FORENSIK DIGITAL TK2

THE CASE OF M57.BIZ

ALVARO AUSTIN - 2106752180

RAHFI ALYENDRA GIBRAN - 2106705764

AUSHAAF FADHILAH AZZAH - 2106630063

MOHAMMAD FERRY HUSNIL ARIF - 2106709112

RADEN MOHAMAD ADRIAN RAMADHAN HENDAR WIBAWA - 2106750540

CASE INTRODUCTION

You have been given:

- A copy of Jean's computer's hard drive
- A copy of the spreadsheet
- Autopsy

The client, one of the first-round funders, wants to know:

01 - CHECK METADATA

When did Jean create this spreadsheet?

02 - FIND OUT HOW

How did it get from her computer to competitor's website?

03 - FIND OUT WHO

Who else from the company is involved?

FACTS OF THE CASE

We know that there are some settings that happened in this case:

- M57.biz is a virtual corporation (they work online)
- Documents are usually exchanged by using email.

Document exfiltration happened because the document is sent by CFO Jean through her computer.

Jean (CFO):

- Alison asked me to prepare the spreadsheet as part of new funding round.
- Alison asked me to send the spreadsheet to her by email.
- That's all I know.

Alison (President):

- I don't know what Jean is talking about.
- I never asked Jean for the spreadsheet.
- I never received the spreadsheet by email.

WHAT CAN WE INFER?

Document exfiltration can be caused by several actions:

