Middlesex University Mauritius

Digital Incident Scene Investigation & Analysis

Coursework 2

Name: Haider, Diren, Aloyce and Byron

Lecturer: Sir Karel

Submission: 7th April 2024

CST2580

Table of Contents

Table of Figures

1.0 Executive Summary

The investigation into M57.biz, a startup specializing in a comprehensive catalog for body art enthusiasts, revealed a critical data breach involving the leak of a sensitive spreadsheet from Jean's computer. The breach, facilitated through an 'outlook.pst' file analyzed via GoldFynch.com, exposed employee information due to a series of vulnerabilities and errors. Key findings indicated a lack of security awareness among employees, particularly in email communications, and the exploitation of this by an attacker through email spoofing. The attacker impersonated Alison, the President, capitalizing on a misconfigured email address to deceive Jean into sending the sensitive spreadsheet to a fraudulent email address. This incident highlighted the absence of basic email security practices within M57.biz, such as SPF, DKIM, and DMARC, which left the company vulnerable to spoofing attacks. The conclusion underscores the importance of cybersecurity vigilance, education on digital security best practices, and the implementation of comprehensive security measures to prevent similar incidents. The case of M57.biz serves as a stark reminder of the complex nature of cybersecurity threats and the critical role of human factors in safeguarding digital assets against potential financial and reputational damage.

1.1 Case Background

M57.biz is an innovative web startup specializing in developing a comprehensive catalog for body art enthusiasts. The company has gained attention and financial support, securing $3 million in initial funding and currently finalizing a $10 million funding round. Founded by two individuals, M57.biz has quickly grown, employing ten staff members within its first year. The current team includes Alison Smith as President, overseeing operations, and Jean as Chief Financial Officer (CFO), managing financial aspects. The programming team, consisting of Bob, Carole, David, and Emmy, works remotely from their homes, holding regular online chats and weekly in-person meetings. Gina and Harris manage marketing, while Indy focuses on business development, often working remotely or in temporary spaces like hotels or cafes.

M57.biz operates virtually, with employees scattered across different locations and staff communicating mainly via email and exchanging documents electronically. However, a recent breach has compromised document security, as a confidential spreadsheet essential for funding was found posted on a competitor's website. The spreadsheet originated from Jean's computer, raising concerns about data integrity and investment security.

In interviews, Alison denies involvement, she refutes receiving the spreadsheet via email or requesting it from Jean. On the other hand, Jean acknowledges creating the spreadsheet at Alison's request and sending it as instructed. Alison and Jean have distinct email identities within the company network. Alison's email is alison@m57.biz with the password "ab=8989," while Jean's email is jean@m57.biz with the password "gick*1212."

The task assigned is to investigate the breach and provide answers to critical questions for the concerned investor, who is a significant contributor to M57.biz's initial funding. Access has been given to Jean's computer's hard drive, the compromised spreadsheet, and EnCase forensic software. Key Questions to be answered are when did Jean create this spreadsheet? How did it get from her computer to the competitor's website? Who else from the company is involved?

2.0 Preparation

2.1 - The five stages of Digital forensics

There are five stages involved in the digital forensic investigation which are, Evidence Identification, Evidence acquisition & collection, Evidence examination, Evidence documenting and Evidence presentation. Evidence identification is described as the initial phase of investigation process in the digital forensics' investigation. It is the first step to identify the suspicious items which were used in the cyber security incident (Subrosa, 2023). Secondly, evidence acquisition and collection are one of the most vital parts in the investigation process since it enables the officers in charge to collect all the useful suspicious data or evidence leading to the suspect. Further on, by collecting the useful evidence, the officers would be able to find loopholes which will ultimately lead to the suspect (Subrosa, 2023).

After collecting the evidence, officers inspect the suspicious evidence carefully which can be termed as evidence examination. Evidence examination in digital forensics can be done via examining various files in the computer like emails, pictures, word document, bank account details, etc. The examiner can simply investigate into the recent modifications made before the cyber security incident like deleted files, encrypted files, archived files, emails, etc. Examiners can easily investigate recent changes made before the cyber security incident, such as emails, encrypted data, deleted files, and archived files. This will help with the investigative process because it will reveal the hacker's intentions and allow for the identification of his objective (Subrosa, 2023).Evidence documenting is referred to the proper paper or digital documentation of the investigation, so if you have missed something and want to connect the dots later, you can simply open a file and easily find whatever you are looking for. Evidence documentation will make the investigation process more organised and clearer, as it will help in presenting the evidence to the court of law as well (Norwich University, 2024).

Lastly, Evidence presentation is termed as presenting the final findings related to the investigation in the court of law or those judicial bodies who are in charge to decide the outcome of the case. Accurate documentation of the evidence is essential for the presentation of the evidence since it will assist the investigating officers in describing the occurrences in a court of justice using a timeline and order. Since, even if the suspected body is a criminal, but investigation officers fail to present the evidence in the court of law, the suspect would be free from all the charges. Presentation of the evidence is therefore one of the most important and vital components (Norwich University, 2024).

2.2 - What is Digital forensic preparation?

Digital forensic preparation is meant by preparing for the incident scene. Raids on the incident site may be followed by the gathering of evidence and interviews with residents. However, a Search warrant, Investigation Team roles, Health and Safety protocols, and Transportation are required to prepare for this strategy.

2.2.1- Health & Safety

Health and safety procedures are mandatory to be followed by the investigation team. It is the most vital part of the investigation process to be thoroughly looked for and to not be compromised. The health and safety procedures can be set by examining the risks associated with the incident place, and what type of investigation is required. The basic SOBs to be followed by the digital forensic investigation team can be to wear the gloves, masks, work boots, and a first-aid box (La Trobe, 2017).

The four members of our investigation team—Haider, Aloyce, Byron, and Diren—wore masks, work boots, and gloves. Gloves were essential since they ensured that our fingerprints wouldn't be altered with or mixed up with the suspect's fingerprints on the evidence. Rubber Work boots were necessary in case the site was broken and for the electrical wires, but the mask was essential because the investigating team was unaware of the incident location and whether the suspect had added anything to the room or the AC vent.

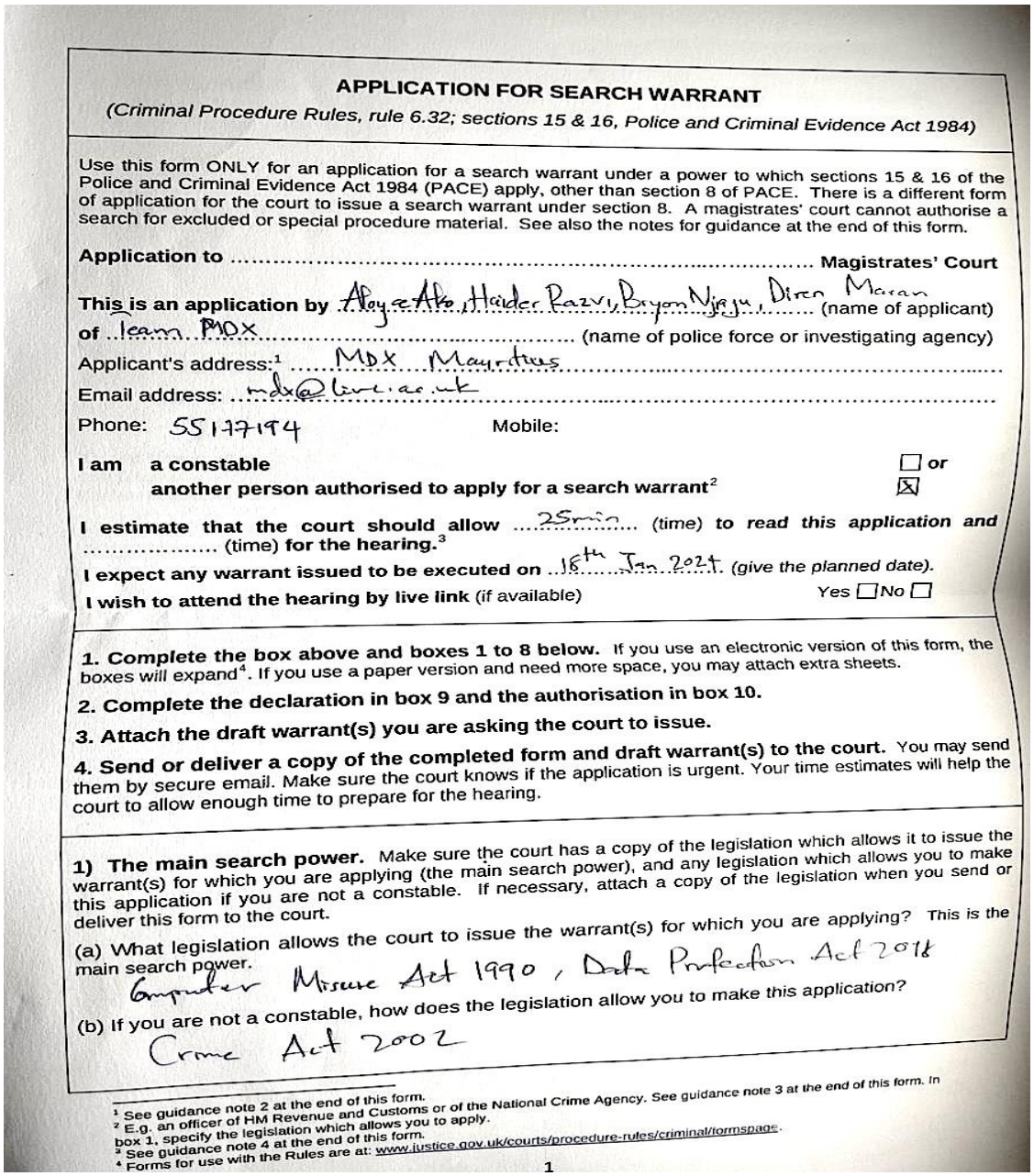
Ensure that all health and safety procedures follow local, national, and international laws and standards.

2.2.2 - Search warrant

Search warrant is defined as an official document signed and authorised by a Magistrate to give the complete authority to the investigation officers to search a specific domain or house. The suspected items can be listed down in another paper which is called as affidavit and is signed by another law enforcement head, like the senior investigation officer. He needs to specify in that document that what things are related to the case and what will be acquired from the site (Shinder and Cross, 2008).

The search warrant gives complete authority and power to seize any suspicious item related to the case including computers, computer hardware or other technology related items.

Our team prepared the search warrant and handed over to Mr. Karel, to search the incident site. See fig.1 for the search warrant.



APPLICATION FOR SEARCH WARRANT

(Criminal Procedure Rules, rule 6.32; sections 15 & 16, Police and Criminal Evidence Act 1984)

Use this form ONLY for an application for a search warrant under a power to which sections 15 & 16 of the Police and Criminal Evidence Act 1984 (PACE) apply, other than section 8 of PACE. There is a different form of application for the court to issue a search warrant under section 8. A magistrates' court cannot authorise a search for excluded or special procedure material. See also the notes for guidance at the end of this form.

Application to ..... **Magistrates' Court**

This is an application by Afoyeza Ako Haider Razvi, Bryon Nigu, Diren Maran (name of applicant)

of Team MDX ..... (name of police force or investigating agency)

Applicant's address:[1] MDX Mauritius

Email address: mdx@live.ac.uk

Phone: 55177194 Mobile:

I am **a constable** ☐ **or**

another person authorised to apply for a search warrant[2] ☒

I estimate that the court should allow 25min (time) **to read this application and** ..... (time) **for the hearing.**[3]

I expect any warrant issued to be executed on 18th Jan 2024. *(give the planned date).*

I wish to attend the hearing by live link (if available) *Yes* ☐ *No* ☐

1. Complete the box above and boxes 1 to 8 below. If you use an electronic version of this form, the boxes will expand[4]. If you use a paper version and need more space, you may attach extra sheets.

2. Complete the declaration in box 9 and the authorisation in box 10.

3. Attach the draft warrant(s) you are asking the court to issue.

4. Send or deliver a copy of the completed form and draft warrant(s) to the court. You may send them by secure email. Make sure the court knows if the application is urgent. Your time estimates will help the court to allow enough time to prepare for the hearing.

1) The main search power. Make sure the court has a copy of the legislation which allows it to issue the warrant(s) for which you are applying (the main search power), and any legislation which allows you to make this application if you are not a constable. If necessary, attach a copy of the legislation when you send or deliver this form to the court.

(a) What legislation allows the court to issue the warrant(s) for which you are applying? This is the main search power.

Computer Misuse Act 1990, Data Protection Act 2018

(b) If you are not a constable, how does the legislation allow you to make this application?

Crime Act 2002

[1] See guidance note 2 at the end of this form.
[2] E.g. an officer of HM Revenue and Customs or of the National Crime Agency. See guidance note 3 at the end of this form. In box 1, specify the legislation which allows you to apply.
[3] See guidance note 4 at the end of this form.
[4] Forms for use with the Rules are at: www.justice.gov.uk/courts/procedure-rules/criminal/formspage.

1

Figure 1: Search warrant

2.2.3 – Investigation team roles

Digital investigation team plays a vital role in the investigation of a sensitive and complexed cyber security incident. The team is responsible for collecting, examining, documenting, and presenting the evidence. For a successful investigation team, the team leader needs to divide the roles between his team members (Financial crime, 2022).

However, our group contained 4 members: Haider, Aloyce, Byron and Diren. Thus, the roles were divided among the team members according to their expertise. Mr. Haider was responsible for conducting the interviews from Jean and Allison, the two suspects. Mr. Diren and Mr. Byron were given the duty to collect the evidence, and examine the site, whereas Mr. Aloyce was responsible for the imaging.

2.2.4 – Planning - Transportation

Transportation is one vital aspect in the digital investigation, whether it's the transport of the investigation officers or the movement of evidence like computer, computer hardware, USB disks, papers, or other suspicious items (National Institute of Justice, 2012).

After using public transportation to get to the meeting place, our team assembled and proceeded to the location. The evidence that was discovered there was transported using plastic bags. Plastic bags reduced the possibility of tampering, helped us preserve the evidence, and helped us document it.

2.2.5 – Standards and Compliance

Digital investigations, encompassing a broad range of activities from computer forensics to network analysis, rely on a set of standards to ensure that the processes are reliable, repeatable, and defensible in a court of law (UNODC, 2012).

i - ISO/IEC 17025

Labs may prove that they function properly and produce accurate results by using ISO/IEC 17025. Encouraging trust in the work they do on international level (ISO, 2017).

The three reasons to imply ISO/IEC 17025 are, Quality management, technical competence, result accuracy (Mayer, 2023).

ii - ISO/IEC 27037:2012

ISO/IEC 27037 outlines the procedures for locating, gathering, acquiring, and storing digital evidence, which is of high value. ISO/IEC 27037 gives guidance to the digital storage of media used in computers like hard drives, floppy disks, etc. and supports other technology related items like smartphones and Networks (ISO, 2018).

iii – ISO/IEC 27041:2015

ISO/IEC 27037 provides advice on how to guarantee the accuracy and dependability of the techniques used to locate, gather, obtain, and store electronic evidence (ISO, 2021).

iv – ISO/IEC 27042:2015

ISO/IEC 27042 gives instructions for evaluating and interpreting digital evidence, which is a crucial step in the investigative process (ISO, 2021).

v - Scientific Working Group on Digital Evidence (SWGDE)

The SWGDE produces essential guidelines and requirements for electronic and multimedia evidence gathering. These documents are highly regarded and recognised in the forensics field (SWGDE, 2024).

3.0 – Identification

Evidence identification can be described as the first step towards the digital forensic investigation process. It is to detect the incident which can be done via detection systems, logs, emails, or notifications from third parties to identify a potential incident. Moreover, Identify and save volatile data (e.g., data in RAM or cache) that could be lost during a power outage or system reboot.

We will highlight on how we took the initial steps for the evidence identification, which includes description of suspects at the scene, securing the incident scene, description of hard-disk, description of the interview, and description of the papers found as evidence.

3.1 – Securing the scene

Securing the scene means to secure the damaged systems to avoid further harm or data losses. This may include physically safeguarding the location or conceptually isolating network portions. Our investigation team proceeded to the location and presented the search warrant to Mr. Karel, the site's incharge.

Our investigation team secured the area by gathering all of the suspects in one location, closing the door, and ensuring that no one could go outside and enter during the inquiry. After gathering all of the suspects in one location, Mr. Haider looked for Jean and Allison to interrogate them one by one. Mr. Diren and Mr. Byron were gathering evidence, while Mr. Aloyce kept an eye on the other two suspects and asked them a few questions. Furthermore, Mr. Haider noticed the computer turned on and the recent activity.

3.1.1 – Photograph of digital scene

Our crew photographed the investigation scene to ensure that no evidence was tampered with or hidden, and that if a suspect fled the scene we could identify and locate them. Photography of the site is critical because it prevents the suspects from rearranging the items on the spot.

3.2 – Description of suspects at the site

There were four suspects at the scene. They attempted to act normal in order to deflect the attention of our investigation officers, but our professional and specialist squad remained focused and gathered all of the suspects in one location.

There were two women and two men. The one guy was Jean, and the other appeared to be in his mid-40s. Whereas one of the girls was Allison, the other one appeared suspicious due to her constant worry.

3.3 – Description of the interview

3.3.1 – Interview analysis with Jean

So, Mr. Haider first interrogated the suspect named as Jean. I asked 14 Questions from Jean. Based on the interview, the questions I asked him, Jean was confused and gave many answers which mismatched to the other questions, he answered. Moreover, Jean's body language was nervous, which sounded suspicious.

It could be due to pressure of being interrogated or it can be the thought of losing his job after this incident, but what I asked him. It looked suspicious. I will go through the questions and answers first, and then provide my full analysis on it.

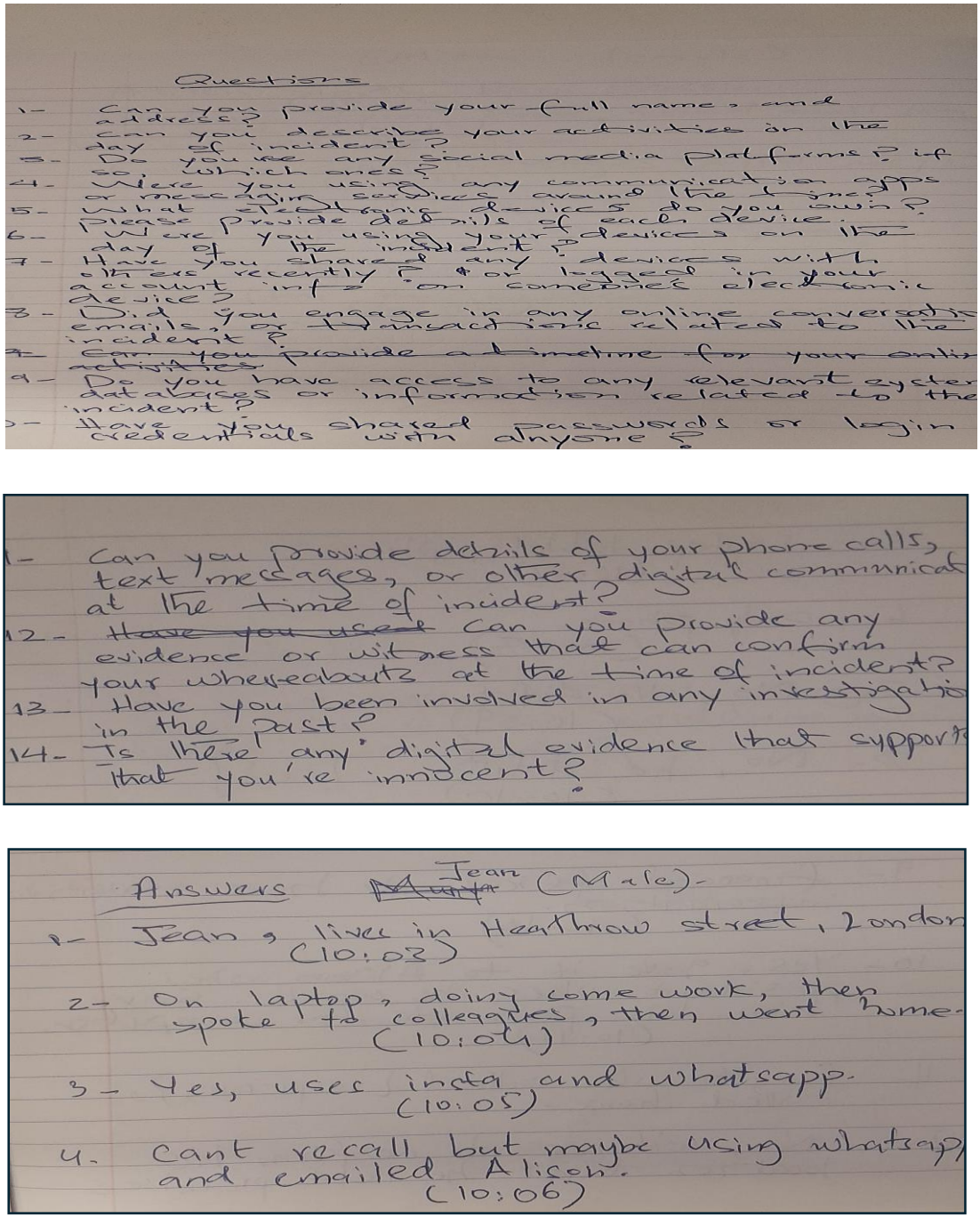


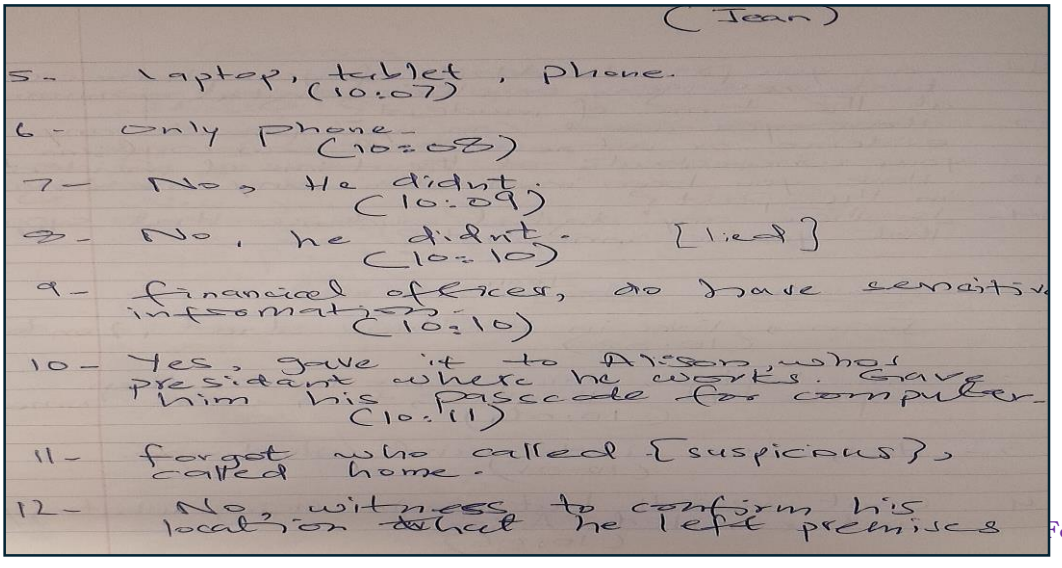
Figure 3: Questions

(10:03 am – 1st Question) So I asked Jean about his name and address in the first question, and he said he resides on Heathrow Street in London, UK. Jean was so panicked and confused that he forgot the interrogation location was in Middlesex, Cascavelle, Mauritius. Suspicion was raised because he failed to answer the most basic question and lied.

