L5 - Computer Forensics (ACCD5000)

END OF APRIL REPORT : TASK 1 & TASK 3

Mr. LE ROY-MEUNIER Maxime

L5 - Computer Forensics (ACCD5000) 1
END OF APRIL REPORT : TASK 1 & TASK 3 1
Task 1 : Digital Forensics Research Report 6
Introduction 6
Definitions and Historical Evolution 6
Distinctions Between Computer and Digital Forensics 6
Applications and Scope in Real-World Scenarios 6
Conclusion 7
Task 3 : Digital Forensics Investigate & Report : 9
Investigation Process in Computer Forensics 9
1. Roles and Responsibilities in the Investigation Team 9
2. Evidence Identification and Collection 9
3. Transport and Storage 10
4. Analysis and Reporting 10
5. Legal Review and Ethical Considerations 10
6. Conclusion and Testimony 10
Report from given evidence - Week 6 11
Step 1 : Downloading and extracting the disk Image. 11
Step 2 : Opening the disk image on Autopsy® : 13
Step 3 : Starting the investigation : 13
Conclusion 25
References 26
Other research techniques 27

Task 1 : Digital Forensics Research Report

Introduction

Digital forensics is simply the process of investigation and recovery of material found in digital devices, which are commonly related to computer crimes. Some people interchange the terms "computer forensics" and "digital forensics," yet there are differences between them. This paper is going to delve into these differences, historical development, scope, and applications of both beside providing examples from real-world cases.

Definitions and Historical Evolution

Digital Forensics is an area that has developed with the emergence of digital devices in our lives, during 1970-1990. It concerns the recovery, investigation, examination, and analysis of data found in digital devices after a cybercrime. A cybercrime is a crime committed through the internet / digital tools.

Computer Forensics is a subbranch of Digital Forensics. It concerns the investigation on computing devices only (Computers, Servers, Hard Drives recovery…).

Other subbranches exist, such as smartphone / mobile data forensics, network forensics, etc.

Distinctions Between Computer and Digital Forensics

While computer forensics confines its activities to computer data, digital forensics pervades a wider class of digital devices. Its general scope has extended to mobile device forensics, network forensics, and even forensic data analysis since digital data gets used and stored in many different ways. General digital Forensics investigations could be carried out in crime scene that affects more than one subbranches (smartphones, hard drives, computers, network systems, IoT,).

Applications and Scope in Real-World Scenarios

Computer Forensics were used in cases involving traditional computer crimes like hacking, fraud, and other cybercrimes. For example, the BTK Killer was apprehended when metadata from deleted computer files linked him to letters sent to police (ABC News, 2019).

Digital forensics tools are frequently used to investigate cases involving the exploitation of children. For instance, in the case of "Operation Pacifier," the FBI used digital forensic techniques to infiltrate a child pornography website on the dark web, leading to the identification and prosecution of numerous offenders.

Digital forensics is critical in investigating terrorist activities, including communication, recruitment, and planning conducted through digital channels. For example, in the investigation of the 2015 San Bernardino shooting, the FBI used digital evidence from the perpetrator's devices to uncover connections to terrorist groups.

Conclusion

The evolution from computer to digital forensics mirrors the advancement of technology in society. Each discipline, while related, serves specific purposes depending on the nature of the investigation. As technology continues to evolve, so too will the strategies and methods of digital forensic investigators, remaining an indispensable tool in the pursuit of justice.

Task 3 : Digital Forensics Investigate & Report :

Investigation Process in Computer Forensics

The investigation process in computer forensics is critical for ensuring the integrity, legality, and admissibility of evidence in legal proceedings. It involves meticulous steps from initial evidence collection to detailed analysis and courtroom presentation. Here one outline the key phases of the process, focusing on the concept of the chain of custody and its crucial role.

1. Roles and Responsibilities in the Investigation Team

Key Roles

- Photographer: Captures the crime scene and physical evidence using photography or imaging techniques, ensuring accuracy and avoiding scene tampering.
- Investigator: Conducts interviews, collects information, and retrieves digital evidence, ensuring its integrity and legal admissibility.
- Incident Analyzer: Assesses the incident's impact, identifies potential evidence sources, and prioritizes the investigative efforts.
- Witness: Provides accurate and consistent courtroom testimony about the evidence and investigation process.
- Documenter: Maintains detailed logs of evidence collection, analysis, and chain of custody.
- Examiner: Analyzes digital evidence while preserving its integrity, following forensic protocols to ensure evidence admissibility.
- Incident Responder: Secures the scene, collects evidence promptly, and helps prevent further incident or tampering.
- Manager: Guides the investigation, ensuring compliance with legal standards and efficient management of resources.

Legal Considerations

- All team members must have clear knowledge of the legal constraints and privileges related to handling digital evidence, including adherence to privacy laws.

2. Evidence Identification and Collection

Procedures

- Initial Assessment: Identify all potential digital evidence sources at the crime scene.
- Documentation: Record the location and condition of each piece of evidence.
- Evidence Collection: Use appropriate tools and methods to collect evidence while maintaining its integrity.

Chain of Custody

The chain of custody is a documentation process that tracks the movement and handling of evidence from the time it is collected until it is presented in court. It serves to establish the integrity and security of evidence by providing a documented history of who handled it, when, and under what circumstances.

Implementation: Document each transfer of evidence, from the crime scene to the lab and eventually to the courtroom, including every person who handled it, the purpose of handling, and any changes to or observations of the evidence.

3. Transport and Storage

- Secure Transport: Use protective containers and secure transportation methods to transfer evidence to the forensics lab, minimizing the risk of damage or tampering.
- Storage: Store evidence in a controlled environment to prevent unauthorized access or degradation.

4. Analysis and Reporting

- Detailed Examination: Use forensic tools to analyze the evidence within the controlled lab environment.
- Ongoing Documentation: Maintain thorough records of all analytical processes and findings, updating the chain of custody with any new interactions with the evidence.

5. Legal Review and Ethical Considerations

- Discuss investigative processes and findings with the team to ensure a thorough and unbiased approach.
- Implement quality assurance measures to verify the investigation's accuracy and compliance with legal and ethical standards.

6. Conclusion and Testimony

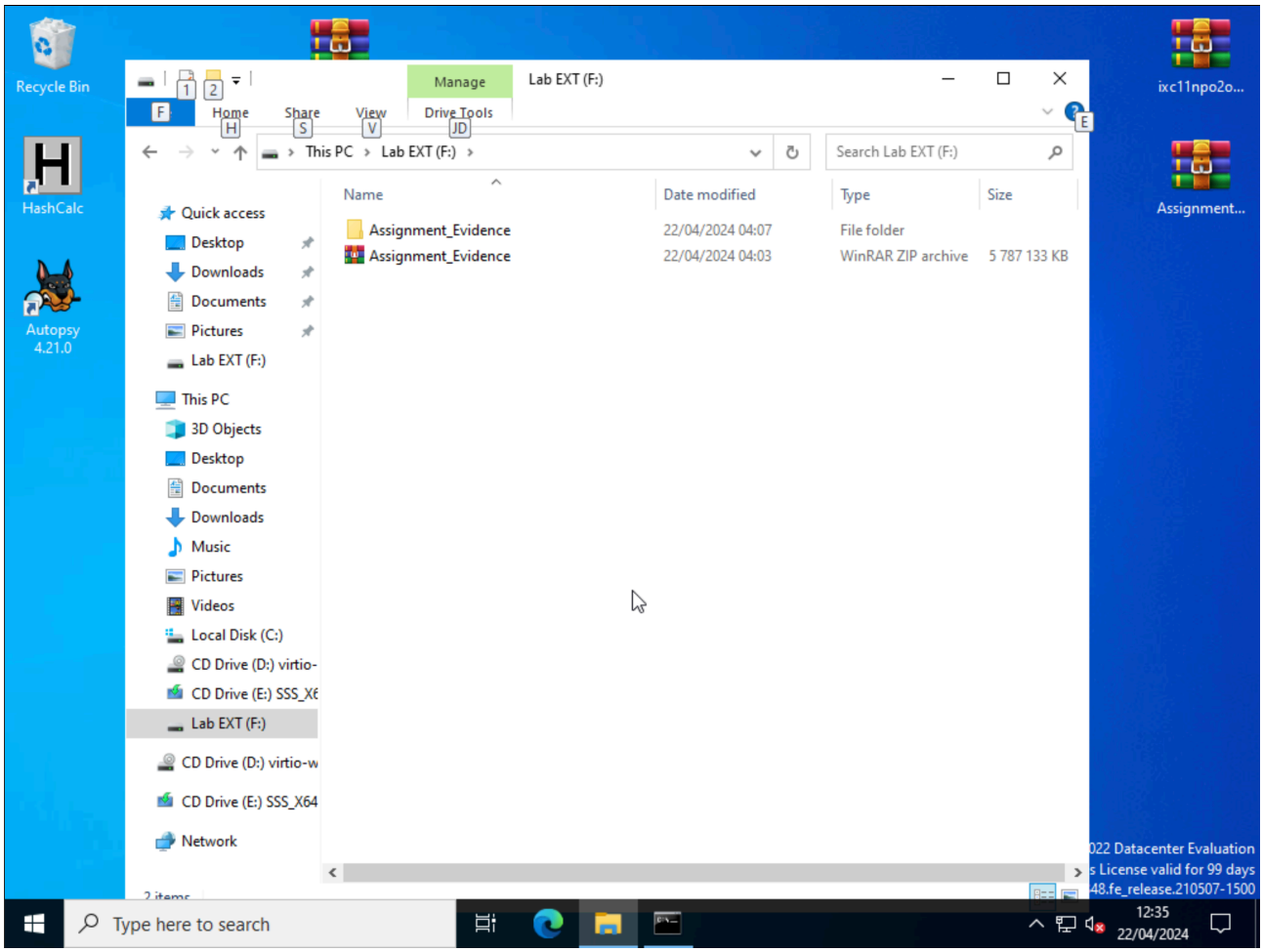
- Reporting: Prepare comprehensive reports detailing the investigation, findings, and the relevance of the evidence.
- Testimony: Ensure that testimonies provided in court are based on the documented evidence and fully consistent with the chain of custody records.

