

Please make sure you answer these three essential questions which are worth 33.33 points each. I am adding this addendum so that you understand 100% what I am looking for and how you will be graded. Each question should be answered explicitly in writing with a narrative of at least eight sentences describing the evidence you found and why/how it is related to your response. Demonstrate how you see the evidence from an investigator's point of view i.e does it implicate anyone? Also explain the forensic tool(s) you used and the advantages or disadvantages of using this tool. Additionally, you should show the path and evidentiary exhibit(s) with your responses. You can use any forensic tool want!!

1. When was the spreadsheet created? Who created the spreadsheet?

Answer:

File Name: m57biz.xls (Verified with data shown in PPT file)

MD5: E23A4EB7F2562F53E88C9DCA8B26A153

Author: Alison Smith (President)

Creation Date: 12th June 2008 (11:13 AM)

Last modify by User: Jean (CFO)

Last Modification date: 19th July 2008 (9:28 PM)

Method:

The investigation utilized **Autopsy** and **Paraben** tools for cross-verification. The **M57-Jean.ppt** case material provided key information, including the spreadsheet m57plan.xlsx data.

1. Autopsy:

- Using the **Keyword Search** feature, a search was conducted on 140,000 values derived from the case material to locate the spreadsheet.

2. Paraben:

- The **Advanced Search** feature was used to verify the 140,000 values, ensuring results were consistent with those obtained in Autopsy.

Both tools were applied to validate the evidence, confirming the accuracy of the findings.

Name	Smith	Position	Salary	SSN (for background check)
Allison	Smith	President	\$140,000	03-44-3134
Jean	Jones	CFO	\$120,000	32-34-6432
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	Counterch	Outreach	240,000	123-45-6789
Annual Salaries			\$1,009,000	
Benefits			30%	\$302,700

Tool	Autopsy	Paraben Corporation's E3
Search For Keyword		
Results for Keyword Search		

Checking Content of m57biz.xls

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	Counterchinq	Outreach	240,000	123-45-6789	
Annual Salaries					
Benefits			30%	\$1,009,000	
				\$302,700	
Total Salaries + Benefits				\$1,311,700	
Monthly burn				\$109,308.33	



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	Counterchinq	Outreach	240,000	123-45-6789	
Annual Salaries					
Benefits			30%	\$1,009,000	
				\$302,700	
Total Salaries + Benefits				\$1,311,700	
Monthly burn				\$109,308.33	



File Location: /img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Desktop/m57biz.xls

e3://Quiz 2 (620)/nps-2008-jean/Partition Parser/Partition63/*binary_file/NTFS/Root /Documents and Settings_3519/ Jean_16144/Desktop_16176?item=m57biz.xls_32712

MD5: E23A4EB7F2562F53E88C9DCA8B26A153

E23A4EB7F2562F53E88C9DCA8B26A153

Properties from Tools for MD5:

/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Desktop/m57biz.xls - Editor	
/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Desktop/m57biz.xls	
Hex	Text
Application	Message
File Metadata	Context
Results	Annotations
Other Occurrences	
Name	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings
Type	File System
MIME Type	application/vnd.ms-excel
Size	291840
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2008-07-19 21:28:03 EDT
Accessed	2008-07-19 21:28:03 EDT
Created	2008-07-19 21:28:03 EDT
Changed	2008-07-19 21:28:04 EDT
MD5	e23a4eb7f2562f53e88c9dca8b26a153
Hash Lookup Results	UNKNOWN
Internal ID	4036

Windows	m57biz.xls
NTFS	
Size (bytes)	
Allocated size (b)	294,912
Complete file size	291,840
File size (bytes)	291,840
Sort Results	
File Name	m57biz.xls
File Path	Quiz 2 (620)/nps-2008-jean/Partition Parser/F
MD5	E23A4EB7F2562F53E88C9DCA8B26A153
Protection	Not detected
Recovery Option	Not available
SHA1	55638AF43DDDD0F1FF8CD4DAB73B2979AC5
SHA-256	

Metadata of file:

m57biz Desktop

Upload

Share

Copy path

Open file location

Read-Only Workbook

Save As

Compatibility Mode

Protect Workbook

Inspect Workbook

Properties

Size

Title

Tags

Categories

Related Dates

Last Modified

Created

Last Printed

Related People

Author

Last Modified By

m57biz Desktop

Upload

Share

Copy path

Open file location

Compatibility Mode

Protect Workbook

Inspect Workbook

Properties

Size

Title

Tags

Categories

Related Dates

Last Modified

Created

Last Printed

Related People

Author

Last Modified By

Author:	Alison Smith	Alison Smith
Creation Date:	12 th June 2008 (11:13 AM)	12 th June 2008 (11:13 AM)
Last Modification Date:	19 th July 2008 (9:28 PM)	19 th July 2008 (9:28 PM)
Last Modified by User:	Jean User	Jean User

Narrative (Investigator's Point of View):

The investigation into the spreadsheet m57biz.xls reveals critical details from both **Excel's internal metadata** and the external file system metadata provided by **Autopsy** and **Paraben** tools.

- Creation Date (Verified from Excel's Metadata):** The internal metadata of the Excel file confirms that the spreadsheet was originally created on **June 12, 2008, at 11:13 AM** by **Alison Smith**, the President of M57.biz. This timestamp confirms that Alison was the initial creator of the document, likely related to the company's financial activities as discussed in the case material.
- Last Modification (Verified from File System Metadata):** The last modification to the spreadsheet occurred on **July 19, 2008, at 9:28 PM**, by **Jean**, the company's CFO. This is evident from the file system metadata retrieved using **Autopsy** and **Paraben** tools. This modification indicates Jean had access to the document and made changes close to the time when the file was exfiltrated, which could potentially implicate her in the unauthorized transfer of this sensitive document.

This timeline highlights the handoff of the document between **Alison** (who created it) and **Jean** (who modified it), providing insight into the workflow within M57.biz and potentially uncovering Jean's involvement in the exfiltration.

