Analysis of Digital Forensic Image

When analysing any digital data, it is important that every step is recorded and hash values are checked to keep the integrity of the data. If steps are missing or investigation is not done properly then it could cause a case to be rejected and evidence might be regarded as invalid.

Analysis of disk image using Autopsy

The following phase of the user guide focuses on the demonstration of analysing the presented scenario below for useful information to find out how breach was unfolded.

Investigation of presented scenario

The UB laboratory received a disk image E/1 from B police in a sealed bag (BP1231). The disk image was extracted from jeans jones laptop. During the data gathering phase it was discovered that a confidential spread sheet containing employees name and their salary was leaked to one of the company's competitor's website. The person who had the possession of spread sheet was jeans, but she was not aware of the information being leaked and denied any acknowledgment. A case was registered with number 295689.

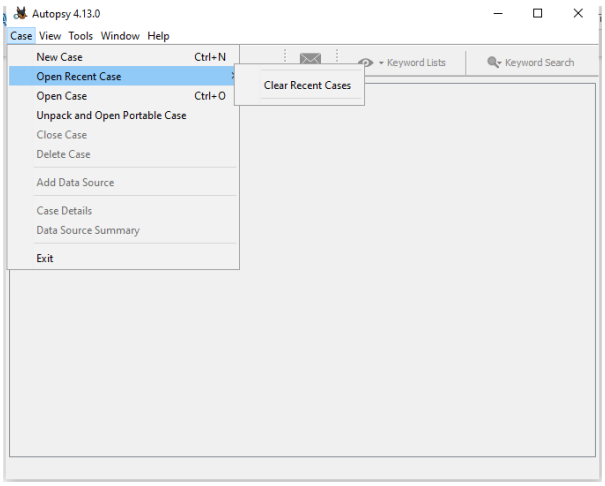

Figure 1: An illustration of creating a case

Step 1: To create a case, open a case option on the left top window on autopsy as shown in figure 1.

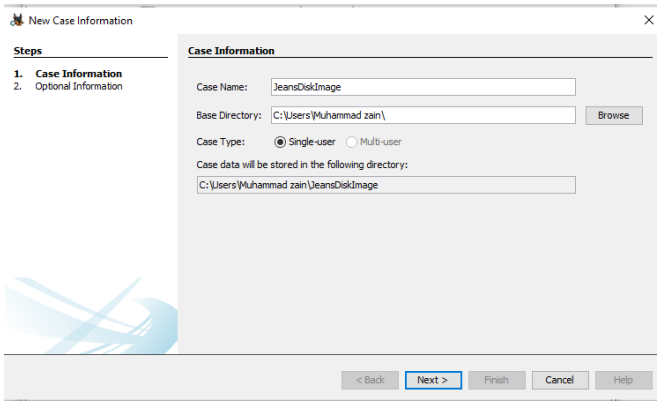

Figure 2: Filling case information

Step 2: Name the case according to your file as shown in figure 2.

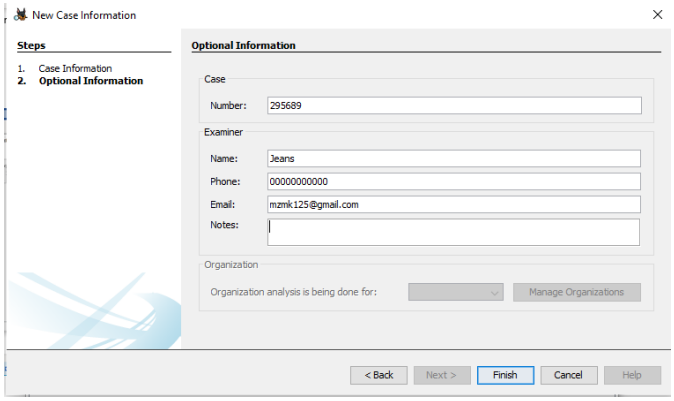

Figure 3: Filling case information

You need to enter information which matches to your scenario. You need to make sure that the information being entered is relevant and suitable to the case. Entering wrong information might confuse the investigation team as demonstrated in figure 3.

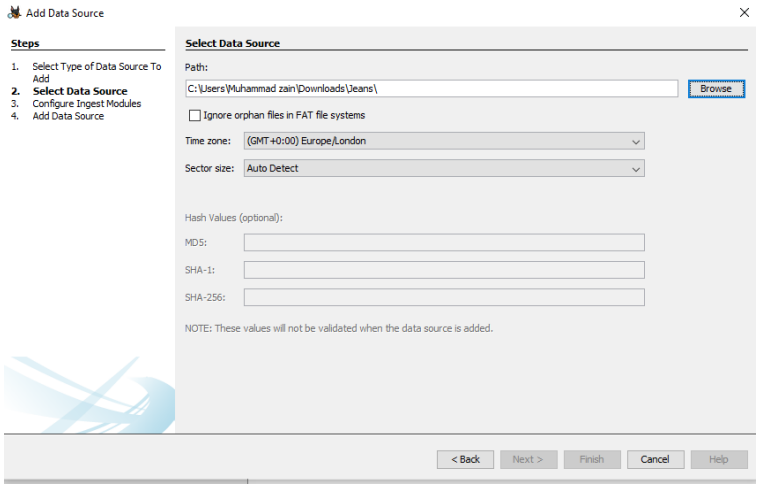

Figure 4: Selecting path for the source data

Step 3: Click on add data source to choose the desired file for analysis as shown in figure 4.