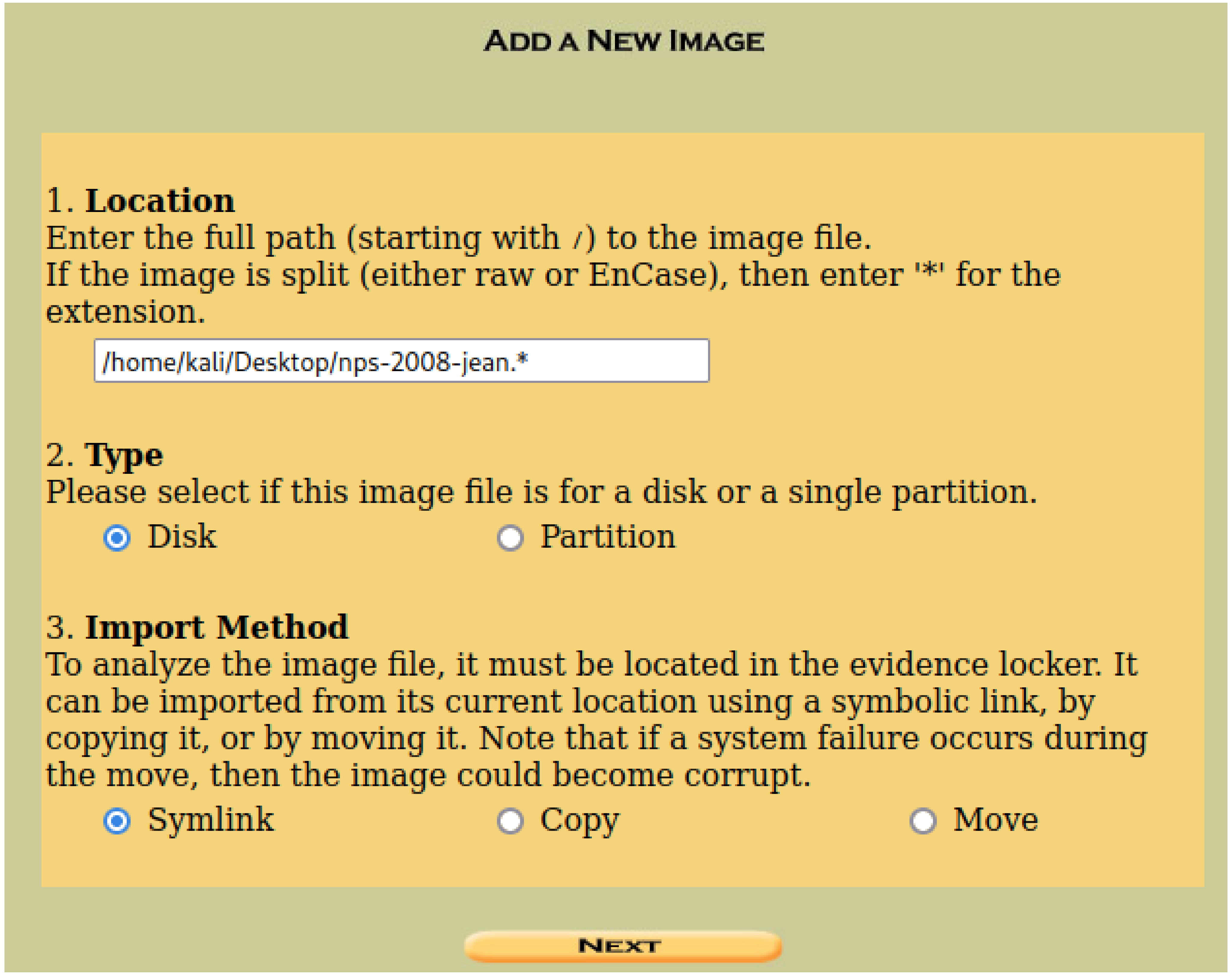
- inside threats
- outside threats

From the testimony by aliso (president), she doesn't remember that they receive emails, so we can narrow down the possibility of outside threats.

Hence we could focus on tracking down the email that has the attachment m57biz.xlsx. Because based from all the facts, we knew that the attack must come from the outside through email. But how? Lets find out!

