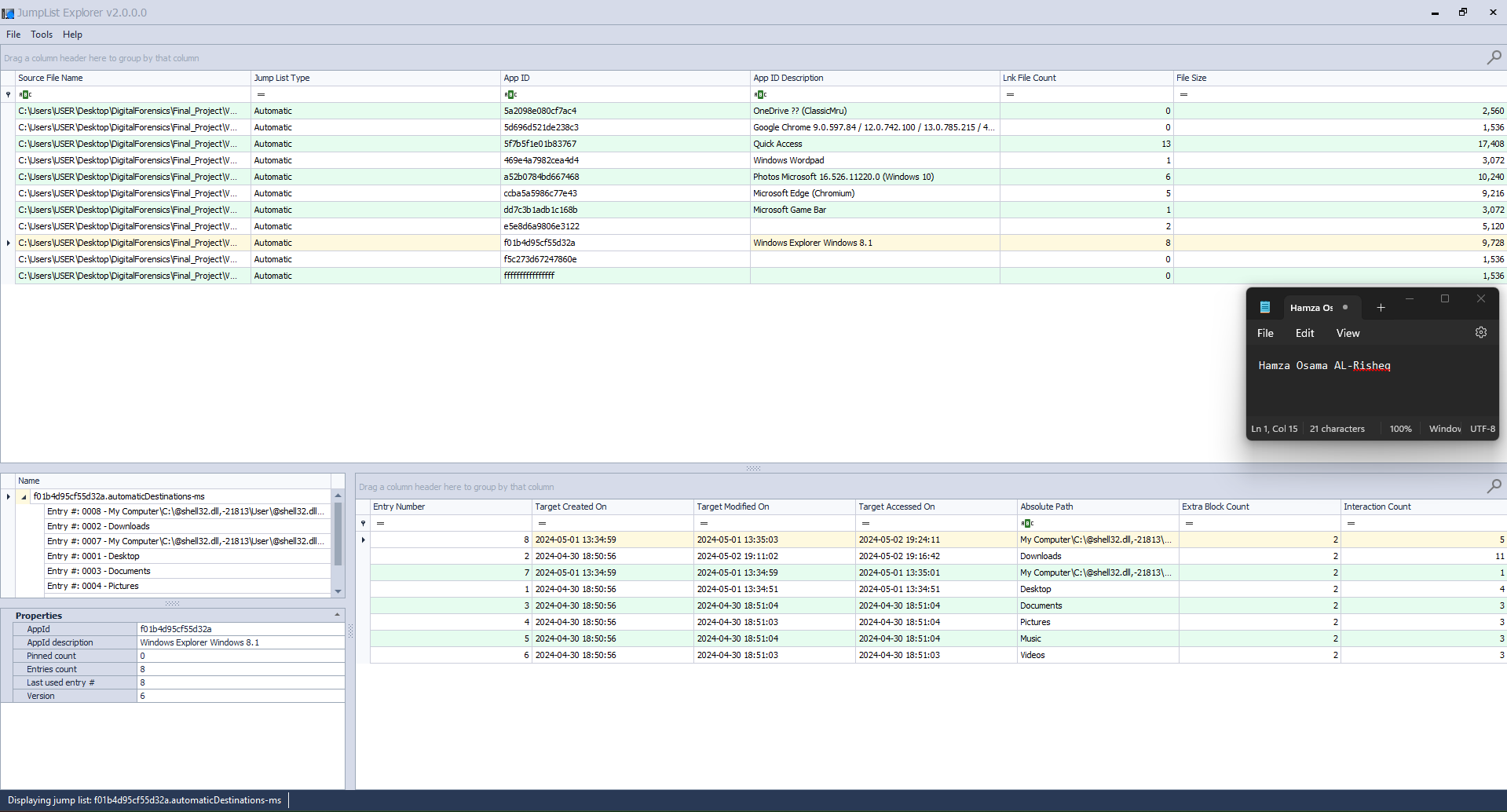


Figure 17: Windows Explorer link file content.

Based on these timestamps in Windows Explorer link file content I can understand that the user first time used this device or did something on this device was in 2024-04-30 at 18:50:56 because on this date the Desktop, Downloads, and libraries link files are created, and these files the system create them in the first time you access your device. May they be edited but for me at this moment of analysis I do not see that the Windows Explorer times are edited. But I must conduct further analysis to make sure of this point.

* Custom Link Files:

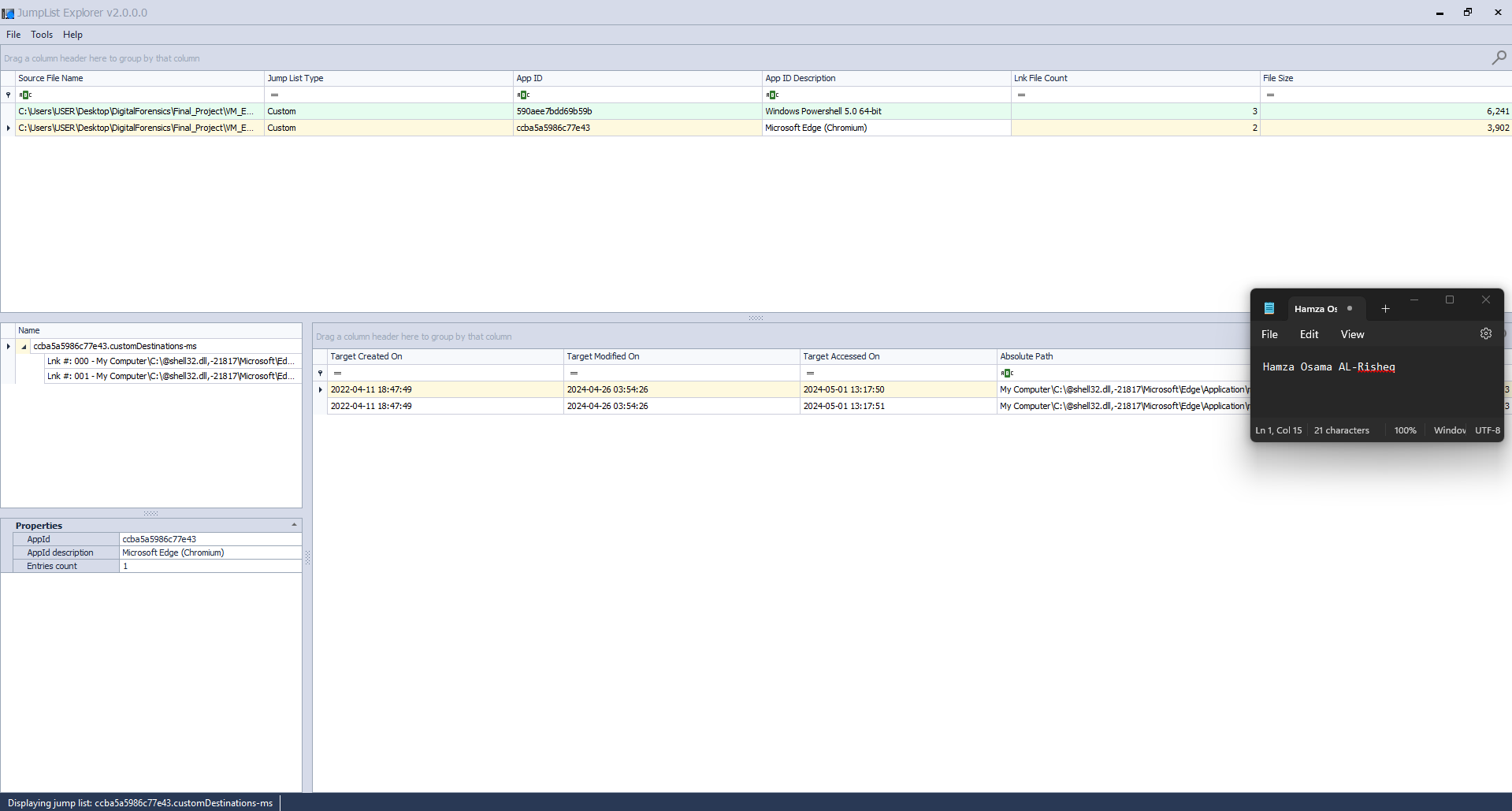


Figure 18: Custom Link Files Content.

The custom link files have two files which are Windows Powershell and Microsoft Edge:

* For Microsoft Edge files we can see here in the custom link files that there is an executable file accessed two times, but I do not know what this file is so I must extract it and try to open it in the VM machine to test and understand their function because maybe they contain something vital, malware, or special code for something. The executable file path is C:\Program Files (x86) \Microsoft\ Edge\ Application\msedge.exe
* For Windows PowerShell files the same as Microsoft Edge we must understand the file's functions.

After the investigation of the jump files, we will start the investigation on the prefetch files. You can see the content of prefetch files in Figure 19.

Prefetch Files Analysis:

* Firstly, we must view the content of the prefetch files in the EaglesEye device. See Figure 19.