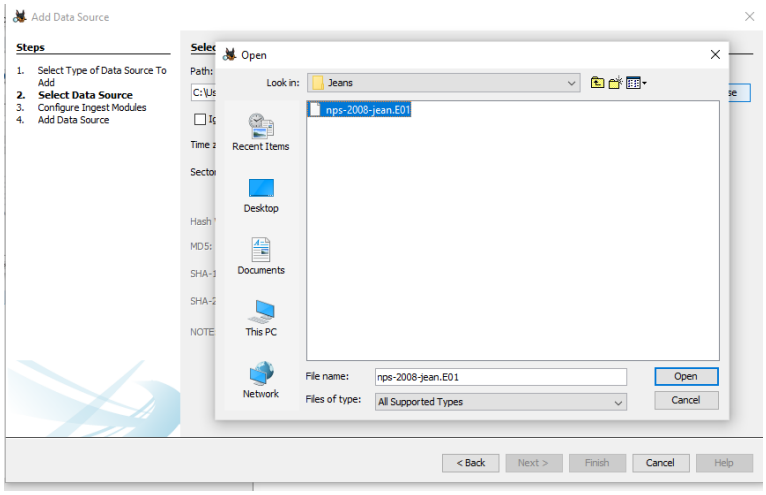

Figure 5: Selecting path to opening case file

Step 4: Once file is selected click on open as shown in figure 5.

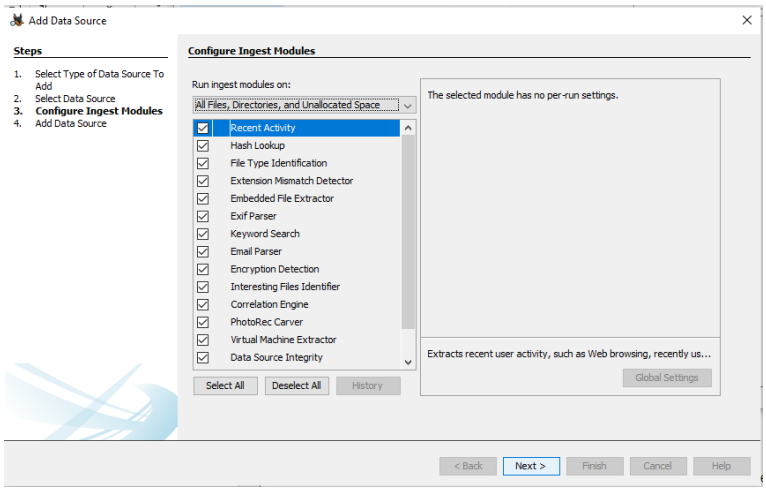

Figure 6: Selecting file data that needed importing

Step 5: You can choose different files from the source data for analysis. In this case all files were chosen for in depth investigation as shown in figure 6.

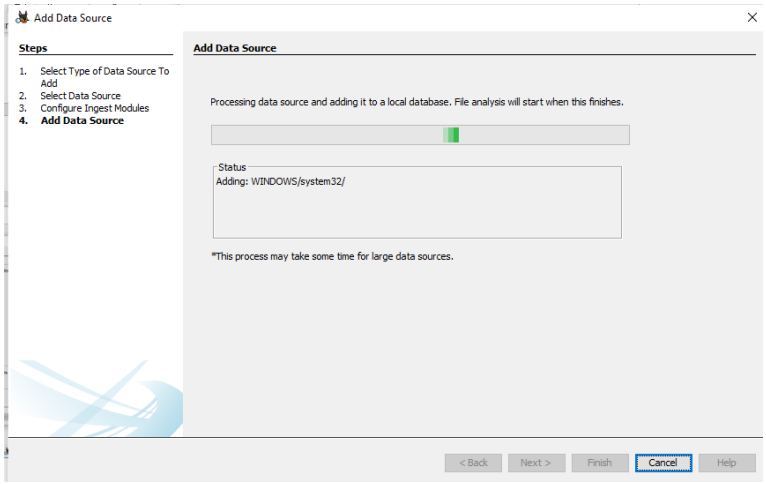

Figure 7: Disk image is being imported

You have to wait for the data source to be imported completely as shown in figure 7.

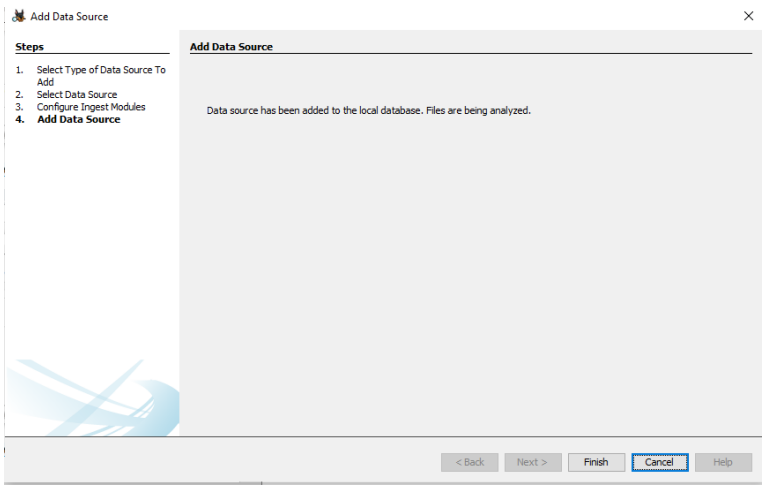

Figure 8: Data source has been added successfully

Step 6: Click cancel to view next widow as demonstrated in figure 8.

