M57.Biz v. Jean Jones Computer Forensic Examination Report

Daniel Cordeiro Marques

University of San Diego

CSOL-590-04-FA21 - Cyber Incident Response and Computer Network Forensics

Professor Ron Fulton

December 13, 2021

INVESTIGATOR	**Ron Fulton**
	Lead Investigator
	University of San Diego
DIGITAL FORENSIC EXAMINER	**Daniel Cordeiro Marques**
	University of San Diego, MSc. Cybersecurity Ops Leadership Candidate
	San Diego, CA
SUBJECT	**Digital Forensics Examination Report**
CASE IDENTIFICATION	M57-JEAN
OFFENSE	Unauthorized Disclosure of Employee Personally Identifiable Information
ACCUSED	**Jean Jones**
	CFO
	M57.Biz
DATE OF REQUEST	**December 7, 2021**
DATE OF CONCLUSION	**December 13, 2021**

Table of Contents

M57.Biz v. Jean Jones Computer Forensic Examination Report

M57.Biz is a web-based company that had a spreadsheet leaked on a competitor's website. The case investigator requested a digital forensic examination of the existing evidence to identify how the breach occurred. This report demonstrates the steps to perform the analysis and presents recommendations and the examiner's conclusion based on existing evidence.

1. Background To The Case

M57.Biz is a web start-up developing a body art catalog that raised $ 3M in seed funding, and it is moving to close $ 10M in the next investment round. The company operates primarily online, with programmers working from home and conducting weekly in-person meetings in the office park. Marketing and Business Development personnel work out of hotel rooms and coffee shops and hold in-person meetings every two weeks. Employees typically share documents by email.

Personally Identifiable Information (PII), including social security numbers and salary from M57.Biz, was posted on a competitor’s forum in the form of a spreadsheet. Investigators suspected that the file came from Jean Jones’ computer. Jean is the company’s CFO. The primary objective of this investigation is to determine if Jean Jones was responsible for publishing the spreadsheet while identifying the following:

- How the spreadsheet was leaked from Jean’s computer.
- Evidence that confirms or exonerates Jean Jones from the data breach.

1.1. Involved parties

Table 1 lists the personnel involved in the case:

Table 1.

Personnel Relevant To The Case.

Name	Position	Email
Alison Smith	President	alison@m57.biz
Jean Jones	CFO	jean@m57.biz

1.2. Summary of Interviews

The investigators interviewed Jean and Alison Smith, the company's president, to obtain additional information pertinent to the case. The interviewees offered the following details:

- **Jean Jones** claims that Alison asked her to prepare the spreadsheet with employee PII as a request associated with the new funding round.
- **Alison Smith** denies ever asking Jean for a spreadsheet.
- **Jean Jones** claims that Alison requested the spreadsheet to be sent by email.
- **Alison Smith** denies receiving the spreadsheet by email.

2. Exhibits Submitted For Analysis

All involved parties consented to collecting and searching their email communication and data stored electronically in M57.Biz's systems and serve as digital evidence. Jean volunteered her computer to the investigator for evidence collection and further analysis.

The investigator collected all evidence following the best practices outlined by the Scientific Working Group on Digital Evidence (SWGDE), including the "Best Practices for Computer Forensic Acquisitions" (Scientific Working Group on Digital Evidence, 2018a) and

"Best Practices for Digital Evidence Collection" (Scientific Working Group on Digital Evidence, 2018c). They used EnCase to obtain a forensic image from Jean's computer. A forensic image is a complete duplicate of the system's disk, allowing the examiner to verify its contents (including deleted files) while preventing modifications to the files. The investigator submitted a forensic image of Jean's computer for analysis.

Table 2 lists the exhibits submitted for analysis.

Table 2.

Digital Evidence Submitted For Analysis.

ID	M57-Jean-001
Description	Forensic disk image of Jean's hard drive
MD5 Hash	78a52b5bac78f4e711607707ac0e3f93
Acquire Date	January 31, 2011 4:38:29 PM PST
Date Submitted	December 6, 2021 2:00:01 PM PST
Submitter	Ron Fulton, Lead Investigator
Method of Delivery	Read-only media delivered through secure file transfer

4. Evidence to Search For

During the interviews with the involved parties, the accused (Jean) indicated that the request to create and share the spreadsheet over email came from the M57.Biz's president (Alison); Alison denied this claim. The search for data to determine if Jean intentionally shared the spreadsheet in the competitor's website will include examining the forensic image to:

- Search Jean's communications for Alison's request to create the spreadsheet.

- Search Jean's files to identify when she created the spreadsheet.
- Search browsing history to identify evidence of Jean submitting the spreadsheet to the competitor's forum.

