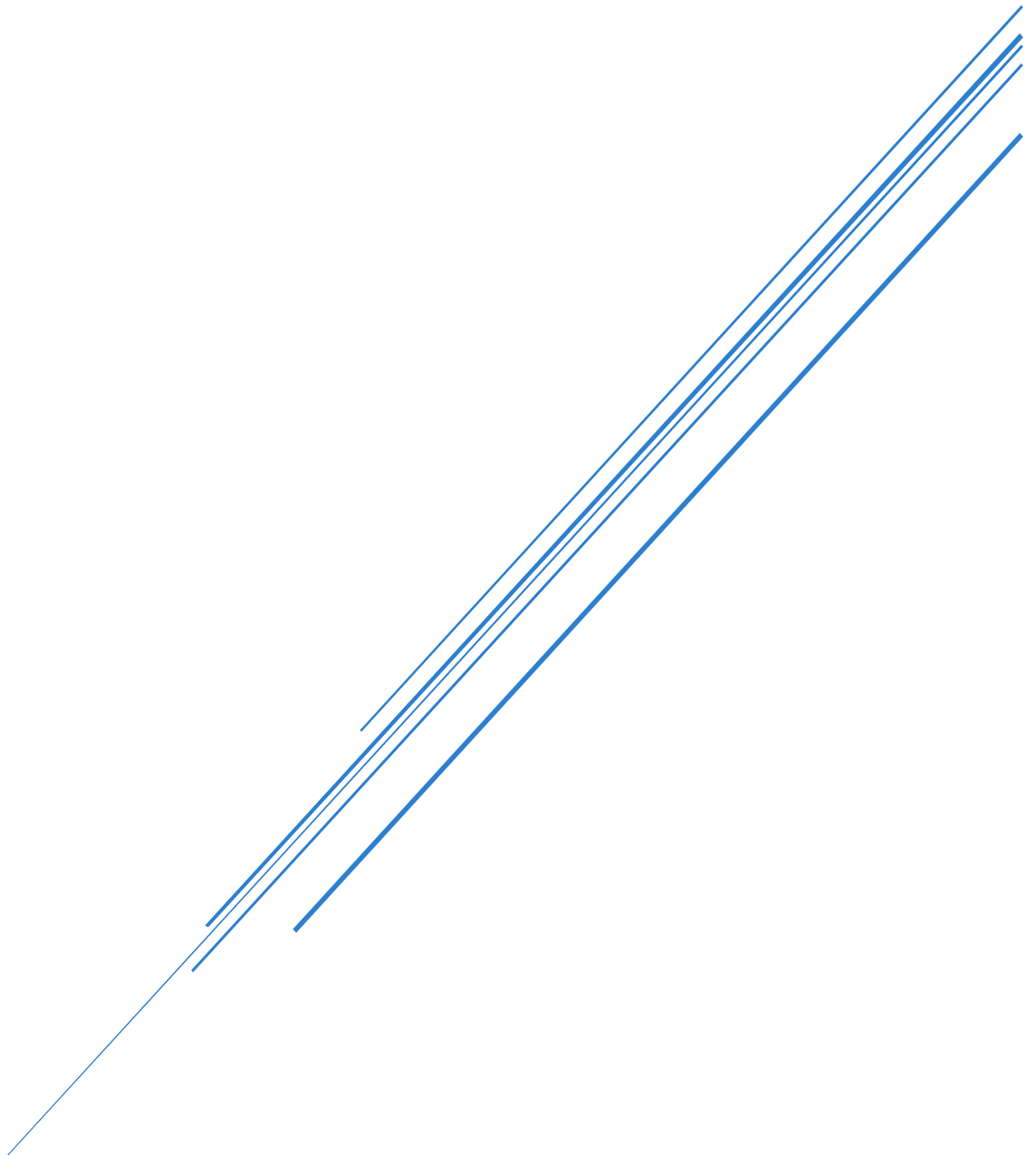


COMPUTER FORENSICS (ACCD5000)

Coursework – Task 1 and Professional Report



Che Morris - 2203458
Cyber Security & Networks

Contents

Task 1 – Research	2
Task 3 – Report	4
Introduction.....	4
Collection of Digital Evidence	4
Chain of Custody	4
Verification of File Integrity	5
Verification of FLASH.E01 hashes	5
Verification of FLASH.E02 hashes	5
Verification of FLASH.E03 hashes	6
Verification of FLASH.E04 hashes	6
Tools Used	7
Analysis of the Digital Evidence	8
Key Findings	13
Encrypting Code + Police Report	13
Chat Logs	14
Fred William aka MustaSeer – Facebook & Twitter	14
Lee Saint - Facebook.....	16
Justine Elias - Facebook.....	18
Justine Elias – WhatsApp Messenger	20
MustaSeer – WhatsApp.....	22
My Conclusion	23

Task 1 – Research

In forensic investigations, there are two main types: computer forensics and digital forensics. Whilst you may think they are interchangeable; they have their own distinctive methodologies and processes.

Computer forensics is the more traditional approach focusing on recovering digital evidence from any computer or storage medium (like USBs) that can store information and then examining those files for use in an investigation [1]. Digital forensics is a broader approach that includes all technology and isn't restricted to just computers and helps when a larger variety of devices are utilized within a cyber-crime [2].

Comparing the two, computer forensics focuses on data stored specifically on computers and digital forensics to be a more open approach as in modern day, crimes can be committed from more than just computers.

Historically, computer forensics didn't actually begin until the 1980s as there wasn't really a need for it and then in the late 1990s, digital forensics was born and the UK set up it's first computer crime unit which was called the "Fraud Squad" [3].

Both concepts focus on examining digital evidence to uncover or solve cyber-crime, but they differ when extracting the data. Computer forensics will target data from just computers and digital forensics can target data from a larger variety of digital devices which can include "networks, cloud storage and phones" [4]. They share important aspects with each other; such as, maintaining a chain of custody, keeping documentation and ensuring information isn't altered [4]. These are important as they allow the investigation to be admissible in court.

Some important processes are shared between both computer and digital forensics. One of these is being able to recover deleted files. This should be done at the beginning of the analysis and can help reverse where a user has tried to delete traces of what they've done on their system [4]. This is done using tools, such as FTK or Autopsy, but a combination of both can be even more effective in some cases. Another important process is recovering metadata from files, this can show when a file was last accessed, created or even deleted [4]. It can also show the hashes of files or depending on what file type you are analysing, the location of where it was taken or even who created said file.

Looking into cases where digital or computer forensics were utilized to solve the case, most of them are quite straightforward. The case of "The BTK Killer" was solved in 2005 after remaining unsolved for almost 30 years through examining the metadata of a Microsoft Word document that was sent to the police by the killer which revealed information that led to his arrest [5]. Another case is the "Larry J. Thomas vs State of Indiana" case where he had been arrested for a suspected robbery, "during the investigation, the authorities took the content posted on the culprit's Facebook account

into consideration. They found he had posted photos of himself with an AR, the ammo used in the case matched the weapon in the photos” [5].

Task 3 – Report

Introduction

The following report will discuss my findings and progression on a cyberbullying case. The information we will be analysing was imaged from a drive and I will be using a multitude of tools to analyse the information.

Due to how we have the information stored, I will be performing this analysis in a forensically secure environment where no data can be written to the files, so the integrity remains intact. As cyberbullying usually leaves a digital footprint in the form of chat logs and communication logs, they are what I will be primarily looking out for when analysing the files.

The purpose of this report is to document the process of me collecting and analysing this evidence, how it has been handled and determining whether I can conclude if cyber bullying has taken place.

Collection of Digital Evidence

Chain of Custody

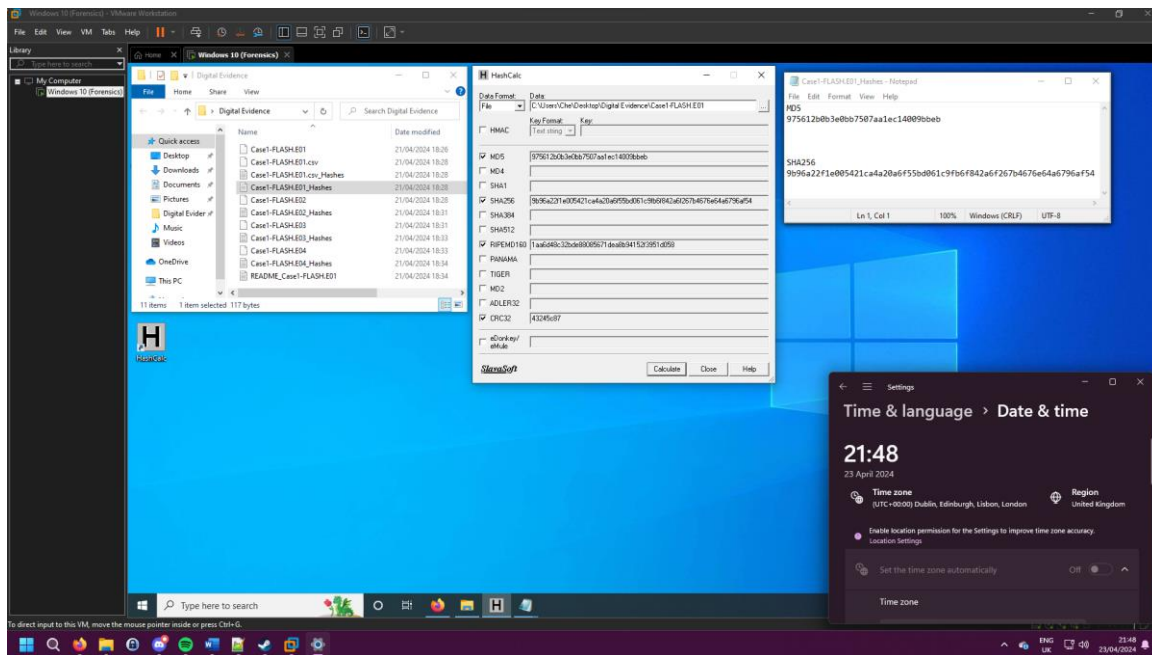
Item	Quantity	Description of Item
1	1	16GB SanDisk Cruzer USB Storage Device

Item	Date and Time	Released By	Received By	Comments
1	17:00 – 11/03/2024	Nitheesh Kaliyamurthy	Jon Morgan	Device was imaged by Jon using FTK Imager 4.3.1.1 and then hashed utilizing HashCalc The image was created in 4 .E0* Files, a CSV file and a README. The hashes were outputted into a separate text file for each .E0* file.
1	12:42 – 18/03/2024	Jon Morgan	Che Morris	Image file was shared to me, hashes are checked below.