Exhibit Path:

- File Location in Autopsy:** /img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Desktop/m57biz.xls
- File Location in Paraben:** e3://Quiz 2 (620)/nps-2008-jean/Partition Parser/Partition63/*binary_file/NTFS/Root /Documents and Settings_3519/ Jean_16144/ Desktop_16176?item=m57biz.xls_32712

Autopsy vs. Paraben in the M57.biz Case

In the M57.biz exfiltration case, both **Autopsy** and **Paraben E3** played essential roles in finding, exporting, and verifying the file m57biz.xls. However, neither tool could provide the **correct creation date** or **author details**, which were confirmed through **Microsoft Excel** itself. Here's how each tool contributed:

Autopsy's Role in Our Case:

- File Discovery:**
 - Autopsy was used to locate the spreadsheet m57biz.xls through its **keyword search** feature.
 - This feature allowed us to search the disk for references to the file name, leading to the identification of the correct file.
- File Export and MD5 Verification:**
 - Once the file was located, Autopsy was used to **export the file**.
 - Autopsy also helped generate an **MD5 hash** of the file, which was crucial for verifying the integrity of the file throughout the investigation. The MD5 hash, E23A4EB7F2562F53E88C9DCA8B26A153, was consistent across both tools.
- Limitation:**
 - Autopsy could not provide the **internal metadata** of the file (creation date or author details), as it focuses on **file system metadata** (e.g., modification dates based on when the file was accessed or modified on the system).

Paraben's Role in Our Case:

1. File Discovery and Export:

- Similar to Autopsy, Paraben's **advanced search feature** helped locate the m57biz.xls file by scanning across partitions.
- Once the file was found, Paraben was used to **export the file** for further examination.

2. MD5 Verification:

- Paraben generated the same **MD5 hash** as Autopsy (E23A4EB7F2562F53E88C9DCA8B26A153), ensuring that the file was consistent across both tools, confirming its integrity.

3. Limitation:

- Like Autopsy, Paraben did not provide the **correct creation date** or **author information** from the Excel file. It is primarily designed for handling **file system metadata** and forensic analysis, not internal document properties.

Microsoft Excel's Role in Our Case:

1. Internal Metadata Extraction:

- The correct creation date of **June 12, 2008**, and the original author, **Alison Smith**, were only confirmed by opening the file in **Microsoft Excel**.
- Excel's internal properties provided the **true creation date** and **author details** that neither Autopsy nor Paraben could retrieve.

Key Differences:

• Autopsy and Paraben:

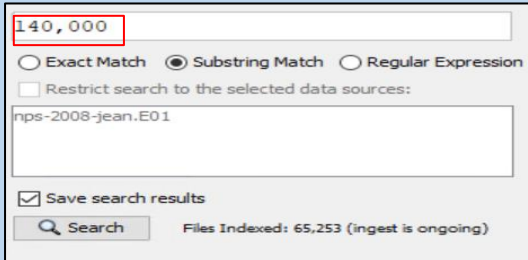
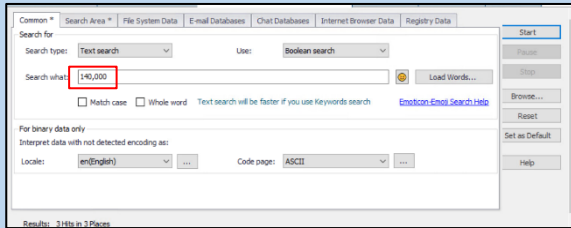
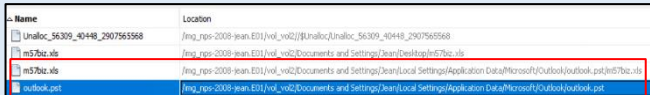
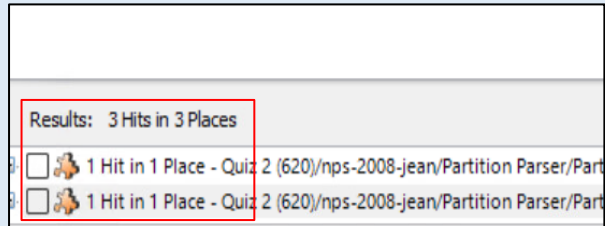
- Both tools were instrumental in **finding** and **exporting the file**.
- Both provided **MD5 hash verification** to ensure the file's integrity.
- Neither tool could retrieve the **internal document metadata** (creation date and author) directly from the Excel file.

• Microsoft Excel:

- Only **Microsoft Excel** could provide the actual **internal metadata** (creation date and author details) embedded in the Excel document.

2. How did the document get to the competitor's website?

Method: We are applying a similar keyword search process in both Autopsy and Paraben E3 as was done for the first question. The goal is to determine how the document (m57biz.xls) was exfiltrated to the competitor's website.

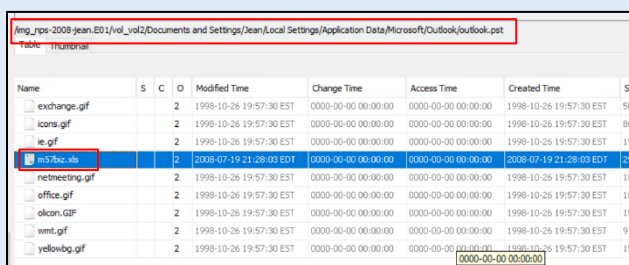
Tool	Autopsy	Paraben Corporation's E3
Search For Keyword		
Results for Keyword Search		

Location of Email Conversation (File):

/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst/m57biz.xls

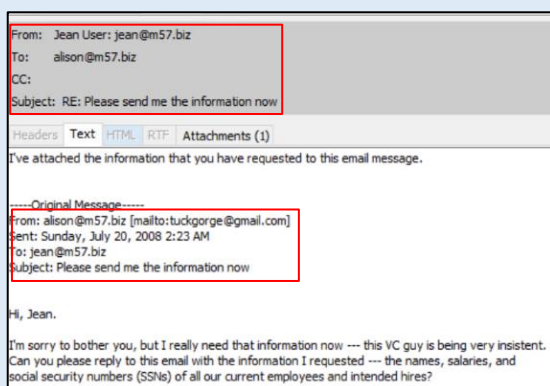
e3://Quiz 2 (620)/nps-2008-jean/Partition Parser/Partition63/*binary_file/NTFS/Root/Documents and Settings_3519/Jean_16144/Local Settings_16159/Application Data_16169/Microsoft_16170/Outlook_17341/outlook.pst_17358/\$DATA3/*binary_file/Outlook Personal Storage/mbx#00000000000008022/mbx#00000000000008022:fld#000000000000080c2/fld#000000000000080c2:msg#0000000000202184/Attachments?item=att#00000000

