M57 JEAN DIGITAL FORENSIC REPORT

Authors:
Muhammad Younas – 2022456
Muhammad Umar Magsood – 2022447
Shamina Durrani – 2022543
Affiliation:
Ghulam Ishaq Khan Institute of Science and Technology
Course: Digital Forensics – CY341
Instructor: Prof. Dr. Shahab Haider

Contents

Phase 1: Identification

Incident Recognition

This report details the forensic examination of CFO Jean Jones' laptop to investigate the unauthorized disclosure of sensitive employee data. The investigation cantered on validating Jean's claim that Alison Smith requested the spreadsheet via email, identifying potential phishing attempts, and reconstructing the timeline of events. Forensic tools such as FTK Imager and CoolUtils Outlook Viewer were employed to analyse disk images and email threads, ensuring adherence to chain-of-custody protocols.

Investigation Objectives

1. Confirm the source of the leaked data (Jean's M57.biz-owned laptop).
2. Validate Jean's claim of email communication with Alison.
3. Identify potential phishing or spoofing activities.
4. Assess compliance with GDPR due to PII exposure.

Phase 2: Collection/Preservation

Evidence Acquisition

- **Voluntary Surrender**: Jean's laptop was voluntarily submitted for forensic examination.
- **Forensic Imaging**: A write blocker was used to create a forensic clone of the hard drive (nps-2008-jean.E01).
-

Chain of Custody:

We preserved the integrity of evidence by adhering to a documented chain of custody (Table 1). Jean's laptop was voluntarily surrendered, and a forensic clone of its hard drive (nps-2008-jean.E01) was created using a write blocker. Two backup copies were stored securely, and MD5 hashes verified data integrity throughout the process.

Date	Time	Description
25/04/2025	12:38 PM	Downloaded nps-2008-jean.E01 and its subpart nps-2008-jean.E02 files from University of San Diego File Server to Analysis Machine's Hard Drive.
25/04/2022	02:12 PM	Copies of the forensic image were burnt into DVDROMs.
26/04/2025	07:26 AM	Forensic Image was imported to Access Data FTK Imager, and a verification scan was executed for data integrity, test successful.
26/04/2025	10:09 AM	User's emails were accessed and extracted from: 'nps-2008-jean.E01/Partition 1 [10228MB]/NONAME [NTFS]/[root]/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/Outlook.pst'
27/04/2025	12:45 PM	Extracted email profile file was verified for integrity.
27/04/2025	12:56 PM	Extracted emails were analyzed using CoolUtils Outlook Viewer.
02/05/2025	08:34 PM	Initial analysis was completed.
02/12/2025	07:53 AM	The report has been completed.

Table 1: Chain of Custody

Questions Asked Relevant to the Case

The case executive summary provided a lot of useful information, mainly that Jean claims her and Alison communicated via email regarding the spreadsheet. The following additional questions were brought forward:

1.Is Jean's computer system personal or is it owned by M57.biz?
2.Does Jean access email on any other device?
3.Does anyone else have access to Jean's laptop?
4.Did any employee use Jean's laptop before it being assigned to her?

These questions were answered before the investigation. We learned that Jean only accesses email on her laptop which is owned by M57.biz. She is the only user of this laptop and no one else has access to it.

Phase 3: Analysis

Tools and Methodology

- **Forensic Tools**: FTK Imager v4.7.3 (disk imaging), CoolUtils PST Reader 4.2.0.11 (email extraction).
- **OS**: Windows 11 Enterprise 24H2.

Key Findings

1. Email Spoofing and Phishing

- **Spoofed Domains**: Attackers used xy.dreamhostps.com and altered return paths (e.g., tuckgorge@gmail.com) to impersonate Alison.
- **Social Engineering**: Urgent requests (e.g., "Please do not mention this to anybody") and fabricated email "misconfigurations" manipulated Jean into sharing data.

2. Spreadsheet Metadata

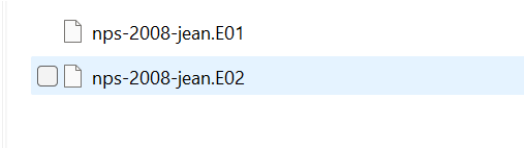
- **File Location**: Desktop/Documents and Settings/Jean/Application Data.
- **Tampering Indicators**: Creation and modification timestamps were two months apart, with Alison listed as the author.

Evidence to Search For

Based on the information gathered before the investigation, and the background questions asked, the analysis will focus on locating and analyzing email conversations on the laptop. Additionally, the confidential spreadsheet will need to be located, and its details need to be obtained. Deleted files and software will be scanned to see if any malware or spyware was installed on the laptop.

Examination Details

Jean's laptop was securely imaged without altering the original storage to preserve the integrity of the evidence. The disk image file was named nps-2008-jean.E01. The MD5 Hash for the evidence file is. The contents of Jean's laptop were not encrypted, and accessing the Outlook.pst file did not require any credentials; therefore, password cracking was not required.



Synopsis of Case Facts

The disk clone was stored in the Encase File Format. Although this file format is sometimes termed an E01 file format, this is a little bit of a misnomer as the official name of the file format is the Encase Image File Format. The disk image is divided into many files using this type usually around the 640 MB threshold. Each chunk starts with a header containing case information, then has a sequence of 32 KB data blocks, followed by cyclical redundancy checks after each data block, and ends with an MD5 sum for the full 640 MB chunk. These disk images will be divided into files with the extensions E01, E02, E03… EXX.

