

Institut supérieur d'électronique de Paris



**Prifysgol Cymru**  
Y Drindod Dewi Sant  
**University of Wales**  
Trinity Saint David

## Summary

|                                                                             |           |
|-----------------------------------------------------------------------------|-----------|
| <b>Chapter I.....</b>                                                       | <b>3</b>  |
| <b>1 Digital forensics and Computer forensics.....</b>                      | <b>3</b>  |
| <b>1.1 Definition, historical evolution,.....</b>                           | <b>3</b>  |
| <b>1.1.1 Definition and historical evolution of digital forensics.....</b>  | <b>3</b>  |
| <b>1.1.2 Definition and historical evolution of computer forensics.....</b> | <b>4</b>  |
| <b>1.2 Real-World case studies.....</b>                                     | <b>4</b>  |
| <b>Task 3:.....</b>                                                         | <b>5</b>  |
| <b>2 Forensics Report.....</b>                                              | <b>5</b>  |
| <b>2.1 Chain of Custody.....</b>                                            | <b>5</b>  |
| <b>2.2 Collection simulation.....</b>                                       | <b>6</b>  |
| <b>2.3 FTK Imager.....</b>                                                  | <b>7</b>  |
| <b>2.4 Autopsy.....</b>                                                     | <b>8</b>  |
| <b>2.5 Image Investigation.....</b>                                         | <b>9</b>  |
| <b>2.6 Police report extraction.....</b>                                    | <b>14</b> |
| <b>Conclusion:.....</b>                                                     | <b>20</b> |
| <b>Référence:.....</b>                                                      | <b>21</b> |

# **Chapter I**

## **1 Digital forensics and Computer forensics**

### **1.1 Definition, historical evolution,**

#### **1.1.1 Definition and historical evolution of digital forensics.**

Digital forensics is the practice of identifying, recovering, analyzing electronic evidence, it covers the investigation of all the devices that can contain digital data.

The data sources can be investigated from various sources such as computers, smartphones, flash drives, in short all the computerized systems.

The goal of digital forensics is in majority to extract data and collect them for court purposes. The find information from digital forensics can be crucial in the result of a prosecution. It can also be used to eliminate potential threats by analyzing suspicious data flows, or create counter measures by analyzing previous cyberattacks and finding solutions to counter them.

The first cyber crime was in 1978 and was treated using existing laws. The emergence of specialized law enforcement units in the 1980s-1990s tackled growing computer crime, though standardization lagged. Efforts in the 2000s addressed skills gaps, enhanced international cooperation, and expanded forensic tools for mobile and internet crimes.

### **1.1.2 Definition and historical evolution of computer forensics.**

Computer Forensics is a branch of digital forensics and it takes the same principles, identifying, recovering, analyzing but it's only applied to computers and storage evidence. This branch also applied additional practice like the chain of custody. The chain of custody, in legal contexts, is the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence. So the purpose of computer forensics is to gather digital evidence in an admissible way as evidence during a trial

The importance of computer forensics started to take place when the first personal computer appeared in the 1980's and the first crime began. But with the development of the internet, all networks could be connected, the cyberattack became much more complex, and cybercrime increased exponentially. So computer forensics became essential and practically in every prosecution because nowadays digital is everywhere, in our pocket, in our car, in our kitchen. It can not only be used in digital crime but also in physical crime with security cameras for example.

## **1.2 Real-World case studies**

With the expansion of digital in this era, the numbers of crime cases expanded and the work for the computer forensics services too, so here are some real case studies.

In 2018, a Chinese engineer named Xiaolang Zhang who was working for Apple, resigned from his functions to take care of his mother and work for car manufacturers near his mother. His choice raised the attention of Apple, and the Apple security divisions inspected his activity on the network, and a day before his resignation, he downloaded Apple secrets from one of the databases. He has been arrested by the FBI in the same year

In 2016, Larry Thomas was convicted of murder on Rito-Llamas Juarez by finding numerous anonymous posts with a fake name, one of the posts showed a bracelet that was found on the crime scene.

In 2001, Enron, an ancient American energy company, was convicted of multiple fraud after the examination of terabytes of complex data by computer forensic analysts.

## **Task 3:**

# **2 Forensics Report**

## **2.1 Chain of Custody**

One of the very important points to respect in digital forensics is the chain of custody. The chain of custody is the process to document every step taken on evidence to ensure its authenticity in a court of law. What I mean by authenticity is that the evidence shown the day of the trial is the same found on the crime scene, the exact same, so without any change from the start to the end. Without the chain of custody document, the evidence is irrelevant in a court of law. So maintaining a chain of custody with the maximum detail is crucial for it to have the most credibility. In this type of document you need to find at the minimum: [1]

- An unique identifier for the evidence
- Date and Time and location of collection
- Name and Signature of the evidence collector
- Name, quantity of the recipient
- Laboratory's address

- Type of analyze required
- Date and method delivery
- Authorization for the analysis of the evidence
- Signature with date of everyone involved with the evidence

But they are the requirements but like I said before, the more detailed the better it is, such chain of custody documents like this could be refused to use with such low precisions. You can add the purpose of every action taken, security taken to protect this evidence, and also the most important of all the conclusions after analysis.

## 2.2 Collection simulation

In class, we made a simulation of an evidence recovery (11/03), and we were given different roles that I will introduce to you. First, the crime scene needs to be secured by restricting the area. I put them in the order of the investigation process. I present it simply but each role may have an impact at different times of the investigation.

**Manager:** Oversees the entire investigation process, setting goals, allocating resources, and ensuring that all activities are conducted in accordance with established protocols and standards.

**Incident Analyst:** Analyzes the nature, scope, and impact of the incident to determine the appropriate course of action. They gather information from various sources to understand the incident's context and severity.

**Incident Responder:** Takes immediate action to contain and mitigate the effects of the incident. They implement security measures, gather evidence, and coordinate with relevant stakeholders to minimize further damage.

**Investigator:** Conducts the initial examination of the crime scene or digital devices to identify potential evidence. They coordinate the collection process, oversee team members, and gather preliminary information about the incident.

**Witness:** Provides information about the incident or evidence based on their observations or involvement. Their testimony may be critical for understanding the context of the incident or verifying the authenticity of the evidence.

