TITLE PAGE

DIGITAL FORENSICS

PROJECT REPORT

CASE: DOCUMENT EXFILTRATION

INVESTIGATORS:

- **MUHAMMAD ARMUGHAN 19I-1685**
- **SYED BAHADUR ALI SHAH 19I-1783**
- **SAHIL RAJA 19I-1755**

DATE:15’06’2021

TABLE OF CONTENTS

TITLE PAGE 1
TABLE OF CONTENTS 2
ABSTRACT 3
SUSPECT SUMMARY 3
EVIDENCE 4
OBJECTIVES 4
CHAIN OF CUSTODY 5
FORENSIC ANALYSIS (STEPS TAKEN) 5
RELEVANT FINDINGS 6
CONCLUSION 8
References 9

ABSTRACT

M57.biz is a hip web start-up developing a body art catalog. A spreadsheet containing confidential information was leaked to the competitor's company by someone inside the M57.biz but there was no proof of who was the culprit behind this act of treachery. So, we as a team of digital forensics decided to perform a thorough digital forensics investigation to find out the culprit in this case. We have been given an image of Jean's computer's hard drive and the spreadsheet file which was leaked by the culprit.

Facts of the case:

• $3M in seed funding; now closing $10M round

• 2 founder/owners

• 10 employees hired first year

Current staff

• President: Alison Smith

• CFO: Jean

• Programmers: Bob, Carole, David, Emmy

• Marketing: Gina, Harris

• BizDev: Indy

SUSPECT SUMMARY

After the leak was known to all the team, some interviews were conducted from the team members to have a record of their saying on the issue. Following are the statements of President and CFO of the company.

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.

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

Since there was a clear contradiction between the statements of the major people of the company who could only have the access to the spreadsheet file containing the confidential information so it was obvious to put these two people under the suspect category because no-one else other than these two had even a little knowledge about the spreadsheet document.

EVIDENCE

Sheet1

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

This was the spreadsheet file that contained the confidential data as shown.

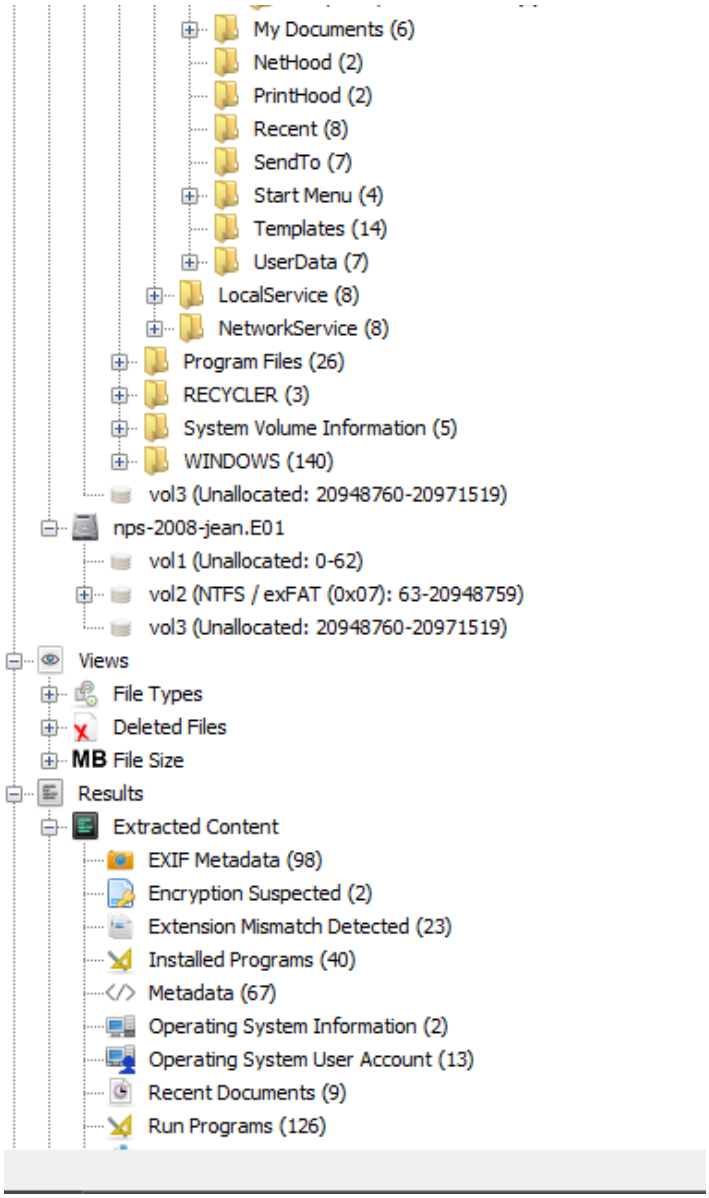
OBJECTIVES

The client, one the first-round funders of the company want to know the following things:

- When did Jean create the spreadsheet containing confidential information?
- How did it get leaked/transferred from her laptop?
- Who else from the company was involved in this treachery?

