Forensics Report

Michelle Pantelouris

Digital Forensics Report

INVESTIGATOR:	**Michelle Pantelouris**
	0001
	United Kingdom

SUBJECT:	**Digital Forensics Examination Report**
Accused 1:	Jean
Offence:	Hacking and leaking sensitive information
Date of Request:	7th December, 2021
Date of Conclusion:	16th December, 2021
Report Publish Date:	17th December, 2021

Contents

Overview/Objectives of the Case

This case is for a start-up company called M57.Biz. A few weeks into them starting a spreadsheet with all of the employees SSN's and salaries were found on a competitor's website. The only place the file existed was on the CFO's (Jean) laptop.

I was given a disk image of Jean's laptop to examine and to answer the following questions:

- When did Jean create this spreadsheet?
- How did it get from her computer to competitor's website?
- Who else from the company is involved?

I have created a logbook with all of the evidence I found, when I found it and what time I found it.

In this report I will summarise my findings and conclude who I think the suspect is.

Facts of the Case

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

Programmers:

- Work out of their houses
- Daily online chat session; Weekly in-person meetings office park

Marketing & BizDev:

- Work out of hotel rooms or Starbucks (mostly on the road)
- In-person meetings once every two weeks.
- Most documents are exchanged by email.

Interviews

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.

Investigation Steps

- Scanned image for viruses
- Imported image to Autopsy
- Found hash value of Image
- Checked which operating system the laptop was using
- Investigated emails
- Investigated documents and images
- Logged all of my evidence in a logbook

Timestamp of Evidence

In this section I will be providing the timestamp of the most suspicious emails in this case, along with a brief explanation of the emails.

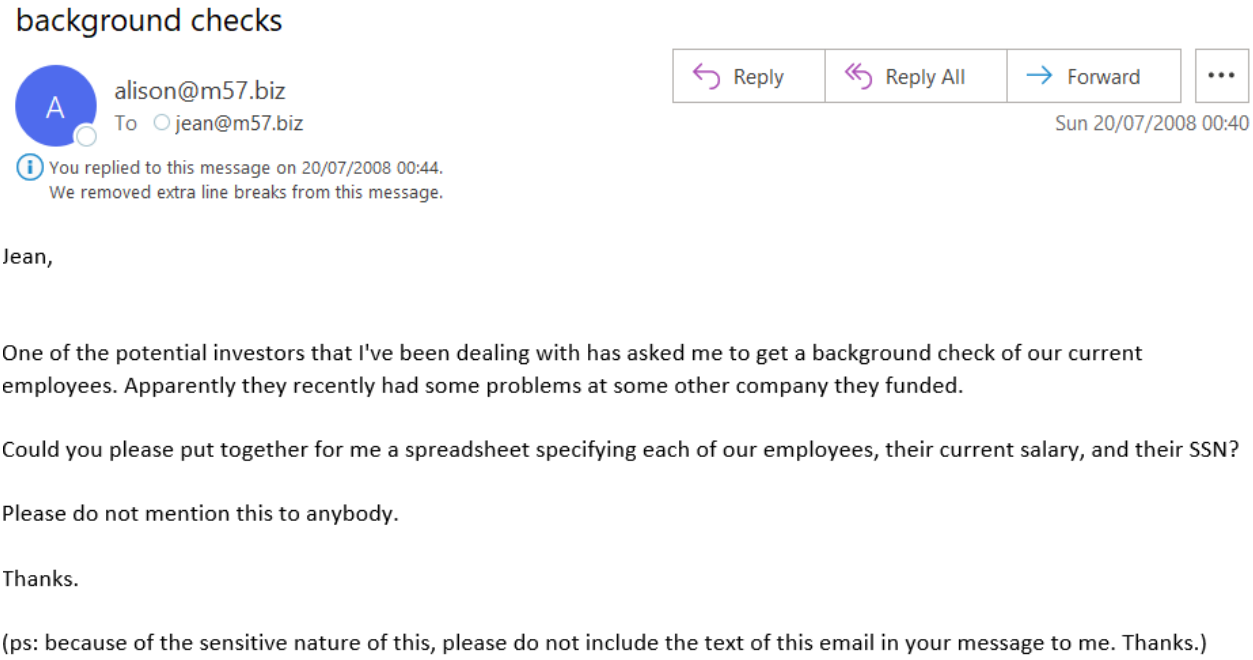
Timestamp	To and From	Message
20/07/2008, 00:44	To Jean from Alison	Asking for SSN's and salaries of all of the employees and asking jean to not tell anyone.
20/07/2008, 00:46	To Jean from Alison	After asking for the information Jean said it would be a sure thing and Alison replied back saying what's a sure thing?
20/07/2008, 00:57	To Jean from Alison	Alison saying that something strange is going on.
20/07/2008, 02:23	To Jean from Alison	Demanding she needs the information now as the VC guy needed it.
20/07/2008, 02:23	To Alison from Jean	Excel file is sent
20/07/2008, 06:04	To Jean from Alison	Thanking Jean for the file and yet again telling her not to tell anyone about it.
06/07/2008, 20:25	To Jean from Alison	Asking Jean not to send her certain links as she doesn't know if its from her or a hacker.

