Computer Forensic Examination Report

Case Title: M57 Jean Case – Data Exfiltration Investigation

Company: M57.biz

Investigator: Aditya aka demon77

Date: 21/07/25

1. Executive Summary

M57.biz, a web-based startup, experienced a data breach involving the unauthorized disclosure of a confidential spreadsheet listing employee salary information. The file was originally located on the laptop of CFO Jean. Jean has denied involvement, claiming her system must have been compromised.

This report documents a forensic investigation of Jean's laptop disk image, aimed at identifying how the breach occurred. The analysis was performed using **FTK Imager** and **Autopsy (Sleuth Kit GUI)**.

2. Objectives

- Determine whether Jean's system was compromised or if the breach originated internally.
- Reconstruct user activity timelines related to the sensitive file.
- Identify any unauthorized file access, deletion, or transfer.
- Investigate email communications and web activity.
- Provide evidence in the form of metadata, deleted files, and user artifacts.

3. Company Background

M57.biz is a fashion-tech startup with $3 million in seed funding and an ongoing $10 million funding round. The company has two founders and ten employees.

Key Staff:

- **President:** Alison Smith
- **CFO:** Jean
- **Programmers:** Bob, Carole, David, Emmy
- **Marketing:** Gina, Harris
- **Business Development:** Indy

4. Investigation Setup

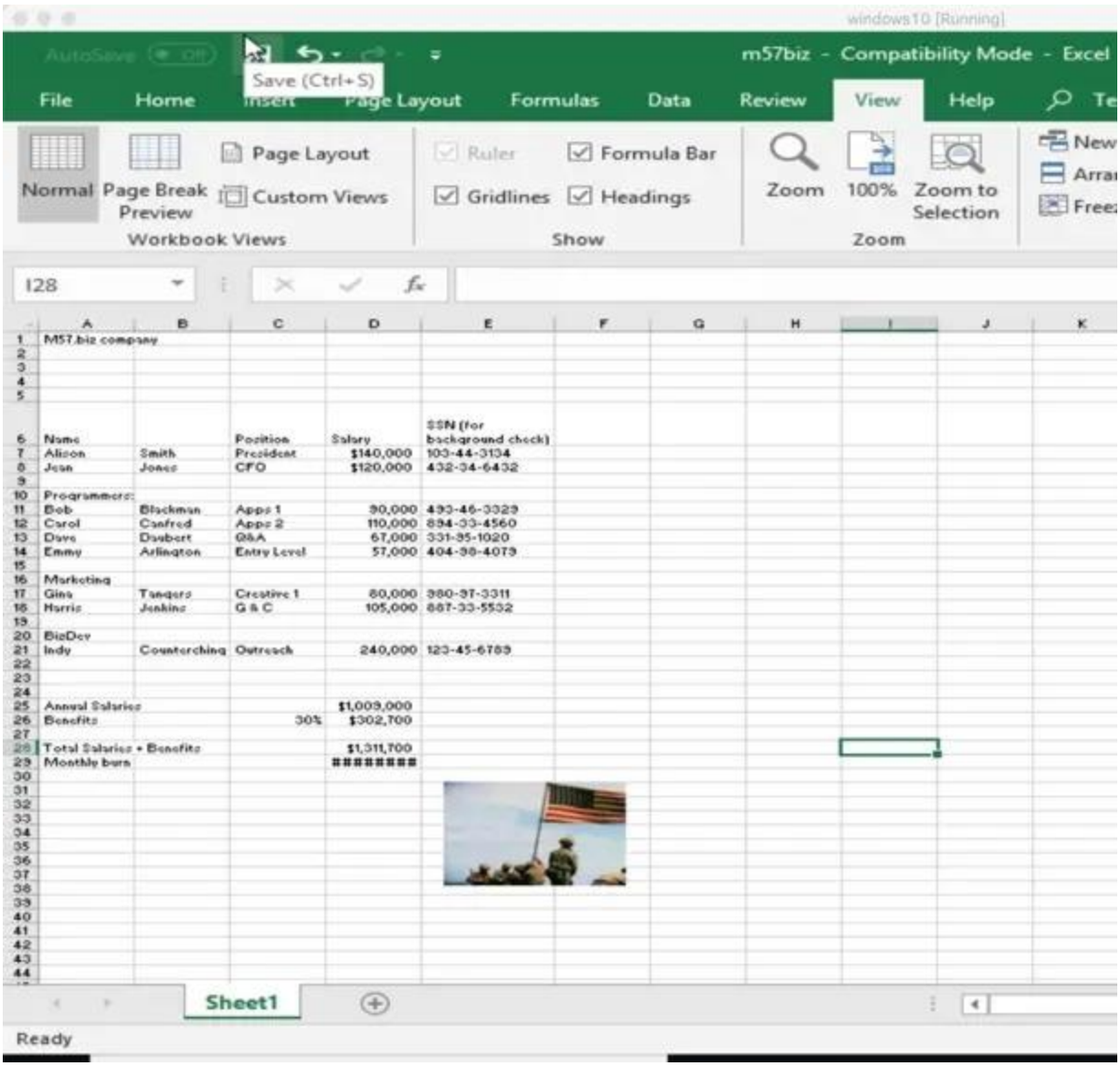
A forensic disk image of Jean's laptop was obtained in EnCase E01 format. The following tools were used in the investigation:

- **FTK Imager** – to acquire and verify the forensic image
- **Autopsy** – to examine file system structure, emails, internet artifacts, and metadata
- **Other utilities** – for PST analysis, hash verification, and timeline reconstruction

5. Key Findings

□ Spreadsheet File Identified

- **File Name:** m57biz.xls
- **Path:** C:/Settings/Jean/Desktop/m57biz.xls
- **Metadata:** Created on July 19, 2008, at 9:28 PM



Email Transmission

- Microsoft Outlook artifacts indicated use of Outlook for communication.
- **PST File Location:**

C:/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst

FILE ANALYSIS | KEYWORD SEARCH | FILE TYPE | IMAGE DETAILS | META DATA | DATA UNIT | HELP | CLOSE

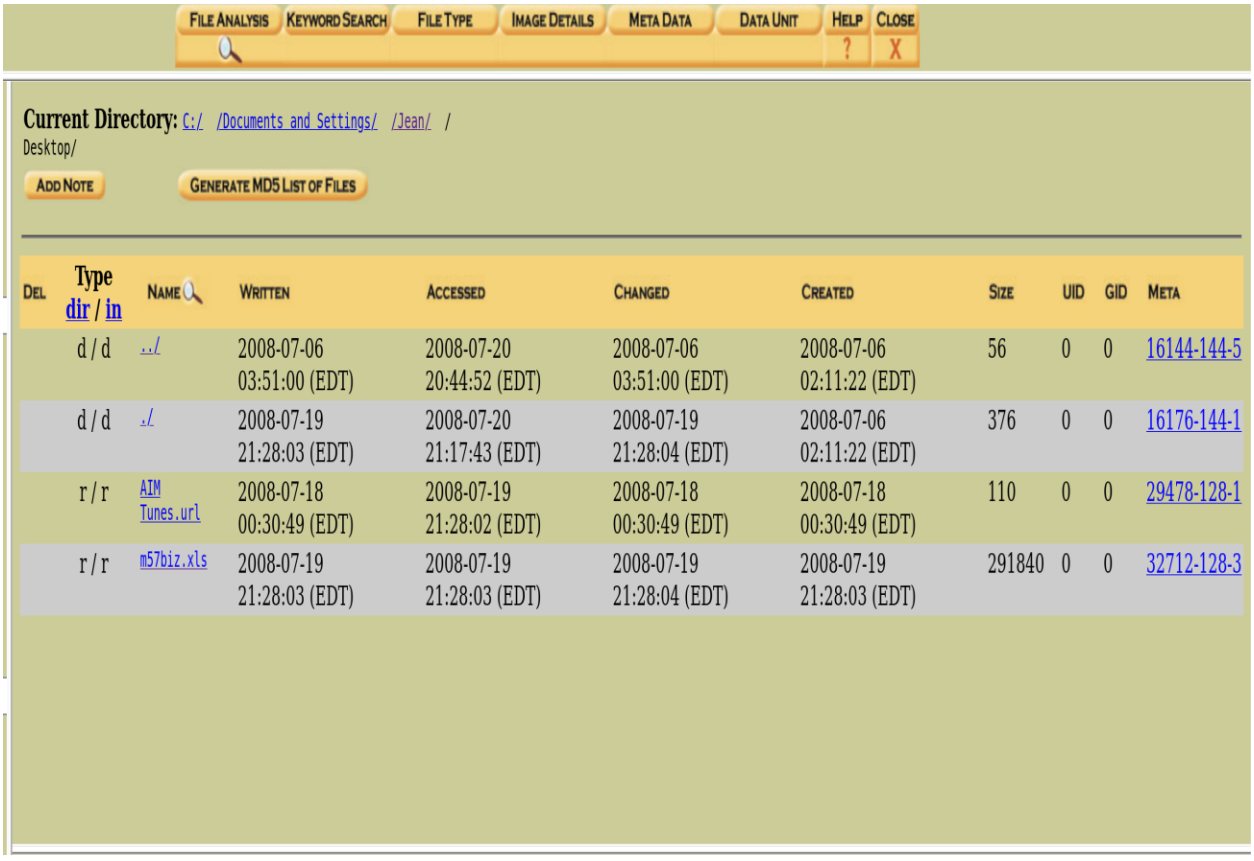
Current Directory: C:/ /Documents and Settings/ /Jean/ /Local Settings/ /Application Data/ /Microsoft/ /Outlook/