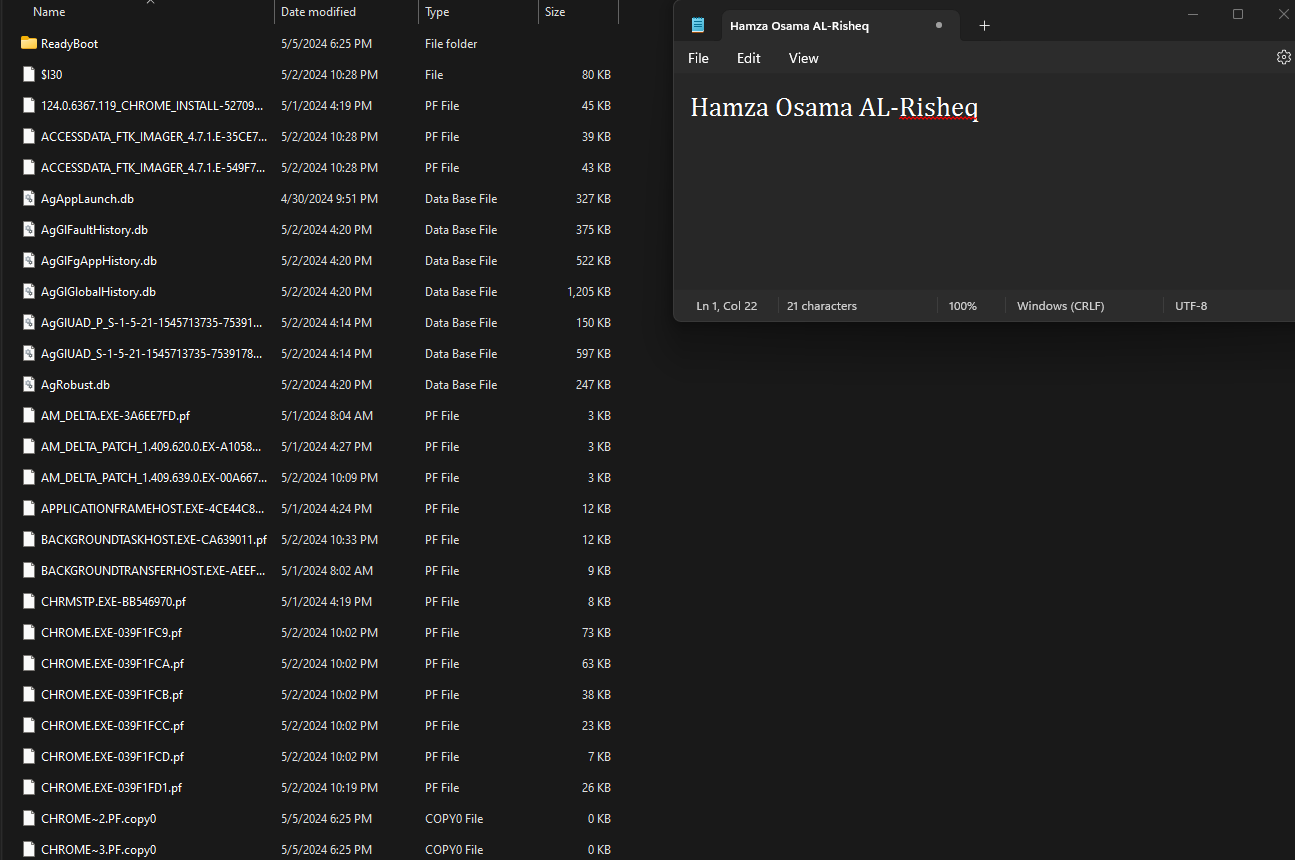


Figure 19: The content of prefetch files in the EaglesEye device.

* Analysis the prefetch files using WinPrefetchView tool, see figure 20.

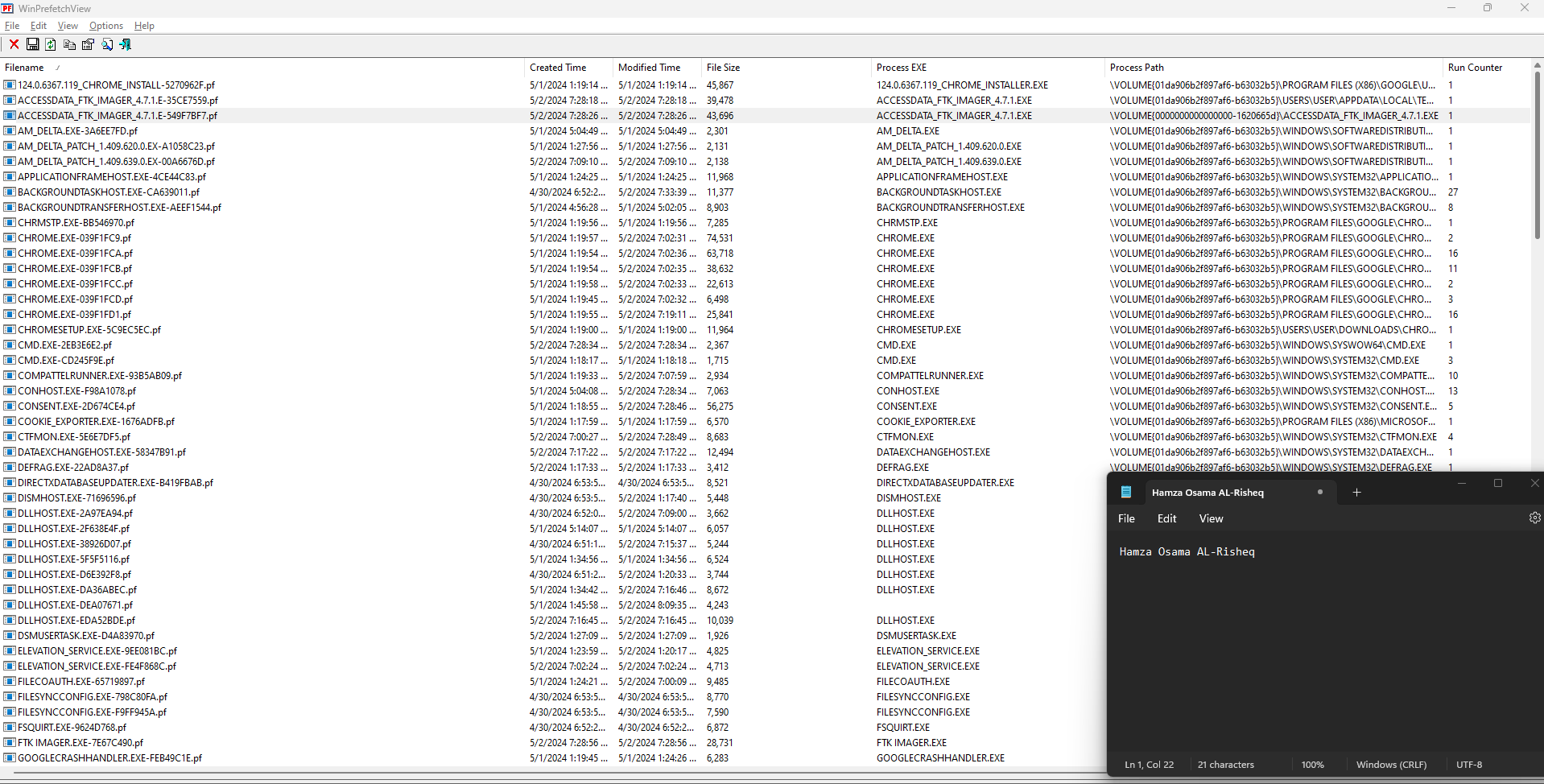


Figure 20: viewing the prefetch files in the WinPrefetchView.

The result of analysis prefetch files:

* Based on the IDs of the volumes in the prefetch files, we can understand that there are two drives within the same machine. Perhaps one of them is external, such as a flash drive. I am still in the process of determining the type of drive, but I am certain that one of them is the main drive (like the C: drive).
* The first drive, which is assumably the external one, has at least 2 downloaded applications: the FTK\_imager tool and the HxD tool. We can observe evidence of this in Figure 12.

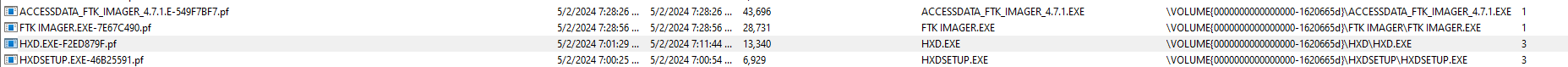


Figure 21: prefetch files for specific volume.

* Based on the other prefetch files from another drive, I can infer that the user of this device utilized their machine to download the FTK\_imager tool and HxD tool, then cut and pasted them to another drive (this is just an assumption for now). From Figure 13, I noticed that both the FTK\_imager tool and HxD tool have temporary prefetch files on a drive. However, when searching for them, they are not found. Perhaps in the subsequent investigation, I may discover additional information.



Figure 22: prefetch files for specific volume.

* Additionally, I can confirm that this user utilized Google Chrome to download the FTK\_imager tool and HxD tool. This assertion is based on the fact that the user downloaded Google Chrome on the same dates and frequently used it, as depicted in Figure 23.

A screenshot of a computer

Description automatically generated

Figure 23: google chrome prefetch files.

By examining the location of Google Chrome, viewing its timestamps, and analyzing the timestamps of the located Google Chrome.exe file, I can conclude that it has been copied and pasted multiple times. This inference is drawn from the numerous prefetch files associated with the location of Google Chrome, as depicted in Figure 24. Additionally, the disparity between the modified and created times of the last version of Google Chrome, as shown in Figure 25, indicates that it has been copied.

