



# COMPUTER FORENSICS EXAMINATION REPORT

By: Cecil Hammett

MS. CYBER SECURITY OPERATIONS AND LEADERSHIP University of San Diego, CSOL-590



## Abstract

The task of the digital forensic investigation team is to unveil how a spreadsheet containing confidential data was leaked from the device of Chief Financial Officer (CFO) Jean Jones and posted to the competitor's public page. Below is a complete and comprehensive forensic examination report that documents the processes taken and the findings uncovered via the stages of a computer forensic examination.

<b><u>Digital Forensics Examiner:</u></b>	Cecil Hammett
<b><u>Company:</u></b>	University of San Diego
<b><u>Location:</u></b>	San Diego, California

<b><u>Subject:</u></b>	Digital Forensics Examination Report
<b><u>Offence:</u></b>	Stolen data from organization device, disclosure of confidential information to the public
<b><u>Accused:</u></b>	tukergorge@gmail.com
<b><u>Date of Request:</u></b>	December 6, 2021
<b><u>Date of Conclusion:</u></b>	December 13, 2021

## Table of Contents

<b>Abstract.....</b>	<b>1</b>
<b>Organization Overview.....</b>	<b>3</b>
<b>Background to the Case.....</b>	<b>3</b>
<b>Questions Asked Relevant to the Case .....</b>	<b>5</b>
1.    When did Jean create this spreadsheet? .....	5
2.    How did it get from Jean's computer to the competitor's website? .....	5
3.    Who else from the company is involved? .....	6
<b>Search and seizer and transport of evidence .....</b>	<b>6</b>
1.    A copy of Jean's computer's hard drive .....	6
2.    A copy of the spreadsheet in question named m57biz.xls .....	7
<b>Evidence to Search for.....</b>	<b>7</b>
<b>List of Criminal Offense .....</b>	<b>8</b>
<b>Collection and Analysis of Digital Evidence .....</b>	<b>8</b>
Adding the image file as an evidence item in the FTK Imager .....	8
Understanding the data provided in the initial analysis .....	9
Conducting the search on email communications .....	11
<b>Discovering the Breach, a Comprehensive Timeline .....</b>	<b>13</b>
<b>Conclusion .....</b>	<b>16</b>
<b>Recommendations .....</b>	<b>17</b>
<b>References.....</b>	<b>20</b>

## Organization Overview

M57dotBIZ is a small startup company that develops a body art catalog. The company initially received \$3M in seed funding but closed at a full funding of \$10M. The significant funding for the company is an aspect that might bring unwanted attention from cybercriminals towards the companies employees.

The organization has two founders and ten employees hired in the first year. Hiring employees within a company can sometimes involve significant onboarding. Onboarding may involve training, employee meet and greet, and review of the organizations' policies and procedures. When onboarding a large group of employees, especially within a startup where there may not be a tested onboarding process, it can be easy to rush into work and skip over essential training aspects like security best practices.

The current employees of the organization are President, Alison Smith, CFO: Jean Jones, Programmers: Bob, Carole, David, Emmy, Marketing: Gina, Harris, and BizDev: Indy.

M57dotBIZ is a virtual corporation meaning the employees are most often working remotely with weekly or bi-weekly in-person meetings. Most document exchanges occur via email. Due to the lack of in-person correspondence, email security is essential and can act as a significant attack vector for those knowledgeable of this aspect.

## Background to the Case

A few weeks into the inception of the new startup company, a spreadsheet document containing confidential organizational information was posted to a competitor's web form. The spreadsheet contained the name, salary, position, and Social Security Number (SSN) of the

company's key employees. Upon initial overview of the employees' devices, the spreadsheet in question was located on only one employee's device, Chief Financial Officer (CFO) Jean Jones.

Jean claims to be innocent, stating in her interview that the company's President, Alison Smith, requested the spreadsheet document to be sent to her via email as part of a new funding campaign. In Alison's interview, she reveals to have no idea what Jean is talking about and never requested the spreadsheet via email.

The high-level goal of the investigation is to determine if the data on the laptop was stolen or if there is a separate crime ongoing within the organization's personnel. If the data was indeed stolen, the next step would be to unveil how this breach occurred. Additionally, the investigation team has attempted to create a comprehensive timeline of the events leading up to the breach, including the complete exfiltration of the spreadsheet.

