Computer Forensic Examination Report

Ahmad Shekib Nawabi

MCSOL, University of San Diego

CSOL-590-04-FA21: Cyber Incident Response/Forensics

Professor Ron Fulton

12/13/2021

Investigator	**Alison Smith**
	CEO
	M57.biz

Digital Forensics Examiner	**Ahmad Shekib Nawabi**
	Master of Cyber Security Operation and Leadership, Student
	University of San Diego

Subject:	Digital Forensic Examination Report

Offence:	Exfiltration of Confidential Document

Accused:	Jean Jones

Date of Conclusion:	12/13/2021

Contents Page

Background to the case

It's essential to understand what M57.biz is before moving to the case information. *M57.biz is a hip web start-up developing a body art catalog.* They started with seed funding of $3 million, and now they are closing at a $10 million round. M57.biz was founded and is owned by two co-owners. In addition, this web start-up has hired ten employees in their first year. Current staff includes Smith, Alison (CEO), Jones, Jean (CFO), three programmers, 2 Marketing, and 1 BizDev. Employees of M57.biz mostly communicate through emails, as programmers work out of their homes with only one in-person meeting weekly, and Marketing & BizDev are mainly working on the go and have in-person meetings only once every two weeks. (M57-Jean.ppt, n.d.)

The case information: Jones, Jeans, the company's Chief Financial Officer (CFO), is accused of exfiltrating company confidential information. An excel document named "M57plan.xlsx" was found posted as an attachment on the technical forum of a competitor's website. This document reveals the names, positions, salaries, and SSNs of M57.biz.

This document comprehensively analyzes a forensic image taken from Jean's computer by a third-party forensic first responder. Based on my expert opinion, M57.biz conducted most business communications through the use of emails, so there must be great details hidden in the emails exchanged.

Questions asked relevant to the case

A thorough investigation by third-party forensics experts revealed crucial information about the case; Jean claims Alison asked her to create this spreadsheet and send to her by email. On the other hand, Alison claims she never asked Jeans to develop such a document and never received such information.

Table 1

1	When did Jeans create this document?
2	How did it get from her computer to the competitor's website?
3	Who else from the company is involved?

Search and seizure of evidence

The incident first responders obtained a search warrant to seize evidence lawfully and legally from M57.biz; Jean's computer device was charged and imaged later in the lab of a non-associating third party. Chain of Custody was maintained to ensure the integrity of data and evidence. The first responder's name and the time and date of the seizure were logged. In addition, good pictures were taken of the evidence and crime scene.

1. Exhibits submitted for analysis

   jeanm57.E01 (EnCase format)

   "*The E01 (Encase Image File Format) file keeps a backup of various types of acquired digital evidence, including disk imaging, storing logical files, etc. When an investigator (or a Forensic Expert) uses Encase to create a backup of data available on the hard disk, a physical bit stream of the data is produced. This procedure is known as Disk Imaging. The basic theory behind the relation between the Encase and*

E01 image file format is that, while creating images of the data available on the hard disk, encase divides the complete data into 640 MB of data chunks. Due to this data division at the pause of 640 MB, multiple data files storing crucial hard disk information are created. The most peculiar feature of these files is that the name of the files remains the same (as named by the user), whereas the file extension changes. For example, if the very first chunk of 640 MB is created with the name "S01.E01", the following 640 MB chunks will be named "S01.E02", followed by "S01.E03", "S01.E04", "S01.E05" and so on.

Note: - Even though the file extension gets changed after crossing a limit of 640 MB (i.e., E01, E02, E03, E04, and so on), the file's internal structure remains intact.

Structure of E01 File: -

The e01 image file format is prefixed with a "Case Info" header, After every block of 64 sectors, i.e., 32 KB. It is interlaced with CRCs (Cyclic Redundancy Checks). The footer of the E01 file contains an MD5 hash value of the entire imaged data." (Forensicsoftware.com, n.d.)