CHAIN OF CUSTODY

#	Evidence	From	To	Date
1	nps-2008-jean	Digital Corpora	Armughan	12’06’2021
2	nps-2008-jean	Armughan	Sahil	13’06’2021
3	nps-2008-jean	Sahil	Bahadur	14’06’2021



FORENSIC ANALYSIS (STEPS TAKEN)

The very first step to start the forensics after downloading the provided image of Jean’s laptop was to create a new case in the autopsy tool and adding the provided image. It took almost two to three hours for analyzing the data in the image completely. The tool categorizes all the data accordingly as shown in the attached screenshot so, it becomes very easy to perform forensics on it. Initially, we started exploring the folders for the spreadsheet file or any other important data related to the case as the image had massive amount of data to analyze so it took a lot of time but the investigators were not to give up soon. We checked all the categories one by one for any valuable information present and added up everything we could find relatable below the heading of relevant findings. The image didn’t only contain files of user Jean but there were other users of the laptop also so, we checked their data in the hope of finding something relatable to the file but no luck there.

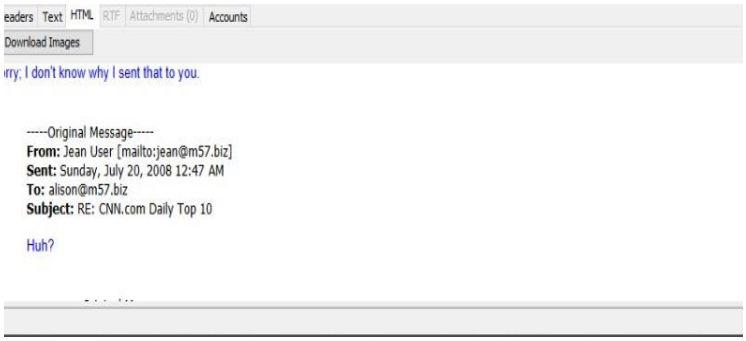
RELEVANT FINDINGS

```
-----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.
```



Jean,

Please do not send me links like this. I have no way of knowing if they are from you or from some hacker.

Thanks.

Alison.

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

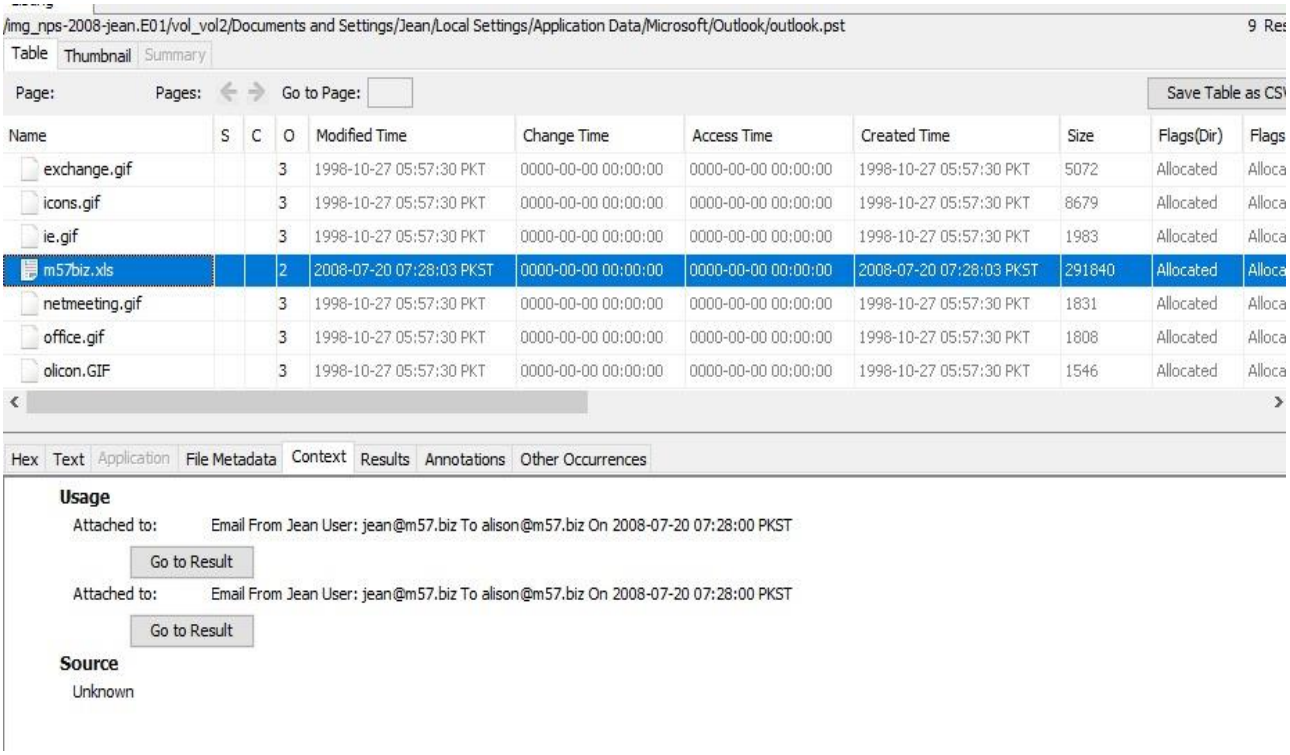
Hi Jean. I'm sorry to bother you, but I really need that information now --- this VC guy is being very insistent.