Report from given evidence - Week 6

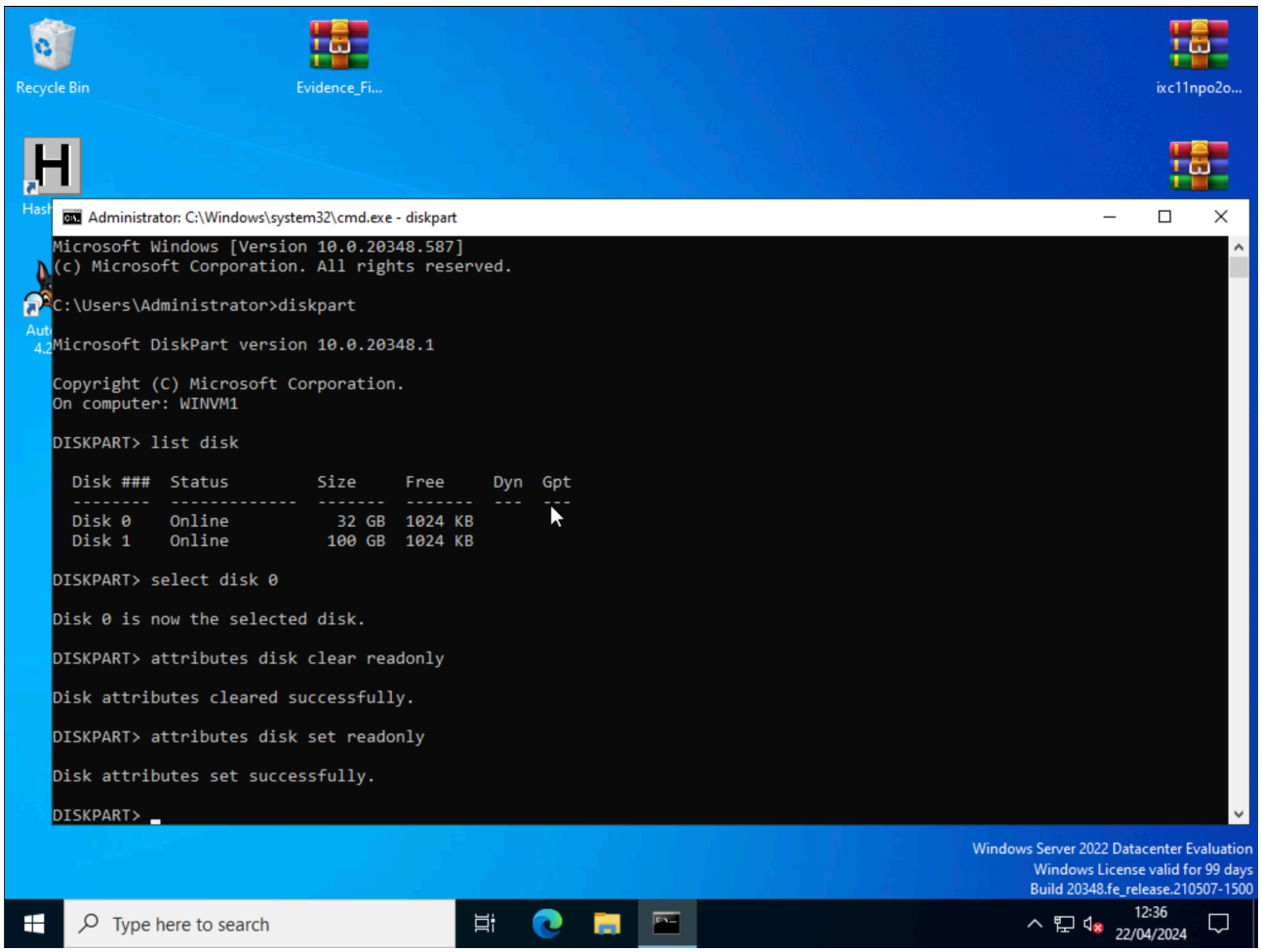
The evidence was originally disposed on an external hard-drive. Thanks to a student from the lecture, the disk image has been uploaded on the cloud so one can separately and easily upload it on a homelab (Windows Server Virtual Machine on Proxmox hypervisor)

Step 1 : Downloading and extracting the disk Image.

A ZIP archive is now available. We extract it on an external drive, then one lock / write protect it so any lecture doesn't affect the integrity of the evidences.



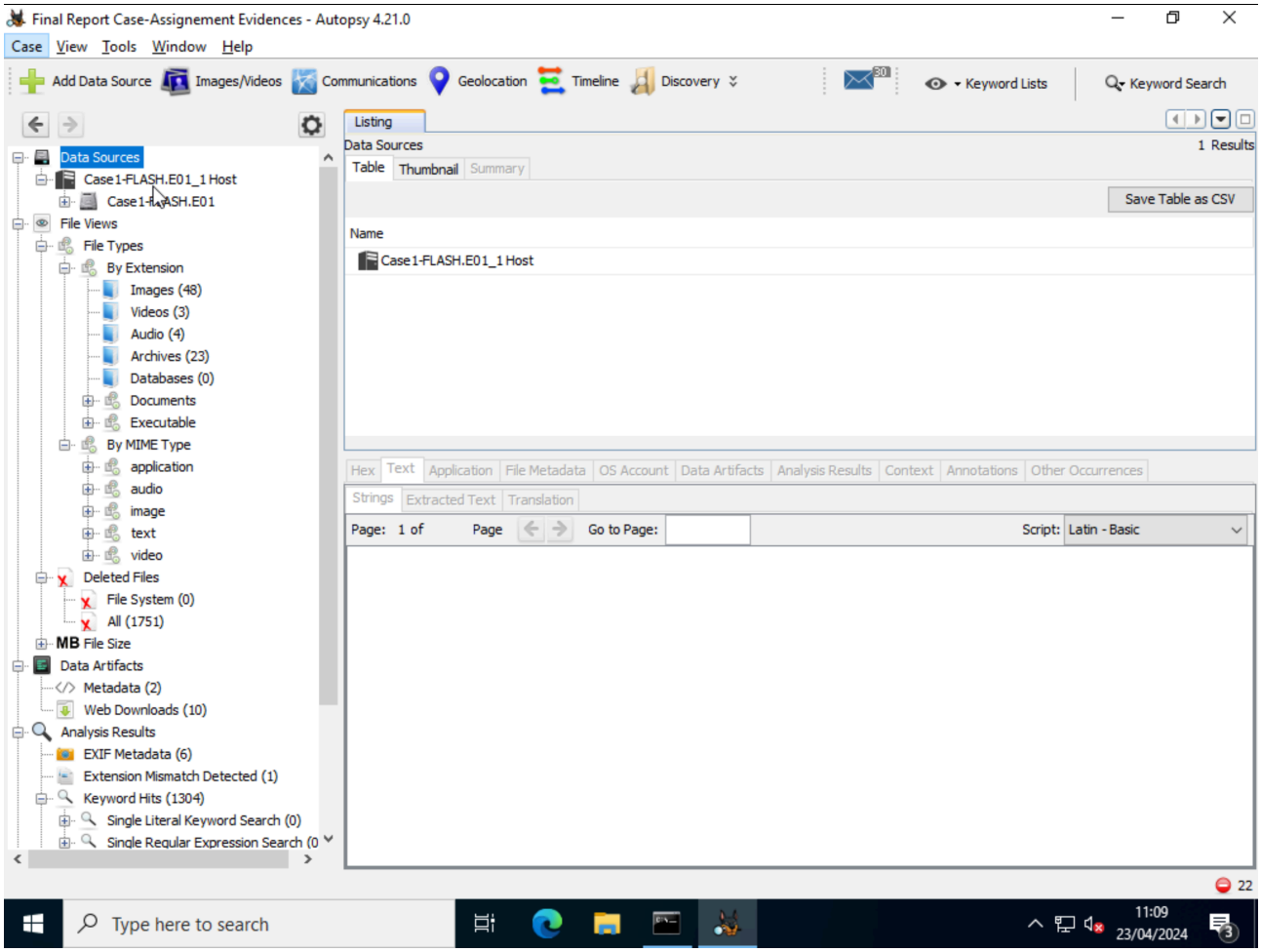
Extracting the evidence archive



Locking external disk with diskpart, where evidence is stored

Step 2 : Opening the disk image on Autopsy® :

The recovery took around 45 min to finish, as the image disk was divided in several parts.

