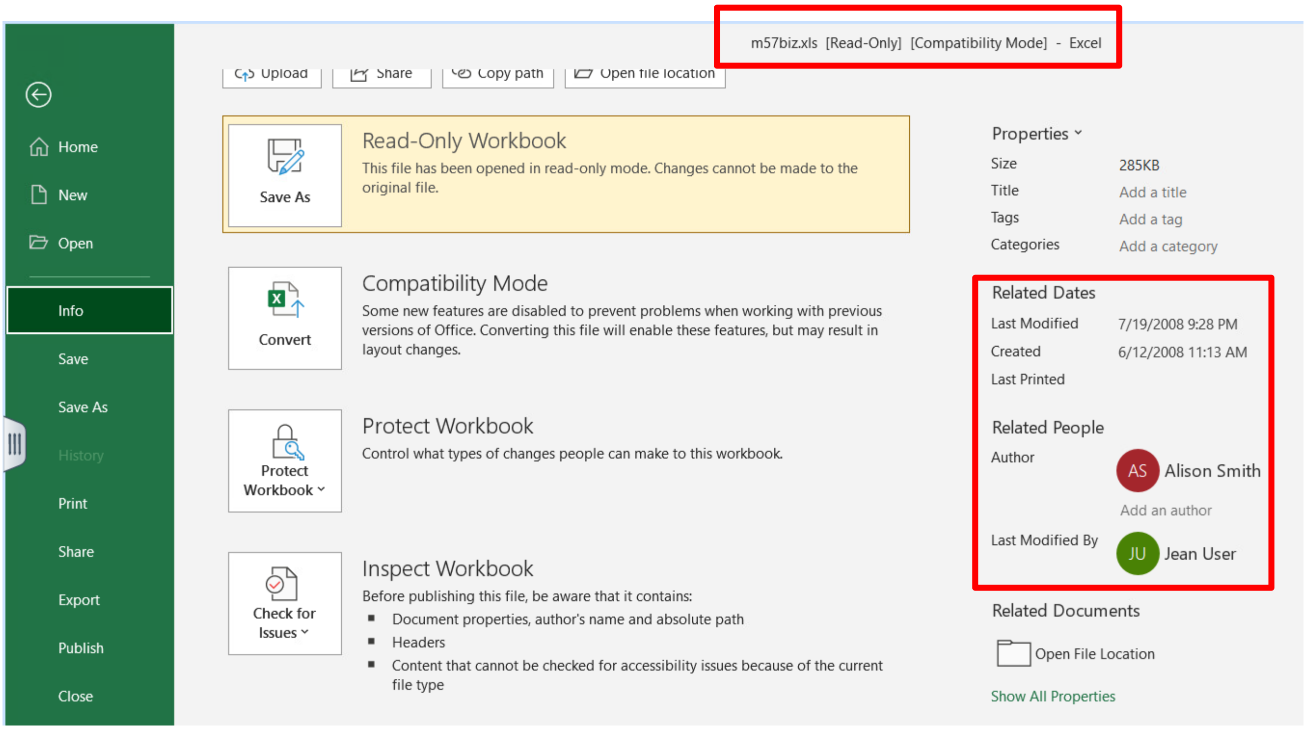
Question 1: When was the spreadsheet created? Who created the spreadsheet?

Answer: According to the metadata, the file "m57biz.xls" was created on **June 12th, 2008, at 3:13:51 PM UTC** and last modified on **July 20th, 2008, at 1:28:03 AM UTC**. This information was confirmed using both **Paraben E3 Forensic Platform** and **Autopsy**.

- ❖ **Evidence and Analysis:** I employed two powerful forensic tools to analyse the evidence:
  1. **Paraben E3 Forensic Platform:** Paraben E3 has a relatively intuitive interface, making it accessible to investigators with varying levels of technical expertise. Wide File Format Support: It supports a wide variety of file formats, ensuring compatibility with diverse evidence sources.
     - o **Path:** /img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Desktop/m57biz.xls
     - o **Analysis**: The file's presence on the desktop of a user named "Jean" suggests it was readily accessible and potentially in active use. This makes it more likely to be relevant to the investigation compared to a file buried deep within the file system or in an obscure folder.
     - o **Method**: To access the file, I exported the file from paraben and then opened it using MS Excel software. In excel, I accessed the “info” section where I found the original file creation date and last modified date along with the Owner/Author’s name and also the last user’s name



m57biz.xls [Read-Only] [Compatibility Mode] - Excel

Read-Only Workbook

This file has been opened in read-only mode. Changes cannot be made to the original file.

Compatibility Mode

Some new features are disabled to prevent problems when working with previous versions of Office. Converting this file will enable these features, but may result in layout changes.

Protect Workbook

Control what types of changes people can make to this workbook.