Since the spreadsheet in question was sent via email, the investigation narrowed down to examining the email trails first. The CoolUtils PST reader provides a standalone platform for opening PST files so that MS Outlook installation on a computer system is not necessary. The program enables users to view their messages, notes, contacts, drafts, and scheduled tasks. Outlook Viewer was utilized to examine the email conversations of Jean and Alison.

Timeline of events

Timestamps can be important pieces of evidence that can establish a connection between the accused and the computer and the offense for which it was used. Nevertheless, there are limitations on time and date stamps: They are restricted to a certain time zone, and the accuracy of the computer's internal clock directly affects their precision, which is also easily modifiable. Below timestamps and events in Table 2 were extracted from the evidence, and they correlate to Jean's local time zone, and the data had not been tampered with.

Highlights of the incident are as follows:

Date	Time	Description
07/19/2008	4:39:57 AM	Sensitive information has been requested to be sent via email. Subject: “background checks.”
07/19/2008	4:33:13 AM	Jean expresses skepticism and inquires through email about Alison using another email.
07/19/2008	4:50:20 AM	There is a confusion on why Jean sent “Sure thing,” which was previously to confirm sending of the data.
07/19/2008	6:22:45 AM	The threat actor urgently requests sensitive information again, the Return-Path has been altered to "tuckgorge@gmail.com".
07/19/2008	6:28:47 PM	Jean sends confidential information to the attacker via email.
07/19/2008	10:03:40 AM	The threat actor expresses gratitude to Jean for sharing the data.
07/20/2008	4:47:32 AM	Jean receives an email from Alison stating that something strange is going on.

Table 2: Timeline of the Events

Phase 4: Documentation

Process Records

- **Forensic Image Logs**: Detailed steps for cloning, hashing, and verification.
- **Email Extraction**: Paths and tools used to access Outlook.pst.
- **Timeline Analysis**: Correlated timestamps with system logs to validate authenticity.

Legal Compliance

- GDPR violations confirmed due to unauthorized PII disclosure.
- Chain-of-custody records ensure admissibility in legal proceedings.

Open the mounted image in FTK imager

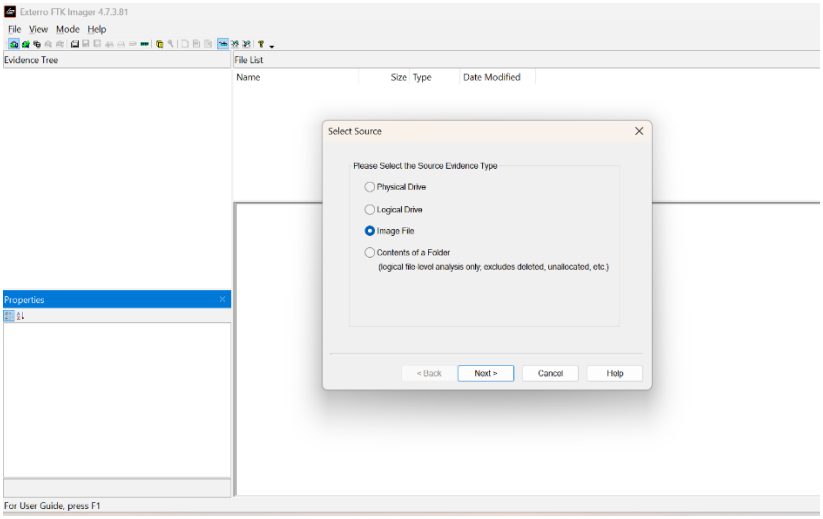


Figure 1: Open FTK Imager

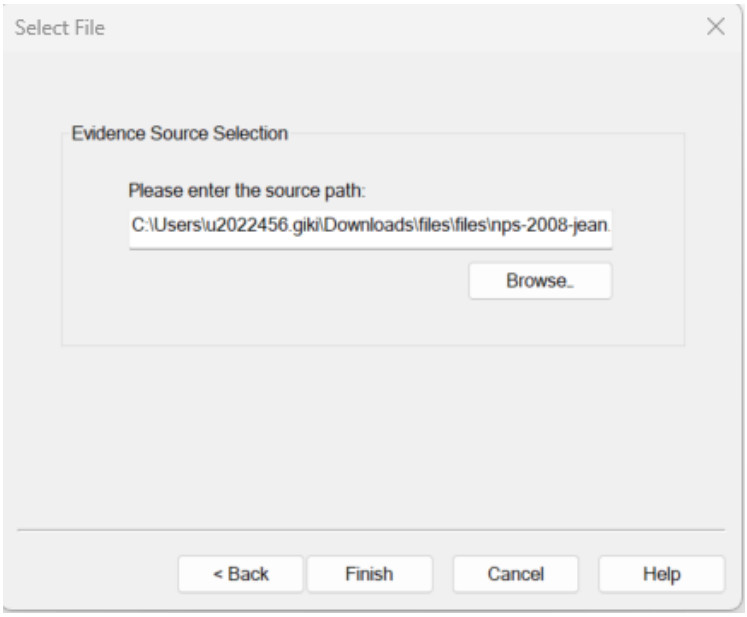


Figure 2: Select the Evidence Image

Verifying the Integrity of the Forensic Image:

One of the most used hash algorithms is the 128-bit MD5 algorithm. It was intended to be used as a cryptographic hash function, but due to the risk of vulnerabilities being exploited, it is now solely used to verify data integrity. Forensic images have a considerable potential of being altered or damaged, throughout the chain of custody. Encase (*.E01) files store the hash inside the file at image creation, making it possible to compare the Stored verification

hash and the computed hash. It should be explicitly stated that for the evidence to be usable to the investigation, the hash tags must match.