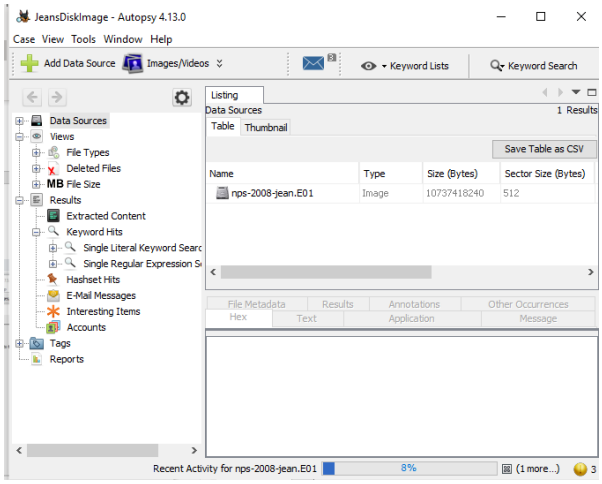

Figure 9: Data source is being analysed by Autopsy as shown in the bottom right corner.

Step 7: Once files are added to the tool. You have to wait for it to be fully analysed so that it does not miss any information as illustrated in figure 9, 10 and 11.

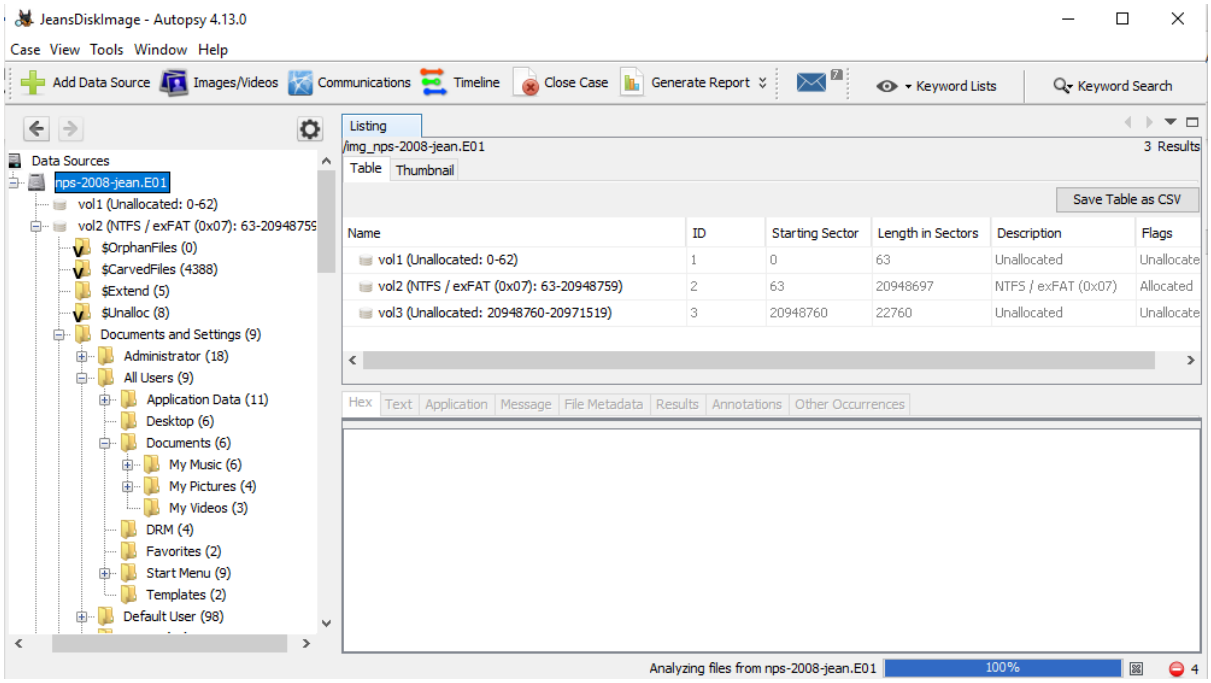

Figure 10: An illustration of Autopsy analysing data source file as shown in the bottom right corner.