(10:04 am – 2nd Question) So, in the second question, I inquired about Jean's activities on the incident day, to which he said that he used his laptop, then did some work, spoke with some colleagues, and then went home. Now I asked Jean which co-workers he spoke with, and he said he doesn't remember.

(10:05 am -3rd Question) Mr. Jean was panicking, so I thought I'd ask him a simple question to help him calm. But the question was a trap for him. It was indirectly asked to determine where he is most active. When asked, he stated that he is active on Instagram and WhatsApp.

(10:06 am- 4th Question) So I checked to see if Mr. Jean was using his social media applications, where he was most active at the time and before to the incident. He became confused again and stated he couldn't recollect, before saying he emailed Allison. This created further suspicions about him.


(Jean)

5- laptop, tablet, phone. (10:07)

6- only phone. (10:08)

7- No, He didnt. (10:09)

8- No, he didnt. [lied] (10:10)

9- financial officer, do have sensitive information. (10:10)

10- Yes, gave it to Alison, who is presidant where he works. Gave him his passcode for computer. (10:11)

11- forgot who called [suspicious], called home.

12- No, witness to confirm his location after he left premises

Figure 4: Answers from Jean 5-12

(10:07 am- 5th Question) I asked him about the electronic equipment he owns, and he said he has a laptop, tablet, and smartphone. Just bear in mind that he was using his laptop at the time of the incident and then claimed to have used WhatsApp as well, so it might have been from his smartphone. But if it was used from his smartphone, wouldn't it be more suspicious? Since he was hiding something and conversing on his smartphone rather than his laptop, who was Mr. Jean talking to?

(10:08- 6th Question) Mr. Jean is lying again, as he stated in question 2 that he used his laptop all day and now claims that he used "only" his phone. So it's strange that Mr. Jean's responses contradict one another, especially if he only used his phone that day. Remember, he stated that he is active on WhatsApp; who was he in communication with?

(10:09 am- 7th Question) No, he didn't share his passcode or any device with someone, well that's what he is saying.

(10:10 am- 8th Question) He lied again, as he stated in Question 4 that he emailed Allison. Also, Mr. Jean stated that he was using his smartphone throughout the day, and how is it possible that he is using his smartphone at work while not speaking with anyone? So Mr. Jean is lying again.

(10:10 am- 9th Question) He does have access to the finance office, which contains sensitive information.

(10:11 am- 10th Question) Mr. Jean stated in Question 7 that he did not give anyone his password or laptop, but in this question, he answers that he gave Allison the passcode for his laptop. Mr. Jean's brazen lying has created suspicions.

(10:12 am- 11th Question) Upon asking about who he called and texted that day. Jean uttered with depressing voice and said that he forgot, but then said, home.

(10:12 am- 12th Question) So, no one saw Mr. Jean leave. Isn't this suspicious? Because if no one saw him leave the office that day, Mr Jean was likely the last person to leave the building. But how come even the security officers did not observe Mr. Jean leave the premises? Did he know of another way out that no one knew about, or did he wait for the guards to change shifts or take a loo break? Mr. Jean is a person who has sparked my doubts.

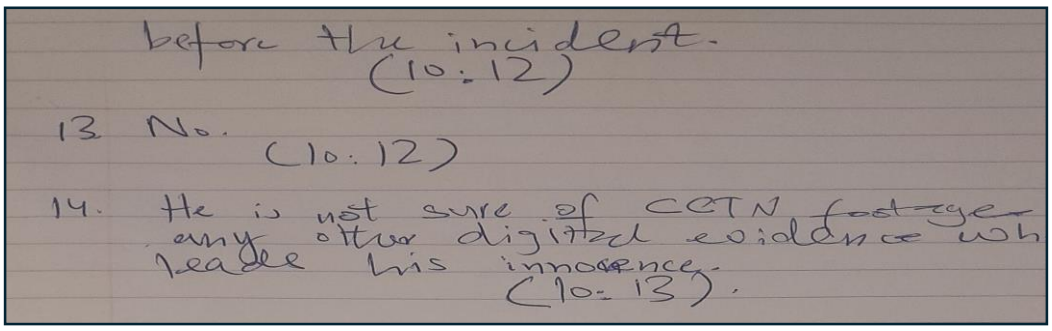


Figure 5: Answers from Jean 13-14

(10:12 am- 13th Question) No, he was not part of any investigation earlier in his life.

(10:13 am- 14th Question) He has no idea whether a CCTV camera caught him as he left the office or not. The question is whether there are security cameras at the entry and exit of the office. If he left the workplace, how could the CCTV camera not have recorded him?

3.3.2 – Interview analysis with Allison

Same Questions were asked from Allison which were asked from Jean.

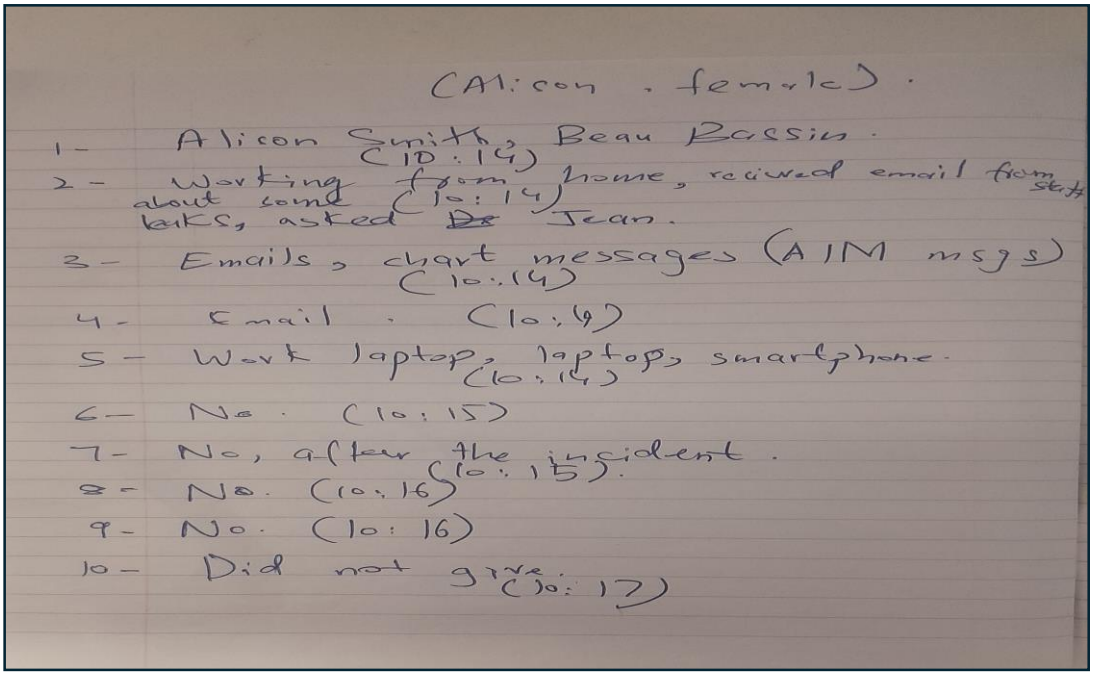


Figure 6: Answers from Allison

(10:14 am- Question 1) Her name is Allison Smith, and she lives in Beau Bassin in Mauritius.

(10:14 am- Question 2) She said, she didn't go to the office that day and worked from home. She received an email from the staff, which possibly can be Mr. Jean and they told her that there are some leaks.

(10:14 am- Question 3) She uses emails and chart messages to communicate.

(10:14 am- Question 4) She used email at the time of incident.

(10:14 am- Question 5) She owns a work laptop, personal laptop, and a smartphone.

(10:15 am- Question 6) She said no, she was not using any device at the time of incident.

(10:15 am- Question 7) She gave her passcode after the incident to the investigation officer.

(10:16 am- Question 8) She doesn't have access to financial information. But how? Isn't she the CEO?

(10:16 am- Question 9) She is not involved in any investigation in the past.

(10:17 am- Question 10) She doesn't have any digital evidence to prove her innocence.

3.3.3 - Combined Analysis on Jean and Allison's interview

Based on the interview, Jean lied frequently and was apprehensive, whereas Allison has a suspicious personality. It appeared that Allison was offering rehearsed responses and had already been fed what to say. Furthermore, Allison responded that she lives in Beau Basin, Mauritius, whilst Jean replied that he lives in London, United Kingdom. Now Jean is lying, but we cannot confirm if Allison is telling the truth or not. Also, Mr. Jean's statements contradicted his own responses. Furthermore, Allison didn't go to the workplace that day and she claimed that she didn't use any smart device like a laptop or a smartphone at the time of the occurrence, but, in Question 4, she said that she used email at the time.

3.4 – Description of Paper evidence found

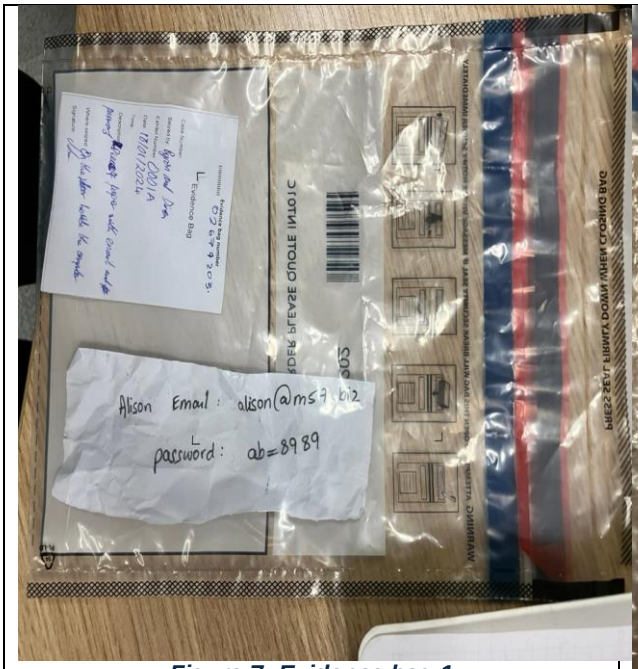


Figure 7: Evidence bag 1

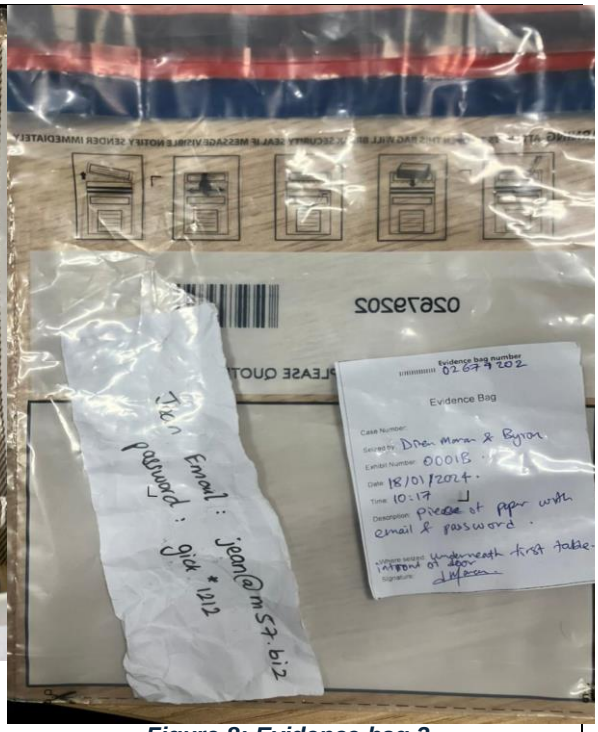


Figure 8: Evidence bag 2

The first image shows a bag labeled with an "Exhibit" number and a description that requests the preservation of paper with an email and password. The note inside lists an email "alison@ms73.biz" and a password. There's also a piece of paper outside the bag with the same information, suggesting it may have been a note meant for inclusion but got separated.

In the second image, the evidence bag has a case number, a date, and a time indicating when the item was seized. The contents include a description of where the evidence was found and a signature of the individual who collected it. The handwritten note inside displays a different email, "jean@ms73.biz," and a password, suggesting that the investigation may involve multiple individuals or accounts associated with the same domain.

4.0 – Acquisition (Acquisition form)

During acquisition of hard-disk image from the computer that was collected during investigation on scene, here is the acquisition form:

Device Type:	**Desktop computer (hard-disk)**
Serial#:	**N/A**
Operating System:	**Windows 7**

Case:	**M57biz**
Agent :	**Aloyce**
Evidence#:	**003**
Chain of Custody:	**Refer to the Appendix A**
Examination Location:	**Middlesex University BG05**
Tool Used:	**FTK Imager 3.2.0.0** **FTK toolkit 8.0.0.305** **Autopsy 4.21.0**
Assessment:	**Chain of Custody Documented**
Acquisition:	**18/01/24 10:00 FTK Forensic Imager used to obtain logical extraction of drive.**

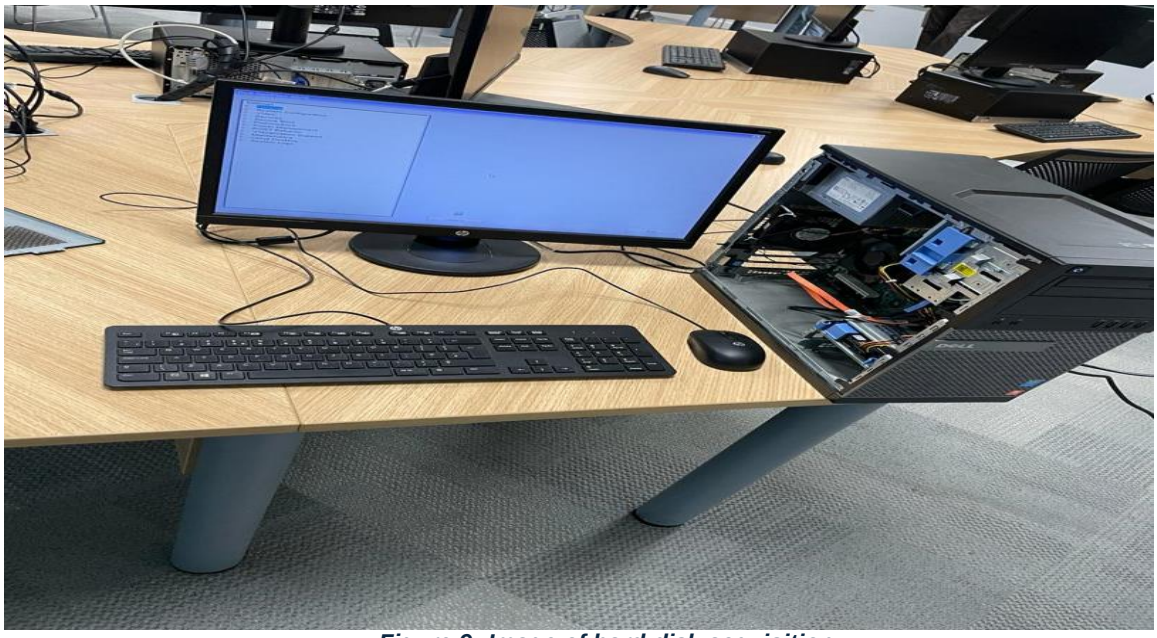


Figure 9: Image of hard-disk acquisition

4.1 Chain of custody

During investigation on scene were able to gather some evidence about the case and we had the custody forms and bags to store any evidence collected. Below is the same of custody form

Case Name	
Case Number	

Evidence Bag Number	
Date	
Time of Seizure	
Seizure Location	
Seized From	
Seized By	
Item Description	
Signature	

Please refer to the appendix to see more the evidence collected during the investigation.

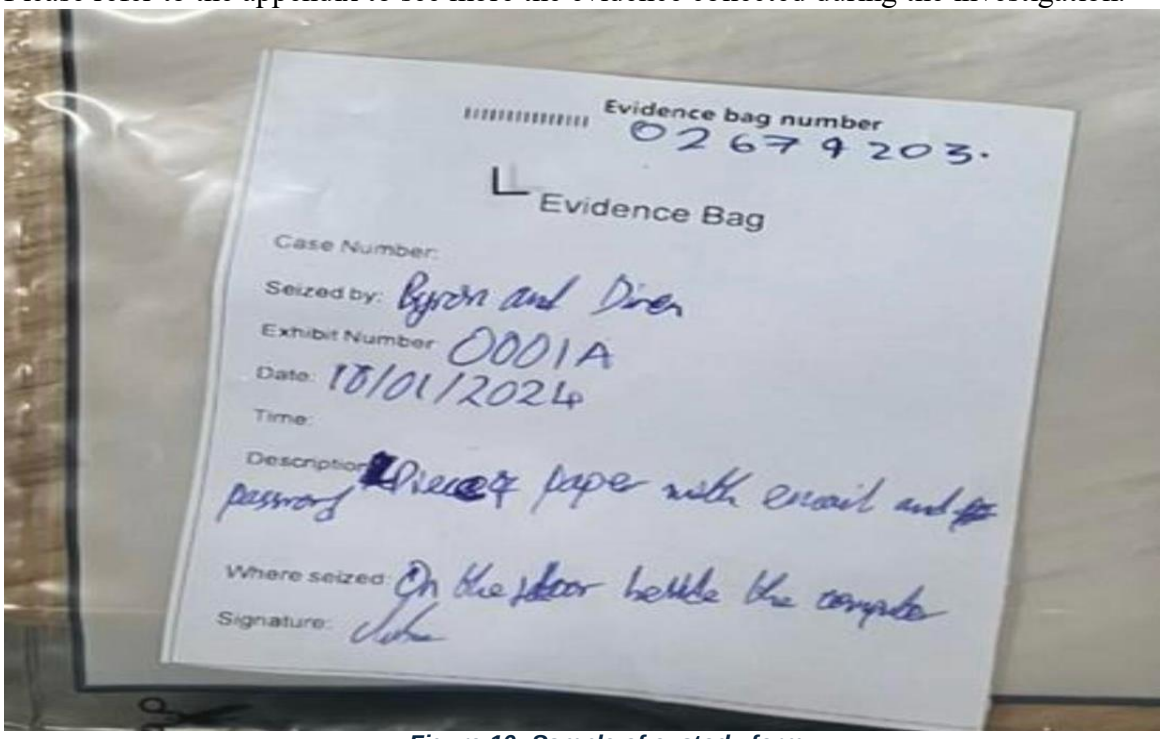


Figure 10: Sample of custody form

5.0 – Examination & Analysis

5.1 - Objective

The examination phase dissects collected evidence, acting as a powerful lens to understand the incident's nature and scope. System logs, network traffic, file metadata, and user activity logs undergo meticulous scrutiny for anomalies.