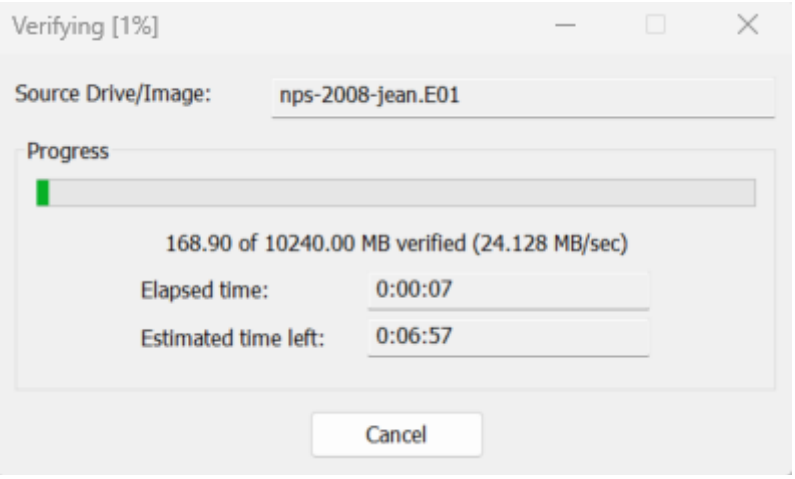


Figure 3: Mounted Image file was verified for Integrity

Verification scans confirmed that the hashes matched, and the data had not been tempered with, hence the data can be presented to the court as evidence.

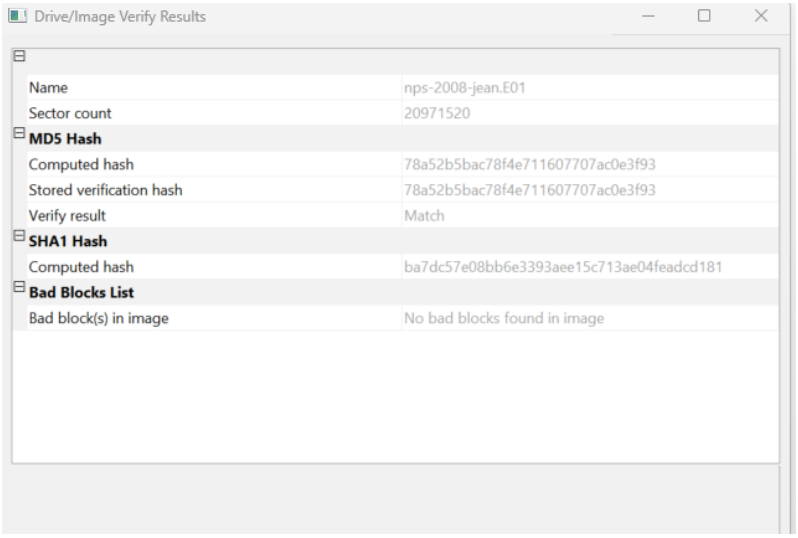


Figure 4: Hashes Matched

The following are the image details:

Image	
Image Type	E01
Case number	
Evidence number	2008-M57-Jean
Examiner	Donny
Notes	
Acquired on OS	Darwin
Acquired using	20101104
Acquire date	1/31/2011 4:38:29 PM
System date	1/31/2011 4:38:29 PM
Unique description	Jean's hard drive from the first M57 project

Figure 5: Image Details

We have extended the image files in FTK imager and we found that the image have only one partition, inside which there are files and directories, upon researching we have found that the image has one directory named “Documents and Settings” inside which there is directory named “Jean”, open it and have found another directory named "Application Data” inside there, there is new directory named “ Desktop” open it and found the confidential file which has been compromised and posted on the competitor website.