5. Corporate Breach

Jean is suspected of having breached her non-disclosure agreement and contract by divulging confidential information from M57.Biz.

6. Examination Details

I examined the read-only forensic image of Jean's computer identified as "M57-Jean-001", which allows access to files while preventing modification of its contents. I verified the digital image hash before and after the examination to ensure the data was not changed and the chain of custody was maintained.

6.1. Tools Utilized for Examination

The examination process utilized three well-known and widely accepted digital forensic tools:

EnCase Forensic Imager. This tool allows the investigator to generate digital forensic images, preserving the data from a device (*EnCase Forensic Imager*, n.d.). The investigator performed an identical copy of Jean's computer using EnCase.

Autopsy. Examiners can use this tool to analyze forensic images and "recover digital evidence from it" (*Autopsy User Documentation: Autopsy User's Guide*, 2021). I utilized Autopsy to recover emails and files stored in Jean's computer.

FTK Imager. This tool allows the examiner to analyze forensic images (*FTK Imager Version 4.5 User Guide*, 2020). I utilized FTK Imager to examine read-only copies of the files found in Jean's computer.

6.2. Preparation

Following the SWGDE's recommendations outlined in (Scientific Working Group on Digital Evidence, 2018b), before beginning the activities, I verified that the examination environment had the adequate infrastructure to conduct the examination and analysis (including power, space, and cooling). The examination workstation consisted of a virtualized operating system functioning in an isolated container. I ensured the operating system and forensic software were patched to its latest version. Additionally, I verified that all required software was working as expected.

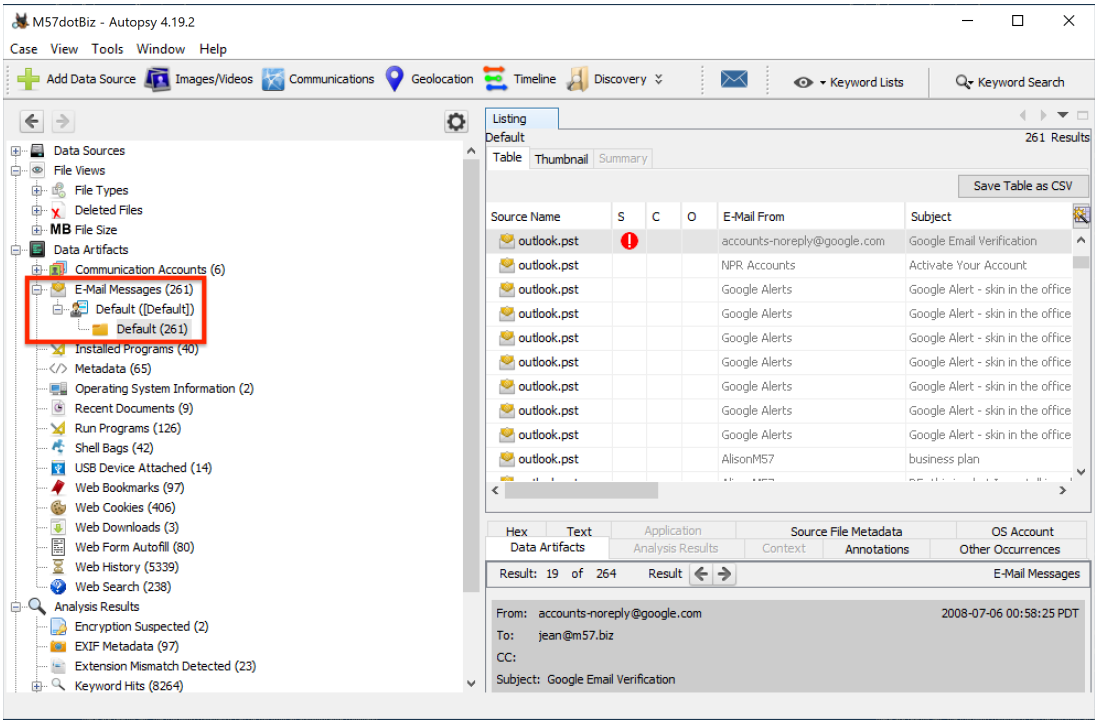
As previously noted, I verified the M57-Jean-001's hash before starting the examination.

6.3. Recovering and Examination of Jean's Email Communications

Jean claimed to have received an email message from Alison requesting the spreadsheet with employee data, which Alison denies. To validate this claim, I utilized Autopsy to recover Jean's emails from the digital forensic image M57-Jean-001. Figure 1 illustrates the recovery of 261 e-mail messages from the "outlook.pst" file; this file stores email messages and other items managed by Microsoft Outlook (*Introduction to Outlook Data Files (.Pst and .Ost)*, n.d.).

