PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Computer Forensics
ACCD5000
Dr Nitheesh Kaliyamurthy

COMPUTER FORENSICS

SYNTHESIZE A SOLUTION TO A POTENTIAL REAL-LIFE SCENARIO

LELONG Lucie

Contents

I/ Task 1: Research 3

II/ Task 3: Investigate 5

Introduction 5

Chain of custody 5

Investigation Methodology 6

Our Case 7

III/ Conclusion 14

I/ Task 1: Research

The digital revolution has irrevocably transformed our world, and the realm of crime is no exception. Criminals now exploit the vast landscape of digital devices and data to commit offenses, leaving behind a trail of electronic evidence. This is where computers and digital forensics step in – specialized fields dedicated to uncovering and analyzing this digital evidence. While often used interchangeably, there is a subtle distinction between the two:

- Computer Forensics: This term originated in the early days of computing when computers were the primary source of digital evidence. It refers to the process of collecting, analyzing, and presenting evidence from computers and their storage media.
- Digital Forensics: This broader term encompasses the recovery and investigation of digital evidence from any source, including computers, mobile devices, tablets, servers, network devices, storage devices, and even cloud storage.

The roots of computer forensics can be traced back to the 1970s with the rise of the first computer crimes. As computers became more prevalent in the 1980s, the need for specialized techniques to investigate them grew. The term "computer forensics" gained wider recognition in the 1990s, and standardized practices began to appear. However, with the explosion of mobile devices and the internet in the 2000s, the field needed to expand beyond just computers, leading to the coining of the term "digital forensics."

Digital forensics plays a critical role in various real-world scenarios. In the realm of law enforcement, it is a vital tool for investigating cybercrime. This includes offenses like identity theft, data breaches, online harassment, and financial fraud. Digital forensics helps collect evidence from suspects' devices to build a compelling case for prosecution. When a company experiences a cyberattack, digital forensics helps find the source of the attack, determine the scope of the damage, and recover lost data, aiding in incident response. Organizations can use digital forensics to investigate employee misconduct, such as data theft or intellectual property violations, for internal investigations. Additionally, in legal proceedings, digital forensics helps find, collect, and produce relevant electronic data for use as evidence, playing a crucial role in electronic discovery (eDiscovery).

To illustrate the power of these disciplines, let's consider some real-world cases. Imagine a company suspects an employee of stealing confidential data and selling it to a competitor. A computer forensics investigation would involve seizing the employee's computer and storage devices. The investigator would then recover deleted files, analyze internet browsing history, and examine emails and documents for evidence of unauthorized data transfer.

Now, let's shift gears to a different scenario. A social media post sparks suspicion in a murder investigation. Digital forensics can come to the rescue by analyzing the suspect's social media activity for incriminating posts or messages. Examining timestamps and location data can help set up a timeline of events, while recovering deleted photos or videos from the suspect's mobile phone can provide crucial missing pieces of the puzzle.

These are just a few examples of how computers and digital forensics are used to solve real-world crimes. As technology continues to evolve at a rapid pace, the scope and importance of these disciplines will only continue to grow. By using the expertise of computer and digital forensics professionals, we can ensure that the digital world remains a place where evidence can be found, analyzed, and used to bring criminals to justice.

II/ Task 3: Investigate

Introduction

In our ultra connected era, cyberbullying is increasingly present. It is the use of technology to harass, threaten, or injure others. It has become a widespread problem with detrimental effects on both individuals and society. Cyberbullying is characterized by its vicious and relentless nature, which extends beyond physical boundaries to infiltrate online areas and permeate victims' lives, often with disastrous results. To clarify the dynamics and ramifications of cyberbullying, we examine a case study in this article. The current case emphasizes how critical it is to address online harassment and the harm it causes to victims' mental and emotional health. Our goal is to find proof of cyberbullying in the evidence files, decrypt and analyze what seems suspect.