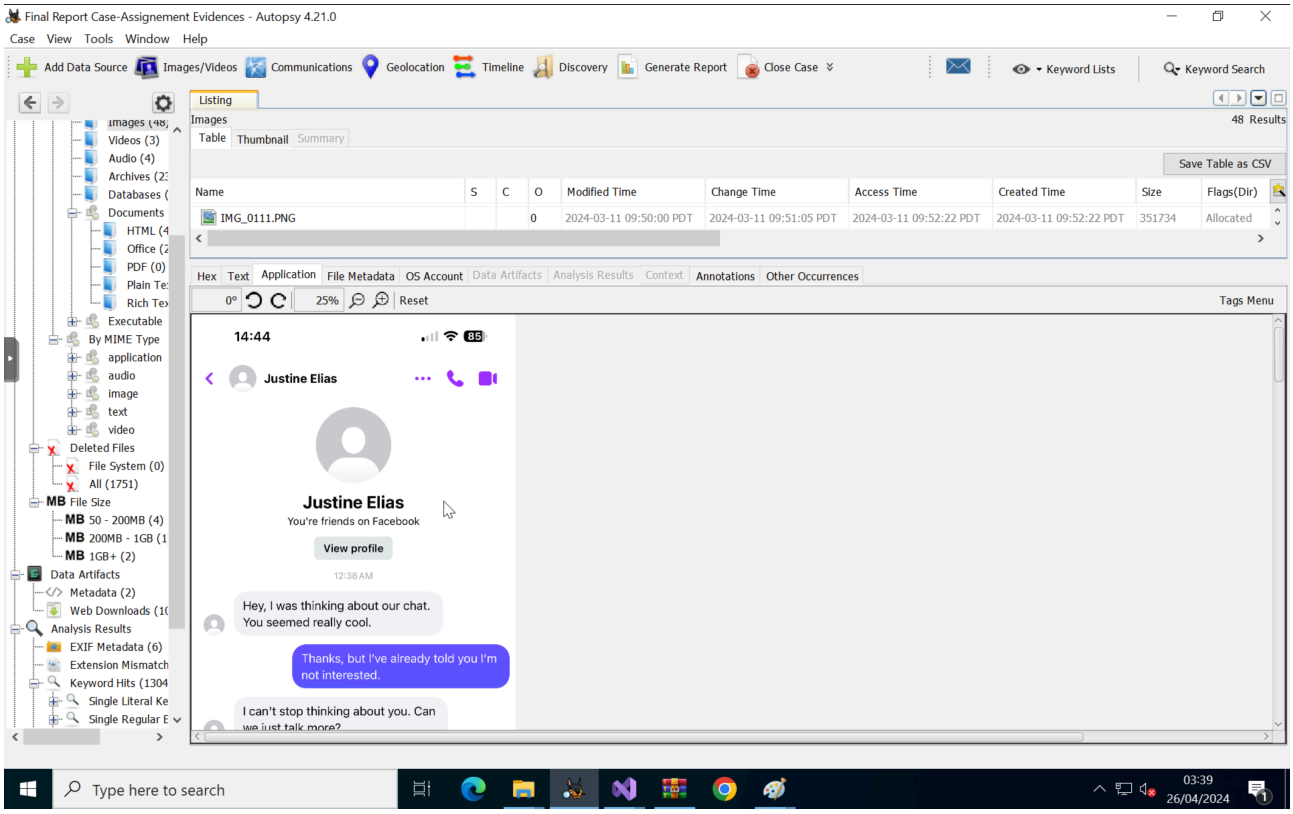


Autopsy® Recovery finished without errors / locks

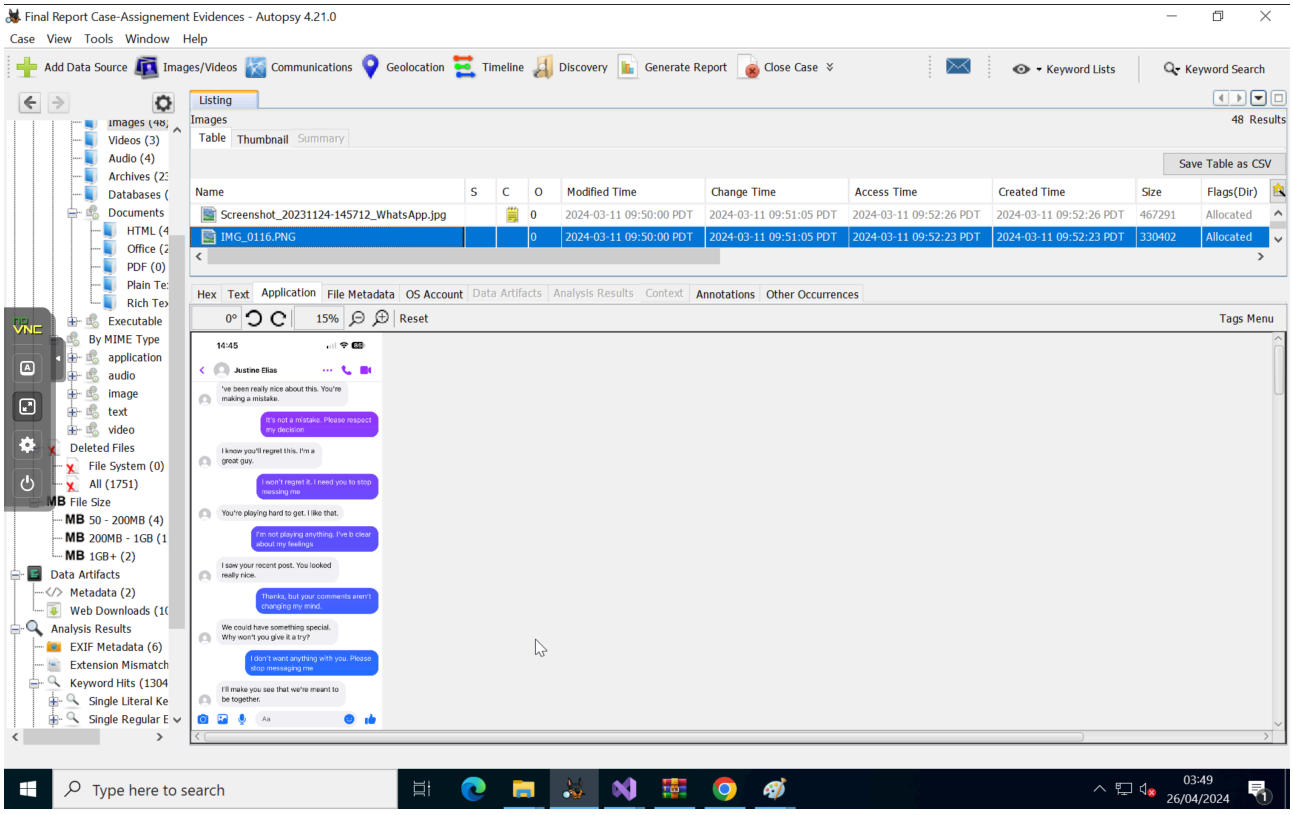
Step 3 : Starting the investigation :

As Autopsy® shows, a lot of files are available for direct opening.
For this investigation, it has been recovered the 48 images, a ZIP archive, a video, and a mail/contact database.

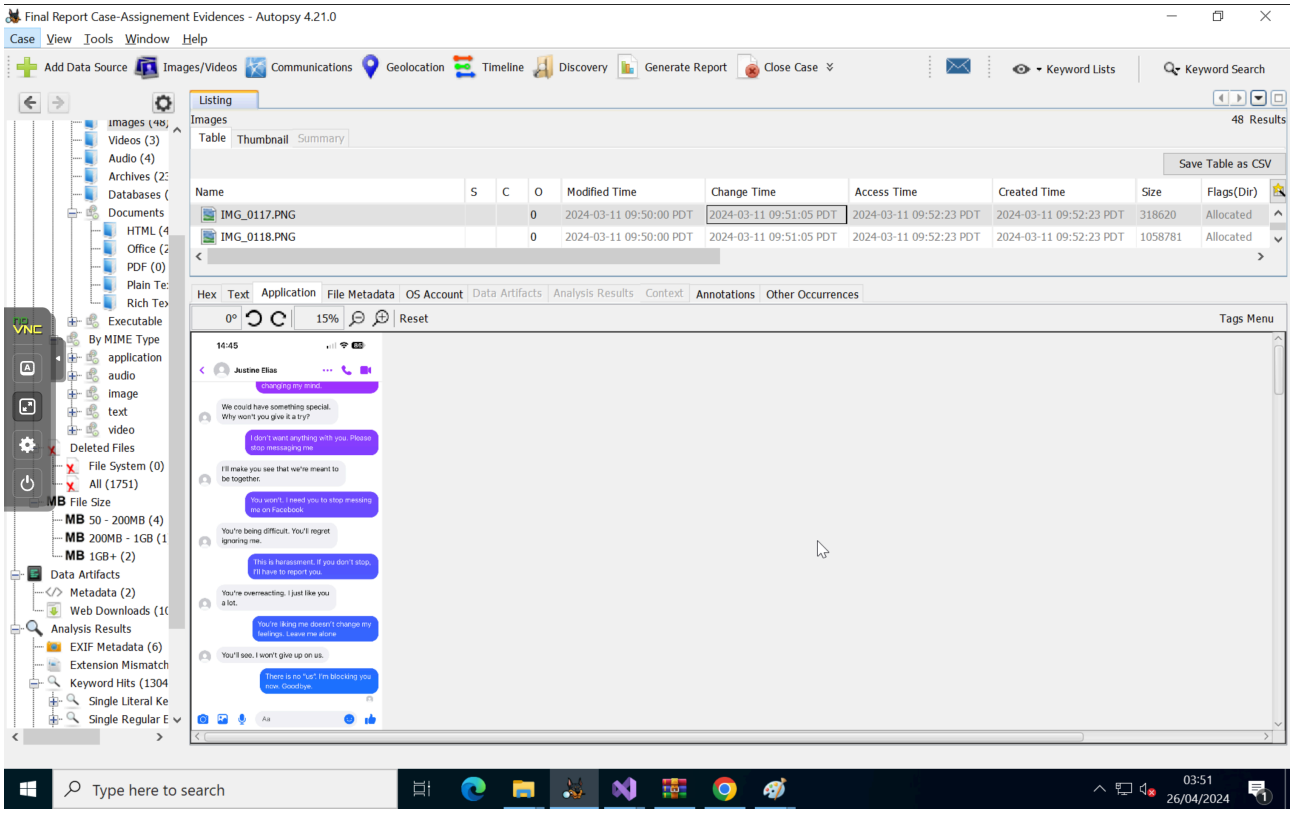
Discovering what is the case :
By analysing conversation screenshots, one understand that a Certain Justine Elias is harassing the victim to force her in a relationship. He threatens to post AI generated explicit content in her Instagram page, at the end.



