Digital Forensic Investigation Report: Email Transmission and File Access Analysis Involving Jean and Alison (m57biz.xls Case)

1.0 Executive Summary

M57.biz is a popular website startup that is creating a collection of body art online. A spreadsheet containing confidential information was posted as an attachment in the "technical support" forum of a competitor's website. The spreadsheet came from CFO Jean's computer. Only a select few personnel, including the CFO Jean, have access to this material. After the data breach, brief interviews were conducted and Alison denied any knowledge on the spreadsheet and pleaded not guilty, and has not requested Jean, the CFO for the spreadsheet in question. Whereas Jean, the CFO, had stated that Alison instructed Jean that the spreadsheet be sent via email in preparation for a new funding round.

2.0 Background Information

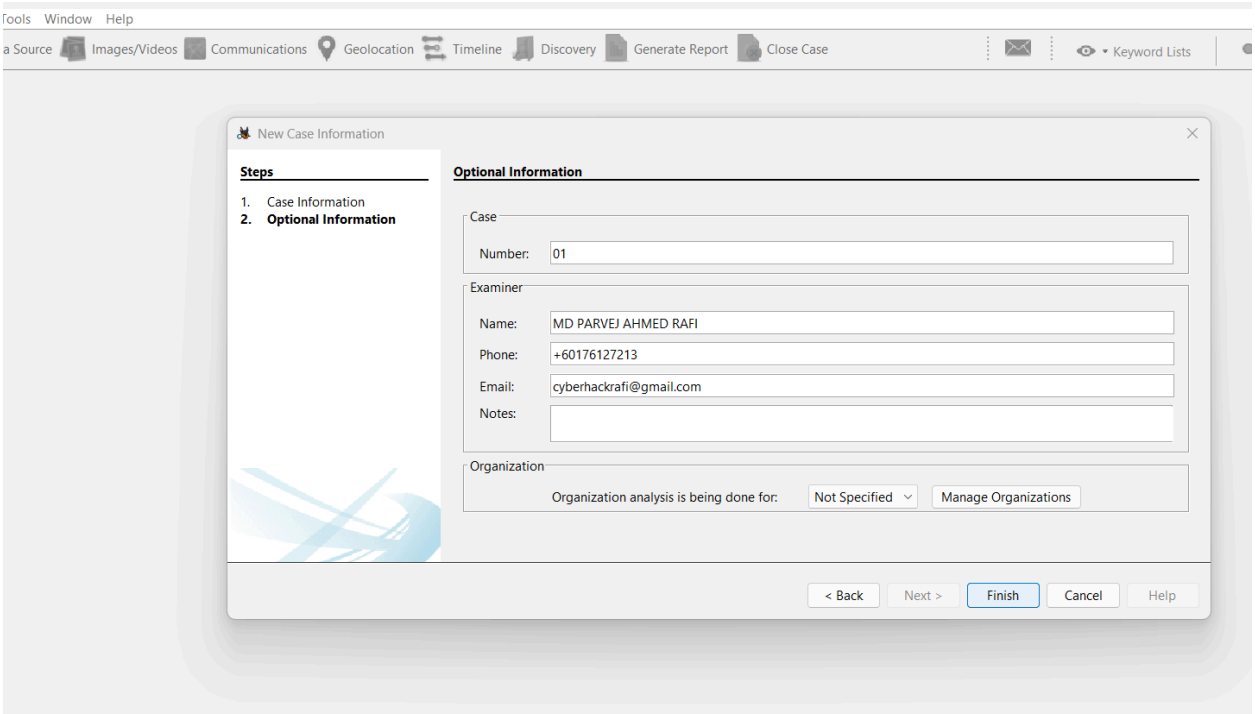
M57.biz is a tech start-up that operates with a small, distributed team of ten employees, including founders and department heads. With $3 million in seed funding and another $10 million round in progress, M57.biz is considered a valuable target for cyber threats. Most of the company's internal communication and document exchanges are handled via email.