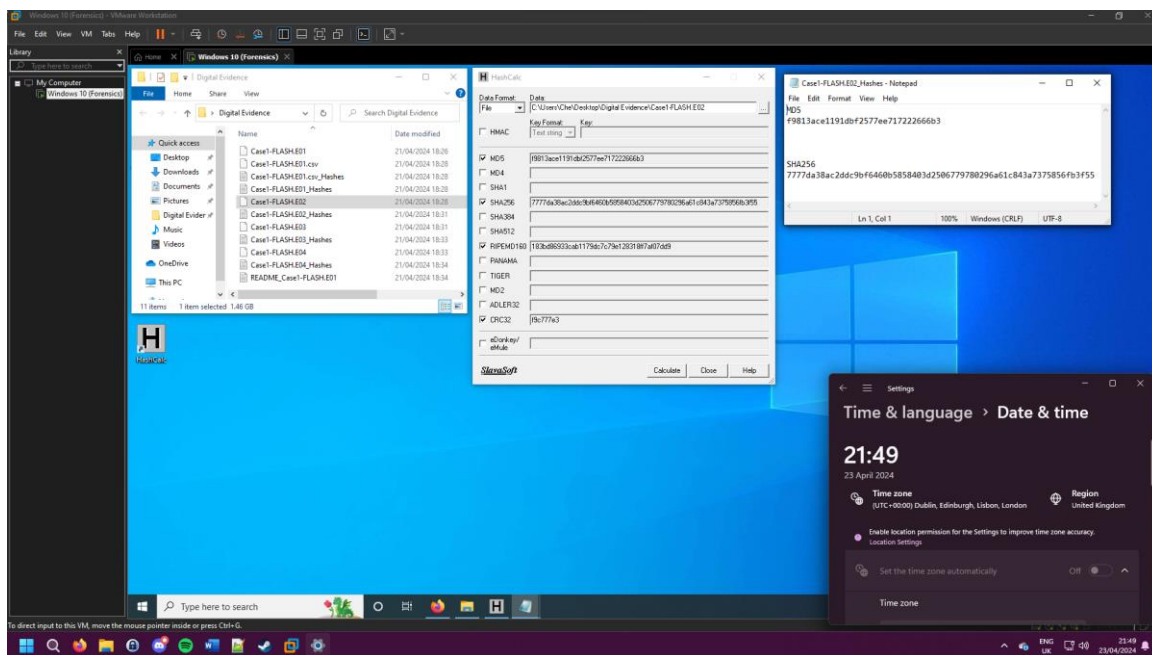
Verification of File Integrity

To ensure that the files have not been tampered with or altered in between being sent to me and me receiving them, I will use a tool called HashCalc (a program that will generate various hashes for files and phrases) to verify that the hashes of each .E01 file has remained the same as documented in the download.

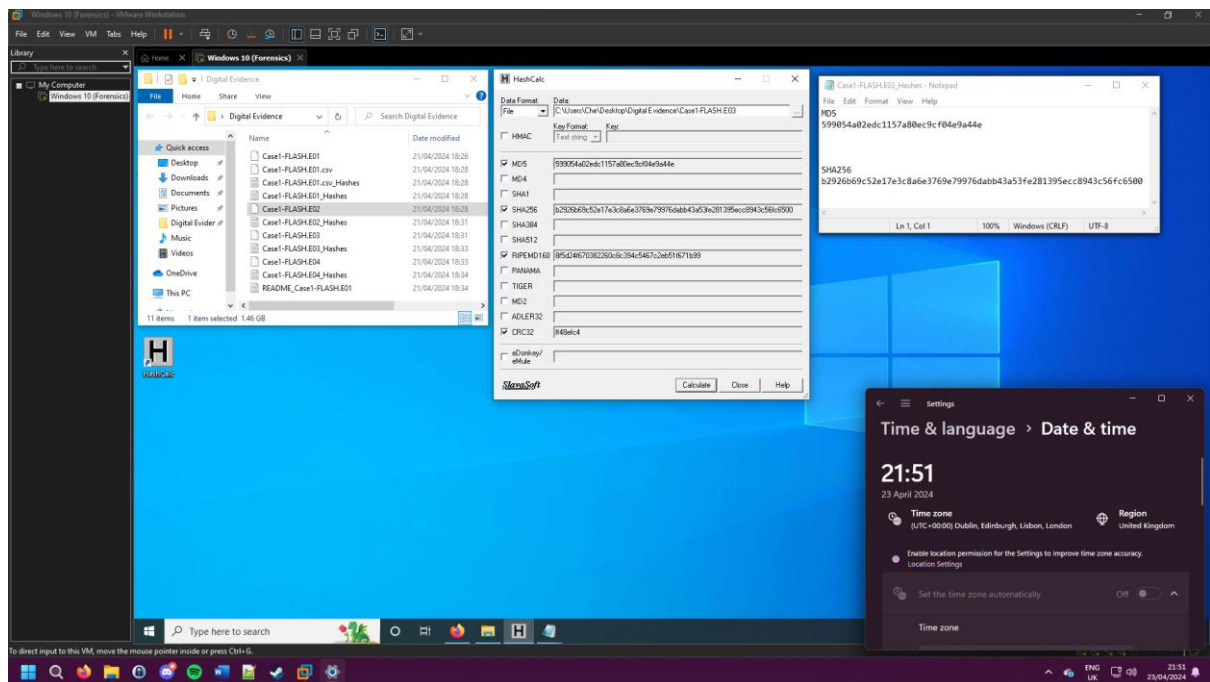
Verification of FLASH.E01 hashes



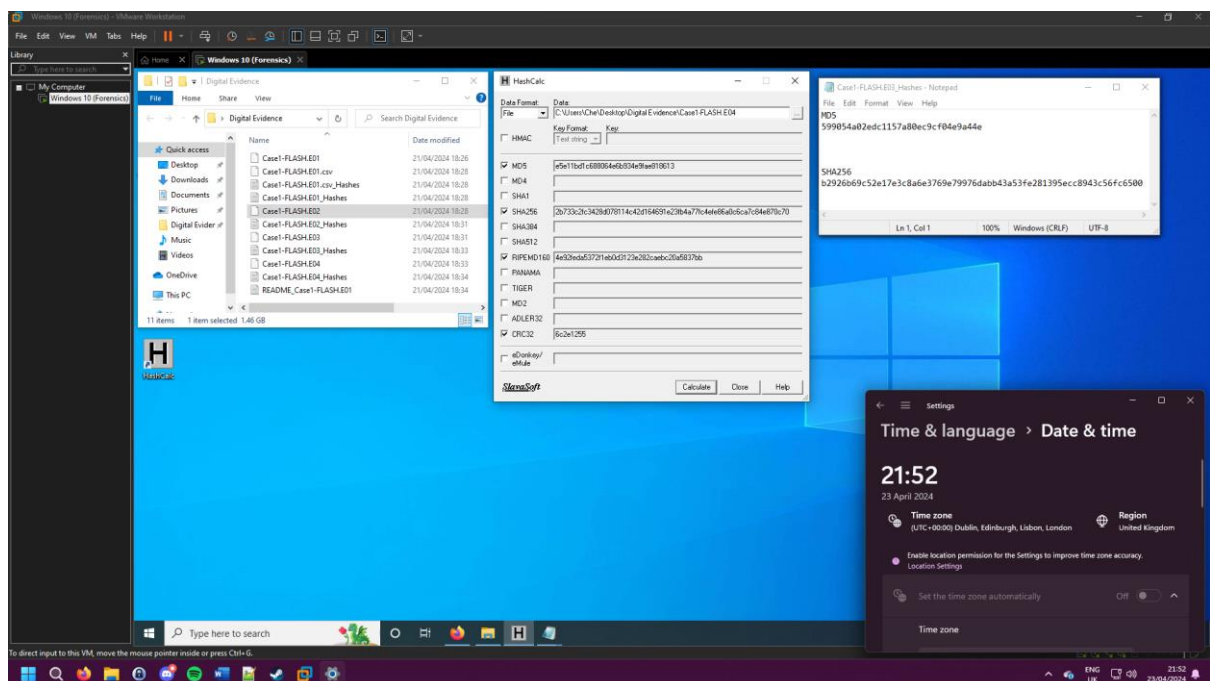
Verification of FLASH.E02 hashes



Verification of FLASH.E03 hashes



Verification of FLASH.E04 hashes



As can be seen for all parts, the hashes for both MD5 and SHA256 remain the same as they were when imaged. This means that we can be sure that the integrity of the files has remained intact and are as they were when imaged by Jon.

Tools Used

The forensics tools that were used throughout the course of this investigation were as follows:

Disk Imaging Software – FTK Imager 4.3.1.1

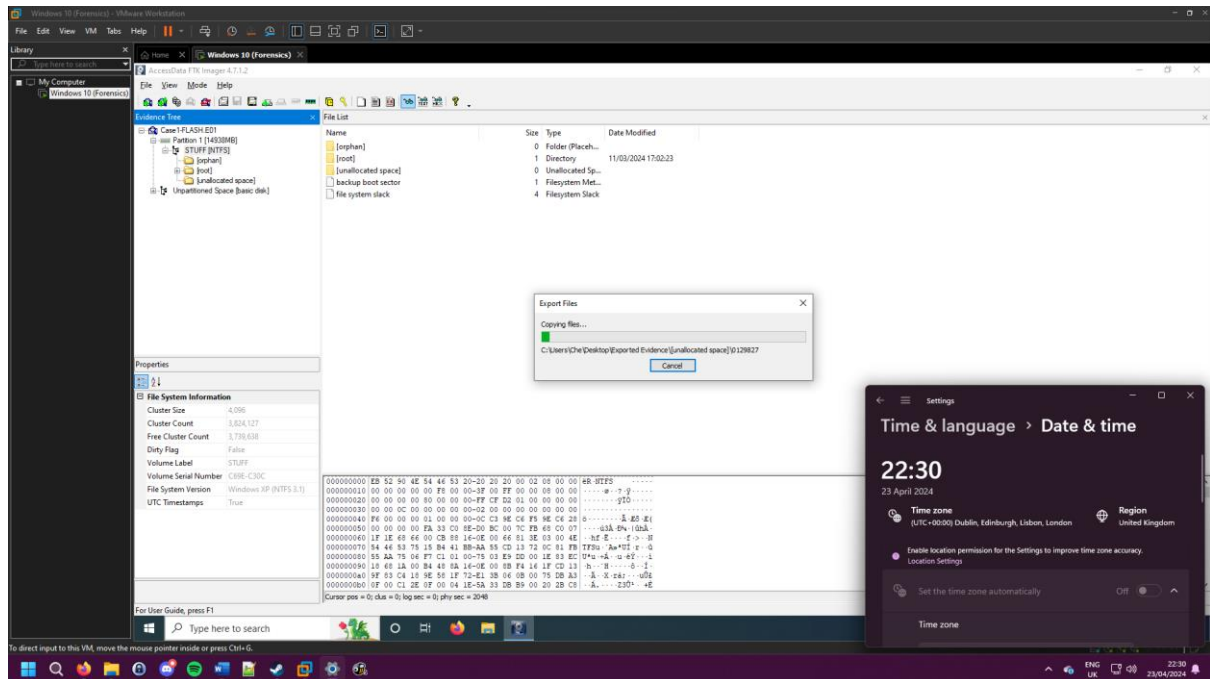
- FTK Imager was used for imaging the file by Jon Morgan and then used by me for exploring the image. FTK Imager is a piece of forensics software that is designed solely for forensics imaging and analysis, it is used for previewing data that may be on these images and creating new images of the devices themselves.