Figure 1.

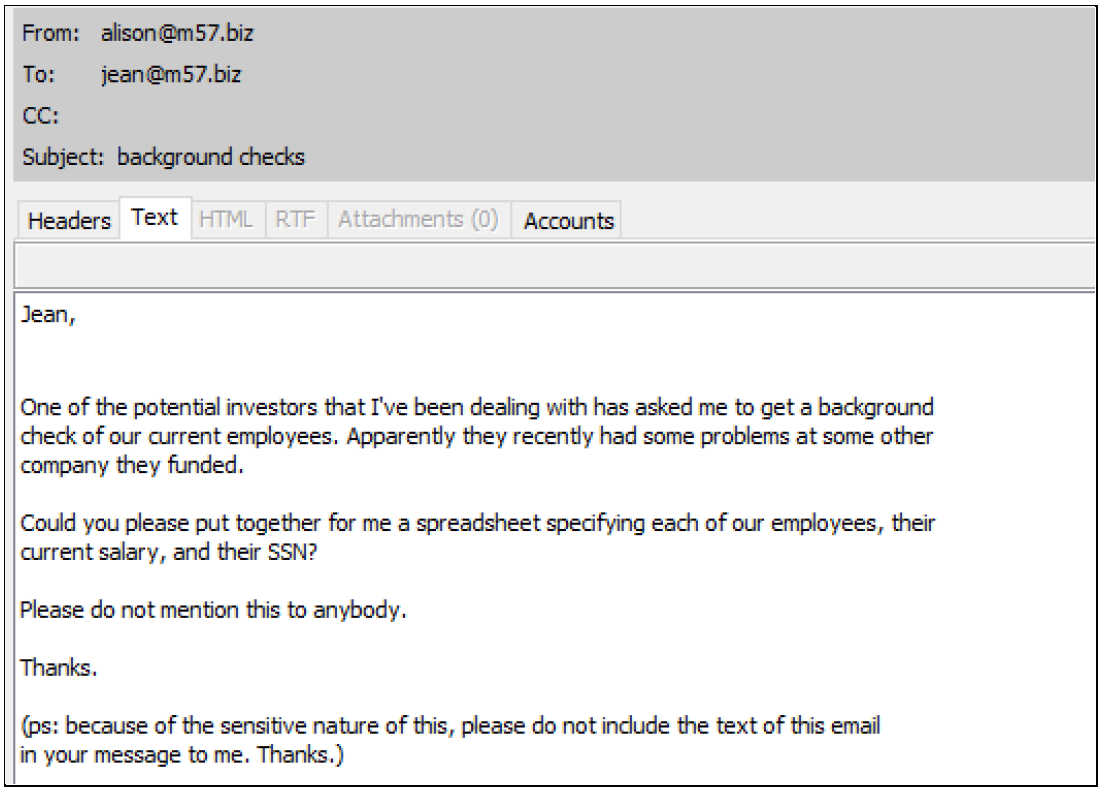
Email messages recovered by Autopsy.



Next, I searched Jean's emails to identify a message coming from Alison requesting the spreadsheet and observed that on July 19, 2008 at 16:39:57 PDT, Jean received an email apparently from "alison@m57.biz" with the subject "background checks" (figure 2). The sender requested Jean to put together a spreadsheet with each employee's name, current salary, and SSN of under the pretext of a background check for a potential investor.

Figure 2.

Message Requesting The Spreadsheet.


From: alison@m57.biz
To: jean@m57.biz
CC:
Subject: background checks

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Jean,

One of the potential investors that I've been dealing with has asked me to get a background check of our current employees. Apparently they recently had some problems at some other company they funded.

Could you please put together for me a spreadsheet specifying each of our employees, their current salary, and their SSN?

Please do not mention this to anybody.

Thanks.

(ps: because of the sensitive nature of this, please do not include the text of this email in your message to me. Thanks.)