2. Further Questions Being Asked Relevant to the Case

   - **Who else had physical access to Jean's computer?**

List of Criminal Offences

Table 2

1	Unlawful exfiltration of confidential information.
2	Violation of company contract with M57.biz

Evidence to Search for

Table 3

1	M57plan.xlsx on Jean's computer and its creation date.
2	The medium used to exfiltrate documents and time analysis.
3	Who else from the company is involved

Data of Evidentiary Value to the Case

After closely analyzing the email communication between Alison and Jean, the evidence listed below will add significant value to the case. I have used Autopsy 4.19.2 to study the forensic image and retrieve email interaction.

Figure 1&2 below are evident that Jean had received an email from Alison asking for the information that was later exfiltrated

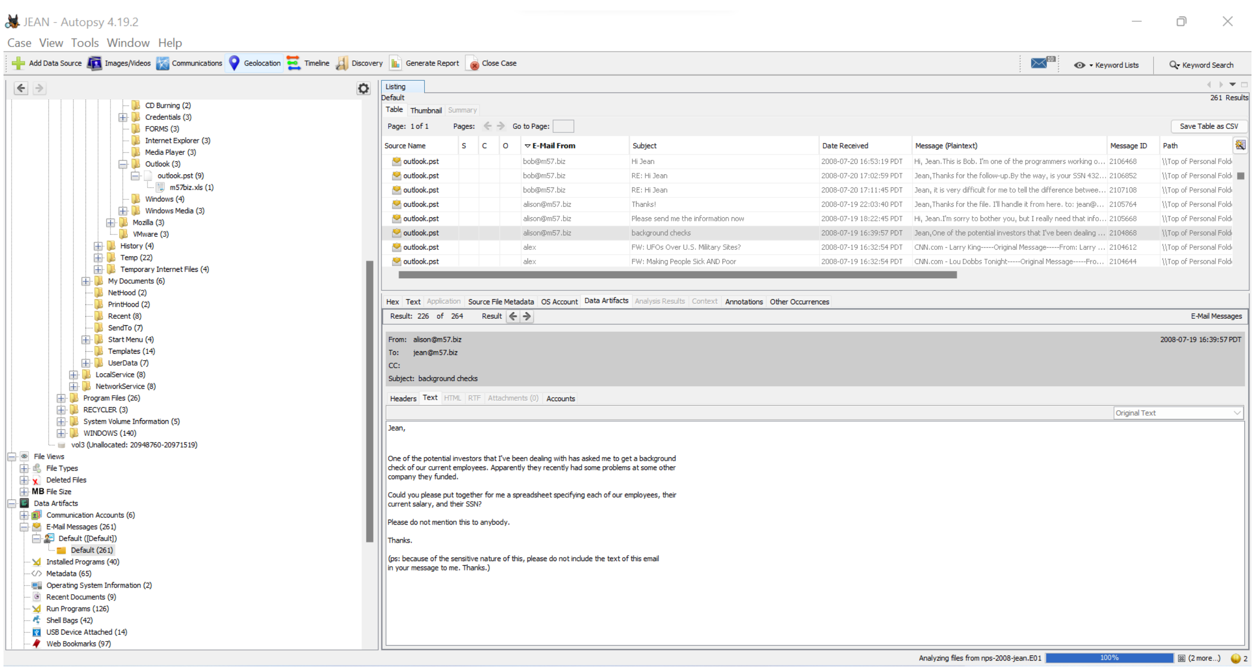

Figure 1

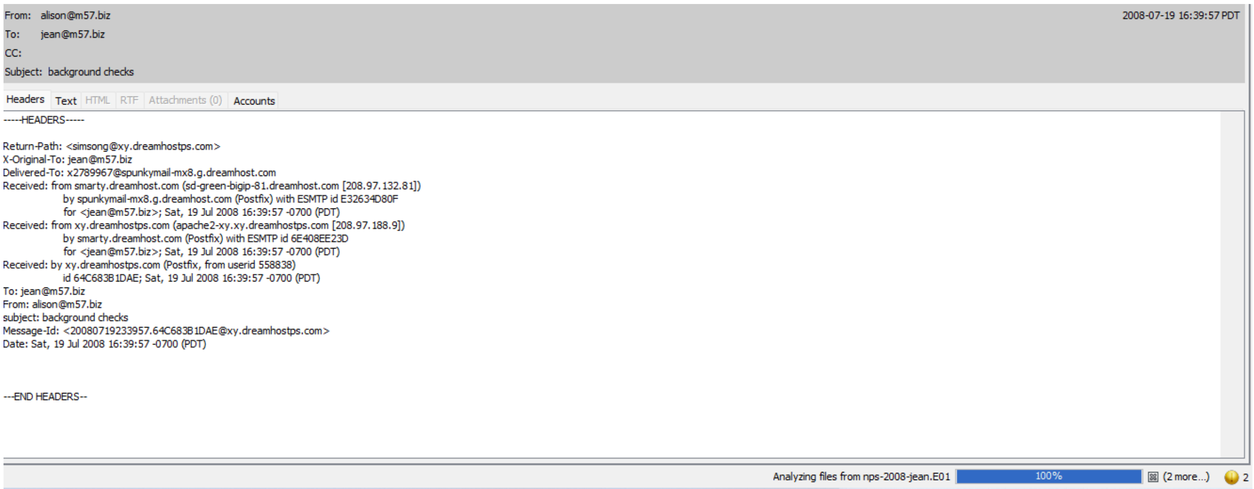

Figure 2

Figure 3 illustrates that Jean created the excel sheet stored on her user desktop.

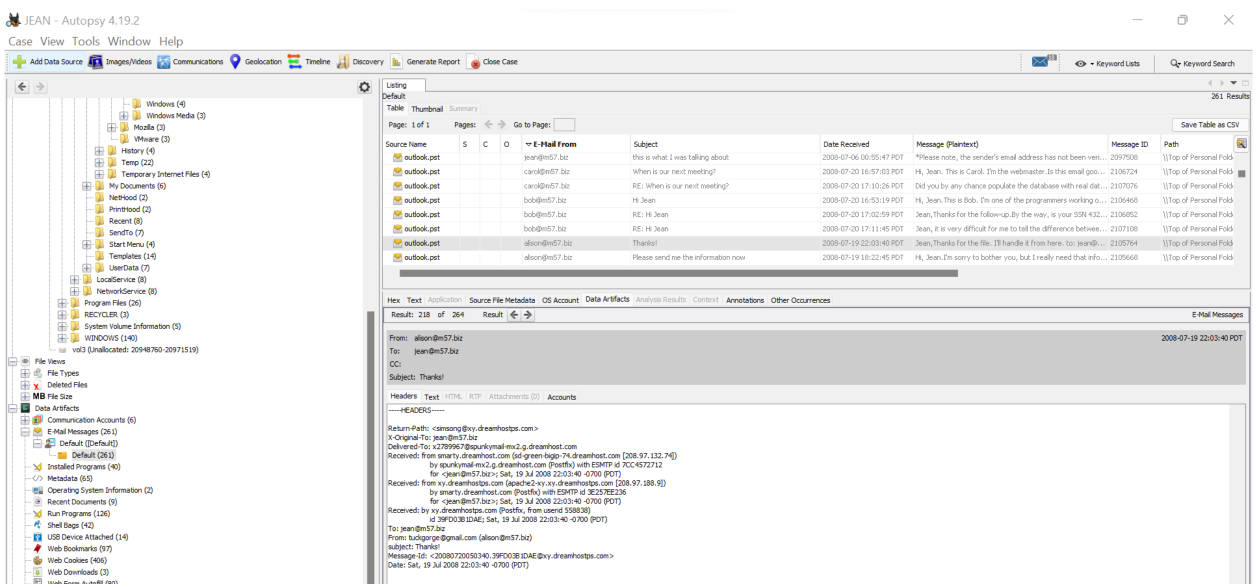

Figure 3

And finally, as illustrated in figure 4, Jean sends the document in reply to an email coming from Alison.