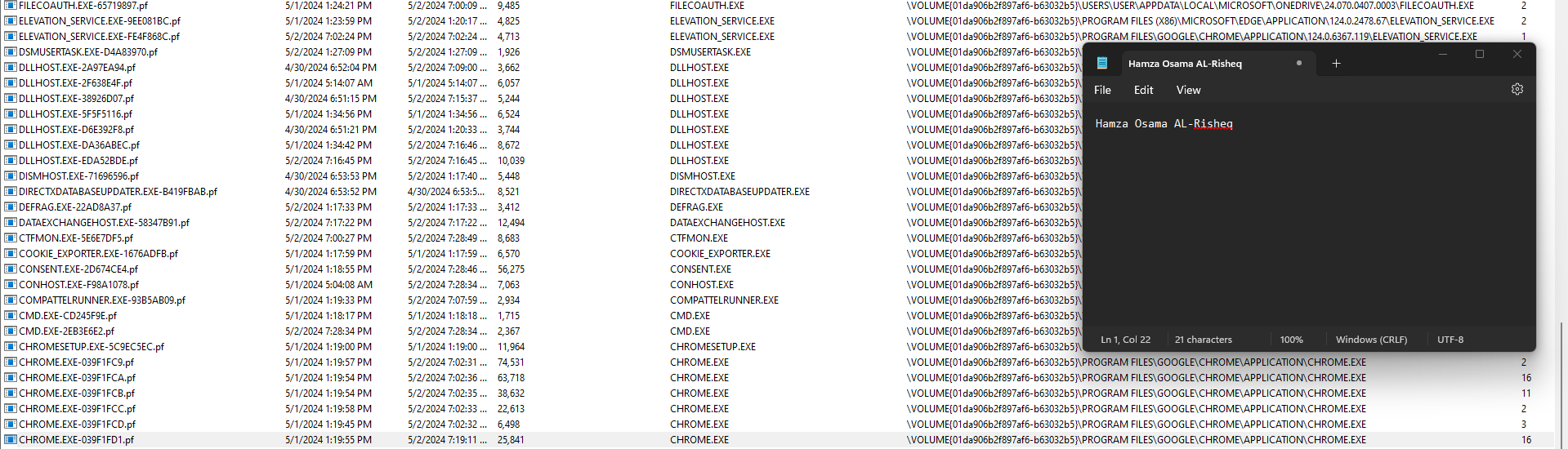


Figure 24: google chrome prefetch file times stamps and target paths.

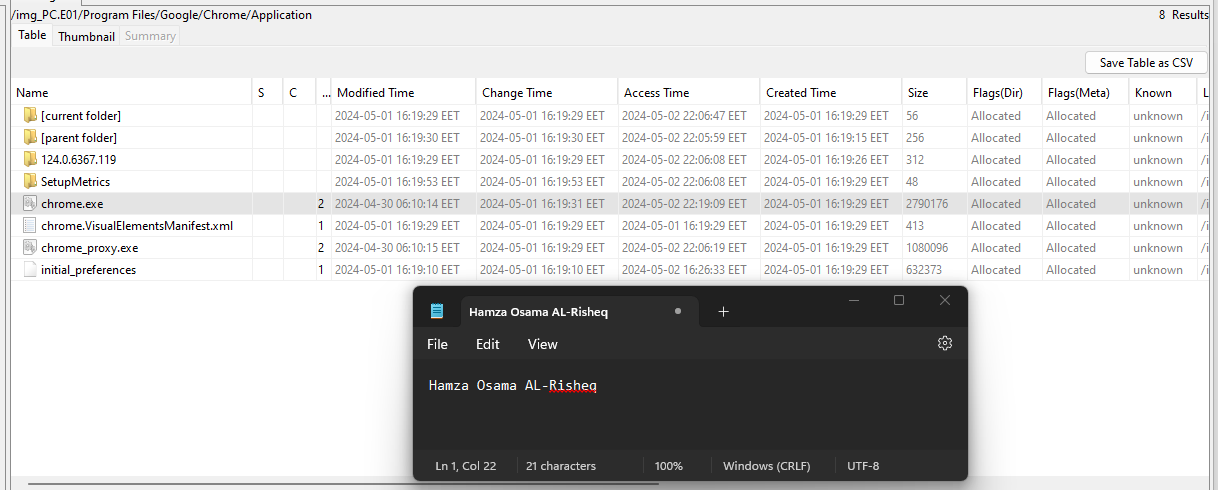


Figure 25: the target googles chrome file path with time stamps.

After finishing analyzing the prefetech files all we can say is that maybe EAglesEye used HxD and FtkImager tools to do something in one of the files in his/her device.

So, now it's time to analyze the Recycle.Bin Folder.

Recycle.Bin Folder Analysis:

Firstly, we must view the content of the Recycle.Bin Folder in the EaglesEye device. See Figure 26.

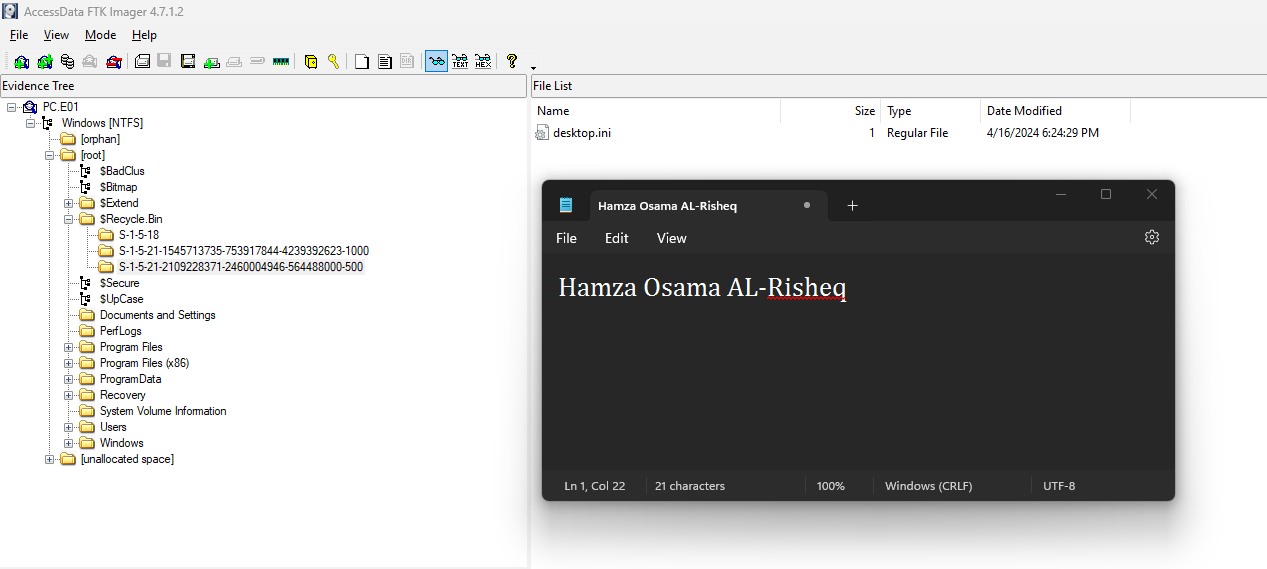


Figure 26: Recycle.Bin Folder Content.

The Recycle Bin folder is empty, implying two main possibilities. Firstly, the user may have deleted all important files, including those within the Recycle Bin. Secondly, it's possible that the user did not delete anything at all.

Now, we need to review the library’s folders.

Library’s Analysis:

Firstly, we must view the content of the Library’s Folder in the EaglesEye device. See Figure 27.

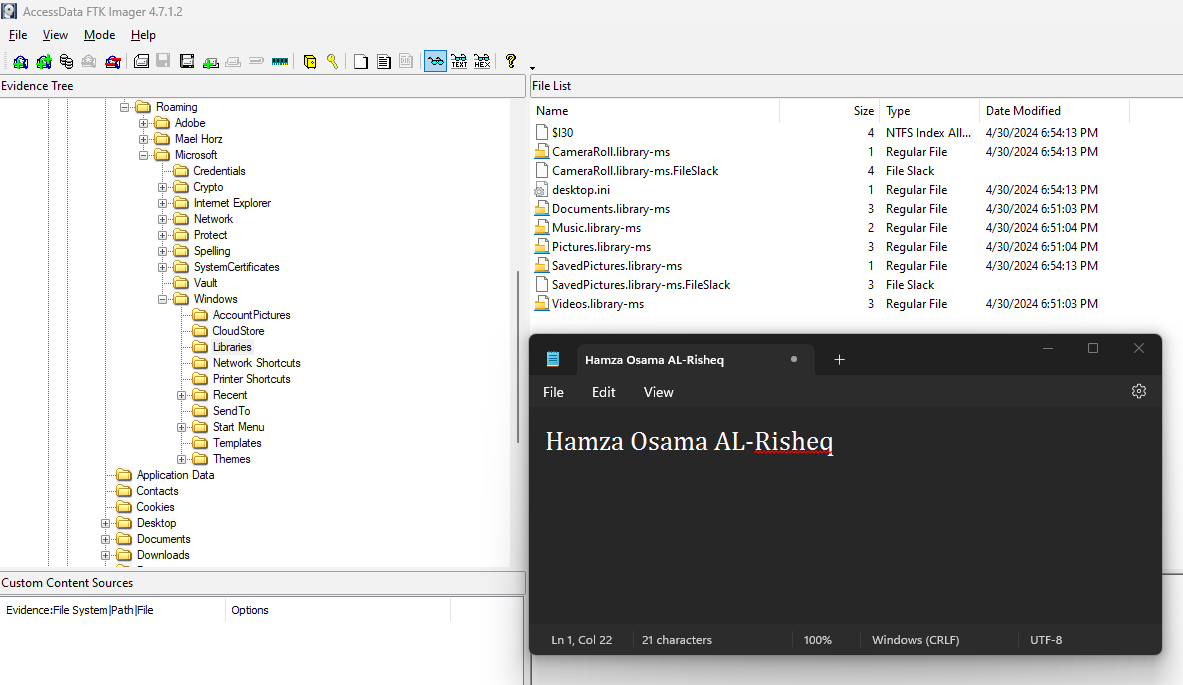


Figure 27: Library's Folder Content.