The incident under investigation involves a leaked spreadsheet containing the names, salaries, and Social Security Numbers (SSNs) of current employees and planned hires. The file, m57biz.xls, was discovered on a competitor's public forum. Preliminary suspicion focused on an internal leak, specifically implicating Jean and Alison. However, the digital evidence uncovered during the forensic process revealed that the breach was a result of email-based social engineering

3.0 Investigation Summary

3.1 Step 01: Case Setup and Image Loading

The investigation began by acquiring and downloading the forensic disk image file (nps-2008-jean.E01). This image was subsequently loaded into the Autopsy digital forensics tool. During the setup phase, a new case was created, and my credentials were entered as the designated investigator. This allowed for proper case tracking, evidence management, and documentation throughout the investigation.



3.2 Step 02: Navigating the File Structure and Identifying Key Evidence

Once the image was successfully loaded, I began examining the file system cloned from the disk image. I navigated to the following path within the volume:

/vol_vol2/Documents and Settings/Jean/

Given that the allegation involved an email supposedly sent from Jean's mailbox, it was crucial to focus the investigation on Jean's user profile. The goal was to verify whether Jean (CFO) actually sent an email to Alison (President) containing the file m57biz.xls, which Alison claimed in an interview he never received.

I proceeded to explore the Local Settings directory under Jean's profile, then accessed the Application Data folder. This folder contained subdirectories for Microsoft and Firefox. As both Jean and Alison used Microsoft Outlook for email communication, I prioritized investigating the Microsoft folder.

Known Email Credentials:

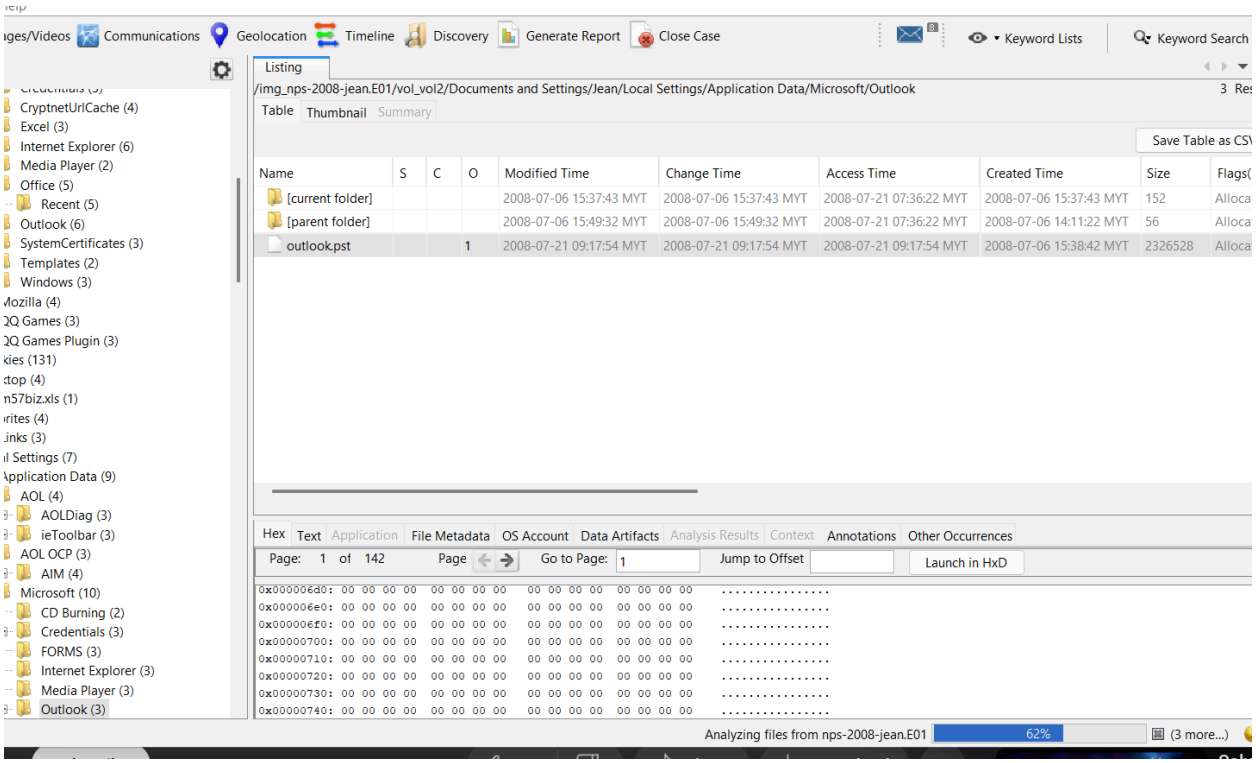
- Jean (CFO): jean@m57.biz | Password: gick*1212