In order to conduct a thorough and effective investigation, three different forensic analysis tools were utilized. Encase by Guidance Software was used to capture the image of the device in question, Forensic Toolkit Imager (FTK Imager) by Access Data was used to analyze the hard drive of Jean's device, and Kernel Outlook PST Viewer unveiled the crucial email information extracted from the outlook.pst file captured by the FTK Imager.

Based on my knowledge as a digital forensic investigator coupled with the miscommunication regarding email correspondence disclosed in the interviews, it is believed the breach occurred via email communication.

## Questions Asked Relevant to the Case

Upon the initial breach within the organization, an analysis was conducted. The following questions were raised by the first-round founders and later answered by the findings in the investigation.

1. When did Jean create this spreadsheet?

The file in question, m57biz.xls, was located on Jean's desktop with the creation date of 07/20/2008.

2. How did it get from Jean's computer to the competitor's website?

In the interviews provided for the investigation, we see Jean discussing email communication. Jean states, *"Alison asked me to prepare the spreadsheet as part of new funding round."*

Upon interviewing Alison, we are provided with a different side of the story. Allison claims to have no knowledge of the communication Jean is disclosing. Due to the inconsistency of the interviews, the email archives located in Jean's Profile were exported to be viewed in Kernel Outlook PST Viewer.

A search was performed on Jean's sent emails to Alison who stated in the interview, *"I never received the spreadsheet by email."* Two emails were found in the sent folder directly regarding the spreadsheet. The email correspondence in question occurred on 07/20/2008. A spoofed email address was found in the sent emails regarding the spreadsheet. It appears Jean unknowingly sent the confidential information to a receiver by the email of [tukergorge@gmail.com](mailto:tukergorge@gmail.com).

### 3. Who else from the company is involved?

The evidence obtained in the investigation displays no other employee was directly involved in the breach. The spear-phishing attack was specifically targeted towards the impersonation of President Alison Smith.

### Search and seizer and transport of evidence

A request to obtain and view the contents of the device belonging to Jean Jones was filed to the company. A search warrant for the information is not required in this case as the private organization holds all ownership of the digital evidence and willingly assisted in the collection of data. The request to the organization contained the permissions to search the device in question to obtain the essential information which will act as digital evidence within the case.

Upon the search and seizure of the necessary devices, which may act as digital evidence, the attained materials were cautiously packaged such that a chain of custody was effectively established, ensuring the integrity of the evidence obtained.

### Exhibits Submitted for Analysis

The forensic team received the required evidence for the case via a copy of the spreadsheet in question and an Encase image of the device belonging to Jean Jones, which is composed utilizing the following files:

#### 1. A copy of Jean's computer's hard drive

##### a. Nps-2008-jean.E01 received via:

<http://downloads.digitalcorpora.org/corpora/drives/nps-2008-m57-jean/nps-2008-jean.E01>

b. Nps-2008-jean.E02 received via:

<http://downloads.digitalcorpora.org/corpora/drives/nps-2008-m57-jean/nps-2008-jean.E02>

2. A copy of the spreadsheet in question named m57biz.xls

M57.biz company				
Name		Position	Salary	SSN (for background check)
Allison	Smith	President	\$140,000	103-44-3134
Jean	Jones	CFO	\$120,000	432-34-6432
Programmers:				
Bob	Blackman	Apps 1	90,000	493-46-3329
Carol	Canfred	Apps 2	110,000	894-33-4560
Dave	Daubert	Q&A	67,000	331-95-1020
Emmy	Arlington	Entry Level	57,000	404-98-4079
Marketing				
Gina	Tangers	Creative 1	80,000	980-97-3311
Harris	Jenkins	G & C	105,000	887-33-5532
BizDev				
Indy	Counterchng	Outreach	240,000	123-45-6789
Annual Salaries			\$1,009,000	
Benefits			30%	\$302,700

## Evidence to Search for

Based on the information obtained via the company overview and personnel interviews the search for digital evidence valuable to the investigation will be in the area of; (A) acquiring the email communications to and from Jean which occurred in the specific timeline of the breach, (B) investigate the email communications and the attributes of the sender and receiver.