The library folder is empty. So, now we need to review the desktop files and folders, paying particular attention to the files that EaglesEye opened, as indicated by the analysis of the jump list and link files.

Desktop Folder Analysis:

Firstly, we must view the content of the desktop folder in the EaglesEye device. See Figure 28 - 32.

A screenshot of a computer

Description automatically generated

Figure 28: Desktop Content.

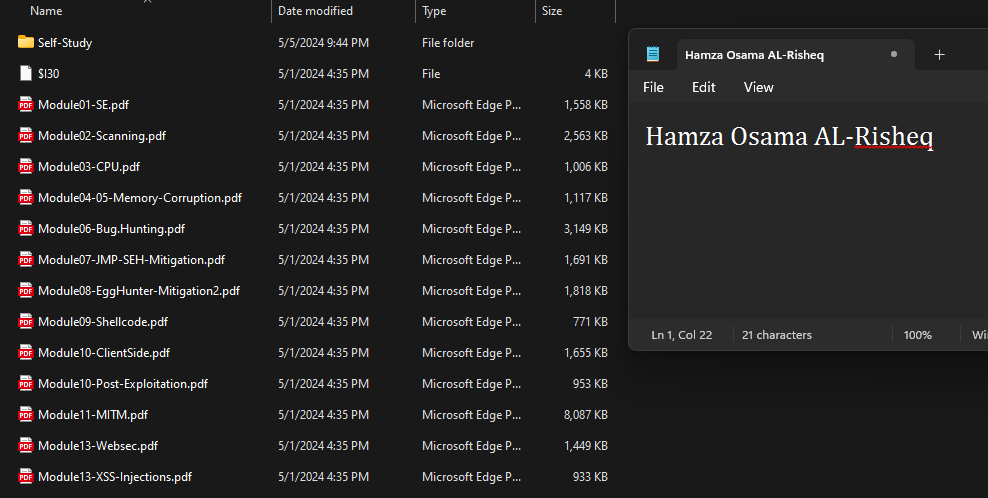


Figure 29: HT Folder Content.

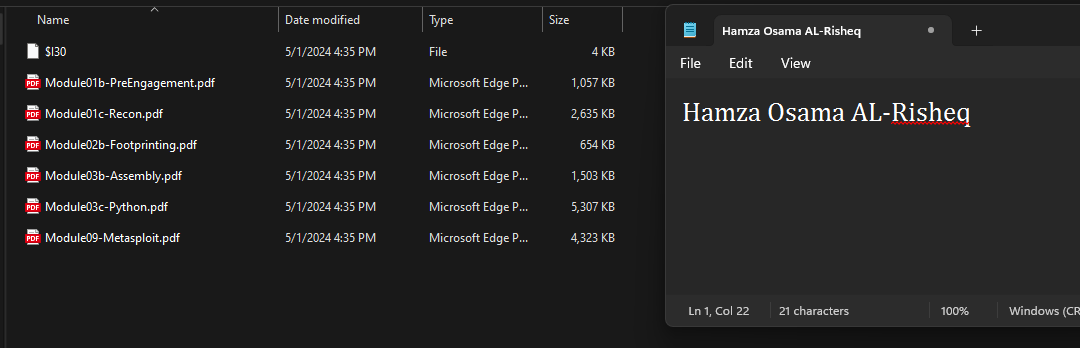


Figure 30: Self Study Folder Content.

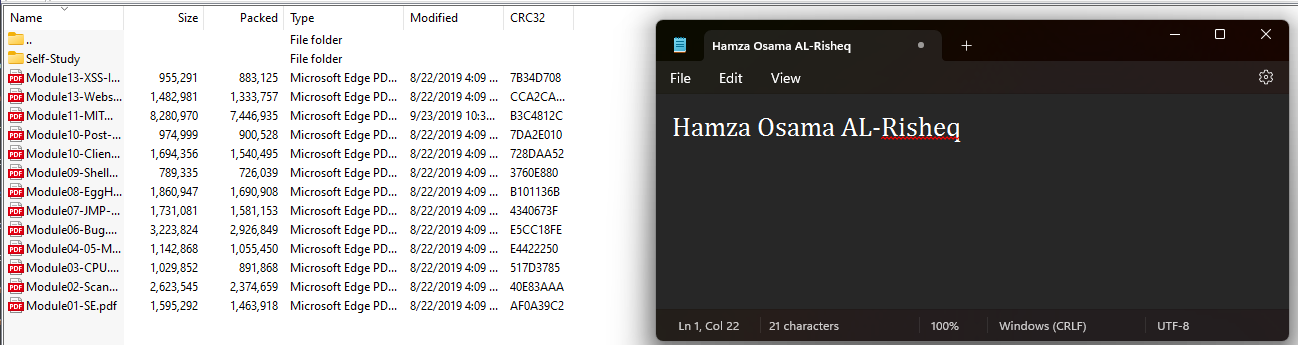


Figure 31: Content of the ZIP folder.

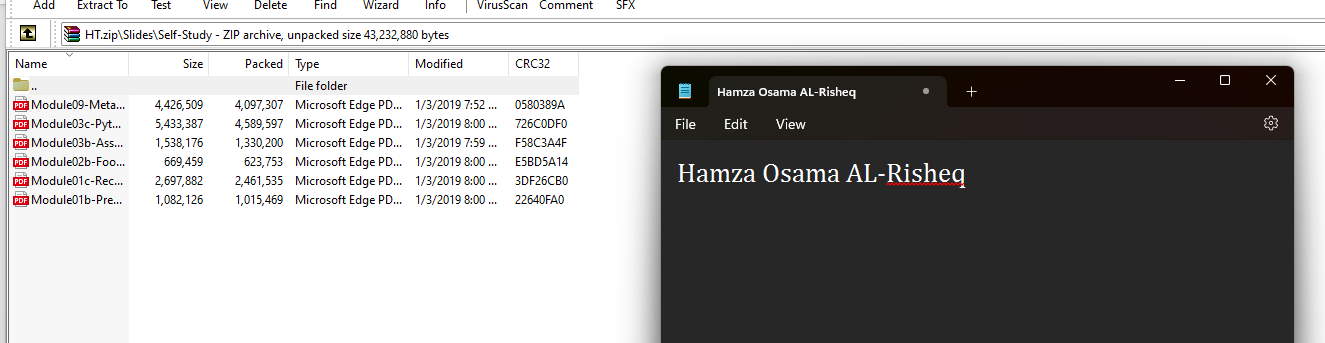


Figure 32: Content of the ZIP Folder.

Based on the analysis of the .LNK files conducted during the jump list phase, we reviewed the following files in both the user GUI and Hexa byte’s view (using 010 Editor) because the user opened them on the desktop:

* C:\Users\User\Desktop\HT\Slides\Module11-MITM.pdf
* C:\Users\User\Desktop\HT\Slides\cage.jng
* C:\Users\User\Desktop\HT\Slides\Module09-Shellcode.pdf
* C:\Users\User\Desktop\HT\Slides\Module03-CPU.pdf
* C:\Users\User\Desktop\HT\Slides\Module02-Scanning.pdf
* C:\Users\User\Desktop\HT\Slides\Module01-SE.pdf

After finishing analysis of all the files in the desktop nothing is found in them so we will go to the next reviewing the files in the downloads. Also, we search for hidden files in the files that EAglesEye accessed in the desktop (Searching for specific headers and footers signatures to find the hidden data in the files, view [Appendix 3](#_Appendix_3:) for the specific header and footer signatures).

Downloads Folder Analysis:

Firstly, we must view the content of the downloads folder in the EaglesEye device. See Figure 33.