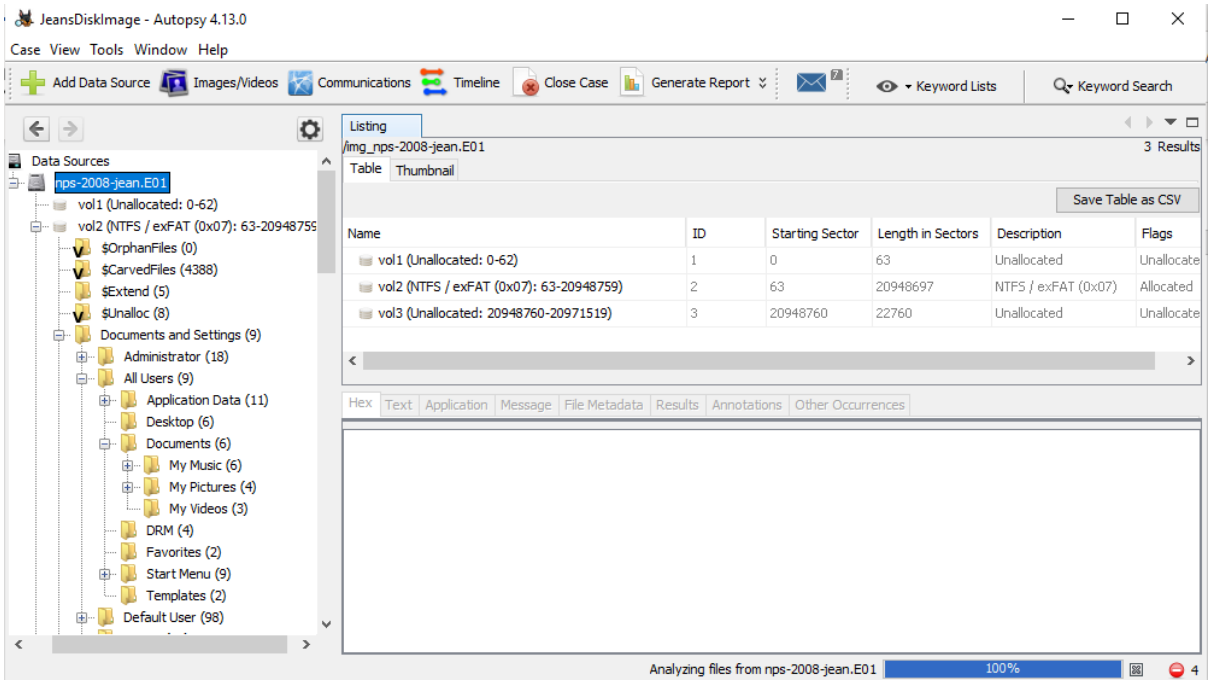

Figure 11: Analysing of the data source completed successfully as shown in the bottom right corner.

Note: You must begin your analysis of finding evidences from the person whose name comes first as there are high chances that there will be a link between that user account and the incident. You should analyse the email of jeans disk image to possible find the evidence as shown in figure 12.

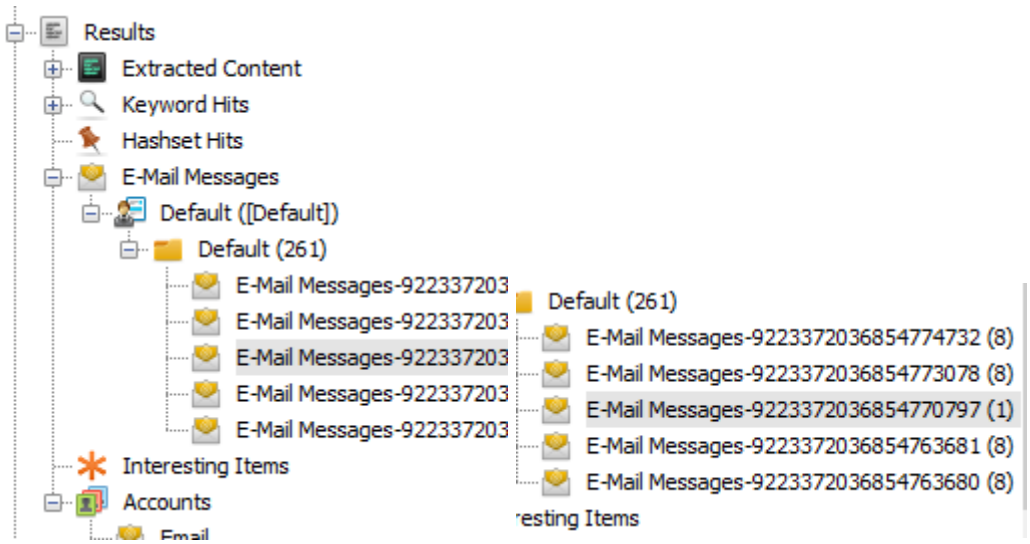

Figure 12: An illustration of Autopsy showing jean's outlook emails.