Locating the Email:

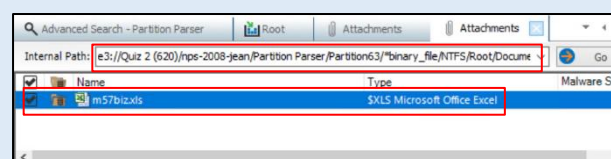
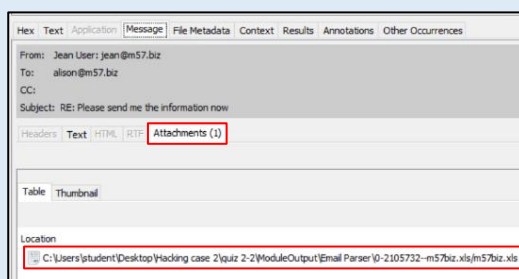


Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
exchange.gif	2			1998-10-26 19:57:30 EST	0000-00-00 00:00:00	0000-00-00 00:00:00	1998-10-26 19:57:30 EST	50
icons.gif	2			1998-10-26 19:57:30 EST	0000-00-00 00:00:00	0000-00-00 00:00:00	1998-10-26 19:57:30 EST	86
ie.gif	2			1998-10-26 19:57:30 EST	0000-00-00 00:00:00	0000-00-00 00:00:00	1998-10-26 19:57:30 EST	18
m57biz.xls	2			2008-07-19 21:28:03 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2008-07-19 21:28:03 EDT	29
netmeeting.gif	2			1998-10-26 19:57:30 EST	0000-00-00 00:00:00	0000-00-00 00:00:00	1998-10-26 19:57:30 EST	18
office.gif	2			1998-10-26 19:57:30 EST	0000-00-00 00:00:00	0000-00-00 00:00:00	1998-10-26 19:57:30 EST	18
olicon.gif	2			1998-10-26 19:57:30 EST	0000-00-00 00:00:00	0000-00-00 00:00:00	1998-10-26 19:57:30 EST	15
wmt.gif	2			1998-10-26 19:57:30 EST	0000-00-00 00:00:00	0000-00-00 00:00:00	1998-10-26 19:57:30 EST	91
yellowbg.gif	2			1998-10-26 19:57:30 EST	0000-00-00 00:00:00	0000-00-00 00:00:00	1998-10-26 19:57:30 EST	15

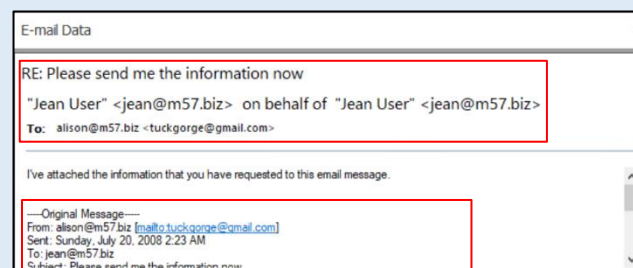
Select the Excel and Select Window from top left bar and select option named select content and go to message category:



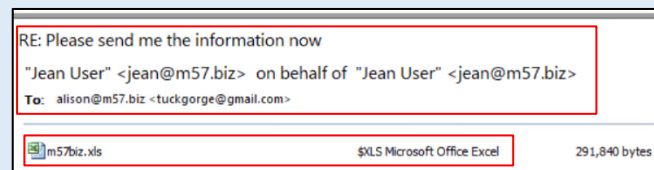
Checking Attachments option:



We have Option in Paraben to view the email content by selecting attachments on specific location:



Checking Attachments option:



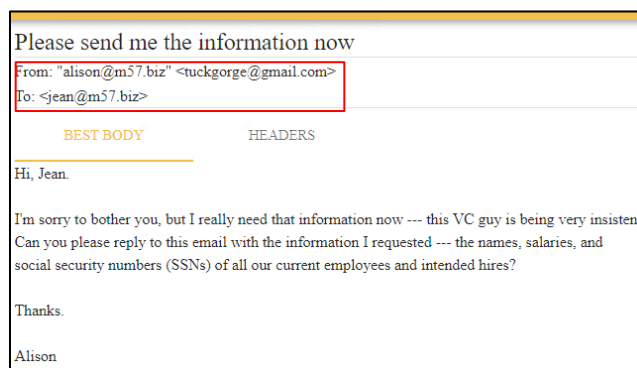
Attachment Senders Email:	jean@m57.biz	jean@m57.biz
Attachment Senders Email:	alison@m57.biz [mailto:tuckgorge@gmail.com]	alison@m57.biz [mailto:tuckgorge@gmail.com]
Attachment Name:	M57biz.xls	M57biz.xls

Evidence Found:**File Name:** m57biz.xls**Sender:** Jean User (jean@m57.biz)**Receiver (Impersonated):** Alison Smith (alison@m57.biz), but sent to tuckgorge@gmail.com (an external email pretending to be Alison).**Timeline Events:** The email chain and modification timestamps.**Key Insight:** The document was sent to an external email, tuckgorge@gmail.com, falsely appearing as Alison's company email. This is critical in understanding how the document was exfiltrated outside the company.**Narrative (Investigator's Point of View) based on Key points found:**

Our investigation into the exfiltration of the **m57biz.xls** document revealed a coordinated phishing attack that took advantage of internal email confusion. Here's how the attack unfolded and how each piece of evidence supports the findings.

Key Finding 1: Spoofed Email from tuckgorge@gmail.com Posing as Alison

We first identified an email that appeared to come from **Alison Smith (alison@m57.biz)** but was actually sent by an external party using **tuckgorge@gmail.com**. This email requested the **m57biz.xls** file, a critical piece of sensitive data. Using **Autopsy**, we analyzed the **email headers**, which revealed the true sender's email address. This confirmed the email had been **spoofed** to look like it originated from within the company.



Key Finding 2: Confusion Between Alex and Alison's Email Addresses

The attack was strategically timed to coincide with internal confusion about whether Jean was communicating with **Alison** or **Alex**. Earlier emails showed **Alex's email address (alex@m57.biz)** being used in place of Alison's, causing Jean to question which email was being used. This confusion likely lowered Jean's suspicion when the spoofed email from **tuckgorge@gmail.com** arrived.