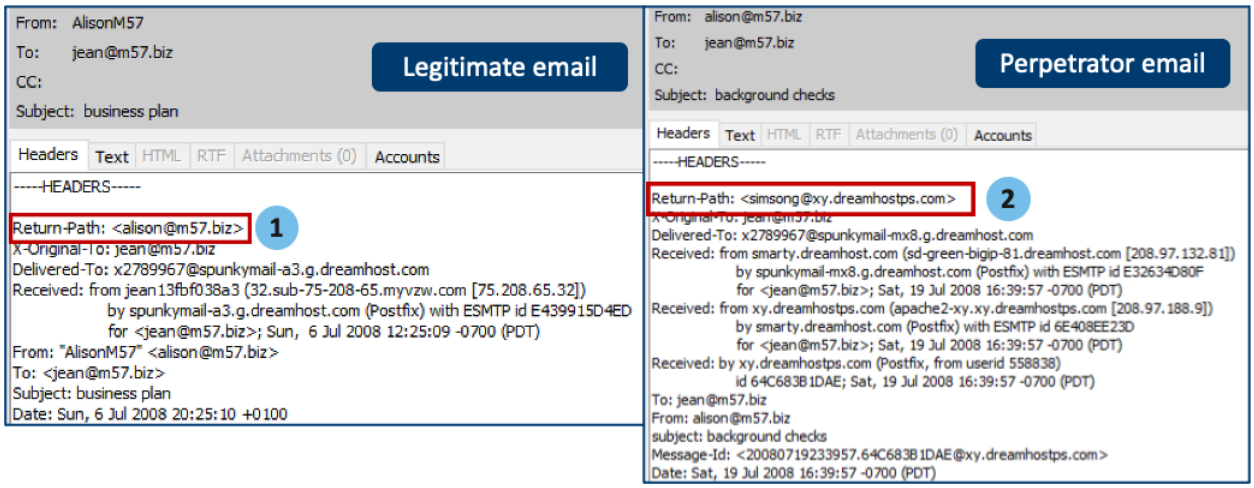
Further examination of the email headers indicates that the message did not come from Alison, but from a third-party masquerading as Alison to convince Jean of the request's legitimacy. Email headers are critical to identifying these attacks, as they provide information about the sender and the route through each email passed until it reached the recipient. For instance, as figure 3 illustrates, the “Return-Path” header is inconsistent with other messages sent by Alison; the message labeled with the number 1 shows the Return-Path value from a legitimate email sent by Alison on July 6. Message number 2 shows the Return-Path of the perpetrator’s email.

Additionally, the “Received” header also demonstrates another sign that Alison did not send the email; this header represents the message’s path from the sender to the recipient. The

legitimate email from Alison only required one hop. The perpetrator's message, in contrast, went through three different servers before being delivered to Jean.

Figure 3.

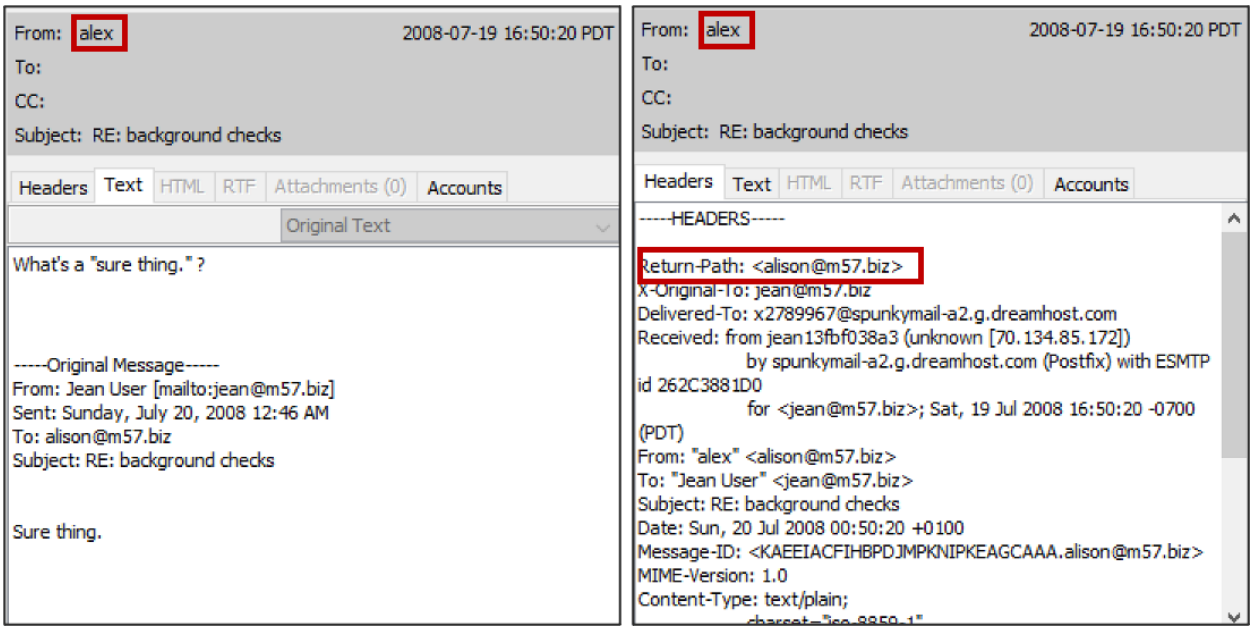
Email Header Comparison.