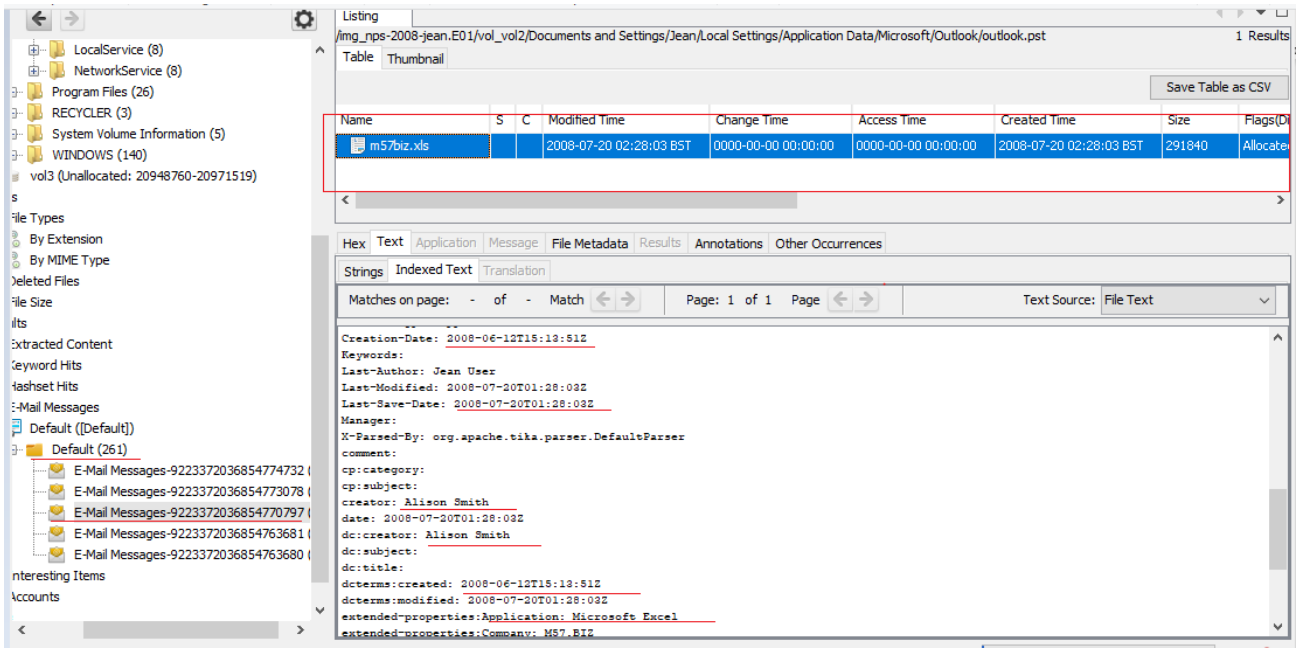

Figure 13: An illustration of Autopsy showing jean's spreadsheet.

You can extract a lot of answers from using the information mentioned in figure 13. List of information extracted from figure 14 is listed below:

- Author of spread sheet: Alison Smith
- Creation date: 2008-06-2012 @ 13: 51
- Last modified: 2008-07-20 @ 20: 03
- Last author: Jean User

```
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
extended-properties:Application: Microsoft Excel
extended-properties:Company: M57.BIZ
extended-properties:Manager:
meta:author: Alison Smith
meta:creation-date: 2008-06-12T15:13:51Z
meta:keyword:
meta:last-author: Jean User
meta:save-date: 2008-07-20T01:28:03Z
modified: 2008-07-20T01:28:03Z
subject:
title:
w:comments:
```

Figure 14: An illustration of Autopsy showing last author of spread sheet

Figure 15 indicates author, date, and modified information of the spread sheet.

You can see that in one email you can find a lot of information.

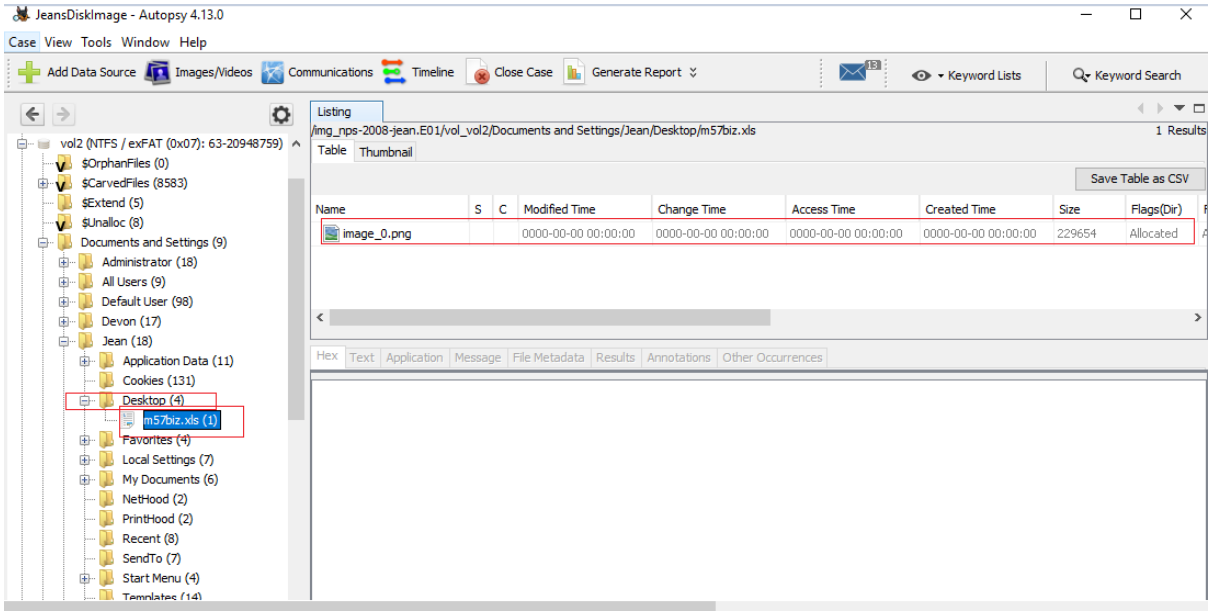

Figure 15: An illustration of spread sheet found under Desktop

The above information shows that the spread sheet was placed on desktop of jean's laptop. Following the case study, now pay attention to the email from where the spread sheet got leaked.

