

Computer Forensics: Coursework

Research and Report:

[1] Forensics is a discipline that encompasses various sub-domains such as digital forensics, including computer forensics, mobile forensics, network forensics, etc.

[2] Digital forensics emerged in the 1970s, while computer forensics, as a sub-domain of digital forensics, emerged in the 1980s.

[3] Computer forensics is about storing data for analysis, The Computer Forensics in the analysis uses many techniques that include cross drive analysis, live analysis, recovery of deleted files, stochastic forensics and steganography. To explain the most used method in this area is Recovery of deleted files, it is often used because criminals often seek to hide the evidence, being able to charge them. One of the facts that allows investigators today not to be ineffective in this technique is that despite files destroyed to the maximum of what we can, it should be known that Operating Systems and File Systems always keep data files, and so the investigators have the ease of being able to rebuild them quite easily.

[5] The evolution of digital forensics over the years, starting from the 1970s, has been driven by the need for robust techniques to collect evidence from digital objects, particularly with the expansion of the internet. Identity theft and hacking were significant issues then and remain so today. In the 2000s, standardisation efforts led by organisations like the International Association of Computer Investigative Specialists (IACIS) and the National Institute of Standards and Technology (NIST) provided guidelines for digital forensic investigations.

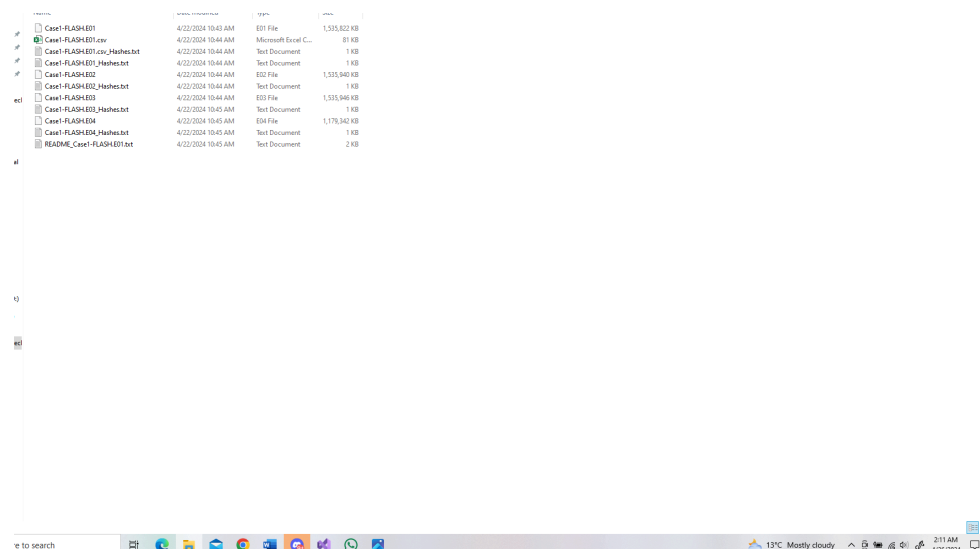
[6] As technology advanced, new branches of digital forensics emerged to address the challenges posed by mobile phones, USB drives, memory cards, cloud computing, and virtualization. These advancements, though complex, have improved the efficiency of digital forensic analysis.

[7]Now we will see an example of cases where digital forensics proved very useful, in 2009 the Craigslist Killer case. Craigslist to understand the case is an American website with classified ads and discussion forums. In April a woman was found dead in her hotel room, with no evidence to suspect an individual, and another complaint was made of an assault for armed robbery. Once the second victim is established, a link is made through the Craigslist application where the two women were in communication with the same person who would be named Andy, where the digital forensics was useful in this case is to trace the IP of this Andy, who will turn out to be Philip Markoff a young man of 23 years. This case will be a great victory in the end demonstrating the usefulness of Digital Forensics in this kind of case.

Today, digital forensics plays a critical role in criminal investigations, including cybercrimes, fraud, and hacking, as well as in counterterrorism efforts, where it is used to track communications, monitor financial transactions, and analyse social media content. Computer Forensics primarily supports Digital Forensics, assisting in tasks such as copying databases, and shares techniques with its parent field.