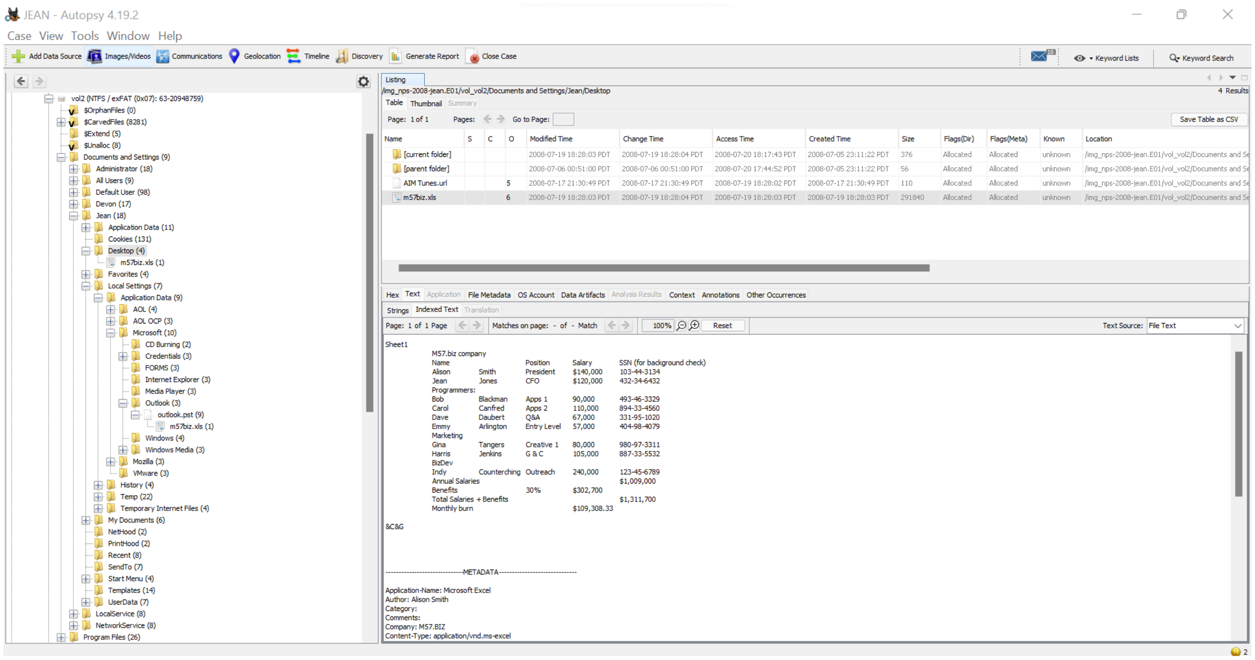

Figure 2

Examination Details

"*An E.01 format image file contains a variety of "meta data" inside the image file, in addition to the original data captured from the original evidence disk. Data captured within an E.01 is broken into "blocks" that are typically 64 sectors (default) in size. A CRC is calculated for each "block" of data and individual CRC values are stored with each block throughout the. E01 image. An overall MD5 and SHA1 are also captured for the entire original data (without any EnCase metadata, just the same as an RBS image) and stored within the E.01 image for future verification.*

Forensic Toolkit verifies an. An E01 image file does two things: Re-calculates a CRC for each block of data in the. E01 and compares the calculated CRC with the CRC stored in the. E01 for each block. Re-calculates an overall MD5/SHA1 for all the data within the. E01 (excluding *any metadata or additional info not part of the original disk) compares the overall value calculated with the general hash stored inside the. E01 image file. Any mismatch of ANY individual CRCs or the overall MD5/SHA1 will result in a verification failure."* (uri.edu, 2011)

In Figure 5, shown below, Forensics Toolkit's verify drive/image option is used to verify the image's hash values, ensuring the data has not been tampered with since acquisition.