AUTOPSY PREPARATION

The disk image files given was split into two (nps-2008-jean.E01 & nps-2008-jean.E02). By declaring the file location as **nps-2008-jean.***, Autopsy will open it as a single disk image.



ADD A NEW IMAGE

1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

/home/kali/Desktop/nps-2008-jean.*

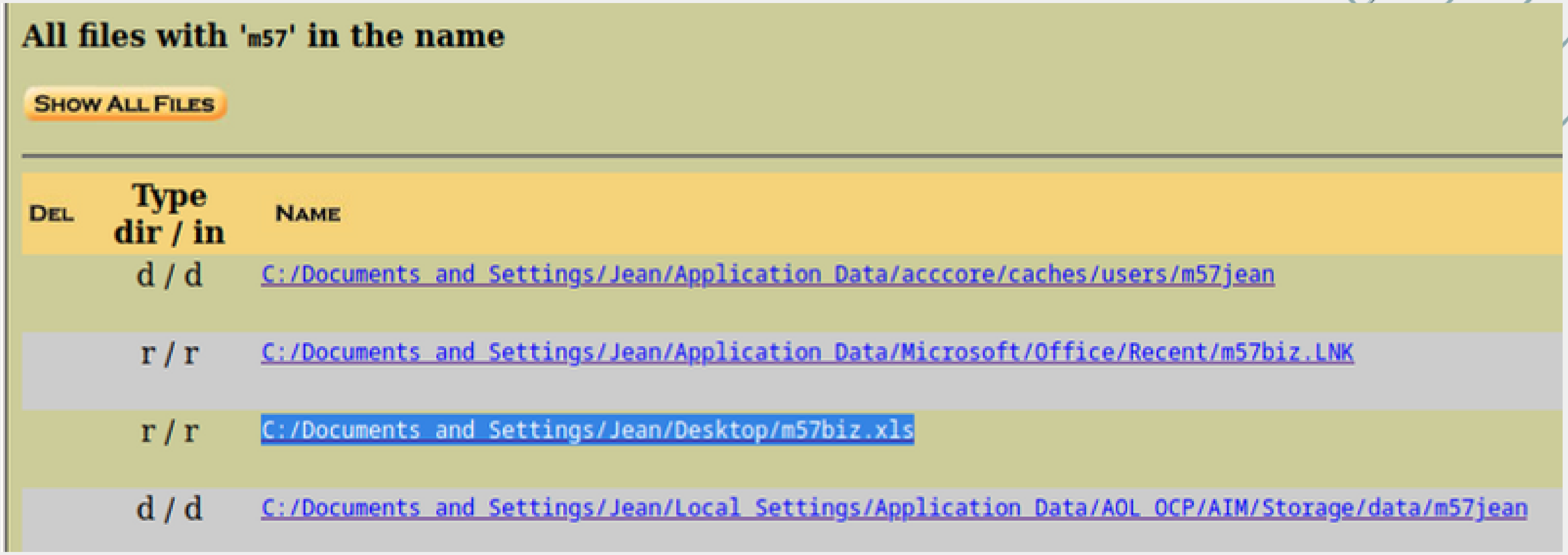
2. **Type**
Please select if this image file is for a disk or a single partition.