Evidence

In this section I will be showing the main evidence that shows who the suspects are.

Evidence 1.0

This email is the first bit of evidence. It was sent by Alison requesting the SSN's and salaries of all of the employees. What struck me as odd was the fact that Alison said not to tell anyone considering it is all of their information that is needed.



background checks

A alison@m57.biz
To jean@m57.biz

Reply | Reply All | Forward | ...

Sun 20/07/2008 00:40

You replied to this message on 20/07/2008 00:44.
We removed extra line breaks from this message.

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?

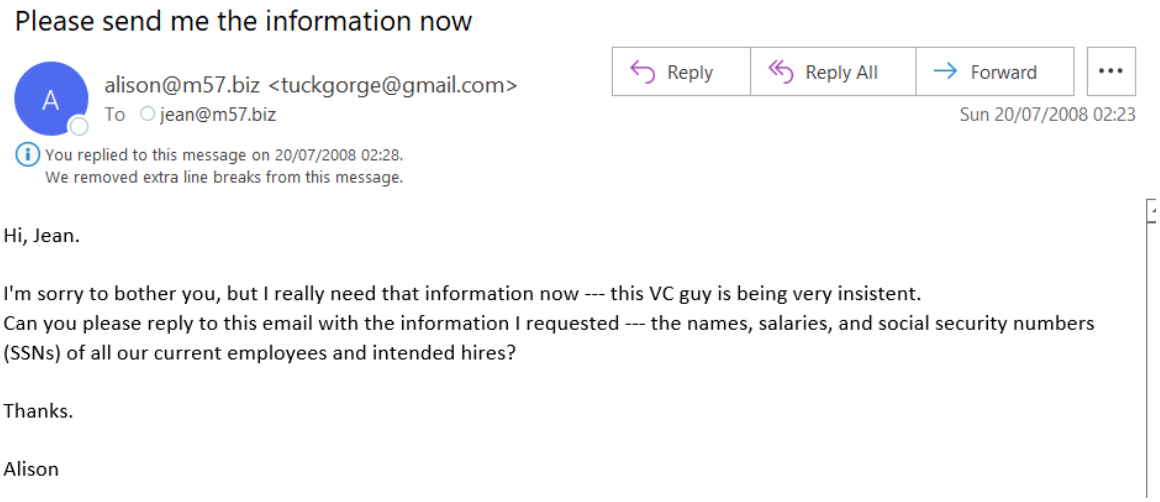
Please do not mention this to anybody.

Thanks.

(ps: because of the sensitive nature of this, please do not include the text of this email in your message to me. Thanks.)

Evidence2.0

This email is one of the pieces of evidence that caught my eye, due to the email address being different from the previous ones Allison used. This email was sent by tuckgorge@gmail.com. I suspect this person is spoofing. There are three other emails associated with this email address. Which means the information was given to the imposter.