Inspect Workbook

Before publishing this file, be aware that it contains:

- Document properties, author's name and absolute path
- Headers
- Content that cannot be checked for accessibility issues because of the current file type

Properties

Size	285KB
Title	Add a title
Tags	Add a tag
Categories	Add a category

Related Dates

Last Modified	7/19/2008 9:28 PM
Created	6/12/2008 11:13 AM
Last Printed	

Related People

Author	AS Alison Smith
	Add an author
Last Modified By	JU Jean User

Related Documents

Open File Location

Show All Properties

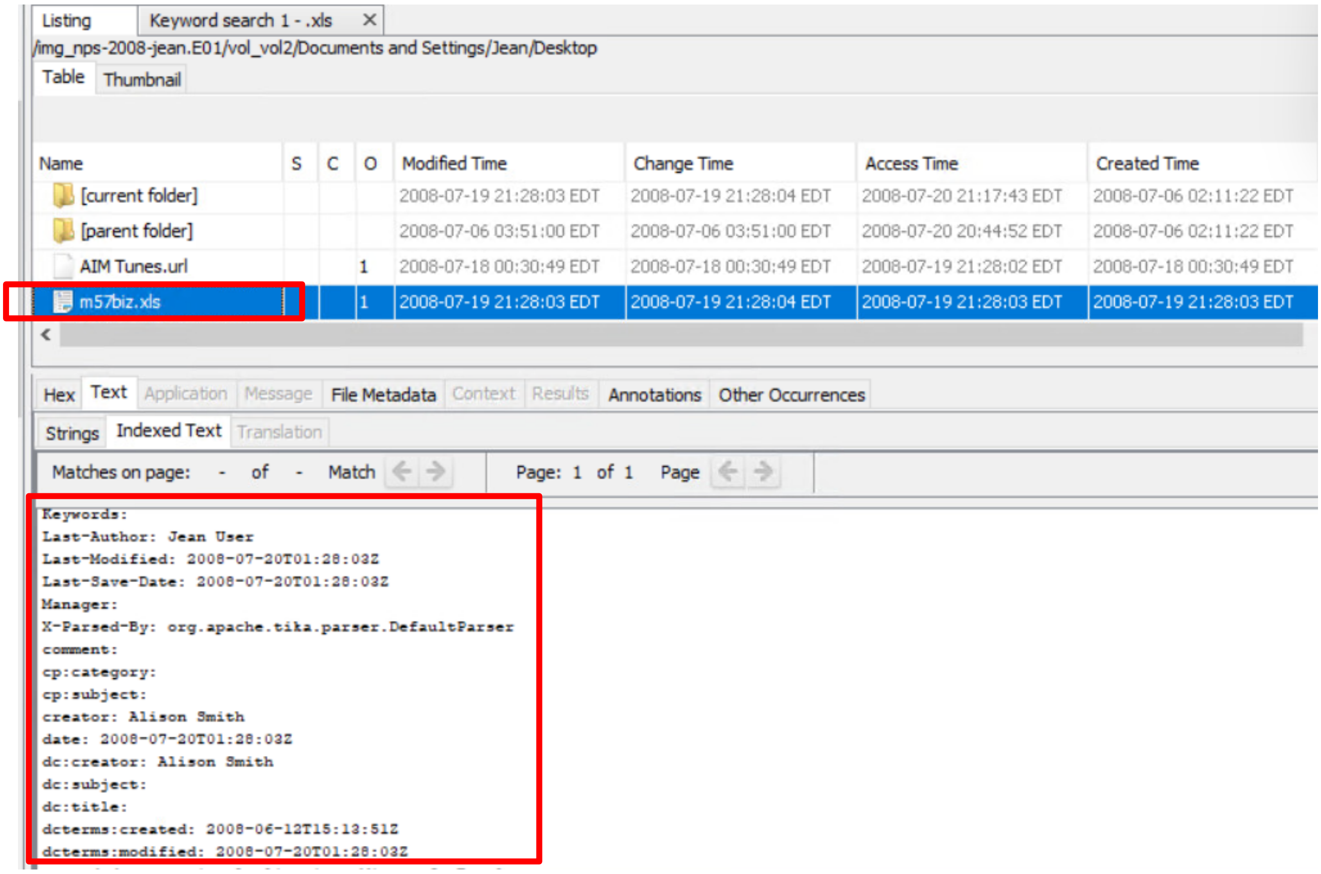
2. **Autopsy:** Autopsy is another widely used open-source digital forensics platform. It's known for its user-friendly interface and powerful analysis capabilities.

   ○ **Metadata Verification:** By examining the metadata within Autopsy, I independently confirmed the creation date as **June 12th, 2008, at 11:13 AM** and the author as **Alison Smith**.

   ○ **Note**: The timing difference can be due to the difference of Time zone settings of the tool and the actual case time zone.

❖ **Why using multiple tools is beneficial:**

○ **Verification and Validation:** Using two different tools to analyse the same evidence provides a crucial layer of verification. If both tools independently arrive at the same conclusion, it strengthens the reliability and accuracy of the findings.