● Disk ○ Partition

3. **Import Method**
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

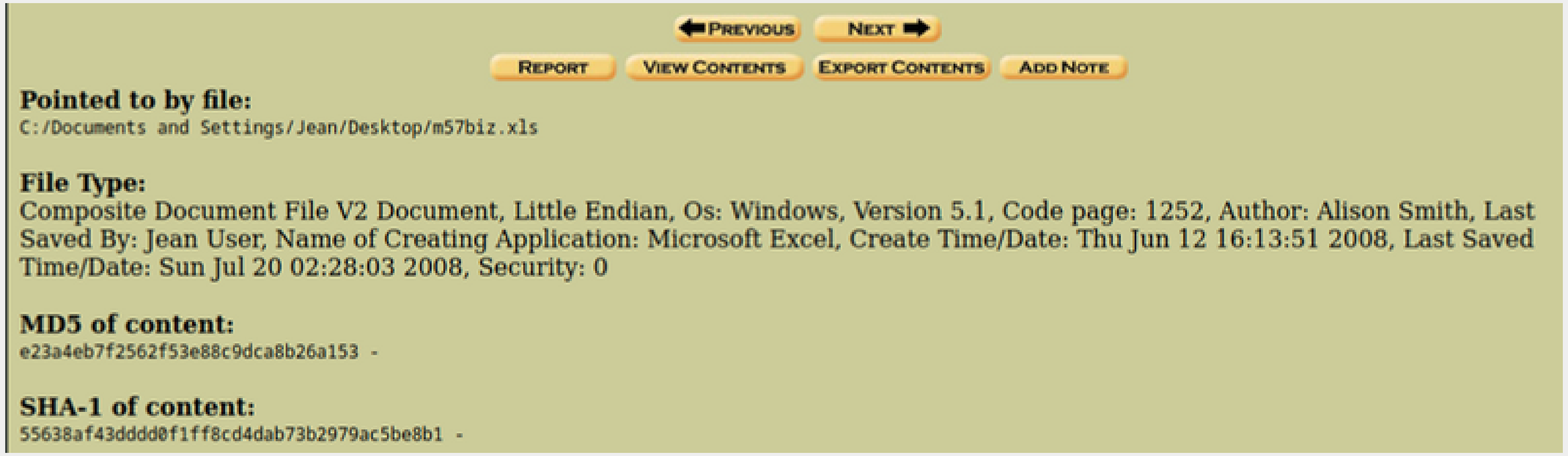
● Symlink ○ Copy ○ Move

Using **File Analysis** tab, we search for files containing “m57” in their name and found the spreadsheet **m57biz.xls**



All files with 'm57' in the name

Del	Type dir / in	Name
	d / d	C:/Documents and Settings/Jean/Application Data/acccore/caches/users/m57jean
	r / r	C:/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/m57biz.LNK
	r / r	C:/Documents and Settings/Jean/Desktop/m57biz.xls
	d / d	C:/Documents and Settings/Jean/Local Settings/Application Data/AOL OCP/AIM/Storage/data/m57jean