Chain of custody

Any forensic investigation's foundation is the chain of custody, which guarantees the accuracy and admissibility of evidence in court. During the lecture we discussed the legal entities that regulate the action of computer forensics. The main one in the UK is UKAS, National Accreditation Body for the United Kingdom.

It is important to respect the legal considerations and to plan accordingly all the things that are legal for use during the case in front of the court. It is having some knowledge about things we can do legally.

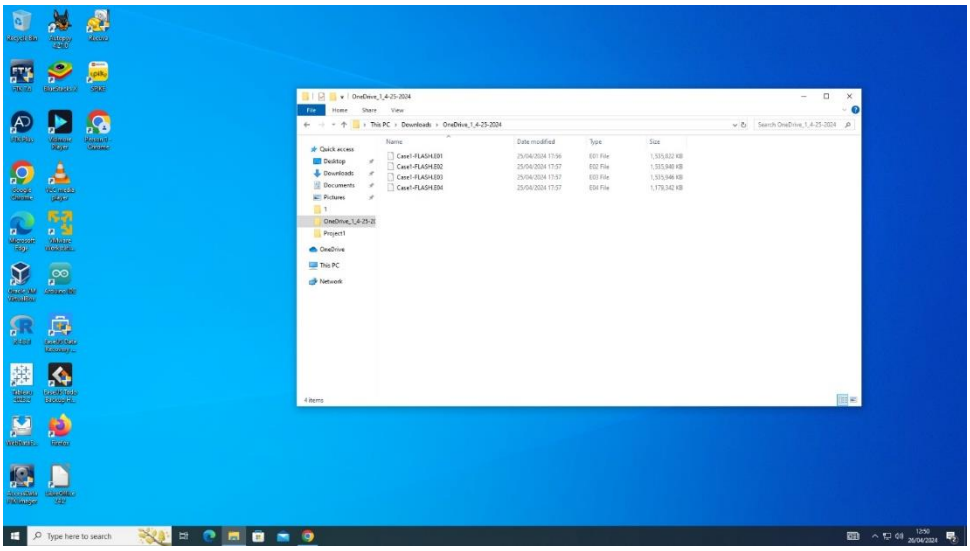
Thorough recording of the possession and management of digital evidence was crucial in this instance. Every stage of the process, from the first data gathering to the data presentation in court, must be painstakingly documented and confirmed. The identification of pertinent digital artifacts and their meticulous capture and preservation mark the beginning of the evidence trail. Strict standards were followed throughout the inquiry, describing who was able to view the evidence, when and where it was stored, and any changes or transfers that took place. It is very important to protect the integrity of the investigation by upholding the credibility and dependability of the evidence through the maintenance of an intact chain of custody. For that every person of the group has been assigned a role, we have a manager, an incident responder, an examiner, a documenter, a witness, an incident analyzer, an investigator and a photographer.

Investigation Methodology

It is essential to adhere to the order of operation for the smooth operation of the case and the respect of the legal considerations. The photographer is essential during the early phases of reacting to a crime scene because they carefully document the scene and any relevant evidence without disrupting the surroundings. Their main responsibility is to take detailed pictures of the situation, making sure that every little detail is captured truthfully and following rigorous guidelines to avoid contamination or manipulation. The incident responder then intervenes to take control of the situation, making sure that all possible evidence is preserved and taking action to stop future events. This calls for a careful balance between protecting the area and gathering pertinent evidence with the right techniques and equipment, especially when it comes to digital evidence, which must be preserved without causing any harm. The gathered evidence is then carefully examined by the analyzer, who carefully considers its importance and effects on the various systems. To guarantee the integrity of the evidence throughout the course of the investigation, the analyzer must create and uphold a strict chain of custody. In addition to these vital tasks, the evidence documenter carefully logs each step and detail supplied by the team in order to maintain an exhaustive record of the crime scene and the investigative process, while the examiner/investigator carefully reviews and ranks the evidence. Finally, the witness provides official testimony in court, acting as a crucial liaison between the legal proceedings and the investigative activities. The documenter is essential to this complex procedure because they record every machine, computer, screen, and piece of evidence with precision. This helps to create a comprehensive layout of the crime scene that is useful for both the legal and investigative processes.