### List of Criminal Offense

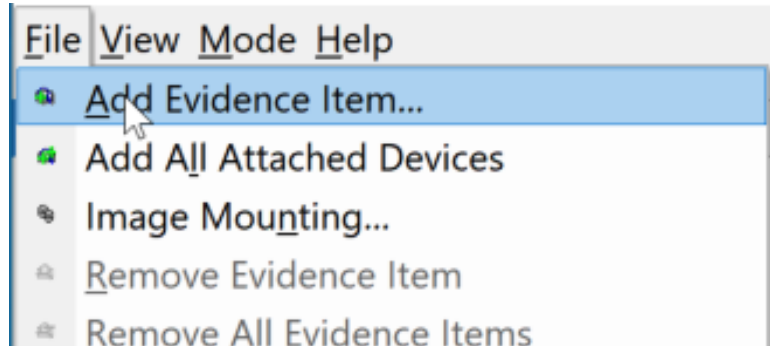
The criminal offense revealed in this case is theft of confidential information via deception of personnel.

### Collection and Analysis of Digital Evidence

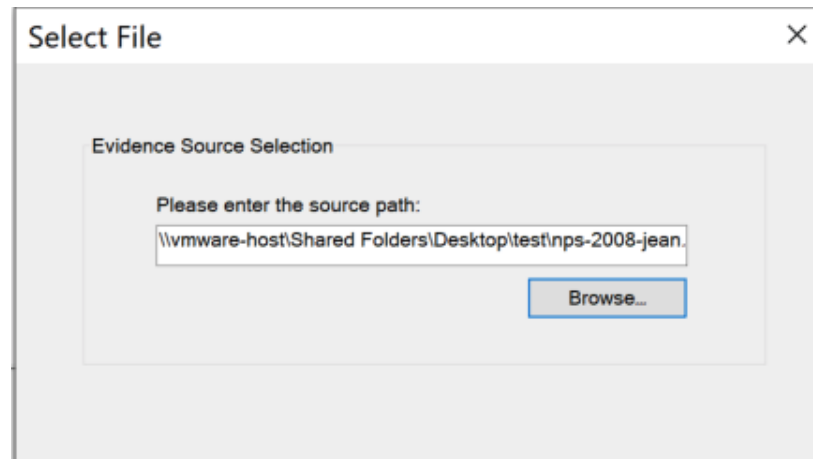
The FTK Imager by Access Data was utilized to view and analyze the data located within the Encase image files captured of the device belonging to CFO Jean Jones. The steps taken to achieve this action are listed below.

#### Adding the image file as an evidence item in the FTK Imager

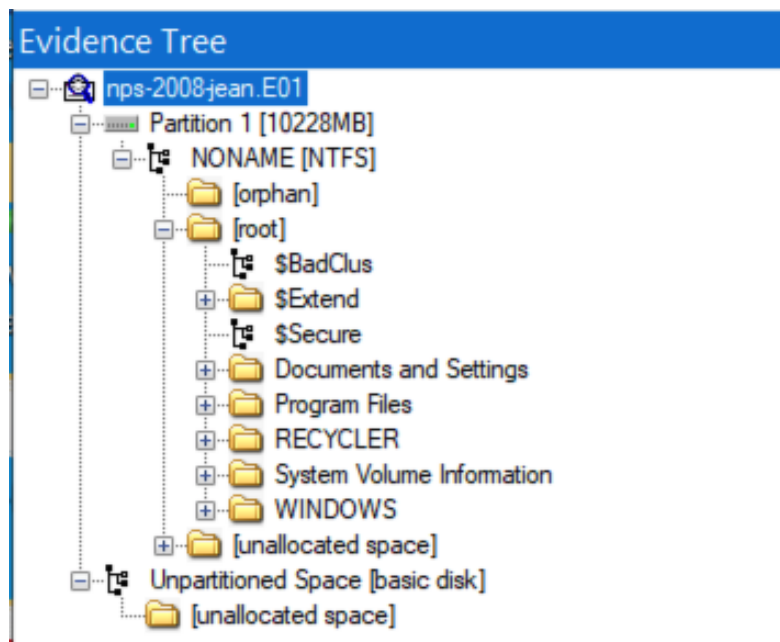
1. Open the FTK Imager application to begin the process of evidence analysis
2. To view the file in question, click "File" located in the top right corner then "Add Evidence Item."