**Photographer:** Documents the crime scene or evidence using photography or video recording. Their visual documentation provides a record for later analysis and presentation in court.

**Documenter:** Records detailed information about the collection process, including the location of evidence, chain of custody, and any relevant observations. Accurate documentation ensures the integrity and admissibility of the evidence.

**Examiner:** Conducts in-depth analysis of the collected evidence using specialized tools and techniques. They extract data, recover deleted files, and reconstruct digital artifacts to uncover relevant information about the incident.

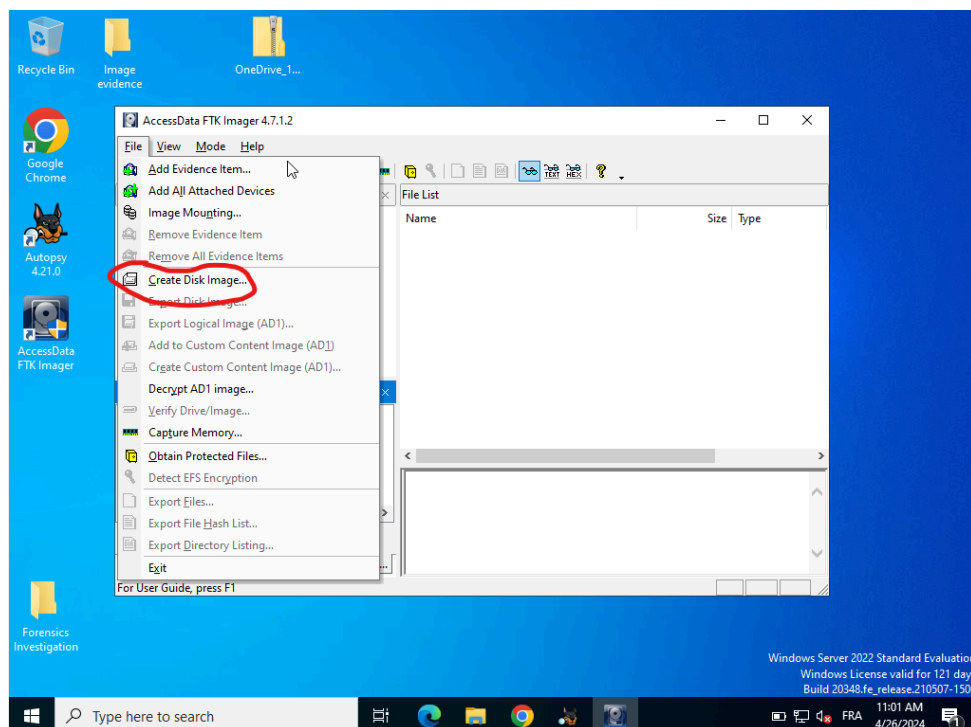
## 2.3 FTK Imager

After the collection, we found as evidence an USB Flash Drive and an external hard drive. For a sake of difficulty, we were given to analyze only a sample on what was on this evidence.

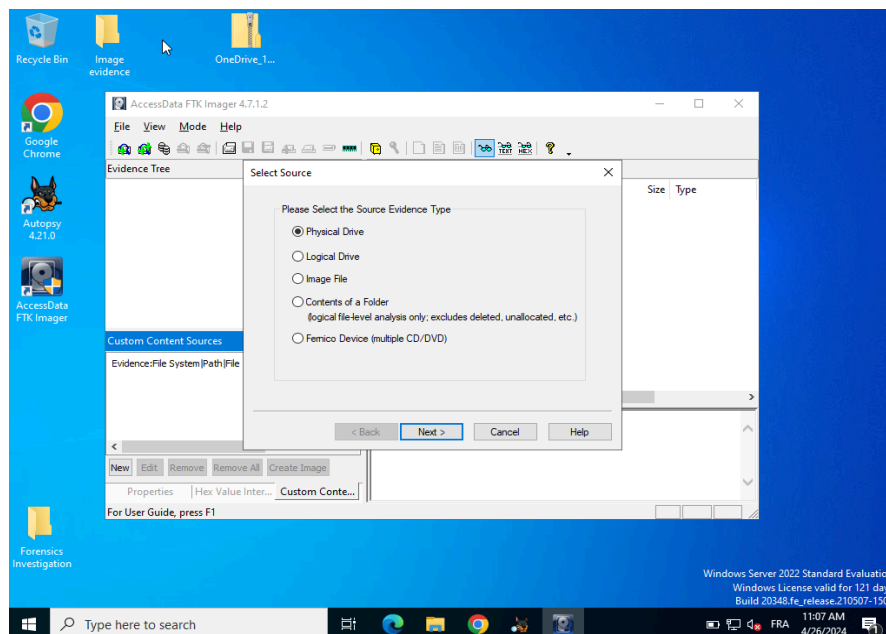
I choose to make my analysis on a virtual machine with an hypervisor type 2 named “Oracle VM VirtualBox” for safety purposes because the machine is isolated and the risk of damaging my main machine is reduced.

The sample of evidences, I took it from Jonh’s message on the forum but he already extract it from the USB Flash Drive, he create an image of the evidence file, so I’m gonna show you how you create a Forensic image :

[9]One of the potential tools usable for this task is FTK Imager. When launching the software, the first thing to do is to create a disk image.



You choose the physical drive



After you just need to choose the file that you want to “duplicate”, the type of format, here we choose EO1(EnCase Evidence File) because it’s a format file commonly used in forensics. Last, you choose the path where you are gonna put your folder and you can add Evidence Item Information.

## 2.4 Autopsy

So for the examination, I decided to use Autopsy.

[2]Autopsy is one of most well-known forensics tools that we have been introduced to in class, it’s an open-source tool that allows us to do timeline analysis, hash filtering, and key word search. It can also allow web artifact extraction, deleted files recovery and permit central repository creation. The first part could be categorized in the disk analysis and the second could be in memory forensics.

[3]These features are all useful in the domain of forensics, timeline analysis for example. Timeline analysis is creating a timeline of activities or events that occurred on a computer system through different data. It's extremely powerful and can have a big impact in a law court to convict or to exonerate someone. With this tools, you can detect what time of the day the connection to a device was done or even a pattern in the connection, these int may allow for example to know if we saw a suspect through a CCTV at Mcdonalds with his friends at 12:05 without device and the attacks has be done at the exact same hour. It would practically immediately delete him from the suspect list.