On July 19, 2008 at 16:44:00 PDT, Jean responded to the email with the phrase “sure thing”. Following the perpetrator’s prompt, Jean removed the contents of the previous message requesting the spreadsheet. Alison replied with a message that indicated she did not understand the original message. Jean’s Outlook was misconfigured to show Alison's contact as “Alex”. However, header analysis shows that the reply did come from Alison. Alison and Jean did not communicate again regarding this email (figure 4).

Figure 4.

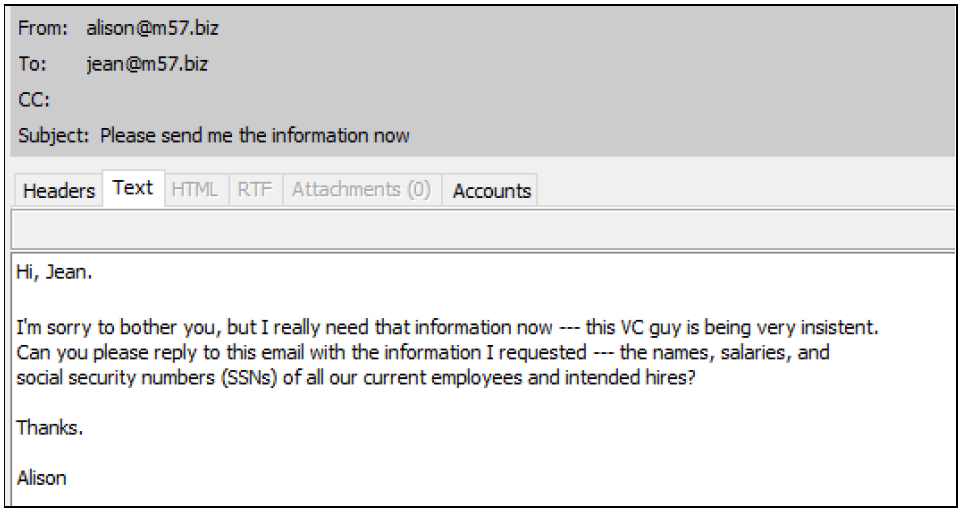
Alison Reply to Jean.



The perpetrator insisted on receiving the spreadsheet. On July 19, 2008 at 18:22:45 PDT, they sent a second email with the subject "Please send me the information now" requesting the data. This time, they also asked Jean to add information related to intended hires (figure 5).

Figure 5.

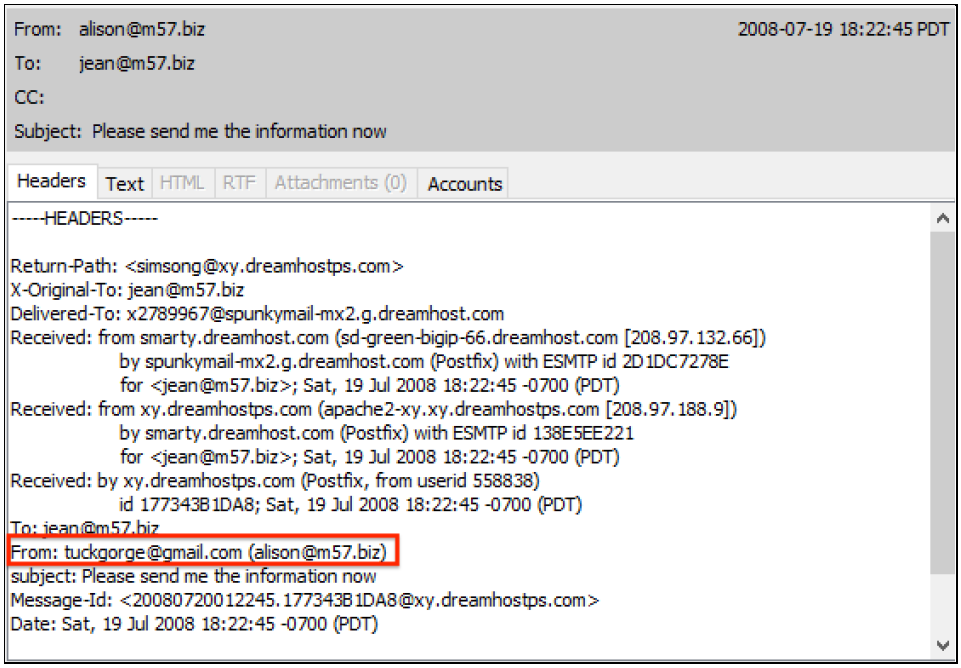
Perpetrator's Second Request.



This time, however, the header analysis provided additional insights on the perpetrator: the “From:” field within the headers leaked the perpetrator’s actual email address, “tuckgorge@gmail.com” (figure 6).