/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Desktop

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2008-07-19 21:28:03 EDT	2008-07-19 21:28:04 EDT	2008-07-20 21:17:43 EDT	2008-07-06 02:11:22 EDT
[parent folder]				2008-07-06 03:51:00 EDT	2008-07-06 03:51:00 EDT	2008-07-20 20:44:52 EDT	2008-07-06 02:11:22 EDT
AIM Tunes.url			1	2008-07-18 00:30:49 EDT	2008-07-18 00:30:49 EDT	2008-07-19 21:28:02 EDT	2008-07-18 00:30:49 EDT
m57biz.xls			1	2008-07-19 21:28:03 EDT	2008-07-19 21:28:04 EDT	2008-07-19 21:28:03 EDT	2008-07-19 21:28:03 EDT

```
Keywords:
Last-Author: Jean User
Last-Modified: 2008-07-20T01:28:03Z
Last-Save-Date: 2008-07-20T01:28:03Z
Manager:
X-Parsed-By: org.apache.tika.parser.DefaultParser
comment:
cp:category:
cp:subject:
creator: Alison Smith
date: 2008-07-20T01:28:03Z
dc:creator: Alison Smith
dc:subject:
dc:title:
dcterms:created: 2008-06-12T15:13:51Z
dcterms:modified: 2008-07-20T01:28:03Z
```

○ **Comprehensive Analysis:** Different tools might have unique strengths and capabilities. Paraben E3 might excel in certain types of analysis, while Autopsy might offer complementary features or a different perspective on the data.

- **Increased Confidence:** By cross-referencing the results from multiple tools, investigators can increase their confidence in the accuracy and integrity of the evidence.

❖ **Investigator's Perspective:** The consistent findings from both Paraben E3 and Autopsy solidify the key facts:

- **Alison Smith** is the creator of the spreadsheet.
- The spreadsheet was created on **June 12th, 2008**.

This enforces us to focus on the importance of Alison Smith as a person of interest and further investigating to understand Alison's potential role in the case.

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

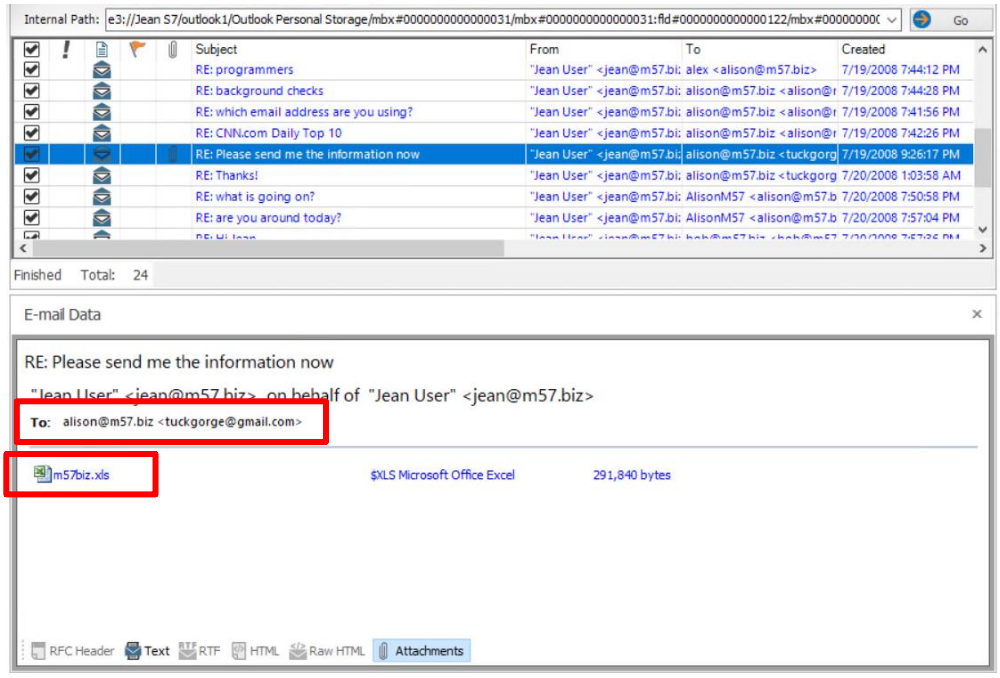
Answer: As per the email conversation found in the email database (outlook.pst), the potential means of the data leak is by Jean sharing the spreadsheet (m57biz.xls) with an unknown person having the email address **tuckgeorge@gmail.com**, who impersonates Alison, the president of the company. The document "m57biz.xls" likely reached the competitor's website through a combination of social engineering, email spoofing, and a possible lapse in data security practices within the company.

❖ **Evidence and Analysis:** I utilized both **Autopsy** and **Paraben E3 Forensic Platform** to analyse the email database (outlook.pst) and other relevant files. These tools allowed me to extract, analyse, and cross-reference data to reconstruct the events leading up to the data leak.

1. **Paraben E3 Forensic Platform:** Paraben E3 has a relatively intuitive interface, making it accessible to investigators with varying levels of technical expertise. Wide File Format Support: It supports a wide variety of file formats, ensuring compatibility with diverse evidence sources.

- **Path:** /img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst

- **Method**: To access the emails, I first exported the entire email database (.pst) file and then added it as a piece of evidence which help me get a better overview of all the email conversations.