3. Select “image file” as the source evidence type. Ensure both the E01 and E02 files are located in a single folder. Point to the E01 file within the folder. Once the correct location is pointed to in the source path click “finish.”



4. After minimal load time, the files should be visible in the Evidence Tree.



Understanding the data provided in the initial analysis

The following notes obtained from the personnel interviews and initial image overview serve as a roadmap for the specific areas which require further analysis in the investigation.




Specifically, this information discloses the need for a detailed review of the data found within Jean's email communications.

- i. CFO Jean Jones claims her reasoning behind making the spreadsheet was per request from President Allison Smith, e.g., *"Alison asked me to prepare the spreadsheet as part of new funding round."*
- ii. The President of the organization, Alison Smith, claims to have no idea what Jean is talking about, e.g., *"I don't know what Jean is talking about,"* and that she did not ask for the spreadsheet or receive it via email.
- iii. The spreadsheet in question, m57.biz, was located on the desktop of Jean's device.

The screenshot displays a forensic analysis interface. On the left, the 'Evidence Tree' shows a hierarchy starting from 'nps-2008:jean.E01' down to 'Partition 1 [10228MB]', 'NONAME [NTFS]', and finally to the 'Jean' user profile, where the 'Desktop' folder is highlighted. On the right, the 'File List' pane shows a table of files found on the desktop:

Name	Size	Type	Date Modified
AIM Tunes.url	1	Regular File	7/18/2008 4:30:4...
m57biz.xls	285	Regular File	7/20/2008 1:28:0...
m57biz.xls.FileSlack	3	File Slack	

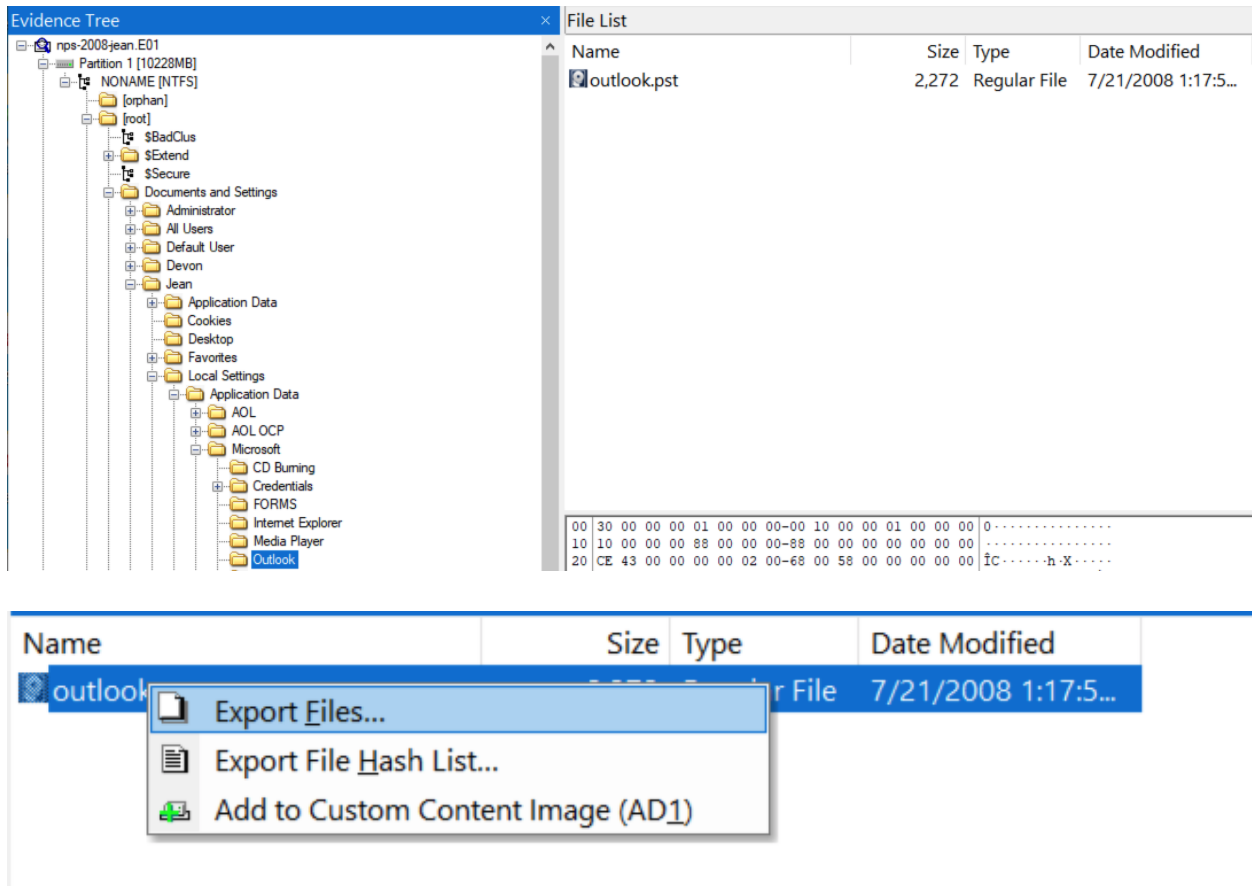
- iv. The file properties disclose the creation date of 07/20/2008.