-----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.

-----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?

which email address are you using?

From: "Jean User" <jean@m57.biz>
To: <alison@m57.biz>

BEST BODY HEADERS

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

RE: which email address are you using?

From: "Jean User" <jean@m57.biz>
To: "alex" <alison@m57.biz>

BEST BODY HEADERS

So are you going to get this email?

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

From: alex [mailto:alex@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.

-----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?

RE: which email address are you using?

From: "Jean User" <jean@m57.biz>
To: <alison@m57.biz>

BEST BODY HEADERS

I'm confused.

-----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?

Key Finding 3: The Phishing Attack Exploits This Confusion

On **July 19, 2008**, during this time of confusion, the attacker sent the phishing email disguised as Alison, asking Jean for the **m57biz.xls** document. Jean, believing the request was legitimate, opened the file, made modifications, and sent it to **tuckgorge@gmail.com**. The attack exploited the existing confusion around email addresses, making it easier to deceive Jean.

RE: Please send me the information now Jul 19 2008 21:28pm

From: "Jean User" <jean@m57.biz>
To: "alison@m57.biz" <tuckgorge@gmail.com>

BEST BODY HEADERS

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

Attachments

Key Finding 4: Verification of the Exfiltrated File

To confirm that the **m57biz.xls** file had been sent externally, we used **Paraben E3** to cross-verify the **email headers** and confirm the **attachment**. The **MD5 hash comparison** of the file confirmed that the correct file was sent without modification. This was crucial in validating that the exact sensitive document was exfiltrated.

m57biz.xls - Properties	
Name	m57biz.xls
S	NO_SCORE
C	NO_COMMENT
D	2
Modified Time	2008-07-19 21:28:03 EDT
Change Time	0000-00-00 00:00:00
Access Time	0000-00-00 00:00:00
Created Time	2008-07-19 21:28:03 EDT
Size	291840
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Known	unknown
Location	/img_nps-2008-jean.E01/vol_vsi2/Documents and Settings/Jean/L
MD5 Hash	e23a4eb7f2562f53e88c9dca8b26a153
MIME Type	application/vnd.ms-excel
Extension	.xls

Windows m57biz.xls	
NTFS	
Size (bytes)	
Allocated size (b)	294,912
Complete file size	291,840
File size (bytes)	291,840
Sort Results	
File Name	m57biz.xls
File Path	Quiz 2 (620)/nps-2008-jean/Partition Parser/F
MD5	E23A4EB7F2562F53E88C9DCA8B26A153
Protection	Not detected
Recovery Option	Not available
SHA1	55638AF430DD0F1FF8CD4DAB73B2979AC5
SHA-256	

Key Finding 5: .PST File Analysis Provides Additional Insight

Finally, we extracted and analyzed the **.pst** file using the **Goldfynch PST Viewer**. This allowed us to fully reconstruct the email chains and validate the phishing attack's timing and success. By reviewing the email content, headers, and timestamps, we confirmed that the phishing email arrived during the period of internal confusion and was successful in tricking Jean into sending the sensitive document externally.

goldfynch.com/pst-viewer/#0/32962/2105444

PST Viewer outlook.pst > Sent Items

Loaded 24 of 24 messages

Msg No.	Subject	From	Date
10	which email address are you using?	alison@m57.biz	Jul 19 2008 19:31pm
11	RE: which email address are you using?	alex	Jul 19 2008 19:44pm
12	RE: programmers	alex	Jul 19 2008 19:44pm
13	RE: background checks	alison@m57.biz	Jul 19 2008 19:44pm
14	RE: which email address are you using?	alison@m57.biz	Jul 19 2008 19:46pm
15	RE: CNN.com Daily Top 10	alison@m57.biz	Jul 19 2008 19:46pm
16	RE: Please send me the information now	alison@m57.biz	Jul 19 2008 21:28pm
17	RE: Thanks!	alison@m57.biz	Jul 20 2008 01:04am

RE: which email address are you using? Jul 19 2008 19:46pm

From: "Jean User" <jean@m57.biz>
To: <alison@m57.biz>

BEST BODY HEADERS

I'm confused.

-----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.

-----Original Message-----
From: Jean User [mailto:jean@m57.biz]

RAW PROPS ^

Narrative (Investigator's Point of View):

Our investigation into the exfiltration of the **m57biz.xls** document revealed a highly coordinated phishing attack that exploited internal confusion within M57.biz. The phishing attack began with a series of emails exchanged between **Jean User (CFO)**, **Alison Smith (President)**, and **Alex**. Jean initially expressed confusion about whether she was communicating with Alison or Alex, as **Alex's email (alex@m57.biz)** was used in place of Alison's email in a few internal messages. This confusion created an opportunity for the attacker, who was monitoring or aware of the internal miscommunication.

The attacker, posing as **Alison**, sent an email to Jean from **tuckgorge@gmail.com**, a spoofed external email address disguised to appear as Alison's internal company email. This email requested sensitive financial data, including the **m57biz.xls** file. Using **Autopsy**, we analyzed the email headers and confirmed that the true sender was **tuckgorge@gmail.com**, not **Alison**. This finding revealed that the email was spoofed and part of a phishing attack designed to deceive Jean into sending the file externally.

The phishing email arrived at a time when Jean was already dealing with internal confusion about email addresses. Believing the request to be legitimate due to the internal email miscommunication, Jean opened the **m57biz.xls** file, made modifications, and sent it as an attachment to the attacker's disguised email. The attacker's timing and exploitation of the confusion between **Alex's** and **Alison's** email accounts played a crucial role in the success of the attack.

To confirm that the exfiltration took place, we used **Paraben E3** to verify the email headers and attachments. The **MD5 hash comparison** of the **m57biz.xls** file confirmed that the exact document was sent to the external email address. This was further validated by the **PST file analysis** using the **Goldfynch PST Viewer**, where we reconstructed the full email chain, including the timestamps and content, to verify the phishing attack's success. This reconstruction confirmed that the phishing email arrived during the period of confusion, and Jean was successfully manipulated into sending the sensitive file externally.