File Extraction and Analysis – Autopsy 4.21.0

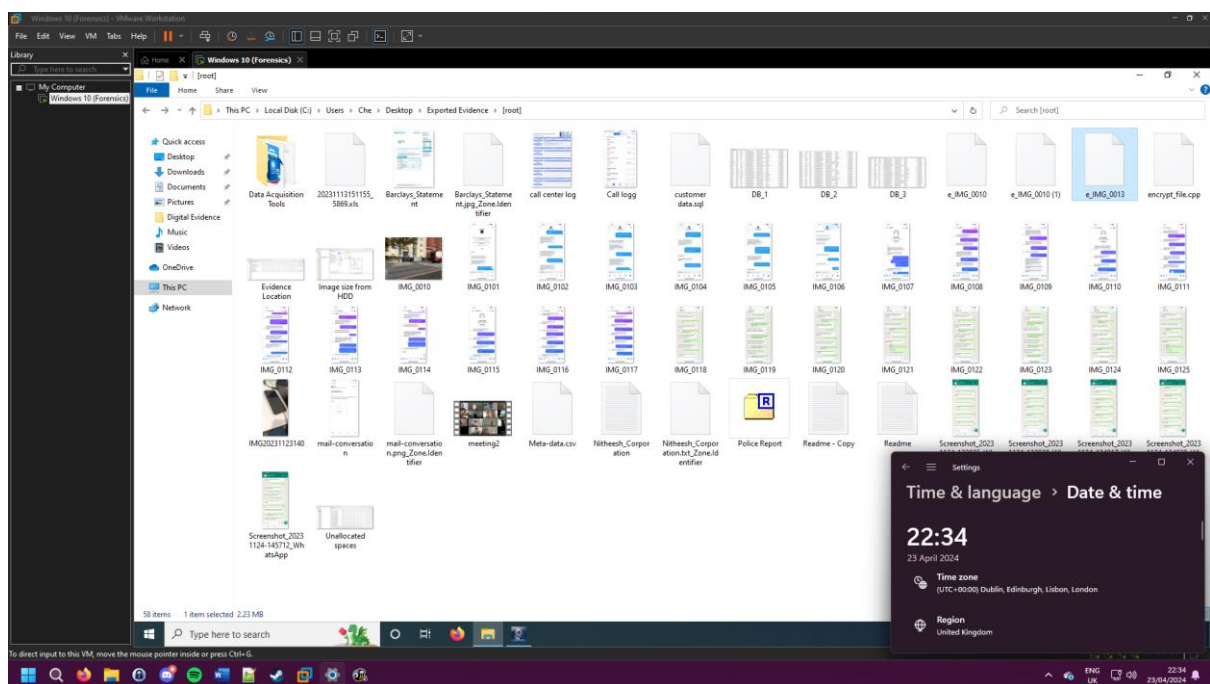
- Autopsy is a piece of software based on the Sleuth Kit which is a piece of open source digital forensics software giving investigators almost a tool kit to use throughout conducting their investigations and can be used to view slack space, unallocated space, files on a volume, anything left behind by a user or OS and can even help look into deleted files.

Analysis of the Digital Evidence

I began by opening the image in FTK Imager just so I could look around the image and found that we had a 15 GB partition labelled “STUFF” as the evidence. After having a look around I discovered that the root of the drive had a bunch of image files and text documents on it so to begin I exported all the files using FTK to a folder so I could open them properly.

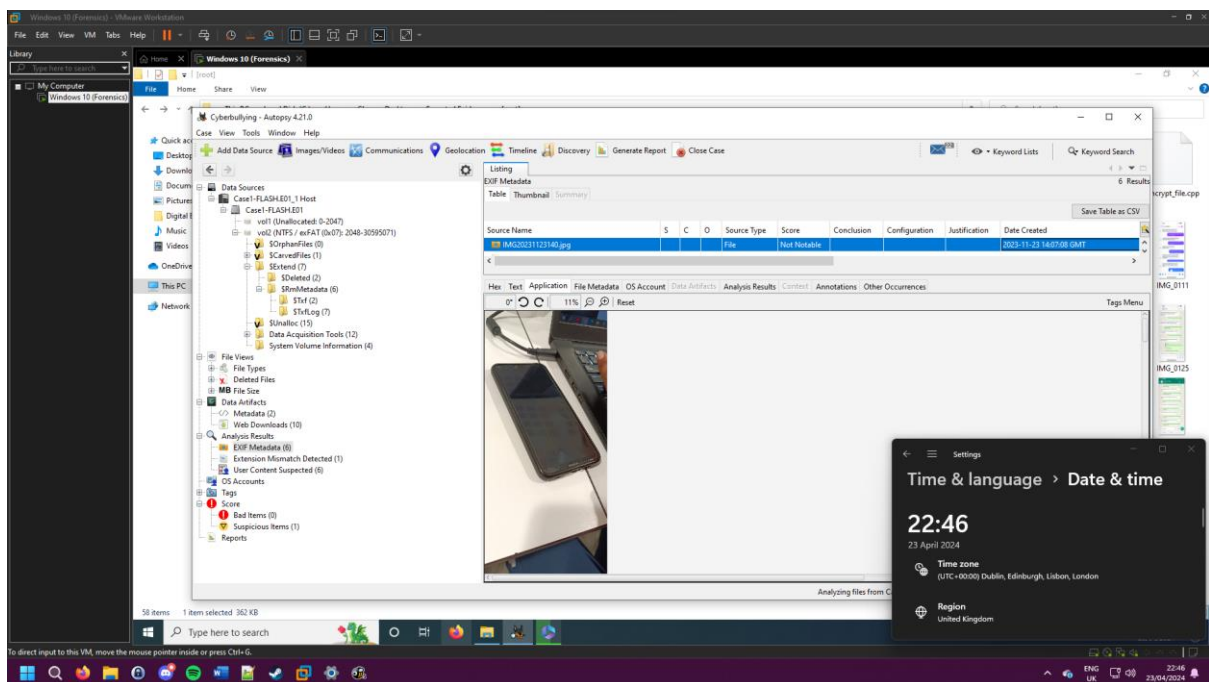


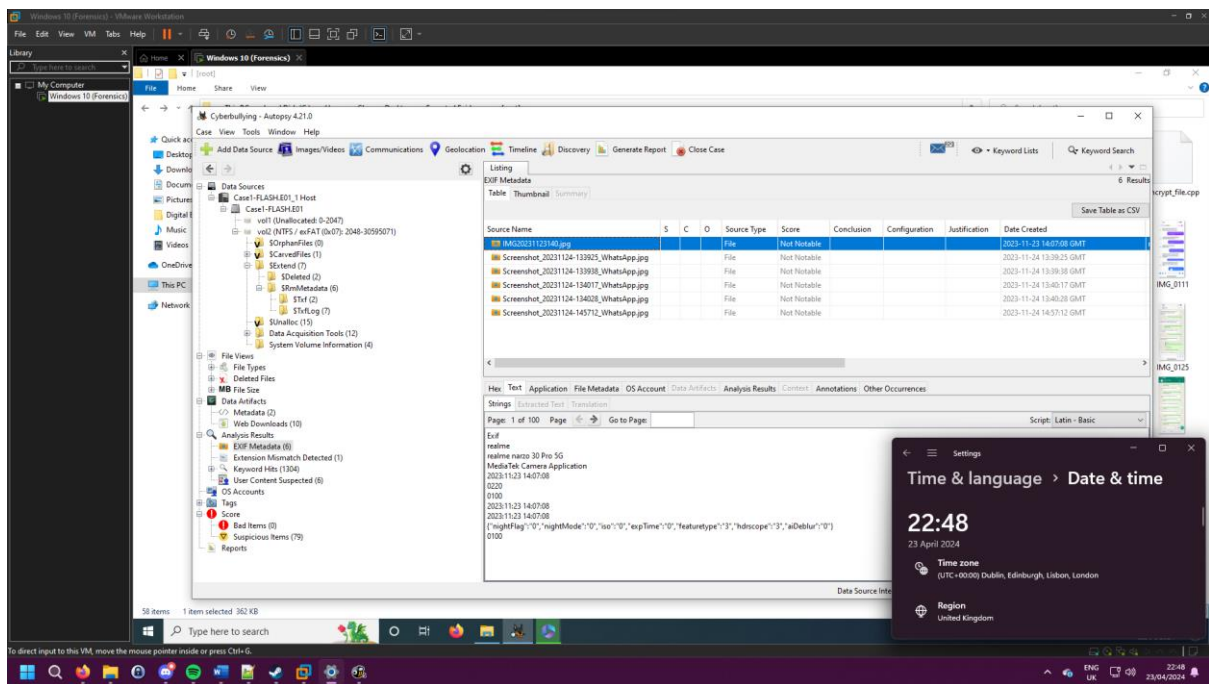
After I exported all the files on the root drive I got a folder with the following.



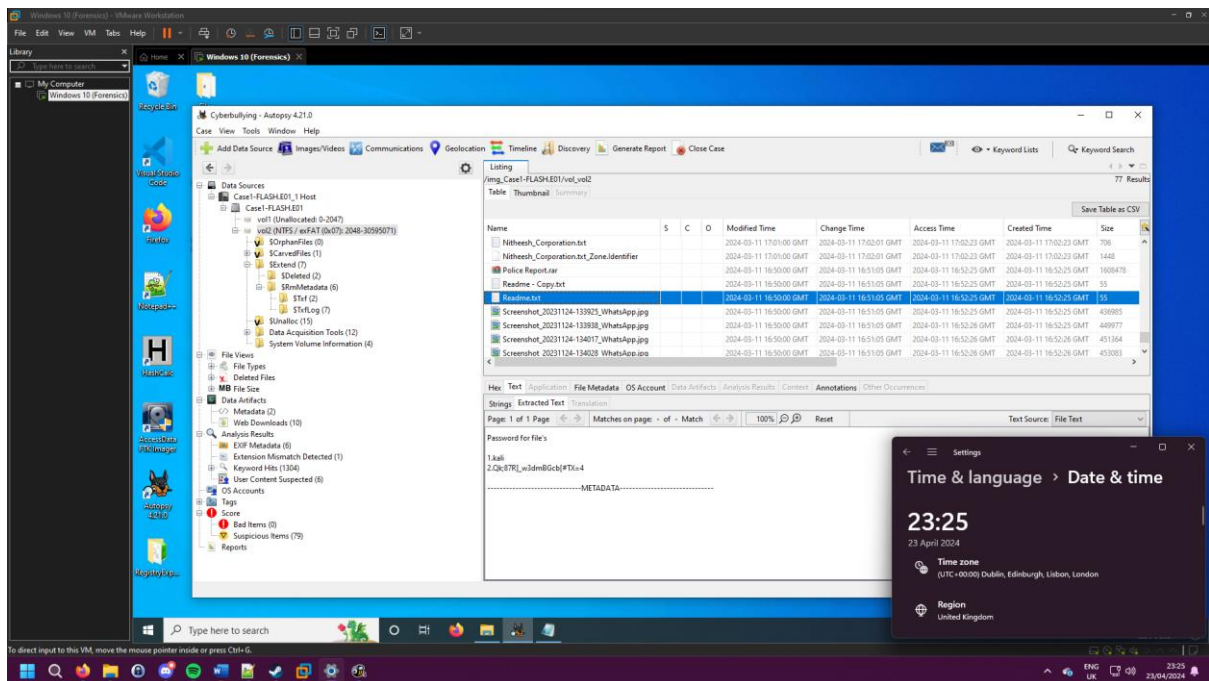
The things that immediately jumped out at me were loads of screenshots of chat logs and a zip file called “Police Report”. The chat logs because the whole point of this investigation is to see whether cyberbullying has taken place or not and typically cyberbullying is done through social media and it’s quite clear that those screenshots are taken from Facebook Messenger and WhatsApp messenger. The police report zip file also because well a police report could give us details about whoever these documents belong to.

For now, I’m going to leave exploring those and drop the image file into Autopsy because it has a feature where it can tell me if any of the files have any metadata that may be useful to me, and it can also tell me if the program itself believe that anything is suspicious and will help extract the metadata without using any other tools.