With Autopsy, you can put timestamp on the files, web artifact, and exclusive data from Autopsy such as Exif.

The timeline analysis of Autopsy has two displays, one will show how much data has

occurred in a given time frame and the second offers event details with a unique feature: clustering similar events to prevent data overload. Instead of overwhelming users with numerous timelines from multiple sources, Autopsy condenses related events, such as files within a folder or URLs from the same domain, into single events. Users can zoom in for more details or keep them hidden for a streamlined view.

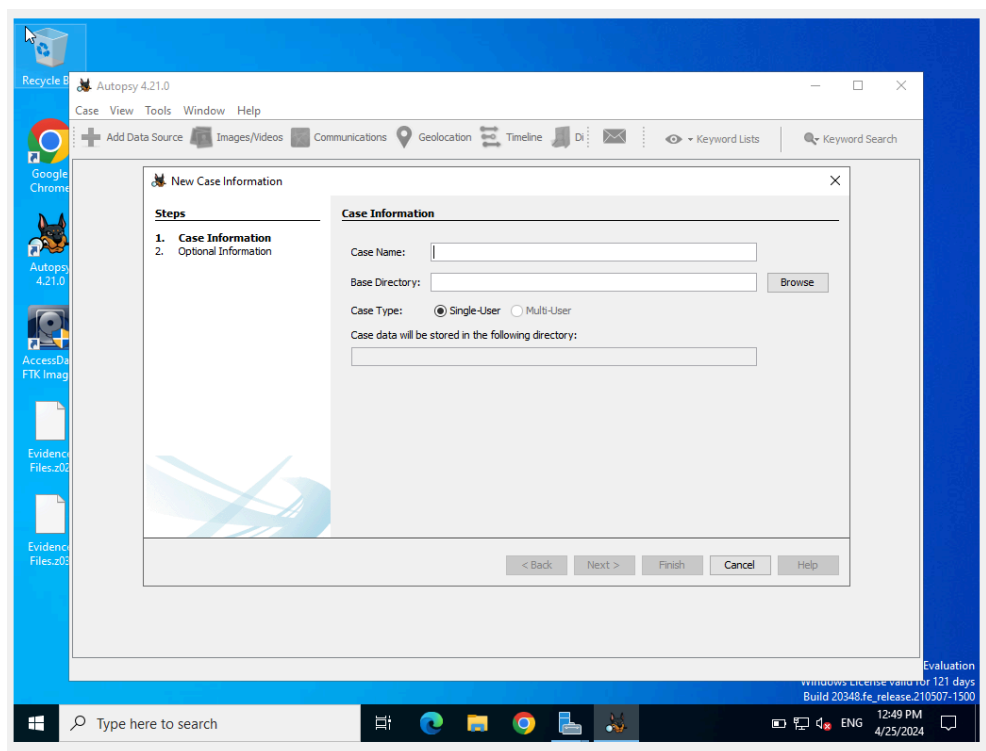
[4][5][6]Hash filtering is also an interesting feature because like the timeline analysis, it reduces the scope of possibilities, so it's a time-saving method. But before talking about hash filtering, we need to introduce the hash, the hash is a method that calculates a 32 to 64 hexadecimal string, also known as hash value, which is associated with files, or groups of files. If the file is altered, when the hash value is recalculated, the result will not be the same, an assigned hash value to a file is like an unique number per file. There are possible collisions but the percentage that this happens is negligible. So the hash filtering method would be that we compared the hash value of the files we investigated and compared it with a previously calculated list of good files and filtered them out if they matched. On the other hand, we could do the same with malicious files to detect them, if they are already registered in a database. There is a need for huge databases of hash sets to execute hash filtering, one of them would be <http://www.nsrl.nist.gov/>. The advantage of hash filtering is that comparing hash values is much faster than comparing files with each other, you conserve the integrity of the files, and the scopes of investigations are reduced or even better you could directly find the threat.

[7]An interesting feature of Autopsy is central repository creation. This feature creates a location where all the data will be gathered, like a database (in autopsy, it will be SQLite or PostgreSQL).

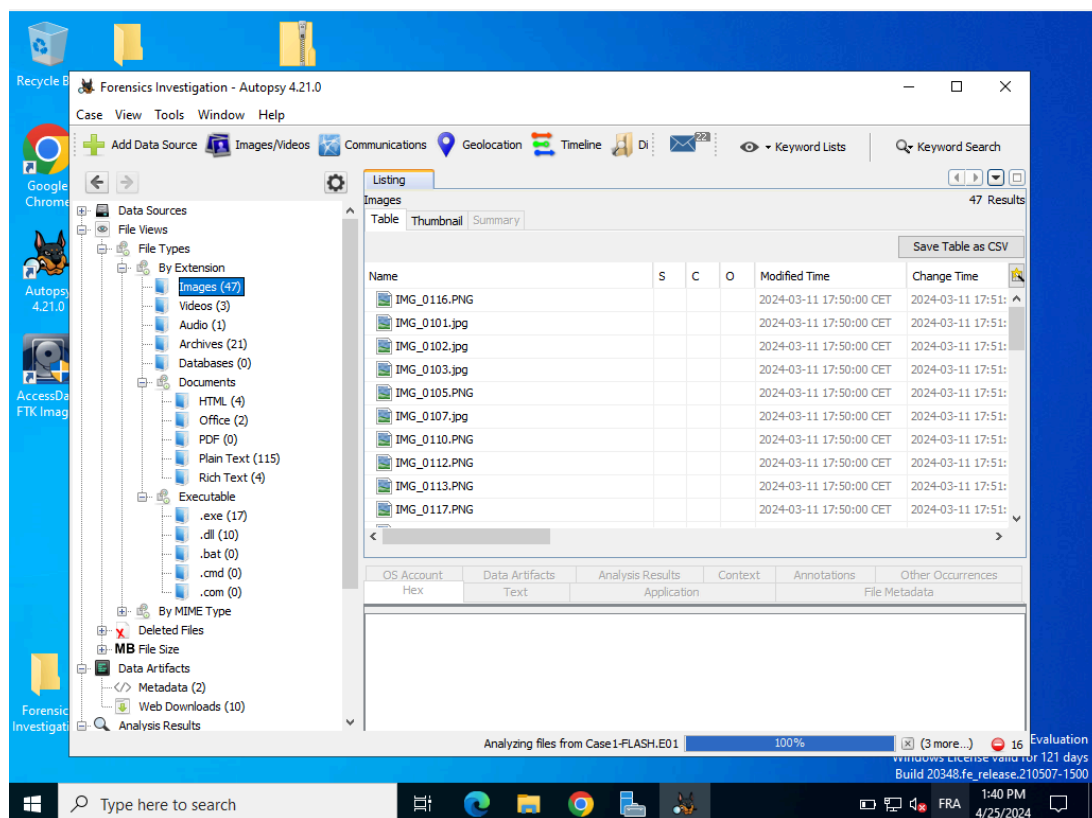
[8]Another time-saving tool, keywords search, as indicated by his name you search a word or a combination of words in a digital evidence.