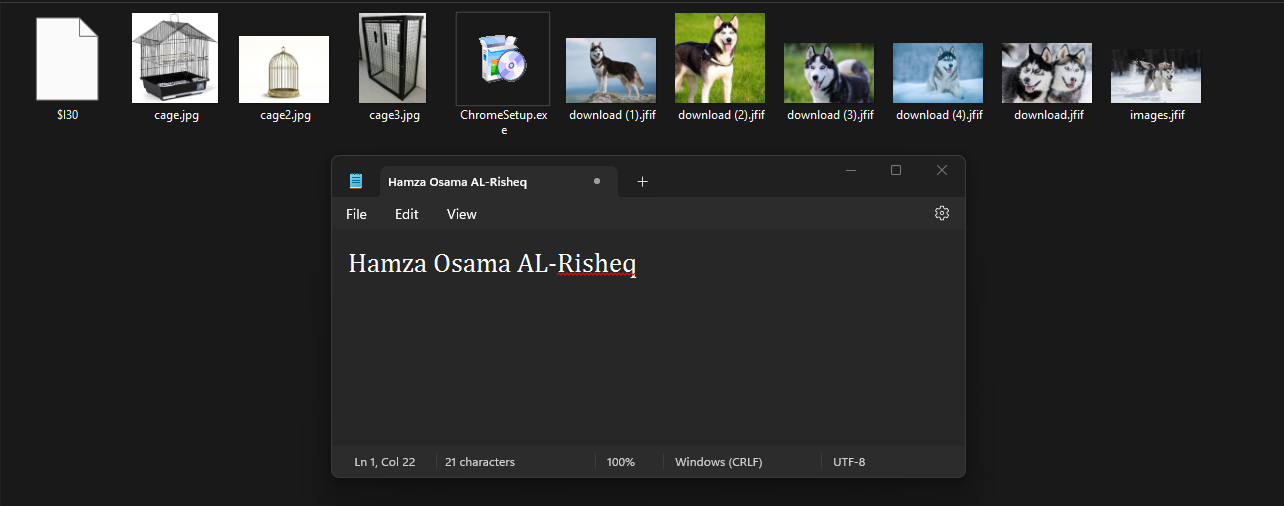


Figure 33: Downloads Folder Content.

Based on the analysis of the .LNK files conducted during the jump list phase, we reviewed the following files in both the user GUI and Hexa byte’s view (using 010 Editor) because the user opened them on the downloads:

* C:\Users\User\Downloads\download (3).jfif
* C:\Users\User\Downloads\download.jfif
* C:\Users\User\Downloads\download (1).jfif
* C:\Users\User\Downloads\download (2).jfif
* C:\Users\User\Downloads\download (4).jfif
* C:\Users\User\Downloads\images.jfif

Based on the viewing the searching for hidden files and data using specific headers and footers inside each .jfif file the user accessed from downloads we found that only one .jfif file contain another docx file we did the following approach until we find it:

* Search for specific footers, view Figure 34.
* We found many headers for DOCX files. Now, we will search for the. jfif footer to determine the end of the image.
* So, from the footer signature to the end of the image I extracted them in alone hex file.
* Then we extracted the docx from its first header to the footer view Figure 35.
* Then we opened the docx file to view its content, searching for any vital information. Figure 36.

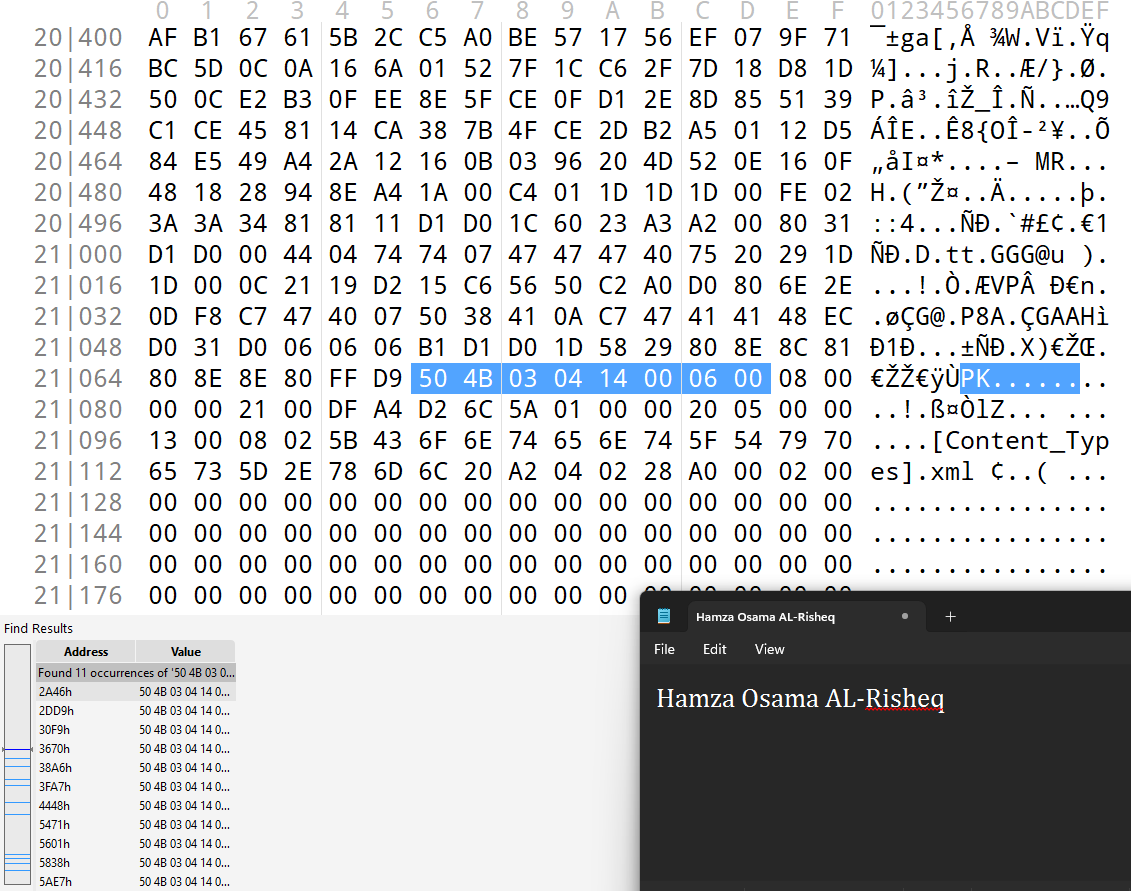


Figure 34: Footer Signatures Searching Results.

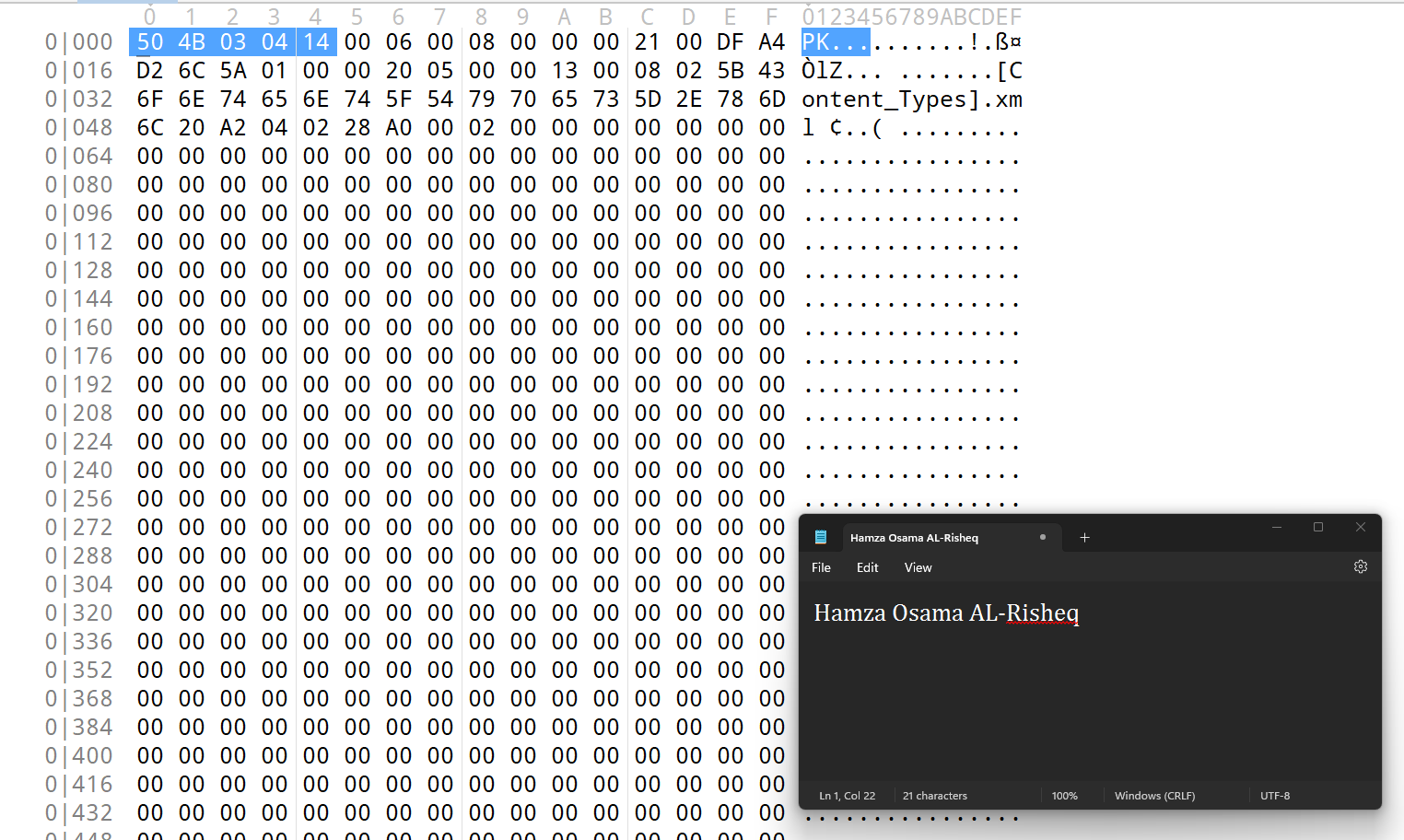


Figure 35: Extracted Docx File.