Pointed to by file:
C:/Documents and Settings/Jean/Desktop/m57biz.xls

File Type:
Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.1, Code page: 1252, Author: Alison Smith, Last Saved By: Jean User, Name of Creating Application: Microsoft Excel, Create Time/Date: Thu Jun 12 16:13:51 2008, Last Saved Time/Date: Sun Jul 20 02:28:03 2008, Security: 0

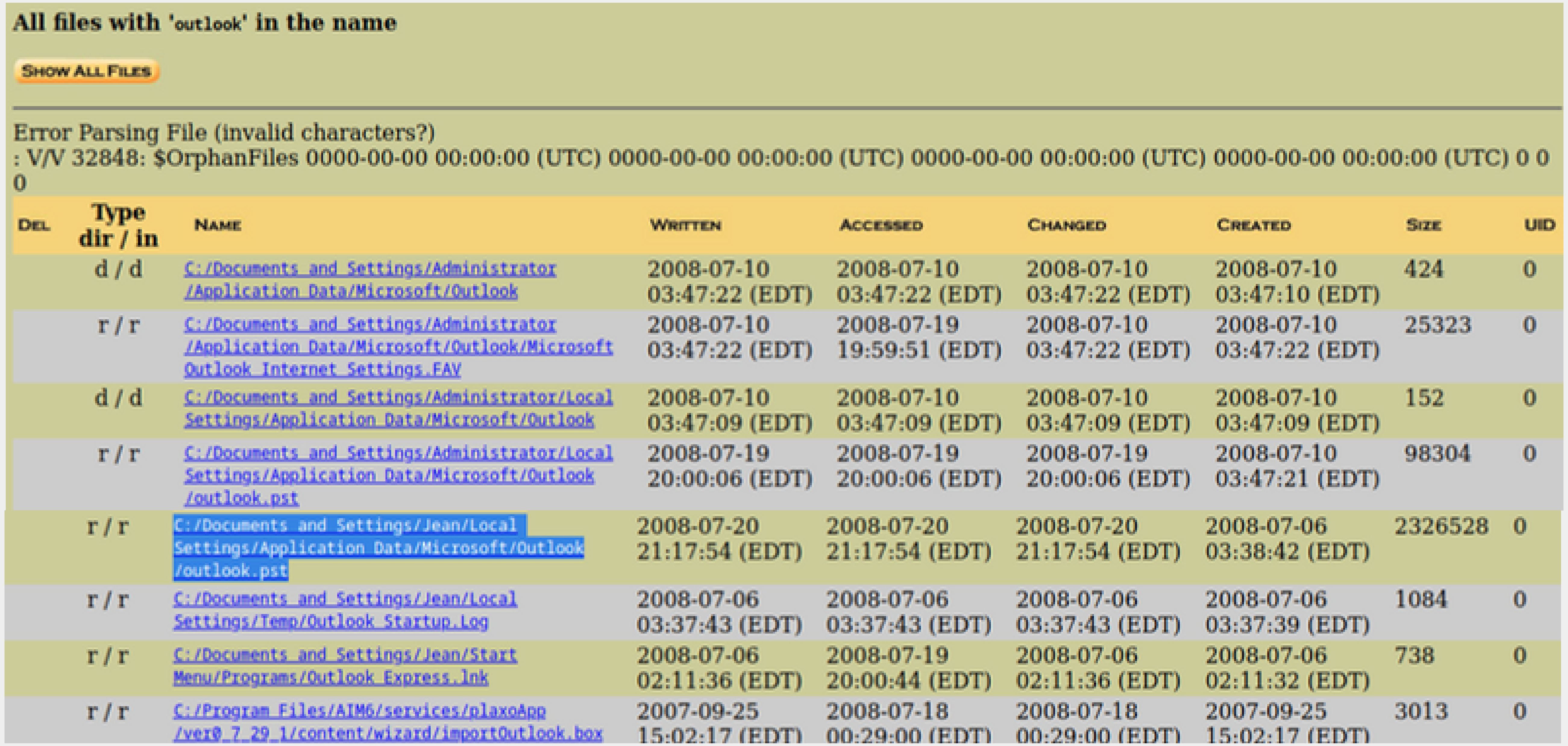
MD5 of content:
e23a4eb7f2562f53e88c9dca8b26a153 -

SHA-1 of content:
55638af43dddd0f1ff8cd4dab73b2979ac5be8b1 -

Clicking on the Metadata, we got the information that the file was actually created by **Alison** on **16:13:51, June 12th, 2008** but was last saved by Jean on 02:28:03, July 20th, 2008

According to the interviews, there is a contradiction. Jean claims Alison **requested the spreadsheet via email** but Alison denies this.