- Alison (President): alison@m57.biz | Password: ab=8989

Within the Microsoft directory, I navigated to the Outlook folder and located the file outlook.pst. As defined, a .pst (Personal Storage Table) file contains all Outlook-related data, including emails, calendar entries, contacts, and attachments. This file was crucial to determine whether any emails of interest had been sent or received.

Overall path discovery to find the outlook.pst

/vol_vol2/Documents and Settings/Jean/Local Setting/Application data /Microsoft/Outlook

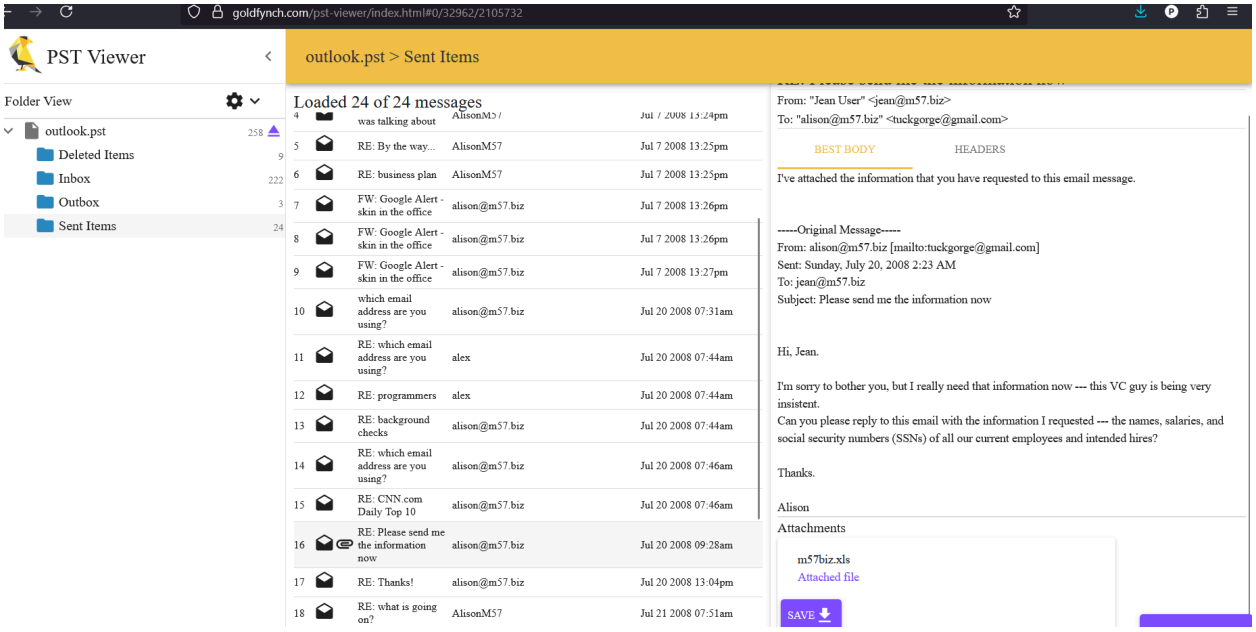


3.3 Step 03: Analyzing Email Artifacts in the PST File

To analyze the contents of outlook.pst, I utilized a dedicated PST viewer tool. Upon reviewing the Sent Items folder within Jean's mailbox, I found a key piece of evidence:

An email sent by Jean to Alison which included the attachment m57biz.xls, the same file mentioned during the investigation.