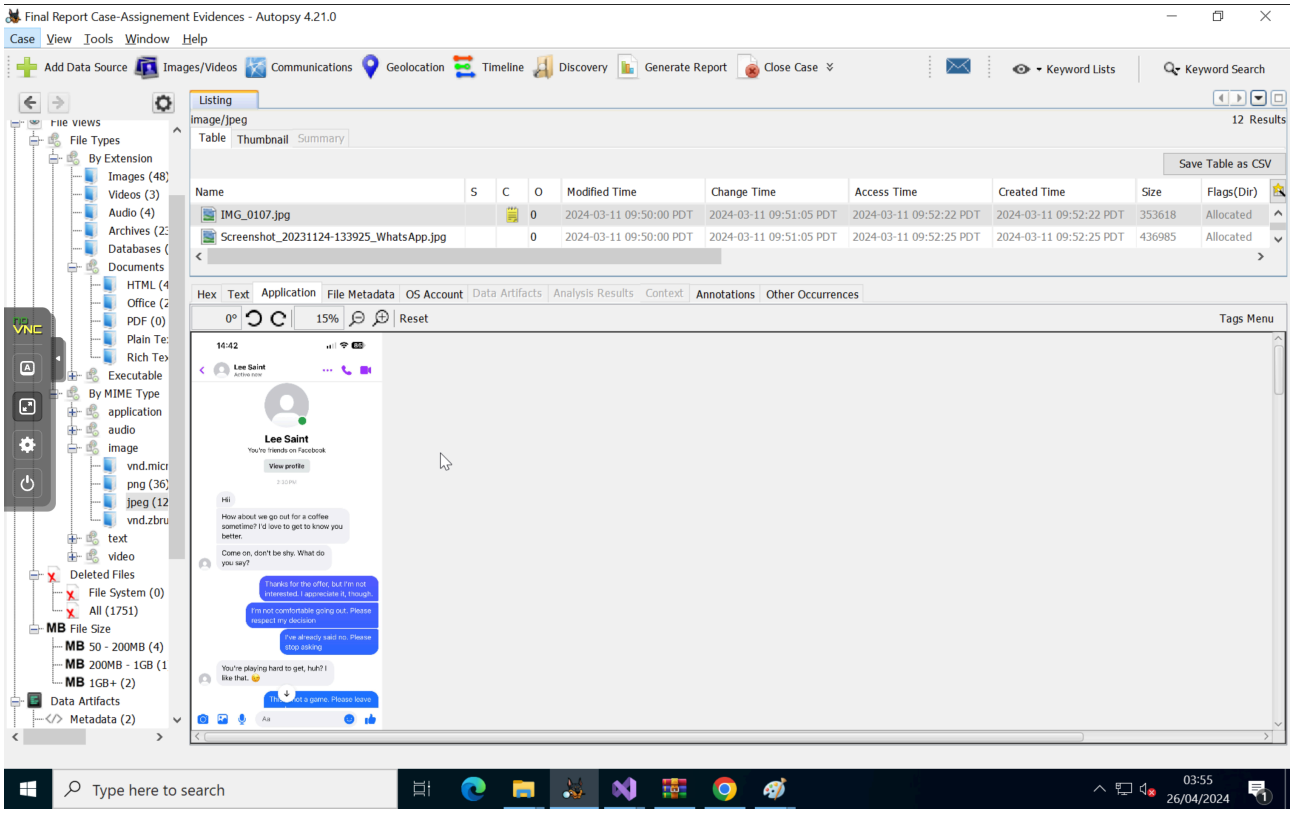
Not interested



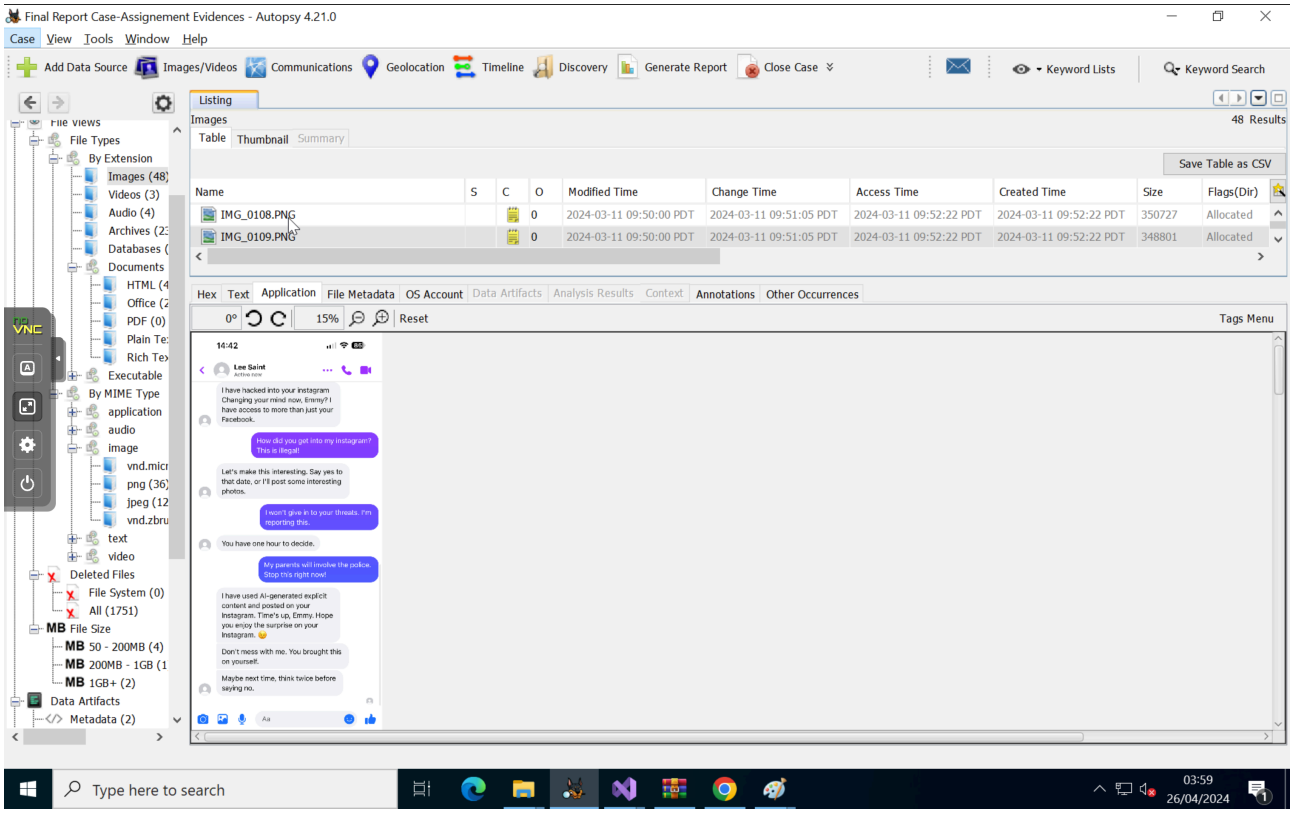
Threats by Justine Elias



She is blocking Justine Elias



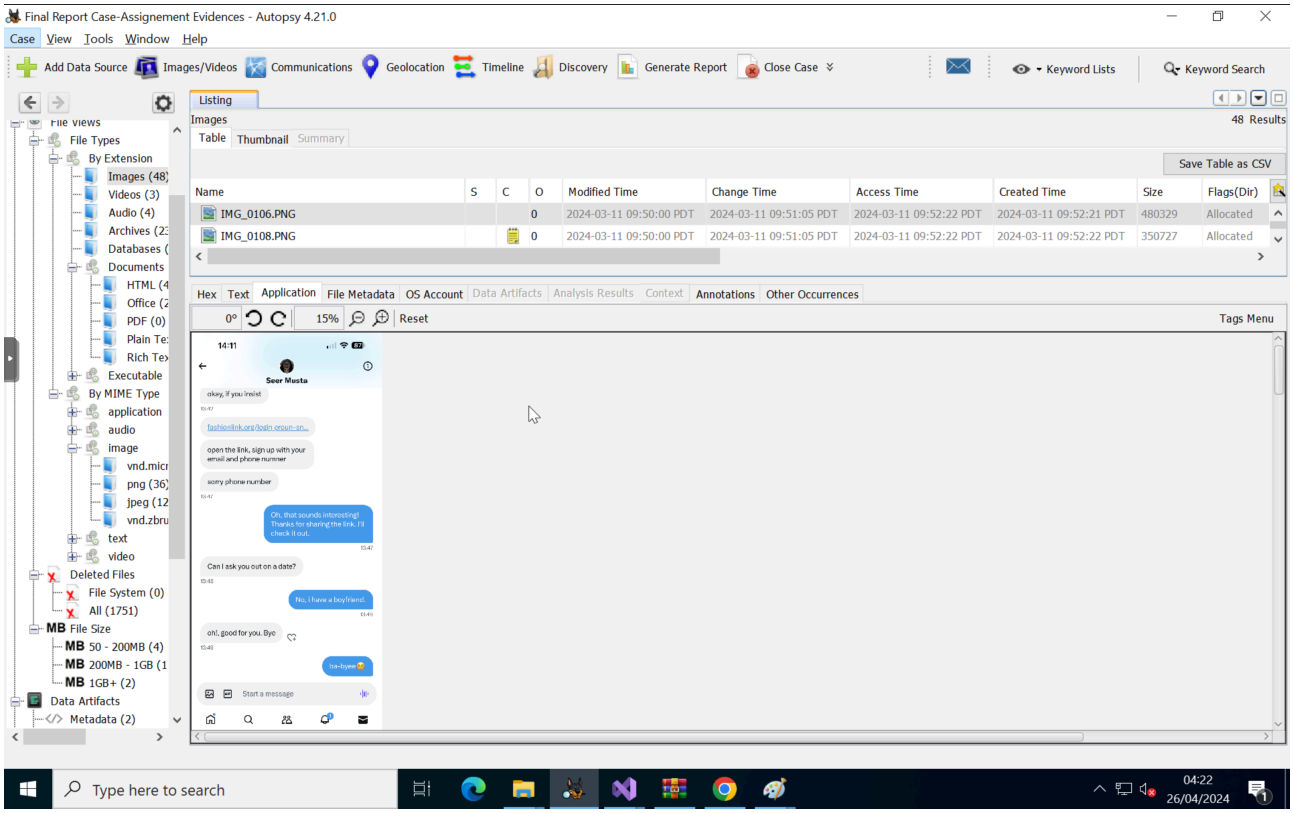
We can suppose that Justine Elias is coming back with an other account



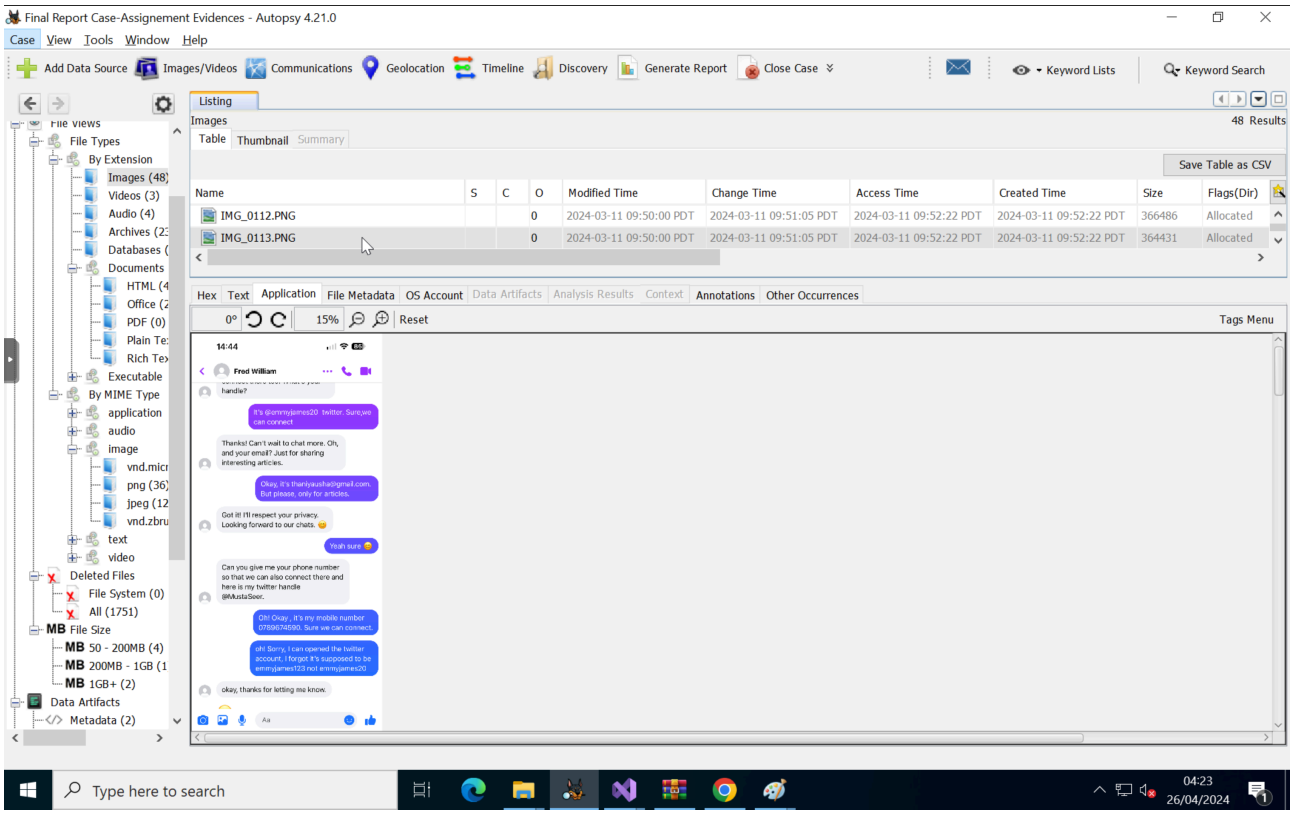
AI Threatening. Hacked accounts on several platforms.

But the question is, how did he obtain access to these accounts ?