Figure 6.

Perpetrator’s Email Observed During Header Analysis.



Jean complies with this request by preparing and sending the spreadsheet to the perpetrator.

6.4. Spreadsheet Creation And Sharing

I searched for spreadsheets in the forensic image of Jean’s computer and identified a file named “m57biz.xls” on her Desktop (figure 7). I analyzed the file’s metadata and observed that it was created approximately on July 19, 2008 at 18:28:00 PDT (figure 8).

Figure 7.

"m57biz.xls" Spreadsheet Data (Redacted To Preserve Privacy).

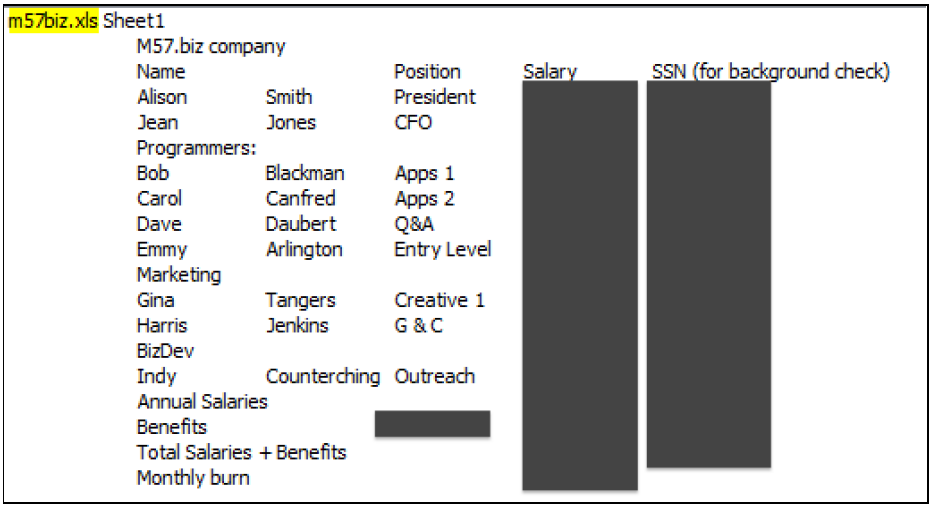
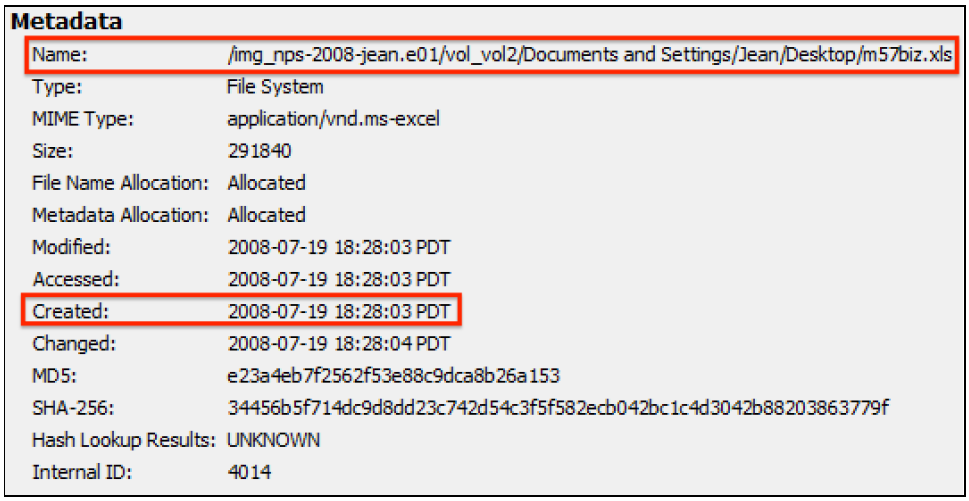


Figure 8.