Internal Path: e3://Jean S7/outlook1/Outlook Personal Storage/mbx#000000000000031/mbx#000000000000031:fld#0000000000000122/mbx#00000000(

Subject	From	To	Created
RE: programmers	"Jean User" <jean@m57.bi:	alex <alison@m57.biz>	7/19/2008 7:44:12 PM
RE: background checks	"Jean User" <jean@m57.bi:	alison@m57.biz <alison@r	7/19/2008 7:44:28 PM
RE: which email address are you using?	"Jean User" <jean@m57.bi:	alison@m57.biz <alison@r	7/19/2008 7:41:56 PM
RE: CNN.com Daily Top 10	"Jean User" <jean@m57.bi:	alison@m57.biz <alison@r	7/19/2008 7:42:26 PM
RE: Please send me the information now	"Jean User" <jean@m57.bi:	alison@m57.biz <tuckgorg	7/19/2008 9:26:17 PM
RE: Thanks!	"Jean User" <jean@m57.bi:	alison@m57.biz <tuckgorg	7/20/2008 1:03:58 AM
RE: what is going on?	"Jean User" <jean@m57.bi:	AlisonM57 <alison@m57.b	7/20/2008 7:50:58 PM
RE: are you around today?	"Jean User" <jean@m57.bi:	AlisonM57 <alison@m57.b	7/20/2008 7:57:04 PM

Finished Total: 24

E-mail Data

RE: Please send me the information now

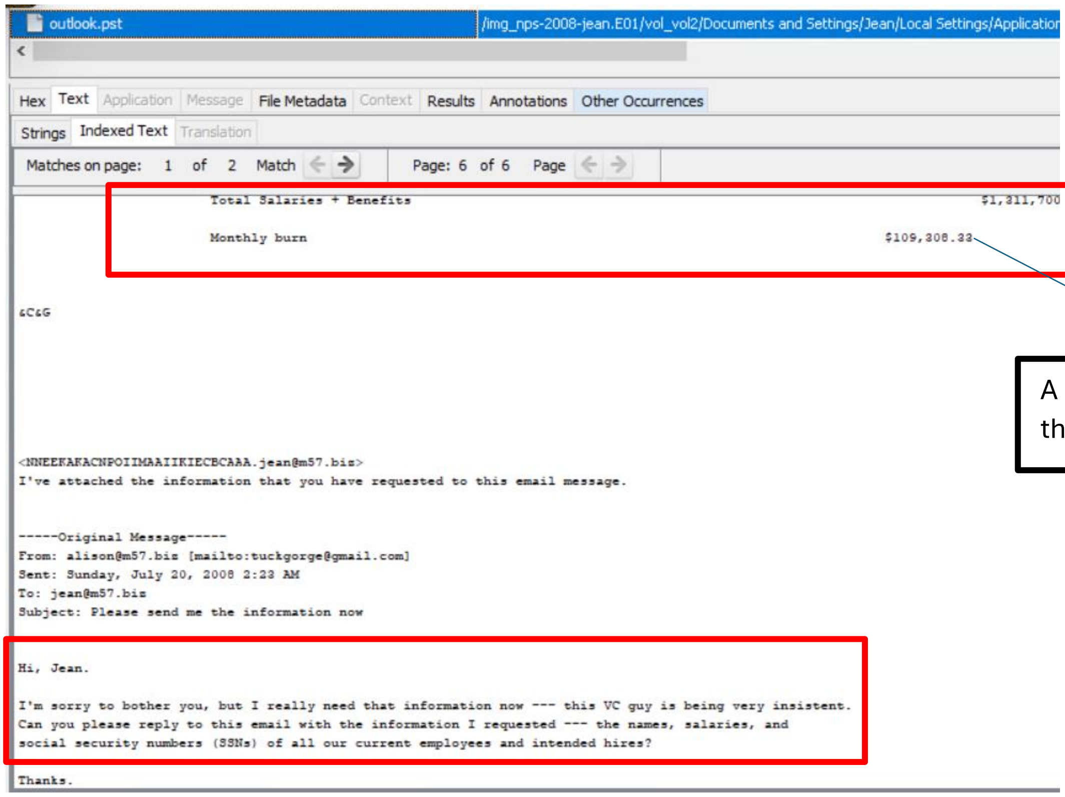
"Jean User" <jean@m57.biz> on behalf of "Jean User" <jean@m57.biz>

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

m57biz.xls	$XLS Microsoft Office Excel	291,840 bytes

2. **Autopsy:** Autopsy is another widely used open-source digital forensics platform. It's known for its user-friendly interface and powerful analysis capabilities.

   - **Metadata Verification:** By examining the metadata within Autopsy, I also verified the presence of the spreadsheet with the email conversation with the threat actor residing in the network and has the email **tuckgeorge@gmail.com.**



outook.pst /img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Local Settings/Application

Matches on page: 1 of 2 Match Page: 6 of 6 Page

```
                    Total Salaries + Benefits                                                  $1,311,700

                    Monthly burn                                                               $109,308.33


&C&G




<NNEEKAKACNPOIIMAAIIKIECBCAAA.jean@m57.biz>
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.
```

A snapshot about the attached .xls file

- **Investigator's Perspective:** This evidence strongly suggests that Jean was a victim of social engineering and email spoofing. However, it also highlights potential weaknesses in the company's data security practices. Jean, likely deceived by the spoofed email and the sense of urgency depicted by requests of threat actor claiming that a "VC guy" is insistent to get the spreadsheet, replies to tuckgorge@gmail.com with the attached spreadsheet.