Please send me the information now

A alison@m57.biz <tuckgorge@gmail.com>
To jean@m57.biz

Reply | Reply All | Forward | ...

Sun 20/07/2008 02:23

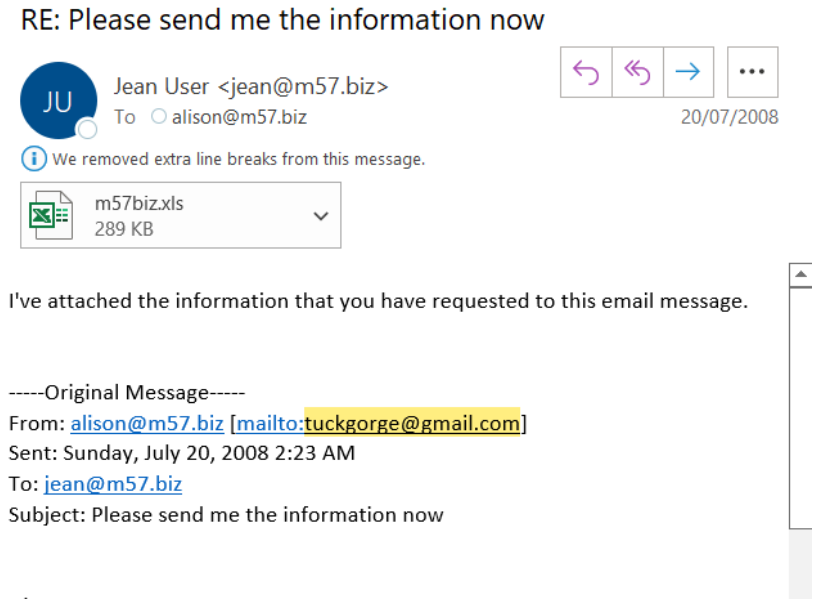
You replied to this message on 20/07/2008 02:28.
We removed extra line breaks from this message.

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



RE: Please send me the information now

JU Jean User <jean@m57.biz>
To alison@m57.biz

20/07/2008

We removed extra line breaks from this message.