Forensic tools become an extension of the investigator's expertise. Advanced software recovers deleted data, hashing algorithms ensure evidence integrity, while specialized utilities unearth hidden files or malicious programs.

Beyond the tools lies the art of forensic analysis. Each piece of evidence is carefully considered for its relevance to the incident timeline, method of acquisition, and any associated metadata. Digital forensic experts meticulously reconstruct events, piecing together fragmented data to form a chronological picture.

The examination extends beyond traditional devices. Cloud storage, social media, and communication channels are explored for additional evidence. This holistic approach ensures no stone is left unturned.

Findings are meticulously documented through detailed notes and forensic reports, forming a crucial foundation for further analysis and potential legal proceedings.

Ultimately, the examination phase aims to provide a detailed and accurate assessment of the digital evidence, guiding decision-making, and future actions. It transforms raw data into actionable insights, empowering investigators to navigate the incident and deliver a resolution.

5.2 - Forensic Software Suite

Digital forensics investigations rely heavily on specialized software suites. These comprehensive toolkits act as an investigator's digital workbench, offering a vast array of functionalities. From securely acquiring evidence from various devices and storage media to meticulously carving deleted data and piecing together a chronological timeline of events, forensic software empowers investigators to analyze, examine, and process digital evidence with precision and efficiency. These suites offer functionalities like data recovery, data

analysis, metadata extraction, keyword searching, and report generation, ensuring a thorough and well-documented examination process.

For this investigation the following software was used:

- FTK 8.0
- Autopsy 4.21.0

5.3 Creating a case in Autopsy

Before creating a case in autopsy. Our case number had to be carefully considered. Factors such as location, date of case initiation, sequential number and investigator initials.

Considering these factors, the case number **MAU-01182024-BDH-001.** Here's a breakdown of why the case number was used:

MAU: This represents the country code for Mauritius, indicating the jurisdiction of the case.

01182024: This denotes the date when the case was initiated, following the format MMDDYYYY (Month-Day-Year). In this case, it's January 18, 2024.

BDH: These are our initials, identifying us as the investigators assigned to the case.

001: This is a sequential number assigned to the case. Since it's our first case in Mauritius on January 18, 2024, it starts with "001."

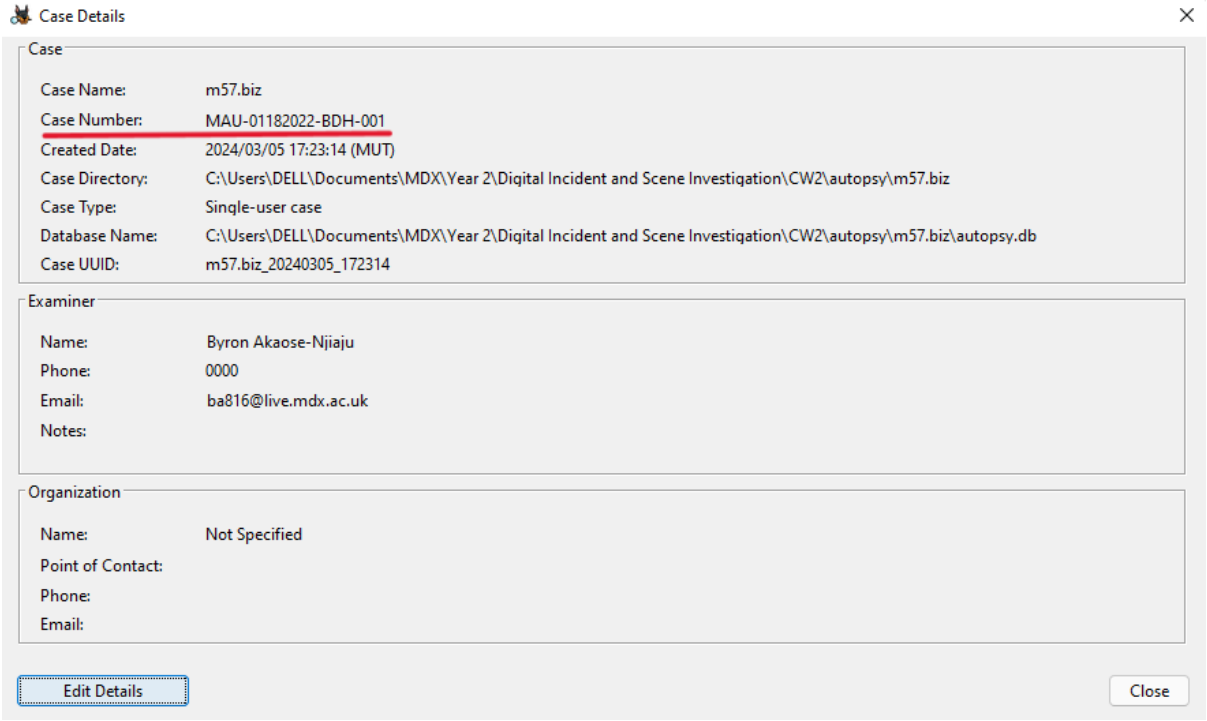
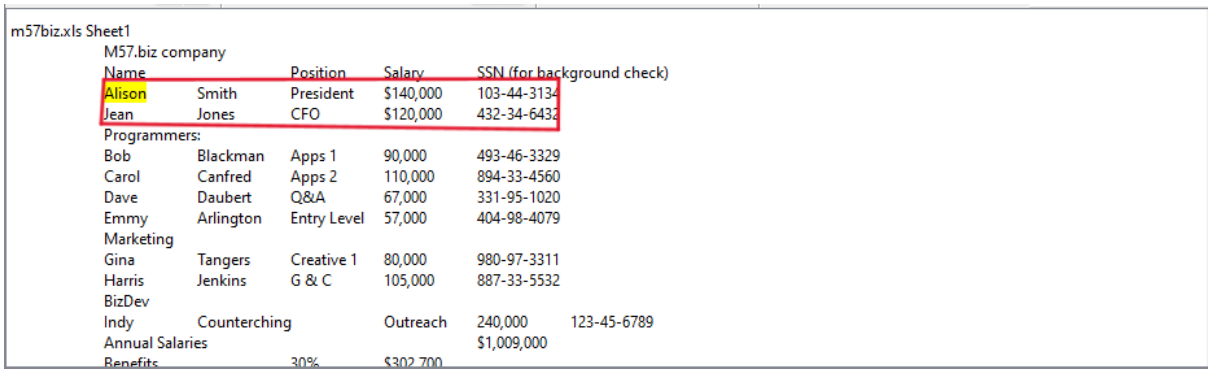


Figure 11: Autopsy Case Information - m57.biz

Figure 7.1 shows the case details of our already created case in Autopsy. Our case number can be clearly seen underlined in the image. This case number helps in organization, tracking, documentation, and reporting.

5.4 - Examination of the exhibits



m57biz.xls Sheet1

M57.biz company					
Name		Position	Salary	SSN (for background check)	
Alison	Smith	President	$140,000	103-44-3134	
Jean	Jones	CFO	$120,000	432-34-6432	
Programmers:					
Bob	Blackman	Apps 1	90,000	493-46-3329	
Carol	Canfred	Apps 2	110,000	894-33-4560	
Dave	Daubert	Q&A	67,000	331-95-1020	
Emmy	Arlington	Entry Level	57,000	404-98-4079	
Marketing					
Gina	Tangers	Creative 1	80,000	980-97-3311	
Harris	Jenkins	G & C	105,000	887-33-5532	
BizDev					
Indy	Counterching		Outreach	240,000	123-45-6789
Annual Salaries				$1,009,000	
Benefits		30%	$302,700		

Figure 12: Employee database

It shows the breakdown of salaries as well as positions for each of the employees in the company.

5.5 - Examination of the USB Pen Drive Case

During the investigation, there was a suspicion of a USB pen drive's involvement in the incident, considering the attack's characteristics and modus operandi. However, upon thorough examination of the scene and relevant devices, the investigative team was unable to locate a physical USB pen drive associated with the incident. This absence raises questions regarding potential data transfer methods and the use of removable media during the attack.

5.5.1 - Potential content of the suspected USB drive

Malicious Payloads: Infected files, executables, or scripts intended to facilitate unauthorized access or compromise.

Data Exfiltration Tools: Software tools designed to extract or transfer sensitive data from compromised systems.

Encryption Tools: Utilities for encrypting or concealing data to evade detection or enhance privacy.

Steganography Software: Applications used to embed data within innocuous files or images, allowing for covert communication or data hiding.

Incident-Related Files: Documents, logs, or configuration files relevant to the attack, providing clues about the attackers' methods and motives.

Persistence Mechanisms: Scripts or tools configured to establish persistent access to compromised systems, enabling continued unauthorized activities.

Evidence of Data Theft: Stolen data files, screenshots, or captured credentials intended for exfiltration.

While the absence of the USB pen drive complicates the investigation, these potential contents highlight the significance of removable media in digital incidents and underscore the need for comprehensive forensic analysis to uncover digital traces left behind by the attackers.

5.6 - Examination of the Hard Disk Drive Case

Physical Examination of the Hard Disk: Upon examination, the hard disk retrieved from the scene was found to be in optimal condition, showing no signs of physical damage or tampering that could compromise its integrity. This observation is crucial in ensuring the reliability of the forensic data extracted from the disk.

Hardware Specifications: The hard disk recovered from the scene is a standard PC disk, typically larger in size compared to those commonly used in laptops. The specifications of the hard disk are as follows:

- Form Factor: 3.5-inch
- Capacity: 256GB
- Interface: SATA
- Rotational Speed: N/A
- Cache Buffer: N/A

The 3.5-inch form factor denotes a standard desktop hard disk size, designed for use in desktop computer systems. This larger form factor is commonly associated with higher capacities and faster performance compared to laptop hard disks.

The interface type (e.g., SATA or IDE) specifies how the hard disk connects to the computer's motherboard, facilitating data transfer and communication between the disk and other system components.

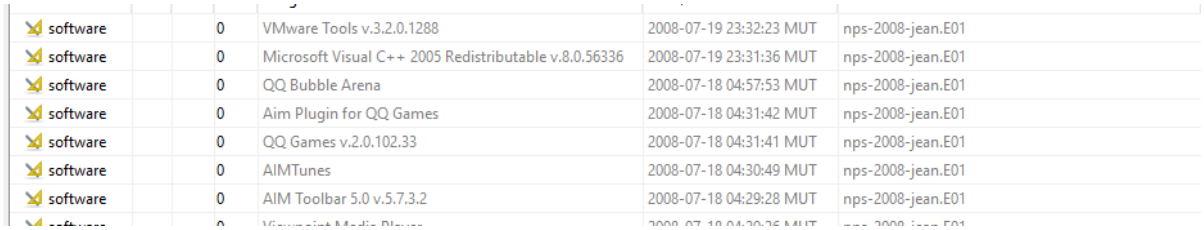
The rotational speed (measured in revolutions per minute, RPM) and cache buffer size contribute to the disk's overall performance, affecting read and write speeds during data access operations.

By providing these hardware specifications, the report aims to contextualize the forensic analysis conducted on the hard disk and highlight key details relevant to the investigation's findings.

5.7 - User Activity:

The examination of user activity plays a critical role in understanding the sequence of events and actions performed on the digital system under investigation. This section presents the methodology and findings of the user activity analysis conducted using Autopsy, including the utilization of screenshots to capture relevant evidence.

5.7.1 - Installed Programs



software		0	VMware Tools v.3.2.0.1288	2008-07-19 23:32:23 MUT	nps-2008-jean.E01
software		0	Microsoft Visual C++ 2005 Redistributable v.8.0.56336	2008-07-19 23:31:36 MUT	nps-2008-jean.E01
software		0	QQ Bubble Arena	2008-07-18 04:57:53 MUT	nps-2008-jean.E01
software		0	Aim Plugin for QQ Games	2008-07-18 04:31:42 MUT	nps-2008-jean.E01
software		0	QQ Games v.2.0.102.33	2008-07-18 04:31:41 MUT	nps-2008-jean.E01
software		0	AIMTunes	2008-07-18 04:30:49 MUT	nps-2008-jean.E01
software		0	AIM Toolbar 5.0 v.5.7.3.2	2008-07-18 04:29:28 MUT	nps-2008-jean.E01

Figure 13: Installed Software

The above image shows a screenshot of some key programs installed on the Jean's computer. Among these programs are games that shouldn't be on a work computer however one of the one's that stand out is VMware Tools. This program is accompanied by VMware and is used by the software optimize user experience when running virtual machines on a system. The strange part about this is I was unable to find VMware on the computer which suggests it might be deleted. It is strange for the CFO of a company to have VMware and need an extra OS apart from the native OS.

5.7.2 - Drive analysis

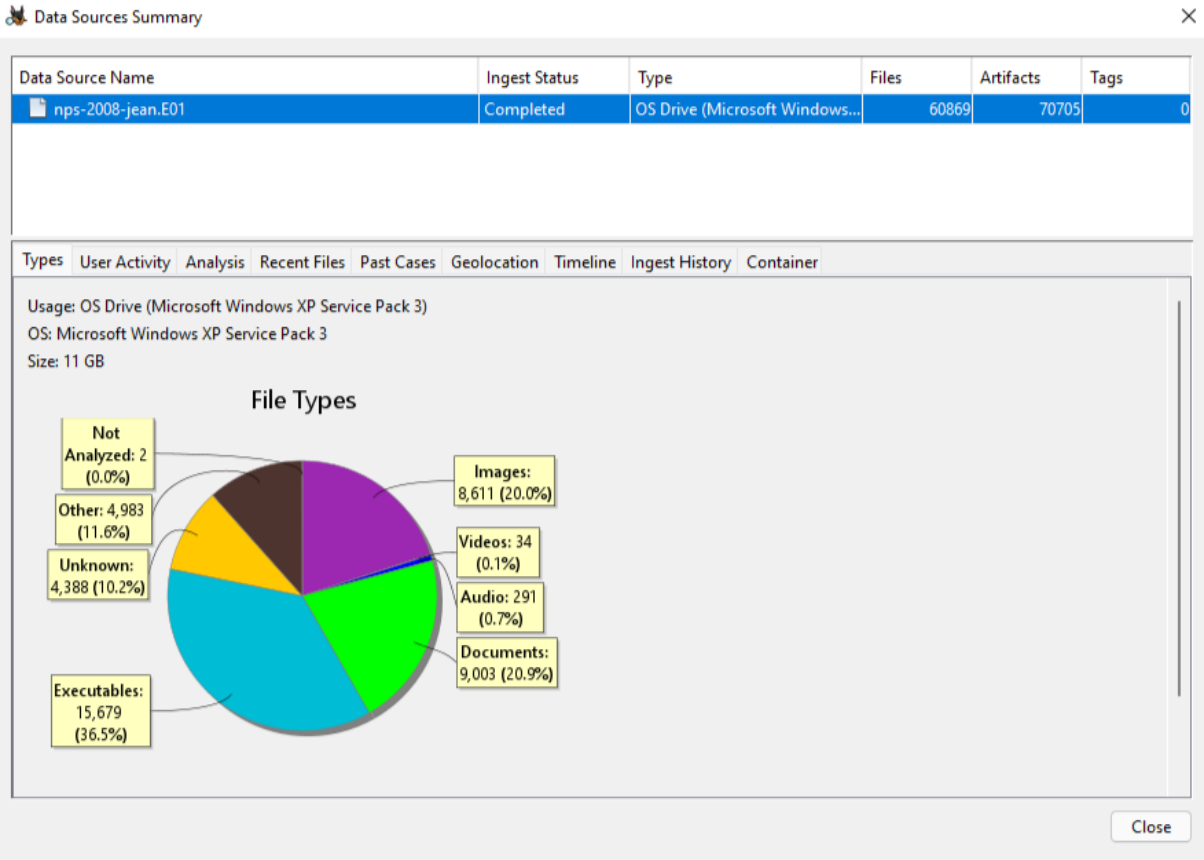


Figure 14: Drive analysis

In the image above we can see a summary of the filetypes and contents of the disk. In this we can see the user quite a large percentage of images and upon analysis of some of these images they seem to have been saved directly from the internet. This can be a security vulnerability as payloads can be injected into images.

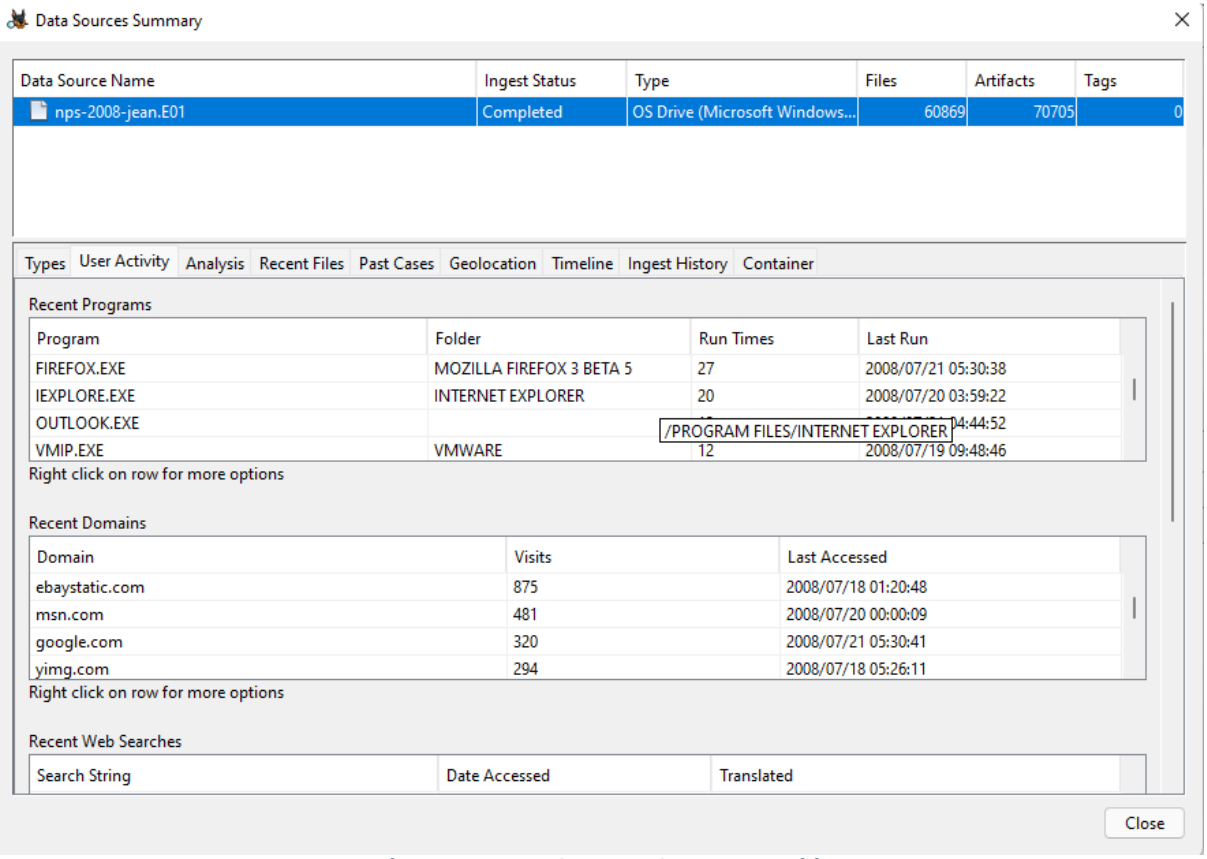


Figure 15: Data Sources Summary Table

In the capture above we can see the most recently used programs are the 2 browsers as well as the email service and VMware. It is strange that the Jean would use 2 different browsers simultaneously instead of opening new tabs to fulfill the work that needs to be done. He would also have his data on one of the browsers which would make using another one less convenient as he would have to start logging in to save cookies and passwords to the new browser. I am thinking the attacker might be using one of the new browsers as well as

VMware. However, this is purely speculation.