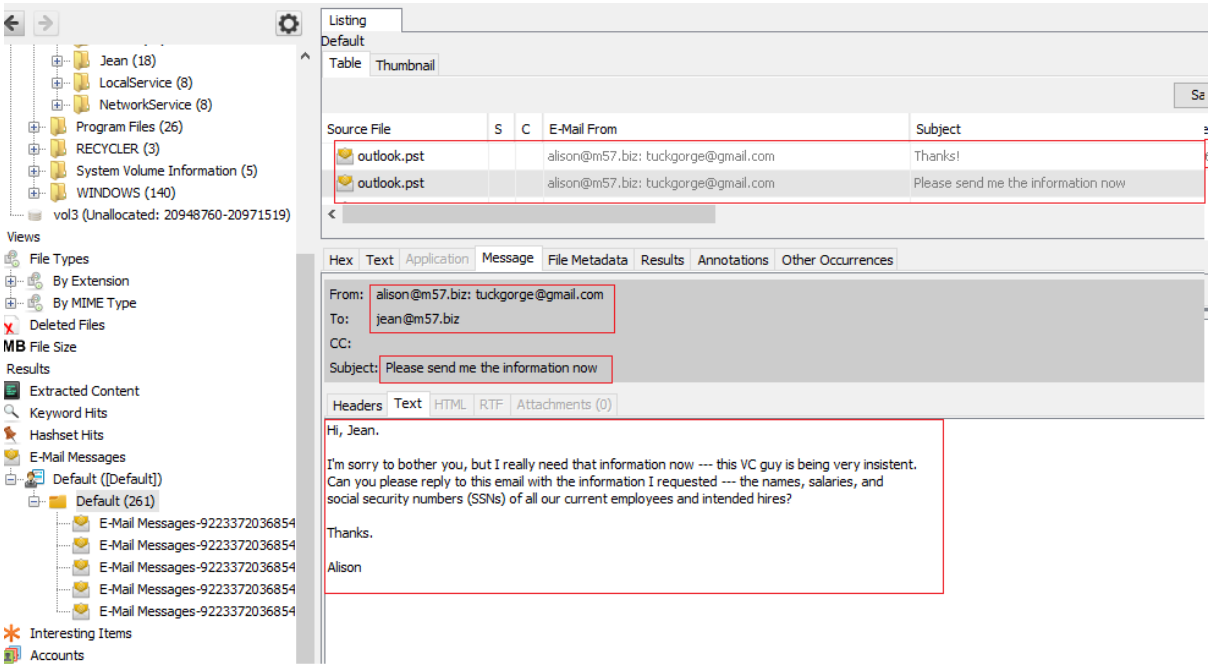

Figure 16: An illustration of an email sends by alison@m57 to jean

You can see that the email tuckgorge@gmail.com pretending to be Alison requesting to get access to the spread sheet. Also, in subject tuckgorge@gmail.com insisting for the information (referring to the spread sheet) as shown in figure 16.