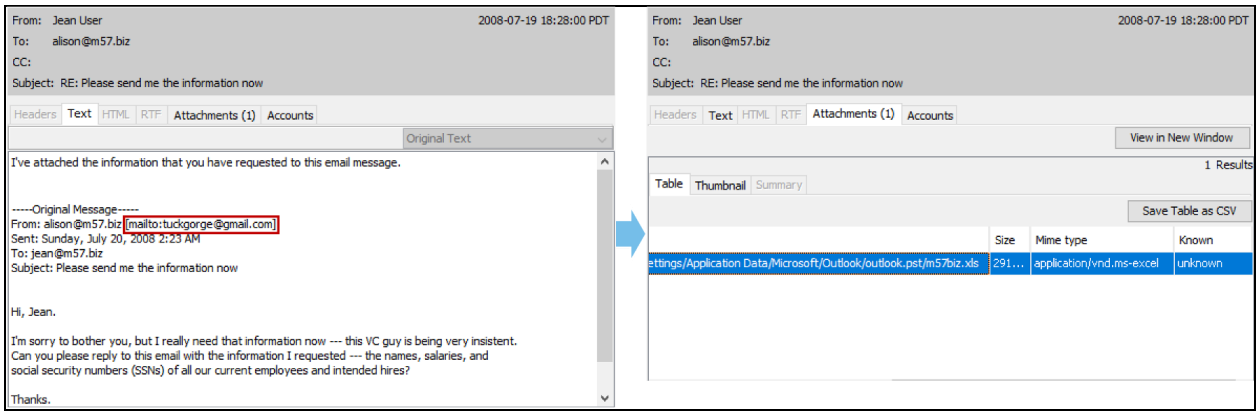
"m57biz.xls"Metadata.



Next, I observed that Jean replied to the perpetrator on July 19, 2008 at 18:28:00 PDT with the spreadsheet attached (figure 9).

Figure 9.

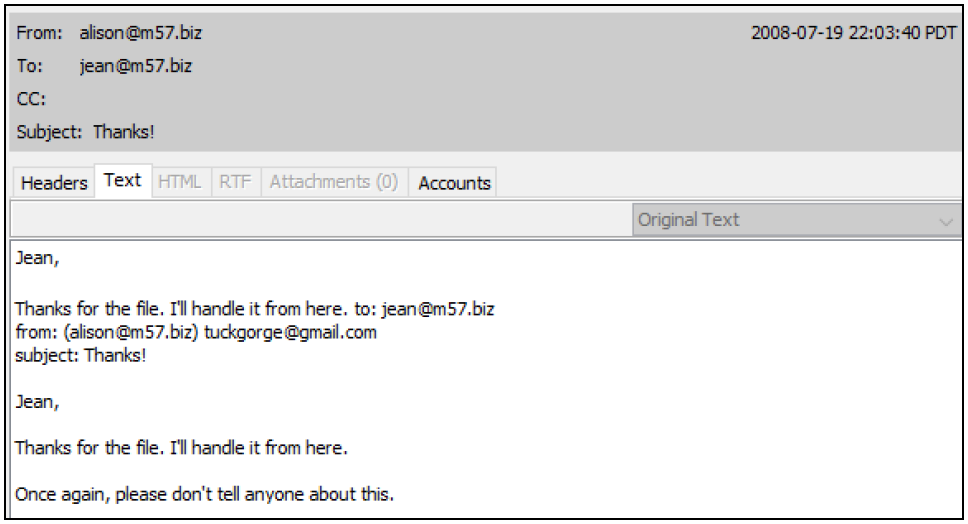
Jean Sends The Spreadsheet To The Perpetrator.



Finally, on July 19, 2008 at 22:03:40 PDT, the perpetrator confirmed receiving the file from Jean, thanked her and reinforced that she should not discuss the exchange with others (figure 10).

Figure 10.

Perpetrator Confirms They Received The Spreadsheet.



6.5. Other Evidence Examined

In addition to email exchanges, I also examined Jean's Instant Messaging (IM) communications, as well as her browser and search history. I did not observe any findings relevant to this case during the examination.

7. Analysis Results

The analysis indicates that a third party impersonated Alison and requested Jean to create and share the spreadsheet over email. Jean complied, and ultimately sent the data to the external email address "tuckgorge@gmail.com." There is no evidence that Jean uploaded the spreadsheet to the competitor's website, or that she moved the data outside of her corporate device.

Table 3 summarizes the timeline of events concerning this case. I did not observe any evidence of timestamp tampering during the examination.

Table 3.

Timeline Of Events.

Date and Time	Event
July 19, 2008 16:39:57 PDT	Perpetrator impersonates Alison's account to email Jean Jones with the subject "background checks" requesting a spreadsheet with employees' names, salaries, and social security numbers.
July 19, 2008 16:44:00 PDT	Jean replies to the email with "Sure thing", but removes the contents of the original message.
July 19, 2008 16:50:20 PDT	Alison replies to Jean's message asking "what is a sure thing?".
July 19, 2008 18:22:45 PDT	Jean receives a second email from the perpetrator with the subject "Please send me the information now", requesting the data immediately.
July 19, 2008 18:28:00 PDT	Jean creates the spreadsheet "m57biz.xls" on her Desktop with employee PII.

July 19, 2008 18:28:00 PDT	Jean replies to the perpetrator's email with the "m57biz.xls" spreadsheet attached.
July 19, 2008 18:28:00 PDT	The perpetrator replies to Jean's email confirming receipt of the email, thanking her, and requesting no to mention the exchange with anybody.