Our Case

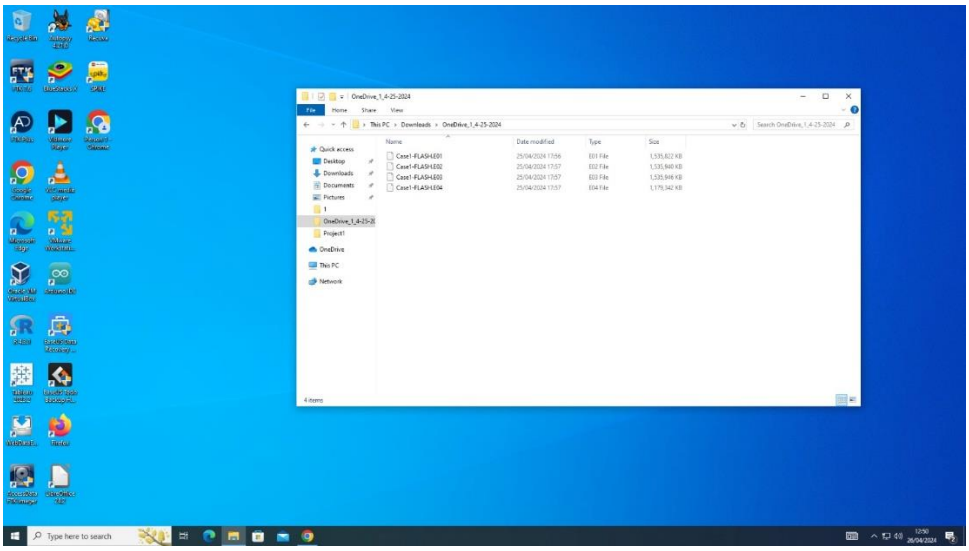
To gather evidence from a USB key, I used AccessData FTK Imager within a virtual machine environment, first I had to make sure my virtual machine was set up and running, with FTK Imager installed. I Connected the USB key to my computer, and within the virtual machine settings, pass through the USB device to the virtual machine. I Selected the USB key as the source, specified the destination for the disk image, configured imaging options, and start the imaging process. Once complete, I verified the integrity of the disk image. Once finished we can review and analyze the contents within the virtual machine environment or export the image for analysis on the host machine.



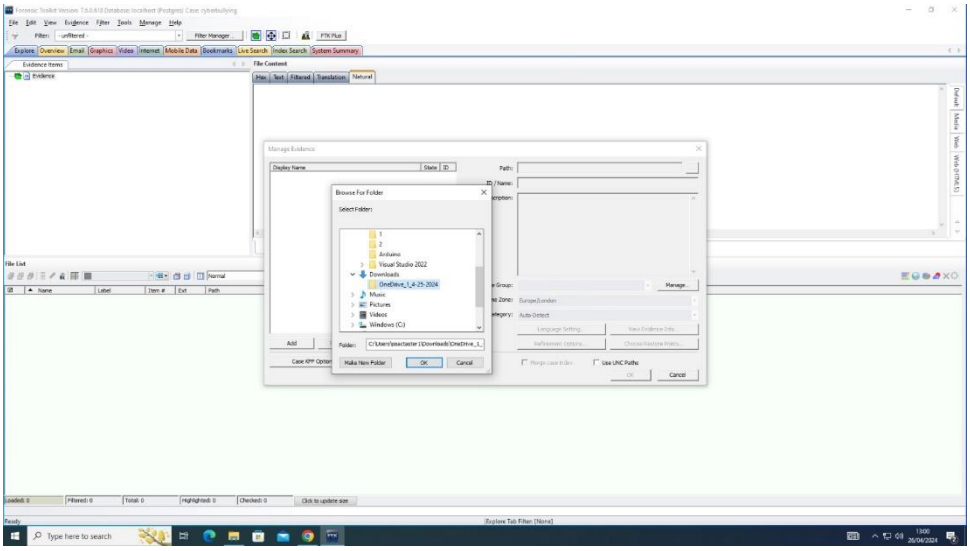
Here is the evidence.