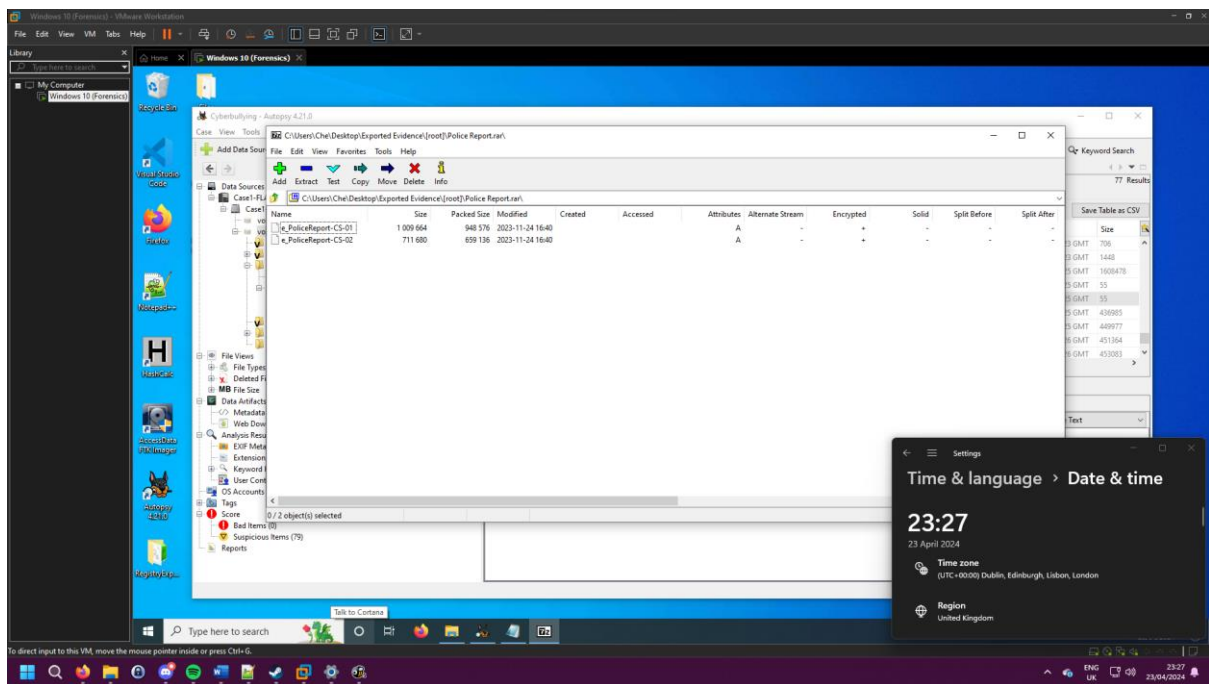




After letting Autopsy analyse the image, it discovered 6 files that had EXIF data available, one of these being an image of a phone which after reading the data seemed to have been taken on the 23rd of November 2023 at 14:07 on a “realme narzo 30 Pro 5G”. There were also a further 5 files discovered that had EXIF data but unfortunately the EXIF data is empty and has nothing notable.

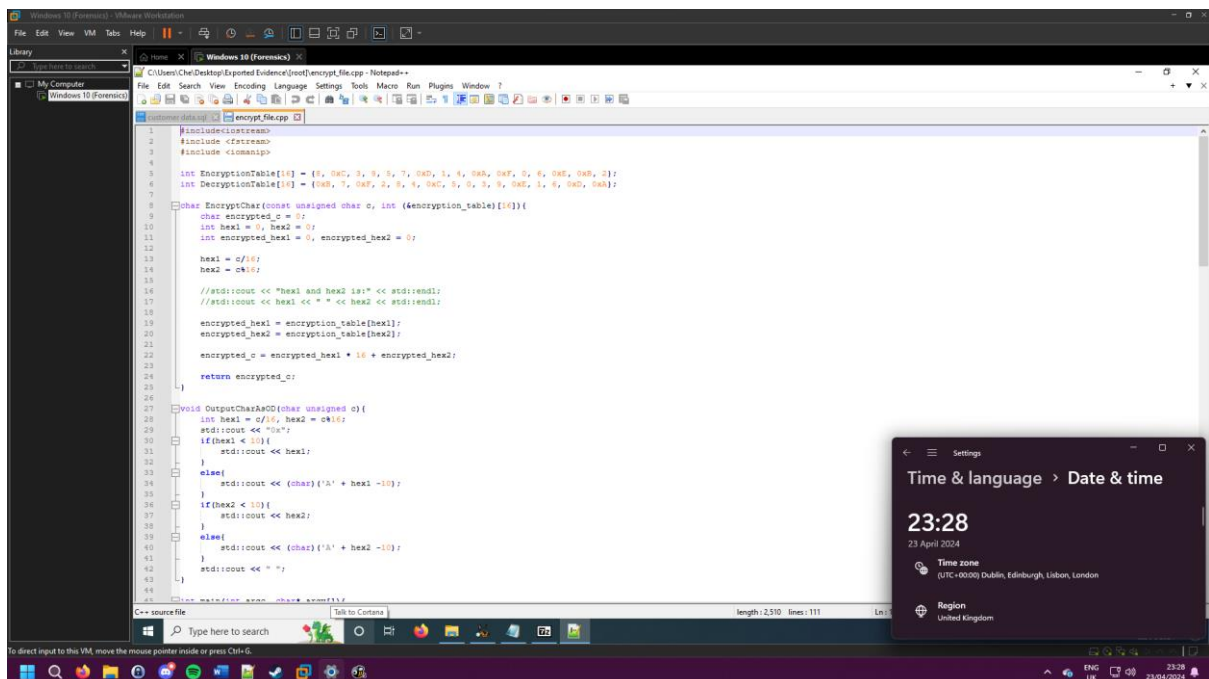


It also discovered some text documents, these were both “Readme” files, both of which contained the same information which were passwords for files, I’m assuming one of these is for the police report zip as that is password protected and therefore unreadable to Autopsy.

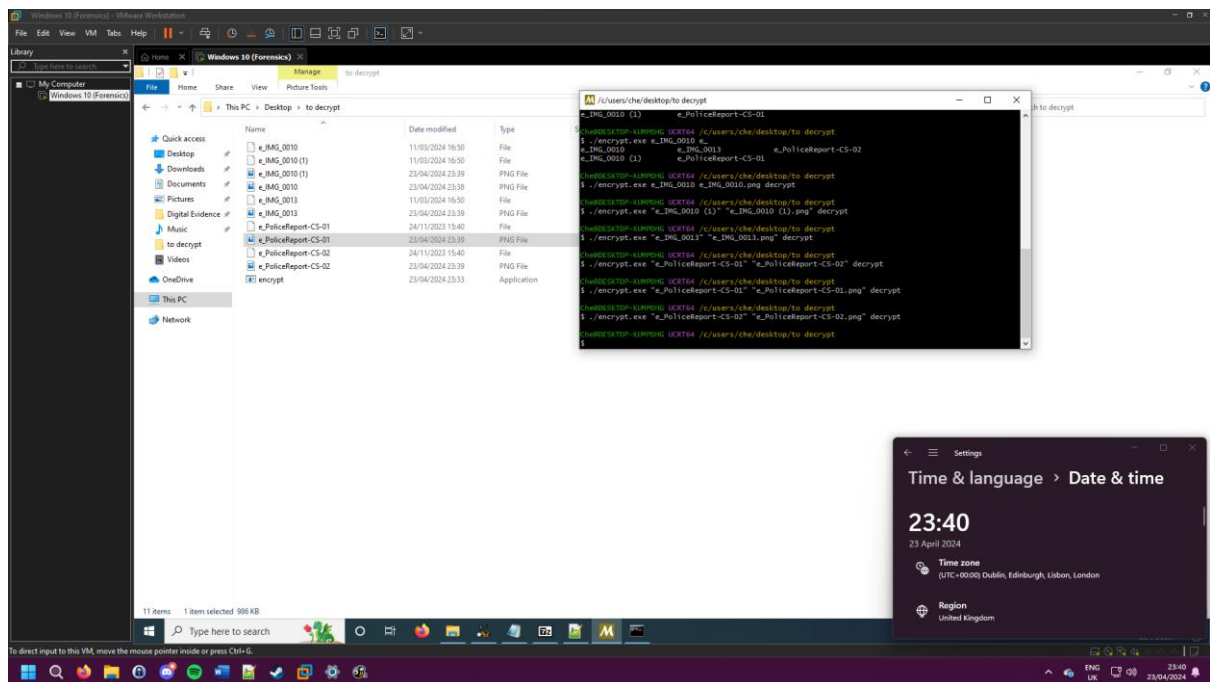


I tried the passwords on the zip, the second one was correct but both files in here seem to be corrupted or encrypted.

Autopsy discovered some files that it labelled “suspicious”, some of these didn’t really seem to stick out but there were some files labelled “e_IMG_0010”, “e_IMG_0010 (1)” and “e_IMG_0013” without file extensions, same as the ones in the zip file. It did not log these as extensions mismatches, so I assumed that they were encrypted in some way. My suspicions were strengthened when I discovered some code on the drive under “encrypt_file.cpp” which I then exported with Autopsy and opened, discovering that it is indeed a file encrypter but also a decrypter.



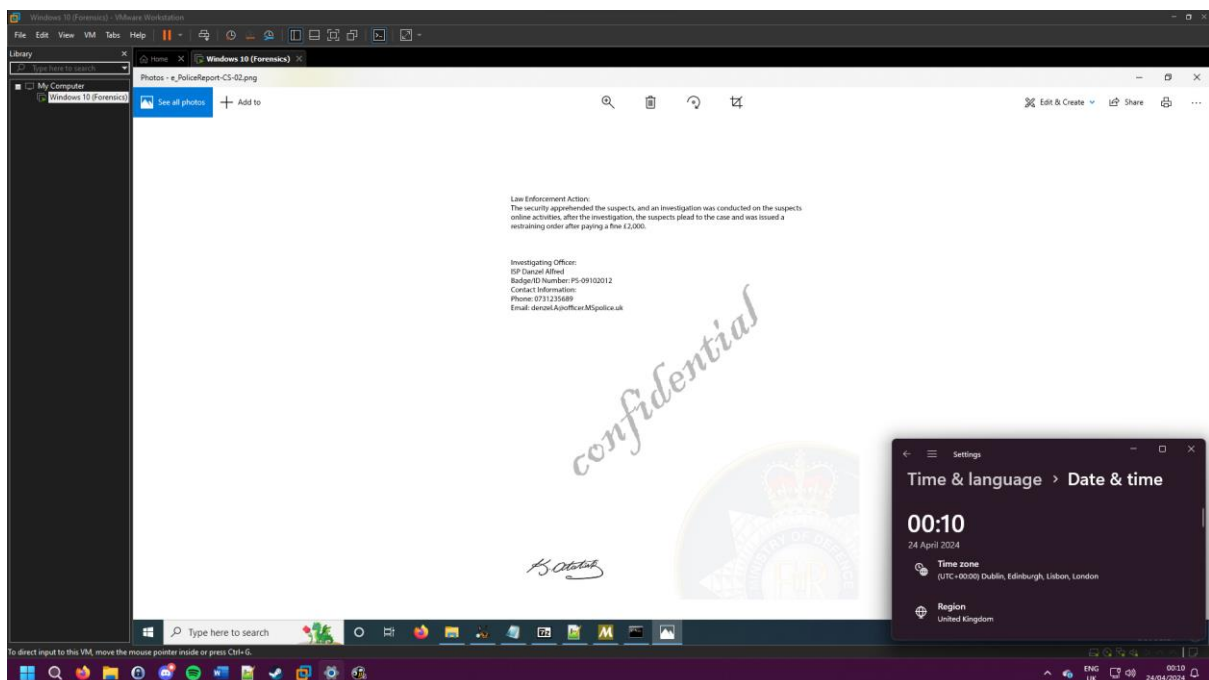
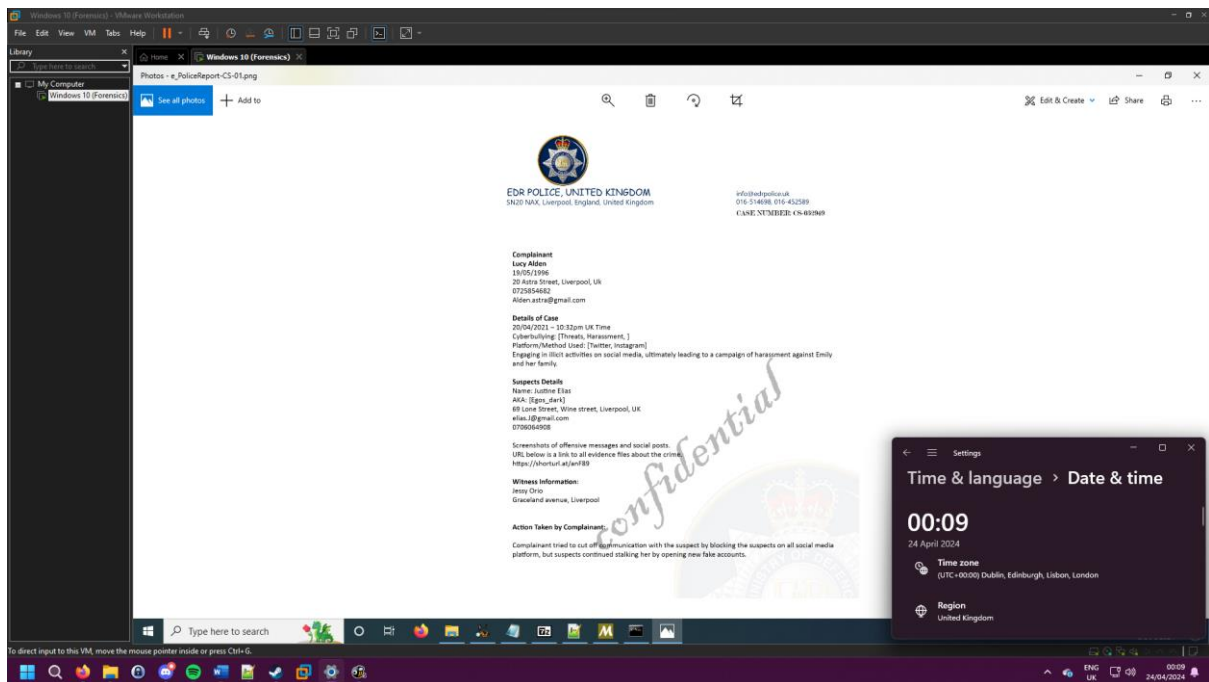
On compiling this file and using it as the code defines, it seems that I was correct and by using the .png file extension, the files are now accessible.