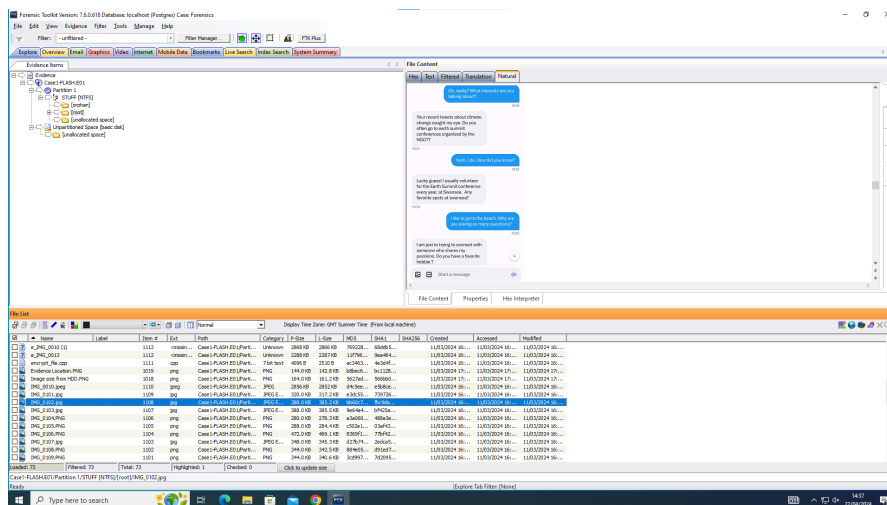
TASK 3:

[8]In week 6 we had to play the role of investigator and analyser of a disc, so following the

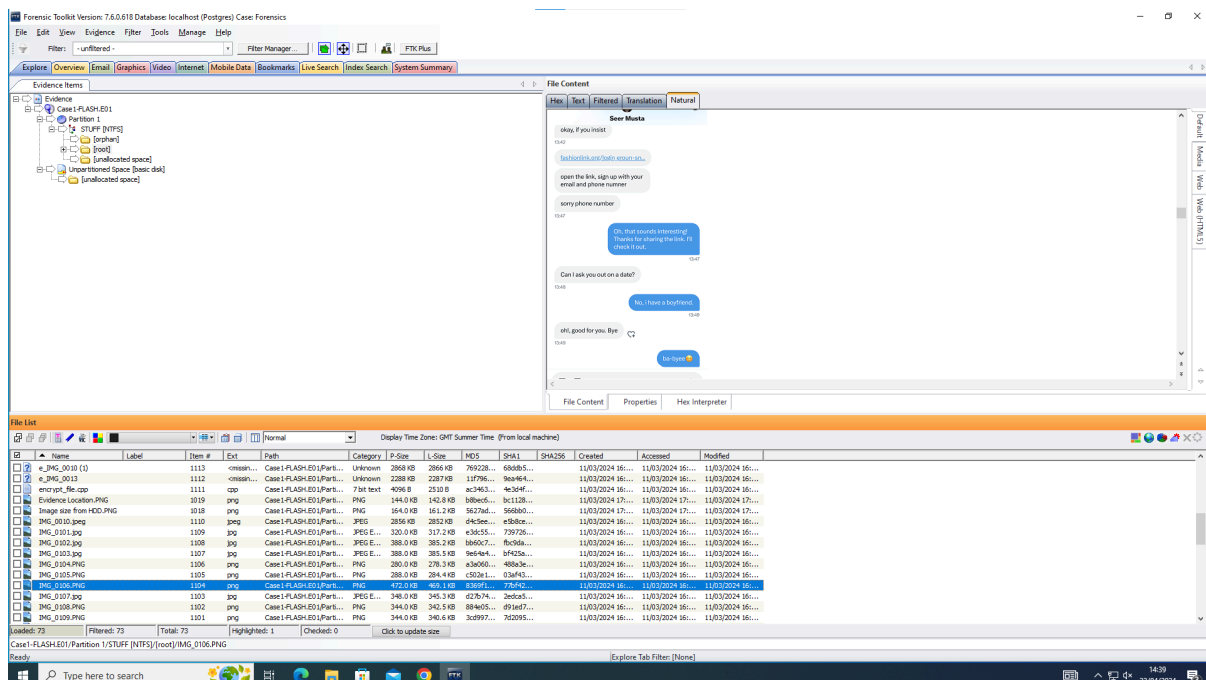


chain of custody, we each established a task to do to avoid attacking the credibility of what we had collected. As a team we managed to extract these files from this image. . To start our investigation we have download all the data on a Windows virtual machine to avoid many problems compared to corrupted files, having seen no problem in perspective following this I put the document in Hash Calculator to obtain a Hash and be able to check the integrity of the data downloaded having had an MD5 which on the virustotal website gave me no problem I