Properties	
 	
	
Name	m57biz.xls
File Class	Regular File
File Size	291,840
Physical Size	294,912
Start Cluster	645,029
Date Accessed	7/20/2008 1:28:03 AM
Date Created	7/20/2008 1:28:03 AM
Date Modified	7/20/2008 1:28:03 AM
Encrypted	False
Compressed	False
Actual File	True
Start Sector	5,160,295

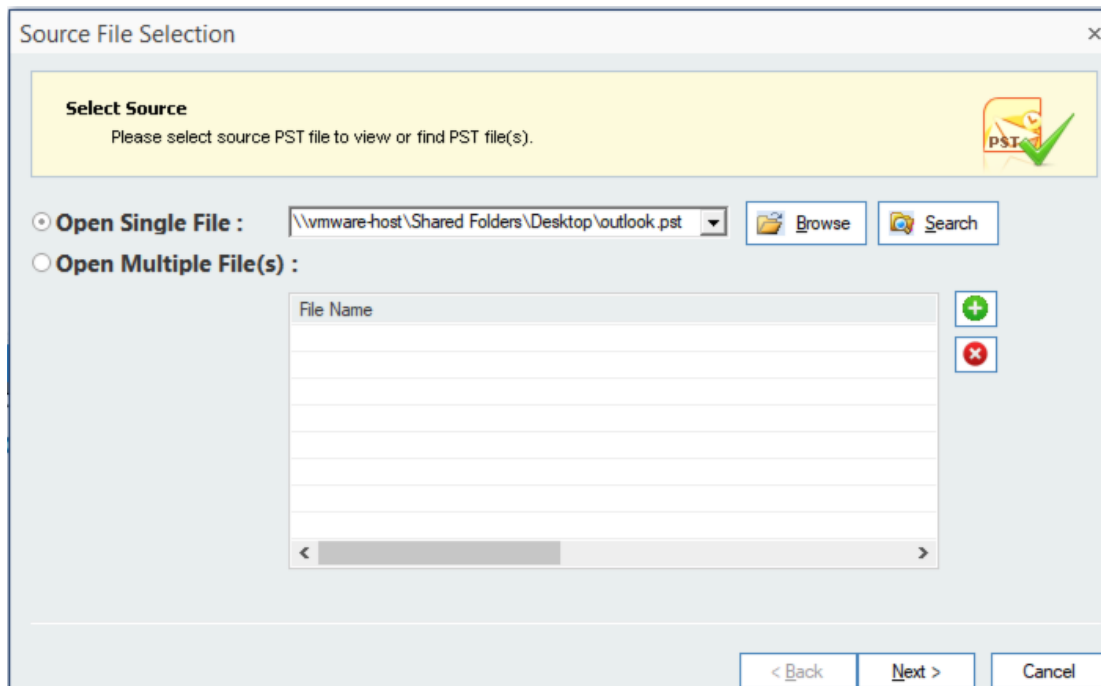
## Conducting the search on email communications