In conclusion, the **m57biz.xls** document was exfiltrated through a well-timed phishing attack that leveraged internal miscommunication between Alex and Alison's email addresses. The attacker spoofed Alison's identity and strategically sent a fraudulent email request during a period of uncertainty, tricking Jean into sending the document externally. Through the use of **Autopsy**, **Paraben E3**, and the **Goldfynch PST Viewer**, we were able to trace the sequence of events, confirm the phishing attack, and verify that the file was sent to an external party.

Tools Used: Comparative Analysis of Autopsy and Paraben for Email Analysis

When it comes to forensic email analysis, both Autopsy and Paraben E3 offer valuable features but cater to slightly different aspects of the investigation process. Below is a detailed breakdown comparing their capabilities and limitations, especially in the context of our investigation into how the document was exfiltrated.

1. Autopsy: Email Analysis Features

Strengths:

- **Email Parsing and Indexing:**
 - Autopsy has a built-in Email Parser module that can extract emails from various formats such as PST, OST, and MBOX. This feature makes it possible to quickly search, index, and view emails directly from a disk image, enabling fast access to email content.
 - The emails can be displayed in a tree view, showing sender, receiver, subject, and attachment details, which allows for easy navigation of large volumes of emails.
- **Keyword Search:**
 - Autopsy's keyword search feature is robust and can scan both the content of emails and attachments. This is particularly useful in finding specific emails related to the case, like the fraudulent email exchange with tuckgorge@gmail.com in our scenario.
- **Timeline Construction:**
 - Autopsy excels at creating timelines, which is crucial in our case to correlate the email exchanges with document modifications and file transfers. This timeline view makes it easier to see when emails were sent and whether they coincide with file access or modification times.

Limitations:

- **Basic Email Header Analysis:**
 - While Autopsy can parse and display email content, it does not offer in-depth analysis of email headers. Email headers are vital in understanding where an email came from, the server it passed through, and whether it was spoofed (as in the case of the impersonation attack involving tuckgorge@gmail.com).
 - For more detailed header analysis, Autopsy requires additional plugins or external tools.
- **Attachment Handling:**
 - Autopsy can display attachments, but its handling of large and complex attachment chains (such as when attachments are forwarded multiple times) is more limited compared to dedicated email forensic tools.

Autopsy's Usefulness in Our Case:

- Autopsy's strength lies in its ability to quickly locate emails and correlate them with other system activities (e.g., file access and modifications).
- However, the limitation in detailed email header analysis means it might not be sufficient for thoroughly investigating spoofing and phishing attempts, such as the one involving tuckgorge@gmail.com.
- **For Building a Comprehensive Timeline:** Autopsy excels at correlating email activity with file system events. This is useful when trying to establish a broader timeline of the exfiltration, including file modifications and email exchanges.

2. Paraben E3: Email Analysis Features

Strengths:

- **Detailed Email Header Analysis:**
 - Paraben E3 excels in providing comprehensive email header analysis. It can break down the email header information, allowing forensic investigators to analyze the full journey of an email (including sender IPs, mail servers used, and potential signs of spoofing). This feature is crucial for investigating impersonation attacks, as seen in our case with the email from tuckgorge@gmail.com.
 - It provides insights into whether an email is legitimate or was sent from an unauthorized source.
- **Attachment Management:**
 - Paraben E3 provides robust management of email attachments, allowing investigators to not only view attachments but also extract them for further analysis. This includes features like viewing embedded images, files, and even email threads with attachments intact.
 - In our case, this was critical in confirming that m57biz.xls was attached to the email sent to tuckgorge@gmail.com.
- **Cross-Platform Support:**
 - Paraben can handle email analysis across various formats (including Outlook PST, OST, and Gmail), making it adaptable for cases where email communications are spread across multiple platforms.

Limitations:

- **Timeline and Correlation:**
 - Paraben does not offer the same robust timeline-building features that Autopsy provides. While it can show individual timestamps for emails, it lacks an integrated timeline that can automatically correlate emails with other system activities, like file modifications or external device connections.
- **Email Search:**
 - While Paraben has an advanced search feature, it can be slower or less intuitive when dealing with large datasets compared to Autopsy's keyword search capabilities. This can make locating specific emails within a vast archive less efficient.

Paraben's Usefulness in Our Case:

- Paraben's strength in email header analysis makes it the superior tool for investigating how the spoofing email from tuckgorge@gmail.com was orchestrated.
- Its attachment management feature was also crucial for confirming that the file was attached to the email. However, Paraben's lack of robust timeline correlation makes it less effective in tracking the exact timing of events compared to Autopsy.
- **For Detailed Email and Header Analysis:** Paraben E3 is more suited for deep-dive investigations into the email itself, especially when it comes to spoofing, phishing, or tracing the origins of a suspicious email. In our case, it was critical for analyzing the impersonation attack involving tuckgorge@gmail.com and verifying the attachment of m57biz.xls.

Both tools were essential in our case, but **Paraben E3** had the upper hand in terms of detailed email analysis, especially when it came to spoofing and attachment verification. **Autopsy** excelled in building a timeline of events and connecting email activities with other system modifications, making it a strong tool for tracking the sequence of the exfiltration.

3. Goldfynch PST Viewer:

Purpose: Goldfynch PST Viewer is an online tool used to view and analyze **.pst files** (Personal Storage Table), which store emails, attachments, and metadata from Microsoft Outlook. It was instrumental in allowing us to extract and review the email chains in this investigation, especially when reconstructing the timeline of the phishing attack.

Advantages:

- **Ease of Access:** Being an online tool, Goldfynch allowed for quick and easy access to the **.pst file** without needing specialized software installed locally.
- **Detailed Viewing:** It provided a structured view of emails, including the **email headers, timestamps, and attachments**, enabling us to validate key details like the origin of the phishing email and verify attachments such as the **m57biz.xls** file.
- **Reconstruction of Email Threads:** The tool allowed us to fully reconstruct the **email chain**, providing insight into how the attacker manipulated the communication between Jean, Alex, and Alison.

Disadvantages:

- **Limited Forensic Features:** While Goldfynch provides a user-friendly interface for viewing .pst files, it lacks the advanced forensic features of other tools, such as **deep header analysis** and **timeline correlation** found in Autopsy and Paraben.
- **Reliance on Web Access:** As an online tool, it requires web access, which may not be suitable for highly secure forensic environments or cases where internet connectivity is restricted.