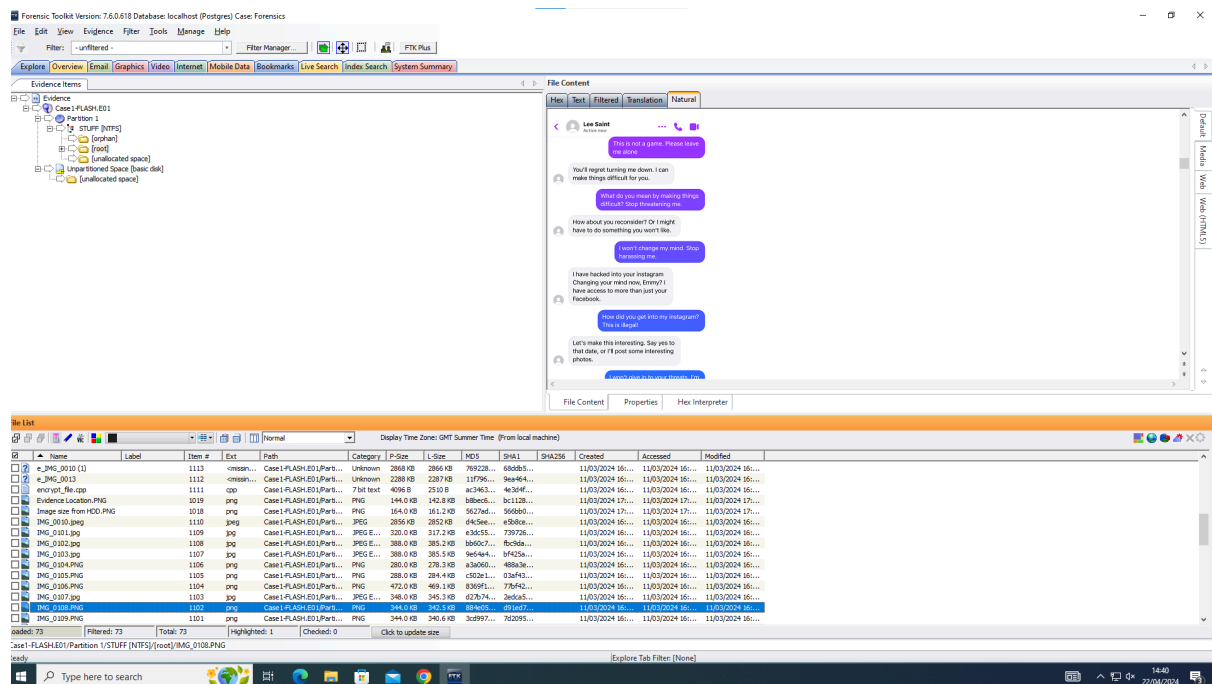
transferred the files to my computer so that FTK can analyse them, which is a tool to make Disk Imaging, to ensure data integrity, it also makes file hashing for individual files, and