## 2.5 Image Investigation

In Autopsy, we open a case with evidence files and can add optional information like a unique number and our personal information like our name, mail, phone number.



The first folder I decide to investigate is the folder image where there is 48 images:

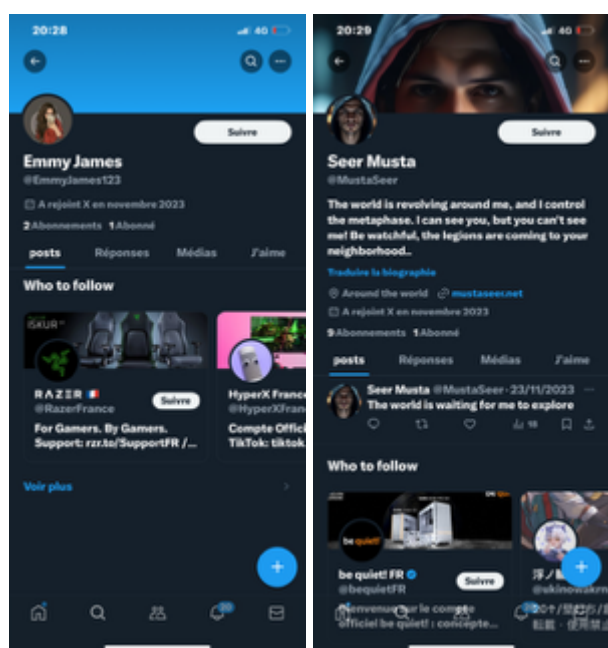


I will note all the observations that I have done from the images folder:

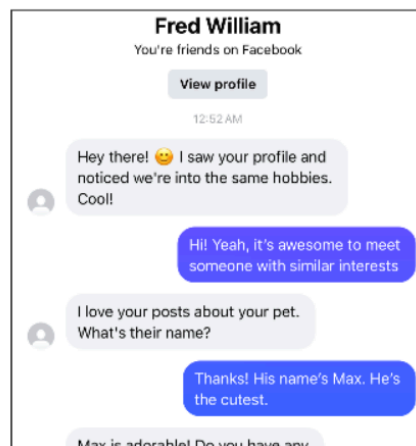
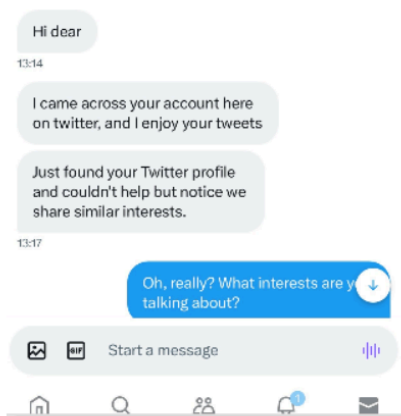
Fred Williams initiated contact with the victim (IMG\_0110) under the guise of shared interests, establishing rapport by discussing mutual hobbies and the victim's pet. During their conversation, he solicited personal information, including the victim's date of birth (5th May 2005) and her preferred recreational spot, which she disclosed to be a park. Furthermore, the victim divulged details regarding her educational institution, identifying it as "Good Shepherd English Medium School". Across various online platforms, the victim identified herself as Emmy James (IMG\_0112) and provided contact details such as her email address (thaniyausha@gmail.com), phone number (0789674590), and Twitter handle (emmyjames123).

An important detail surfaced during the investigation: the victim has a brother, a fact potentially exploited by perpetrators for further manipulation.

Seer Musta, another persona, made contact with the victim on Twitter (IMG\_0101, IMG\_0102, IMG\_0103). Notably, the victim engaged in an interaction on a purported fashion website, requiring registration with personal details, indicating potential vulnerability to identity theft or further exploitation. When searching the account of Emmy James, we found her account on her follower. We see Seer Musta who has a rather threatening description and also a Website but the domain is not attributed.



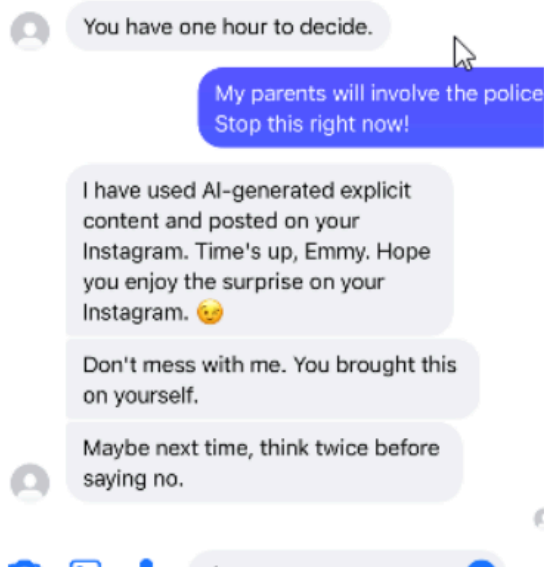
Upon thorough examination of the interactions between the victim and the personas of Fred Williams and Seer Musta, a notable inconsistency emerged. Despite Fred Williams ostensibly introducing the Seer Musta account to the victim via Messenger, both personas initially interacted with the victim as if they were unfamiliar with her, contradicting their supposed connection.