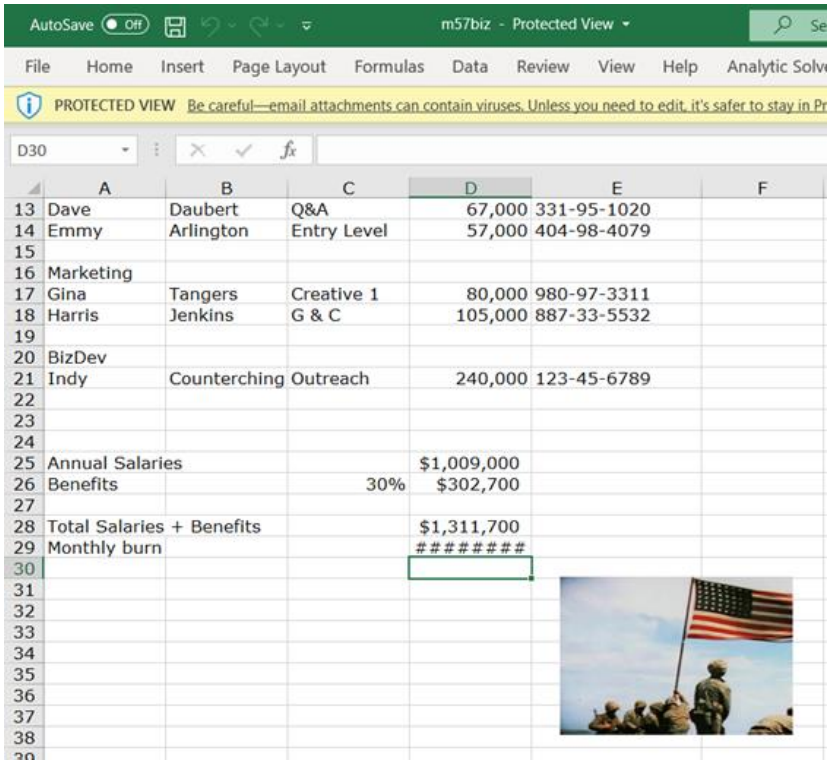
m57biz.xls
289 KB

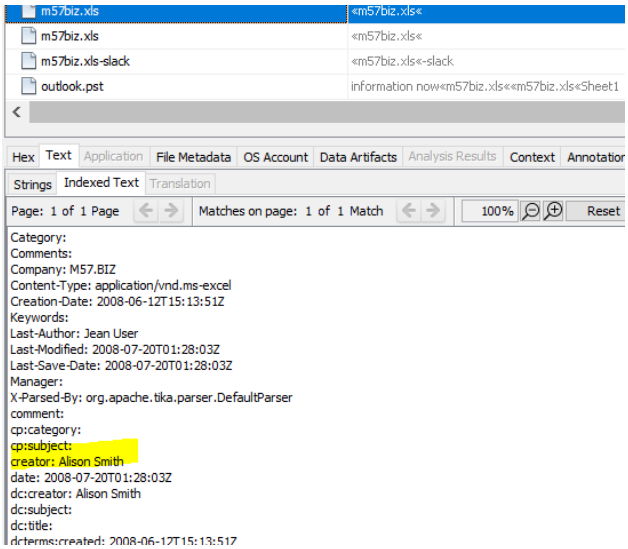
I've attached the information that you have requested to this email message.

-----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

Evidence 3.0

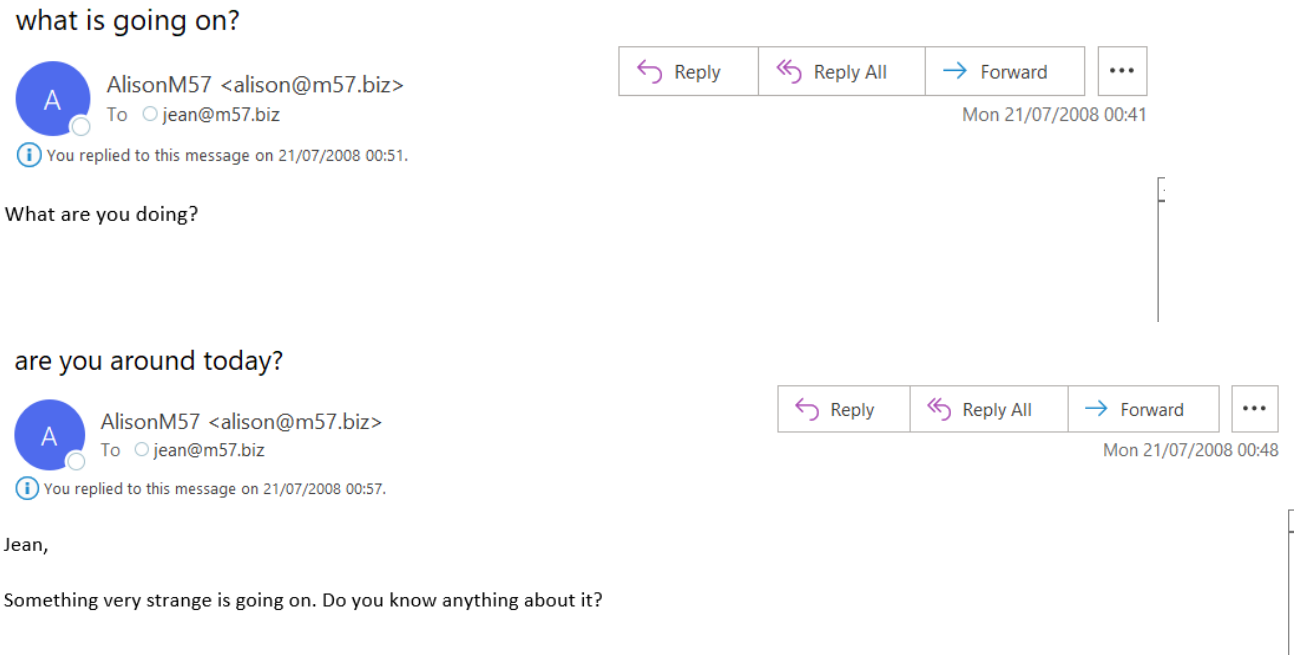
The file that was sent to tuckgorge@gmail.com was this excel file with all of the information that was needed. After some more investigation on autopsy, I realised it was created by Alison on the 2008-06-12 at 15:13 and not my Jean as first anticipated.