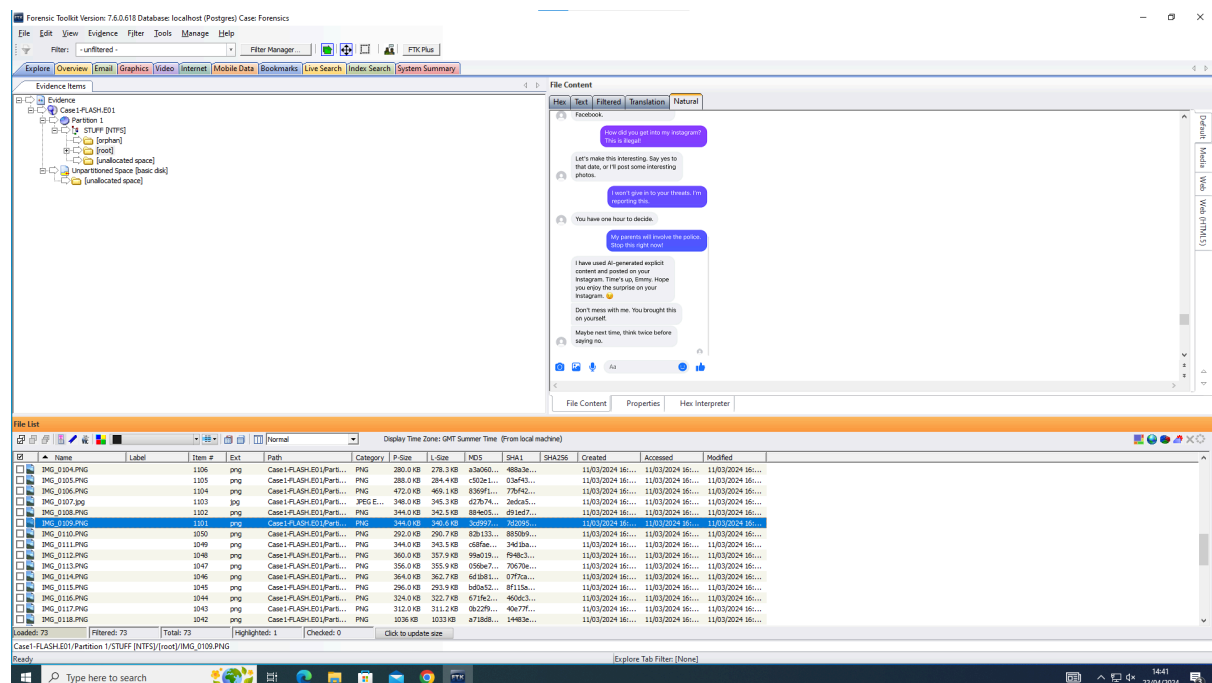
finally it makes reports on the files with the information it gets by analysing them. So I made manipulations using FTK to grant me editing rights to create boxes that I can not do if I do not have Admin rights on my profile. Once this is done, the goal is to create a file where the data can be downloaded as well as the images, it is filled in the "Case Folder Directory" frame. Then once this was done I could import a file named E01 to analyse it in FTK to have the images of the files present in this document. I then observed thanks to the analysis of the files on FTK many documents with extension png, jpeg and jpg, which are thus image files,



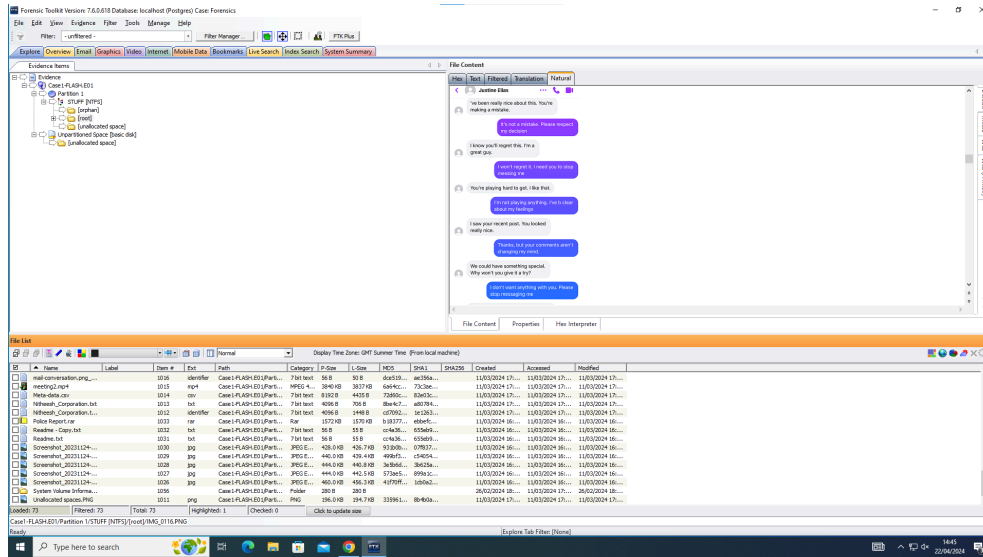
above one observes numerous discussions between two people, made on social networks such



as Messenger, Whatsapp and even Instagram. In the first screenshots I found, we find a naive person being asked for personal information by someone she doesn't know, one can therefore assume that there is an attempt to take information about a person for malicious purposes to



act under a different identity. The attempt to take information on the first screenshot is made by taking confidence from the scammer to the victim who grants his trust easily only because of interest in similar activities. In the second image we can see that a certain named Seer