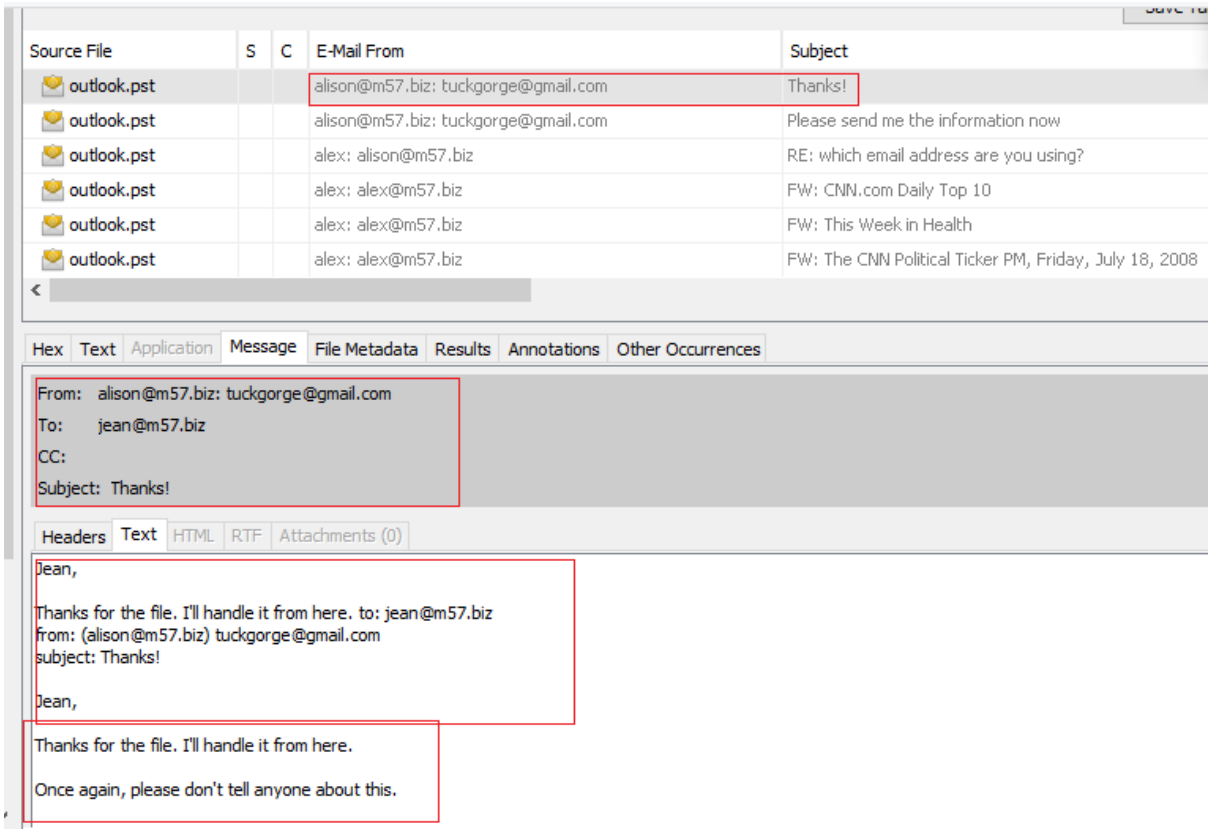

Figure 17: An illustration of an email attached with spread sheet was send to tuckgorge@gmail.com.

You can see that after file was being sent to tuckgorge@gmail.com who pretended to be Alison. The hacker pretending to be Alison thanked jean for the file. Also tuckgorge@gmail.com requested jeans to keep this as a secret and do not tell anyone as shown in figure 17.

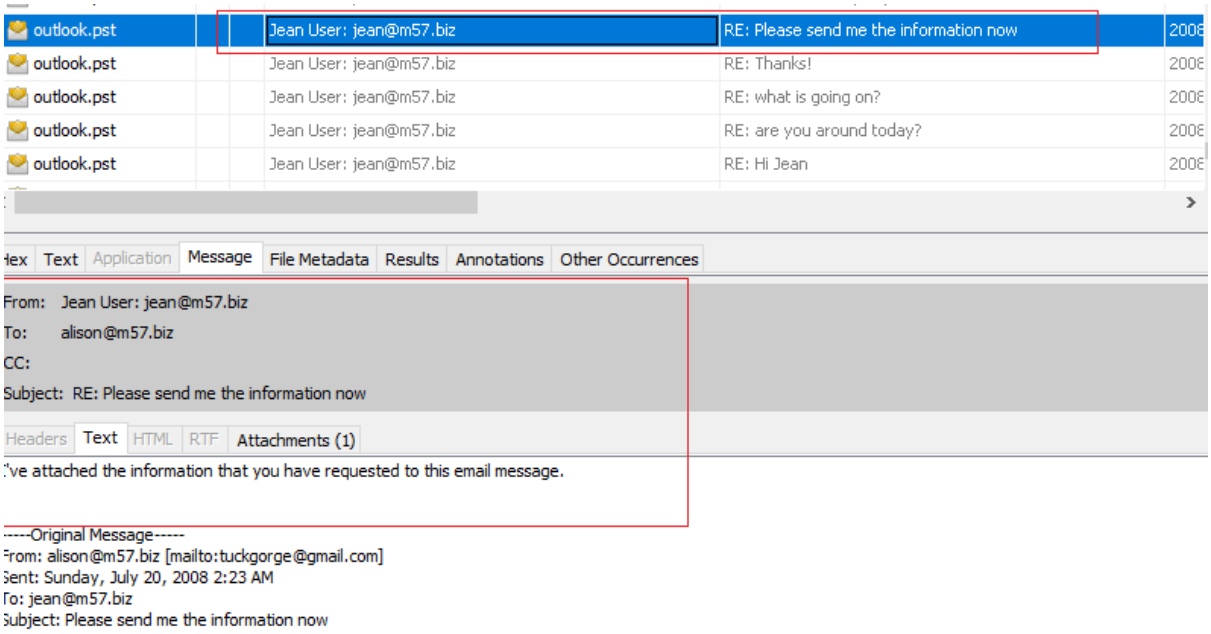

Figure 18: Jeans send spread sheet to Alison email address (tuckgorge@gmail.com)

You can see that the information was send to Alison (tuckgorge@gmail.com) by jean's email account from figure 18 and 19.