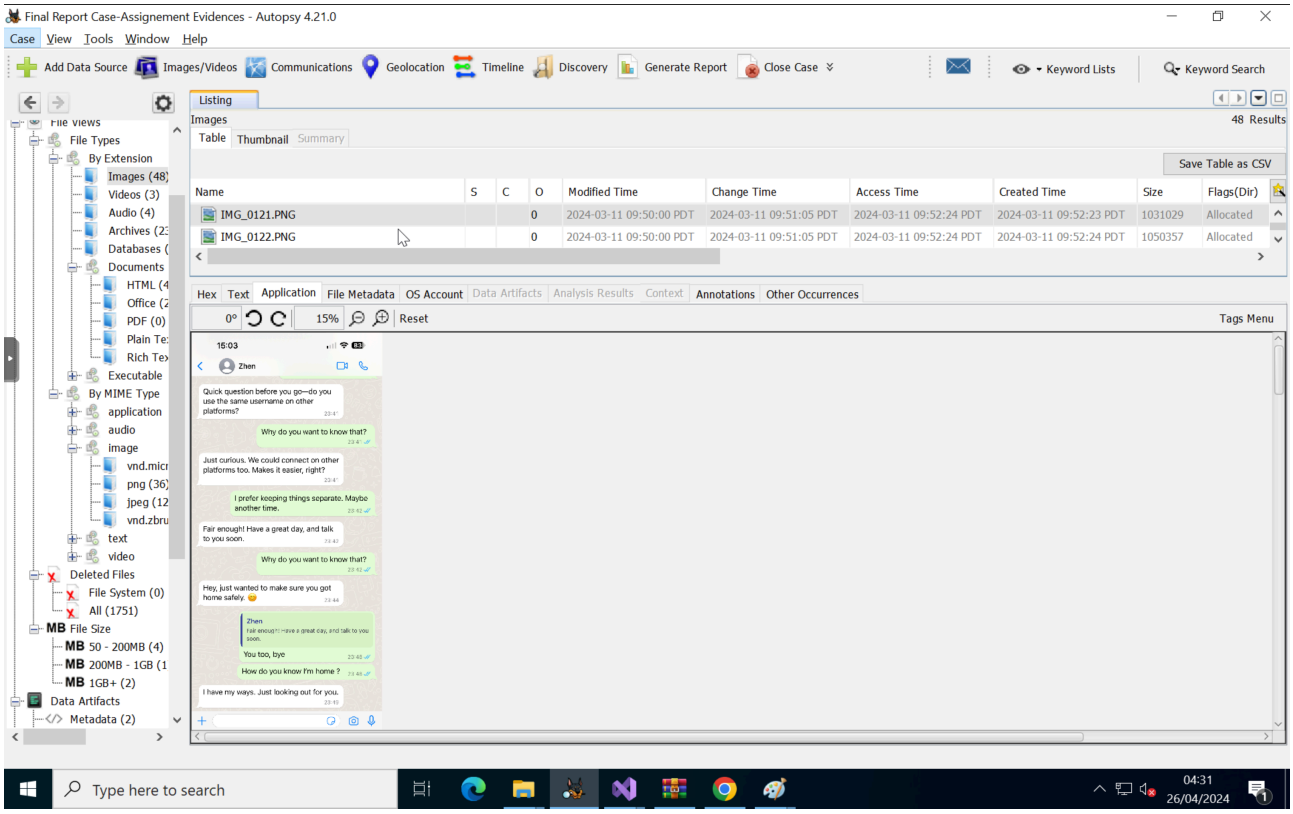
Well, one suppose that the other conversations on Twitter, Facebook, and whatsapp let him collect data (emails, telephone number, hack via url on twitter).



Suspicious Link on Twitter



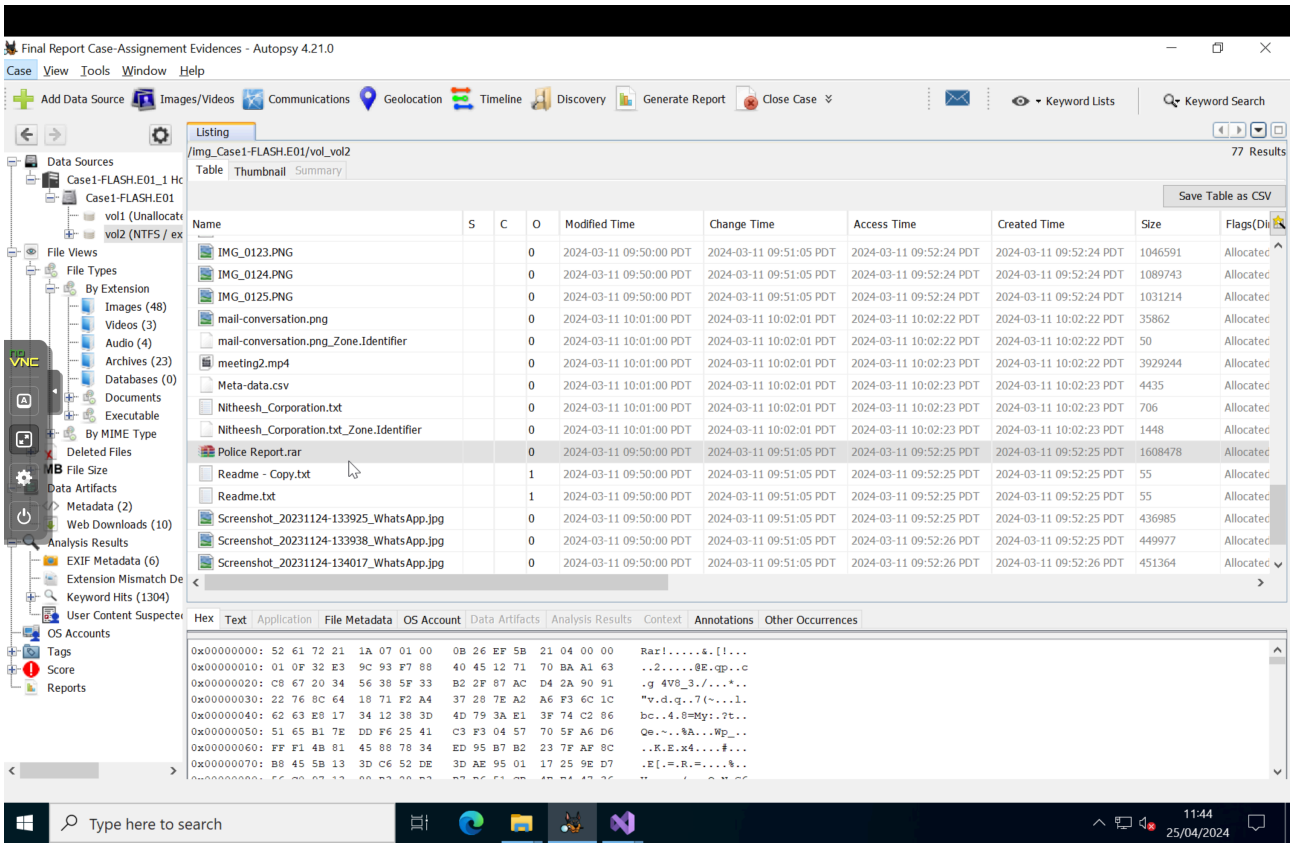
Gathering emails and phone numbers (via Messenger / Facebook)



Stalking home

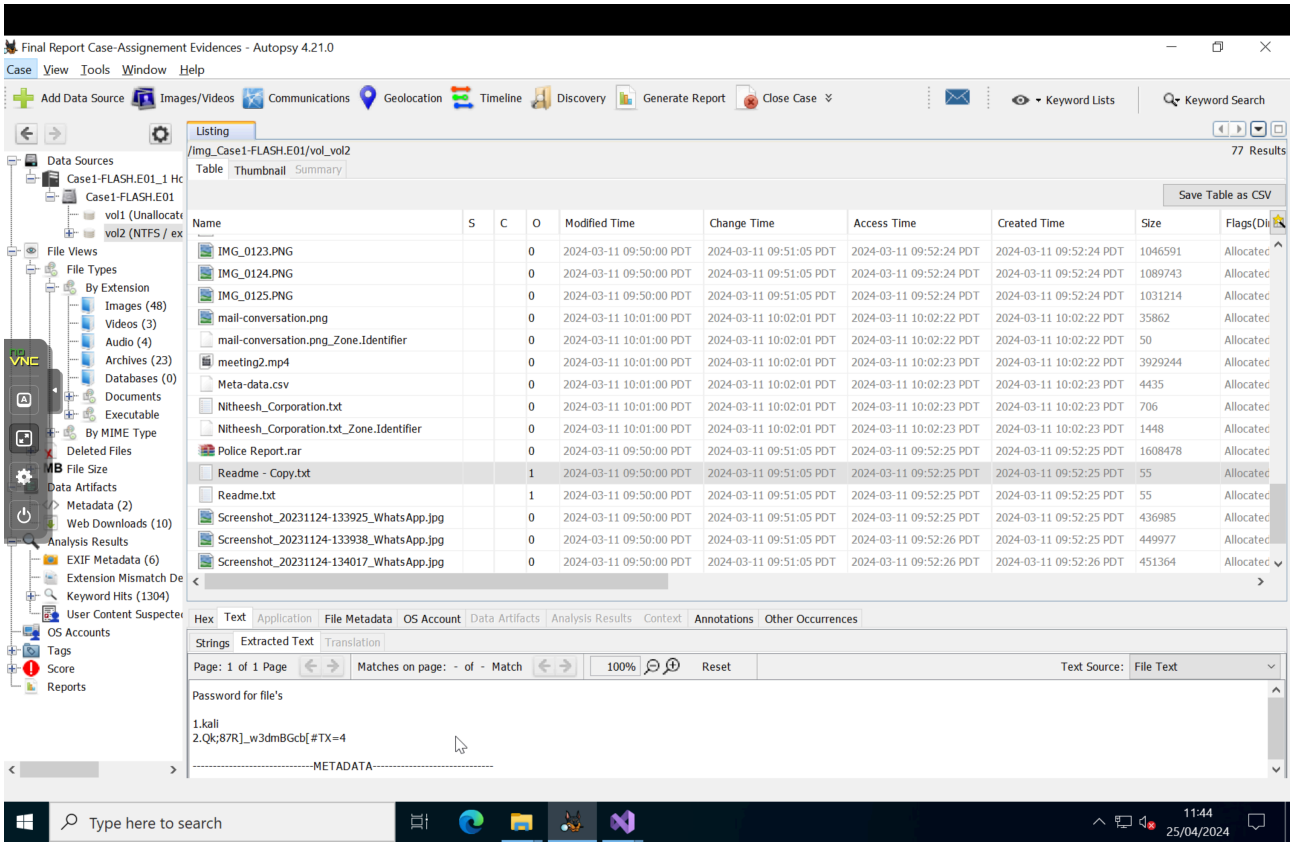
Hidden Police Report :

By searching on the evidence, one discovered a .rar (WinRAR) archive by the name of « police report.rar »