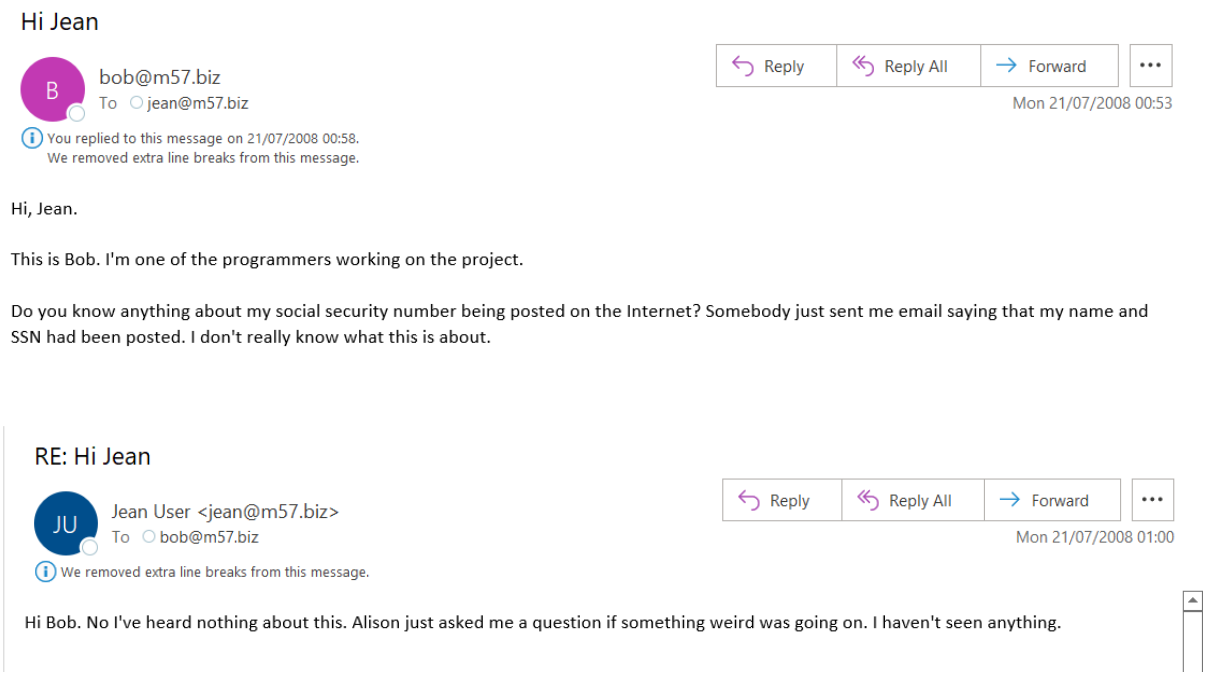
Evidence 4.0

Some emails from Alison asking Jean what she is going and what is going on. This shows me that she doesn't know what is happening and is suspicious that Jean is doing something wrong. It is sent by a different email from the other ones which shows to me this is the real Alison.



Evidence 5.0

This email from one of programmers saying that all of their information has been posted online and asking if she knew about it, which she denies knowing.



Hi Jean

B bob@m57.biz
To jean@m57.biz

Reply | Reply All | Forward | ...
Mon 21/07/2008 00:53

You replied to this message on 21/07/2008 00:58.
We removed extra line breaks from this message.

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 don't really know what this is about.