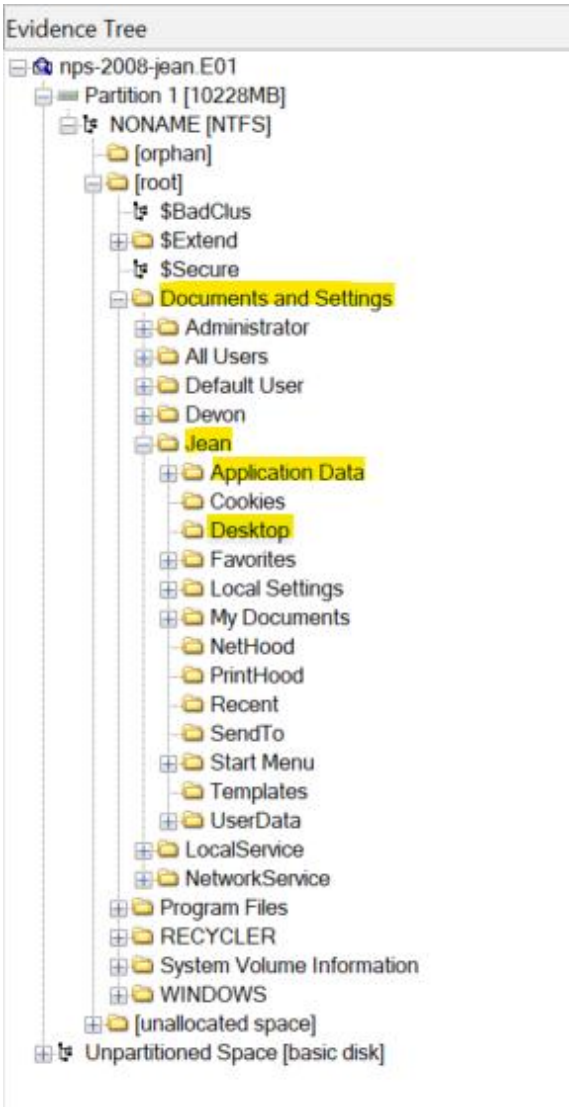


Figure 6: Nested Directory inside mounted Image

Confidential spreadsheet inside Desktop Directory

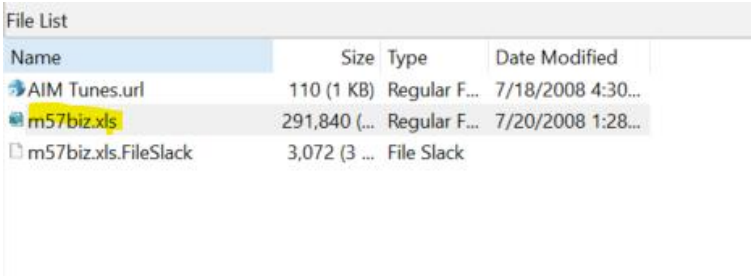


Figure 7: Compromised File

We have exported the file to our local machine and check its properties. The spreadsheet that contains details about an employee's social security number and salary details is seen in the image below.

M57.biz company

Name		Position	Salary	SSN (for background check)
Alison	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	Counterching	Outreach	240,000	123-45-6789
Annual Salaries			$1,009,000	
Benefits		30%	$302,700	
Total Salaries + Benefits			$1,311,700	
Monthly burn			########	

Figure 8: The leaked spreadsheet with confidential information

The document's creation time and its last saved times are two months apart, which is unusual, and the file contains Allison as the Author of the file. Additionally, it indicates that Alison created the file two months ago.

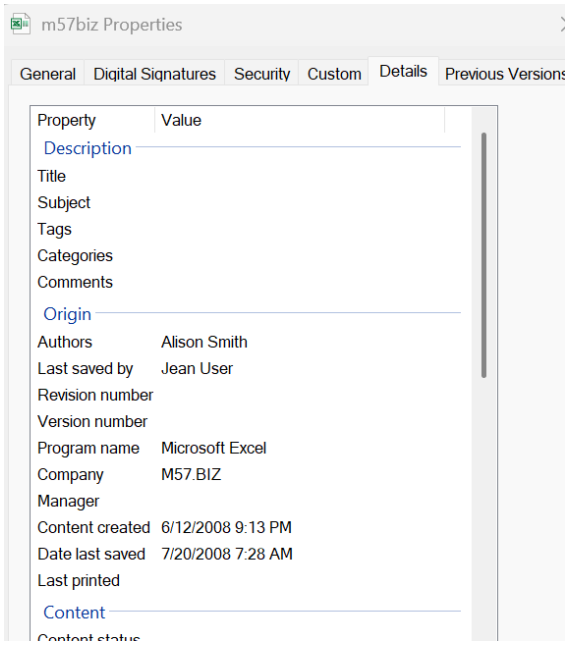


Figure 9: Properties of the leaked spreadsheet

Given that the emails sent between Jean and Alison and other pertinent individuals are the primary focus of the inquiry. The email account of the company's CEO, Jean, which is jean@m57.biz was analyzed, and the platform

she uses for email clients is Microsoft Outlook. The organization's domain is M57.biz, as apparent from the email address, which is reserved for the purpose of authority and is in line with strict strategies/policies and safety measures provided by the organization.

A threat actor had spoofed the organization emails in a spear phishing attack, to target the CFO, Jean, into disclosing confidential data. The details requested are Personally identifiable information and should not be disclosed to 3rd parties without reviewing a MSA and doing proper vendor security assessments. In this scenario, the sense of urgency and the suspicious request not to disclose the task to anyone are red flags, confirming this could be a phishing email.

The email domain had been spoofed, and the return path was later changed to tuckgorge@hotmail.com which originated from the xy.dreamhostps.com domain, , (Please see Appendix x), leaking the confidential information.

List of the Criminal Offense:

We have found another file in the same directory Jean, folder name "Local Settings" inside this folder there another folder named is "Microsoft", inside this folder we found a folder called "Outlook" and upon checking we have found that there an Outlook email format file, exported it and open it with CoolUtils Outlook Viewer.