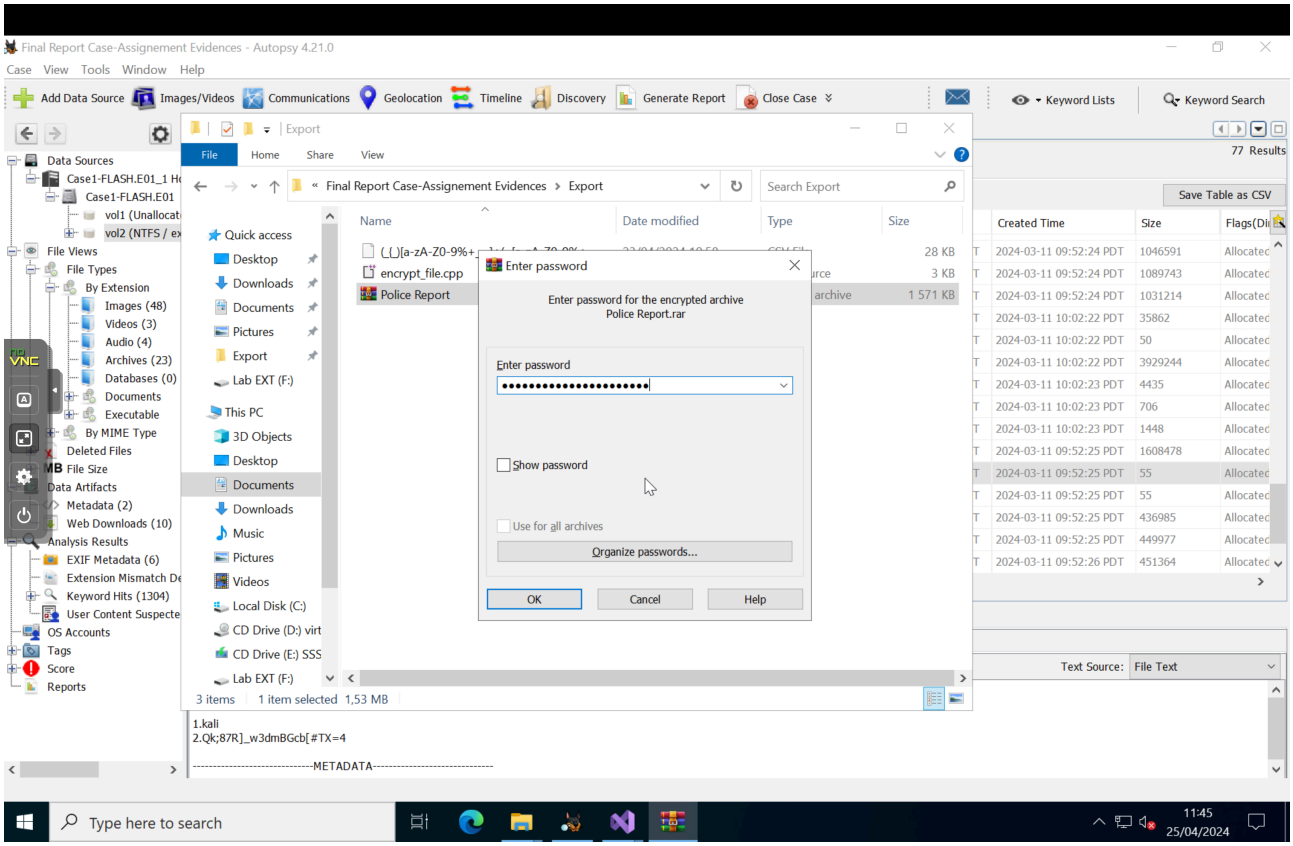


Finding the archive

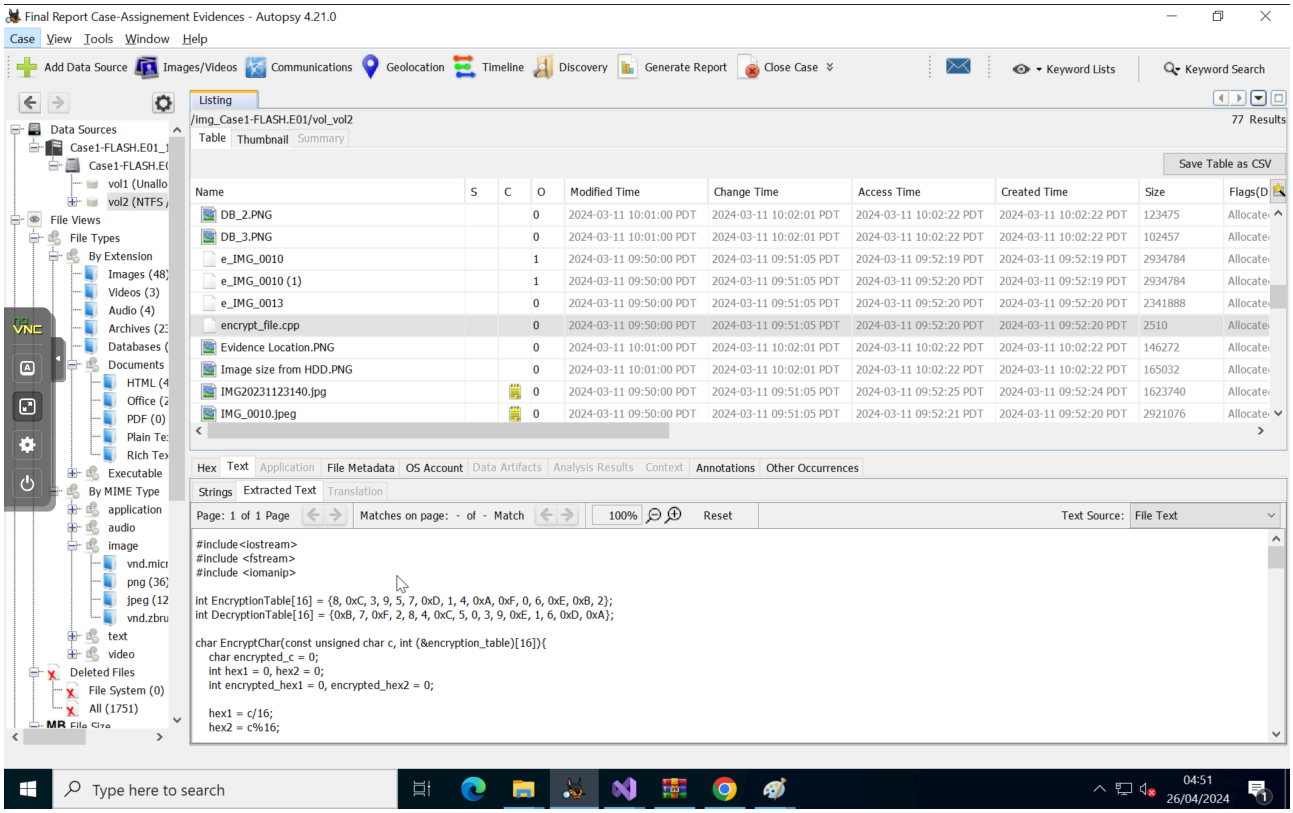
The archive was Password protected. We found the password in « readme.txt »



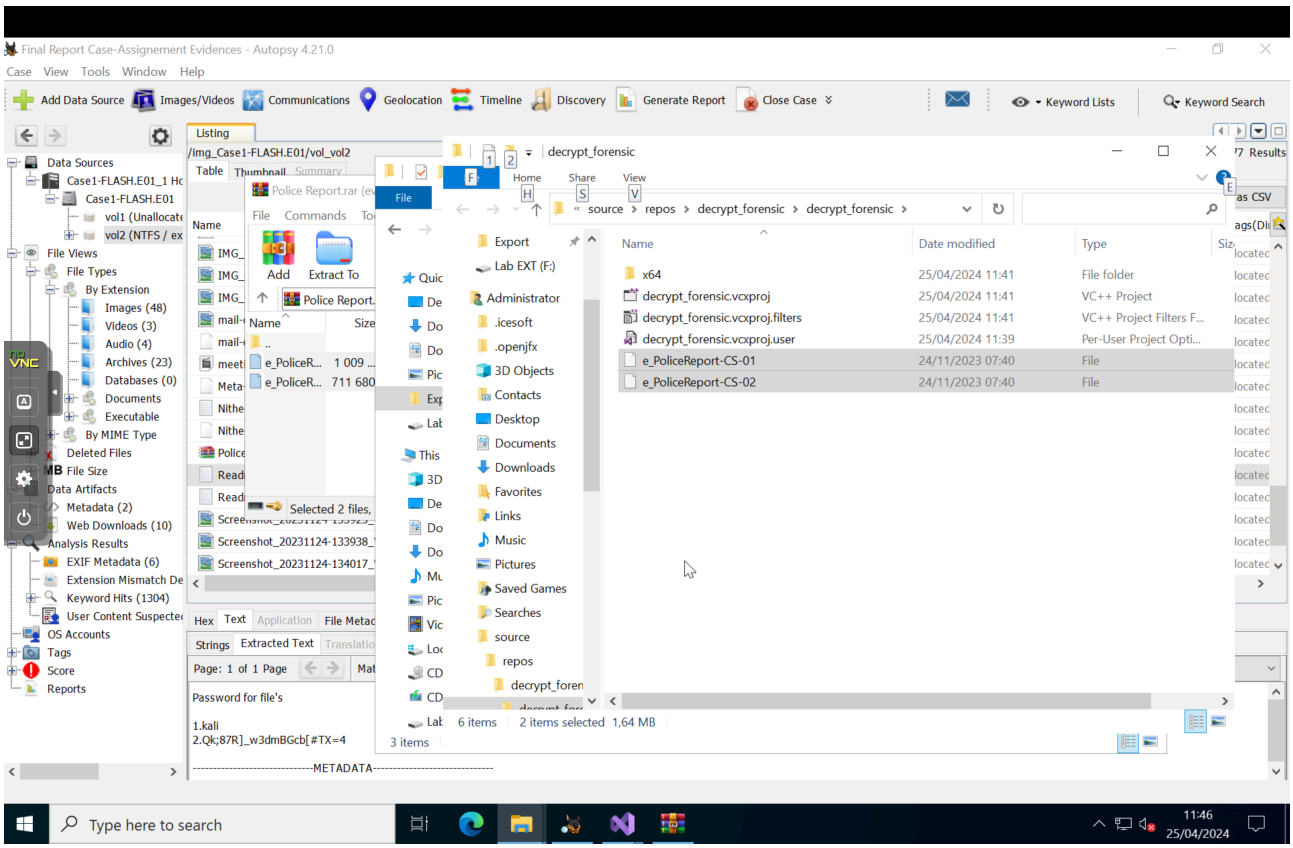
The two passwords were tested. The second one worked