ADD NOTE | GENERATE MD5 LIST OF FILES

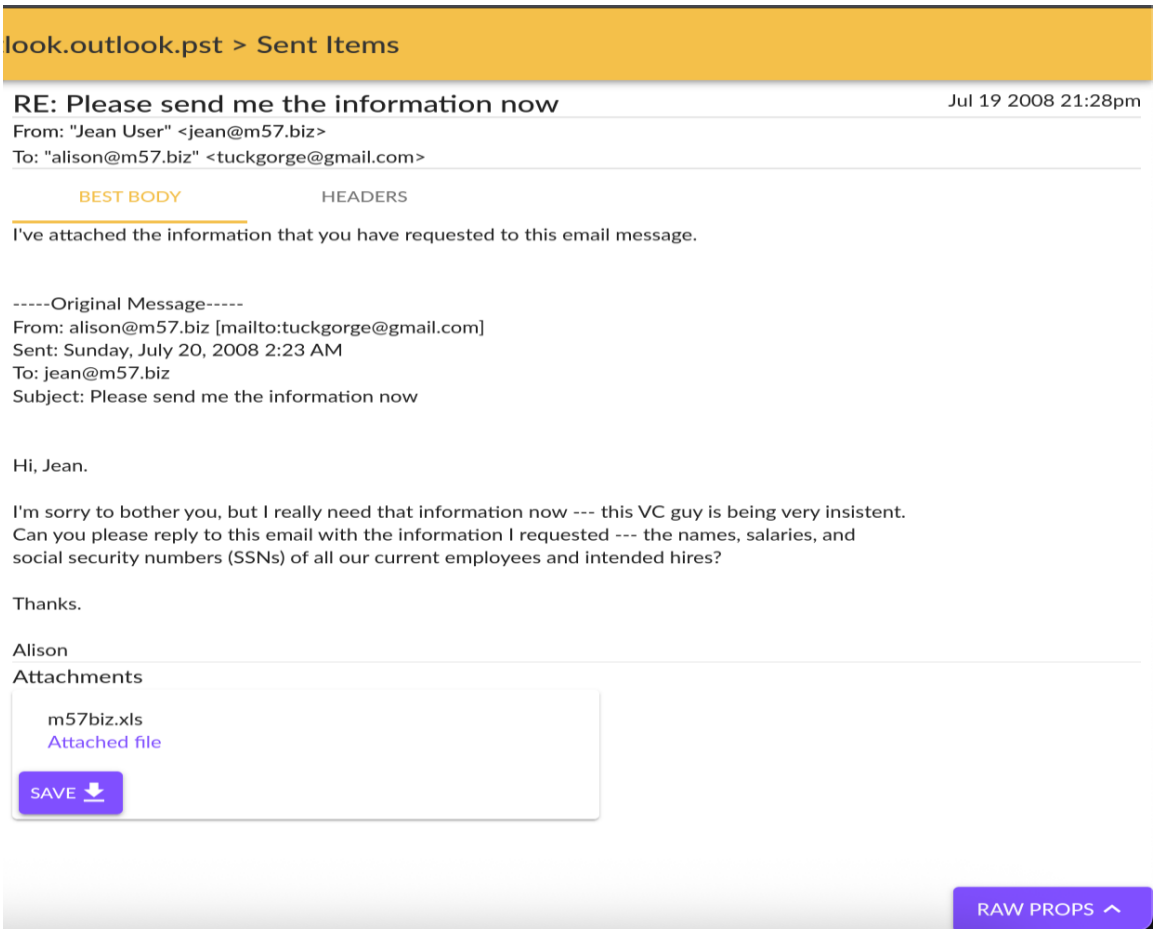
DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
	d / d	../	2008-07-06 03:49:32 (EDT)	2008-07-20 19:36:22 (EDT)	2008-07-06 03:49:32 (EDT)	2008-07-06 02:11:22 (EDT)	56	0	0	16170-144-6
	d / d	./	2008-07-06 03:37:43 (EDT)	2008-07-20 19:36:22 (EDT)	2008-07-06 03:37:43 (EDT)	2008-07-06 03:37:43 (EDT)	152	0	0	17341-144-1
	r / r	outlook.pst	2008-07-20 21:17:54 (EDT)	2008-07-20 21:17:54 (EDT)	2008-07-20 21:17:54 (EDT)	2008-07-06 03:38:42 (EDT)	2326528	0	0	17358-128-3