Subsequently, an individual named Zhen reached out to the victim via WhatsApp (IMG\_0118), employing a similar modus operandi to Fred Williams and Seer Musta. Zhen's approach included suggestive language and inquiries into the victim's relationship status, alongside a demand for her usernames on other platforms, which the victim refused. Additionally, Zhen exhibited concerning behavior by claiming knowledge of the victim's residence, suggesting potential stalking tendencies.

Further investigation revealed Lee Saint (IMG\_0107) and Justine Elias persistently soliciting the victim for outings, employing coercive tactics such as threatening to compromise her social media accounts and posting explicit content in retaliation for her refusal. Justin Elias emerged as a really persistent individual contacting the victim across multiple social media platforms, despite her repeated refusals and explicit discomfort.

Lee Saint [IMG\_0109]:



Justin Elias[IMG\_0117]:



The "call center log" document provided insight into troubling interactions, indicating repeated calls to a telecommunications company resembling cyberbullying. Notably, a specific phone number (0723245256) is associated with Alfred Adams, potentially a key figure in the investigation.

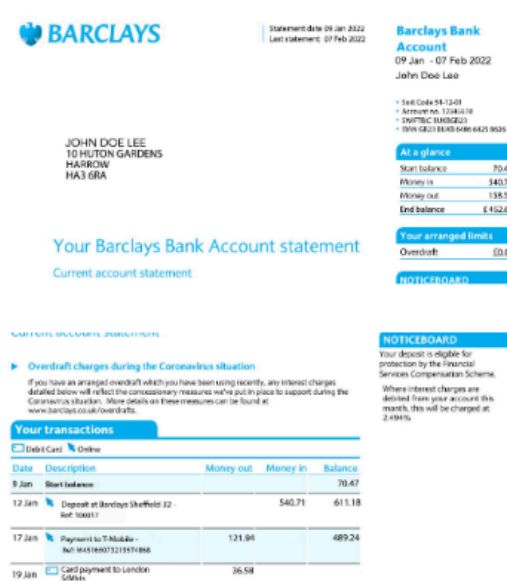
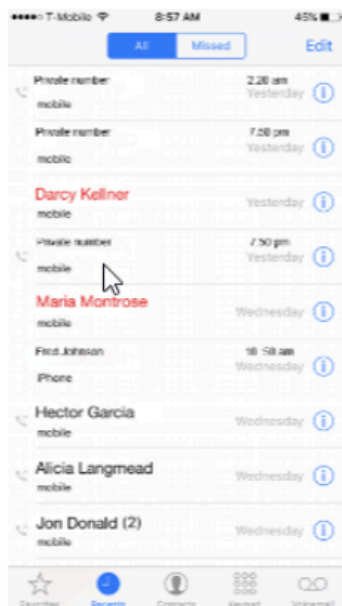
## NKT Mobile Communication Network

Street Name, City, Country



| Call#                                       | Date       | Time                                                                                                                                                                         | Contact Person | Company   |
|---------------------------------------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-----------|
| 1                                           | 25/11/2023 | 10:00                                                                                                                                                                        | Lottie Piers   | SunEnergy |
| Call Type                                   |            | Call Notes:                                                                                                                                                                  |                |           |
| <input checked="" type="checkbox"/> Inbound |            | User Name: Alfred Adam<br><br>User called a particular number repeatedly, using this number at different times.<br>Details of the conversation sounded like a cyber bullying |                |           |
| <input type="checkbox"/> Outbound           |            |                                                                                                                                                                              |                |           |
| Phone Number                                |            |                                                                                                                                                                              |                |           |
| 0723245256                                  |            |                                                                                                                                                                              |                |           |

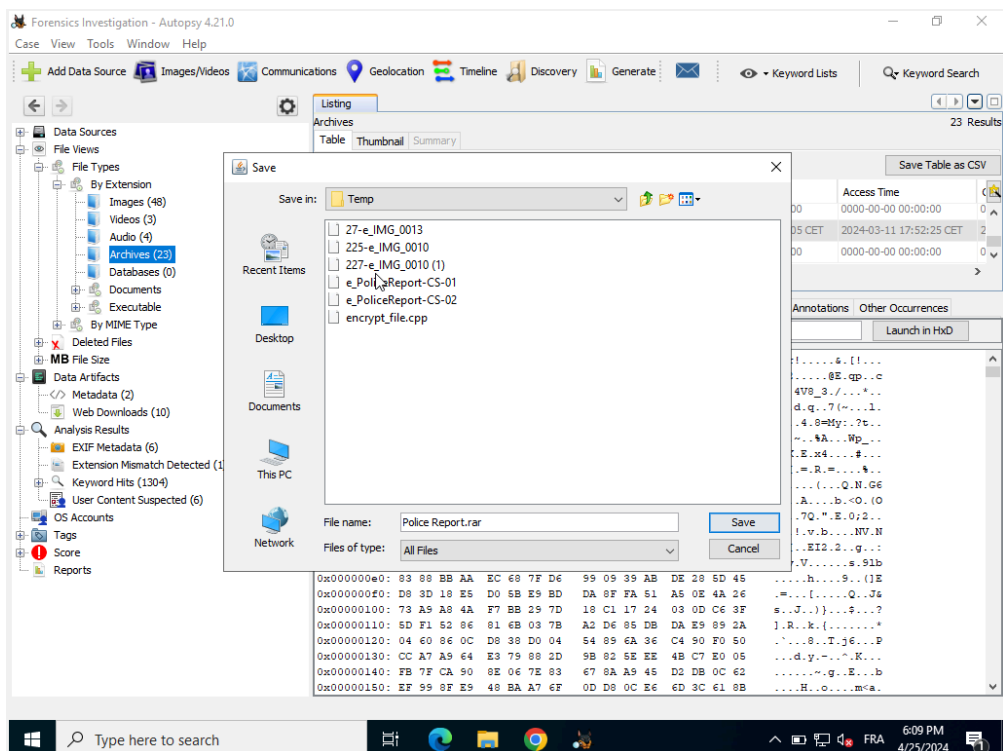
Additionally, the "call logg" document highlighted numerous calls from an unidentified "private number". Moreover, the victim's phone plan correlated with a bill under the name John Doe Lee, revealing a substantial payment of €540 at Barclay's Sheffield 32, warranting further scrutiny.