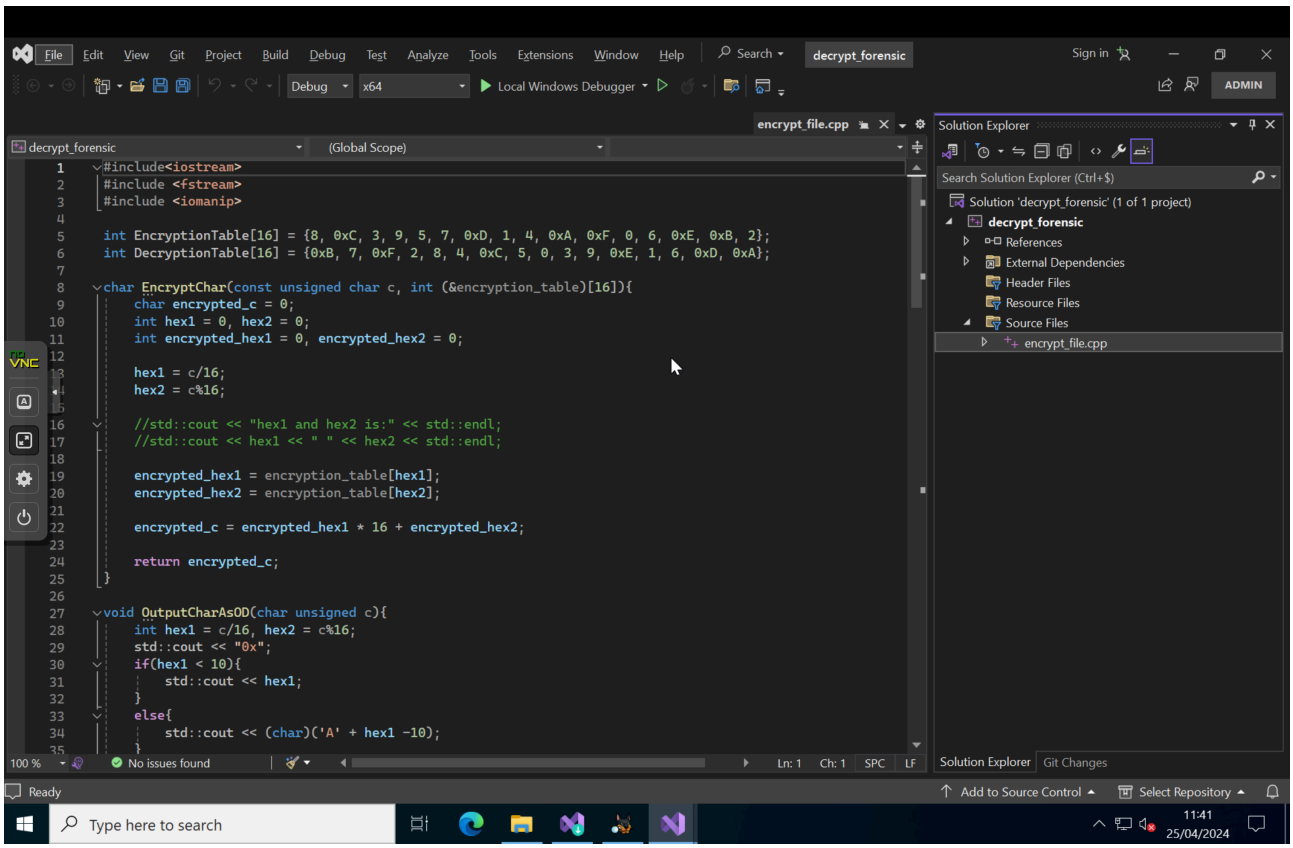
Two non-readable files were on the archive. After some research on the disk image with Autopsy®, one found a C++ program that decrypts files. It has been extracted, built, and run. Two images were finally decrypted and found.



Program found with Autopsy®



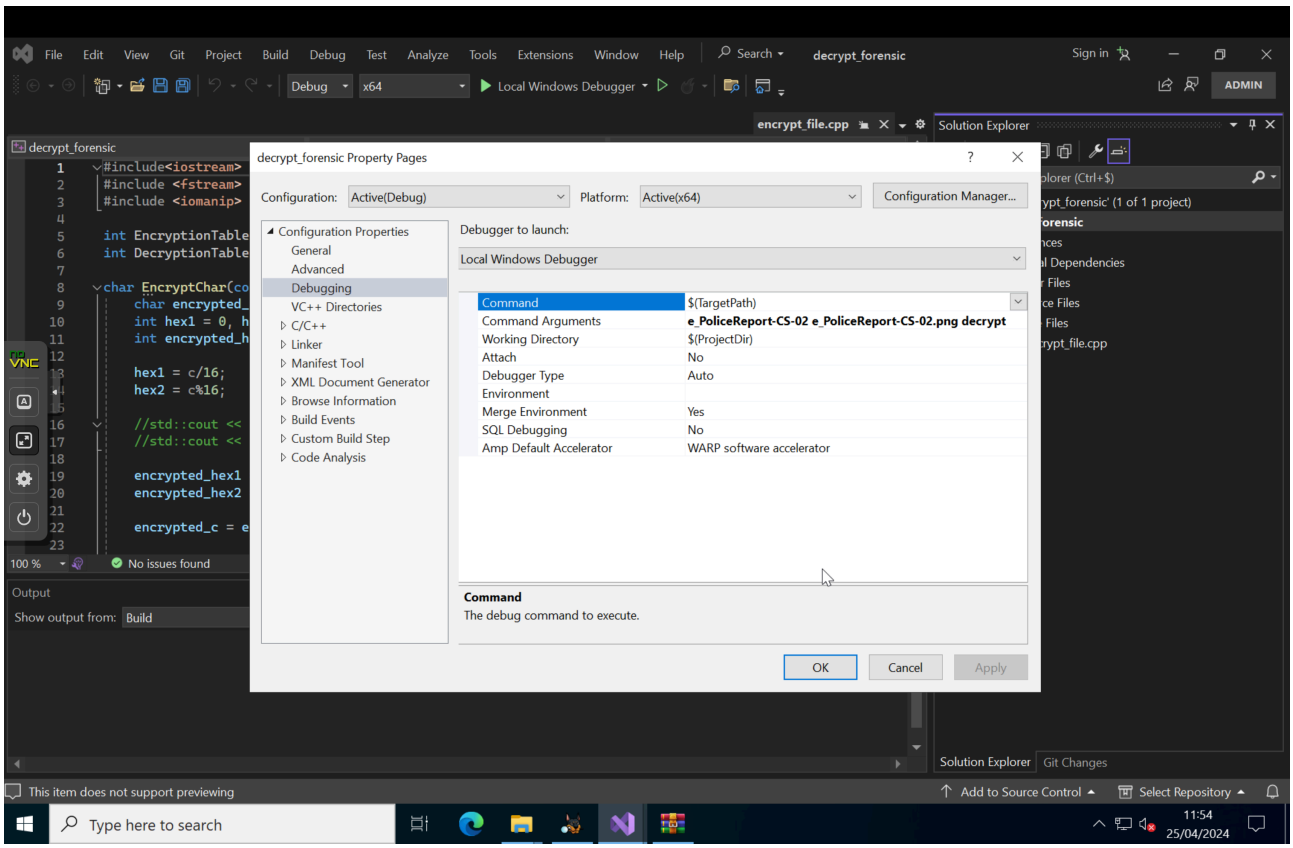
The two encrypted files and the program built with VSCode



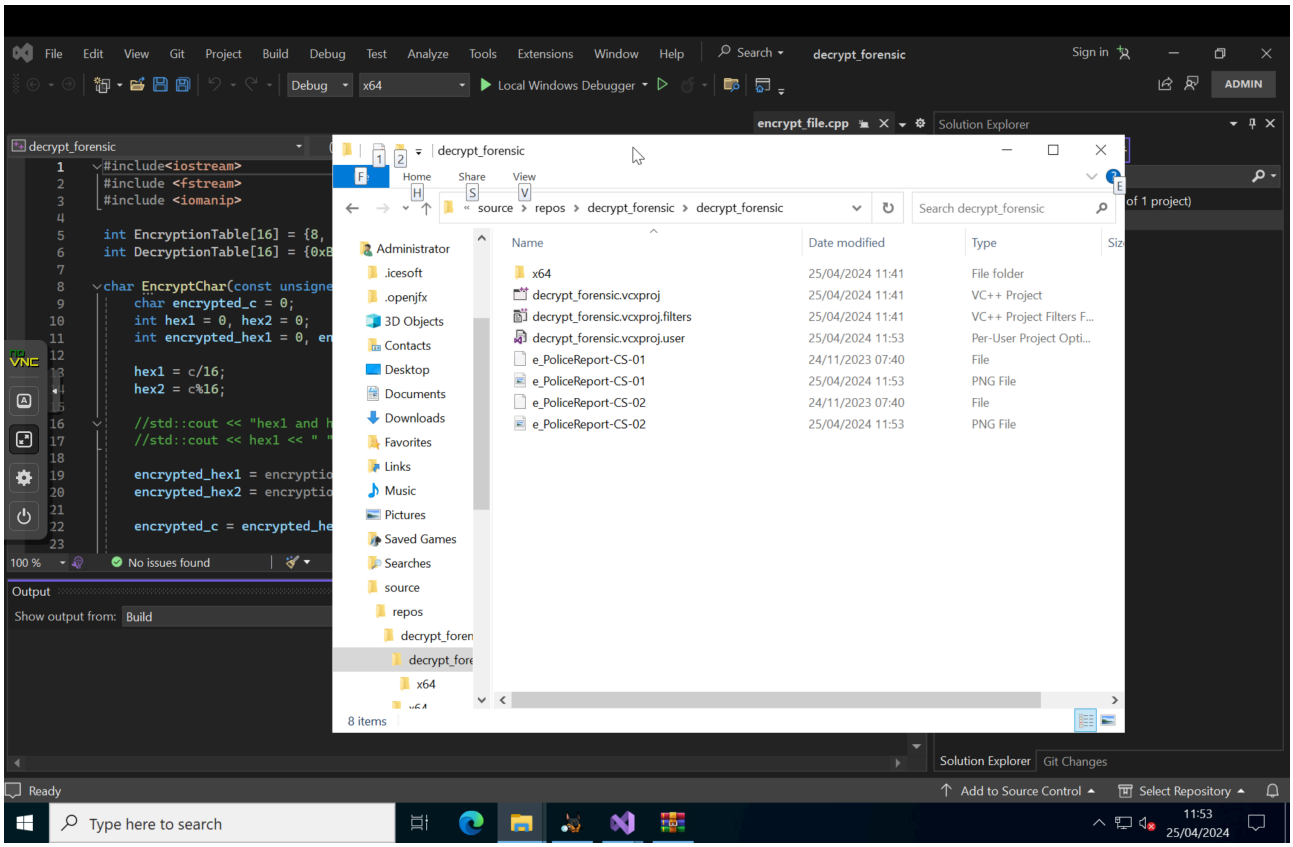
The C++ program source code

To decrypt the files, they had to be placed in the current directory of the build. Then, this command had to be entered before running it without debugging :