RE: Hi Jean

JU Jean User <jean@m57.biz>
To bob@m57.biz

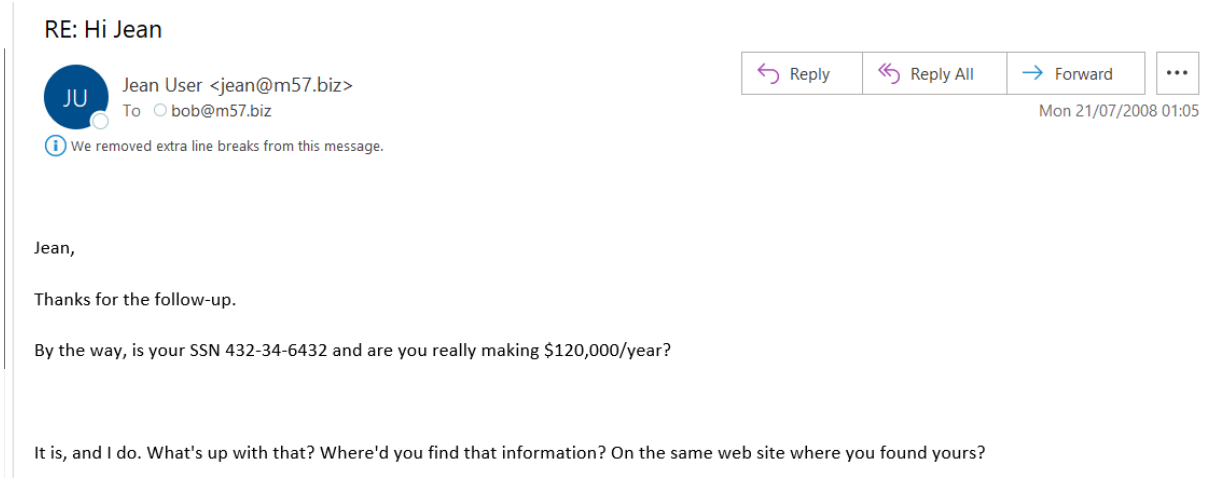
Reply | Reply All | Forward | ...
Mon 21/07/2008 01:00

We removed extra line breaks from this message.

Hi Bob. No I've heard nothing about this. Alison just asked me a question if something weird was going on. I haven't seen anything.

Evidence 6.0

Bob then sent another email with Jeans social security number and salary and asked if it was her. She said it was which confirms that the information was posted online.



RE: Hi Jean

JU Jean User <jean@m57.biz>
To bob@m57.biz

Reply | Reply All | Forward | ...
Mon 21/07/2008 01:05

We removed extra line breaks from this message.