Now I choose to use FTK 7.6 to open the evidence.

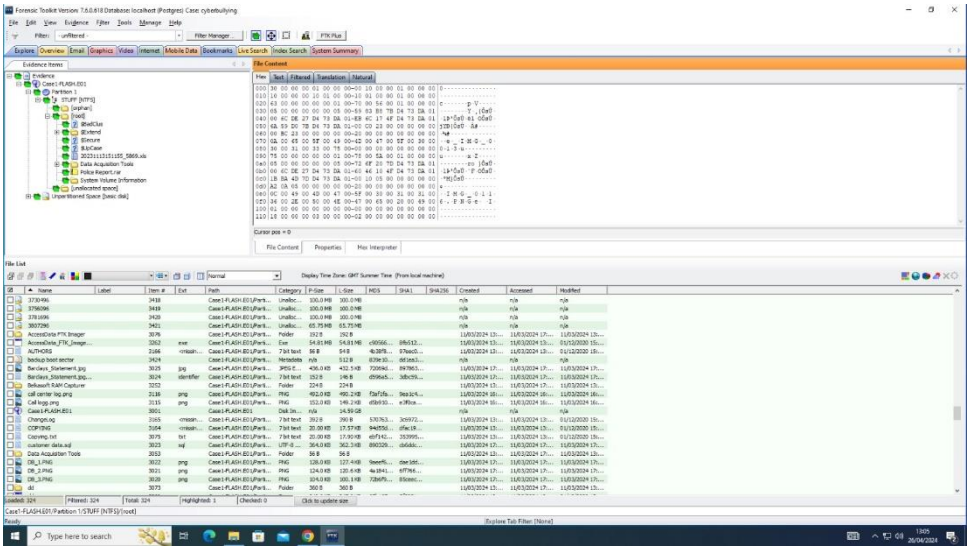
Case->New



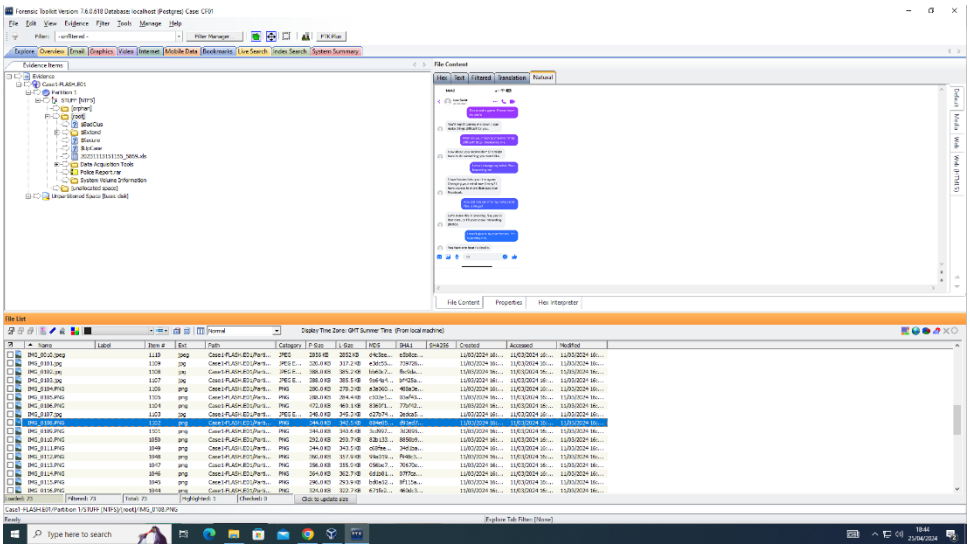
I imported the evidence file.