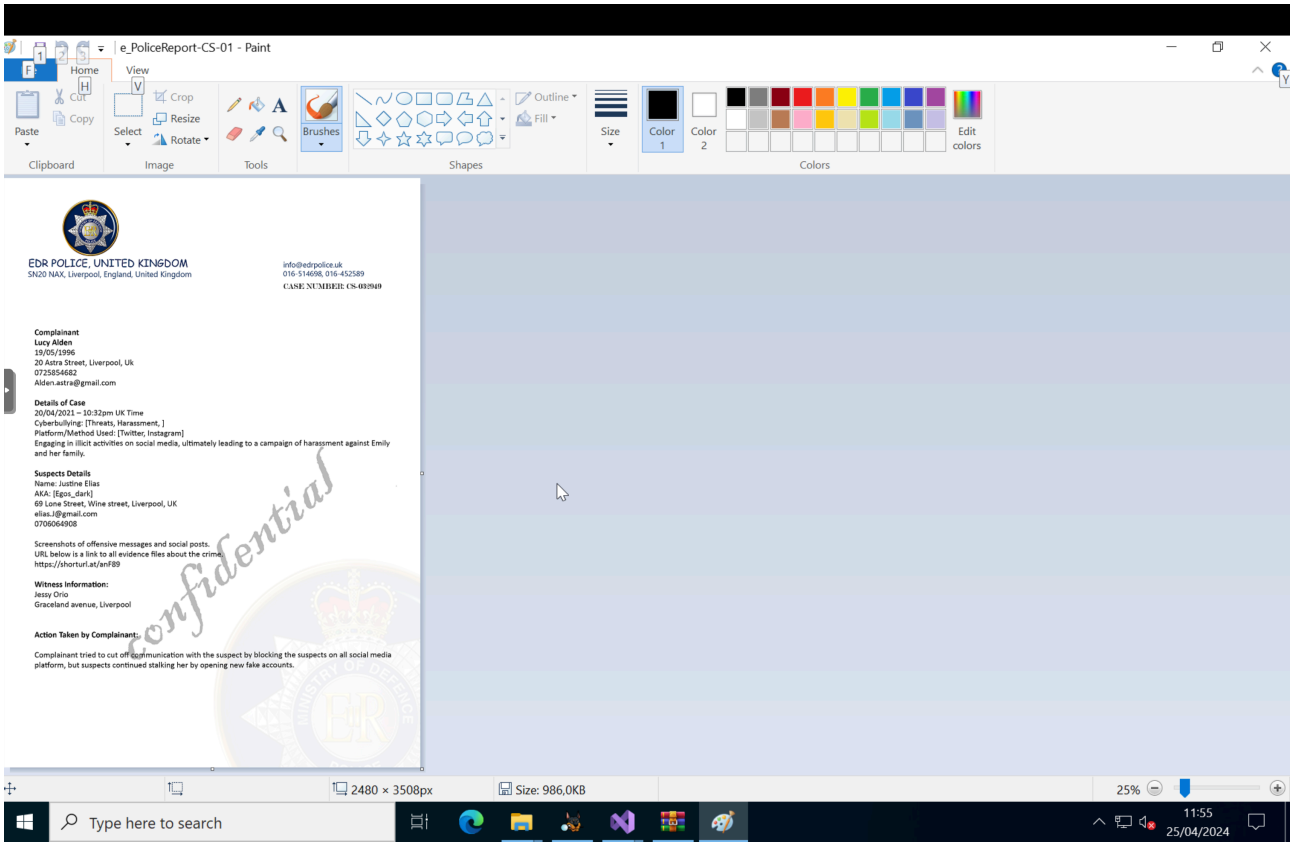
<file encrypted name> <file encrypted name>.<extension> decrypt



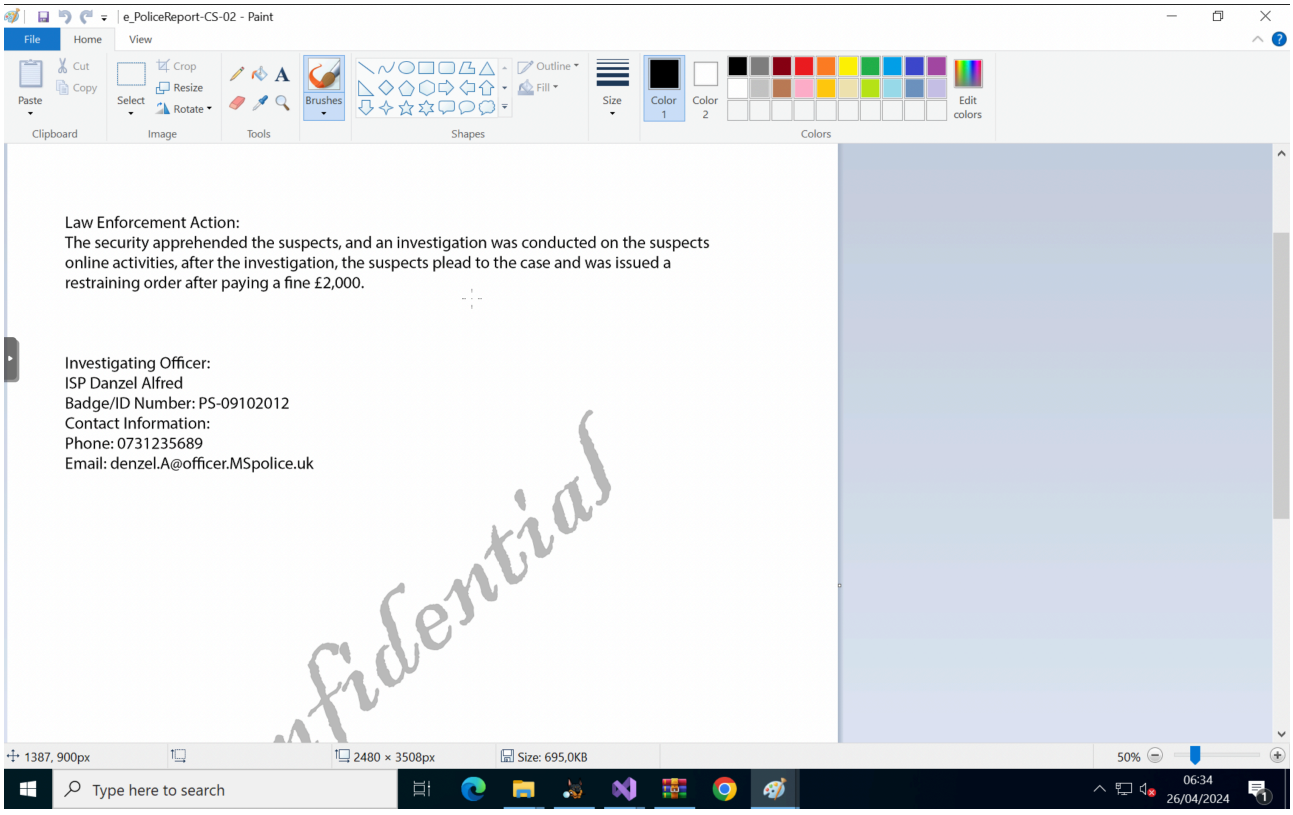
The command to enter. After several researches, the good extension was .png



Two .png files were recovered.



The victim complained



Justine Elias has been condemned

Justine Elias has been condemned to pay 2000£ of damage fine in 2021, for Cyber Bullying, usage of multiple fake accounts, and hacking.

Conclusion

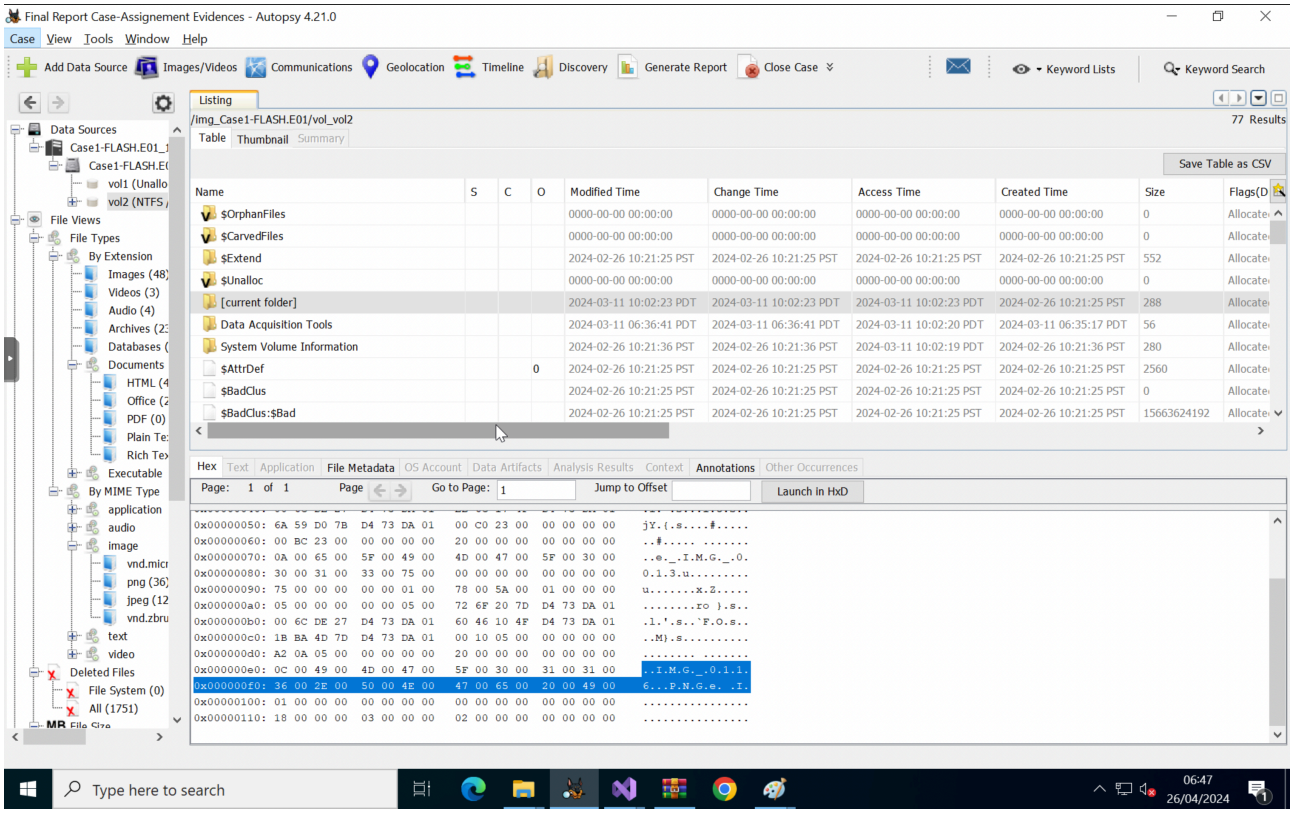
The digital forensics investigation process is meticulously detailed, highlighting its critical role in ensuring the integrity, legality, and admissibility of evidence within legal proceedings. The steps outlined, from initial evidence collection to the final courtroom presentation, underscore the rigorous standards and structured methodologies that are fundamental to the discipline. Emphasizing the chain of custody and the roles of each team member, the report demonstrates how digital forensics combines technical expertise with strict legal compliance to effectively address and solve complex cybercrime cases, thereby reinforcing its indispensable value in maintaining justice and security in the digital age.

References

- Kruse II, Warren G., and Jay G. Heiser. _Computer Forensics: Incident Response Essentials_. Addison-Wesley, 2002.
- Casey, Eoghan. _Digital Evidence and Computer Crime_. Academic Press, 2004.
- ABC News. "BTK serial killer's daughter: 'We were living our normal life. ... Then everything upended on us'". ABC News, 22 January 2019.
- Dooley, Sean. “The Capture of Serial Killer Dennis Rader, BTK.” _Psychology Today_, 17 March 2023.
- Operation Pacifier : https://en.wikipedia.org/wiki/Playpen_(website)
- https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/
- Chain of Custody, Wikipedia UK, https://en.wikipedia.org/wiki/Chain_of_custody
- Autopsy®, digital forensics software, https://www.autopsy.com/download/
- Windows Server 2022, Operating System, isolated in homelab for investigation, https://www.microsoft.com/en-us/windows-server
-

Other research techniques

Several techniques were not fully developed on this document to find other hidden evidences, such as analysing metadata (location of pictures, original phone used…), and hexadecimal values in files or partitions.



Folder potentially hiding an image