Jean,

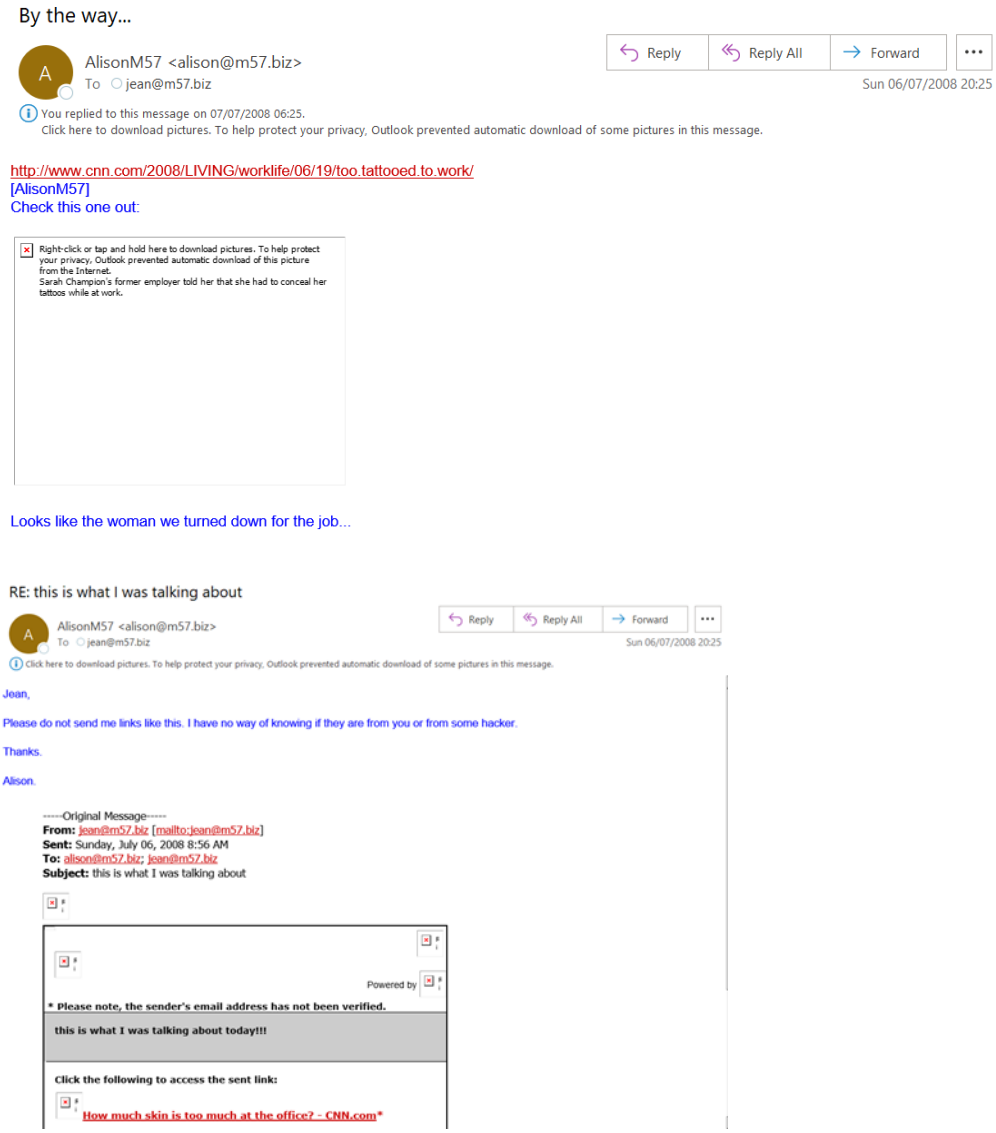
Thanks for the follow-up.

By the way, is your SSN 432-34-6432 and are you really making $120,000/year?

It is, and I do. What's up with that? Where'd you find that information? On the same web site where you found yours?

Evidence 7.0

These emails between Alison and Jean about someone they rejected for a job then Alison going on about her not knowing if it's from Jean or a hacker, which shows me that this sort of thing has happened before.



By the way…

AlisonM57 <alison@m57.biz>
To jean@m57.biz

Reply | Reply All | Forward | …

Sun 06/07/2008 20:25

You replied to this message on 07/07/2008 06:25.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

http://www.cnn.com/2008/LIVING/worklife/06/19/too.tattooed.to.work/
[AlisonM57]
Check this one out:

Right-click or tap and hold here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.
Sarah Champion's former employer told her that she had to conceal her tattoos while at work.

Looks like the woman we turned down for the job…

RE: this is what I was talking about

AlisonM57 <alison@m57.biz>
To jean@m57.biz

Reply | Reply All | Forward | …

Sun 06/07/2008 20:25

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

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.

-----Original Message-----
From: jean@m57.biz [mailto:jean@m57.biz]
Sent: Sunday, July 06, 2008 8:56 AM
To: alison@m57.biz; jean@m57.biz
Subject: this is what I was talking about

Powered by

*** Please note, the sender's email address has not been verified.**

this is what I was talking about today!!!

Click the following to access the sent link:

How much skin is too much at the office? - CNN.com*

Conclusion

In conclusion after analysing all of the evidence it is clear to me that Jean has nothing to do with this crime. She was sure that the information she was giving was to Alison the president of the company. If Jean had looked at the email address more thoroughly then this incident may not have occurred. I suspect that the information was leaked by the person behind the tuckgorge@gmail.com account. The file was originally said to have been created by Jean but was in fact created by Alison on the 2008-06-12 at 15:13. It is unclear as to who the person is behind this attack and behind the spoof email account.