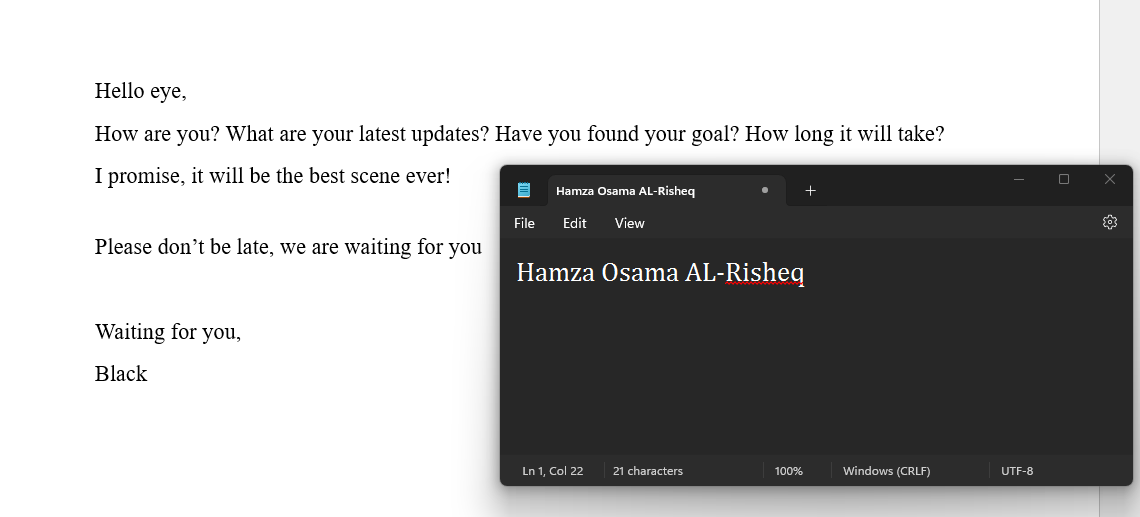


Figure 36: Opened Docx.

We need to select all the content of the DOCX file and change it to one color to check if the user attempted to hide information within the DOCX file. Alternatively, we can open the DOCX file with an XML extension to view all the content. Please refer to Figure 37 for further details.

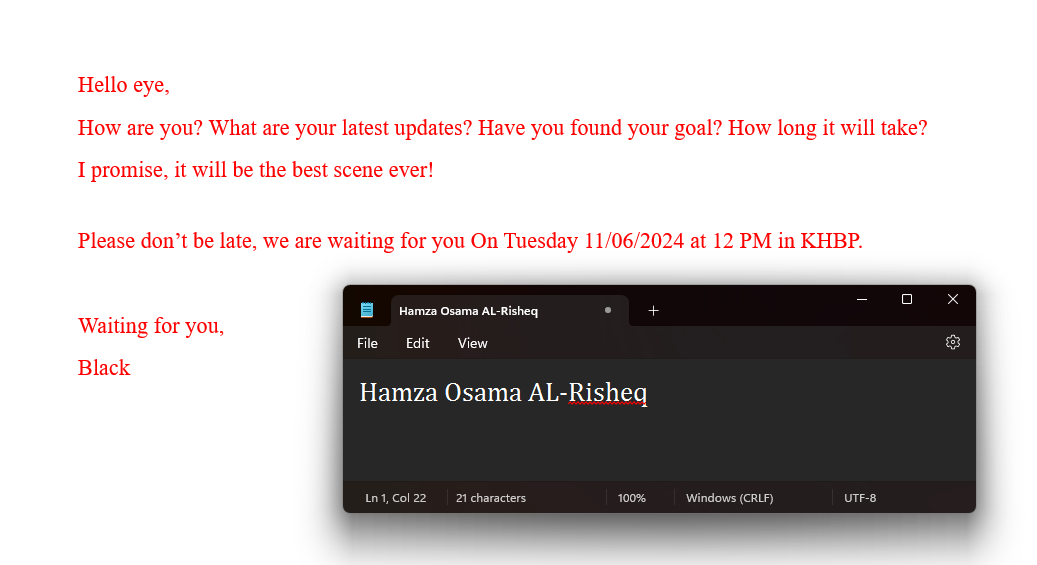


Figure 37: Docx After Coloring all the Content.

Based on Figure 37, we have discovered evidence indicating the location and time of BlackEagle's next crime. Therefore, we will conclude the investigation on EaglesEye's device. However, we will proceed to recover the USB to thoroughly search for any vital information it may contain.

**USB recovery:**

Firstly, I will open the USB using 010 editor and view the MBR entries table to understand the number of partitions and their types, view Figure 38.

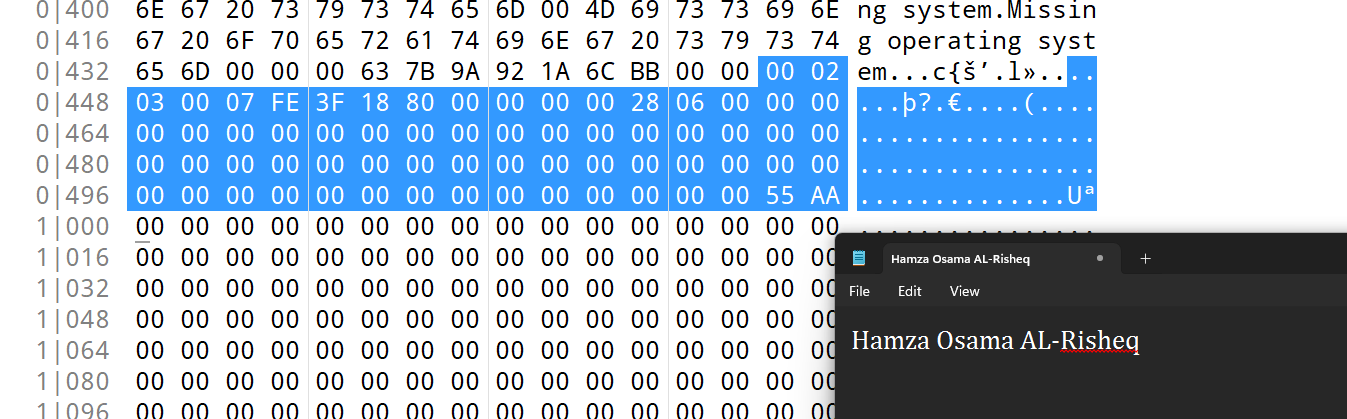


Figure 38: USB MBR Entries Table.

Based on the MBR table entries, we determined that there is one partition containing an NTFS file system. We then proceeded to the first sector of the NTFS to view the Volume Boot Record (VBR) or NTFS header, which is sector number 128 in decimal. However, we discovered that the VBR table has been deleted, as shown in Figure 39.

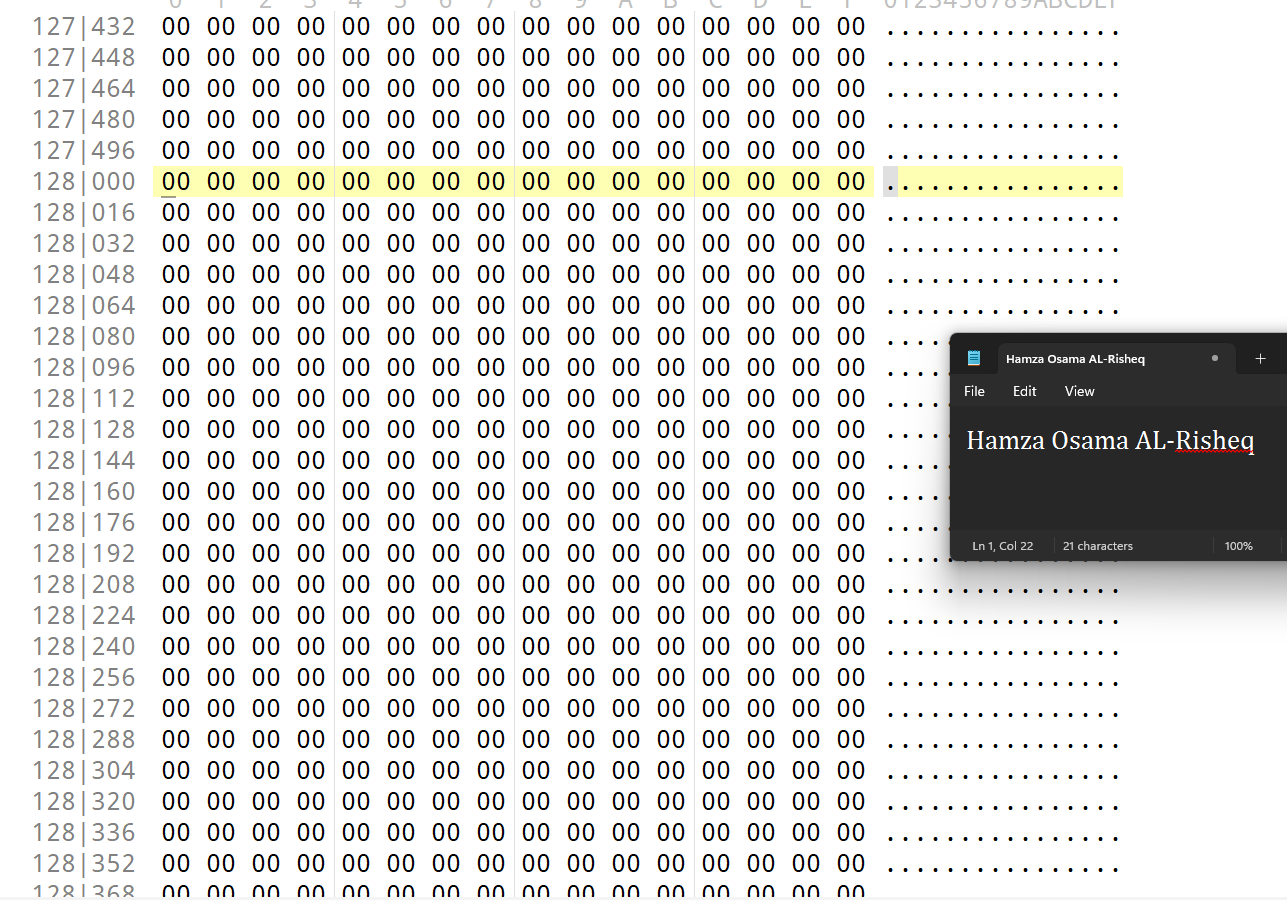


Figure 39: VBR Sector.