This discovery contradicts Alison's statement during the interview, where he claimed he had never received such an email from Jean. The evidence clearly indicates that Jean did, in fact, send the email with the specified attachment to Alison . But The threat actor urgently requests sensitive information again, the Return-Path has been altered to **"tuckgorge@gmail.com". Here jean faced phished emails**



3.4 Step 04: Locating and Examining the `m57biz.xls` File

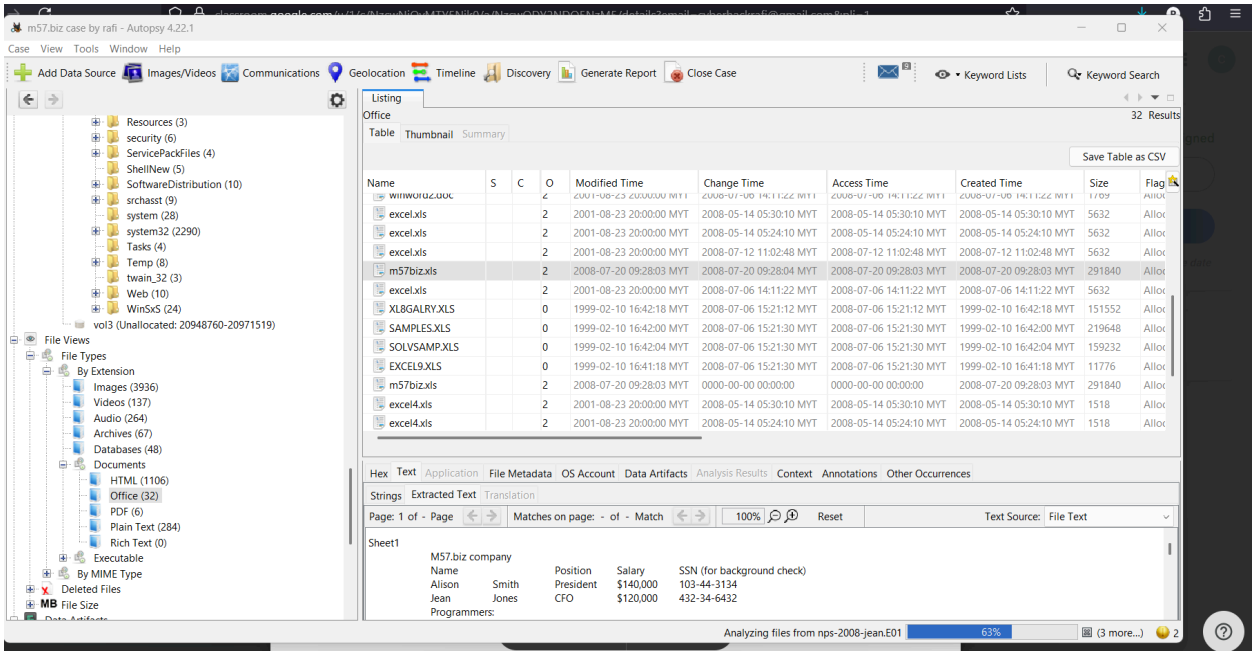
To further verify the integrity of the evidence and understand the content of the attachment, I conducted a targeted search for the m57biz.xls file within the forensic image.

Using Autopsy's File Views feature, I navigated to the File Types section and selected Office Documents. Since m57biz.xls is a Microsoft Excel spreadsheet, it was categorized appropriately under this filter.