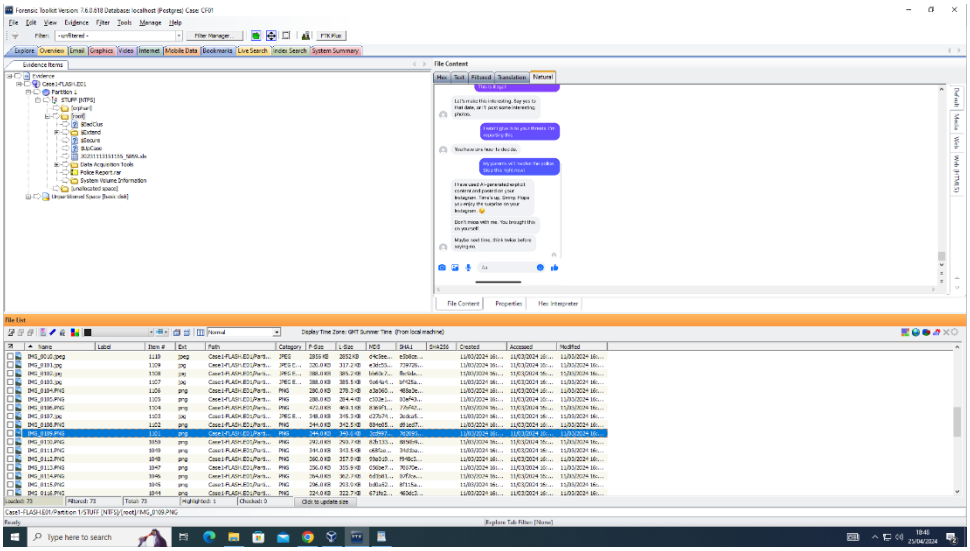


And then I go in '[root]'

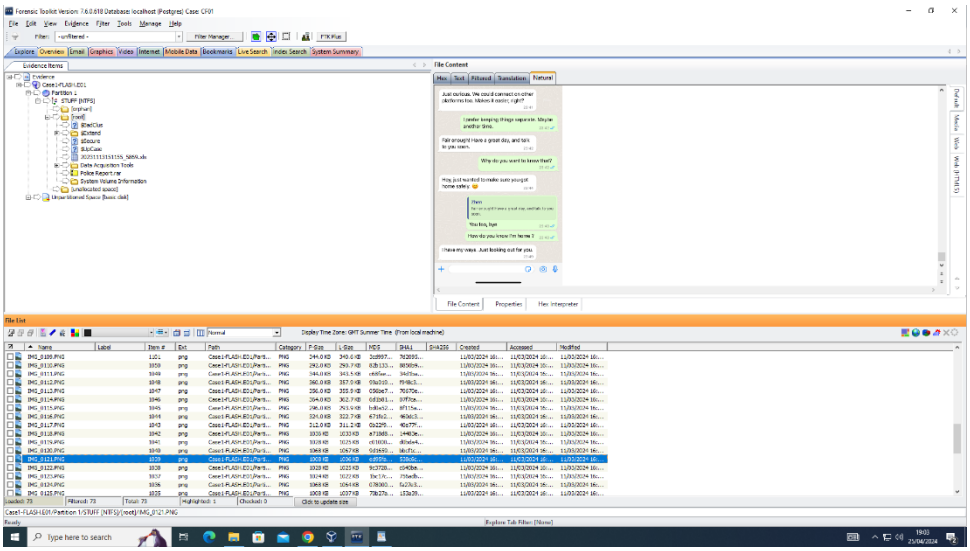


And analyze every element one by one to find proofs of cyberbullying.





In those 2 screenshots, Lee Saint threatens Emmy to leak explicit content.