So, we will recover the VBR from the last sector in the partition. Subsequently, we can view the backup VBR in Figure 40. (We accessed the backup VBR by using the size of the partition). The size of partition is 403,456 sectors in decimal which means the last sector is 403,456.

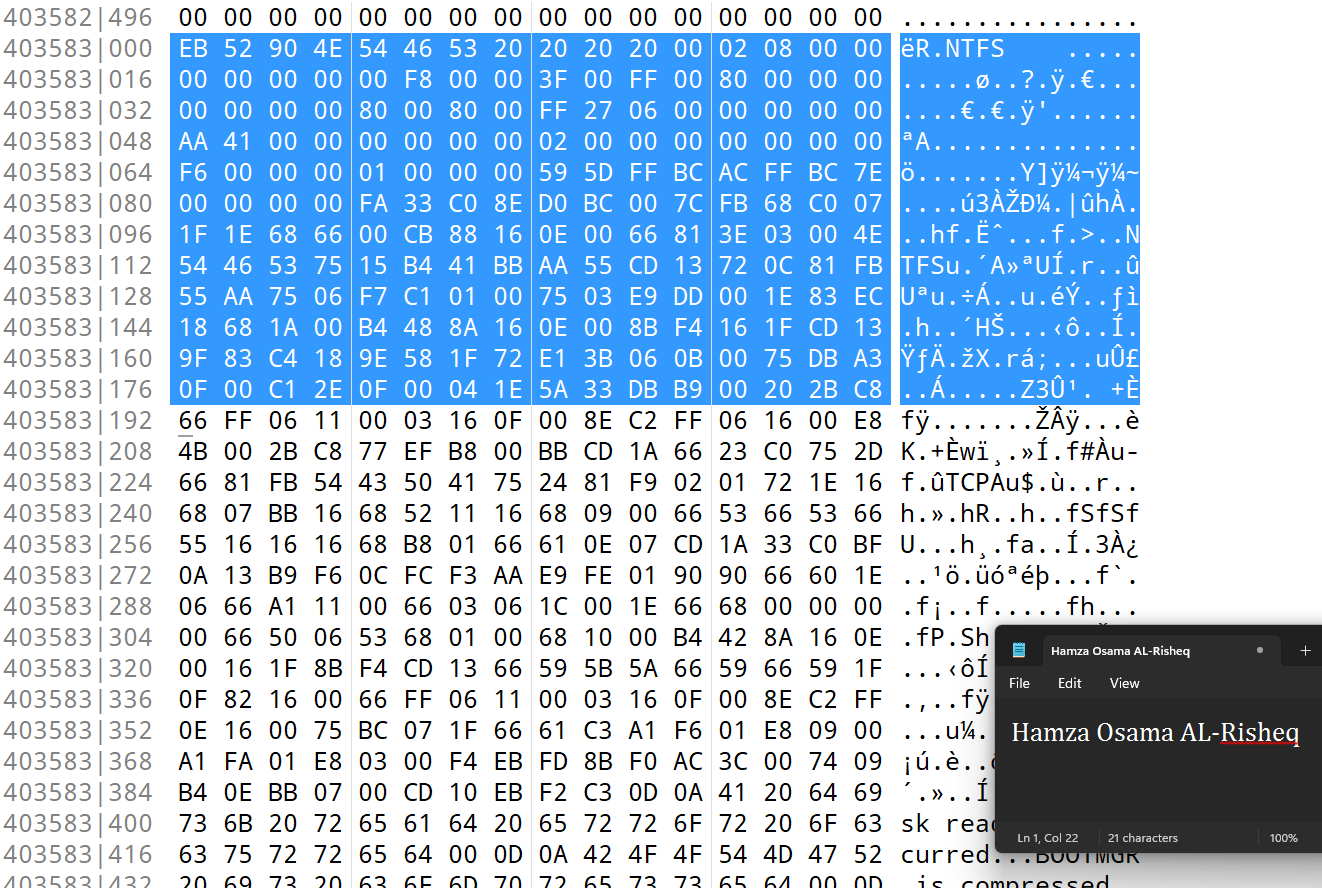


Figure 40: Backup VBR in Last Sector.

After copying the Backup VBR and pasting it in the VBR in the first NTFS. View Figure 41.

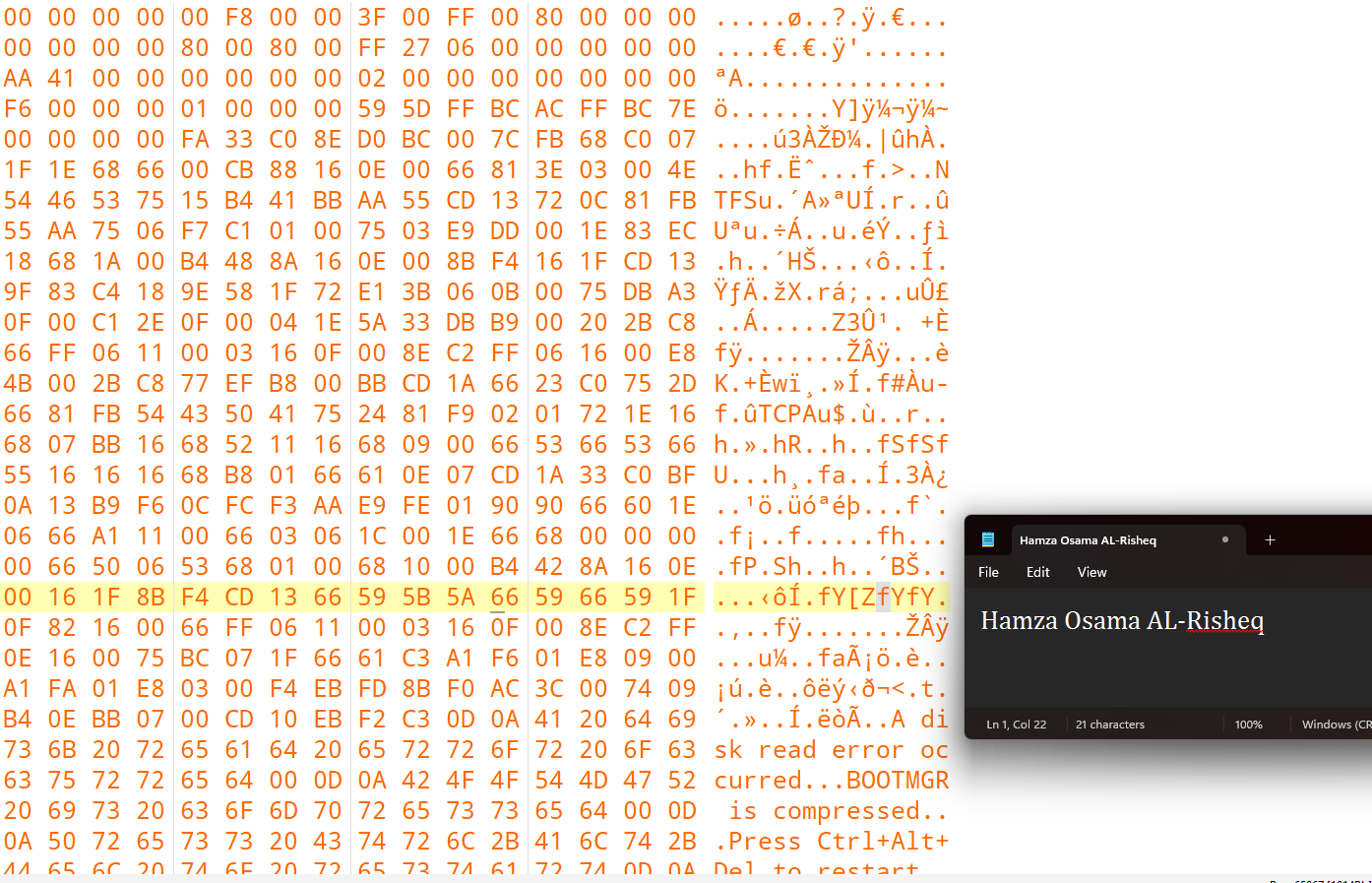


Figure 41: Pasting VBR.

Next, we opened the USB using FTK Imager to view the files. Please refer to Figure 42.