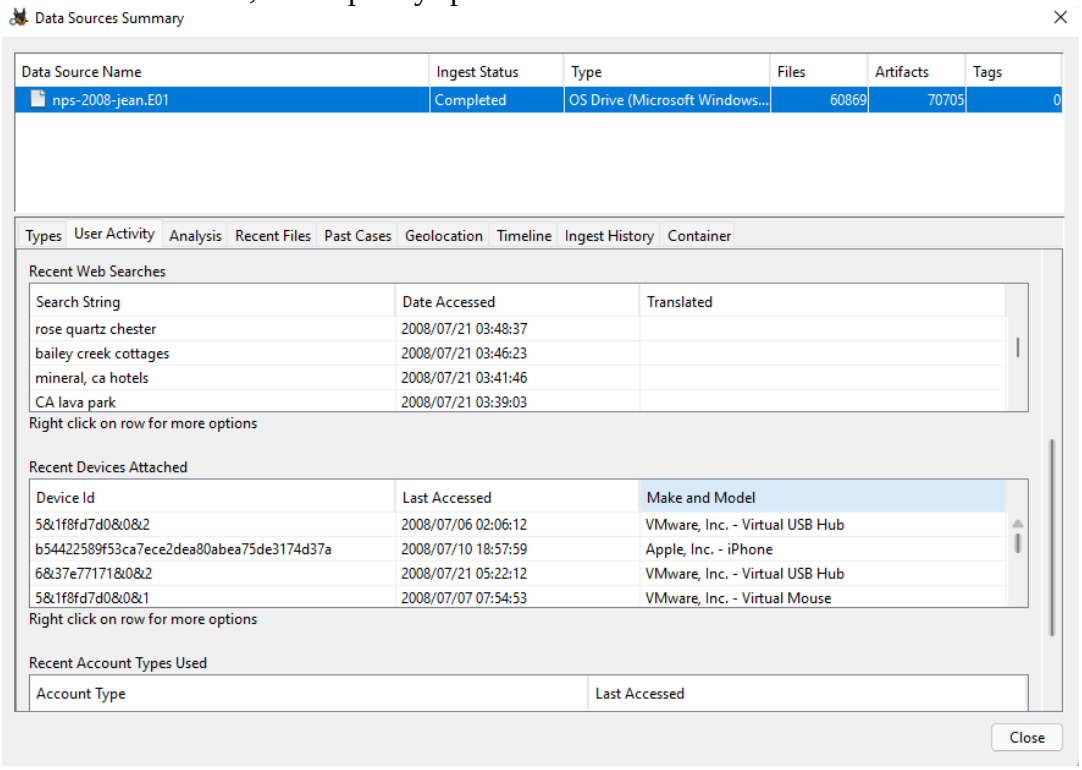


Figure 16: Summary of User Activity Including Web Searches and Devices Attached

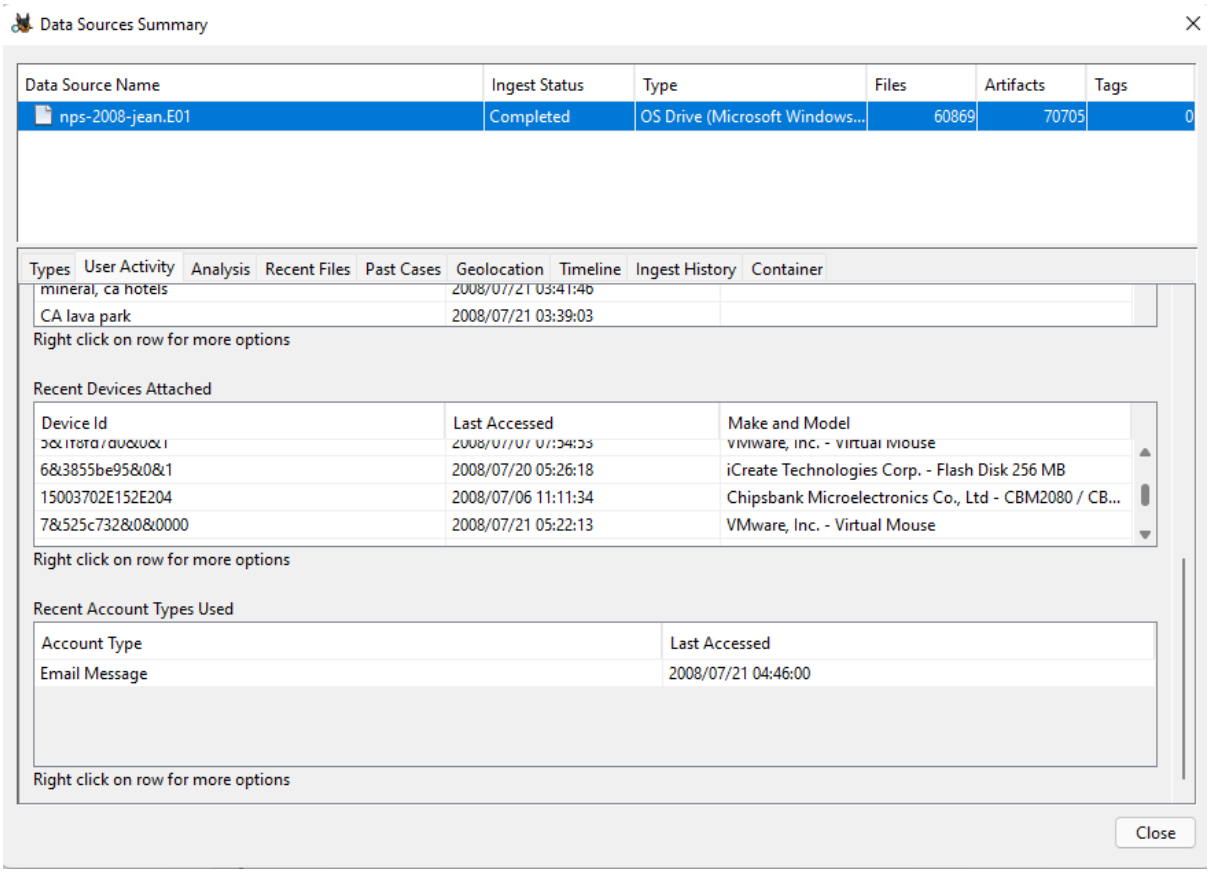


Figure 17: Data Source Report with Ingest Status, File/Artifact Counts, and User Activity

In the captures above (7.6 and 7.7) It shows the devices recently connected to the computer as well as recent web search history. From the devices connected we can 2 flash drives connected as well as multiple VMware connection including that of a USB hub which is usually used to expand the number of USB ports on a computer. I believe at least one of these flash drives belongs to the attacker and is the one that was expected on the crime scene.
As for the VMware connections I suspect the attacker used this program to compromise the security of the company further.

5.8 - System Activity

During the investigation, we employed forensic tools and techniques to access and parse these registry hive files, extracting relevant data and metadata to reconstruct the system's operational state. By examining timestamps, configuration details, and user-related information, we reconstructed a timeline of system events, user activities, and changes made to the system configuration.

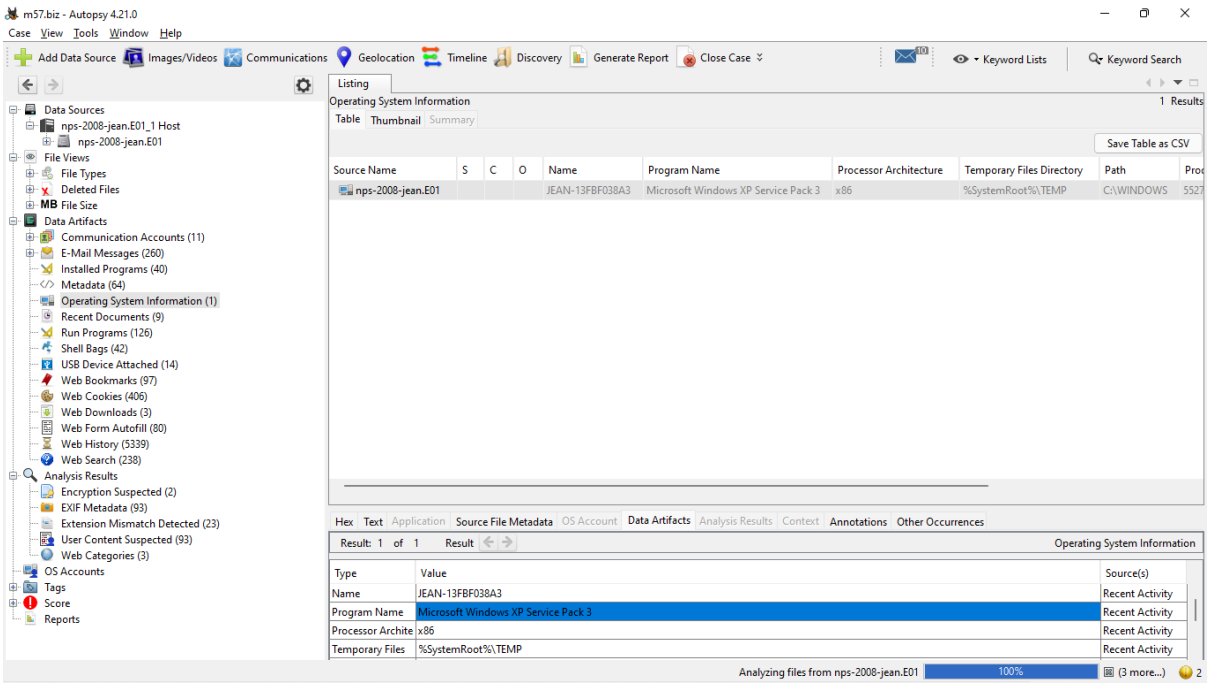


Figure 18: Forensics Analysis Interface with OS Details and File Data.

From the screenshot above we can see the operating system being run is Microsoft Windows XP Service Pack 3

Installation Date

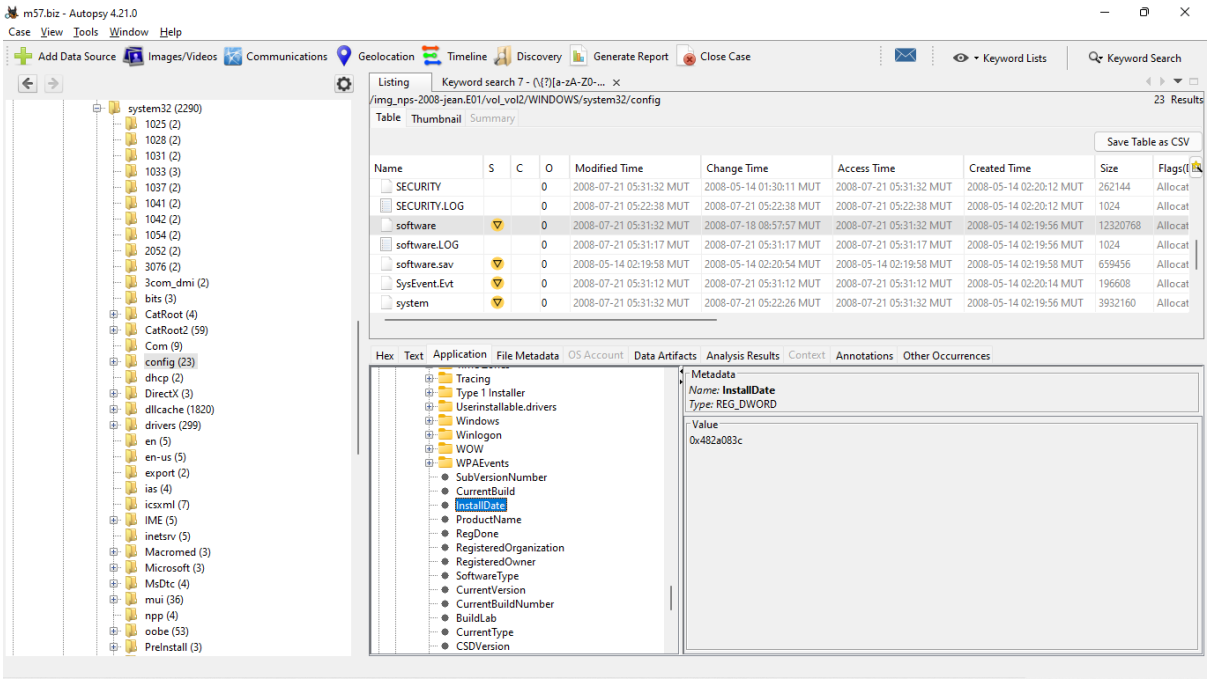


Figure 19: System Configuration Files in a Forensic Software Analysis

From the image we get a hexadecimal value of 0x482a083c. This would then be converted to a date using the encoding scheme.

Time Zone

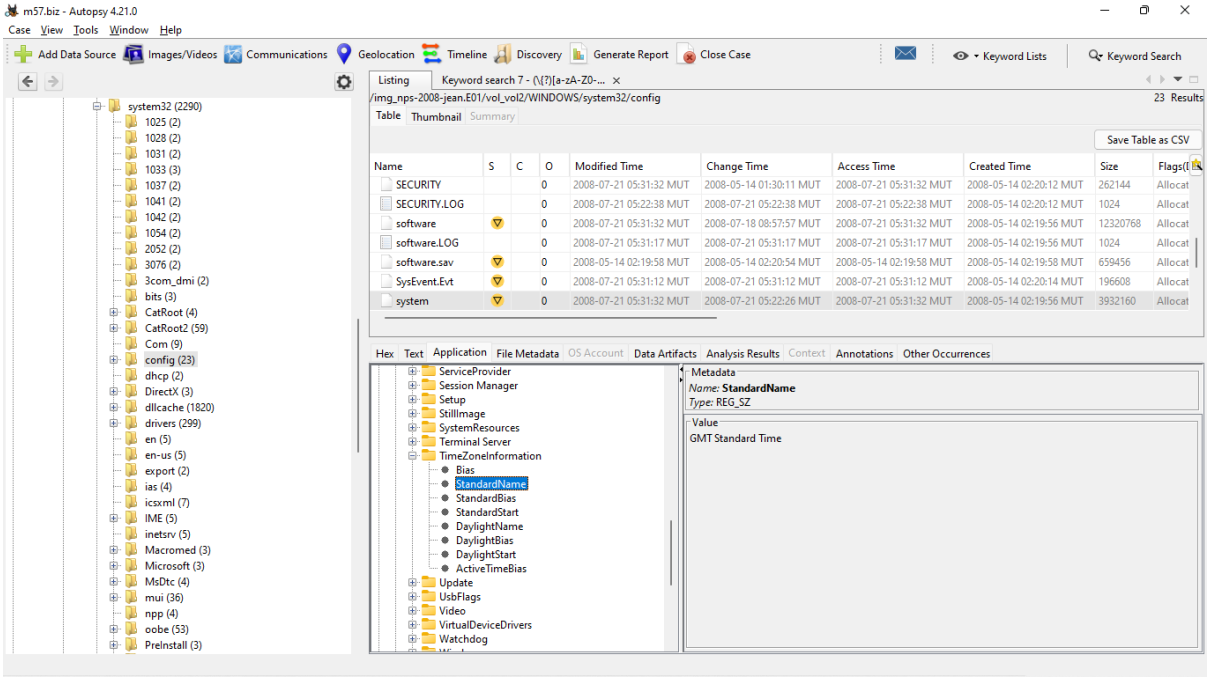


Figure 20: GMT Standard Time.

From the image above we can see the Time zone of the computer is using GMT Standard Time.

User Accounts and Properties

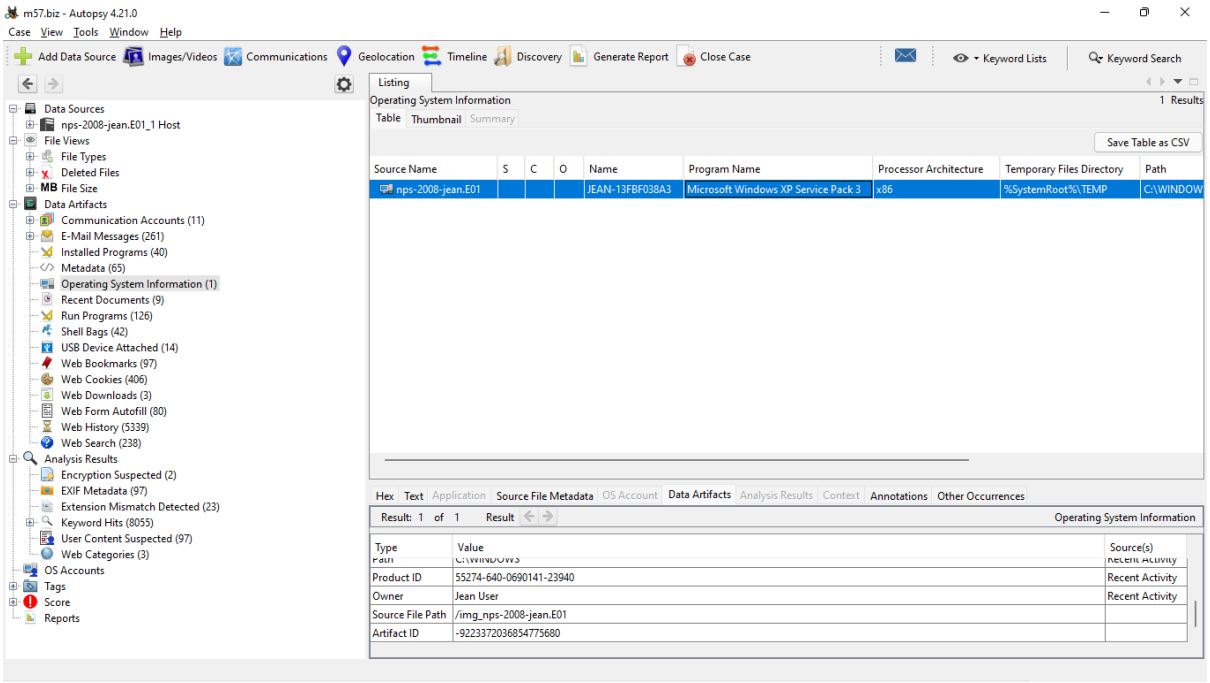


Figure 21: User account

From the screenshot above we can see that the registered user of this computer is Jean User

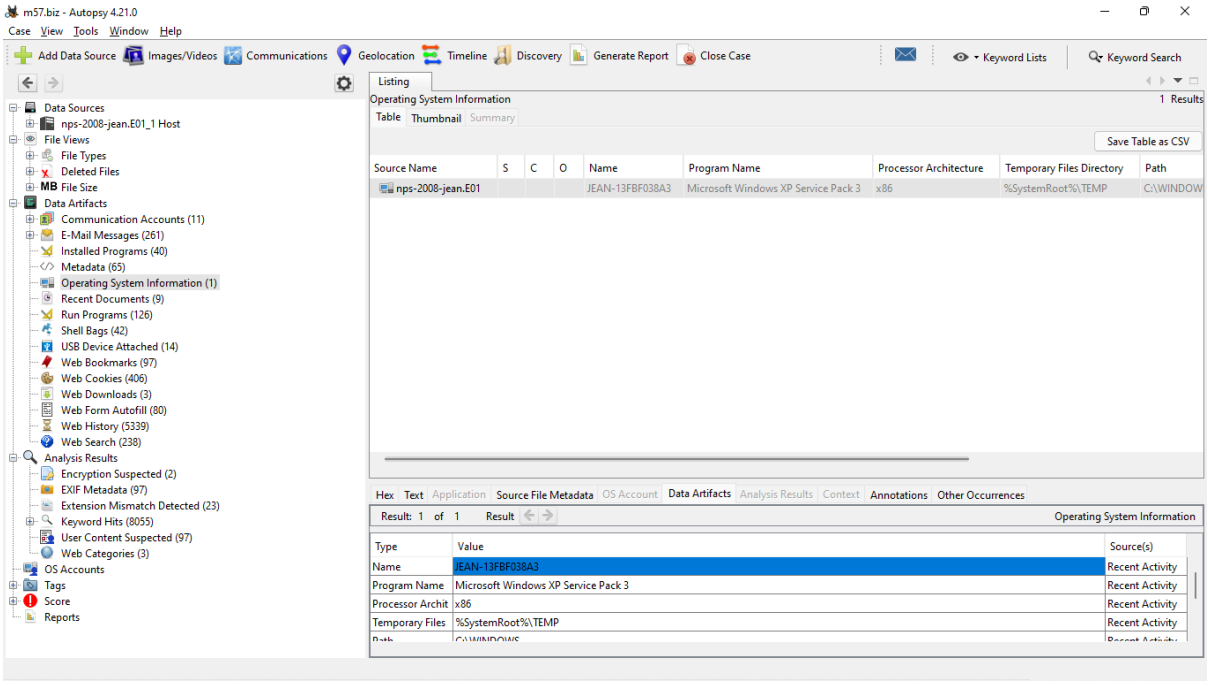


Figure 22: Computer account name

From this screenshot we can also see that the computer account name is JEAN-13FBF038A3.