- **Implication:** While Jean might not have had malicious intent, her actions inadvertently led to the data leak. The primary responsibility lies with the attacker who orchestrated the social engineering and email spoofing scheme.

- **Leak to Competitor**: The individual controlling tuckgorge@gmail.com, now in possession of the spreadsheet, proceeds to leak it to the competitor's website. The exact method of transfer (upload, copy/paste, sharing) remains to be determined through further investigation of the competitor's website and the attacker's online activity.

This analysis, supported by evidence from both Autopsy and Paraben E3, provides a plausible explanation for how the document reached the competitor's website. It highlights the importance of employee cybersecurity awareness and robust data protection measures to prevent such incidents.

Question 3. Who else from the company is involved?

Answer: Upon the analysis of all the email conversations, there are no direct evidence confirming that any other employee of the company is involved in this case. I have created a timeline of the events as found from the email conversations. Let's break down this information and analyse it from an investigator's perspective.

- **Path:** /img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst

- **Timeline of Events:**

The timeline constructed is very helpful in understanding the sequence of events leading up to the data leak:

1. **June 12th, 2008, 3:13 PM UTC:** Alison Smith creates the spreadsheet "m57biz.xls."
2. **July 19th, 2008:**

- **Afternoon:**
  - Jean accesses her email using Firefox (unusual for her).
  - Jean asks Alison about which email address she uses.
  - Alison informs Jean about a potential investor who needs employee information for background checks.
  - Alison sends emails to Jean using the alias "Alex," with a correction to her email address.
- **Evening:**
  - **6:22 PM PDT:** Someone using the email address tuckgorge@gmail.com sends a spoofed email to Jean, urgently requesting the spreadsheet.
  - **6:28 PM PDT:** Jean sends the spreadsheet to tuckgorge@gmail.com.
  - Someone using the email address tuckgorge@gmail.com sends another spoofed email to Jean, thanking her for the file and asking her to keep it confidential.

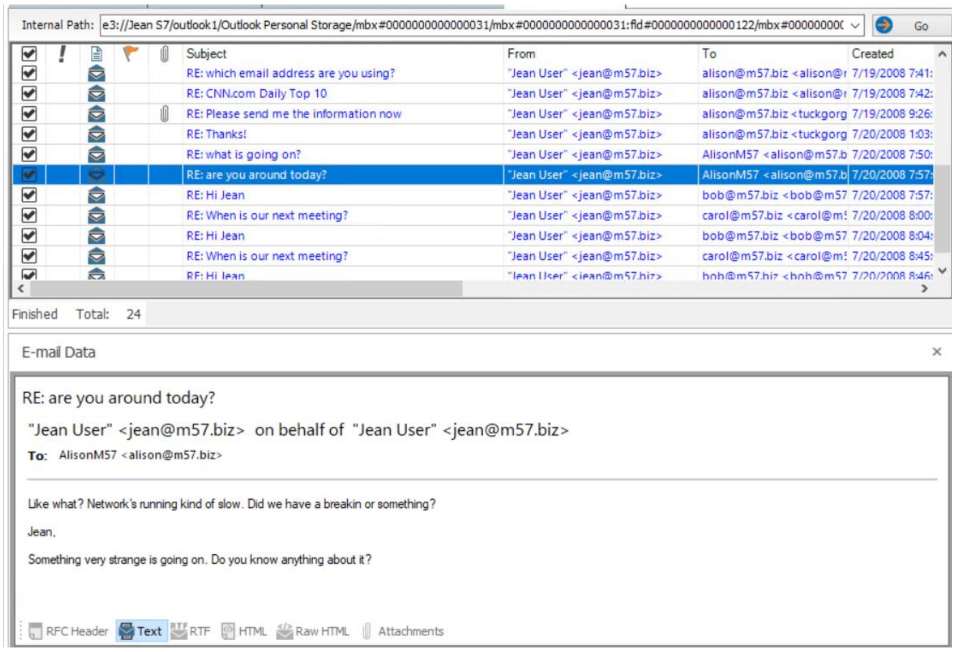
3. **July 20th, 2008:**

- **Morning:** Jean sends a thank-you email to tuckgorge@gmail.com.
- **Evening:**
  - Jean complains to Alison about slow network speed.
  - Bob and Carol confront Jean about their personal data being leaked online.

❖ **Data Exfiltration:**

- Jean, likely deceived by the spoofed email and the sense of urgency, replies to tuckgorge@gmail.com with the attached spreadsheet. This action inadvertently exposes sensitive employee data to an unknown individual.

❖ **Post incident activity:** This can also be proven from the conversation between Alison, Jean and other employees like Bob and Carol about this incident. This is evident from the email that Jane received from both Bob and Carol about their data breach. Also, there is a conversation among Jane and Alison about some suspicious activity in their network.