I checked these newly decrypted files, unfortunately they did not contain any useful EXIF data, likely due to the decrypter creating new files.

Key Findings

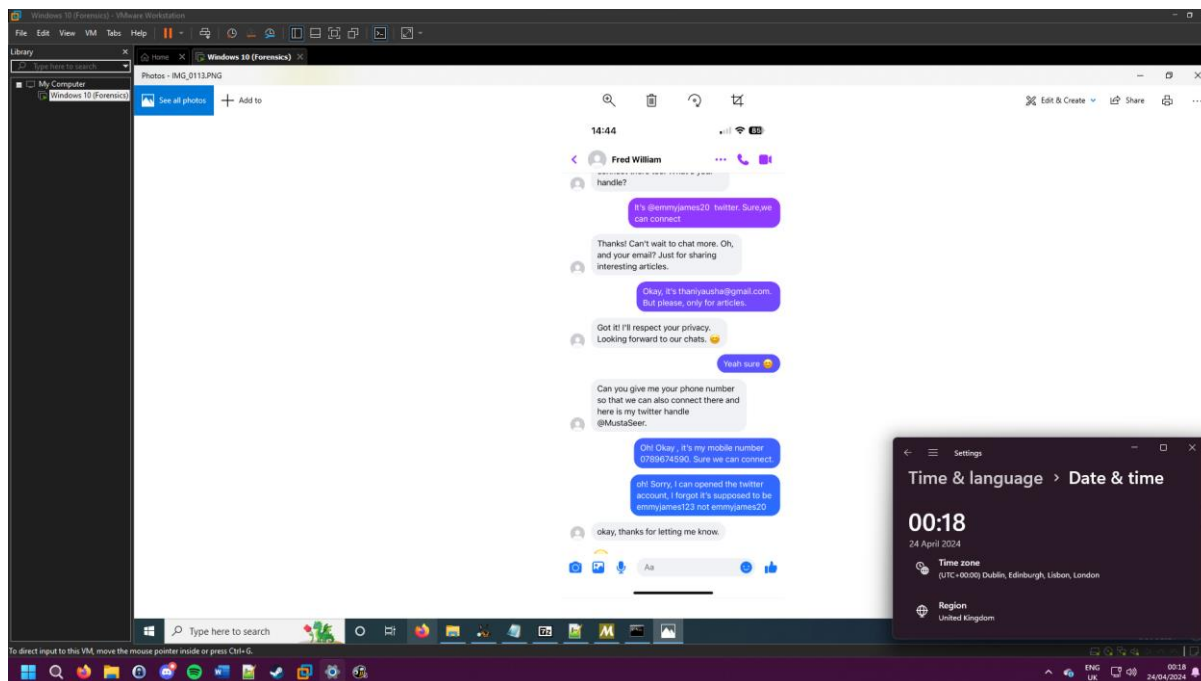
Encrypting Code + Police Report



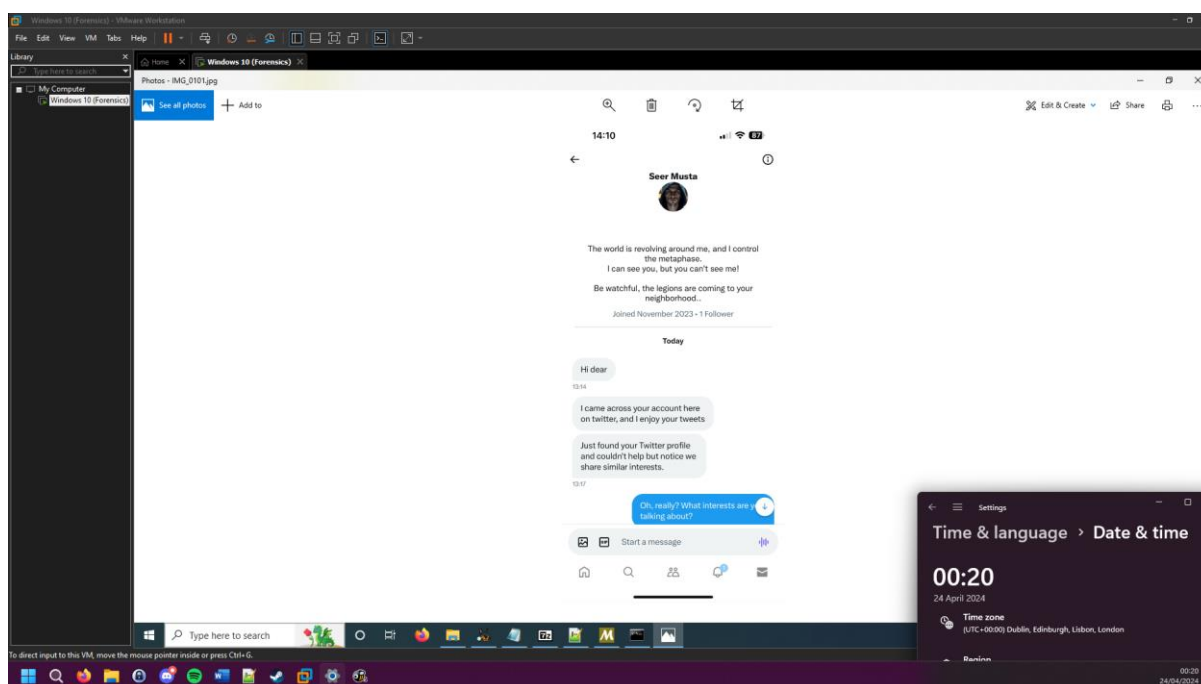
When compiled, the code was able to successfully decrypt the images giving us a police report where someone called 'Lucy Aiden' reported a case of cyber bullying by a suspect called 'Justine Elias'. The URL linking to all of the evidence files goes nowhere but it states that the complaint attempted to cut off communication with the suspect, but they continued to stalk her via other accounts. It also states that after the investigation, the suspect plead guilty and was issued a restraining order and a fine.

Chat Logs

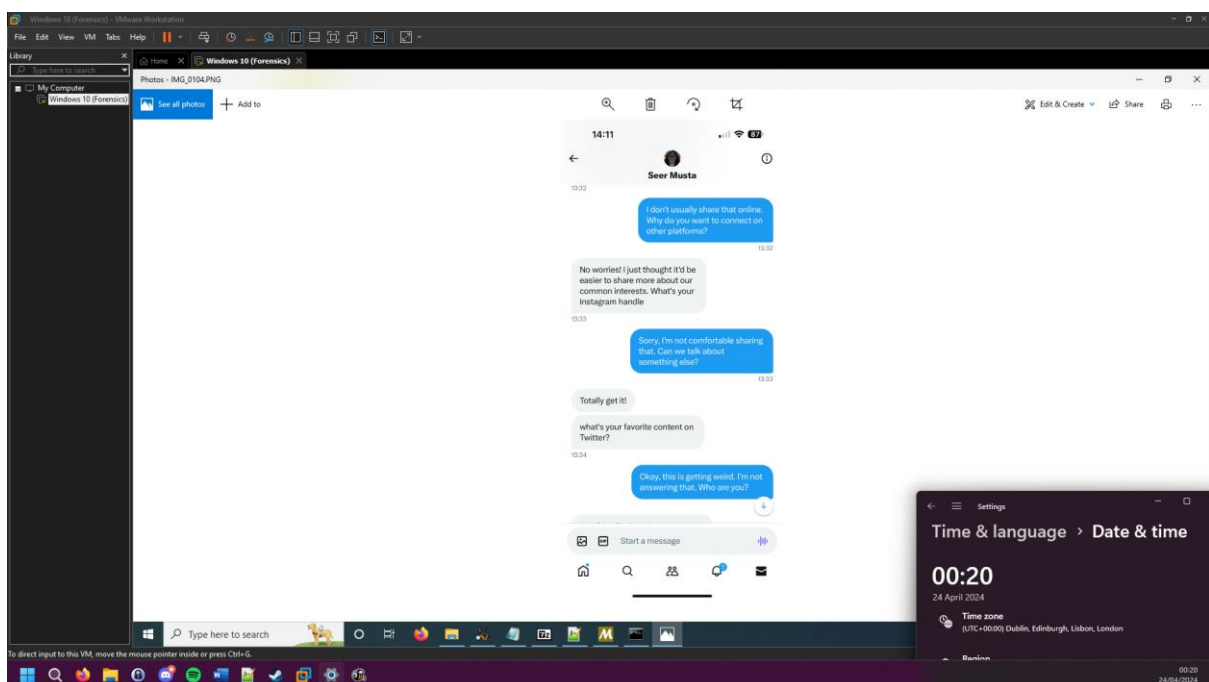
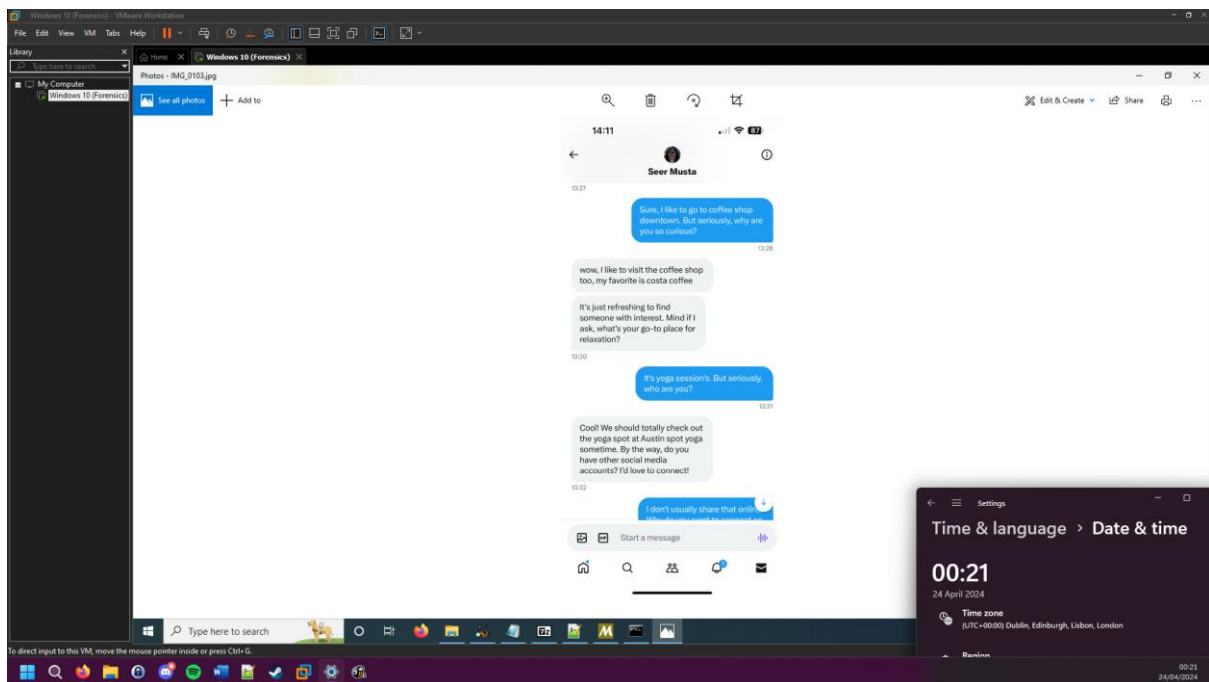
Fred William aka MustaSeer – Facebook & Twitter