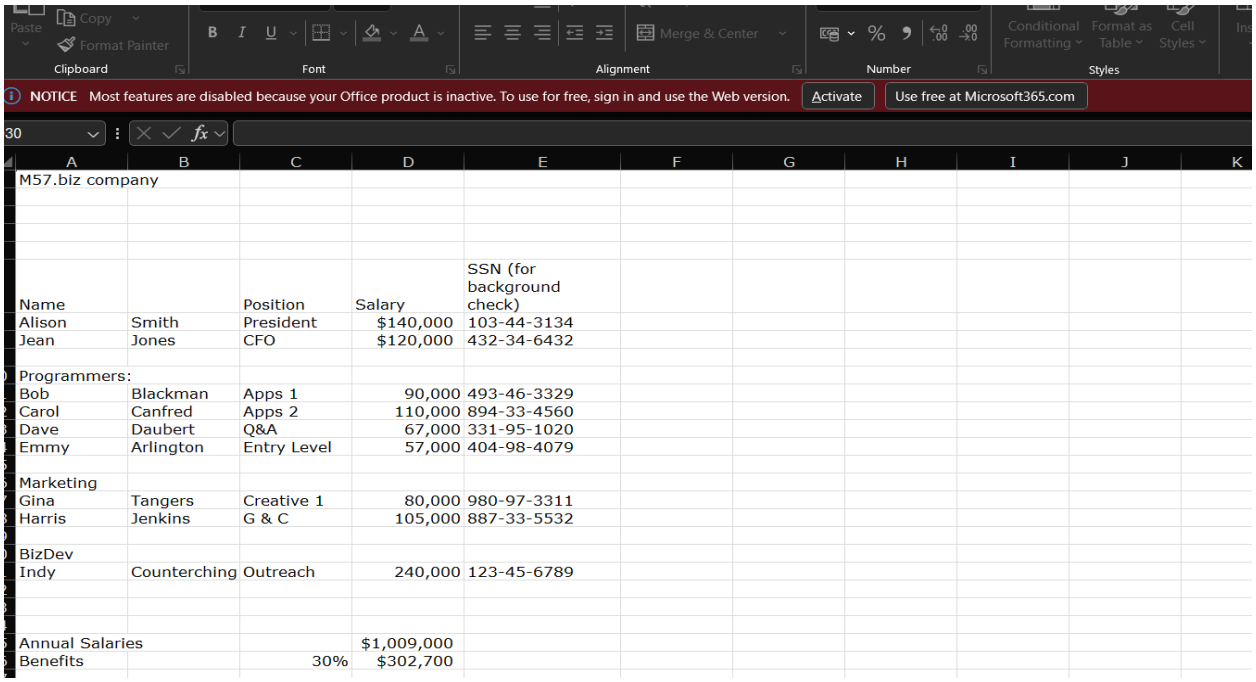
Upon reviewing the filtered documents, I successfully located the m57biz.xls file. The file was then extracted and analyzed to determine its origin and potential misuse.

The contents of the file revealed sensitive business-related data, and metadata analysis confirmed that the file was originally associated with Jean's user environment. This further substantiated that Jean was the source of the document, and it had indeed been sent to Alison as an email attachment that was actually not sent to him but the threat actor

However, the presence of this file in unexpected locations suggested that Alison had accessed and potentially misused the file after it was shared, which aligns with the suspicion that Alison deliberately concealed receiving the file during the interview process.