Internal Path: e3://Jean S7/outlook1/Outlook Personal Storage/mbx#0000000000000031/mbx#0000000000000031:fld#0000000000000122/mbx#0000000(

☑	Subject	From	To	Created
☑	RE: which email address are you using?	"Jean User" <jean@m57.biz>	alison@m57.biz <alison@r	7/19/2008 7:41:
☑	RE: CNN.com Daily Top 10	"Jean User" <jean@m57.biz>	alison@m57.biz <alison@r	7/19/2008 7:42:
☑	RE: Please send me the information now	"Jean User" <jean@m57.biz>	alison@m57.biz <tuckgorg	7/19/2008 9:26:
☑	RE: Thanks!	"Jean User" <jean@m57.biz>	alison@m57.biz <tuckgorg	7/20/2008 1:03:
☑	RE: what is going on?	"Jean User" <jean@m57.biz>	AlisonM57 <alison@m57.b	7/20/2008 7:50:
☑	RE: are you around today?	"Jean User" <jean@m57.biz>	AlisonM57 <alison@m57.b	7/20/2008 7:57:
☑	RE: Hi Jean	"Jean User" <jean@m57.biz>	bob@m57.biz <bob@m57	7/20/2008 7:57:
☑	RE: When is our next meeting?	"Jean User" <jean@m57.biz>	carol@m57.biz <carol@m!	7/20/2008 8:00:
☑	RE: Hi Jean	"Jean User" <jean@m57.biz>	bob@m57.biz <bob@m57	7/20/2008 8:04:
☑	RE: When is our next meeting?	"Jean User" <jean@m57.biz>	carol@m57.biz <carol@m!	7/20/2008 8:45:
☑	RE: Hi Jean	"Jean User" <jean@m57.biz>	bob@m57.biz <bob@m57	7/20/2008 8:46:

Finished Total: 24

E-mail Data

RE: are you around today?

"Jean User" <jean@m57.biz> on behalf of "Jean User" <jean@m57.biz>

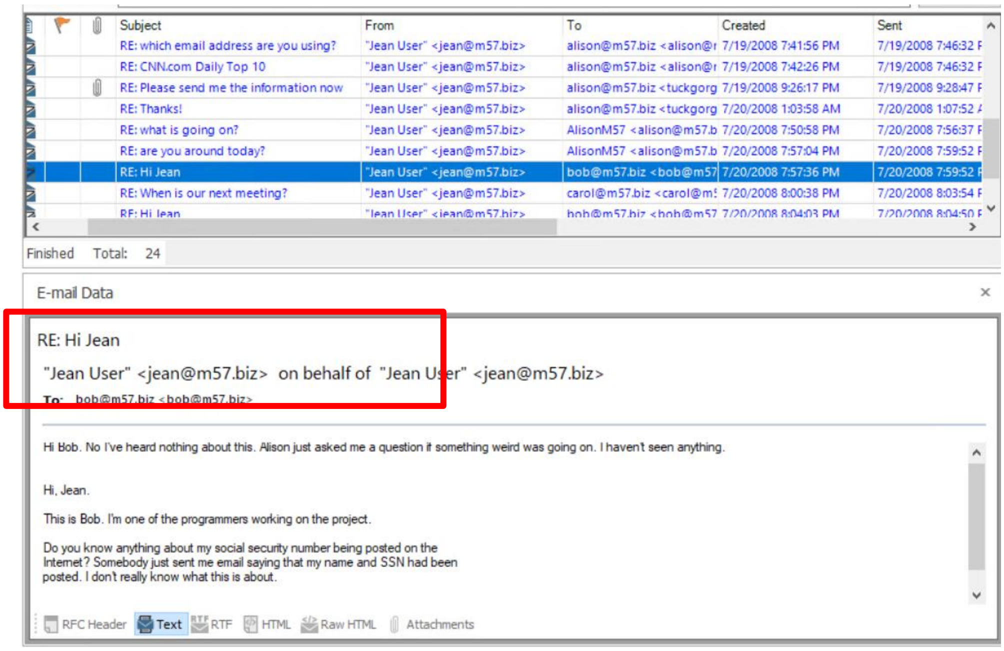
To: AlisonM57 <alison@m57.biz>

Like what? Network's running kind of slow. Did we have a breakin or something?

Jean,

Something very strange is going on. Do you know anything about it?

1. Email conversation between Alison and Jane about some issue in the network.



Subject	From	To	Created	Sent
RE: which email address are you using?	"Jean User" <jean@m57.biz>	alison@m57.biz <alison@r	7/19/2008 7:41:56 PM	7/19/2008 7:46:32 F
RE: CNN.com Daily Top 10	"Jean User" <jean@m57.biz>	alison@m57.biz <alison@r	7/19/2008 7:42:26 PM	7/19/2008 7:46:32 F
RE: Please send me the information now	"Jean User" <jean@m57.biz>	alison@m57.biz <tuckgorg	7/19/2008 9:26:17 PM	7/19/2008 9:28:47 F
RE: Thanks!	"Jean User" <jean@m57.biz>	alison@m57.biz <tuckgorg	7/20/2008 1:03:58 AM	7/20/2008 1:07:52 A
RE: what is going on?	"Jean User" <jean@m57.biz>	AlisonM57 <alison@m57.b	7/20/2008 7:50:58 PM	7/20/2008 7:56:37 F
RE: are you around today?	"Jean User" <jean@m57.biz>	AlisonM57 <alison@m57.b	7/20/2008 7:57:04 PM	7/20/2008 7:59:52 F
RE: Hi Jean	"Jean User" <jean@m57.biz>	bob@m57.biz <bob@m57	7/20/2008 7:57:36 PM	7/20/2008 7:59:52 F
RE: When is our next meeting?	"Jean User" <jean@m57.biz>	carol@m57.biz <carol@m!	7/20/2008 8:00:38 PM	7/20/2008 8:03:54 F
RE: Hi Jean	"Jean User" <jean@m57.biz>	bob@m57.biz <bob@m57	7/20/2008 8:04:03 PM	7/20/2008 8:04:50 F