This one is quite notable as it shows us the victim's name, this being Emmy James who has a Twitter account called @emmyjames123 and her phone number is 0789674590 and her email being thaniyausha@gmail.com. It also shows that this person "Fred William" who is messaging through Facebook Messenger has a twitter account called @MustaSeer.

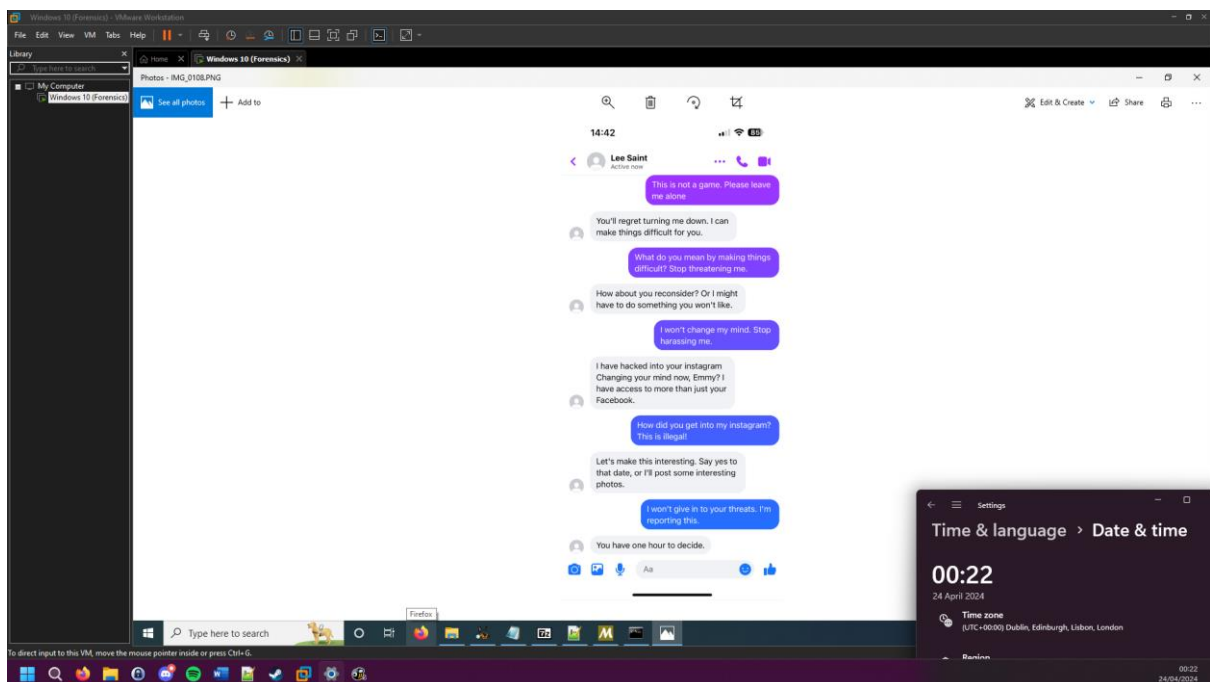
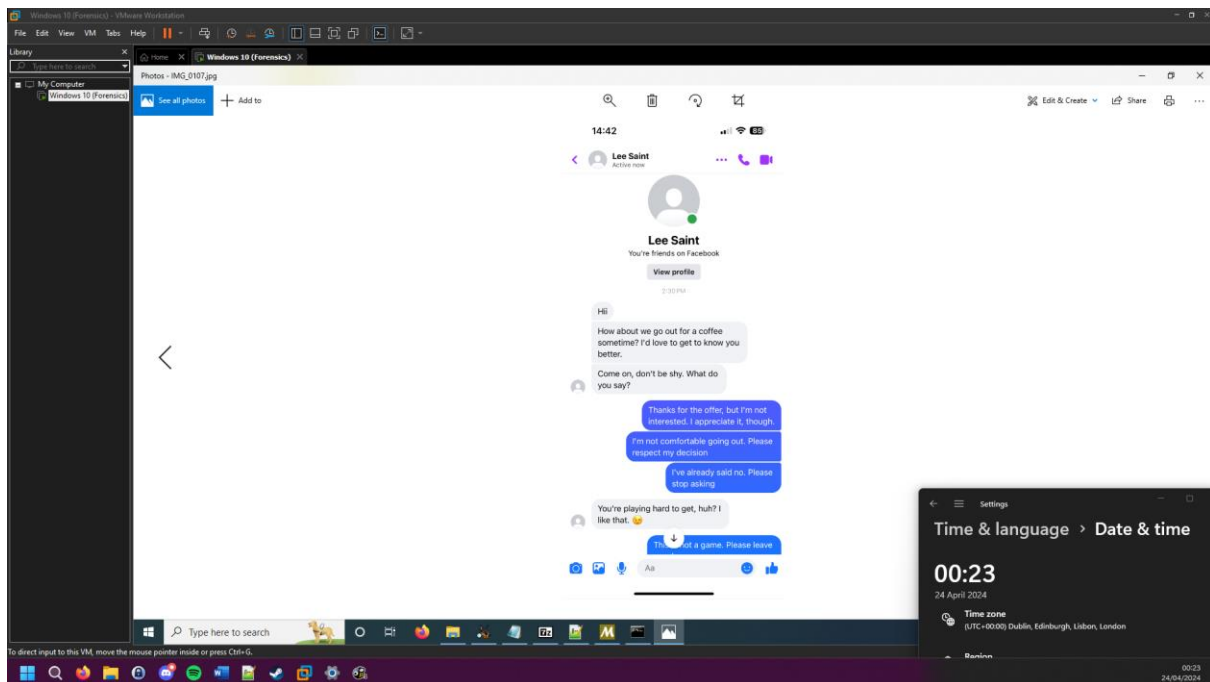


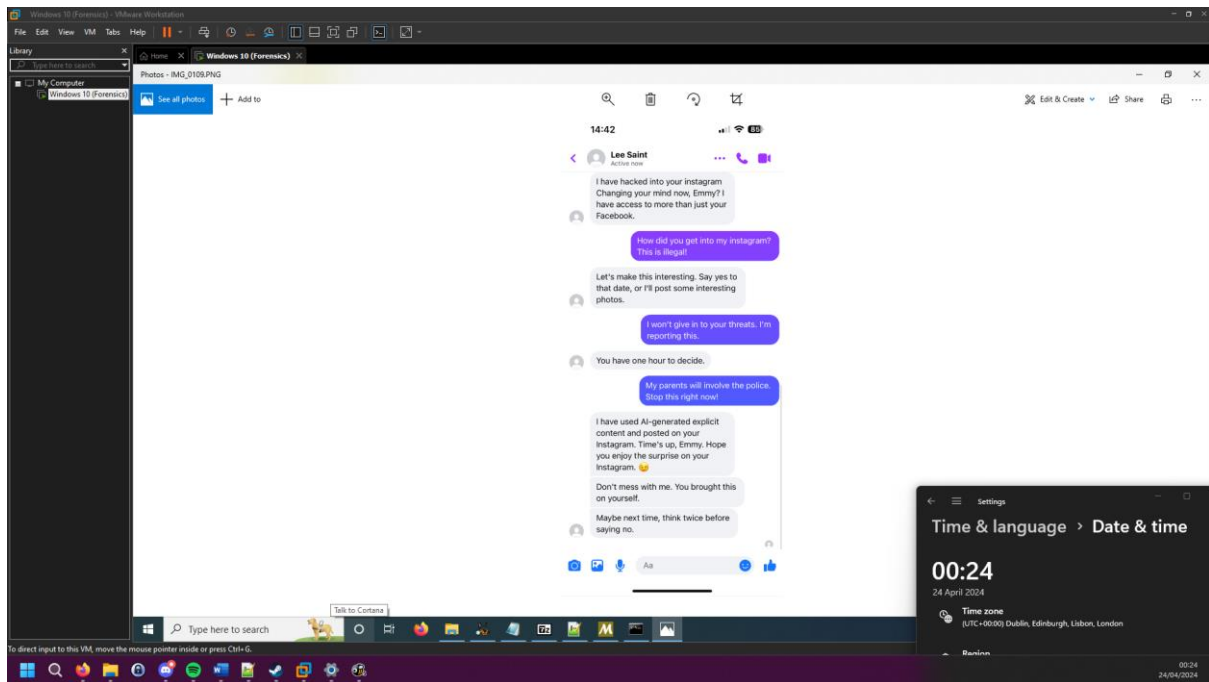
This one as well, this one seems to be the Fred William person now messaging Emmy on Twitter.



Continuing with the other Twitter screenshots, he seems to be making Emmy uncomfortable, asking her personal questions and asking her to meet up.