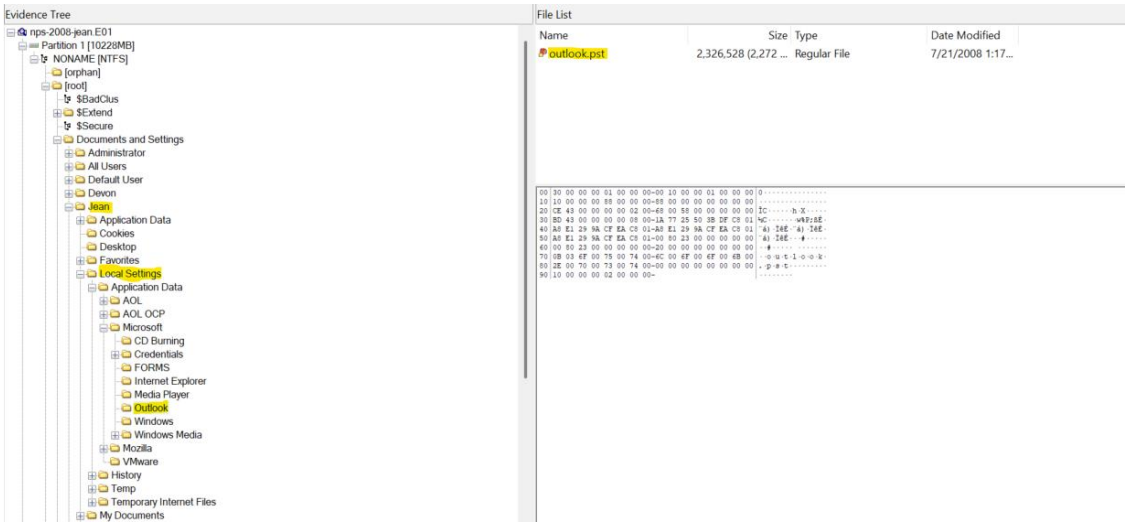


Figure 10: Email File

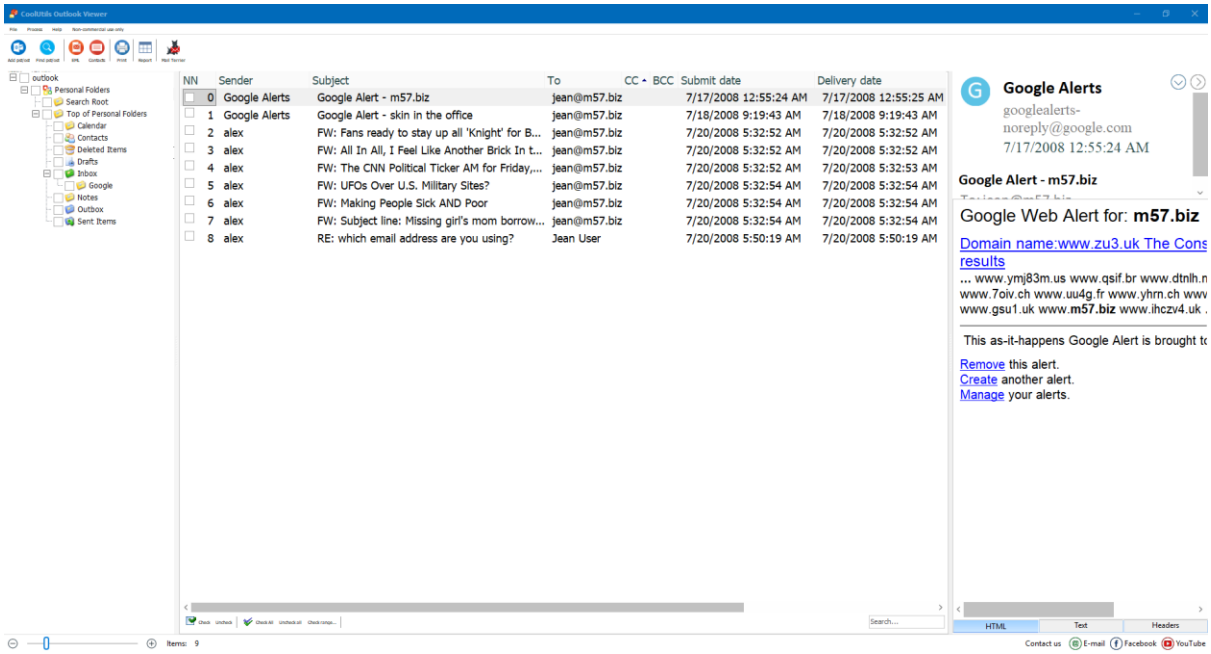


Figure 11: Open Email file in CoolUtils Outlook Viewer

In deleted tab there as an email sujected “RE: which email address are you using?”

```
-----Original Message-----
From: Jean User [mailto:jean@m57.biz]
Sent: Sunday, July 20, 2008 12:32 AM
To: alison@m57.biz
Subject: which email address are you using?


Are you going to use alex@m57.biz or alison@m57.biz?
```

Figure 12: first message from Jean

```
-----Original Message-----
From: alex [mailto:alex@m57.biz]
Sent: Sunday, July 20, 2008 12:33 AM
To: Jean User; alison@m57.biz
Subject: RE: which email address are you using?


This one, obviously.
```

Figure 13: Reply to first email by alex@m57.biz

```
Yes, I got this email.


-----Original Message-----
From: Jean User [mailto:jean@m57.biz]
Sent: Sunday, July 20, 2008 12:46 AM
To: alex
Subject: RE: which email address are you using?


So are you going to get this email?


-----Original Message-----
From: alex [mailto:alison@m57.biz]
Sent: Sunday, July 20, 2008 12:44 AM
To: Jean User
Subject: RE: which email address are you using?



Whoops. It looks like my email was misconfigured.

My email is alison@m57.biz, not alex. Sorry about that.
```

Figure 14: Ongoing Emails

Summary:

Below is the summary of the email conversation above subjected “RE: which email address are you using?”

Timeline:

- **12:32 AM** – Jean questions which email Alison is using.
- **12:33 AM** – A response from **alex@m57.biz** claims "This one, obviously" and includes both Jean and alison@m57.biz in recipients.
- **12:44 AM** – A message from **alison@m57.biz** clarifies the email was misconfigured and "alison@m57.biz" is the real one.
- **12:46 AM** – Jean replies with skepticism, asking if this email will be received.