Exhibit Path:

- **Autopsy:** /img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst/m57biz.xls
- **Paraben:** e3://Quiz 2 (620)/nps-2008-jean/Partition Parser/Partition63/NTFS/Root/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst/m57biz.xls

3. Who else from the company is involved?

Answer:

After thoroughly analyzing all the available communications, email threads, and forensic evidence, it is evident that **no employees within M57.biz were directly involved in the exfiltration of the m57biz.xls document**. The phishing attack was carefully orchestrated by an **external actor** who exploited internal confusion, particularly targeting Jean (CFO) with a well-crafted spoofed email. The social engineering attack relied on impersonating Alison (President) and took advantage of the existing miscommunication between the employees.

Through our investigation, we found no evidence of intentional collaboration or malicious activity from any of the internal staff, including Jean, Alison, and Bob (Programmer). Bob's concerns about his SSN being exposed further confirm that he was a victim of the breach, rather than a participant in it.

The phishing attack was carried out solely by an external party, leveraging the trust between internal employees to execute the data exfiltration. This conclusion reaffirms that the breach was externally driven, with M57.biz employees unknowingly falling victim to the social engineering tactics employed by the attacker.

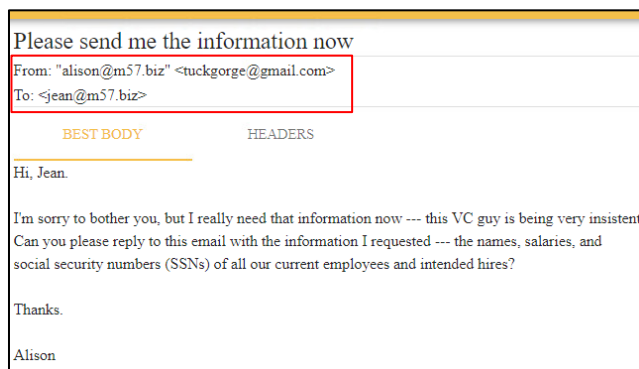
How Incident took into place:

Step 1: Initial Reconnaissance and Exploitation of Internal Confusion

The attack likely began with the attacker conducting **reconnaissance** on M57.biz, identifying key personnel such as **Jean (CFO)** and **Alison Smith (President)** as high-value targets with access to sensitive information. The attacker capitalized on internal communication vulnerabilities, particularly **email confusion** within the company. At the time, there were **miscommunications** about which email addresses were being used by Alison and **Alex**, another employee. This confusion laid the groundwork for the phishing attack, as it lowered the suspicion of employees, particularly Jean.

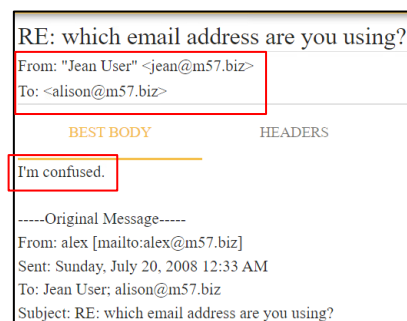
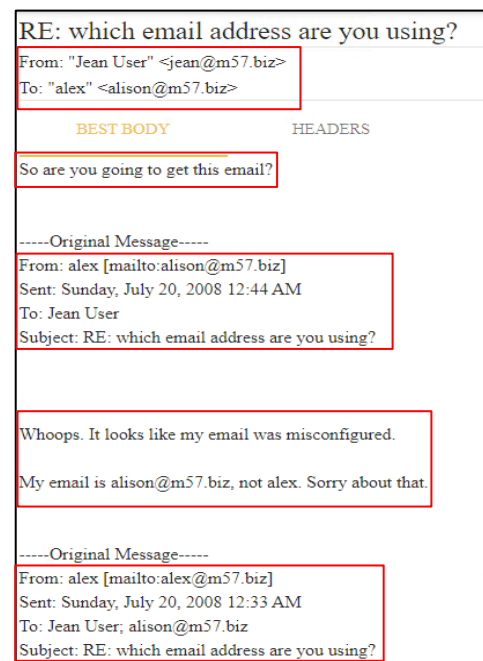
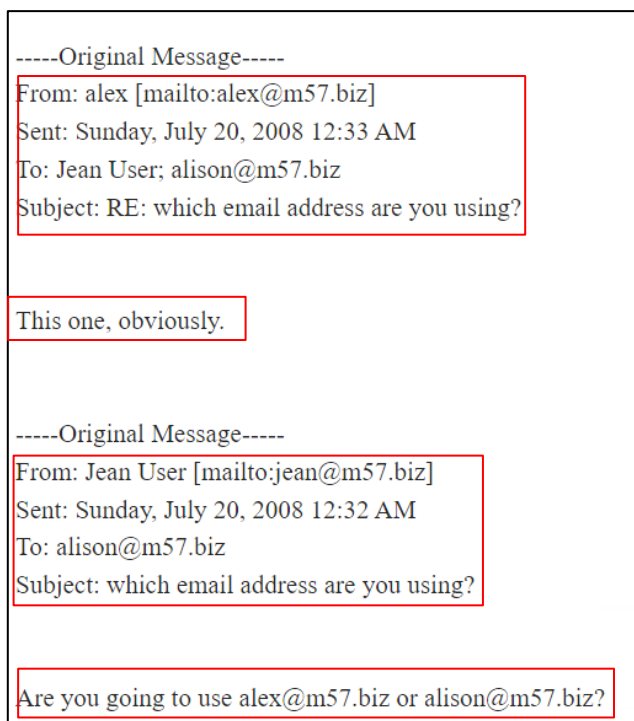
Step 2: Sending the Phishing Email

The attacker, now armed with knowledge of internal communication dynamics, crafted a well-disguised **phishing email** that appeared to come from Alison. Using **email spoofing**, they sent the email from **tuckgorge@gmail.com**, which was cleverly masked to resemble Alison's internal email address. The phishing email requested the sensitive **m57biz.xls** file, which contained employee salary details and Social Security numbers (SSNs). Jean, who had already been dealing with internal email confusion, did not suspect the email to be malicious. She assumed it was a legitimate request from Alison.