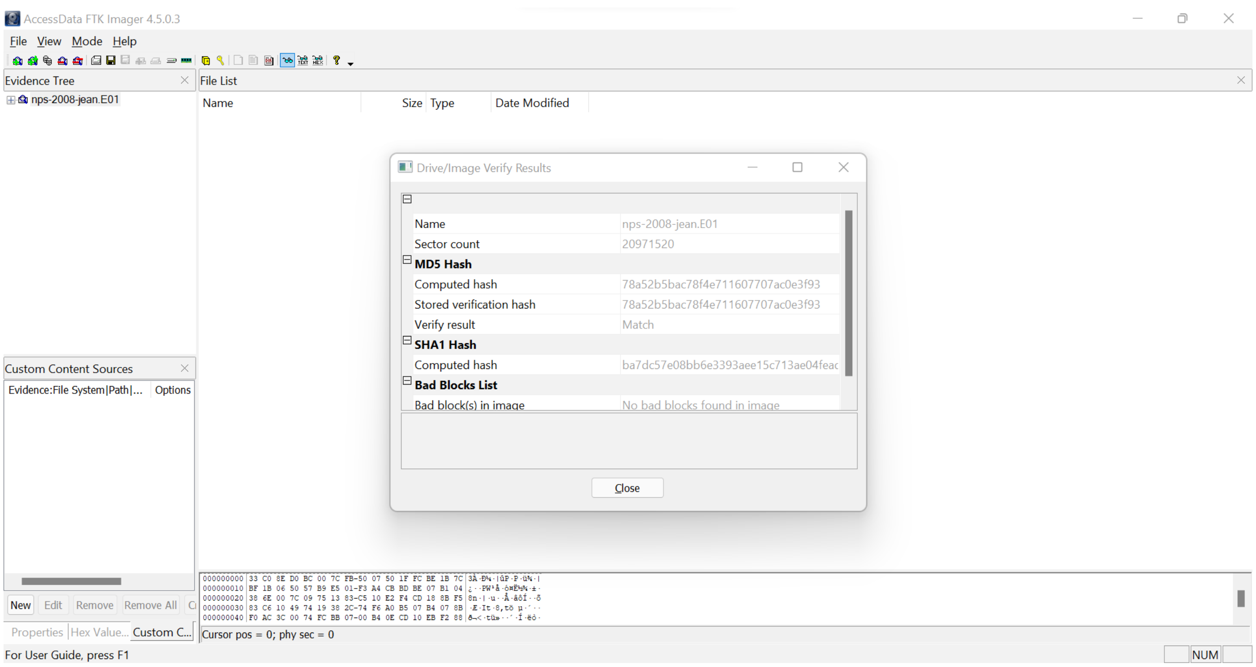

Figure 3

Timeline Analysis

Timeline analysis is helpful for various investigation types. It is often used to answer questions about when a computer is used or what events occurred before or after a given event. Autopsy contains an advanced timeline interface that was built with funding from DHS S&T. It pulls timestamp info from the following places:

. Files

. Web artifacts

. Other Autopsy extracted data, such as EXIF and GPS" (sleuthkit.org, n.d.)

Figure 6 below is the image of a timeline established using Autopsy, which shows when M57plan.xlsx was created along with other details, like location, MD5 hash, SHA-256 hash, etc.

Also, visible in figure 6, we know Jean created the document, and the file is on the Desktop of Jean's computer.