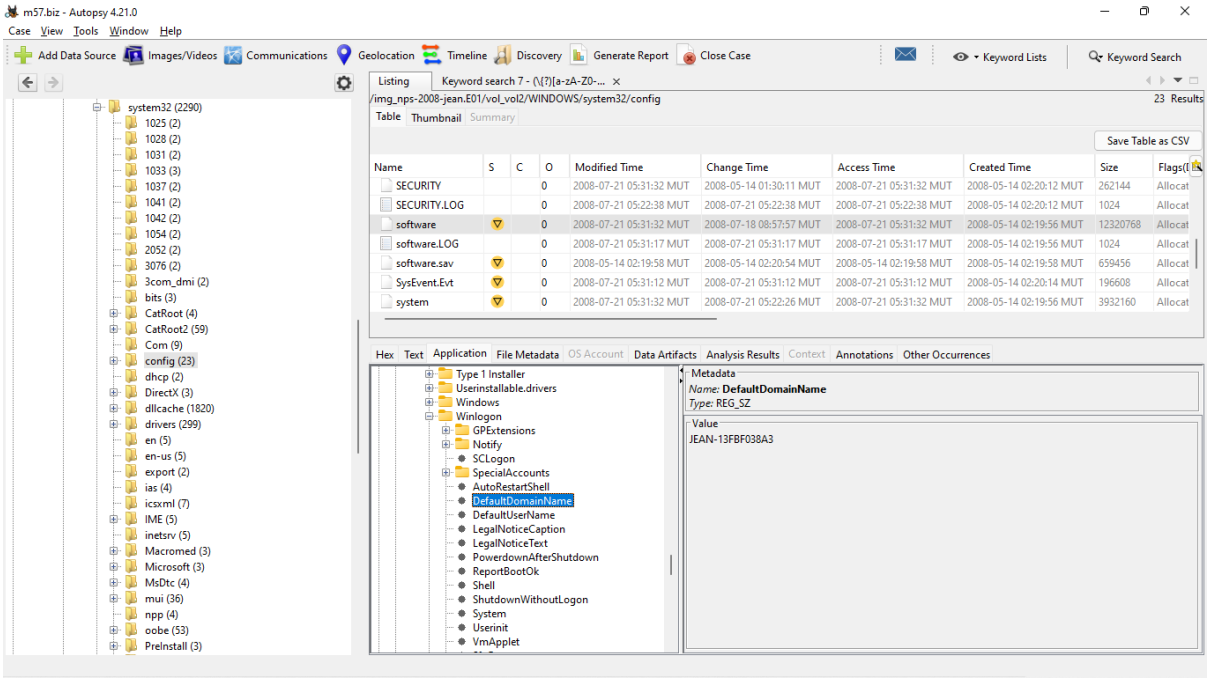


Figure 23: Default domain name

We can deduct from this capture that the Primary or Default Domain name is JEAN-13FBF038A3

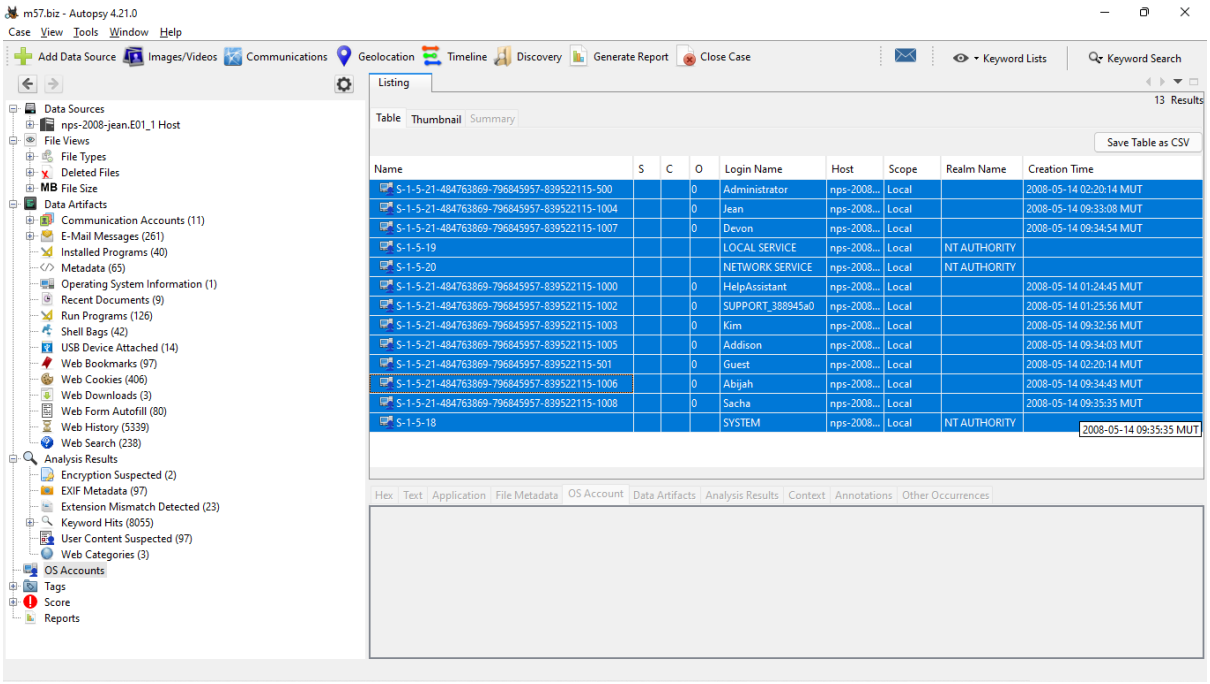


Figure 24: Accounts accessed, created, users

From this screenshot we can see the number of accounts present on the computer, both accounts that were user and system created. There seem to be 10 user created accounts and 3 system created accounts. We can also see the time the accounts were last accessed which are as follows:

Administrator – 2008-07-21 05:22:18 MUT

Jean – 2008-07-20 04:00:41 MUT

Devon – 2008-07-12 07:02:47 MUT

HelpAssistant – N/A

SUPPORT_388945a0 – N/A

Kim – N/A

Addison – N/A

Guest – N/A

Abijah – N/A

Sacha – N/A

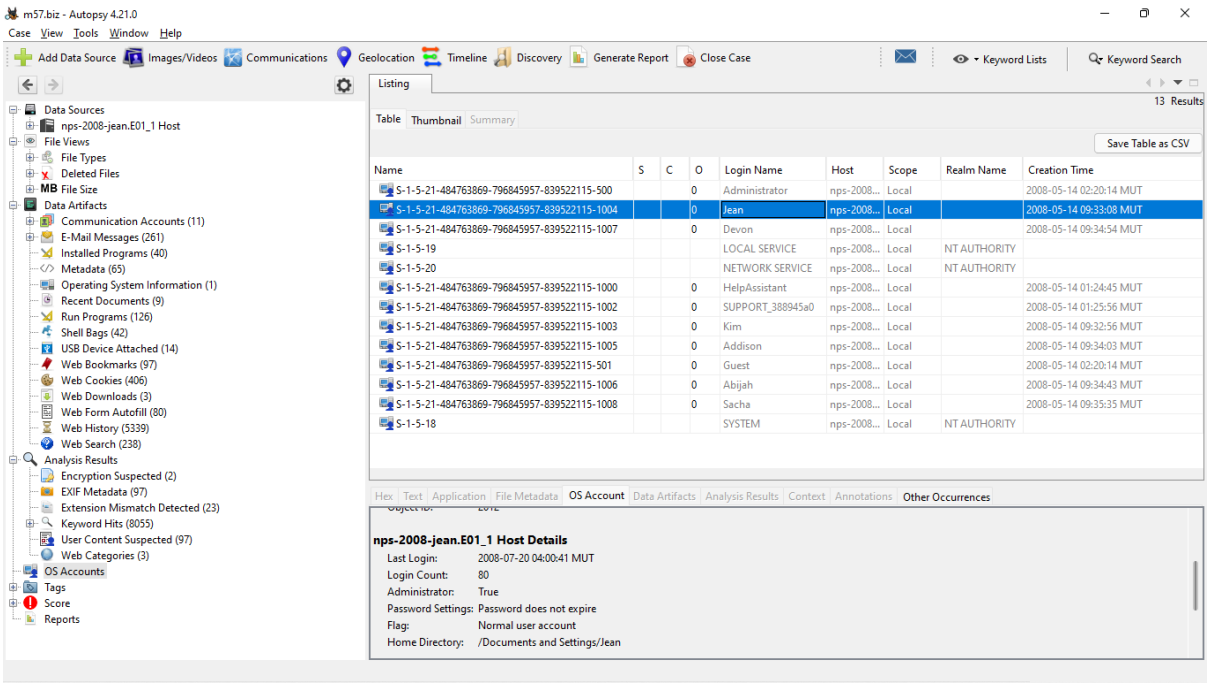


Figure 25: Frequent user of the computer

We can also see from this capture that the user that uses the computer the most is Jean.

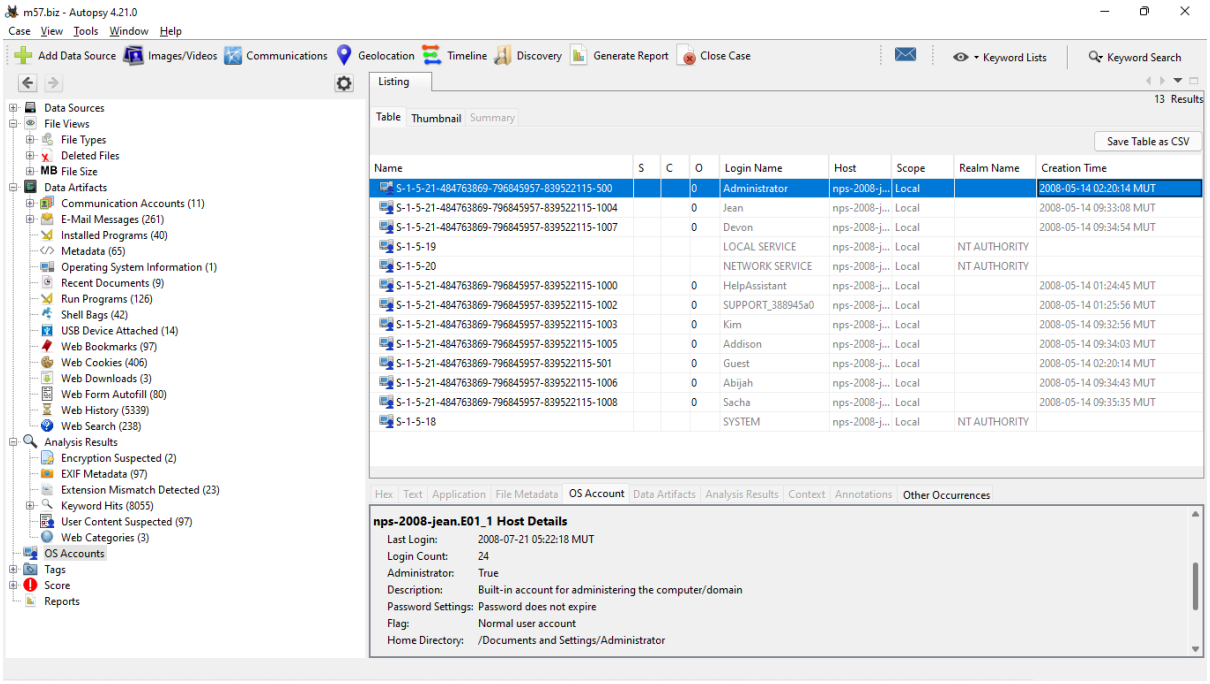


Figure 26: Last login

We can see in this screenshot the user that logged onto the system last was the user called administrator.

5.9 - E-mail analysis

The 'outlook.pst' file found at '/vol_vol2/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst' was used to gather more information about how the spreadsheet containing details about the salary and SSN of the employees got leaked. To investigate the 'outlook.pst' file, an online website called 'GoldFynch.com' (offering the facility to view pst files) was used. Once the file was uploaded, Jean's full Email Inbox, Deleted Items, Outbox, Sent Items were fully accessible. First let us note down who is communicating with which Email address. Alison would be using the Email address <alison@m57.biz>, Jean would be using the Email address <Jean@m57.biz>, Email of suspected attacker <tuckgorge@gmail.com>, a programmer bob <bob@m57.biz> and the webmaster carol <carol@m57.biz> .

On Jul 6, 2008, 23:25pm, Jean sends Emails Alison a link to which Alison replies that she would not know if this link were from an attacker or not. This indicates that Jean is not aware of the dangers of malicious links propagated through email inboxes. This further proves the point as Jean's Email inbox is found loaded with a bunch email which can lead to malicious websites.

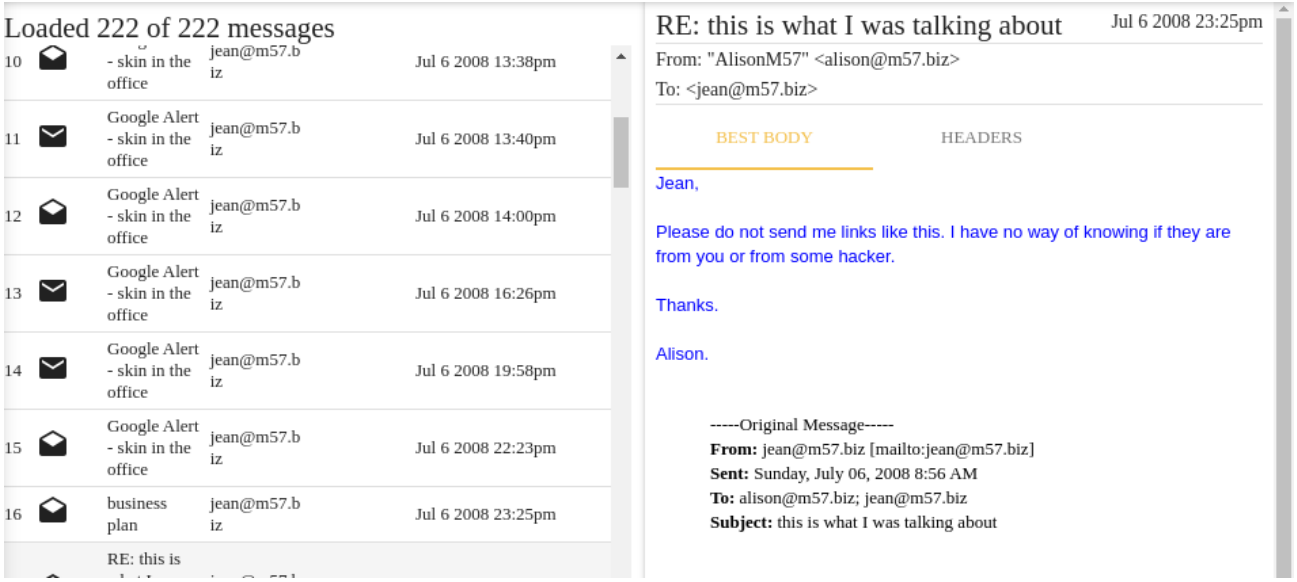


Figure 27: Alison warning Jean that any link sent by Email can by from an attacker

On Jul 20, 2008, 03:32am, Alison Emails Jean about financial plans without noticing that her Email address has been misconfigured from <alison@m57.biz> to <alex@m57.biz> to which Jean notices and sends and Alison email on the same day stating which Email address she would be using. Note: the time difference is because of different time zones as the employees are scattered across different countries.

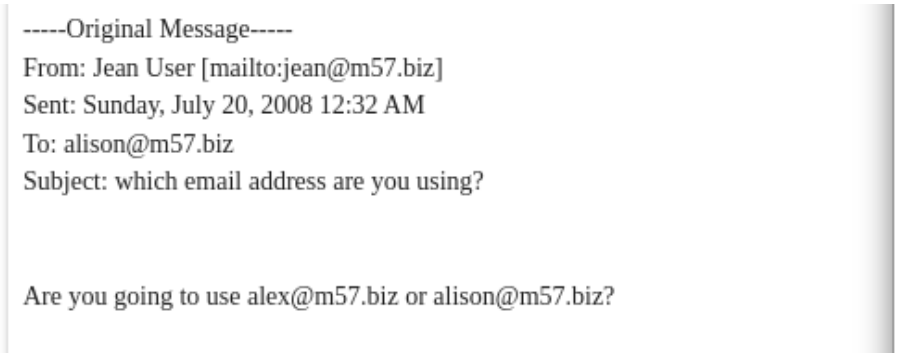


Figure 28:Jean asking which email Alison would use.

After ignorantly and impulsively replying to Jean's Email on the same day without checking the email header, she states that she will be using the currently misconfigured Email address.

-----Original Message-----
From: alex [mailto:alex@m57.biz]
Sent: Sunday, July 20, 2008 12:33 AM
To: Jean User; alison@m57.biz
Subject: RE: which email address are you using?

This one, obviously.

Figure 29: Alison instantaneously replying

She later replies that she will be using <alison@m57.biz> after she notices that her Email address has been misconfigured, which Jean unfortunately misunderstands.

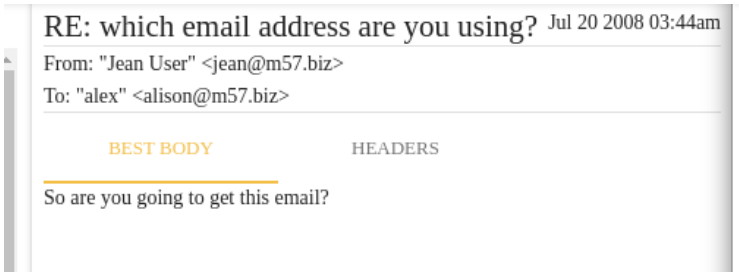
-----Original Message-----
From: alex [mailto:alison@m57.biz]
Sent: Sunday, July 20, 2008 12:44 AM
To: Jean User
Subject: RE: which email address are you using?

Whoops. It looks like my email was misconfigured.

My email is alison@m57.biz, not alex. Sorry about that.

Figure 30: Alison later finds out her about the misconfiguration

Figure 31: Jean replies without taking into consideration Alison's last reply



-----Original Message-----
From: Jean User [mailto:jean@m57.biz]
Sent: Sunday, July 20, 2008 12:47 AM
To: alison@m57.biz
Subject: RE: which email address are you using?

I'm confused.

Figure 32: Jean confused

Note: Jean replied to the email still confused at what email address Alison would be using.

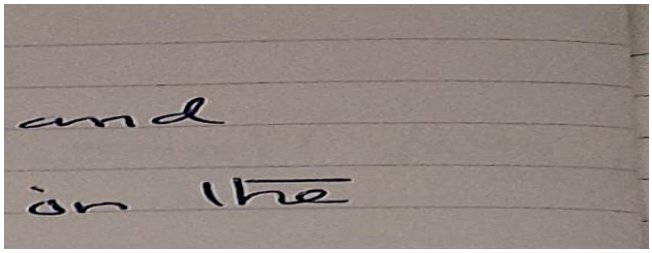


Figure 33: Alison tells Jean to stop emailing about this issue

This eventually leads to confusion down the road where Jean cannot tell which Email address Alison would be using in the future. Moreover, this results in Jean not really paying attention to the header of the Emails that she receives as long as the Body of the Email has something related to their business.

Furthermore, according to (Admin, 2023) It is true that email spoofing from well-known domains can be made possible by Misconfigured email servers. Email spoofing is a phishing and spam tactic in which the sender modifies the email header's "From" part to make it seem as though the email is coming from a reliable site or source. Hence it can be concluded that Alison tends to not check the “From:” part of an Email which also led to Jean adapting the same habit.

On Jul 20, 2008, 03:39am, Jean receives an email “background checks” from Alison telling her to compile a spreadsheet about the employees, their current salary, and their SSN (Social Security Number) to which Jean agrees. She also told Jean to keep this to herself. Keep in mind Jean is still confused about which Email address Alison could be using.

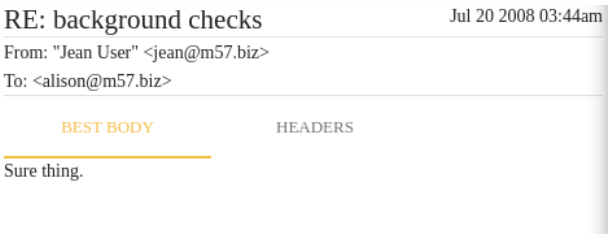


Figure 34: reply from Jean

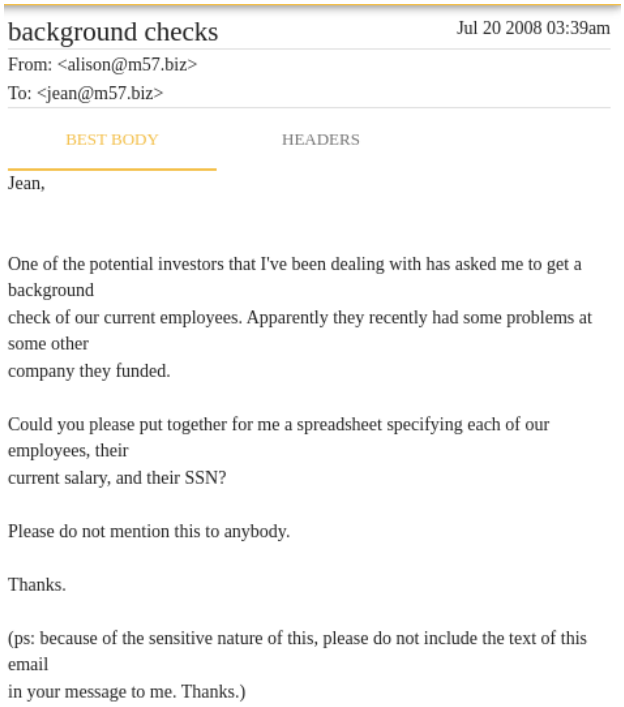


Figure 35: background checks.