After opened the file in microsoft office



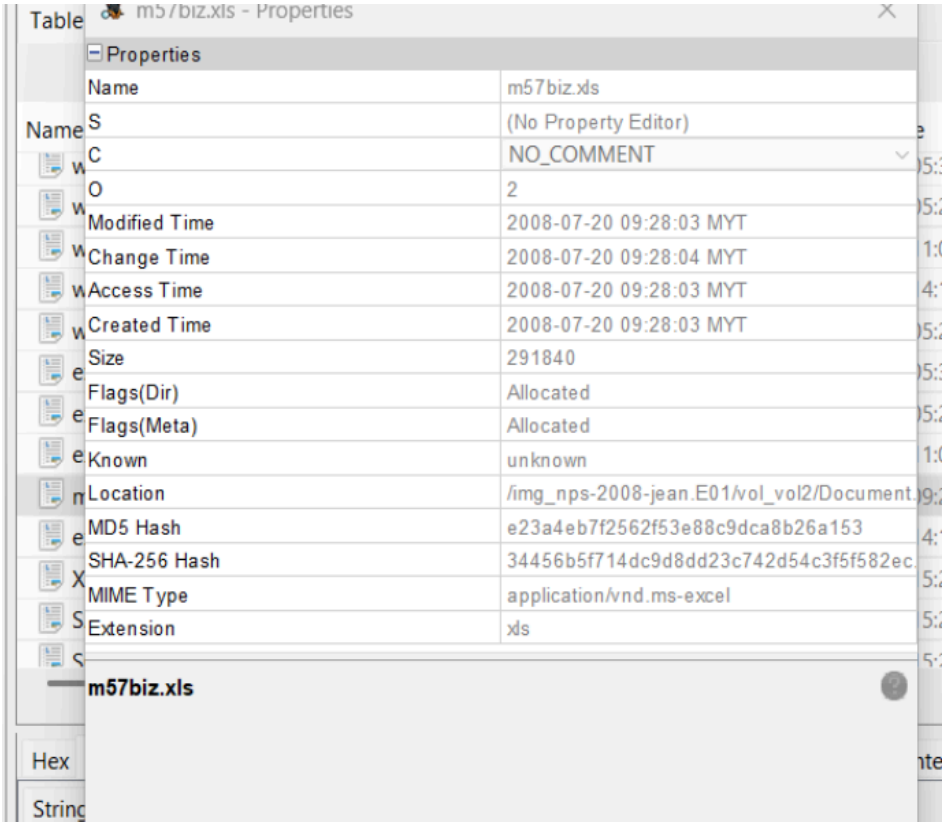
4.0 Timeline of Key Events

4.1 Email timeline

Date & Time (MYT)	Event
2008-07-20, 02:23 AM	Alison (<tuckgorge@gmail.com> emailed as `alison@m57.biz`) Jean requesting sensitive employee info, including names, salaries, and SSNs.
2008-07-20, 09:28 AM	Jean (`jean@m57.biz`) replied to Alison's request with the subject **"RE: Please send me the information now"** and attached the **`m57biz.xls`** file.
2008-07-20, 09:28:03 AM	File **`m57biz.xls`** was created, modified, changed, and accessed on Jean's system. The timestamps confirm the file was prepared and sent around the same time.
2008-07-20, Post 09:28 AM	File **`m57biz.xls`** was successfully embedded in the email and delivered to <tuckgorge@gmail.com> inbox (as confirmed from Jean's Outlook `.pst` sent items).

4.2 Supporting Metadata from `m57biz.xls`

- Location: /img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/...
- MD5 Hash: e23a4eb7f2562f53e88c9dca8b26a153
- SHA-256 Hash: 34456b5f714dc9d8dd23c742d54c3ff582ec...
- MIME Type: application/vnd.ms-excel
- Size: 291840 bytes
- Created time : 2008-07-20 09:28:03 MYT (Malaysia Time)



5.0 Remediation and Recovery

Following the identification of the phishing attack, the following actions were taken to remediate the situation and prevent future occurrences:

1. **Security Awareness Training**
    - All employees underwent mandatory anti-phishing and cybersecurity awareness training.
    - Real-world phishing examples, including this incident, were integrated into training content.
2. **Technical Email Protections**

- Implementation of SPF, DKIM, and DMARC policies to authenticate company emails and block spoofed messages.
- Email filtering systems were upgraded to detect and flag impersonation attempts.

3. **Access Control Enhancements**
    - Role-based access control (RBAC) was reinforced to ensure only authorized individuals can handle sensitive documents.
    - Logging and monitoring were introduced for sensitive data access.
4. **Incident Response Improvement**
    - The digital forensic evidence, including email headers and attachments, was preserved for legal purposes.
    - M57.biz began regular monitoring of external sites to detect possible data exposure.
5. **Policy Updates**
    - Clear guidelines for verifying internal requests for sensitive information were established.
    - Approval workflows were updated to require multi-step validation for sharing confidential files.
    -

6.0 Conclusion

The forensic investigation determined that Jean was not at fault in the data leak. Instead, the breach resulted from a well-executed phishing attack that exploited trust within the organization. The threat actor spoofed Alison's identity using an external Gmail address and tricked Jean into sharing highly confidential employee data. The response email containing m57biz.xls was sent on July 20, 2008, at 09:28 AM MYT, shortly after the phishing message was received.

This case highlights the critical importance of email authentication technologies, user training, and verification protocols. M57.biz has taken significant steps to recover from the breach and strengthen its defenses to prevent similar incidents in the future. The evidence also exonerates Jean of wrongdoing and shifts focus toward improving the organization's cyber resilience.