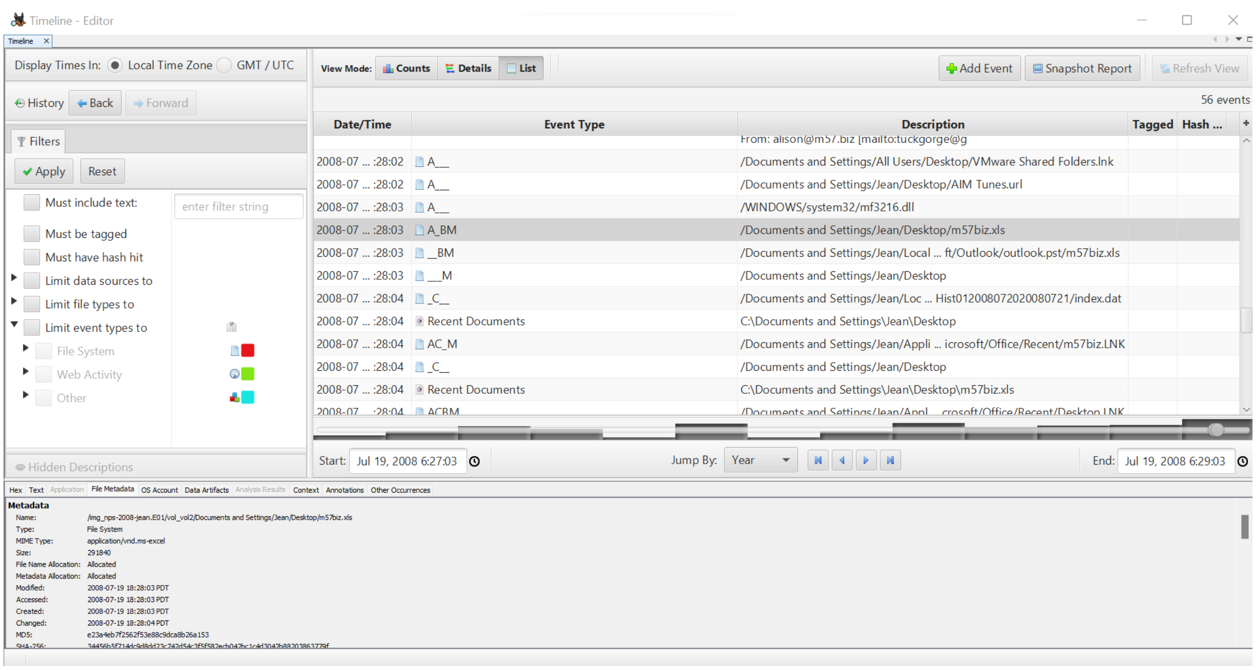

Figure 4

Below in figure 7 is the screenshot of the first email from Alison to Jean, shown using Autopsy, followed by a figure 8 screenshot of when a reply by Jean is sent to the email.

Using this information, it's visible by the return path that a hacker successfully spoofed to Alison.