On Jul 20, 2008, 05:22am, an unknown sender impersonating Alison using the Email address <tuckgorge@gmail.com>, Emails Jean requesting her the spreadsheet the real Alison told her to create. As Jean is confused about which Email address Alison might be using, when she saw the "From: " part of the Email saying "alison@m57.biz" <tuckgorge@gmail.com>, as long as Alison's Email address was mentioned and as long as the "Body" had something relating to their business, the Email seemed pretty legit and the Email address of the attacker next to the spoofed display name "alison@m57.biz" didn't matter to her since it looked like it was coming from a trusted source.

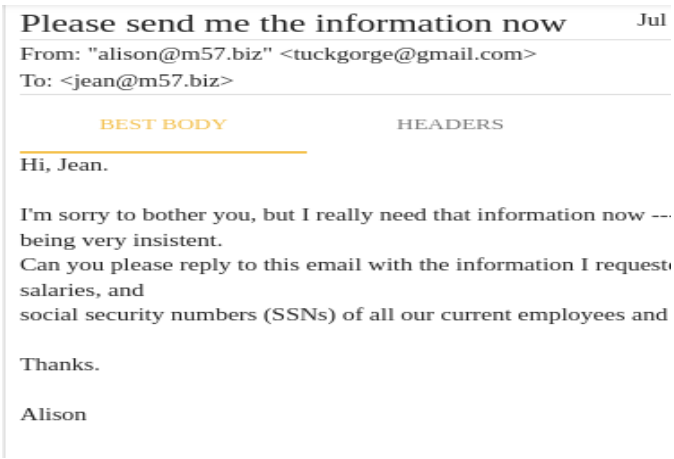
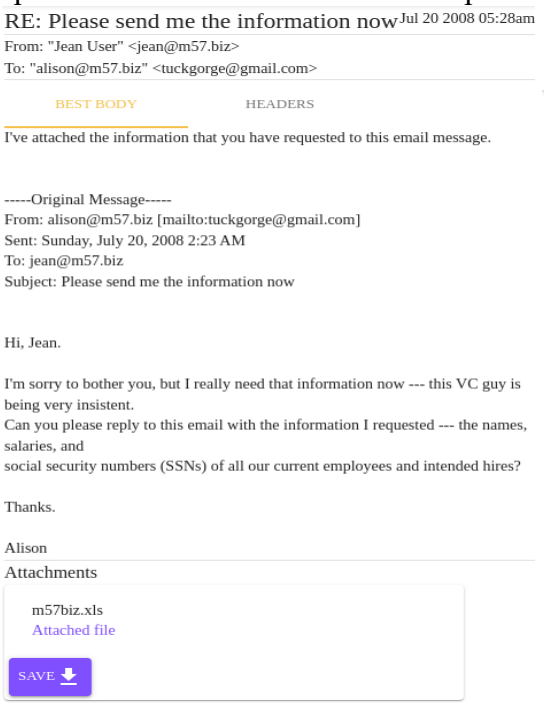


Figure 36: asking for information

Unfortunately, at 05:28 on the same day, Jean did reply to the Email by accessing the file from 'C:\Documents and Settings\Jean\Desktop\m57biz.xls' and attaching the spreadsheet containing the sensitive info and sent it to the attacker. If by any chance Jean did not reply to the Email but instead sent it directly to Alison using her legitimate Email address, the spreadsheet would not have ended up in the attacker's inbox.



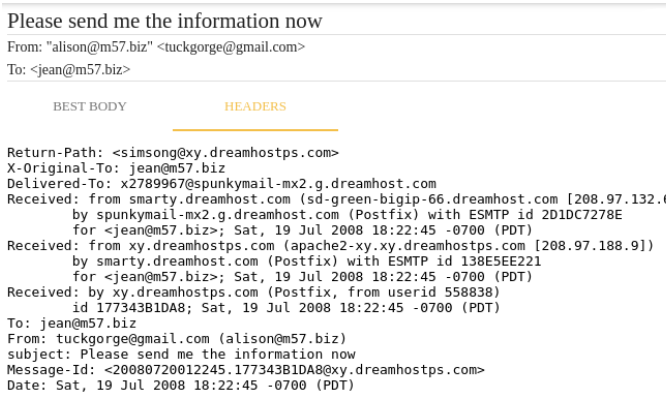


Figure 37: Attaching the file and the header of the email sent by the attacker

Note: simsong@xy.dreamhostps.com
using the reply address tuckgorge@gmail.com to email Jean...

Note: tuckgorge@gmail.com originating from the xy.dreamhostps.com domain to email Jean…

The attacker also thanks her and tells her to not tell anyone about this. This attack is called "Email display name spoofing."

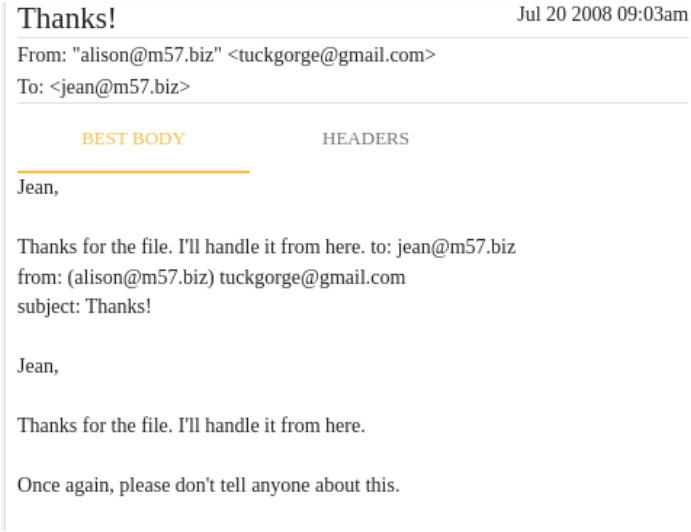


Figure 38: attacker thanks Jean

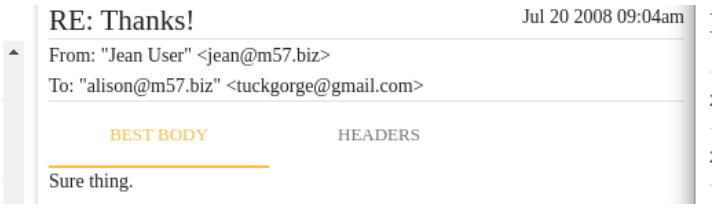


Figure 39: Jean replies back

From there everything started to go wrong. On Jul 21, 2008, 03:47am Jean receives an Email from Alison stating that Something very strange is going on to which Jean thinks she is talking about the slow network or a breaking.

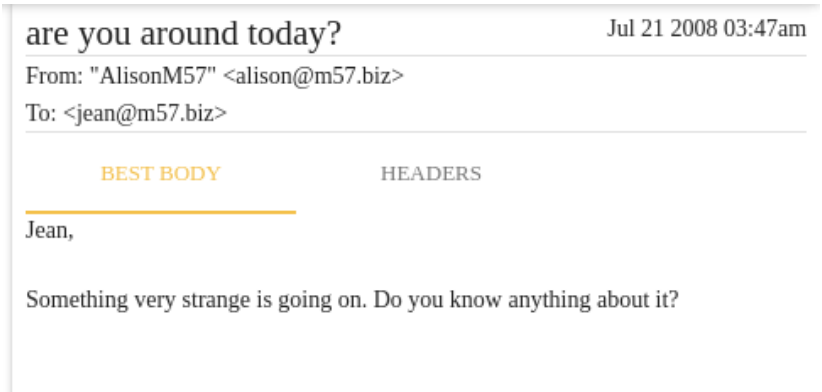


Figure 40: something strange

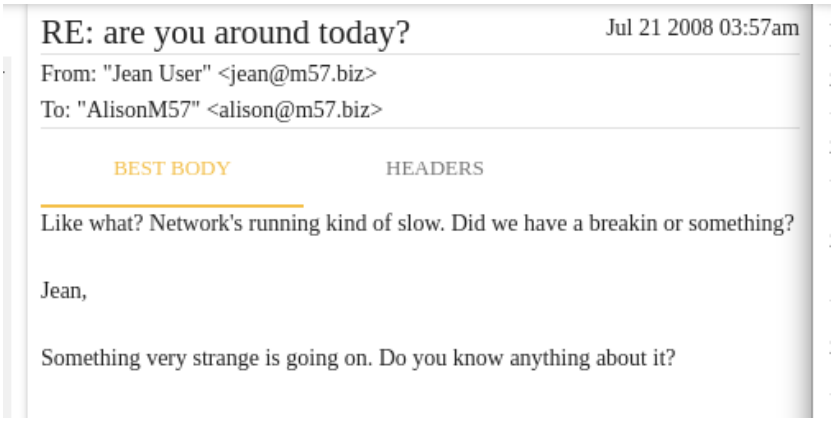


Figure 41: reply to something strange.

On the same day at 04:02am jean receives an email from bob <bob@m57.biz> where he asks jean if she was aware that his SSN was being passed on the internet. Jean was still unaware of what was going on. Note: read from bottom to top.

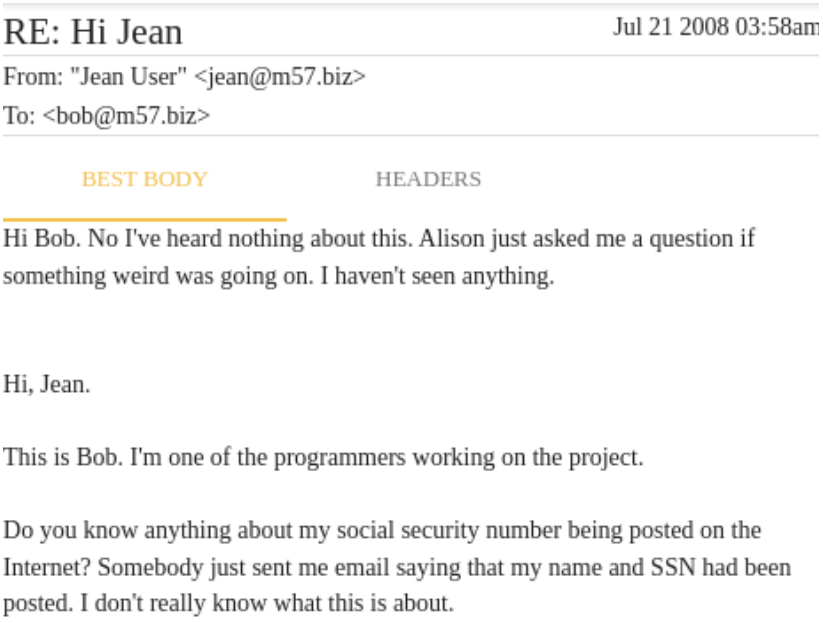


Figure 42: bob emails Jean about his SSN and Jean replies

On another email bob ask Jean if her SSN was 432-34-6432 and if she was making $120,000/year to which Jean confirmed and asked bob if he found that info on the same website that he found his.

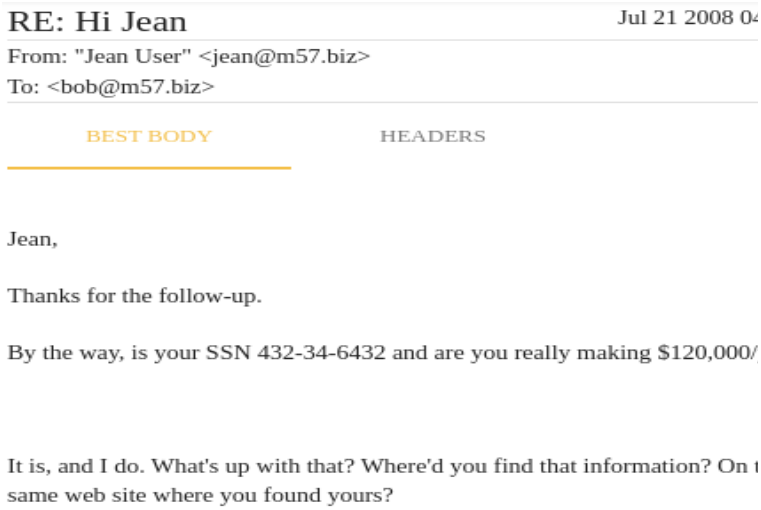
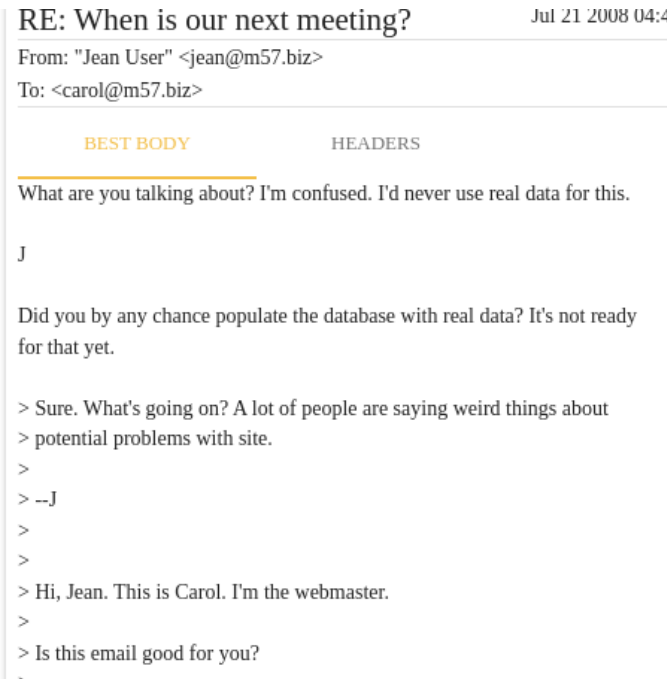


Figure 43: Jean surprised that Bob knows about that

At 04:10am the webmaster carol <carol@m57.biz> Emails Jean asking if she ever populated the database with real data to which Jean replies that she would never do that. Note: read from bottom to top.



On the same day at 04:11am Jean receives a last email from bob stating that since it is difficult for him to tell the difference between what he is sending and what Jean is sending and that his Email could be used as evidence in a court of law, he told her answer the following questions: '1. is your SSN 432-34-6432? 2 Are you really making $120,000year?' To which Jean confirmed. Jean still could not identify the problem. Note: read from bottom to top.

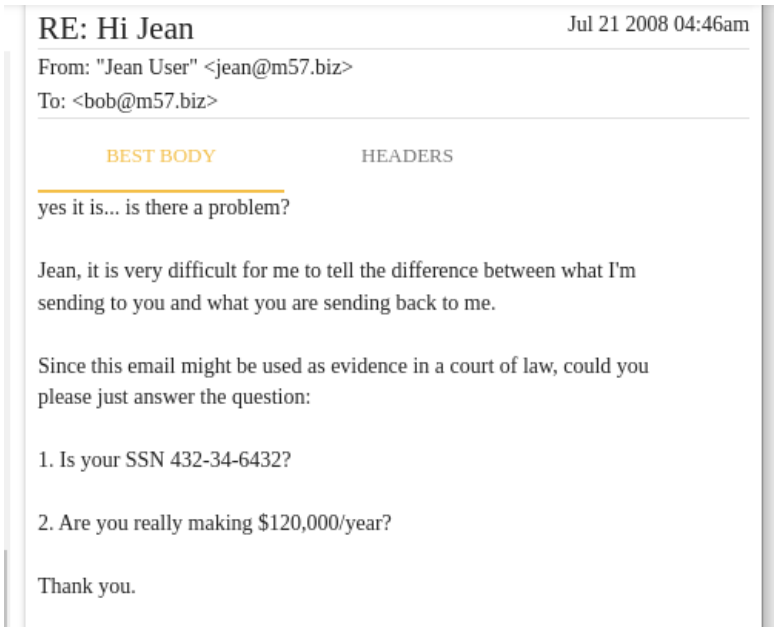


Figure 45: Last email from bob

When the Emails were being analyzed, none of them had adopted any of the three email authentication measures (SPF, DKIM, DMARC) which can leave the door open for spoofed emails. Email spoofing is theoretically possible because of the Simple Mail Transfer standard (SMTP), which is the primary email communication standard. Because SMTP lacks a way for authenticating the origin of an email, spoofing the source of an email is comparatively simple (Admin, 2023).

6.0 - Timeline

Date and Time	From	To	Subject	Notable Content
2008-07-20 02:23:45	alison@m57.biz	jean@m57.biz	Please send me the information now	Request for names, salaries, SSNs of employees and intended hires from VC.
2008-07-20 02:43:48	alex alison@m57.biz	-	RE: which email address are you using?	Notification of email misconfiguration, correct email is alison@m57.biz.
2008-07-20 02:59:57	alison@m57.biz	jean@m57.biz	background checks	Request for background checks from a VC, asking for employee details including SSNs.
2008-07-20 04:28:00	Jean User jean@m57.biz	alison@m57.biz	RE: Please send me the information now	Confirmation of attached information requested in the email.
2008-07-20 08:03:40	alison@m57.biz	jean@m57.biz	Thanks!	Acknowledgment of received information with a note to handle it from there.
2008-07-20 08:04:00	Jean User jean@m57.biz	alison@m57.biz	RE: Thanks!	Short acknowledgment.

On July 20, 2008, a series of email communications took place between Alison and Jean from m57.biz, involving sensitive employee information. At 02:23:45, Alison sent an urgent email to Jean requesting the names, salaries, and Social Security numbers of all current employees and potential hires. This request was prompted by the insistence of a venture capitalist (VC). Shortly after, at 02:43:48, a clarification email was sent from Alison's misconfigured email alias 'alex' at m57.biz, noting the correct email address to use for future communications.

At 02:59:57, Alison sent another email to Jean regarding background checks. The message indicated that a VC had asked for a background check of current employees, including sensitive information such as Social Security numbers. Jean responded at 04:28:00, confirming the requested information had been attached to their email, suggesting compliance with Alison's earlier request. Alison acknowledged receipt of this information at 08:03:40, expressing gratitude and indicating an intent to manage

the matter moving forward. Finally, at 08:04:00, Jean sent a brief reply to Alison simply stating "RE: Thanks," which appears to be a closure to the email thread.

6.1 - RECYCLER

When it comes to the 'RECYCLER' folder, nothing alarming was really discovered. In the folder 'S-1-5-21-484763869-796845957-839522115-1004' inside the 'RECYCLER' folder, 3 files were found namely: 'Dc1.jpg', 'desktop.ini', 'INFO2'. 'Dc1.jpg' was only an image about the website del.icio.us which were showing tags such as 'game', 'CSS', 'linux', 'internet' etc… which were not important to the case.

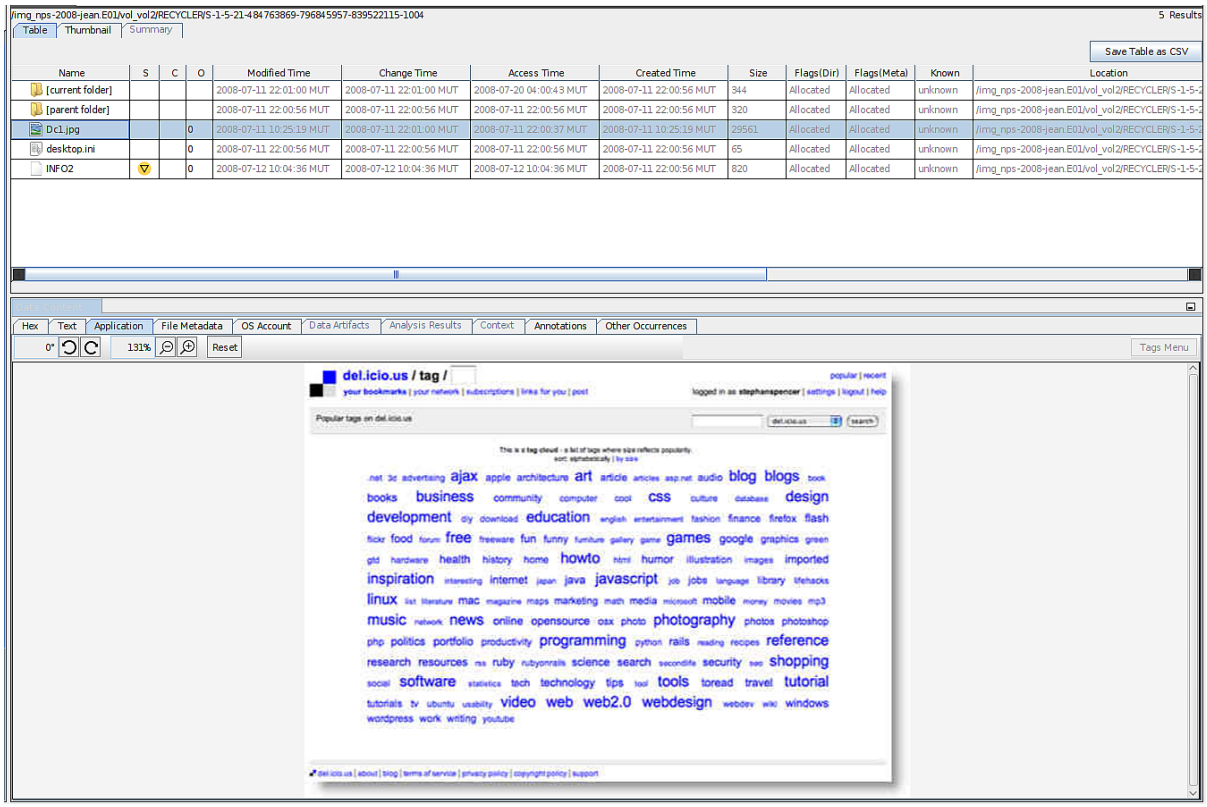


Figure 46:Dc1.jpg image

Metadata

Name:	/img_nps-2008-jean.E01/vol_vol2/RECYCLER/S-1-5-21-484763869-796845957-839522115-1004/Dc1.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	29561
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2008-07-11 10:25:19 MUT
Accessed:	2008-07-11 22:00:37 MUT
Created:	2008-07-11 10:25:19 MUT
Changed:	2008-07-11 22:01:00 MUT
MD5:	6d98ecf092fbb774eb8da5850203dd41
SHA-256:	573f247c595baf81919a59e18f56d7f2f244bbc045fda9a2b4649ca55f0abe62
Hash Lookup Results:	UNKNOWN
Internal ID:	24064

Figure 47: Metadata

The last file ‘INFO2’ file provided us with a directory ‘C:\Documents and Settings\Jean\Desktop\tag-cloud.jpg’ which when looking for the specific file ‘tag-cloud.jpg’ through the file system did not provide anything except for when a Keyword search for the directory was used which gave me the resulting files: ‘tag-cloud.ink’, ‘INFO2’, ‘$MFT’, ‘Recent Documents Artifact’. All of the files had almost the same information that the previous file ‘INFO2’ had. The only kind of valuable information that was found in the file ‘tag-cloud.ink’ was that it had the MIME Type: application/octet/stream.