Finished Total: 24

E-mail Data

RE: Hi Jean

"Jean User" <jean@m57.biz> on behalf of "Jean User" <jean@m57.biz>

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

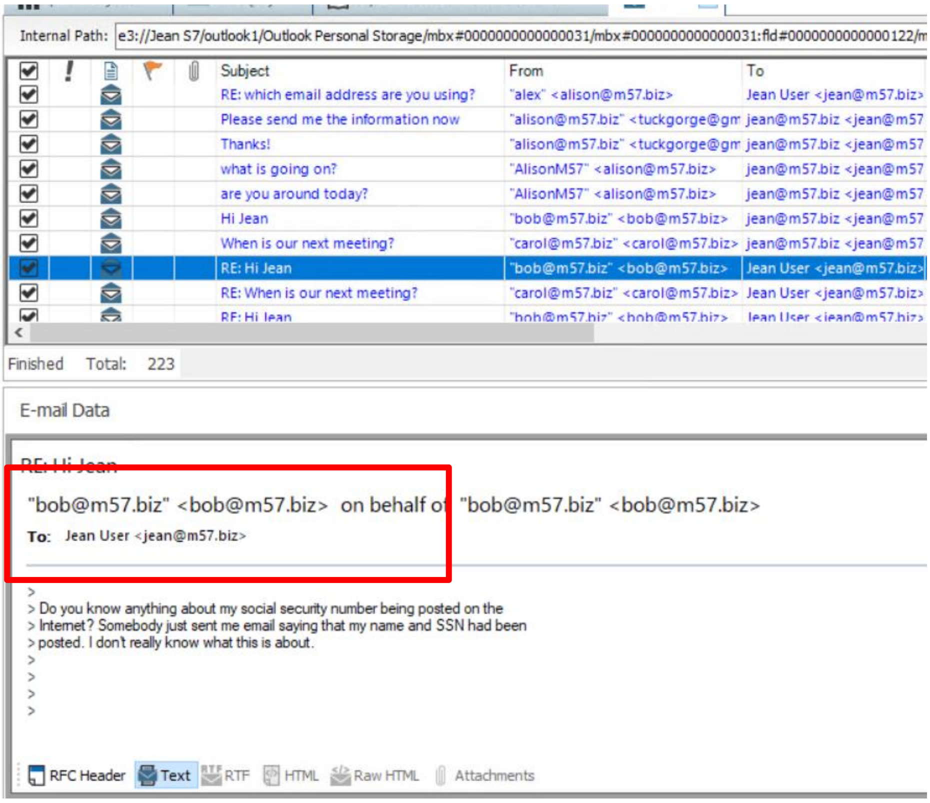
Hi Bob. No I've heard nothing about this. Alison just asked me a question if something weird was going on. I havent seen anything.

Hi, Jean.

This is Bob. I'm one of the programmers working on the project.

Do you know anything about my social security number being posted on the Internet? Somebody just sent me email saying that my name and SSN had been posted. I dont really know what this is about.

2. Bob and Carol mails Jane asking about the data leak



Internal Path: e3://Jean S7/outlook1/Outlook Personal Storage/mbx#0000000000000031/mbx#0000000000000031:fld#0000000000000122/m

☑	!				Subject	From	To
☑					RE: which email address are you using?	"alex" <alison@m57.biz>	Jean User <jean@m57.biz>
☑					Please send me the information now	"alison@m57.biz" <tuckgorge@gm	jean@m57.biz <jean@m57
☑					Thanks!	"alison@m57.biz" <tuckgorge@gm	jean@m57.biz <jean@m57
☑					what is going on?	"AlisonM57" <alison@m57.biz>	jean@m57.biz <jean@m57
☑					are you around today?	"AlisonM57" <alison@m57.biz>	jean@m57.biz <jean@m57
☑					Hi Jean	"bob@m57.biz" <bob@m57.biz>	jean@m57.biz <jean@m57
☑					When is our next meeting?	"carol@m57.biz" <carol@m57.biz>	jean@m57.biz <jean@m57
☑					RE: Hi Jean	"bob@m57.biz" <bob@m57.biz>	Jean User <jean@m57.biz>
☑					RE: When is our next meeting?	"carol@m57.biz" <carol@m57.biz>	Jean User <jean@m57.biz>
☑					RE: Hi Jean	"bob@m57.biz" <bob@m57.biz>	Jean User <jean@m57.biz>