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

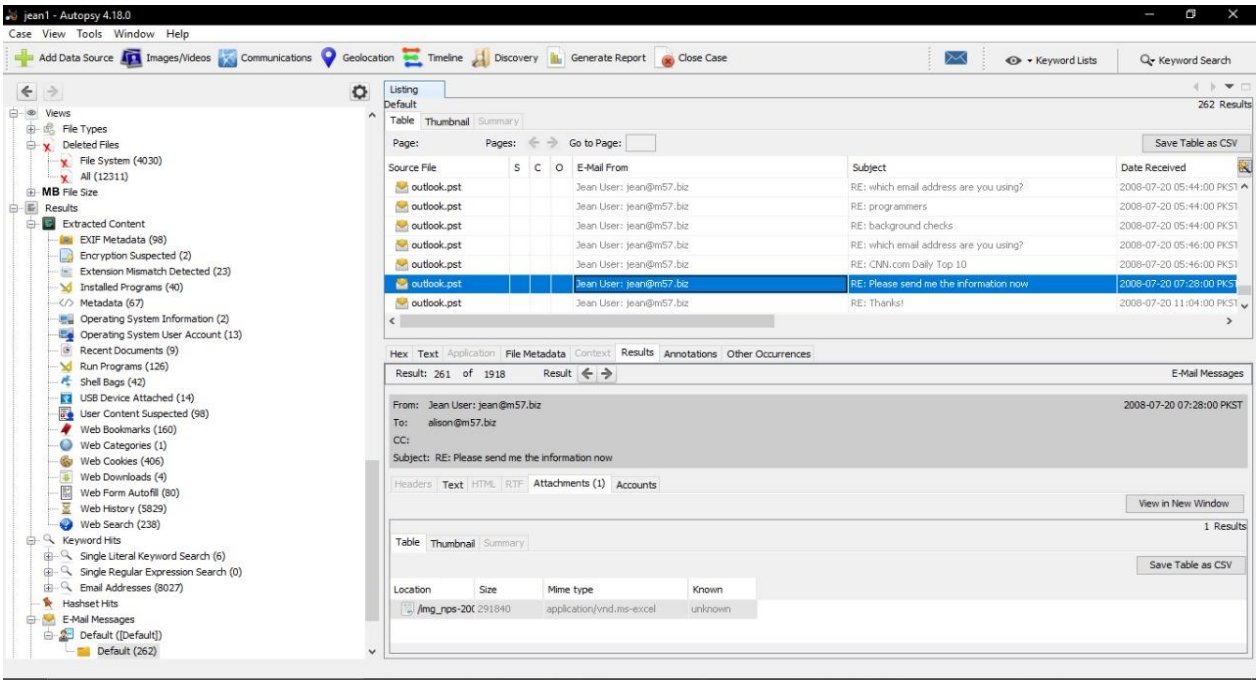
These were some relevant findings about the case from the email conversation between Alison and Jean which shows that there were some confusions related to email addresses between the both and they believed to be exposed to hacking.



After a thorough search of the jean's laptop, we were finally able to locate the spreadsheet file which had the confidential information. The file had two occurrences one was placed the desktop of jean's laptop while the other was found as an attachment in the outlook directory which gave us the path to our second objective and we dug in further to find out more about the second occurrence of the file.

Type	Value
Organization	M57.BIZ
Date Modified	2008-07-20 01:28:03
Program Name	Microsoft Excel
Date Created	2008-06-12 15:13:51
User ID	Jean User
Owner	Alison Smith
Source File Path	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Desktop/m57biz.xls
Artifact ID	-9223372036854772211

Attached above are the details about the spreadsheet file fetched using the help of autopsy tool. As you can see the date and time of creation of the file which is our first objective asked by the client. In addition to the date and time it can be seen that the owner of the file was Alison Smith and the User ID is of Jean which makes our doubt on the suspect more solid since now we have the proof that only these two people were involved with the file and either one of them is involved in leakage or both of them.



At last, we were finally able to find the second occurrence of the spreadsheet document in the outlook folder of user jean which gave us complete details that Alison asked Jean about the information and Jean sent the confidential file to her email address in reply to her mail. Jean also attached a bogus picture so that the file doesn't look like something confidential which for an instance made us thought that she just sent a picture but we opened the attachment it was the same spreadsheet file which was leaked.

CONCLUSION

In the end, we conclude after a thorough forensics of Jean's laptop that Alison the president of the company lied that she didn't ask Jean for any spreadsheet but we have solid proof that Alison did ask Jean for the spreadsheet file and Jean did send the required document which proves that Jean was telling the truth and Alison did the treachery by leaking the confidential information and planned to put the blame on Jean.

References

Case taken from:

- https://digitalcorpora.org/corpora/scenarios/m57-jean

Tool used:

- https://www.autopsy.com

Under the jurisdiction and rules:

- http://nu.edu.pk