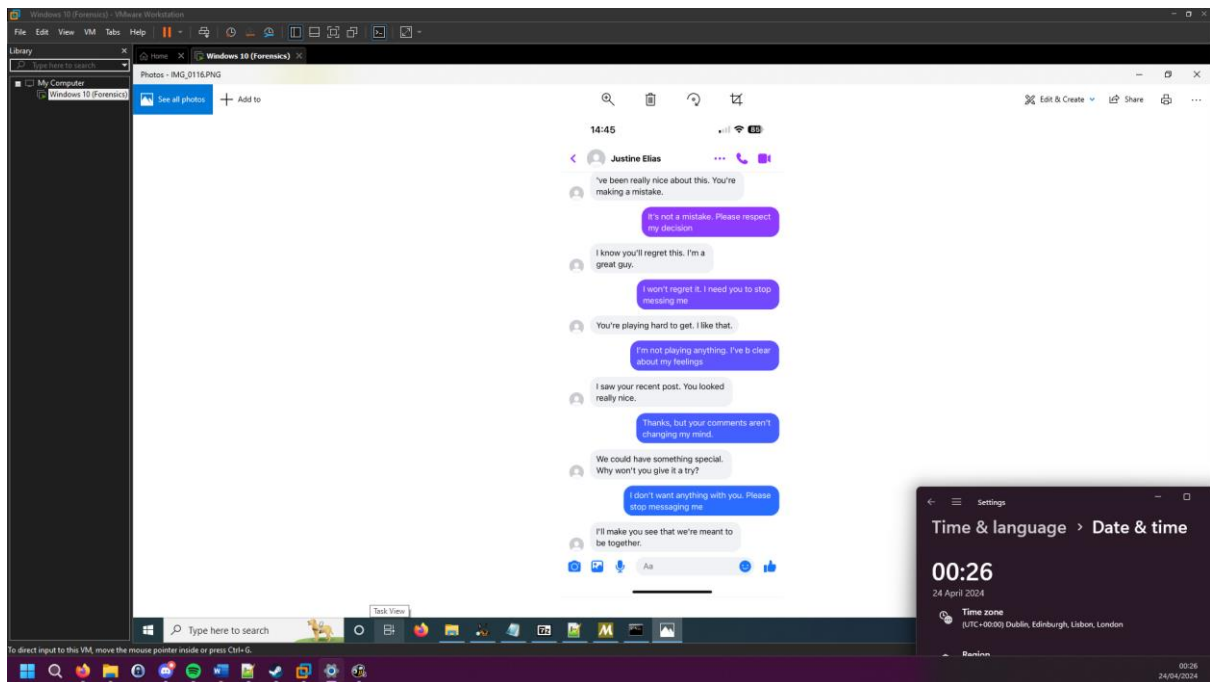
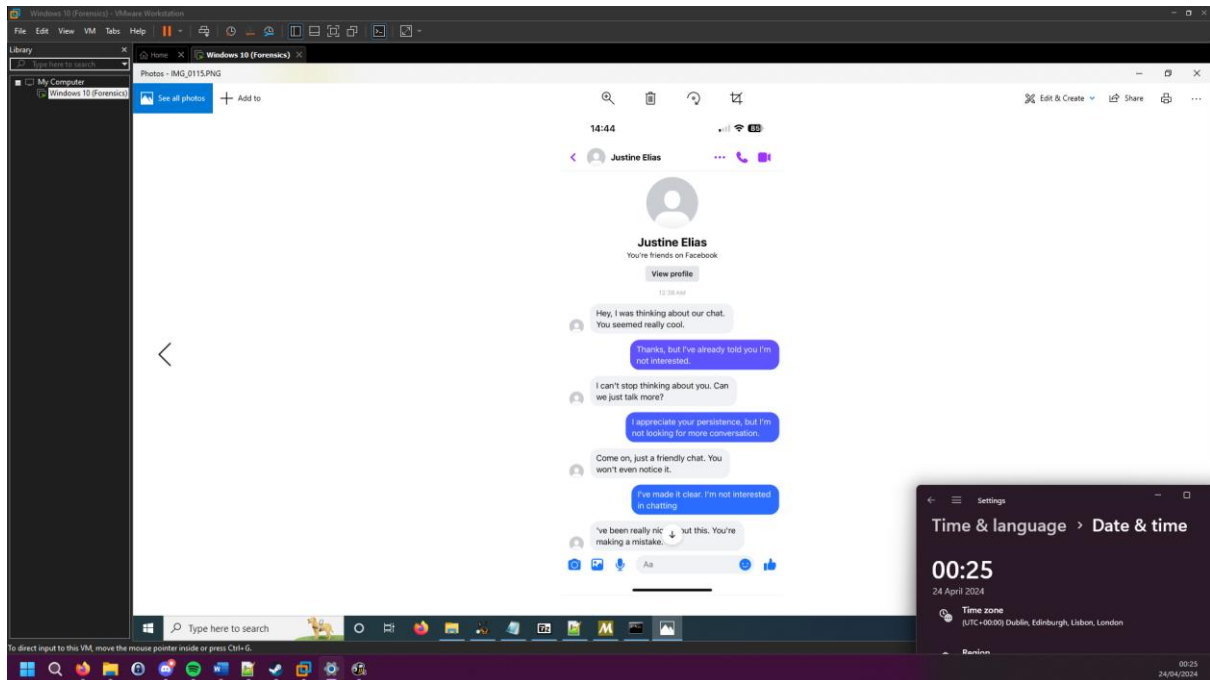
Lee Saint - Facebook

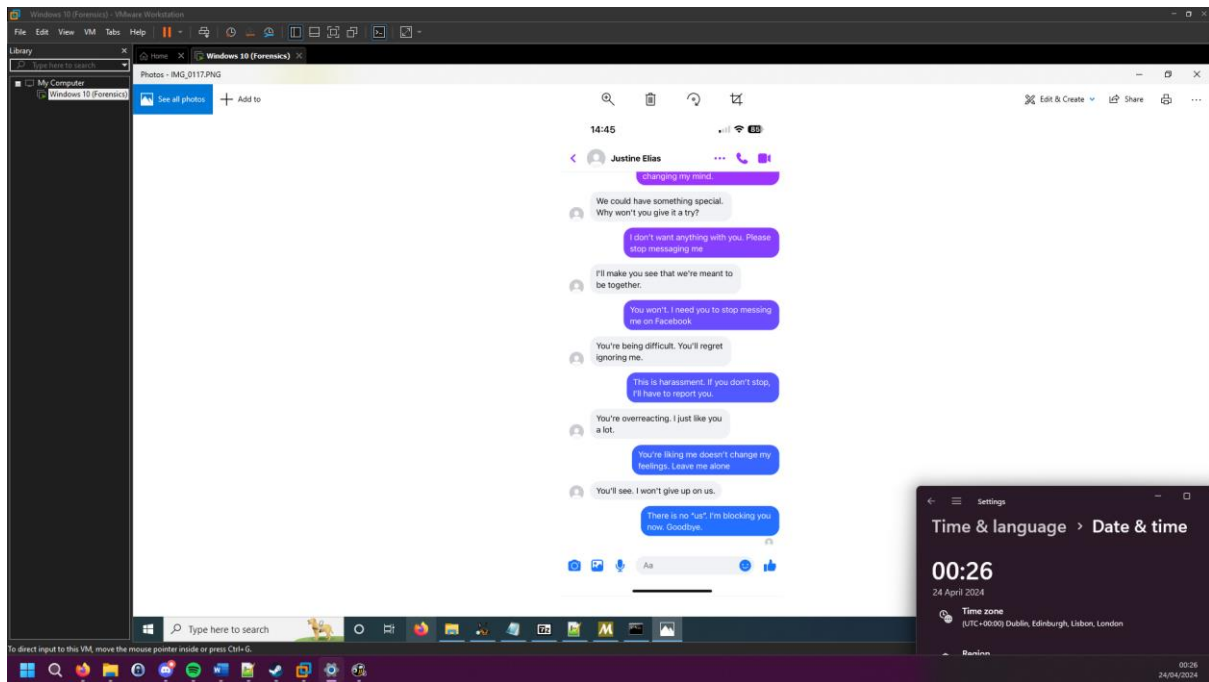




There are three more Facebook Messenger screenshots, these two are Emmy talking to someone called “Lee Saint” who appears to be asking the same questions as the “MustaSeer” from Twitter and after he gets rejected once again, he threatens to hack Emmy and says he’s hacked her Instagram and Facebook and is threatening to leak “interesting pictures”. These turn out to be AI-generated explicit content, I’m assuming of her, onto her Instagram account.

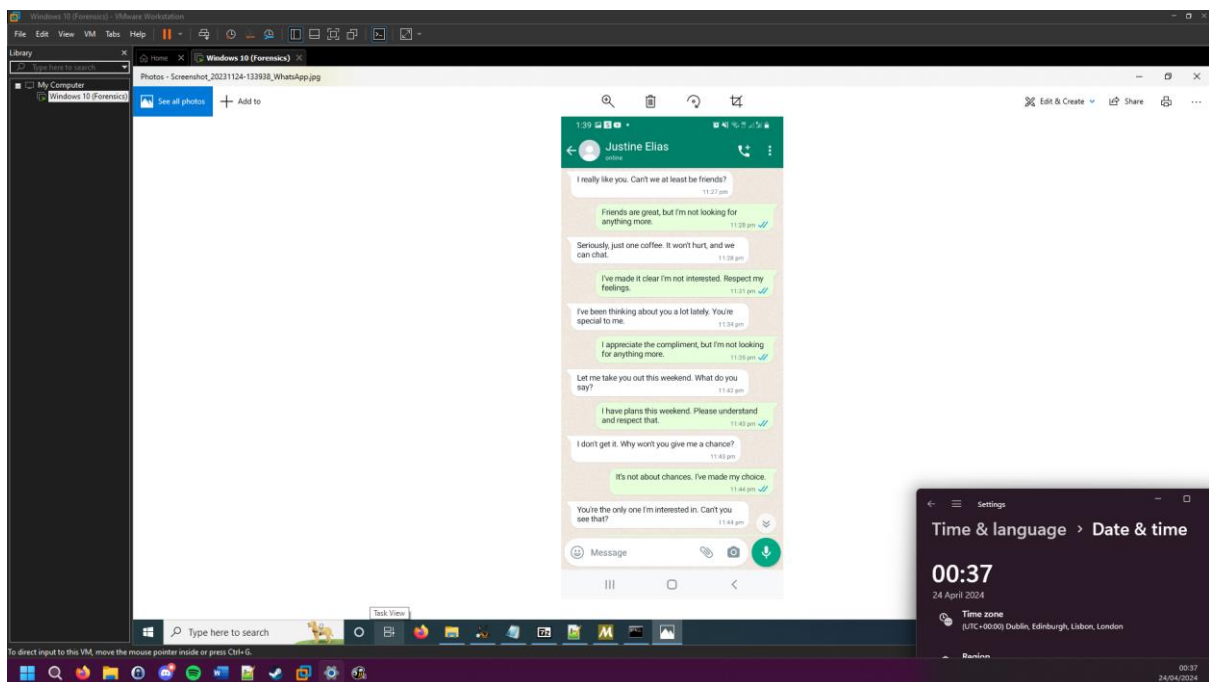
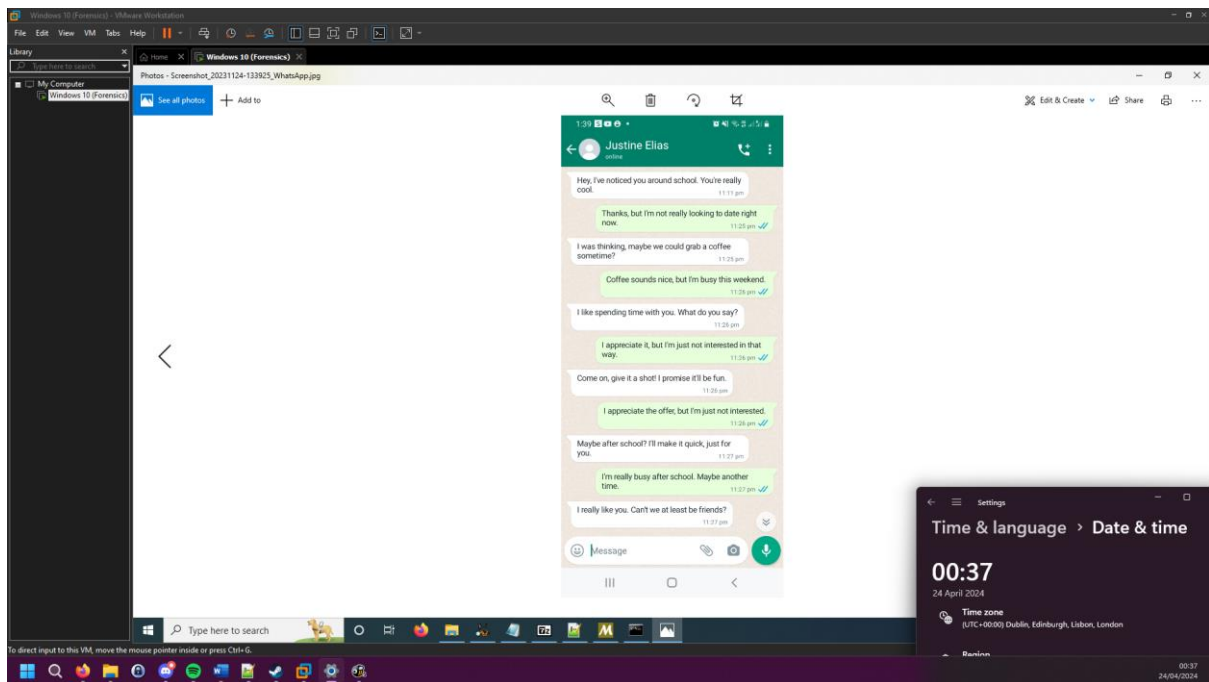
Justine Elias - Facebook