We will try to investigate Jean's email inbox which should be saved on Outlook's data file. We found it on **C:/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst**



All files with 'outlook' in the name

SHOW ALL FILES

Error Parsing File (invalid characters?)
: V/V 32848: $OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0

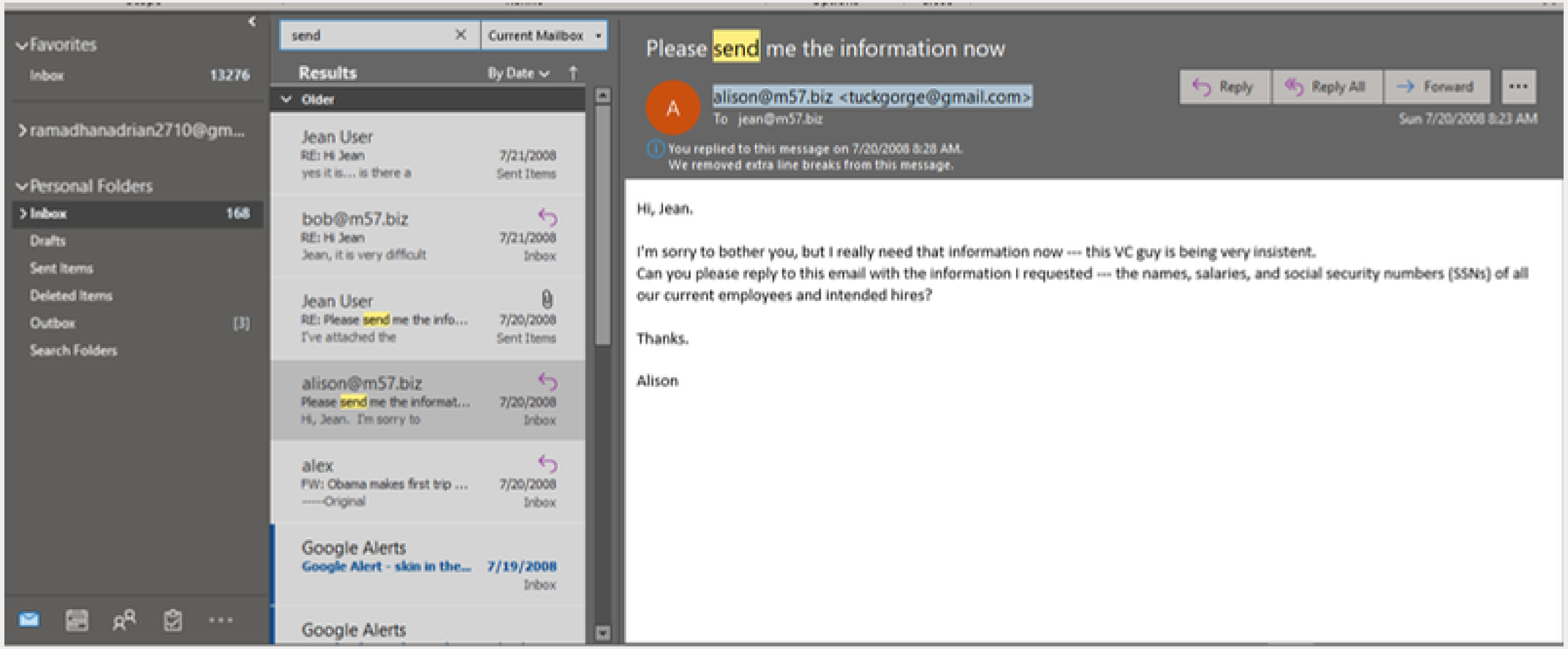
DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID
	d / d	C:/Documents and Settings/Administrator /Application Data/Microsoft/Outlook	2008-07-10 03:47:22 (EDT)	2008-07-10 03:47:22 (EDT)	2008-07-10 03:47:22 (EDT)	2008-07-10 03:47:10 (EDT)	424	0
	r / r	C:/Documents and Settings/Administrator /Application Data/Microsoft/Outlook/Microsoft Outlook Internet Settings.FAV	2008-07-10 03:47:22 (EDT)	2008-07-19 19:59:51 (EDT)	2008-07-10 03:47:22 (EDT)	2008-07-10 03:47:22 (EDT)	25323	0
	d / d	C:/Documents and Settings/Administrator/Local Settings/Application Data/Microsoft/Outlook	2008-07-10 03:47:09 (EDT)	2008-07-10 03:47:09 (EDT)	2008-07-10 03:47:09 (EDT)	2008-07-10 03:47:09 (EDT)	152	0
	r / r	C:/Documents and Settings/Administrator/Local Settings/Application Data/Microsoft/Outlook /outlook.pst	2008-07-19 20:00:06 (EDT)	2008-07-19 20:00:06 (EDT)	2008-07-19 20:00:06 (EDT)	2008-07-10 03:47:21 (EDT)	98304	0
	r / r	C:/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook /outlook.pst	2008-07-20 21:17:54 (EDT)	2008-07-20 21:17:54 (EDT)	2008-07-20 21:17:54 (EDT)	2008-07-06 03:38:42 (EDT)	2326528	0
	r / r	C:/Documents and Settings/Jean/Local Settings/Temp/Outlook Startup.Log	2008-07-06 03:37:43 (EDT)	2008-07-06 03:37:43 (EDT)	2008-07-06 03:37:43 (EDT)	2008-07-06 03:37:39 (EDT)	1084	0
	r / r	C:/Documents and Settings/Jean/Start Menu/Programs/Outlook Express.lnk	2008-07-06 02:11:36 (EDT)	2008-07-19 20:00:44 (EDT)	2008-07-06 02:11:36 (EDT)	2008-07-06 02:11:32 (EDT)	738	0
	r / r	C:/Program Files/AIM6/services/plaxoApp /ver0_7_29_1/content/wizard/importOutlook.box	2007-09-25 15:02:17 (EDT)	2008-07-18 00:29:00 (EDT)	2008-07-18 00:29:00 (EDT)	2007-09-25 15:02:17 (EDT)	3013	0