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note

File Type: Microsoft Outlook Personal Storage (<=2002, ANSI, version 14), dwReserved1=0x58, dwReserved2=0x51a084c, dwUnique=0x9d4, 2326528 bytes, bCryptMethod=1



- Jean sent the spreadsheet to:
  - **alison@m57.biz** (internal address)
  - **tuckgorge@gmail.com** (external Gmail address — unauthorized)



Suspicious Browser Activity

- **File:** utm[1].htm

Location:

/Documents and Settings/Jean/Local Settings/Temporary Internet Files/...

Contents: Contains a session ID (uid=7b3a09b5166b634915a989b44dae7e6b), possibly from a redirection or phishing link.

- **File:** __utm[1].htm

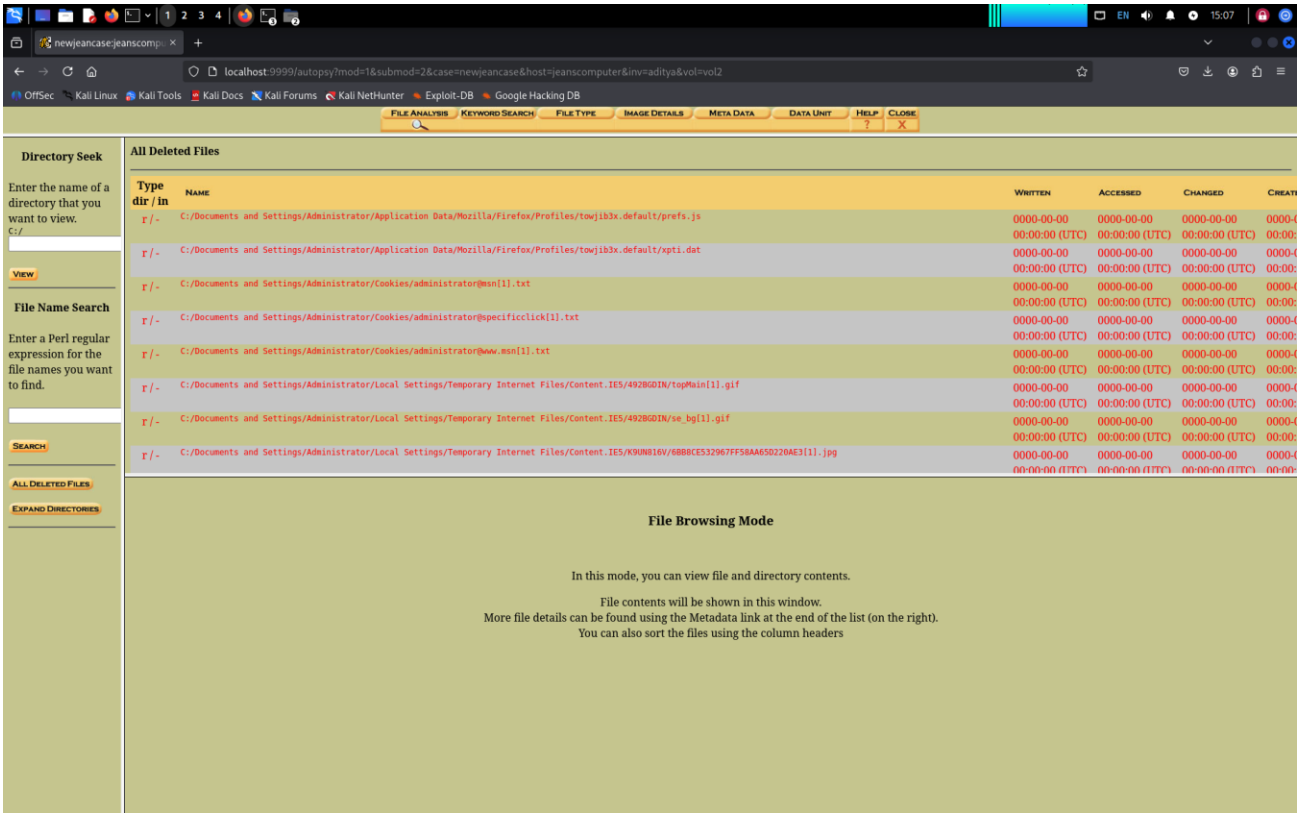
Downloaded by: Administrator user (not Jean)

Timestamps: All identical — May 14, 2008, 11:07:55 IST

Implication: This file did not come through Jean's account, raising questions about other user access.

Deleted Files Discovered

- Numerous deleted .txt and .exe files found in unallocated space
- File attributes:
  - Size: 0
  - Timestamps: Unset
  - Status: Deleted



Recovered Email Evidence

- Jean responded to a request (seemingly from Alison) and attached the salary spreadsheet.

- Email sent to both **alison@m57.biz** and **tuckgorge@gmail.com**
- Alison denies making such a request

6. Analysis & Hypothesis

The presence of a Gmail address in the recipient list and Alison's denial of the request create a contradiction. There are two possible scenarios:

1. **Jean was tricked** through a spoofed or compromised email request and unknowingly sent the confidential data externally.
2. **Alison or another actor** misused internal access to request and forward the data deliberately.

Jean's behavior, based on email timestamps and metadata, appears compliant, but she lacked verification of the email's legitimacy.

7. Recommendations

- **Email Security:** Implement DMARC, SPF, and DKIM validation to prevent spoofed emails.
- **Access Control:** Limit administrative access and log all login activity.
- **Training:** Educate employees about phishing and suspicious communication.
- **Data Protection:** Avoid sharing sensitive data via email. Use secure portals.
- **Further Investigation:** Audit server and email gateway logs. Validate the Gmail account's owner.

8. Conclusion

- Jean created and sent the spreadsheet in response to an internal email.
- The file was also sent to an unauthorized external Gmail address.
- The internal requester (Alison) denies making the request, suggesting the possibility of email spoofing.
- The presence of artifacts on the Administrator account adds a layer of suspicion.

- While Jean may have acted in good faith, Alison’s involvement or impersonation must be further investigated.

9. References

- Jarrett, M., Bailie, M.W., Hagen, E., & Judish, N. (2002). *Searching and Seizing Computers and Obtaining Electronic Evidence*.
- INFOSEC (n.d.). *Computer Forensics: Chain of Custody*.
- US-CERT (2008). *Computer Forensics*. Retrieved from the US-CERT website.