1. Jean User (jean@m57.biz) initiates:
“Are you going to use alex@m57.biz or alison@m57.biz?”
This shows Jean is confused about which email address Alison is using — possibly because of inconsistent sender info.

---

2. Reply from "alex@m57.biz":
“This one, obviously.”

This reply seems abrupt and evasive. Someone using alex@m57.biz responds but gives no clarity. Note: This could be a case of **spoofing** or someone intentionally using a different alias.

---

3. Follow-up from "alex" (alison@m57.biz):
“My email is alison@m57.biz, not alex. Sorry about that.”
Here, "Alison" admits she mistakenly sent from the alex@m57.biz account — which raises red flags. She's acknowledging that her configuration caused her emails to come from an **incorrect alias**.

---

4. Jean replies again:
“So are you going to get this email?”
Jean still seems unsure if the message is reaching the correct recipient, possibly due to conflicting headers or suspicious sender info.

---

5. Final confirmation:
“Yes, I got this email.”
Alison (or whoever is responding) confirms receipt — but the confusion remains.

Forensic Observations:

- The attacker (likely **alex@m57.biz**) inserted themselves between Jean and Alison.
- The attacker tried to impersonate Alison or sow confusion using multiple aliases.
- The "misconfiguration" excuse is a classic **social engineering tactic** to bypass suspicion.

Email Thread Analysis – Potential Impersonation Attempt

On July 20, 2008, a suspicious email thread occurred involving Jean and an individual posing as Alison. The attacker, using the alias **alex@m57.biz**, responded to Jean’s query before the legitimate user **alison@m57.biz** could reply. The real Alison later clarified the email mix-up. This sequence suggests an impersonation or spoofing attempt to manipulate Jean into trusting the attacker’s identity.

In Inbox there are some emails which are looking very suspicious

Sensitive information has been requested to be sent via email. Subject: “background checks.”

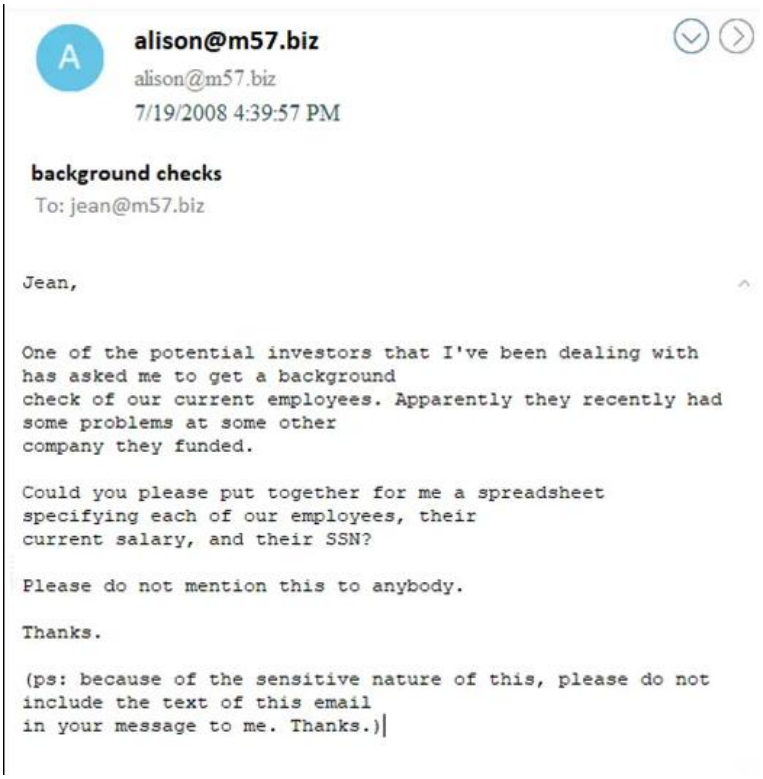


Figure 15: Background Check Email: Initial

There is a confusion on why Jean sent “Sure thing,” which was previously to confirm sending of the data.

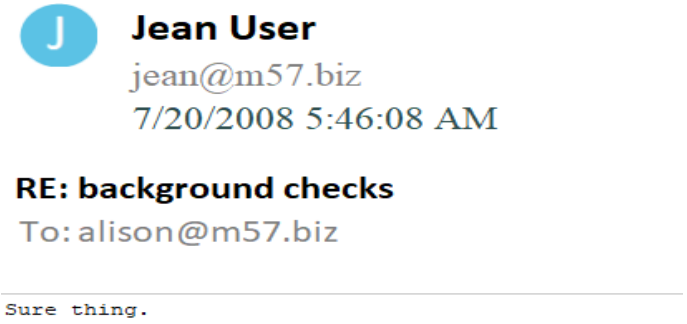


Figure 16: email: RE: background checks: last

Header analysis of phishing emails

```
Return-Path: <simsong@xy.dreamhostps.com>
X-Original-To: jean@m57.biz
Delivered-To: x2789967@spunkymail-mx8.g.dreamhost.com
Received: from smarty.dreamhost.com (sd-green-bigip-81.dreamhost.com [208.97.132.81])
        by spunkymail-mx8.g.dreamhost.com (Postfix) with ESMTP id E32634D80F
        for <jean@m57.biz>; Sat, 19 Jul 2008 16:39:57 -0700 (PDT)
Received: from xy.dreamhostps.com (apache2-xy.xy.dreamhostps.com [208.97.188.9])
        by smarty.dreamhost.com (Postfix) with ESMTP id 6E408EE23D
        for <jean@m57.biz>; Sat, 19 Jul 2008 16:39:57 -0700 (PDT)
Received: by xy.dreamhostps.com (Postfix, from userid 558838)
        id 64C68381DAE; Sat, 19 Jul 2008 16:39:57 -0700 (PDT)
To: jean@m57.biz
From: "alison@m57.biz" <alison@m57.biz>
Subject: background checks
Message-ID: <20080719233957.64C68381DAE@xy.dreamhostps.com>
Date: Sat, 19 Jul 2008 16:39:57 -0800

Content-Type: text/plain; charset=us-ascii

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.
```