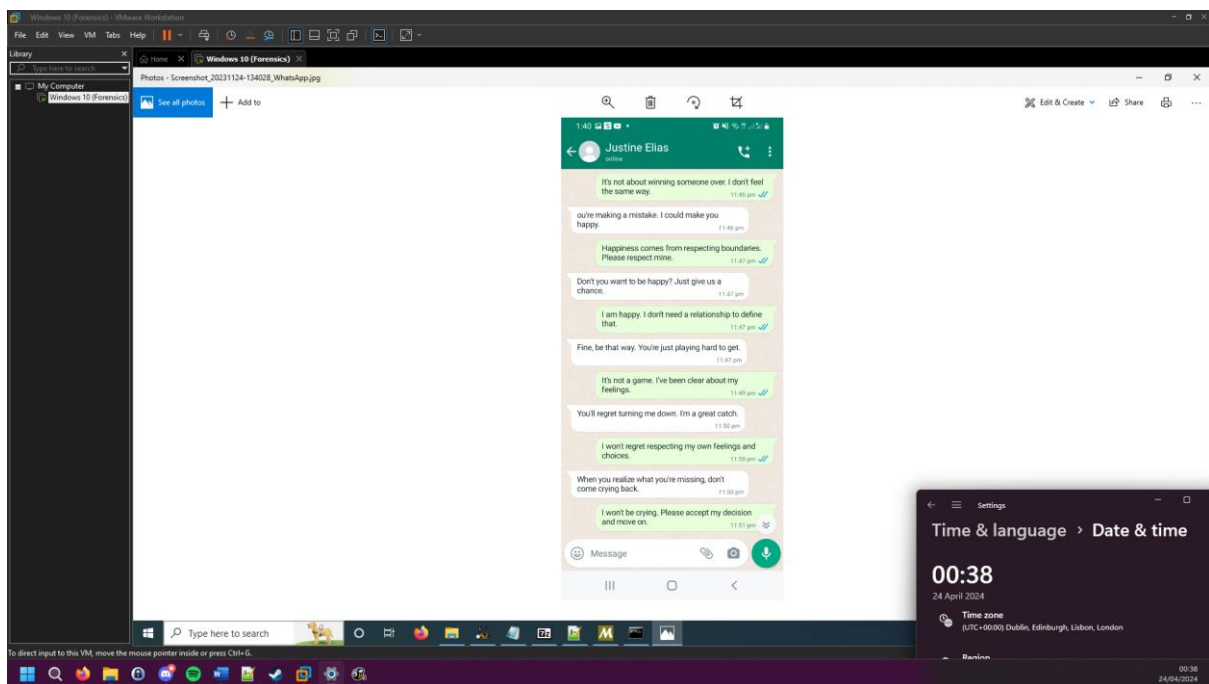
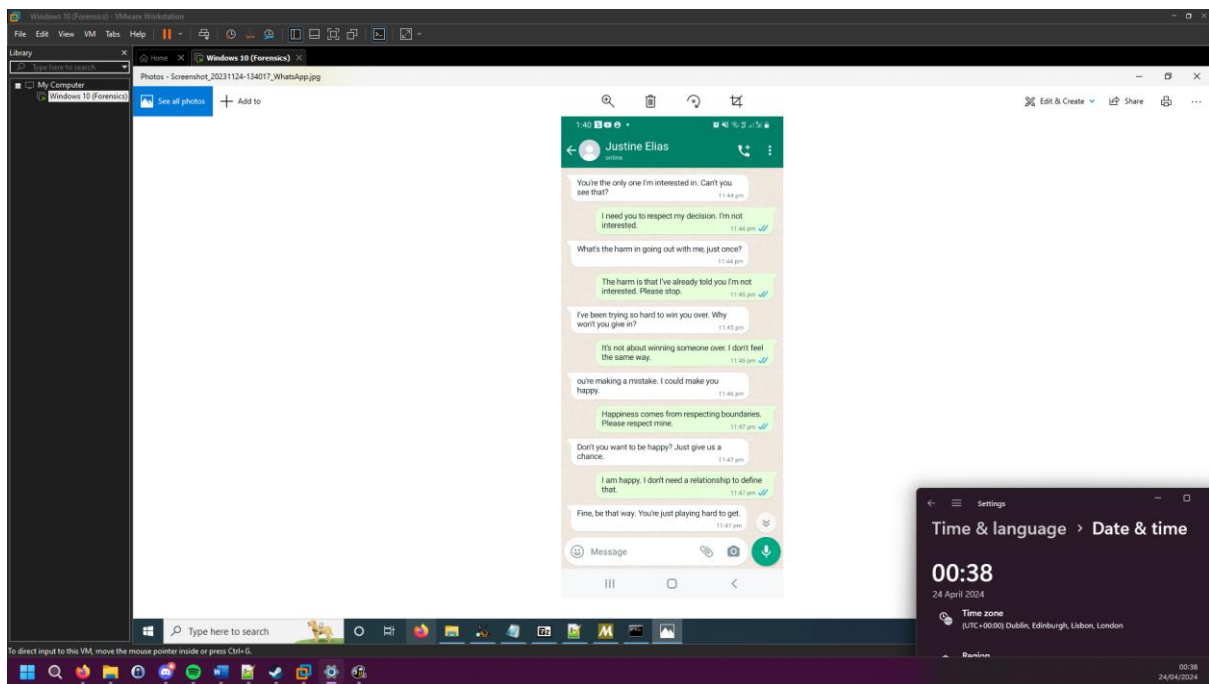




These next three Facebook Messenger screenshots show another account called “Justine Elias”, these ones are particularly interesting as this is the same name as the person who is stated as the suspect on the police report that I decrypted. It seems that he’s back at it again this time with a different victim to the first time. I’m guessing that all these accounts are also his and given the nature of the logs, he seems to be probing Emmy for more information in each chat he has with her.

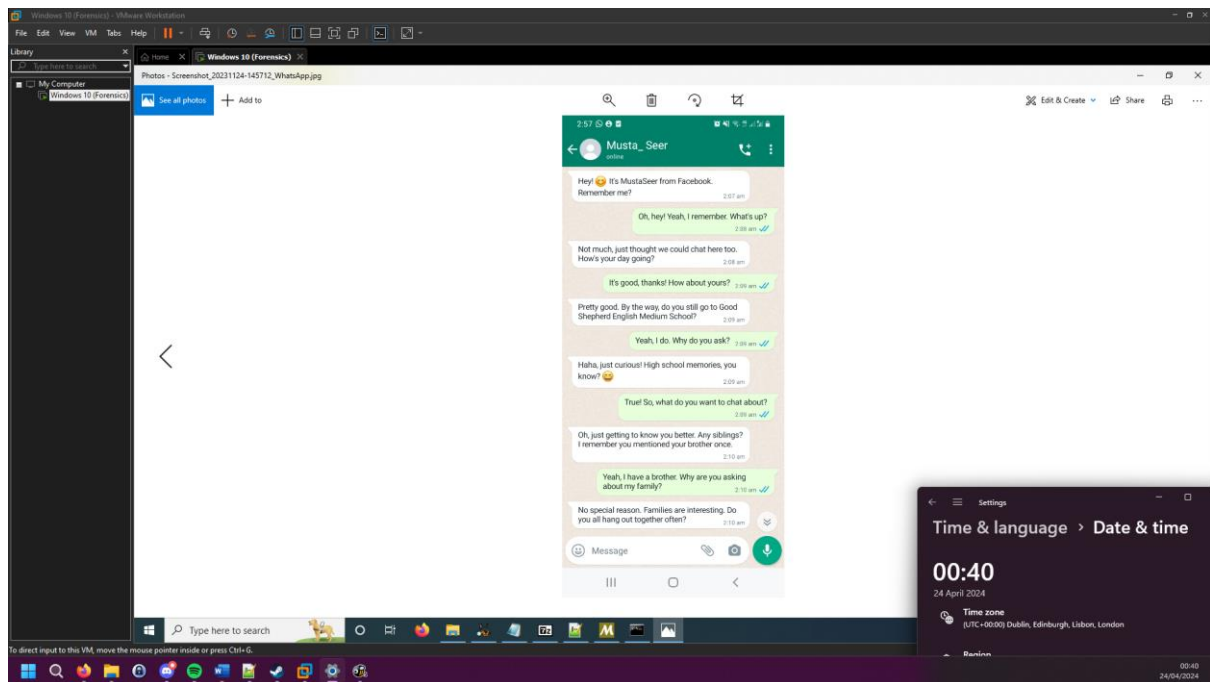
Justine Elias – WhatsApp Messenger





This is once again Justine Elias contacting Emmy, this time through WhatsApp. Once again asking Emmy to meet up. Emmy is clearly uncomfortable here and doesn't want to meet up or be involved with Justine at all.

MustaSeer – WhatsApp



MustaSeer contacts Emmy again, this time through WhatsApp. He seems to be probing Emmy for more information here, asking her what school she goes to and if she has any siblings. I'm guessing he's doing this to gather information to blackmail her.

My Conclusion

I feel like given the evidence that has been recovered, I can conclude that cyberbullying has taken place when taking the evidence found into account. The chat logs make it quite clear that a victim named “Emmy James” has been targeted by someone who continues to ask personal questions and is trying to gather information on her, perhaps to gather enough information to attempt to blackmail her into meeting up with him as that is also something he continues to request for her to do.

The police report also almost confirms my suspicions as whilst the report does not reference Emmy as the complainant, the suspect who was prosecuted in that case for cyberbullying who went by “Justine Elias” has also taken part in cyberbullying and harassing Emmy here. The police report also states that the suspect in that case liked to use alternative accounts to continue to harass and bully the victim, this also leads me to believe that all the users in the chat logs recovered are the same person.

References

[1] D. R. Hayes. *A Practical Guide to Computer Forensics Investigations A Practical Guide to Computer Forensics Investigations* 2015.

[2] M. Reith, C. Carr and G. Gunsch. An examination of digital forensic models. An examination of digital forensic models. 112003.

[3] The Open University. 4.2 *A brief history of digital forensics*. Available: <https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.2>.

[4] I. Resendez, P. Martinez and J. Abraham. I. Resendez. An introduction to digital forensics. An introduction to digital forensics. 17172014.

[5] Eclipse Forensics. 3 famous cases solved through digital forensics. 3 famous cases solved through digital forensics. 2021. Available: <https://eclipseforensics.com/3-famous-cases-solved-through-digital-forensics/>.