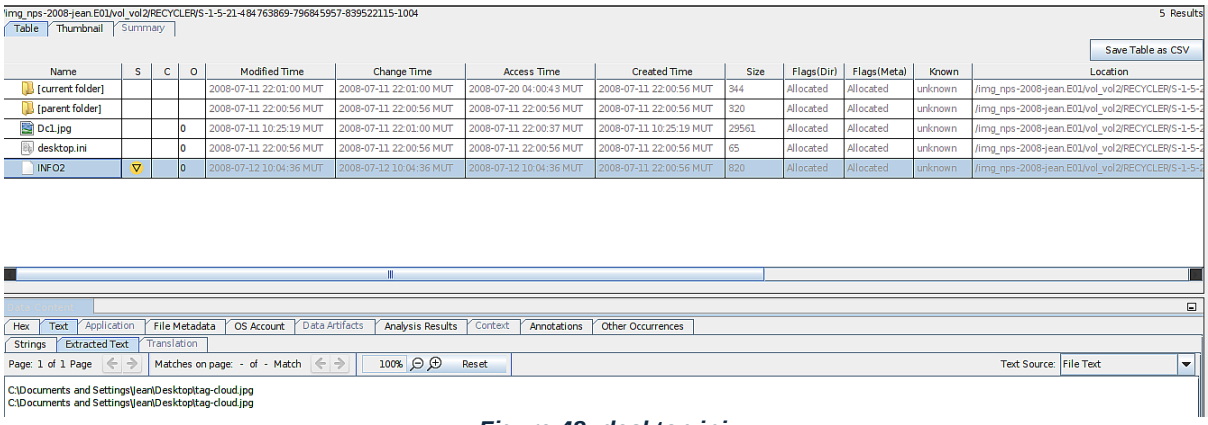


Figure 48: desktop.ini.

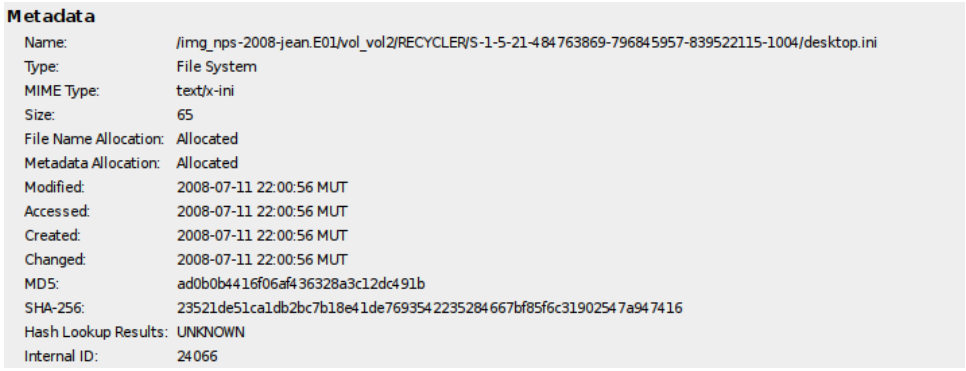


Figure 49: desktop.ini. meta data

The last file ‘INFO2’ file provided us with a directory ‘C:\Documents and Settings\Jean\Desktop\tag-cloud.jpg’ which when looking for the specific file ‘tag-cloud.jpg’ through the file system did not provide anything except for when a Keyword search for the directory was used which gave me the resulting files: ‘tag-cloud.ink’, ‘INFO2’, ‘$MFT’, ‘Recent Documents Artifact’. All of the files had almost the same information that the previous file ‘INFO2’ had. The only kind of valuable information that was found in the file ‘tag-cloud.ink’ was that it had the MIME Type: application/octet/stream.

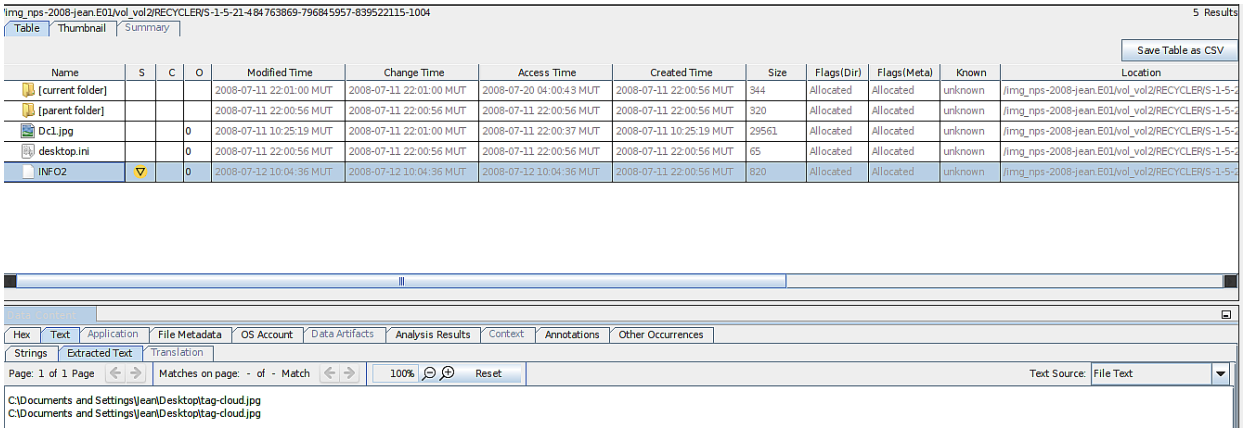


Figure 50: INFO2

Metadata

Name:	/img_nps-2008-jean.E01/vol_vol2/RECYCLER/S-1-5-21-484763869-796845957-839522115-1004/INFO2
Type:	File System
MIME Type:	application/octet-stream
Size:	820
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2008-07-12 10:04:36 MUT
Accessed:	2008-07-12 10:04:36 MUT
Created:	2008-07-11 22:00:56 MUT
Changed:	2008-07-12 10:04:36 MUT
MD5:	e49f95e9219ebe0a16d1e69658bc1526
SHA-256:	997220390993a85fc7171d88f74c83be72e124fd09780f234d106aa417541284
Hash Lookup Results:	UNKNOWN
Internal ID:	24067

Figure 51: INFO2 Metadata

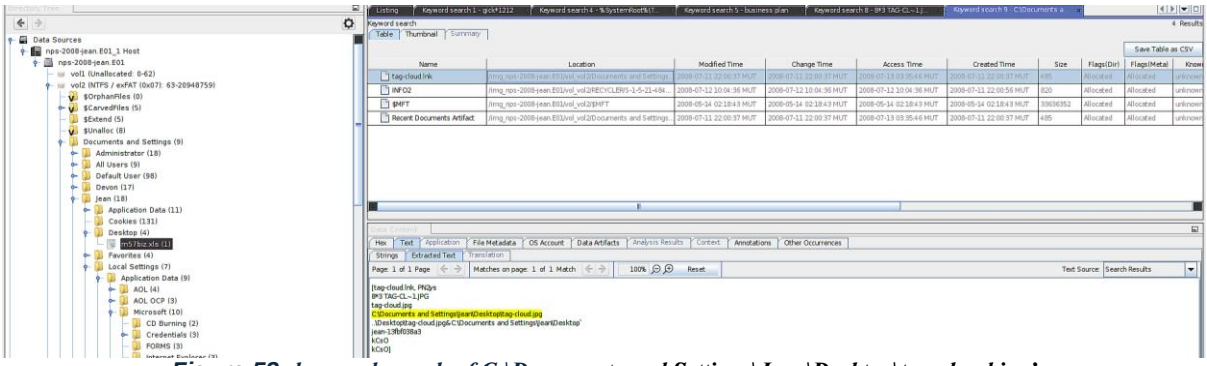


Figure 52: keyword search of C:\Documents and Settings\Jean\Desktop\tag-cloud.jpg'

6.2 - Encrypted files

A file commonly associated with Microsoft Windows operating systems is OEMBIOS.BIN. Original Equipment Manufacturer Basic Input/Output System Binary is what it stands for. This file includes information on a computer system's BIOS (Basic Input/Output System), which has been specially modified or adapted for a single manufacturer (OEM).
BIOS is a firmware interface that gives the operating system and applications runtime services and initializes devices upon booting. OEMs frequently alter the BIOS to offer new functionality or to fit their unique hardware configurations.
Drivers, settings, and configurations unique to the hardware the OEM installed on the computer may be found in OEMBIOS.BIN. Usually, it's incorporated in the motherboard's firmware or

concealed behind a hard disk partition. End users are not supposed to access or modify it directly because doing so could lead to system failure or instability (Flicker, 2024).

Source Name	S	C	O	Source Type	Score	Concl
oembios.bin			1	File	Likely Notable	
oembios.bin			1	File	Likely Notable	
oembios.bin			1	File	Likely Notable	
oembios.bin			1	File	Likely Notable	

Figure 53: oembios.bin from encryption suspect files folder

The Encryption suspect files only contained 'oembios.bin' files.

6.3 - Deleted files

The most pertinent files that were found in the deleted files were Jean's deleted cookies namely: 'jean@2o7[2].txt', 'jean@abmr[1].txt', 'jean@msnbc.msn[2].txt', 'jean@msn[2].txt'. Those might have been deleted because of a number of reasons such as, to enhance security, especially if it is suspected that the particular device has been compromised or if they want to prevent unauthorized access to the account on the website that the cookies were assigned to the user, may it be First-party or Thrid-party cookies. Another reason might be the routine maintenance of the device without any specific motive related to privacy or security.

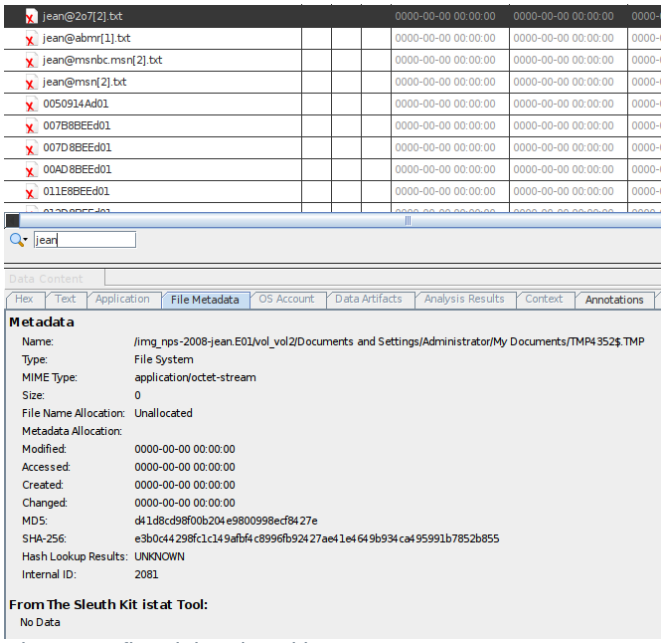


Figure 54: first deleted cookie

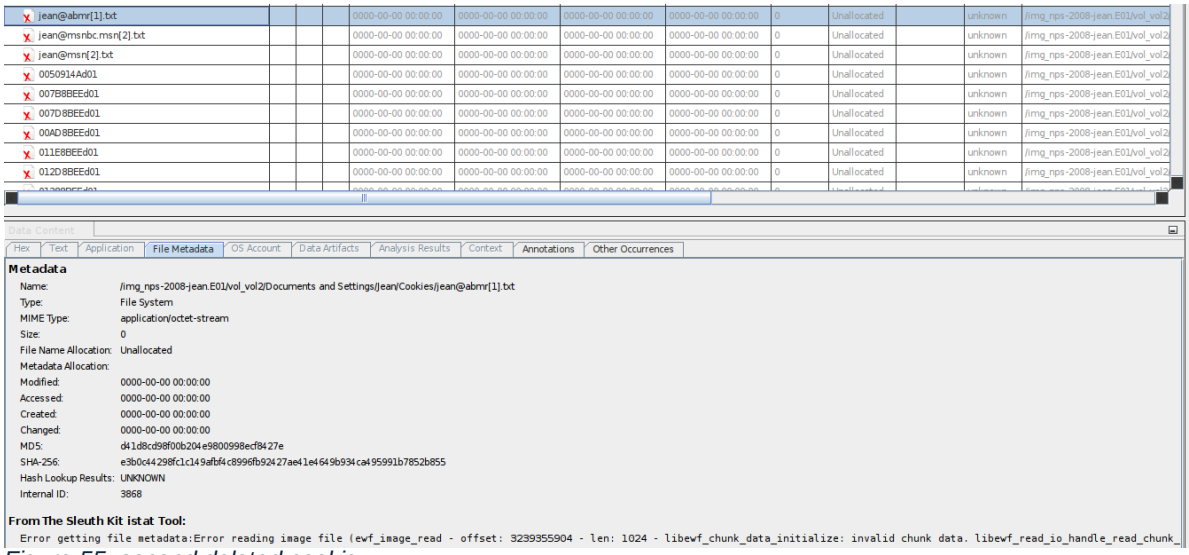


Figure 55: second deleted cookie

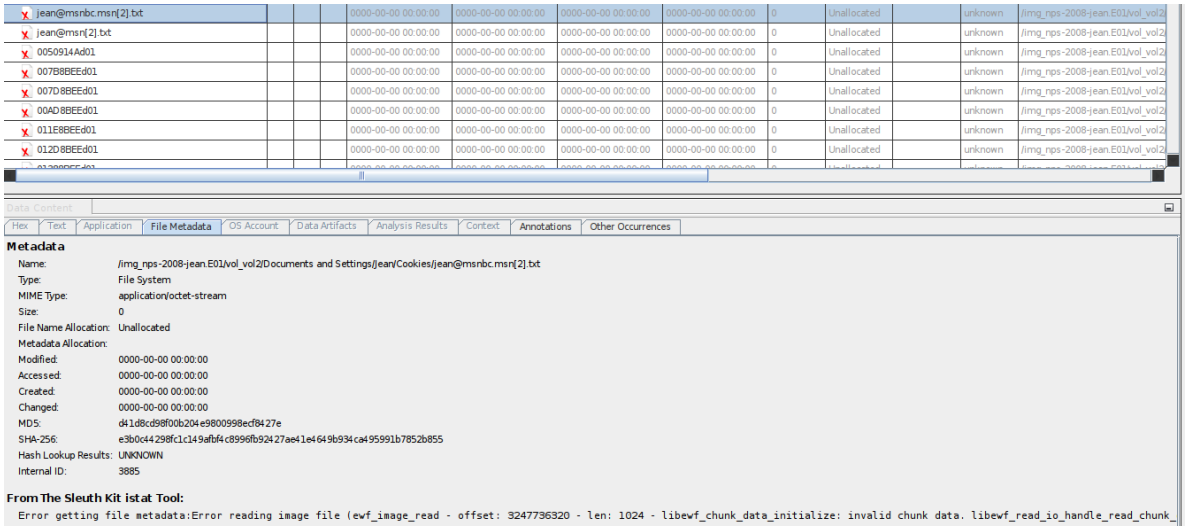


Figure 56: third deleted cookie

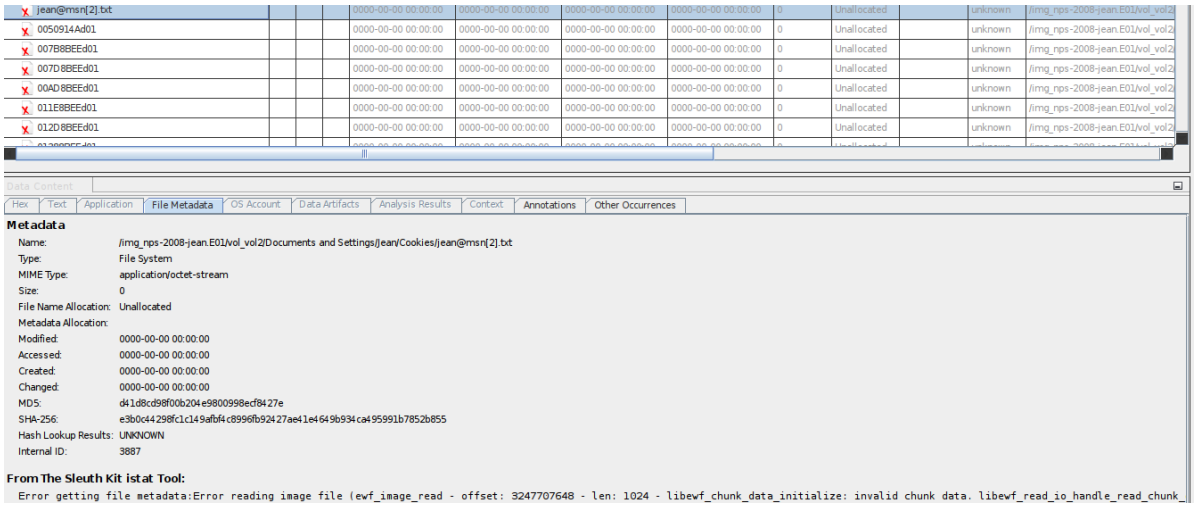


Fig 57: 4th deleted cookie

Other than that, it might be possible that Jean's cookies were compromised and that's how that attacker gained access to one of Jean's accounts from a particular vulnerable website.

NOTE: Jean's cookie directory

Figure 57: Jean's cookie directory

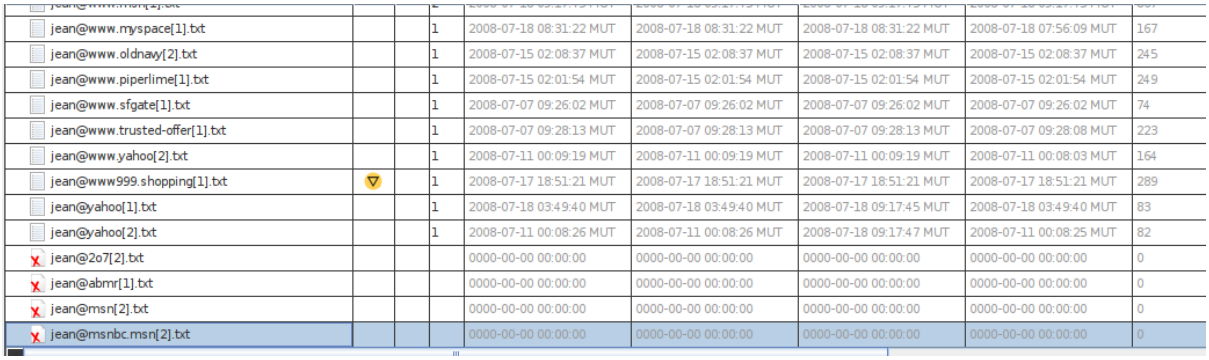


Figure 58: pic 2. a bunch of other cookies among which some are deleted

7.0 - Internet Activity

7.1 - Web Bookmarks

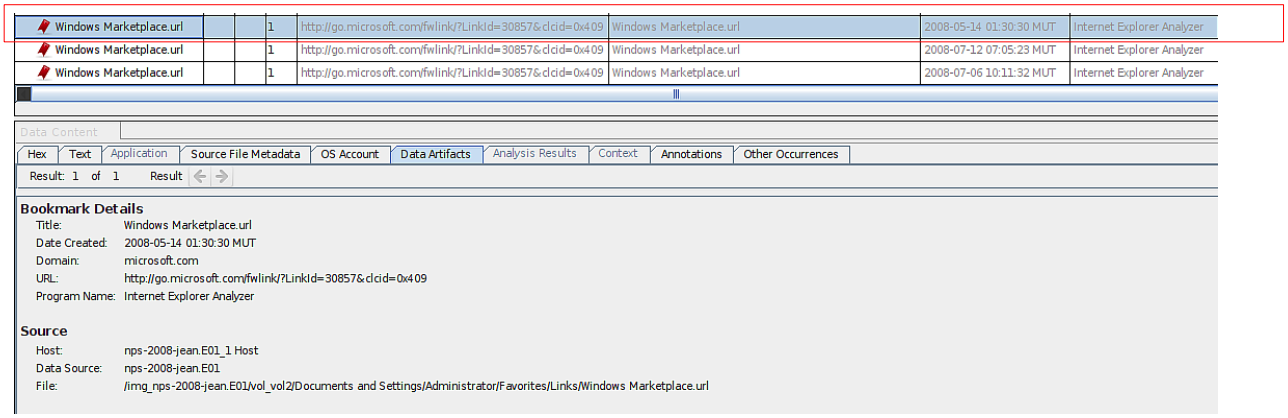


Figure 59: Windows marketplace

For the Web Bookmarks nothing suspicious other than the user bookmarked 'Windows Marketplace.url' which might suggest that she might have made plans to download a software off the website without knowing for sure if it is trusted or not.