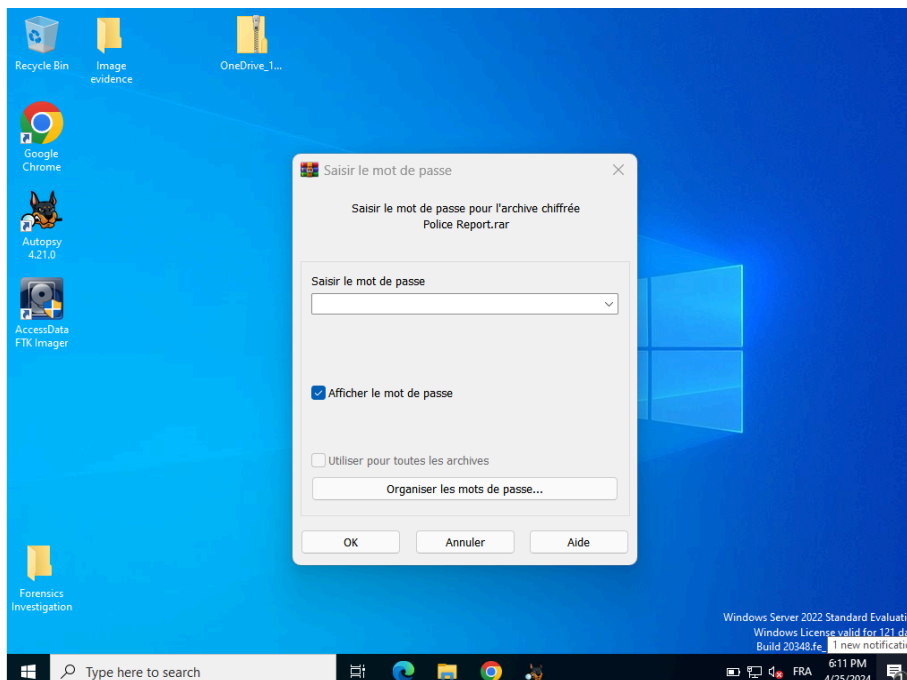
To conclude on the image inspections, the comprehensive examination of the evidence underscores a troubling pattern of predatory behavior targeting the victim across various online platforms. The tactics employed include coercion, manipulation, and potential cyberbullying especially for Justin Elias and Lee Saint. The other people who contacted have also suspicious tendencies like questioning a lot about her private life but I don't think we can call it cyberbullying. BUT there are similarities between them, they all reached out from the same manner but the approach is different, it's like it's the same person who tried different things with a false name to have better results, so we need to find the truth in the false. I think there is more to explore with the telephonic bill for example or the call of "Alfred Adams" but I haven't found further pist

## 2.6 Police report extraction

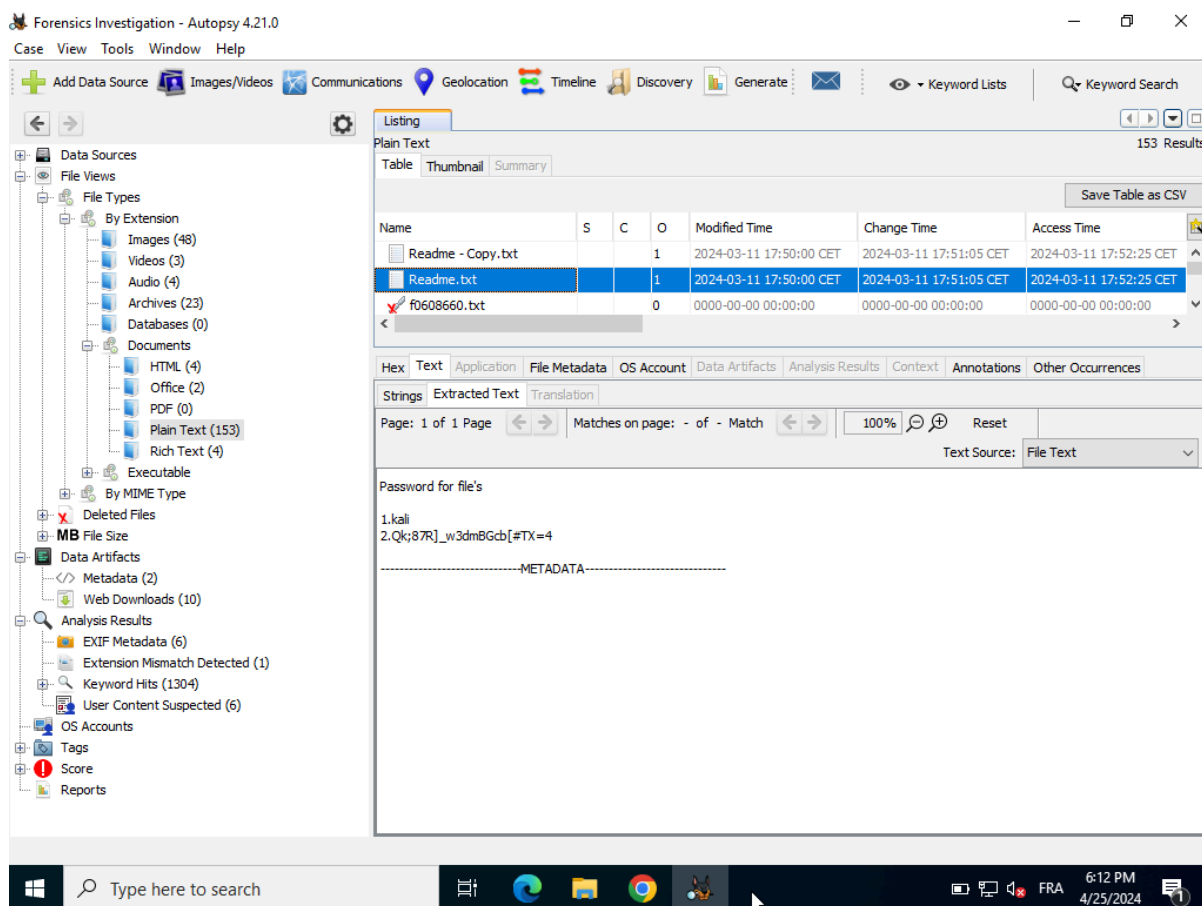
So going through the data , in the file Archives, there is a file named "Police Report.rar"