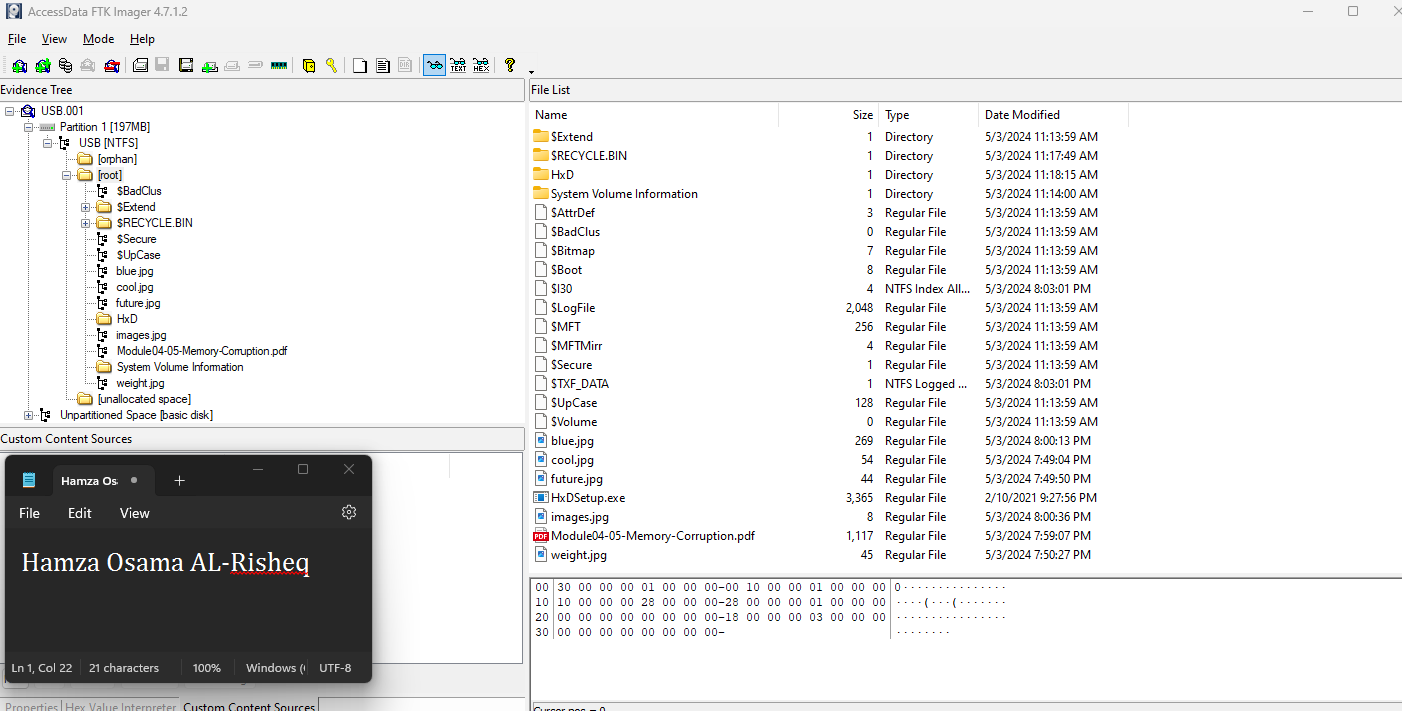


Figure 42: Recovered USB.

# 6. Conclusion

Through conducting comprehensive investigation in Eagle Eye’s Device and USB has yielded significant insights (HPKI-2024-001). Through rigorous forensic analysis of digital evidence, we have uncovered a complex network of communication that led to find out the location and time for BlackEAgle’s next crime,

Key findings point to an intentional effort to conceal data within digital artifacts, including file hiding and manipulation of timestamps. This deliberate attempt to obscure incriminating evidence underscores the gravity of the situation.

Notably, the discovery of abnormal pictures, particularly those depicting cages and husky dogs, raises questions about the motives behind the file overwrites and the potential significance of the concealed data.

Moving forward, these findings will inform law enforcement strategies aimed at disrupting the operations of BlackEagle and safeguarding our community. This investigation exemplifies our commitment to justice and security.

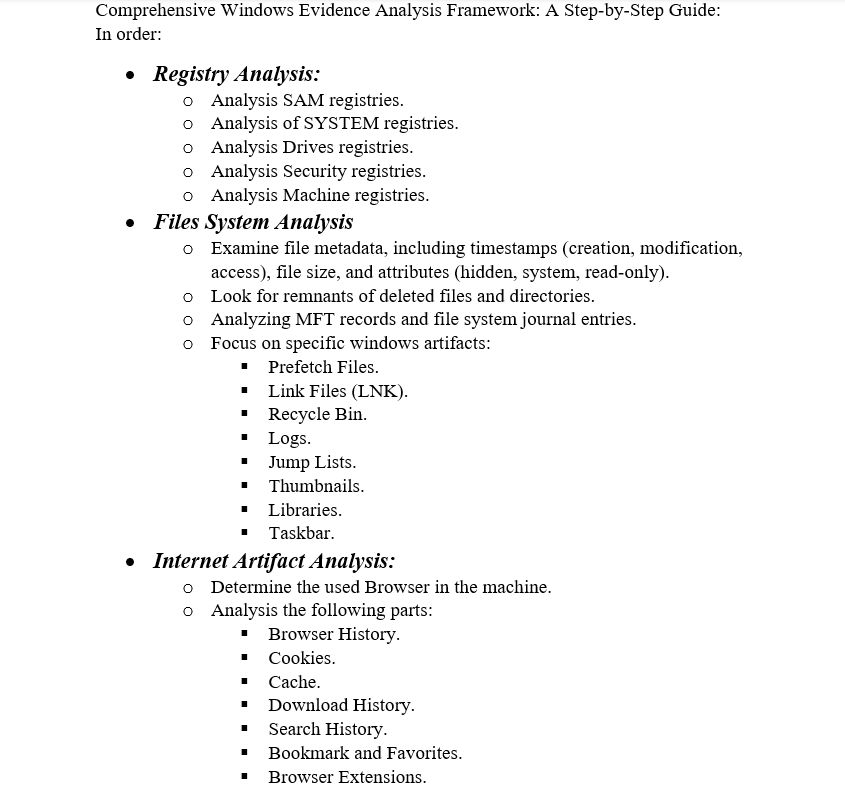
Finally, the evidence has been securely transmitted following established transaction protocols to the commanders of the metropolitan capital city for further action.

# 7. Exhibits

## ***COC (Chain of Custody)***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Capital City Digital Investigation Police Department**  This form is to be used only for one piece of evidence.  Fill out a sperate form for each piece of evidence | | | | | | |
| Case No: | | HPKI-2024-001 | | Unit Number: | HT\_1 | |
| Investigator: | | Hamza Osama AL-Risheq. | | | | |
| Number of Case: | | 1 | | | | |
| Location where evidence was obtained: | | Room 105, Random Forest Hotel, Shahid Hamza Street, Hebron City. | | | | |
| Item #ID | Description of evidence: | | Vendor Name: | | Model No/Serial No: | |
| 1 | A device with a Windows Operating system related to EAgleEye contains vital information that led to finding the location and time for Black Eagle's next crime. | | Asus | | 85966314H5HSH | |
| 2 | A corrupted flash drive after fixing it contained vital software that led to how the criminal (Eagle’s Eye) was hiding the data and information. | | Kingston | | 0VSKP1808332 | |
| Evidence Recovered by: | | OldGuard, KingH, WolfEyes, and PineappleFlavor. | | | Date & Time: | May 10, 2024  11:25 AM |
| Evidence Placed in Locker: | | Tableau TX1 | | | Date & Time: | May 10, 2024  11:25 AM |
| Evidence Processed By | | | Disposition of Evidence | | | Date/Time |
| OldGuard | | | Everything is sent securely with helping of police officers to the commanders of the metropolitan capital city. | | | May 10, 2024  11:25 AM |
| KingH | | |  | | |  |
| WolfEyes | | |  | | |  |
| PineappleFlavor | | |  | | |  |
|  | | |  | | |  |
|  | | |  | | |  |
|  | | |  | | |  |
|  | | |  | | |  |
|  | | |  | | |  |
|  | | |  | | |  |
|  | | | | | | Page\_1\_of\_1\_ |

## ***Appendix 1***



A close-up of a document

Description automatically generated

## ***Appendix 2***

|  |  |
| --- | --- |
| ***Artifact*** | ***Path*** |
| Jump List Files | C:\Users\User\ AppData\Roaming\Microsoft\Windows\Recent |
| Prefetch Files | C:\Windows\Prefetch |
| Recycle.Bin Folder | C:\$Recycle.Bin |
| Library Folder | C:\Users\User\AppData\Roaming\Microsoft\Windows\Libraries |
| Desktop Folder | C:\Users\User\Desktop |
| Downloads Folder | C:\Users\User\Downloads |

## ***Appendix 3***

|  |  |  |
| --- | --- | --- |
| ***File Data Type*** | ***Header Signature*** | ***Footer Signature*** |
| Docx, Pptx, XLSX | 50 4B 03 04 14 00 06 00 | 50 4B 05 06 followed by 18 bytes. |
| Png | 89 50 4E 47 0D 0A 1A 0A | 49 45 4E 44 AE 42 60 82 |
| Jfif | FF D8 FF E0 | FF D9 |
| Jpeg | FF D8 | FF D9 |

# 8. Revision History