Based on the information provided in the initial analysis, a search was conducted on Jean's email outlook.pst file obtained via the FTK Imager and viewed using the Kernel Outlook PST Viewer. The steps were as follows:

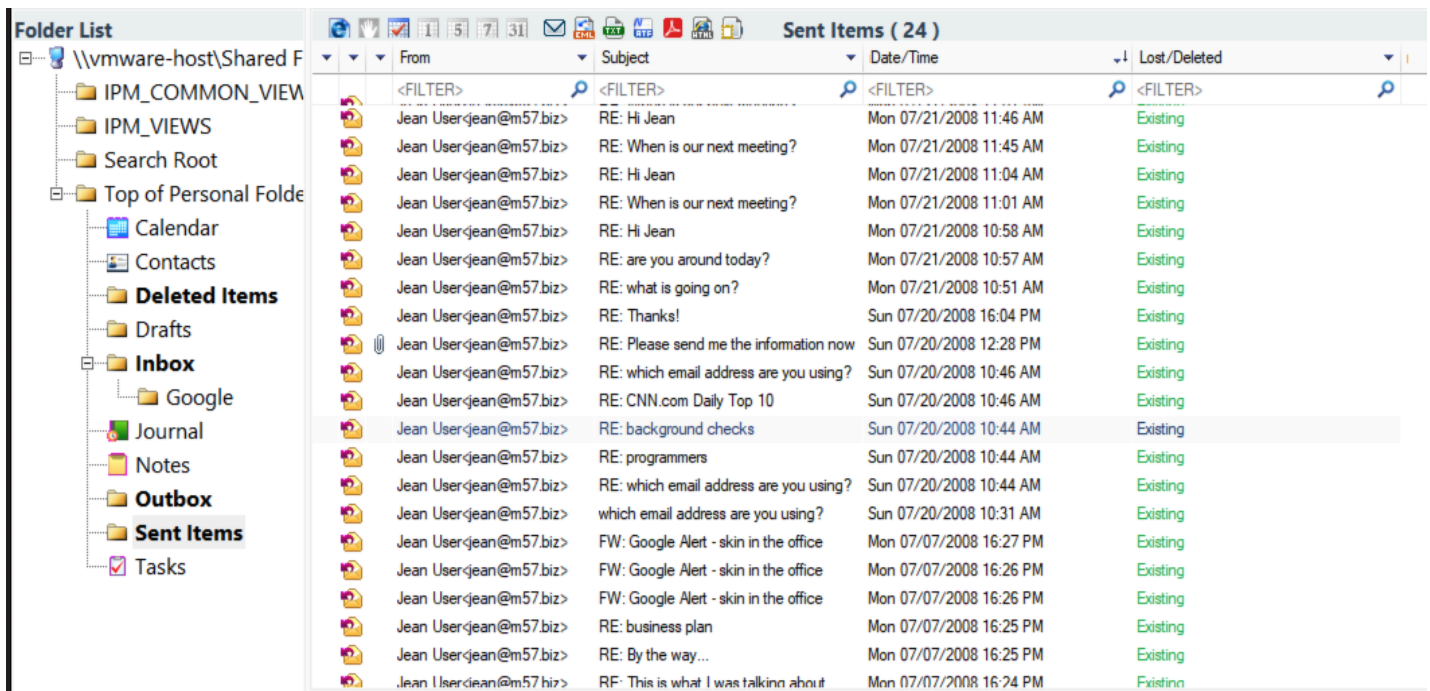
1. Locate and export the outlook.pst file within the FTK Imager.



- Open the single file within the Kernel Outlook PST Viewer and click "Next" then "Finish."



- Once successfully launched a folder list containing Jean's emails should appear.



### Discovering the Breach, a Comprehensive Timeline

Based on the data gained from the evidence provided, a comprehensive timeline was created that outlines the events leading to the exfiltration and the exfiltration itself.

- a. Sunday, July 20, 2008, at 10:39 AM Jean receives an email from who she believes to be Alison with the subject "background checks" requesting the confidential information in question.

**alison@m57.biz** <alison@m57.biz>  
To: jean@m57.biz

July 20, 2008.

background checks

---

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.)