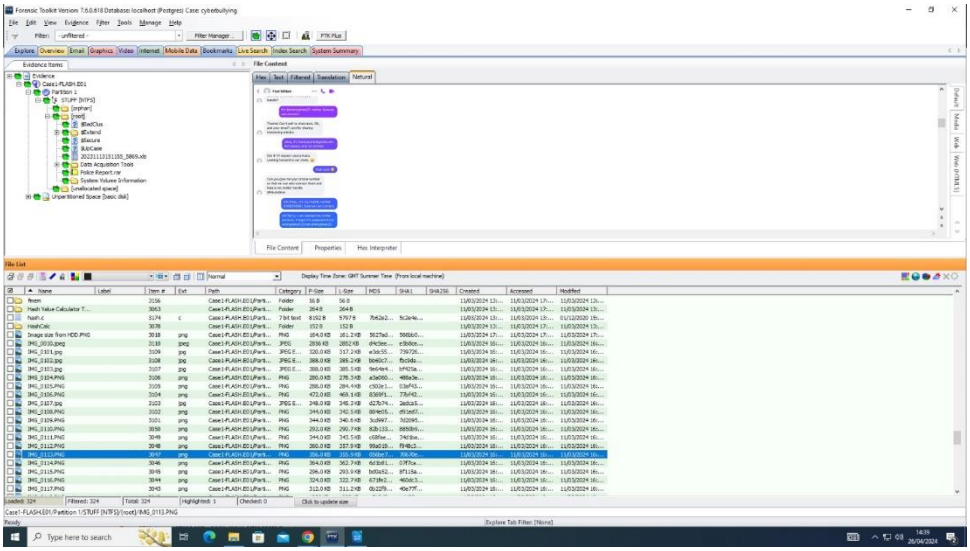


All these are examples of cyberbullying.

There are a few screenshots showing a conversation between the victim, Emmy and her bully.

He talked to her on Facebook under the name of Fred William, Seer Musta is also his Twitter account.

Fred Wiliam, Lee Saint, Seer Musta and Justine Elias may be potentially the same person.



There is also an encrypted police report, I figure out how to decrypt the file using visual studio 2022 and end up with 1 document.

EDR POLICE, UNITED KINGDOM
SN20 NAX, Liverpool, England, United Kingdom

info@edrpolice.uk
016-514698, 016-452589

CASE NUMBER: CS-032949

Complainant
Lucy Alden
19/05/1996
20 Astra Street, Liverpool, Uk
0725854682
Alden.astra@gmail.com

Details of Case
20/04/2021 – 10:32pm UK Time
Cyberbullying: [Threats, Harassment,]
Platform/Method Used: [Twitter, Instagram]
Engaging in illicit activities on social media, ultimately leading to a campaign of harassment against Emily and her family.

Suspects Details
Name: Justine Elias
AKA: [Egos_dark]
69 Lone Street, Wine street, Liverpool, UK
elias.J@gmail.com
0706064908

Screenshots of offensive messages and social posts.
URL below is a link to all evidence files about the crime.
https://shorturl.at/anF89

Witness Information:
Jessy Orio
Graceland avenue, Liverpool

Action Taken by Complainant:

Complainant tried to cut off communication with the suspect by blocking the suspects on all social media platform, but suspects continued stalking her by opening new fake accounts.