Musta sent a link via Messenger to the alleged victim. This may sound strange given that this is the beginning of a discussion, so we can establish the fact that in this case Seer Musta is only trying to do phishing, a technique that consists of the scammer to impersonate an organisation by copying their website or by message. [9] Then the victim writes confidential data such as his email with his password and is redirected to the real page of the organisation, but at the same time the scammer was able to get the victim's username and password. In the case that we have besides Seer Musta explains in the form to need the mail, which therefore seems this directed towards my intuition. In the third image we have a case of cyberbullying where the harasser is called Lee Saint, who seeks to have a date with the victim of his messages. Lee Saint made threats in these messages, despite the victim's reluctance to talk to him. He ends up telling her that if the victim continues to refuse, using the hacking he did on the victim's account, he would post content without any agreement from the owner of that account. To conclude Lee Saint gives a time limit before posting content on the account. So this is a case that totally represents cyberbullying. In image 5 we can see again a case of harassment against a victim who seeks to cut off contact with his harasser and refuses all requests. In the following case we have a discussion on Whatsapp, where two people discuss their interests in their lives. The harasser, therefore the blank messages, asks for a lot of different information about the victim and his habits. The victim in his naivety answers his questions allowing the harasser to know a little better his victim for some unknown purpose. At the very end of the discussion, however, the victim realises that his attacker knows that she has returned, and therefore asks him with doubt how he is aware, while he does not normally know the address of each. One can therefore assume in this case that the harasser does illegal spying on the victim surely for ill-intentioned purposes.

[10] In the rest of my research, I noticed in the analysis of the disk two suspicious files. One

[illegible]

with the name of the Police report and the second, with an extension in .cpp (emcrypt_file). So I guess I had to decrypt a file. By doing a search on the internet I found that it was a code in C++ and that would allow me to decode files. So using visual studio I imported it into a

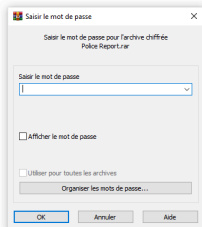
ID	Name	Label	Type #	Ext.	Path	Category	P-Size	L-Size	MDS	DNA1	DNA26	Created	Accessed	Modified
?	e_img_010 (1)		1113	csp	C:\e-FLASH-E01\Part...	Unknown	266B KB	266B KB	769228	49d6d1...		11/03/2024 16...	11/03/2024 16...	11/03/2024 16...
?	e_img_0013		1112	csp	C:\e-FLASH-E01\Part...	Unknown	228B KB	2237 B	137596	9ea464...		11/03/2024 16...	11/03/2024 16...	11/03/2024 16...
?	enrpf_rec.opg		1111	opg	C:\e-FLASH-E01\Part...	7bit text	4096 B	2310 B	ca3ec3...	4efc9af...		11/03/2024 16...	11/03/2024 16...	11/03/2024 16...
?	enrpf_loader.PNG		1109	pnp	C:\e-FLASH-E01\Part...	PNG	144.0 KB	143.9 KB	b8bc65...	bc1328...		11/03/2024 17...	11/03/2024 17...	11/03/2024 17...
?	Image size from HCD.PNG		2018	pnp	C:\e-FLASH-E01\Part...	PNG	164.0 KB	161.2 KB	96c2da...	5ee880...		11/03/2024 17...	11/03/2024 17...	11/03/2024 17...
?	HCD_0101.jpg		1110	jpgp	C:\e-FLASH-E01\Part...	PJPG	285B KB	2852 KB	643ccc...	e59ebc...		11/03/2024 16...	11/03/2024 16...	11/03/2024 16...
?	HCD_0101.jpg		1109	pnp	C:\e-FLASH-E01\Part...	PJPG	320.0 KB	317.2 KB	a4c655...	739728...		11/03/2024 16...	11/03/2024 16...	11/03/2024 16...
?	HCD_0103.jpg		1108	pnp	C:\e-FLASH-E01\Part...	PJPG	388.0 KB	385.3 KB	89cc77...	6c566e...		11/03/2024 16...	11/03/2024 16...	11/03/2024 16...
?	HCD_0103.jpg		1107	pnp	C:\e-FLASH-E01\Part...	PJPG	388.0 KB	385.5 KB	9e04dc...	bf4f25a...		11/03/2024 16...	11/03/2024 16...	11/03/2024 16...
?	HCD_0104.PNG		1106	pnp	C:\e-FLASH-E01\Part...	PNG	280.0 KB	279.3 KB	d3e0e0...	40ba3e...		11/03/2024 16...	11/03/2024 16...	11/03/2024 16...
?	HCD_0105.PNG		1105	pnp	C:\e-FLASH-E01\Part...	PNG	288.0 KB	284.4 KB	c5021c...	03a4f3...		11/03/2024 16...	11/03/2024 16...	11/03/2024 16...
?	HCD_0106.PNG		1104	pnp	C:\e-FLASH-E01\Part...	PNG	472.0 KB	469.1 KB	8369f1...	75a4a2...		11/03/2024 16...	11/03/2024 16...	11/03/2024 16...
?	HCD_0107.jpg		1103	jpgp	C:\e-FLASH-E01\Part...	PJPG	348.0 KB	346.3 KB	d2707a...	3edac5...		11/03/2024 16...	11/03/2024 16...	11/03/2024 16...
?	HCD_0108.PNG		1102	pnp	C:\e-FLASH-E01\Part...	PNG	344.0 KB	342.5 KB	8b4c65...	d91aff7...		11/03/2024 16...	11/03/2024 16...	11/03/2024 16...
?	HCD_0109.PNG		1101	pnp	C:\e-FLASH-E01\Part...	PNG	344.0 KB	340.6 KB	3c9997...	7d2095...		11/03/2024 16...	11/03/2024 16...	11/03/2024 16...