Figure 17: Headers of phishing email "background checks"

The threat actor urgently requests sensitive information again, the Return-Path has been altered to "tuckgorge@gmail.com".

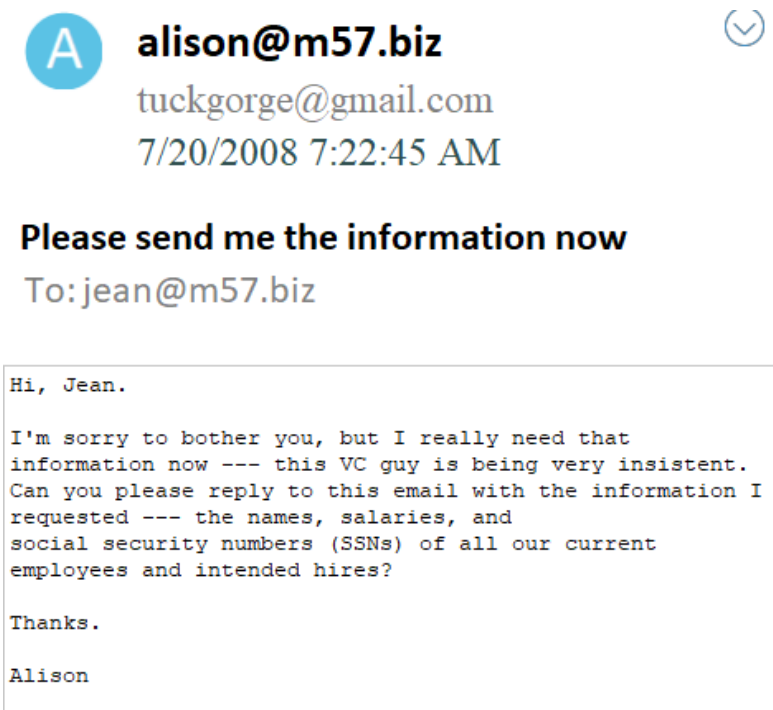
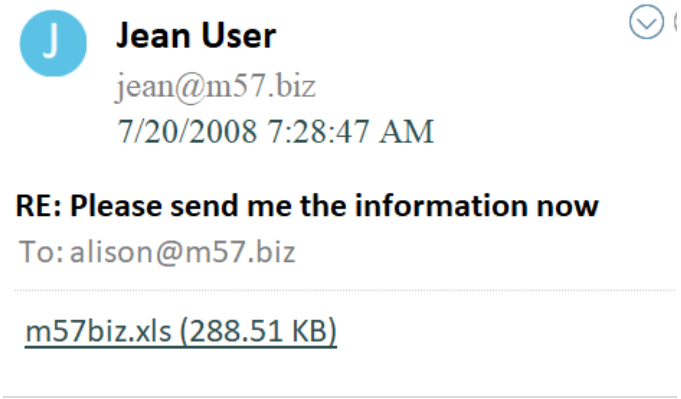


Figure 18: email: Please send me the information now

Jean sends confidential information to the attacker via email.



Jean User
jean@m57.biz
7/20/2008 7:28:47 AM

RE: Please send me the information now
To: alison@m57.biz

m57biz.xls (288.51 KB)

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

Figure 19: email: RE: Please send me the information now

Header analysis of phishing emails

```
Return-Path: <simsong@xy.dreamhostps.com>
X-Original-To: jean@m57.biz
Delivered-To: x2789967@spunkymail-mx2.g.dreamhost.com
Received: from smarty.dreamhost.com (sd-green-bigip-66.dreamhost.com [208.97.132.66])
        by spunkymail-mx2.g.dreamhost.com (Postfix) with ESMTP id 2D1DC7278E
        for <jean@m57.biz>; Sat, 19 Jul 2008 18:22:45 -0700 (PDT)
Received: from xy.dreamhostps.com (apache2-xy.xy.dreamhostps.com [208.97.188.9])
        by smarty.dreamhost.com (Postfix) with ESMTP id 138E5EE221
        for <jean@m57.biz>; Sat, 19 Jul 2008 18:22:45 -0700 (PDT)
Received: by xy.dreamhostps.com (Postfix, from userid 558838)
        id 177343B1DA8; Sat, 19 Jul 2008 18:22:45 -0700 (PDT)
To: jean@m57.biz
From: "alison@m57.biz" <alison@m57.biz>
Subject: Please send me the information now
Message-ID: <20080720012245.177343B1DA8@xy.dreamhostps.com>
Date: Sat, 19 Jul 2008 18:22:45 -0800

Content-Type: text/plain; charset=us-ascii

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
```

Figure 20: Headers of email : "please send me the information now"

The threat actor expresses gratitude to Jean for sharing the data.