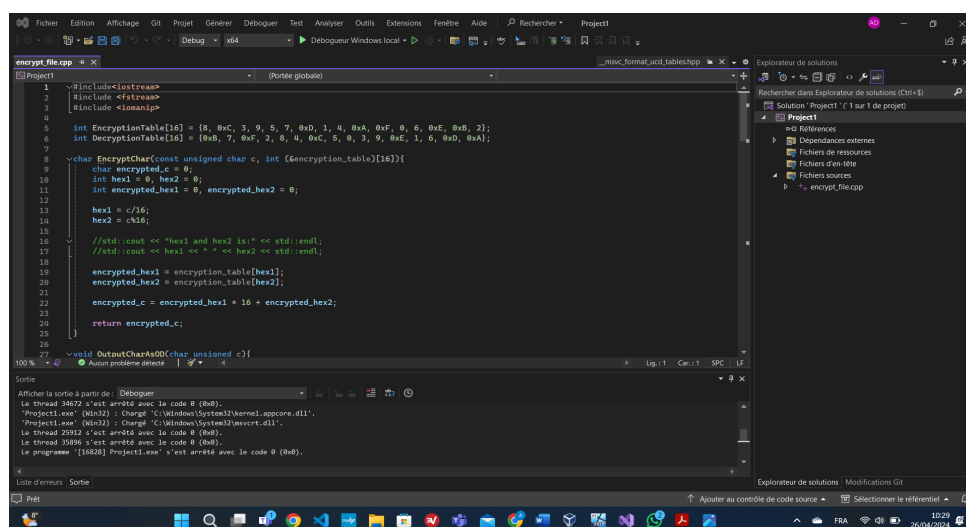
When you want to extract it, you need a password to open it:



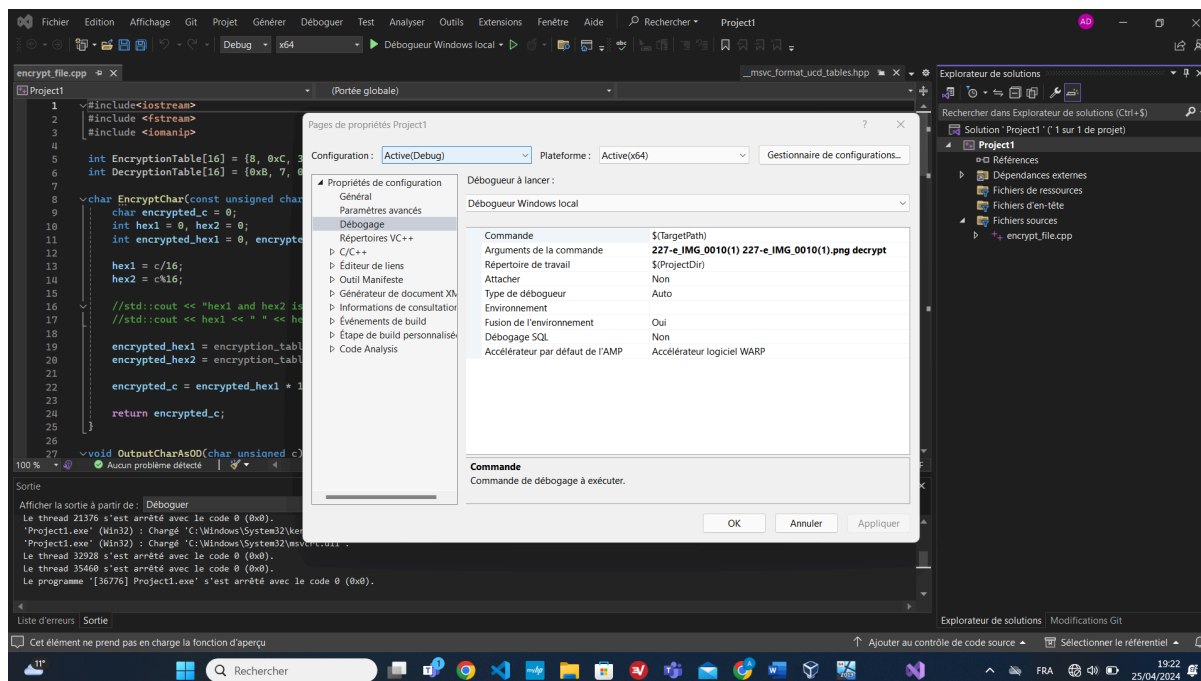
After further investigation, I found it in the file Readme.TXT and there were two passwords, I tested both and the second one works.



The results of our extraction have given us encrypted files that we need to decrypt. In searching again in Autopsy we found a name that gives us an it "encrypt\_file.ccp", when we opened it, we found a code.



The code is already done so we just need to put the input and the output wanted with the file format, here the file format is png and to specify that we want to decrypt the file .



And the result is giving us 5 images, with three that I haven't been able to find something interesting to exploit in it. But two of them were actually extremely interesting.

In the document below, we learn that Lucy Alden born in 1996, filed a complaint (with the case number Cs-032949) against Justine Elias, one of the people who aggressively threaten Emily James, if we recall the message from before, she told him to stop at multiple times but he continued stubbornly, even when she involves her parents. All the suppositions I have made about all the accounts reveal to be true if we believe the police document . There is a link where supposedly all the evidence incriminating Justine Elias is gathered but it doesn't work. As a sentence, he was on a restraining order and paid 2000£ in fines.



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

info@edrpolic.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.