Loaded: 73 Filtered: 73 Total: 73 Highlighted: 1 Checked: 0 Click to update size

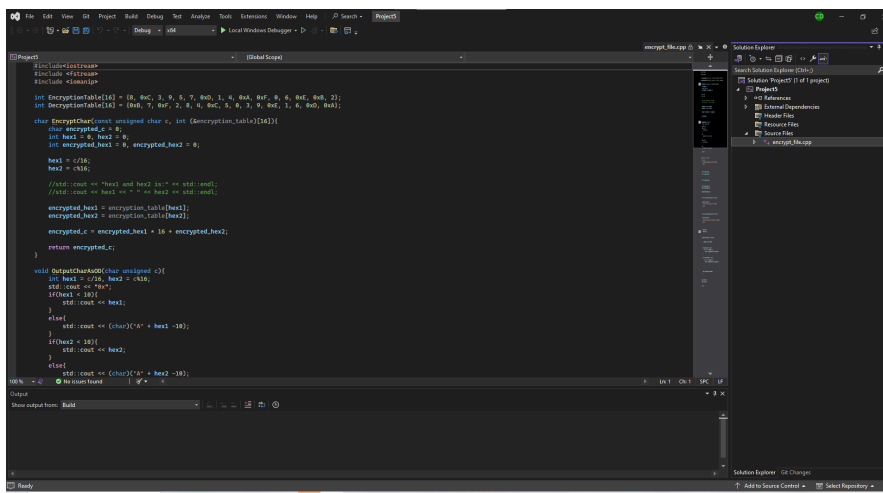
C:\e-FLASH-E01\Partition 1\STUFF (NTFS) [root]\HCD_0102.jpg

Ready Explore Tab Filter: [None]

project. The goal for me was then to find files to decrypt. The font report interested me because of its extension .rar. So I tried to access this file, on which Winrar asked me for a password. The password was in the disk scan in a text file named README. So I discovered



two files without any extension and tried to decrypt them with the program in C++. By



Clement DURYE
2325578

Coursework Computer Forensics

working a little with Visual Studio I was able to get a .png. The image document is a complaint made by Lucy Alden to Justien Ellias for reasons of harassment on social networks, including threats, The owner continues to stalk the victim by creating new fake accounts. This seems to be an official document from the Police and 2000 pounds has been defined as a fine.



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

info@edrpolic.uk
016-514698, 016-452589
CASE NUMBER: CS-032949

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.