Exporting the **outlook.pst** file and opening it on Microsoft Outlook (on Windows) gives us access to Jean’s inbox.

After looking into it we found an email received from **alison@m57.biz <tuckgorge@gmail.com>** requesting Jean to send the file on 08:23 AM, July 20th 2008.

Notice how the actual sender email address is tuckgorge@gmail.com

alison@m57.biz is just the **display name**



Jean User
RE: Hi Jean 7/21/2008
yes it is.... is there a Sent Items

bob@m57.biz
RE: Hi Jean 7/21/2008
Jean, it is very difficult Inbox

Jean User
RE: Please send me the info... 7/20/2008
I've attached the Sent Items

alison@m57.biz
Please send me the informat... 7/20/2008
Hi, Jean. I'm sorry to Inbox

alex
FW: Obama makes first trip ... 7/20/2008
-----Original Inbox

Google Alerts
Google Alert - skin in the... 7/19/2008
Inbox

Google Alerts

Please send me the information now

alison@m57.biz <tuckgorge@gmail.com>
To jean@m57.biz
Sun 7/20/2008 8:23 AM

You replied to this message on 7/20/2008 8:28 AM.
We removed extra line breaks from this message.

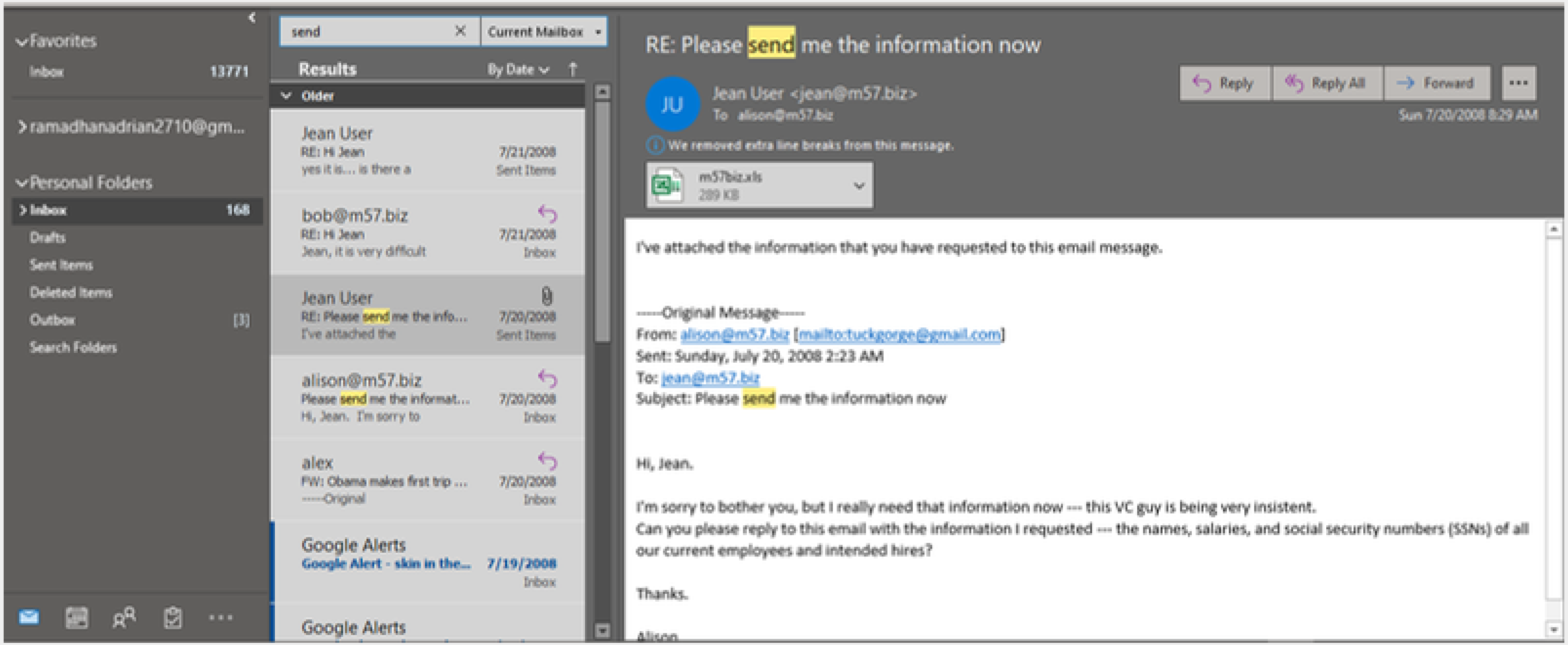
Hi, Jean.

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

We then found Jean’s response to that email sending the spreadsheet on **08:29 AM, July 20th 2008**, nine minutes after the request email.



Jean User
RE: Hi Jean
yes it is.... is there a
7/21/2008
Sent Items

bob@m57.biz
RE: Hi Jean
Jean, it is very difficult
7/21/2008
Inbox

Jean User
RE: Please send me the info...
I've attached the
7/20/2008
Sent Items

alison@m57.biz
Please send me the informat...
Hi, Jean. I'm sorry to
7/20/2008
Inbox

alex
FW: Obama makes first trip ...
-----Original
7/20/2008
Inbox

Google Alerts
Google Alert - skin in the...
7/19/2008
Inbox

Google Alerts

RE: Please send me the information now

JU Jean User <jean@m57.biz>
To alison@m57.biz
Sun 7/20/2008 8:29 AM

We removed extra line breaks from this message.

