

Week 4 Lab

When did Jean create this spreadsheet? (0.5 marks)

Jean created the spreadsheet at 2008-07-20 11:28:03 AEST. You can see this by looking at the "created at" timestamp in Autopsy. This is the version that can be found on her Desktop. Another version can be found at Jean/Local Settings/ Application Data/Microsoft/Outlook/outlook.pst/m57biz.xls. This implies it is the version that outlook copied when sending the spreadsheet via email. It was also created at the same time as the Desktop version.

How did it get from her computer to the competitor's website? (0.5 marks)

It got from Jean's computer to the competitor's website as someone under the email "tuckgorge@gmail.com" aliased themselves as the President Alison and sent an email to Jean asking for the spreadsheet. Jean, then following the orders of who she thought was Alison, replied to the message with the spreadsheet thereby actually sending it back to the outsider "Tuck Gorge". This is the most likely scenario that occurred, then it is assumed that Tuck Gorge must have uploaded it to the competitor's website or passed it on.

```
Thanks!
<20080720050340.39FD03B1DAE@xy.dreamhostps.com>
Jean,

Thanks for the file. I'll handle it from here. to: jean@m57.biz
from: (alison@m57.biz) tuckgorge@gmail.com
subject: Thanks!

Jean,

Thanks for the file. I'll handle it from here.

Once again, please don't tell anyone about this.

Please send me the information now
<20080720012245.177343B1DA8@xy.dreamhostps.com>
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
```

Who else from the company is involved? (0.5 marks)

The people involved with this transaction that can be clearly identified are Jean (from the company) and a man named Tuck Gorge. Although there are other suspicious interactions such as with someone called "Alex", nothing determinate can be inferred from it.

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?

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?

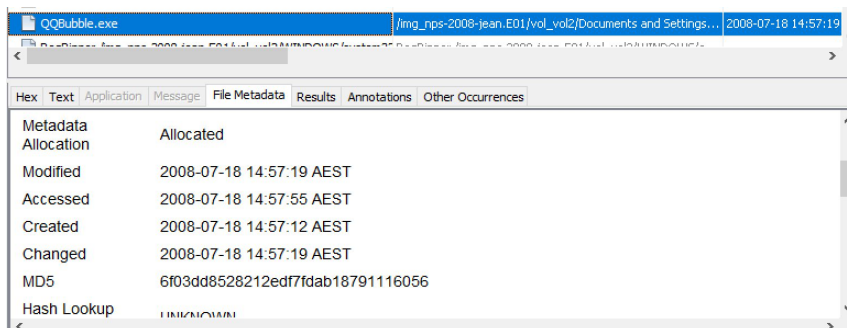
Are you going to use alex@m57.biz or alison@m57.biz?

How did you figure this out? (1 mark)

All this information was gathered via usage of the Autopsy tool and interpretation of various sources of data. The majority of information gathered was found through email transactions which could be accessed at the folder Jean/Local Settings/ Application Data/Microsoft/Outlook and looking at the outlook.pst files.

USB information could be found in WINDOWS/system32/config/system/mounteddevices. The most suspicious device is the E drive. This is suspicious compared to the others as drives such as the C drive are usually default-name harddrives. The last accessed time was also around the time that the excel file was created.

Some other interesting things that were found were applications that were also downloaded around the time that the excel file was created for example "QQBubble.exe". These are suspicious apps that could be further looked into.



The screenshot shows the Autopsy interface with the file 'QQBubble.exe' selected. The file is located at '/img_nps-2008-jean.E01/vol_vol2/Documents and Settings...'. The metadata table shows the following details:

Metadata	Value
Allocation	Allocated
Modified	2008-07-18 14:57:19 AEST
Accessed	2008-07-18 14:57:55 AEST
Created	2008-07-18 14:57:12 AEST
Changed	2008-07-18 14:57:19 AEST
MD5	6f03dd8528212edf7fdab18791116056
Hash Lookup	LINK/CHAIN