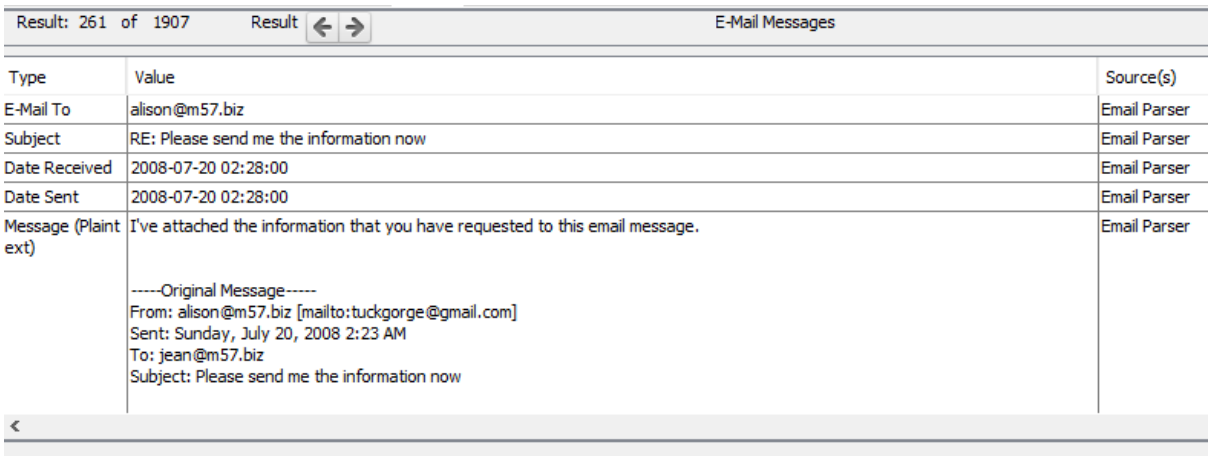

Figure 19: An illustration of an email attached with spread sheet was send to tuckgorge@gmail.com.

An email was send to tuckgorge@gmail.com with spread sheet attached. This is where the spread sheet was leaked.

- Date of spread sheet when it was being sent: 2008-07-20 at 2:28:00
- Received by Alison (tuckgorge@gmail.com) : 2008-07-20 at 2:28:47

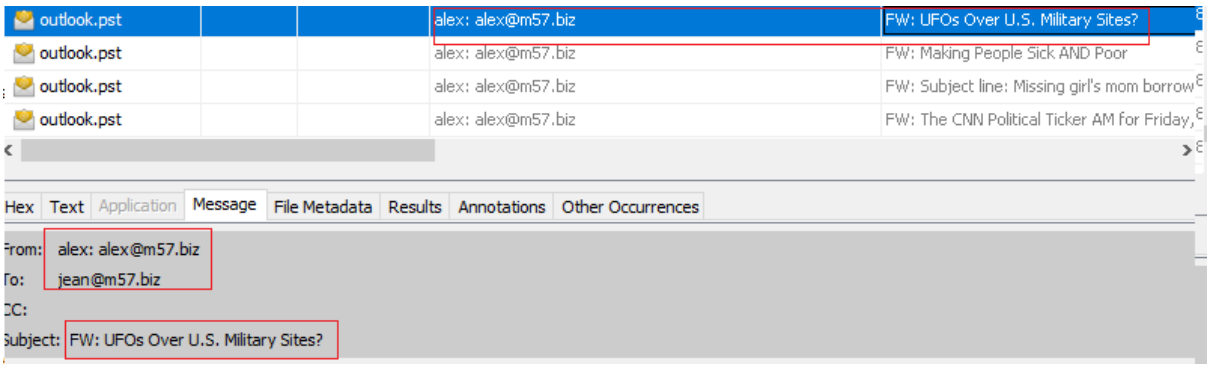

Figure 20: Illustration of possible first phishing attack to jean email account by alex@m57.biz

This could be the starting point of where jean's email was compromised.

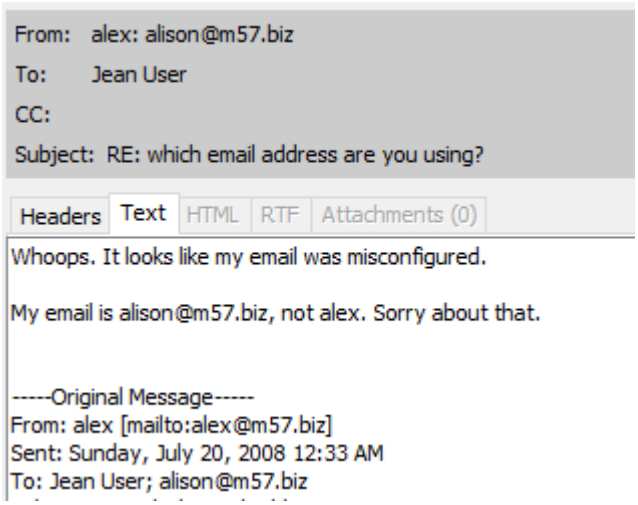

Figure 21: Illustration of Alison complaining about his email being misconfigured.

You can see that Alison found out that there as a problem. However, it could be assumed that Alison was the first person to be affected by the phishing attack. Another possible explaining could be that Alex was a hacker who was using different email to extract the information from all employees.

Findings

The spread sheet was created by Alison 2008-06-2012 13: 51 which was given to Jeans and last modification was done by Jeans at 2008-07-20 2: 28:47. The possible phishing attack at Jean's email address started at 28-07-20 00:32:54 and carried on until 2008-07-20 06:03:40. The spread sheet was sent by Jean to email tuckgorge@gmail.com 2008-07-20 02:28:47. Furthermore, Alison found out that his email had some problem indicating that his email might have been compromised.