Finished Total: 223

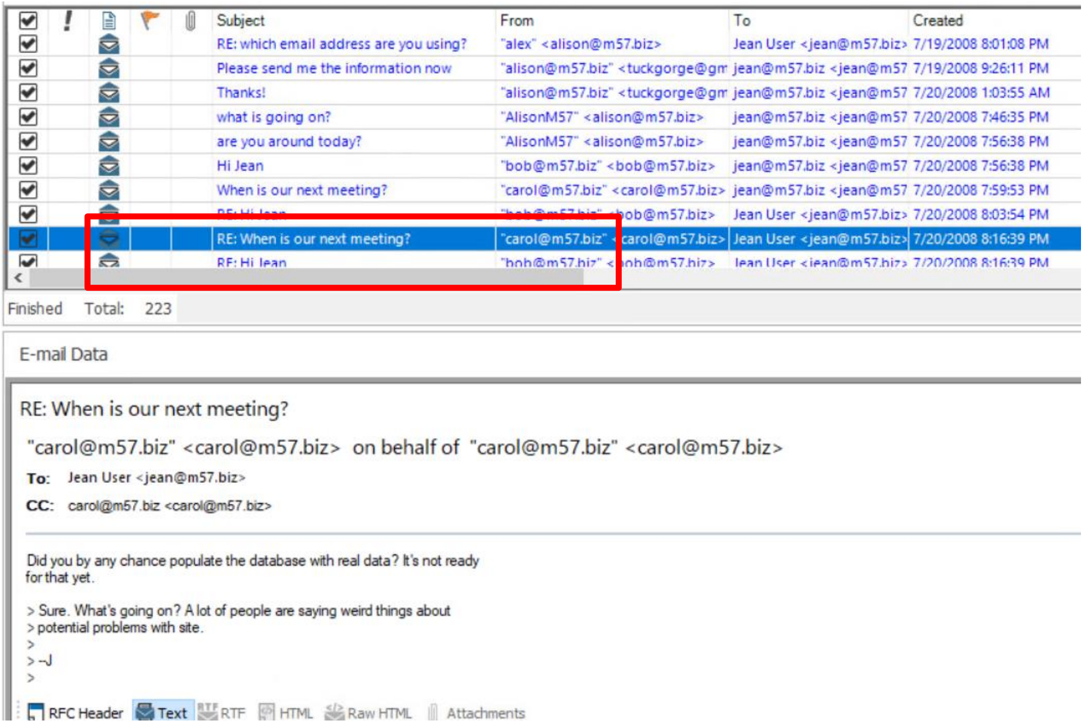
E-mail Data

RE: Hi Jean

"bob@m57.biz" <bob@m57.biz> on behalf of "bob@m57.biz" <bob@m57.biz>

To: Jean User <jean@m57.biz>

```
>
> Do you know anything about my social security number being posted on the
> Internet? Somebody just sent me email saying that my name and SSN had been
> posted. I don't really know what this is about.
>
>
>
>
```



☑	!				Subject	From	To	Created
☑					RE: which email address are you using?	"alex" <alison@m57.biz>	Jean User <jean@m57.biz>	7/19/2008 8:01:08 PM
☑					Please send me the information now	"alison@m57.biz" <tuckgorge@gm	jean@m57.biz <jean@m57	7/19/2008 9:26:11 PM
☑					Thanks!	"alison@m57.biz" <tuckgorge@gm	jean@m57.biz <jean@m57	7/20/2008 1:03:55 AM
☑					what is going on?	"AlisonM57" <alison@m57.biz>	jean@m57.biz <jean@m57	7/20/2008 7:46:35 PM
☑					are you around today?	"AlisonM57" <alison@m57.biz>	jean@m57.biz <jean@m57	7/20/2008 7:56:38 PM
☑					Hi Jean	"bob@m57.biz" <bob@m57.biz>	jean@m57.biz <jean@m57	7/20/2008 7:56:38 PM
☑					When is our next meeting?	"carol@m57.biz" <carol@m57.biz>	jean@m57.biz <jean@m57	7/20/2008 7:59:53 PM
☑					RE: Hi Jean	"bob@m57.biz" <bob@m57.biz>	Jean User <jean@m57.biz>	7/20/2008 8:03:54 PM
☑					RE: When is our next meeting?	"carol@m57.biz" <carol@m57.biz>	Jean User <jean@m57.biz>	7/20/2008 8:16:39 PM
☑					RE: Hi Jean	"bob@m57.biz" <bob@m57.biz>	Jean User <jean@m57.biz>	7/20/2008 8:16:39 PM

Finished Total: 223

E-mail Data

RE: When is our next meeting?

"carol@m57.biz" <carol@m57.biz> on behalf of "carol@m57.biz" <carol@m57.biz>

To: Jean User <jean@m57.biz>

CC: carol@m57.biz <carol@m57.biz>

```
Did you by any chance populate the database with real data? It's not ready
for that yet.

> Sure. What's going on? A lot of people are saying weird things about
> potential problems with site.
>
> --J
>
```

Jean M57 Exfiltration