7.2 – Web cookies

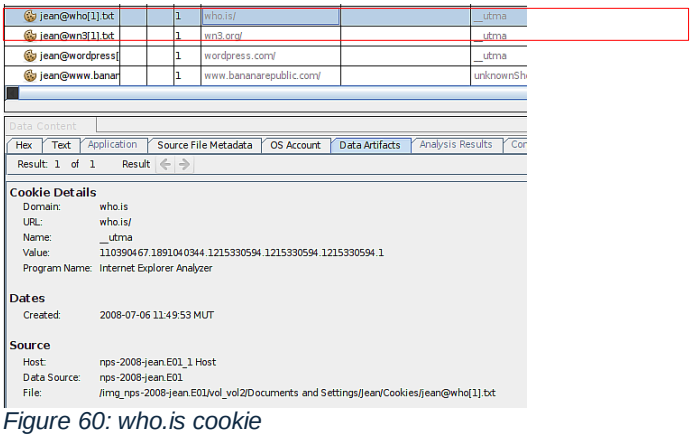


Figure 60: who.is cookie

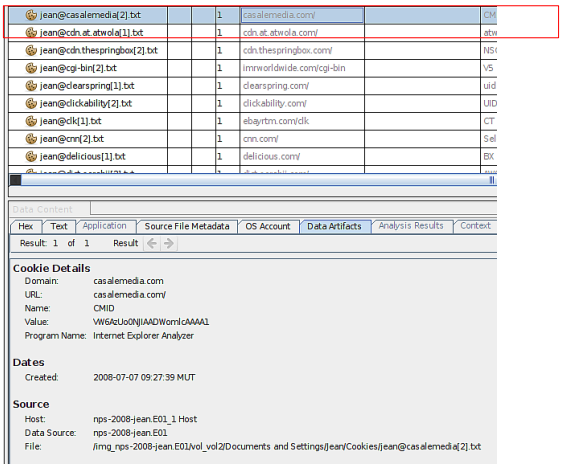


Figure 61: casalamedia cookie

For the web cookies, some tracking cookies were found. These tracking cookies can be used to monitor internet browsing habits, to provide ads based on your preferences etc... Furthermore, it can sometimes be detected as Spyware or Adware by your anti-virus.

7.3 – Web downloads

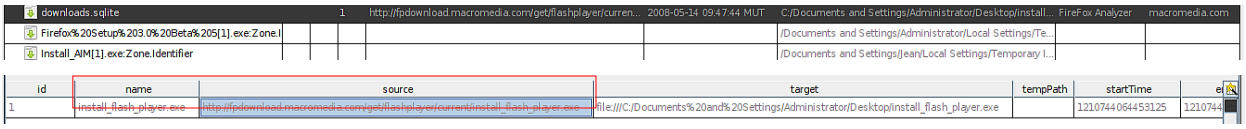


Figure 62:flash player installer

Figure 63: Firefox installer

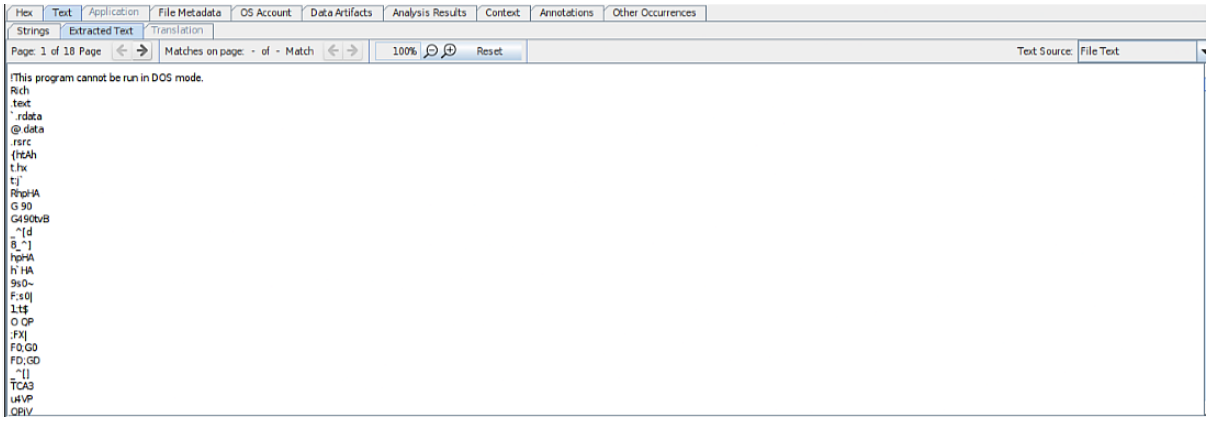
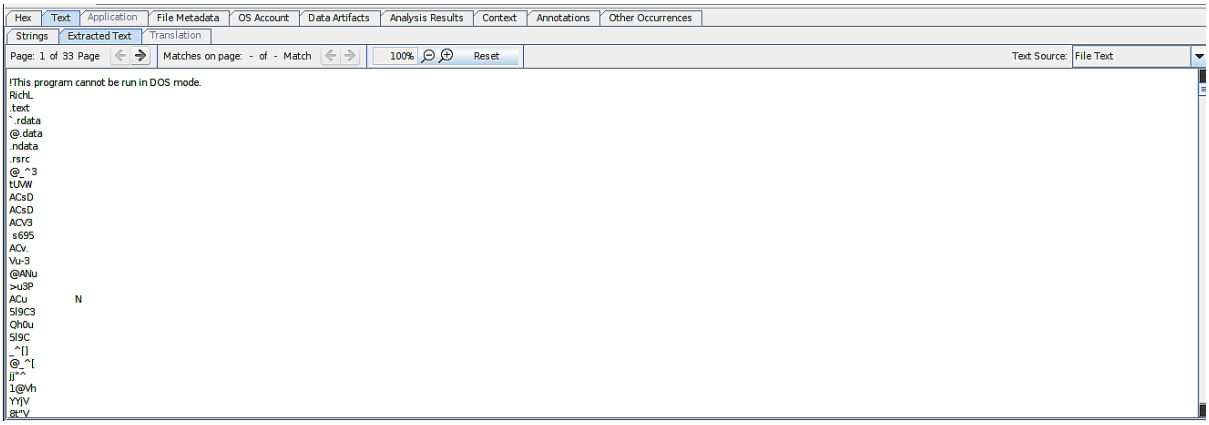


Figure 64: AIM Installer



7.4 – Web form Autofill

For the Web Form Autofill, some evidence was found that Jean might have been travelling. Since those web form autofill files were created 2 months before the leak, it was worth a check. Some information about loginId: m57Jean, displayName: m57Jean, email: jean@m57.com, brithDate_yyyy: 1980, zipCode: 19103, was found. It looked like Jean was trying to login or signup on a website. It was suspected that it was either for AIM (Aol mail) service or some hotel booking websites.

Source Name	S	C	O	Name	Value
formhistory.sqlite				searchbar-history	ix chel isis
formhistory.sqlite				q	ix chel
formhistory.sqlite				loginId	m57jean
formhistory.sqlite				displayName	m57 jean
formhistory.sqlite				email	jean@m57.com
formhistory.sqlite				birthDate_yyyy	1980
formhistory.sqlite				zipCode	19103

Figure 65: Login info

- ‘reglmgWord’ seems related to CAPTCHAs, used for human verification on websites.
- Another account possibly linked to Jean spotted: loginid: jeanm57.

formhistory.sqlite				regImgWord	PSL3CHT9	r
formhistory.sqlite				regImgWord	CPQ72WS7	r
formhistory.sqlite				loginId	jeanm57	r
formhistory.sqlite				regImgWord	KbP8ZPSV	r
formhistory.sqlite				regImgWord	4NFJTKXP	r
formhistory.sqlite				regImgWord	J8JJSKG3	r
formhistory.sqlite				searchbar-history	larry king ufo	r

Figure 66: Suspected captchas

Source Name	S	C	O	Name	Value
formhistory.sqlite				searchbar-history	larry king ufo
formhistory.sqlite				saddr	Monterey, CA
formhistory.sqlite				daddr	Crater Lake, OR
formhistory.sqlite				searchbar-history	CA lava fields
formhistory.sqlite				searchbar-history	CA lava park
formhistory.sqlite				q	hotels
formhistory.sqlite				q	lava national park, CA
formhistory.sqlite				q	mineral, ca hotels
formhistory.sqlite				chk_in	10/13/2008
formhistory.sqlite				chk_out	10/14/2008
formhistory.sqlite				searchbar-history	bailey creek cottages
formhistory.sqlite				searchbar-history	rose quartz chester
formhistory.sqlite				hs_arrival	10/13/2008
formhistory.sqlite				hs_departure	10/14/2008

Figure 67: Jean planning vacation suspected details

formhistory.sqlite				saddr	Crater Lake, OR	nps
formhistory.sqlite				daddr	Lava National Park, CA	nps
formhistory.sqlite				ddwcd	Lava National Park, CA	nps

Figure 68: confirmation of starting & destination addresses

formhistory.sqlite				searchbar-history	larry king ufo

Figure 69: Larry king UFO

7.5 - Web History

Thanks to the web history, it can now be confirmed that Jean was registering for an aim.com (Aol mail) email account. Keep in mind AIM.com is vulnerable to stored XSS attacks and it is very possible that this is how the hacker gained access to the emails being shared between Jean and Alison.

places.sqlite			1	http://www.aim.com/redirects/inclient/register.adp?distID...	2008-07-18 08:32:22 MUT	register.adp	FireFox Analyzer	aim.com	nps

Figure 70: registration on aim.com

Moreover, as the second login from the web for autofill was from a different loginid which was ‘jeanm57’ and not ‘m57jean’ it can also be confirmed that the ‘jeanm57’ loginid was for a social networking platform known as ‘weeworld’ and that the loginid ‘m57jean’ was for the Aol mail which she had to register first to gain access to

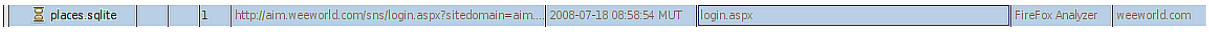


Figure 71: login on weeworld

Furthermore, it was also validated that Jean was looking for a hotel to stay in California.

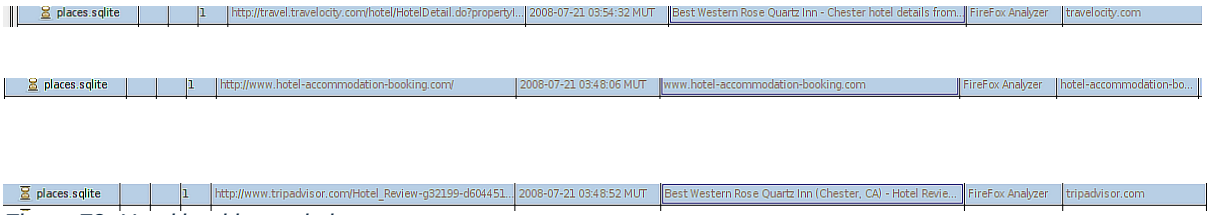


Figure 72: Hotel booking websites

7.6 – Web search

There were just other web searches about the tourist attractions such as ‘CA lava fields’ etc

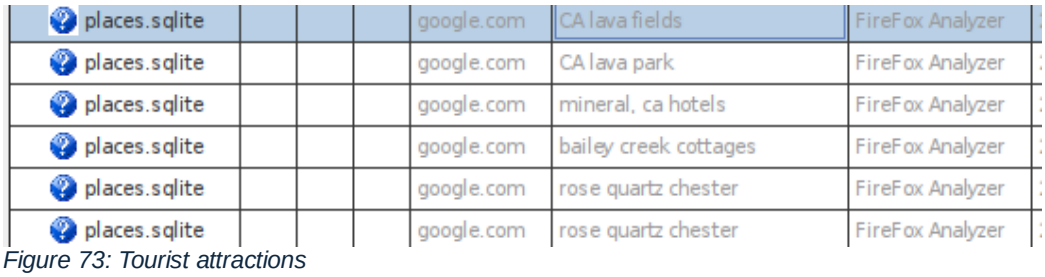


Figure 73: Tourist attractions

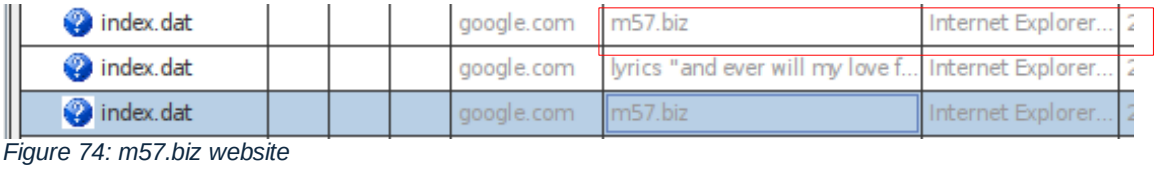


Figure 74: m57.biz website

6.0 – Conclusion

The investigation into the leak of a spreadsheet containing sensitive employee information, including salaries and Social Security Numbers (SSNs), has revealed a complex interplay of human error, technological vulnerabilities, and malicious intent. The focal point of this breach was an 'outlook.pst' file, accessed through the online platform GoldFynch.com, which provided a comprehensive view into Jean's email communications. This analysis has uncovered several critical points of failure that led to the unauthorized disclosure of private data.

Firstly, the email exchanges between Jean and other employees showcased a lack of awareness and vigilance regarding the security risks associated with email communications. Jean's indiscriminate interaction with emails, without verifying the authenticity of the senders' addresses, laid the groundwork for the breach. The confusion arising from Alison's misconfigured email address and the subsequent use of this misconfiguration by the attacker exemplifies the ease with which employees can be manipulated.

Furthermore, the attacker's clever exploitation of this confusion, by impersonating Alison through email spoofing, underscores the sophistication of phishing tactics. The use of a seemingly legitimate request for sensitive information, coupled with Jean's failure to recognize the deceptive email address, facilitated the leak. Jean's decision to send the requested spreadsheet to an email address mentioned within the spoofed sender information, rather than verifying the correct recipient, directly resulted in the exposure of confidential information.

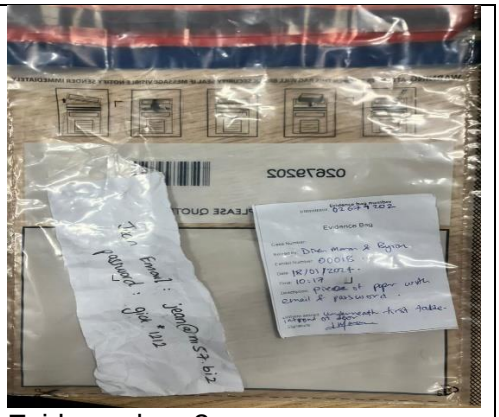
The breach was compounded by the absence of basic email security practices among the employees. The lack of adoption of email authentication measures (SPF, DKIM, DMARC) by the organization left them vulnerable to email spoofing. This oversight highlights a fundamental flaw in the company's cybersecurity framework, emphasizing the critical need for educational initiatives on digital security and the implementation of robust security measures.

In conclusion, this incident serves as a stark reminder of the multifaceted nature of cybersecurity threats. It underscores the importance of continuous vigilance, education on digital security best practices, and the adoption of comprehensive security measures to safeguard sensitive information. Organizations must prioritize cybersecurity to prevent similar incidents in the future, recognizing that human factors play a significant role in the security of digital assets. This case illustrates the dire consequences of neglecting these aspects, leading to the potential for significant financial and reputational damage.

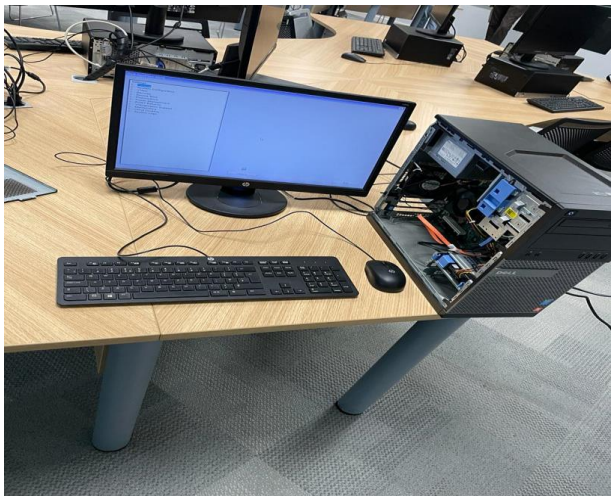
Appendix A

Evidence collected during investigation on scene

Evidence bag 1



Evidence bag 2



Main Computer hard-disk

References

Flicker, S. (2024). Demystifying Computer Components: An In-Depth Look at Hardware and Software. Ashton Falls, Virginia: TechWise Publications.

Financial Crime (2022). The Investigation Team And Their Roles: The Important Role Of Investigation Team. [online] Available at: https://financialcrimeacademy.org/the-investigation-team-and-their-roles/ .

ISO (2021a). ISO/IEC 27041:2015. [online] ISO. Available at: https://www.iso.org/standard/44405.html [Accessed 24th march 2024].

ISO (2021b). ISO/IEC 27042:2015. [online] ISO. Available at: https://www.iso.org/standard/44406.html [Accessed 24th march 2024].

ISO - International Organization for Standardization (2018). ISO/IEC 27037:2012. [online] ISO. Available at: https://www.iso.org/standard/44381.html [Accessed 3rd april 2024].

Kovacs, E. (2012) *AOL.com and Ask.com vulnerable to XSS attacks*, *softpedia*. Available at: https://news.softpedia.com/news/AOL-com-and-Ask-com-Vulnerable-to-XSS-Attacks-255047.shtml (Accessed: 07 April 2024).

Hope, C. (2018) *What is the windows desktop.ini file and can I delete it?*, *Computer Hope*. Available at: https://www.computerhope.com/issues/ch001060.htm (Accessed: 03 April 2024).

La Trobe (2017). Health and Safety Procedure - Incident Investigation / Document / La Trobe Policy Library. [online] policies.latrobe.edu.au. Available at: https://policies.latrobe.edu.au/document/view.php?id=320 [Accessed 6th Apr. 2024].

Mayer, J. (2023). Digital Evidence: The Forensic Science Regulator's Code and ISO 17025. [online] Sytech Consultants. Available at: https://sytech-consultants.com/enhancing-trust-in-digital-evidence-the-role-of-forensic-science-regulators-code-and-iso-17025/#:~:text=For%20digital%20forensics%2C%20the%20Regulator [Accessed 7 Apr. 2024].

National Institute of Justice (2012). DNA Evidence: Basics of Identifying, Gathering and Transporting. [online] National Institute of Justice. Available at: https://nij.ojp.gov/topics/articles/dna-evidence-basics-identifying-gathering-and-transporting.

Norwich (2024). 5 Steps for Conducting Computer Forensics Investigations | Norwich University - Online. [online] online.norwich.edu. Available at: https://online.norwich.edu/online/about/resource-library/5-steps-conducting-computer-forensics-investigations#:~:text=Prior%20to%20any%20digital%20investigation [Accessed 5 Apr. 2024].

Shinder, L. and Cross, M. (2008). Search Warrant - an overview | ScienceDirect Topics. [online] www.sciencedirect.com. Available at: https://www.sciencedirect.com/topics/computer-science/search-warrant .

Subrosa (2023). Unveiling the 9 Crucial Phases of Digital Forensics in Cybersecurity: A Comprehensive Guide | SubRosa. [online] www.subrosacyber.com. Available at: https://www.subrosacyber.com/blog/9-phases-of-digital-forensics#:~:text=The%20preparation%20phase%20includes%20preparing [Accessed 1st Apr. 2024].

SWGDE (2024). SWGDE. [online] www.swgde.org. Available at: https://www.swgde.org [Accessed 2nd April 2024].

UNODC (2012). Cybercrime Module 4 Key Issues: Standards and best practices for digital forensics. [online] : Available at: https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html [Accessed 2nd April 2024].