8. Conclusions

The digital evidence indicates that Jean did not intentionally leak the spreadsheet to the competitor. During the examination, I recovered an email chain showing that a third party impersonated Alison and contacted Jean to request the spreadsheet with employee data, which aligns with the interviews conducted by the investigator. There is no evidence that the perpetrator's email account ("tuckergorge@gmail.com") belongs to Jean Jones, nor that she had previous knowledge of the account.

This event is a typical spear-phishing attack, and Jean's inability to identify the malicious email led to the incident. As an opportunity for improvement, M57.Biz should consider reviewing its anti-phishing strategy, including social engineering training and email filtering capabilities. The company should also consider Data Loss Prevention (DLP) technologies that detect and prevent threat actors from removing sensitive information from the M57.Biz systems.

In conclusion, Jean Jones should be considered not guilty of breach of contract and breach of the non-disclosure agreement. The court should consider the fact that the perpetrator impersonated Alison and that the plaintiff does not have the appropriate training to recognize the fake email.

9. Evidence Disposition

Once I completed the examination of evidence, I returned the media storing the forensic copies of the files to the investigators. I sanitized the virtual operating system at the conclusion of the analysis and all evidence files associated with the case.

10. Chain Of Custody

Table 4 documents the chain of custody for evidence used in this case.

Table 4.

Chain Of Custody.

ID	M57-Jean-001
Description	Forensic disk image of Jean's hard drive
MD5 Hash	78a52b5bac78f4e711607707ac0e3f93
Acquire Date	January 31, 2011 16:38:29 PST
Date Submitted	December 6, 2021 14:00:01 PST
Submitter	Ron Fulton, Lead Investigator
Method of Delivery	Read-only media delivered through secure file transfer
ID	M57-Jean-002
Description	Outlook.pst file
MD5 Hash	8c862a8c7ad8b7aff1df4d44fbf1fe95
Acquire Date	December 7, 2021 10:03:20 PST
Date Submitted	December 13, 2021 2:00:01 PST
Submitter	Daniel Cordeiro Marques, Examiner
Recipient	Ron Fulton, Lead Investigator

Method of Delivery	Read-only media delivered through secure file transfer
ID	M57-Jean-003
Description	Spreadsheet with employee data (m57biz.xls)
MD5 Hash	e23a4eb7f2562f53e88c9dca8b26a153
Acquire Date	December 8, 2021 14:00:48 PST
Date Submitted	December 13, 2021 2:00:01 PM PST
Submitter	Daniel Cordeiro Marques, Examiner
Recipient	Ron Fulton, Lead Investigator
Method of Delivery	Read-only media delivered through secure file transfer

References

Autopsy User Documentation: Autopsy User's Guide. (2021, December 13). The Sleuth Kit. Retrieved December 13, 2021, from http://sleuthkit.org/autopsy/docs/user-docs/4.19.2/

EnCase Forensic Imager. (n.d.). OpenText Security. Retrieved December 10, 2021, from https://security.opentext.com/docs/default-source/document-library/product-brief/ef-fs-encase-forensic-imager-web-ready_70f143c6-24ca-4728-aaf6-fd697b6b0b26.pdf

FTK Imager Version 4.5 User Guide. (2020, October 8). AccessData. Retrieved December 12, 2021, from https://accessdata.com/product-download/ftk-imager-version-4-5

Introduction to Outlook Data Files (.pst and .ost). (n.d.). Microsoft Support. Retrieved December 13, 2021, from https://support.microsoft.com/en-us/office/introduction-to-outlook-data-files-pst-and-ost-222eaf92-a995-45d9-bde2-f331f60e2790

Scientific Working Group on Digital Evidence. (2018a, April 25). *SWGDE Best Practices for Computer Forensic Acquisitions*. swgde.org. Retrieved December 5, 2021, from https://drive.google.com/open?id=1KeEI1DUkSE2DSPZyPFEFIGfzbZS3-zZC

Scientific Working Group on Digital Evidence. (2018b, July 11). *SWGDE Best Practices for Computer Forensic Examination.pdf*. swgde,org. Retrieved December 13, 2021, from https://drive.google.com/file/d/12z6Vrtmts6oxg9HHORFkHrwUPa7cGAck/view

Scientific Working Group on Digital Evidence. (2018c, July 11). *SWGDE Best Practices for Digital Evidence Collection*. swgde.org. Retrieved December 5, 2021, from https://drive.google.com/open?id=1zP4OgpRrj-t9sVGNcqndqIgsemq7u5XQ

Vandeven, S. (2014, September 19). *Forensic Images: For Your Viewing Pleasure*. SANS Reading Room. https://www.sans.org/white-papers/35447/