Tous les favoris

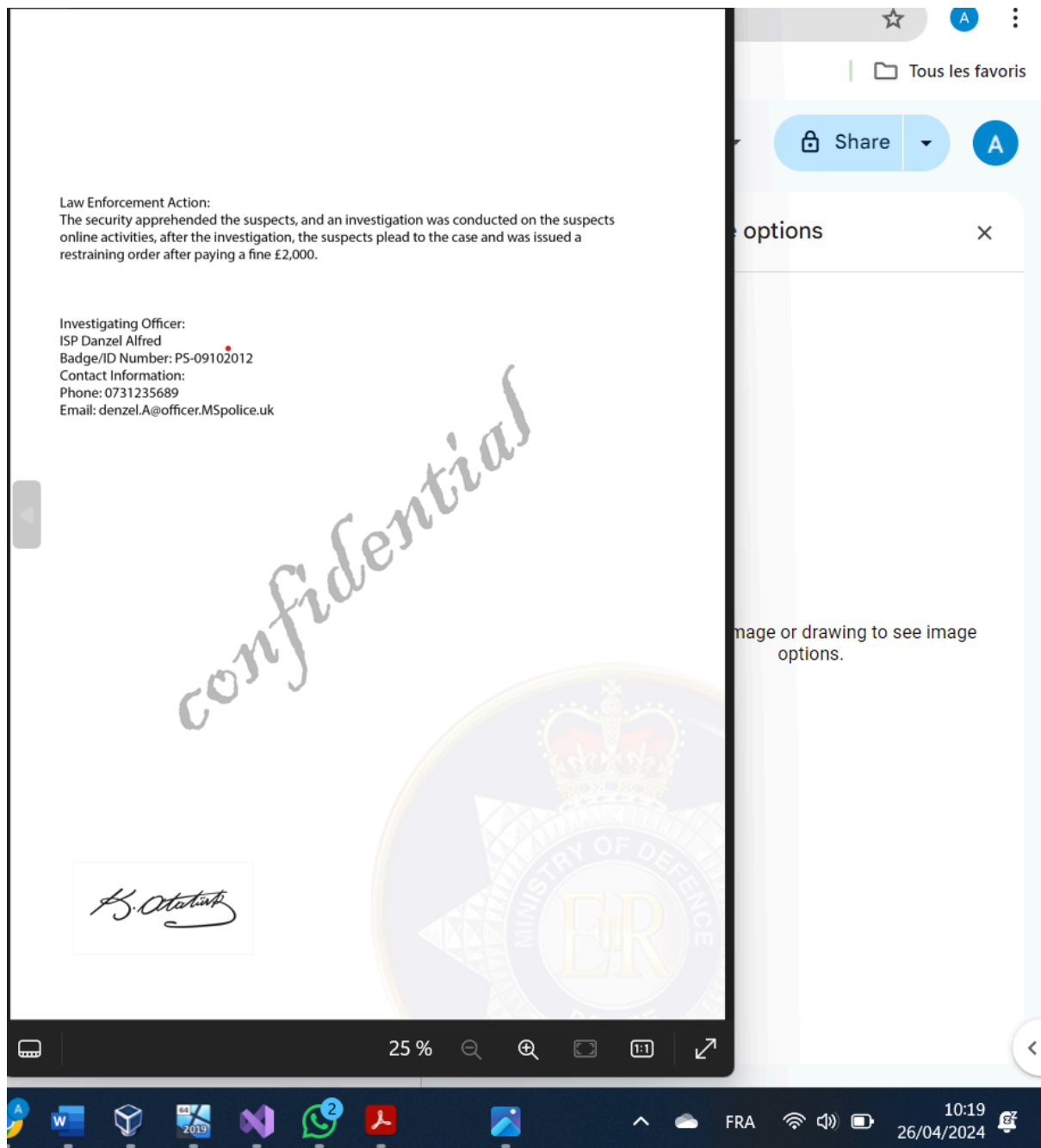
Share

A

options

X

image or drawing to see image options.



But by checking the date of complaint something bothers me, the victim's Twitter account date of creation is in 2023, and the complaint was filed in 2021. And he gave him an alias for the cybercrime as [Egos\_dark] but I've never seen it during all the investigation unless it is an Instagram account name which I haven't found. So it's possible that it's a fake but I don't know the reason why it would be fake.

## **Conclusion:**

To conclude, Emily James is a victim of cyberbullying, it's already pretty clear when you check the message she received and the police report confirms the suspicion.

# Référence:

## Task 1

<https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/what-is-digital-forensics/>

[https://en.wikipedia.org/wiki/Digital\\_forensics](https://en.wikipedia.org/wiki/Digital_forensics)

<https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics#:~:text=Digital%20forensics%20is%20a%20branch,crucial%20for%20law%20enforcement%20investigations.>

<https://www.ibm.com/topics/computer-forensics>

[https://en.wikipedia.org/wiki/Computer\\_forensics](https://en.wikipedia.org/wiki/Computer_forensics)

<https://www.techtarget.com/searchsecurity/definition/computer-forensics>

<https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools>

[https://www.researchgate.net/publication/335766409\\_Digital\\_Forensics\\_-\\_A\\_Literature\\_Review](https://www.researchgate.net/publication/335766409_Digital_Forensics_-_A_Literature_Review)

<https://academic.oup.com/itnow/article-abstract/64/2/46/6585375?redirectedFrom=fulltext>

Marcus K. Rogers, in Digital Forensics, 2016

## TASK 3

[1]-<https://www.ncbi.nlm.nih.gov/books/NBK551677/#:~:text=The%20chain%20of%20custody%20is%20said%20to%20be%20the%20sequential,of%20physical%20or%20electronic%20evidence.>

[2][https://en.wikipedia.org/wiki/Autopsy\\_\(software\)](https://en.wikipedia.org/wiki/Autopsy_(software))

[3]<https://www.sciencedirect.com/topics/computer-science/timeline-analysis#:~:text=Timeline%20analysis%20allows%20viewing%20and,dates%20or%20specific%20event%20types.>

<https://www.sleuthkit.org/autopsy/timeline.php>

[4]<https://www.sans.org/blog/extracting-known-bad-hash-set-from-nsrl/>

[5]<https://www.stellarinfo.com/blog/hash-values-in-digital-forensics/>

[6]<https://www.computerforensics.com/news/what-is-a-hash-value>

[7][https://sleuthkit.org/autopsy/docs/user-docs/4.15.0/central\\_repo\\_page.html](https://sleuthkit.org/autopsy/docs/user-docs/4.15.0/central_repo_page.html)

[8][https://sleuthkit.org/autopsy/docs/user-docs/3.1/keyword\\_search.html#:~:text=The%20keyword%20search%20ingest%20module,from%20the%20files%20being%20indexed.](https://sleuthkit.org/autopsy/docs/user-docs/3.1/keyword_search.html#:~:text=The%20keyword%20search%20ingest%20module,from%20the%20files%20being%20indexed.)

<https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools>

[9]<https://medium.com/@tojopthomas/ftk-imager-5df0c870074#:~:text=on%20each%20feature.,Creating%20A%20Forensics%20Image,on%20the%20drive%20you%20have.>