DIGITAL FORENSICS INVESTIGATION REPORT

This report was created as part of an independent study in the field of Digital Forensics. Not intended for comercial use.

By : Amar - Independent DFIR Analyst

Digital Forensics Report
M57-Jean

Investigator: Amar
Investigation Date: 14/07/2025
Tools: Autopsy v4.22.1, PST Viewer
Document Number: 01.001

1. Executive Summary

This case investigates the alleged leak of a sensitive file (m57biz.xls) from the laptop of Jean, an employee of M57 company. Based on the results of a digital investigation using Autopsy, it was found that Jean sent the file via email to an external address after being tricked by a spoofing email. There is no evidence indicating attempts to hide or delete the file.

2. Purpose of the Investigation

- Determine how the file m57biz.xls was created and sent
- Identify the email recipients
- Assess whether there was intentional action or violation of SOP
- Find supporting artifacts (emails, files, activity logs)

3. Methodolgy

- Imaging: File nps-2008-jean.E01 loaded in Autopsy.
- Ingest Modules: Metadata, File System, Email Parser, Timeline, Recent Activity
.- Data Analysis: .xls files, .pst files (Outlook), deleted files, and timeline.

4. Finding and Evidance

4.1 Spreadsheets File

Asset	Value
File Name	m57biz.xls
Location	/Documents and Settings/Jean/Desktop/
Created Date	2008-07-20 08:27
Access Date	2008-07-20 08:28
Action	Attached in the email and sent out

4.2 Email

Aset	Value
PST File	Outlook.pst
Sender	Jean (jean@m57.biz)
Receiver	tuckgorge@gmail.com (External Mail)
Subject	I've attached the information that you have requested to this email message. -----Original Message----- From: alison@m57.biz [mailto:tuckgorge@gmail.com] Sent: Sunday, July 20, 2008 2:23 AM To: jean@m57.biz Subject: Please send me the information now Hi, Jean. I'm sorry to bother you, but I really need that information now --- this VC guy is being very insistent. Can you please reply to this email with the information I requested --- the names, salaries, and social security numbers (SSNs) of all our current employees and intended hires? Thanks. Alison
Attachment	m57biz.xls
Timestamp	2008-07-20 08:28

Note: The address tuckgorge@gmail.com is not part of the official company domain and is suspected to be a result of a spoofing attack.

4.3 Deleted Files
- The file m57biz.xls or important artifacts were not found
- The deleted files are mostly system files (shortcut, temp)

4.4 Activity Timeline

Time	Activity
08:27	File m57biz.xls created
08:28	File accessed and email sent
08:29	Outlook email sending activity log
Afterwards	There is no deletion or suspicious activity.

5. Conclusion

Based on the investigation results:
- Jean created and sent the file within a very short time frame
- The file was sent to an external Gmail address that is not a legitimate address
- The email was a spoof from Alison, which triggered the leak
- No efforts to delete or conceal evidence were found

Final conclusion: Jean is a victim of a phishing attack and did not act with malicious intent.

6. Appendix

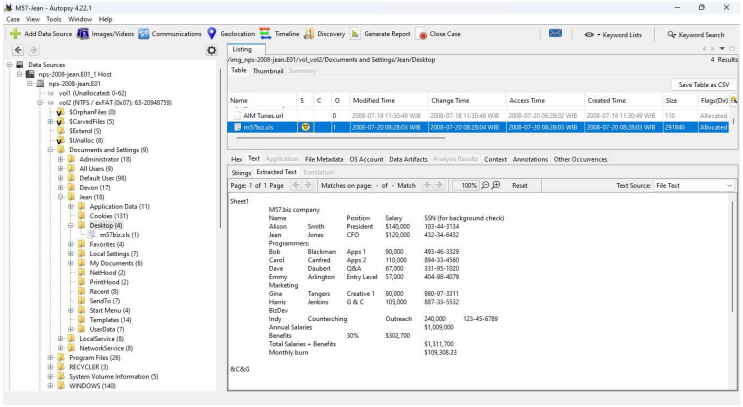

Image 1. M57biz.xls file found at Jean Dekstop

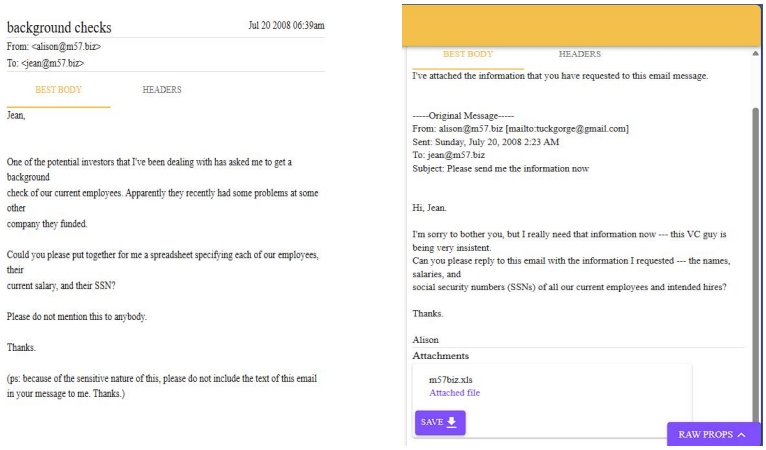

Image 2. Mail from alison@m57.biz & jean send m57biz.xls file

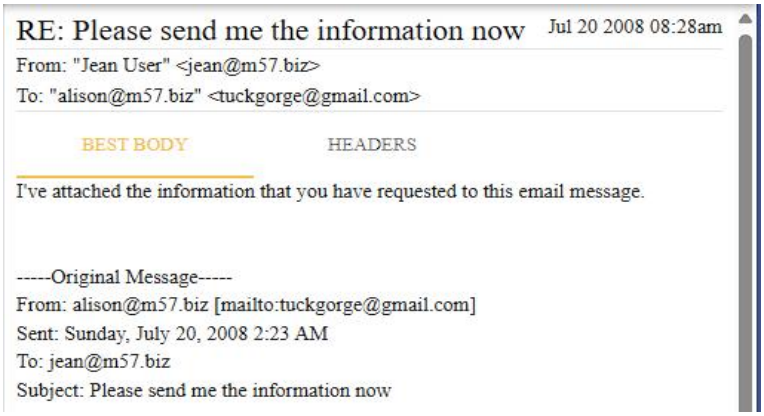

Image 3. External mail destination is tuckgorge@gmail.com