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:

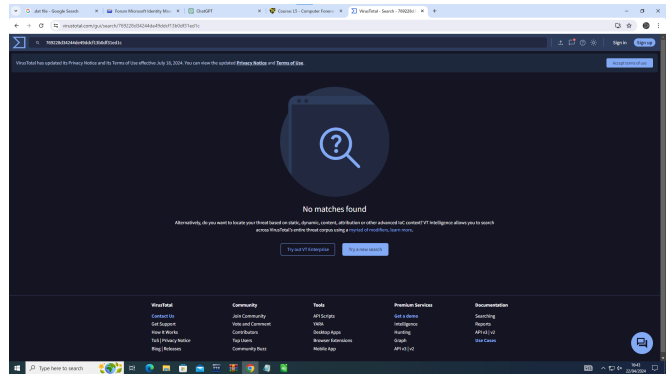
Jessy Orio
Graceland avenue, Liverpool

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.

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

The rest of my research concerned other files without extension that I tried to decrypt, but with no success it was the files, e_IMG_0013 and e_IMG_0010. So I still before putting in decryption managed to calculate a hash value that did not correspond to anything known, moreover the photos show it. It is marked that the given hash is unknown in VirusTotal databases, I wanted to check if the hash also changed between two calculators so first I did it with FTK and then with Hash Calculator and both found the same. Despite all my efforts on these two files, I could not find what it corresponded to. By also trying to assign them an image extension it did not work. So I abandoned my research on his files without any clue as to what he could give me as information.



The screenshot displays the Forensic Toolkit (FTK) interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, Manage, and Help. Below the menu is a toolbar with icons for file operations and a filter dropdown set to 'unfiltered'. The main window is divided into several panels:

- File List:** A table listing files with columns for Name, Label, Item #, Ext, Path, Category, P-Size, L-Size, MBS, SHA1, SHA256, Created, Accessed, and Modified. The table contains 20 entries, including various .PNG files and a .py file.
- Evidence Items:** A tree view showing the file system structure. The root is 'Case1-FLASH.E01', which contains 'Partition 1'. 'Partition 1' contains 'STUFF [ntfs]', which contains 'root'. 'root' contains 'Unpartitioned Space [basic disk]' and 'Unallocated space [unallocated space]'. The 'Unpartitioned Space [basic disk]' contains 'Unallocated space [unallocated space]'.
- File Content:** A panel on the right showing the content of the selected file, 'root\Unpartitioned Space [basic disk]\Unallocated space [unallocated space]'. It displays a hex dump and a corresponding image of a smartphone.

For the rest of my research I analysed other documents by looking at the information FTK gave me without really finding important information allowing a thorough analysis, including

Clement DURYE
2325578

Coursework Computer Forensics

a document in . dat that I tried to modify and open in txt format, but nothing allowed me to know if all the other documents had information that would allow me to go further.

REFERENCES:

- [1] → <https://www.quora.com/What-is-the-difference-between-computer-forensics-and-digital-forensics>
- [2] → <https://online.champlain.edu/blog/evolution-digital-forensics#:~:text=Emergence%20in%20the%201980s%20and,related%20crimes%20started%20to%20occur.>
- [3] → <https://www.nu.edu/blog/what-is-computer-forensics/#:~:text=It%20uses%20specialized%20tools%20and,%2C%20theft%2C%20and%20cyber%20attacks.>
- [4] → https://en.wikipedia.org/wiki/Computer_forensics
- [5] → <https://online.champlain.edu/blog/evolution-digital-forensics>
- [6] → <https://oxygenforensics.com/en/resources/what-is-digital-forensics/#:~:text=Mid%202000s%20%E2%80%93%20Mobile%20Devices%20and,USB%20drives%2C%20and%20memory%20cards.>
- [7] → <https://eclipseforensics.com/3-famous-cases-solved-through-digital-forensics/>
- [8] → <https://cyberw1ng.medium.com/ftk-imager-a-comprehensive-guide-to-forensic-imaging-and-analysis-2023-4eca04272614>
- [9] → <https://en.wikipedia.org/wiki/Phishing>
- [10] → <https://docs.fileformat.com/programming/cpp/#:~:text=Files%20with%20CPP%20file%20extension,files%20as%20application%20source%20code.>