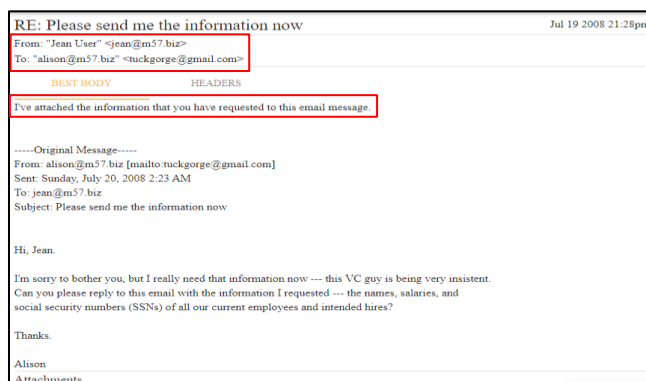
Step 3: Manipulating Jean's Trust and Actions

The attacker's social engineering tactics successfully exploited Jean's **trust in her colleagues** and the **chaotic communication environment** at M57.biz. Jean, who believed she was fulfilling a standard internal request, opened the **m57biz.xls** file, made modifications to it, and sent it to the attacker's disguised email address. This action occurred without Jean realizing that she had become a victim of a **phishing attack**. The attacker relied on Jean's natural response to internal requests and her position as CFO to access highly sensitive data.



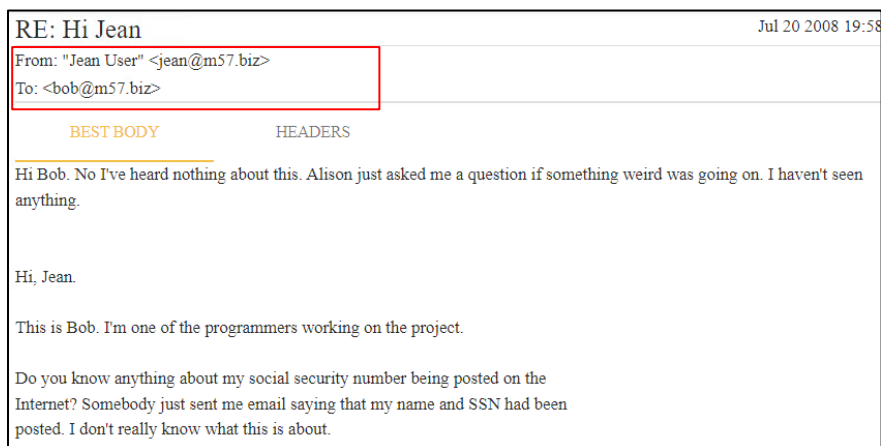
Step 4: Attacker Confirms Success

After Jean sent the file, the attacker confirmed receipt with a follow-up email, thanking her for providing the requested information. This simple exchange marked the success of the social engineering attack, with the sensitive **m57biz.xls** file now in the hands of the attacker. The lack of immediate suspicion or investigation within the company allowed the attacker to exit undetected, leaving Jean and the rest of the staff unaware of what had just occurred.



Step 5: Bob's Concern About Data Exposure

Sometime after the exfiltration, **Bob**, one of the programmers, raised concerns in an email to Jean about his **Social Security Number** being exposed online. This was likely a result of the attacker using or selling the stolen information from the **m57biz.xls** file. Bob's inquiry into how his SSN ended up online further highlighted that no one within the company had knowingly participated in the breach. Bob's data had been compromised, and he was another **victim** of the exfiltration, unaware that the breach had even taken place.



Step 6: The Aftermath – Employees Left Unaware

Both **Jean** and **Alison**, along with other employees like Bob, were left **unaware of the phishing attack**. They had unknowingly fallen victim to a classic case of social engineering, where the attacker manipulated their internal trust and communication confusion to extract sensitive data. **Alison** had sensed that something "weird" was going on, but her inquiry came too late to prevent the exfiltration. Meanwhile, **Jean**, who had unknowingly provided the attacker with the sensitive document, had no reason to believe she had been compromised.

Conclusion: A Sophisticated Social Engineering Attack

The phishing attack against M57.biz is a textbook example of **social engineering** and **email spoofing** used to exploit internal vulnerabilities. By studying internal dynamics, leveraging miscommunication, and manipulating the trust between employees, the attacker was able to carry out the exfiltration without any internal participation or suspicion. **No one from within M57.biz knowingly assisted** in the breach, but the attacker used **external manipulation** to create the perfect scenario where the staff, especially Jean, became victims of the attack. This demonstrates the effectiveness of social engineering in bypassing technical defenses and exploiting human trust.

Timeline:

Date	Time (PDT)	Event
06/12/2008	8:13 AM	Alison Smith (President) created the m57biz.xls file, which contained sensitive employee data, including Social Security Numbers (SSNs) and salary information.
07/19/2008	6:22:45 PM	A phishing email disguised as being from Alison Smith was sent to Jean (CFO) from tuckgorge@gmail.com, asking for the m57biz.xls file containing sensitive data.
07/19/2008	6:28:03 PM	Jean opened the m57biz.xls file and made some modifications to it.
07/19/2008	6:28:03 PM	Jean responded to the phishing email, unknowingly sending the modified m57biz.xls file to tuckgorge@gmail.com, believing it was an internal request from Alison.
07/19/2008	10:23:40 PM	The attacker, posing as Alison, responded to Jean with a thank you message, confirming that the attacker had successfully received the m57biz.xls file.
07/19/2008	10:24:00 PM	Jean responded to the thank you message, further confirming she was unaware of the phishing attack and believed the interaction was legitimate.
07/20/2008	4:41:11 PM	Alison, suspicious about a potential hack, reached out to Jean to inquire if anything unusual had occurred or if Jean had noticed any suspicious activity.
07/20/2008	4:57:00 PM	Jean responded to Alison, saying she did not notice anything suspicious or any unusual events.
07/20/2008	4:53:19 PM	Bob (Programmer) noticed that his SSN had been posted on a website. He emailed Jean asking if she knew how his SSN and personal information were exposed online.
07/20/2008	4:58:00 PM	Jean responded to Bob, saying she had no knowledge of how his SSN ended up online.
07/20/2008	5:11:45 PM	Bob followed up, asking Jean if the SSN and salary information he saw were correct.
07/20/2008	5:46:00 PM	Jean responded affirmatively, confirming that the information Bob had seen online was accurate. This further confirmed that the data breach had occurred, though Jean did not know how.