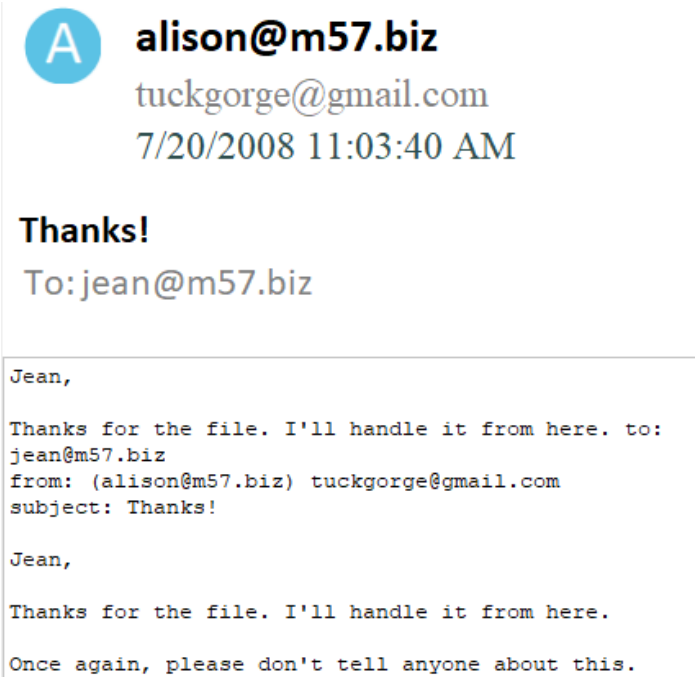


Figure 21: email: Thanks

There is a confusion on why Jean sent "Sure thing," which was previously to confirm sending of the data.

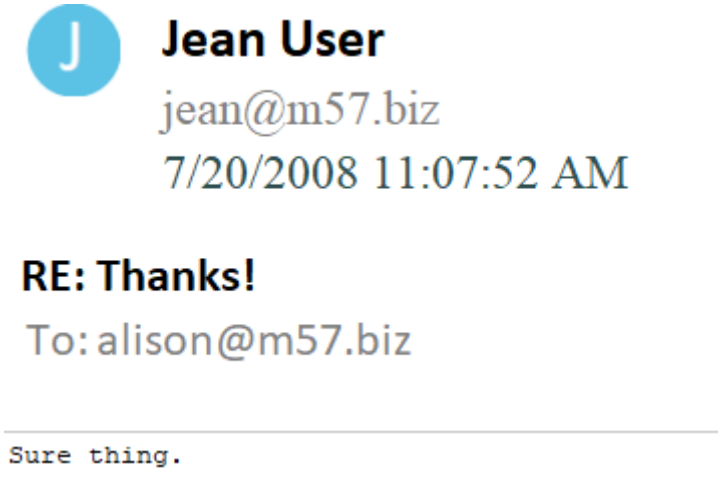


Figure 22: email: RE: Thanks!

Jean receives an email from Alison stating that something strange is going on.

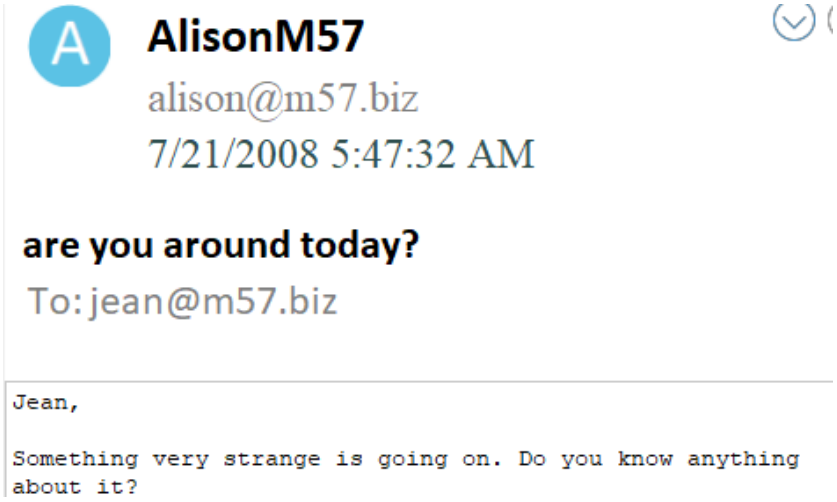


Figure 23: email: are you around today?

Phase 5: Presentation

Executive Summary:

M57.biz, a startup specializing in online body art collections, experienced a data breach when a confidential employee spreadsheet was leaked on a competitor's forum. The spreadsheet originated from the laptop of CFO Jean Jones, who asserted that CEO Alison Smith requested the document via email for a funding round. Alison denied involvement, prompting a forensic investigation of Jean's laptop. Our analysis focused on email communications, file metadata, and potential phishing activities to determine the breach's origin.

Conclusion:

We conclude that Jean Jones was a victim of a spear-phishing attack, not a willing participant in the data breach. Key factors include:

1. **Spoofed Communications**: Attackers mimicked Alison's identity to solicit confidential data.
2. **Lack of Technical Expertise**: Jean's accounting background limited her ability to detect email anomalies.
3. **GDPR Violation**: The breach exposed PII, highlighting insufficient organizational cybersecurity measures.

Recommendation: While Jean's actions violated her NDA, we attribute the breach to phishing rather than malice. We recommend cybersecurity training for employees and enhanced email authentication protocols for M57.biz.