m57biz.xls
289 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

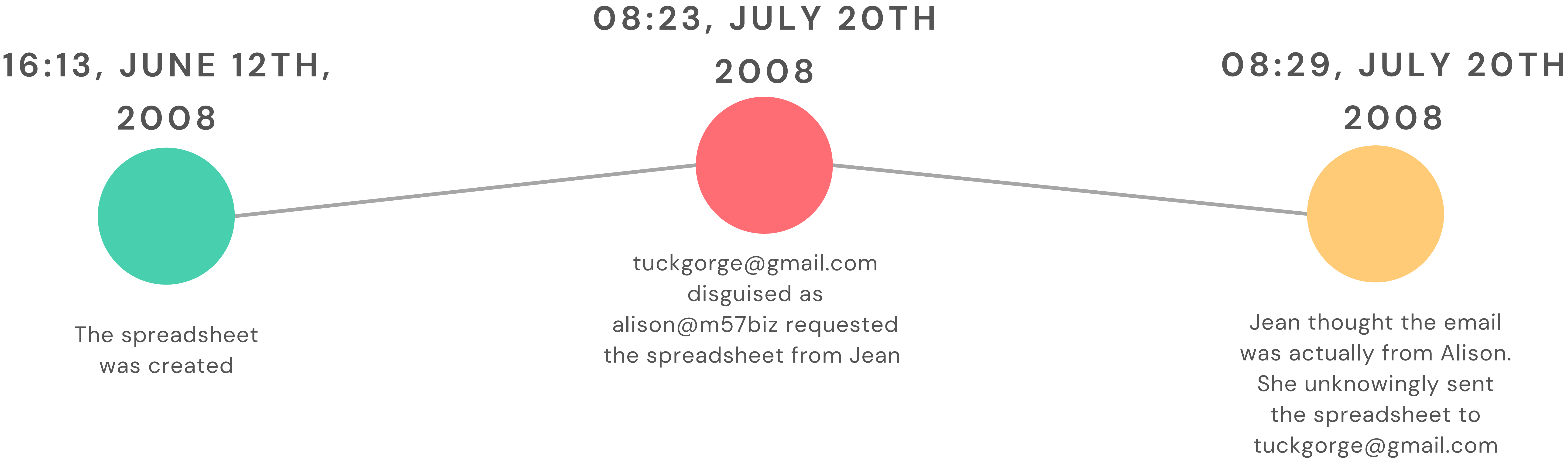
Hi, Jean.

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

CHRONOLOGY OF THE CASE



16:13, JUNE 12TH, 2008

The spreadsheet was created

08:23, JULY 20TH 2008

tuckgorge@gmail.com disguised as alison@m57biz requested the spreadsheet from Jean

08:29, JULY 20TH 2008

Jean thought the email was actually from Alison. She unknowingly sent the spreadsheet to tuckgorge@gmail.com

WHAT HAPPENED?

So someone with the email **tuckgorge@gmail.com** forged their own email to be viewed as **alison@m57biz**. This causes Jean to be convinced that the email is from Alison herself. This incident is called Email Spoofing.

EMAIL SPOOFING

Email spoofing is a type of cyberattack that targets businesses by using emails with forged sender addresses. Attacker could do this by changes field within the message headers (such as the changing FROM, REPLY-TO, and RETURN-PATH).

CASE SUMMARY

We believe that what happened was
a case of Email Spoofing.

Questions answered:

1. When did Jean create this spreadsheet?
   - The spreadsheet created by Alison on 16:13:51, June 12th, 2008 but was last saved by Jean on 02:28:03, July 20th, 2008
2. How did it get from her computer to competitor's website?
   - Through email sent by Jean because tuckgorge@gmail.com disguised as Alison utilizing email spoofing.
3. Who else from the company is involved?
   - We couldn’t find anyone from the company that’s involved in this case except Jean and Alison (through her email).

THANK YOU