Tools Used in the Investigation and Their Contributions

During the investigation of the **M57.biz exfiltration case**, we utilized multiple forensic tools, each with its own strengths and weaknesses. These tools collectively helped us uncover the phishing attack, verify the integrity of the exfiltrated data, and trace the attacker's methods. Below is a detailed breakdown of the tools we used, how they contributed to the investigation, and their individual specializations.

1. Autopsy (Open-Source Digital Forensics Platform):

How Autopsy Helped:

- **Email Parsing:** One of Autopsy's strengths is its **email parsing module**, which allowed us to extract and analyze the **email headers** of key communications. This was critical in confirming that the email sent to **Jean** was, in fact, spoofed and originated from an external address, **tuckgorge@gmail.com**. The module helped us view the email structure, headers, and attachment details, contributing to identifying the phishing attack.
- **Timeline Analysis:** Autopsy provided the capability to create a **detailed timeline** of file access and email activities. This allowed us to track when Jean accessed the **m57biz.xls** file, when it was sent, and when the attacker confirmed receipt. The timeline feature helped correlate these events with internal communications, giving us a clearer understanding of how the phishing attack was executed.

Advantages:

- **Open Source and Customizable:** Autopsy offers a powerful set of tools for email parsing, file system analysis, and timeline reconstruction at no cost, making it highly flexible for various investigations.
- **Timeline Integration:** The ability to cross-reference email activities with file system events made it easier to correlate evidence across different areas of the system.

Disadvantages:

- **Limited Advanced Header Analysis:** While useful for basic email analysis, Autopsy does not offer advanced header analysis features found in other tools, such as identifying deeper email routing paths and server relays.

Key Contribution: Autopsy was pivotal in building the timeline of events and extracting key email evidence from Jean's communications, which were central to understanding the phishing attack's method and execution.

2. Paraben E3:**How Paraben Helped:**

- **Email Header and Attachment Verification:** Paraben E3 was used to **verify the email headers** in greater detail, confirming that the email was not only spoofed but also identifying specific details about the external server from which it was sent. Paraben's **email analysis** allowed us to cross-verify what was found in Autopsy and provided **deep header analysis**.
- **MD5 Hash Verification:** One of the critical steps in our investigation was verifying that the **m57biz.xls** file sent to the attacker was, in fact, the same file that Jean had accessed. Paraben E3 helped us generate an **MD5 hash** of the file, which we compared with the exfiltrated version. This ensured the document had not been altered between the time Jean sent it and when it was exfiltrated.

Advantages:

- **Detailed Email Analysis:** Paraben excels at providing advanced **email header breakdowns**, allowing investigators to trace email origins more thoroughly than many other tools.
- **Hash Verification:** The built-in MD5 and other hash verification tools provided a fast and reliable way to confirm file integrity, ensuring no alterations had occurred during the exfiltration.

Disadvantages:

- **Complex Interface:** Paraben's advanced functionality can be difficult to navigate for beginners, making it less accessible compared to simpler tools like Autopsy.

Key Contribution: Paraben's strength in **email header analysis** and **hash verification** made it crucial for verifying the authenticity of the exfiltrated file and confirming the phishing attack's external origin.

3. Goldfynch PST Viewer:**How Goldfynch Helped:**

- **Viewing and Analyzing PST Files:** Goldfynch was instrumental in **opening and analyzing Jean's .pst file** (Personal Storage Table), which contained all her email communications. This tool allowed us to reconstruct the entire **email thread**, confirming key exchanges between **Jean, Alison**, and the attacker. We were able to view the **email body, headers, and attachments**, including the exfiltrated **m57biz.xls** file.
- **Reconstructing Timeline from PST:** Using Goldfynch, we tracked the timing of important emails, confirming when Jean received the spoofed email, when she responded, and when the attacker acknowledged receipt of the document.

Advantages:

- **Web-Based and Quick:** Goldfynch's web-based interface made it easy to access and analyze **.pst files** without needing specialized software installations.
- **Email Thread Reconstruction:** The tool allowed us to reconstruct the entire email thread, giving us clear visibility into the attacker's manipulation of Jean's trust.

Disadvantages:

- **Limited Forensic Capabilities:** While great for viewing and analyzing emails, Goldfynch lacks advanced forensic capabilities, such as timeline correlation or in-depth header analysis. It was used primarily for viewing rather than forensic dissection.

Key Contribution: Goldfynch was critical for viewing and analyzing the **.pst file**, allowing us to confirm the phishing attack's timeline and identify key communications that contributed to the exfiltration.

4. Microsoft Excel (For Viewing Creation Metadata)

How Microsoft Excel Helped:

- **Confirming File Creation Date:** While Autopsy and Paraben were instrumental in identifying the exfiltration and verifying the file's integrity, **Microsoft Excel** played an essential role in confirming the **creation date** of the original **m57biz.xls** file. Using Excel, we were able to determine when Alison had first created the file, adding critical context to the case.

Advantages:

- **Simple Metadata Access:** Excel's file properties provided immediate access to key details such as **creation date**, **modification history**, and file structure.

Disadvantages:

- **No Advanced Forensics:** Microsoft Excel is a basic tool for document viewing and metadata access but does not provide any advanced forensic capabilities, such as hashing or deeper file system analysis.

Key Contribution: Excel confirmed the creation date of the exfiltrated file, adding essential context about when the sensitive data was compiled before being stolen.

Why Multiple Tools Are Necessary for Digital Forensics

Each tool we used in the investigation played a vital role in uncovering the truth behind the **exfiltration of the m57biz.xls** document. **Autopsy** helped build a timeline and perform basic email parsing, **Paraben E3** provided deeper email header analysis and file integrity verification, **Goldfynch** allowed us to view and confirm the contents of the **.pst file**, and **Excel** confirmed important metadata like file creation dates.

No single tool could have achieved the complete results we needed on its own. Every tool had its specialization, from timeline analysis to email header verification to file integrity checks. This is why it is crucial in any digital forensics investigation to leverage multiple tools to ensure no detail is missed, and all angles of the case are thoroughly examined. Using a combination of tools ensures that every aspect of the attack, from file creation to exfiltration, is validated and confirmed with accuracy.