confidential

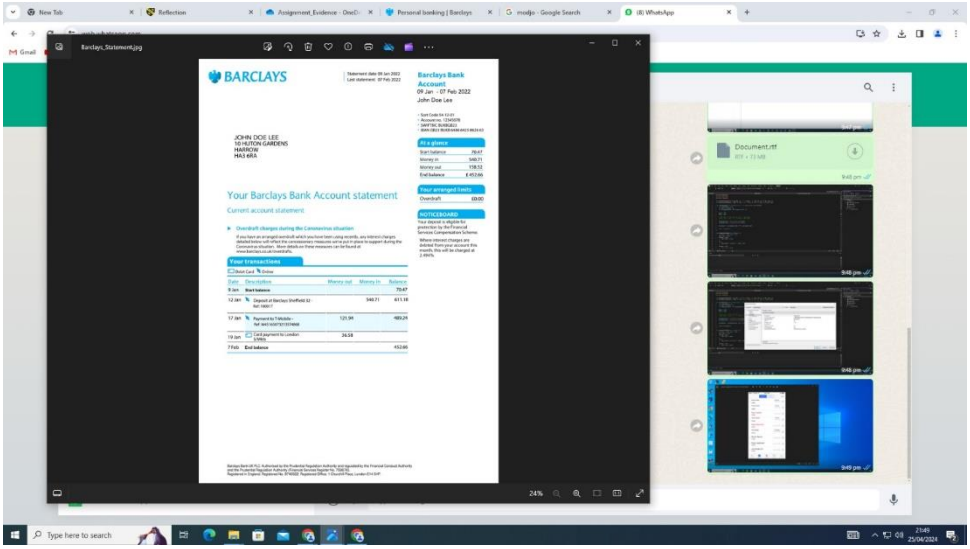
Law Enforcement Action:
The security apprehended the suspects, and an investigation was conducted on the suspects online activities, after the investigation, the suspects plead to the case and was issued a restraining order after paying a fine £2,000.

Investigating Officer:
ISP Danzel Alfred
Badge/ID Number: PS-09102012
Contact Information:
Phone: 0731235689
Email: denzel.A@officer.MSpolice.uk

confidential

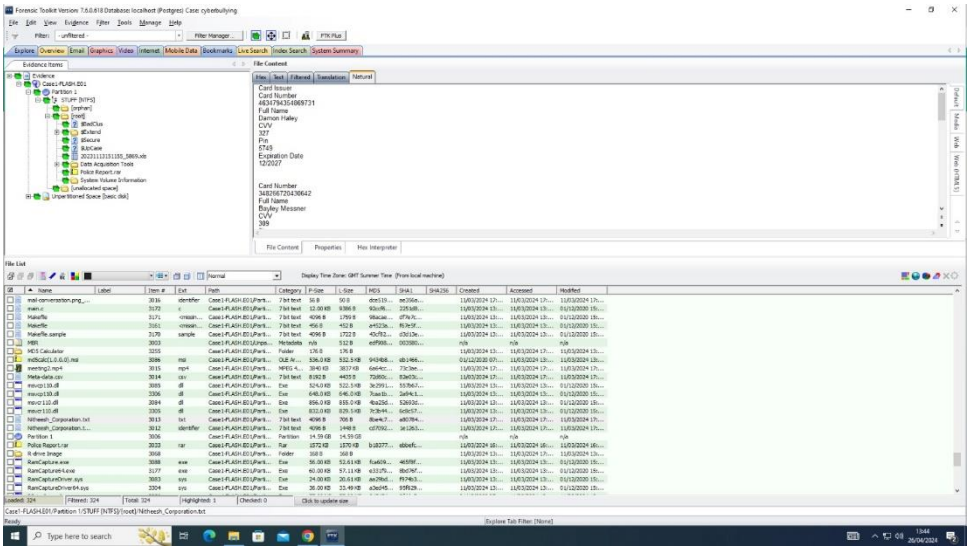
However, the URL of the document does not work.

I also found a bank statement from Barclays with a payment to T-Mobile.



So, I tried to connect to an account on Barclays.

I also tried with the text document, Nitheesh_Corporation.txt which have multiple names and Card number, but only one have 16-digit numbers but it did not work.



III/ Conclusion

In conclusion, a number of important pieces of evidence showing harassment and threats on social media platforms have been uncovered during the investigation into the cyberbullying case involving Emmy and Justine Elias. By utilizing FTK and Visual Studio to carefully analyze digital data, I have discovered a pattern of activity that is compatible with cyberbullying, and it seems that Justine Elias is the one who is targeting Emmy. The data gathered sheds light on the type and severity of Emmy's harassment and emphasizes the pervasiveness and consequences of cyberbullying in the current digital era. Even while the material that has been found thus far provides a clear picture of the harassment that Emmy experienced, it is crucial to recognize that there might be more pertinent evidence that has not yet been found.