The following correspondence does not show an obvious sign of spoofing; however, upon further inspection of the advanced properties in the email, it was uncovered that the return path for the sender was altered.

Property Type	Data
<FILTER>	<FILTER>
Extended ASCII string	SMTP
Extended ASCII string	alison@m57.biz
Extended ASCII string	background checks
Extended ASCII string	SMTP
Extended ASCII string	jean@m57.biz
Extended ASCII string	SMTP
Extended ASCII string	jean@m57.biz
Extended ASCII string	Return-Path: <simsong@xy.dreamhostps.com> X-Original-To: jean@m57.biz Delivered-To: x2789967@spunkymail m...
Binary data	00 00 00 00 81 2B 1F A4 BE A3 10 19 9D 6E 00 DD 01 0F 54 02 00 00 01 00 61 6C 69 73 6F 6E 40 6D 35 37 2E ...
Extended ASCII string	alison@m57.biz
Binary data	53 4D 54 50 3A 41 4C 49 53 4F 4E 40 4D 35 37 2E 42 49 5A 00
Extended ASCII string	SMTP
Extended ASCII string	alison@m57.biz
Extended ASCII string	jean@m57.biz

The malicious sender was sending emails from the address [simsong@xy.dreamhostps.com](mailto:simsong@xy.dreamhostps.com); however, the emails appeared to be coming from Alison's correct email address with a different cover name in Jean's inbox.

b. Sunday July 20, 2008, at 10:44 AM Jean replies to the background checks message.

The “reply to” portion of the “background checks” email was directed back to Alison’s legitimate inbox, so Allison received the response from Jean.

**RE: background checks**

Jean User <jean@m57.biz>

To: alison@m57.biz <alison@m57.biz>

Sun 07/20/2008 10:44 AM

Sure thing.

- c. Sunday July 20, 2008, at 10:50 AM Alison responds to Jean's message and discloses her confusion.

**alex <alison@m57.biz>**

**To: Jean User**

**RE: background checks**

---

What's a "sure thing." ?

-----Original Message-----

**From:** Jean User [mailto:jean@m57.biz]

**Sent:** Sunday, July 20, 2008 12:46 AM

**To:** alison@m57.biz

**Subject:** RE: background checks

Sure thing.

- d. Sunday July 20, 2008, at 12:22 PM Jean receives another email with the subject "Please send me the information now." The message contains the same malicious return path of [simsong@xy.dreamhostps.com](mailto:simsong@xy.dreamhostps.com); however this time the "reply to" portion of the email was spoofed to redirect to [tuckgorge@gmail.com](mailto:tuckgorge@gmail.com) instead of Alison's legitimate email. This is the email correspondence which reveals the malicious user spoofed their email to appear as Alison.
- e. Sunday July 20, 2008, at 12:28 PM Jean sends the spreadsheet to the spoofed email.



RE: Please send me the information now

Jean User <jean@m57.biz>

Sun 07/20/2008 12:28 PM

To: alison@m57.biz <tuckgorgne@gmail.com>

Attachments: m57biz.xls attachedFile.txt

I've attached the information that you have requested to this email message.

-----Original Message-----

From: alison@m57.biz [mailto:tuckgorgne@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

- f. Sunday July 20, 2008, at 4:03 PM Jean receives the final message from the attacker with the subject "Thanks!"

Thanks!

alison@m57.biz <tuckgorgne@gmail.com>

Sun 07/20/2008 16:03 PM

To: jean@m57.biz

## Conclusion

Based on the evidence unveiled throughout the analysis of Jean's hard drive the forensic investigation team was able to compose a comprehensive summary of the events that led up to the breach of confidential information regarding the employees of M57dotBIZ. These events, which occurred on Sunday, July 20, are how the attacker effectively infiltrated the organization's email communication system, obtained the information, and leaked the data to the competitors of M57dotBIZ.

1. President Alison Smith was the victim of a spear-phishing attack. Her email, [alison@m57.biz](mailto:alison@m57.biz), was attained and spoofed by a malicious attacker.
2. CFO Jean Jones was tricked into unveiling confidential information by the malicious attacker. She believed the request for information came from President Alison Smith.
3. Jean Jones unknowingly released the confidential information to a user at [tuckergorge@gmail.com](mailto:tuckergorge@gmail.com).