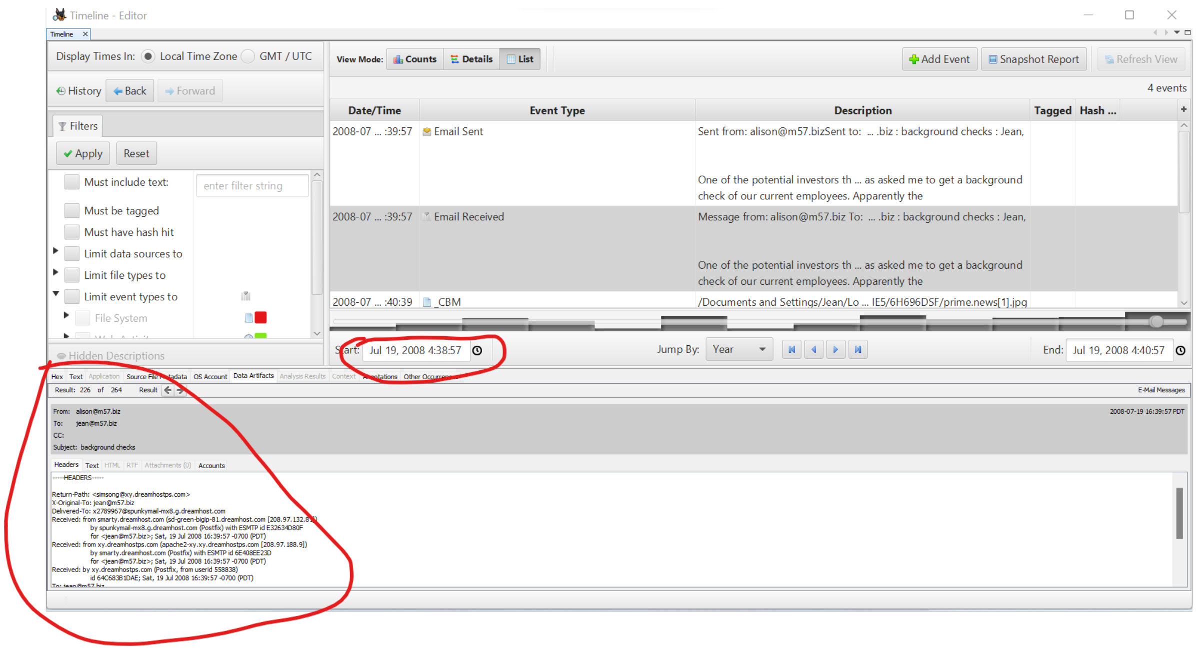

Figure 5

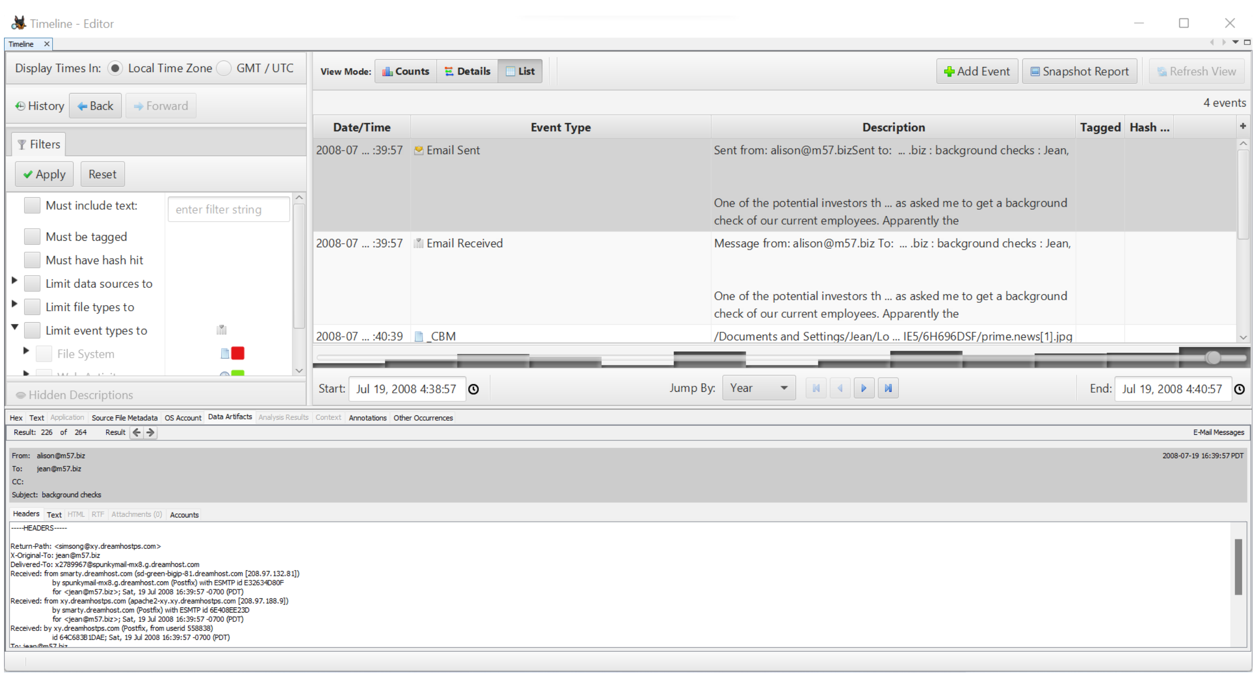

Figure 6

Findings and Recommendation

Based on the analysis of Jean's computer forensic image, it's visible that Jean is not guilty of exfiltrating the M57plan.biz and posting it on a technical forum of the competitor's website. This document was created by Jean using her computer, but as seen in the results of the forensic image analysis, the intention to compromise company data wasn't there. Findings also suggest that Alison was phished through email by clicking a phishing link in an email sent to her, resulting in her email account and credentials being stolen. The hacker then sends Jean an email requesting confidential company information by changing the return path of the email to simsong@xy.dreamhostps.com; Jean fails to check the return path of the email and falls into the trap as well. There are many other possibilities of how the hack occurred, but based on the data provided, it seems that no one else from the company was involved in the exfiltration of the document.

Going on forward, my recommendations for M57.biz would be:

1. **Better Password Policies:**

The National Institute of Standards and Technology (NIST) offers Digital Identity Guidelines for a sound password policy, including the following recommendations:

Password complexity and length

Many organizations require passwords to include a variety of symbols, such as at least one number, both uppercase and lowercase letters, and one or more special characters. However, the benefit of these rules is not nearly as significant as expected, making passwords much more complex for users to remember and type.

Password length, however, is a primary factor in password strength. Accordingly, NIST recommends encouraging users to choose long passwords or passphrases of up to 64 characters (including spaces).

Password age

Previous NIST guidelines recommended forcing users to change passwords every 90 days (180 days for passphrases). However, changing passwords too often irritates users and usually makes them reuse old passwords or use simple patterns, which hurts your information security posture. While strategies to prevent password reuse can be implemented, users will still find creative ways around them.