## Recommendations

The evidence displays that the attack occurred due to insecure email communication and a lack of security policy and controls. The organization is highly advised to read and implement these actions to prevent a future breach of this nature. The recommendations have been split into security controls and policy adjustments.

First and foremost, the attack targeted what is almost always the most insecure feature of a system, the human factor. What must be noted here is that the best and first defense against cybercriminals infiltrating an organization's system is employee awareness. In a security chain, the weakest link will always be an employee who is either unknowing or unaware of a potential attack and accepts each scenario at face value.

In our specific case, we see Jean does not pay much attention to Alison's confusion in her message reply regarding the background checks. On the other hand, Alison also does not take action once receiving the message, even with the subject containing the information "background checks." Jean's first response should have been to give Alison a call to confirm the information before the confidential documents were sent with such sensitive information at stake. Allison should also have checked in with Jean to confirm the reasoning for the message.

There are numerous ways to promote employee awareness in the workplace. Providing anti-fraud training is a great way to show employees how to recognize and prevent deception attacks. Employees should be trained on what information is confidential and pushed to understand that this information should never be released to anyone that does not have valid approval for needing it, even if they are in a higher ranked position. Access to said confidential information should be highly restricted. For this specific case, we see a significant lack of encryption which should have been placed not only on the email communications but on the data itself. Additionally, employees who have access to the organization's financial information or the authority to make payments on the organization's behalf should be closely monitored and regularly coached on all security policies and procedures. Most times, like in the situation for Jean, they are the primary targets for malicious attackers.

Next, a secure email system should be required and implemented. M57dotBIZ is a virtual corporation. Due to this factor, specific awareness of virtual security, especially surrounding their primary form of communication, needs to be in place. Two options are provided below that promote higher security within the organization's email communications and overall network if implemented.

First, it is strongly advised that the organization establish a Security Information and Event Management (SIEM) platform for overall network security, including email delivery (Petters, 2020). SIEM can be managed by a third party or in-house by hired system administrators depending on the company's needs.

Second, the organization should implement a Secure/Multipurpose Internet Mail Extension (S/MIME ) protocol. S/MIME is a broadly accepted and tested protocol used for

sending encrypted and digitally signed messages. Encryption protects the information within the message while the digital signature confirms the sender's identity. By setting up a secure email protocol, the organization can ensure encrypted email delivery for outgoing mail and digital signatures, which are used to authenticate the sender with a nonrepudiation policy so the receiver can authenticate that the sender is whom they say they are. Furthermore, any alterations made to the message while in transit after it has been signed will invalidate the signature. This aspect helps provide even greater assurance than signatures alone (Microsoft, 2021).

Finally, holding quarterly or semiannual audits of the network security infrastructure, including internal and external email communications and data integrity, will further educate and protect the organization from future breaches.

Through implementing and expanding on the recommended training and policies mentioned above, it is hoped that the organization will have the tools needed to detect and prevent a breach of this nature from occurring in the future.

## References

Abnormal. (2021, December 3). *Enhance Your Email Security Visibility Within Your SIEM*.

<https://abnormalsecurity.com/blog/enhance-your-email-security-visibility-within-your-siem>

AccessData. (2020). Imager User Guide. *Imager User Guide*, 10–

24. [https://ole.sandiego.edu/bbcswebdav/pid-2463021-dt-content-rid-34914640\\_1/xid-34914640\\_1](https://ole.sandiego.edu/bbcswebdav/pid-2463021-dt-content-rid-34914640_1/xid-34914640_1)

Crawford, V. (2013, November). *EXAMPLE OF AN EXPERT WITNESS DIGITAL FORENSIC REPORT*.

University of Technology (U-Tech), Jamaica.

Microsoft. (2021, August 20). *S/MIME in Exchange Online*. Microsoft Docs.

<https://docs.microsoft.com/en-us/exchange/security-and-compliance/smime-exo/smime-exo>

Petters, J. (2020, June 15). *What is SIEM? A Complete Beginner's Guide - Varonis*. Inside Out

Security. <https://www.varonis.com/blog/what-is-siem/>