Therefore, the current NIST recommendation on maximum password age is to ask employees to create a new password only in the case of a potential threat or suspected unauthorized access.

2. **End-user training**

"In addition, be sure to educate your users about the following:

. *Remembering your password without writing it down somewhere is vital, so choose a strong password or passphrase that you will easily remember. If you have a lot of different passwords, you can use password management tools, but you must choose a strong master key and remember it.*

. *Be aware of how passwords are sent across the Internet. URLs (web addresses) that begin with "https://" rather than "http://" are more likely to be secure for the use of your password.*

. *If you suspect someone else may know your password, change it immediately.*

. *Don't type your password while anyone is watching.*

. *Avoid using the same password for multiple websites containing sensitive information.*

Providing adequate user training on cybersecurity best practices is vital to any organization in the modern world." (netwrix.com, n.d.)

3. Virtual Private Networks ensure user interaction with the leading site remains secret through encryption tunnels. Using a VPN is recommended for M57.biz to ensure malicious activities do not intercept their interactions through different channels.

Conclusion

The analysis of the forensic evidence has suggested that neither Jean nor Alison has deliberately exfiltrated confidential information of M57.biz. A study of the evidence also has concluded that they have been negligent in using industry-compliant practices to prevent the hacker from gaining access to their system or credentials. Implementing cyber security in the foundation of a company's IT structure is a must. It has been proven crucial as we move on to digitalization.

References

Uri.edu. (2011, October 21). Image Verification. Retrieved from

http://students.cs.uri.edu/~forensics/courses/CSC485/Week8/ImageVerification.pdf

Forensicsoftware.com. (n.d.). E01 (Encase Image File Format). Retrieved from

https://www.forensicsware.com/blog/e01-file-format.html

Sleuthkit.org. (n.d.). Autopsy. Retrieved from

https://www.sleuthkit.org/autopsy/desc.php

netwrix.com. (n.d.). Password Policy Best Practices for Strong Security in AD. Retrieved from

https://www.netwrix.com/password_best_practice.html