M57-Jean - Exfiltration de données

L'objectif de ce TP est de trouver dans l'image disque de Jean les 3 informations suivantes:

1. Quand es-ce que Jean à crée la feuille de calcul ?
2. Comment l'information est-elle passée de son ordinateur au site web du concurrent ?
3. Qui d'autre dans l'entreprise est impliqué ?

Installation des outils nécessaires

Dans un premier temps, afin de réaliser l'exfiltration des données et répondre aux questions précédentes ils faut installer autopsy qui nous permettra de réaliser ce dont nous avons besoin.

Récupération et installation des pré-requis

```
wget
https://raw.githubusercontent.com/sleuthkit/autopsy/develop/linux_macos_ins
tall_scripts/install_prereqs_ubuntu.sh
./install_prereqs_ubuntu.sh
```

Installation de The Sleuth Kit

On récupère le paquet débian disponible depuis le nextcloud et on l'installe:

```
sudo apt update && sudo apt install /tmp/sleuthkit-java_4.12.1-1_amd64.deb
```

Installation d'Autopsy

J'ai récupérer l'archive zip d'autopsy sur le nextcloud, il faut aussi récupérer le script d'installation sur le github d'autopsy:

```
# Récupération du script d'installation
wget
https://raw.githubusercontent.com/sleuthkit/autopsy/develop/linux_macos_ins
tall_scripts/install_application.sh

./install_application.sh -z autopsy-4.21.0.zip -i ~/autopsy -j
/usr/lib/jvm/java-17-openjdk-amd64
```

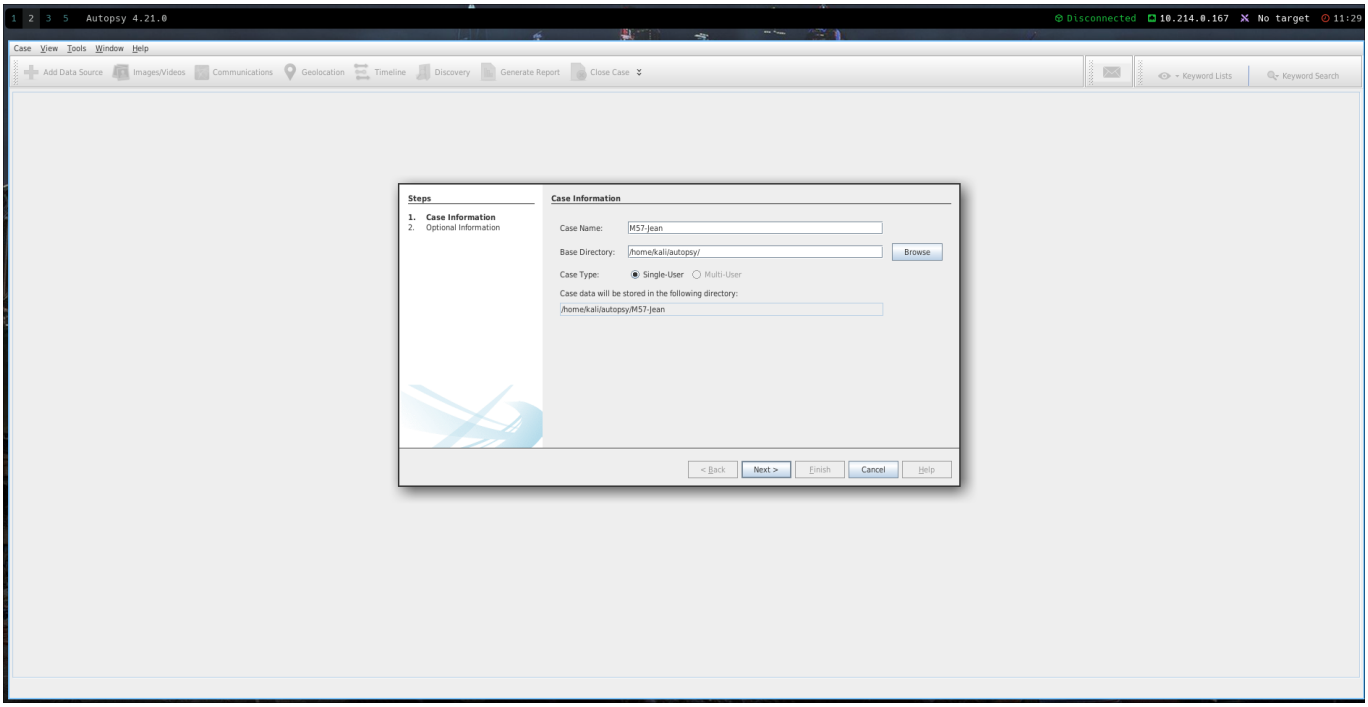
Une fois l'installation d'autopsy installé on peut commencer à examiner le disque dur.

Analyse du disque dur de Jean

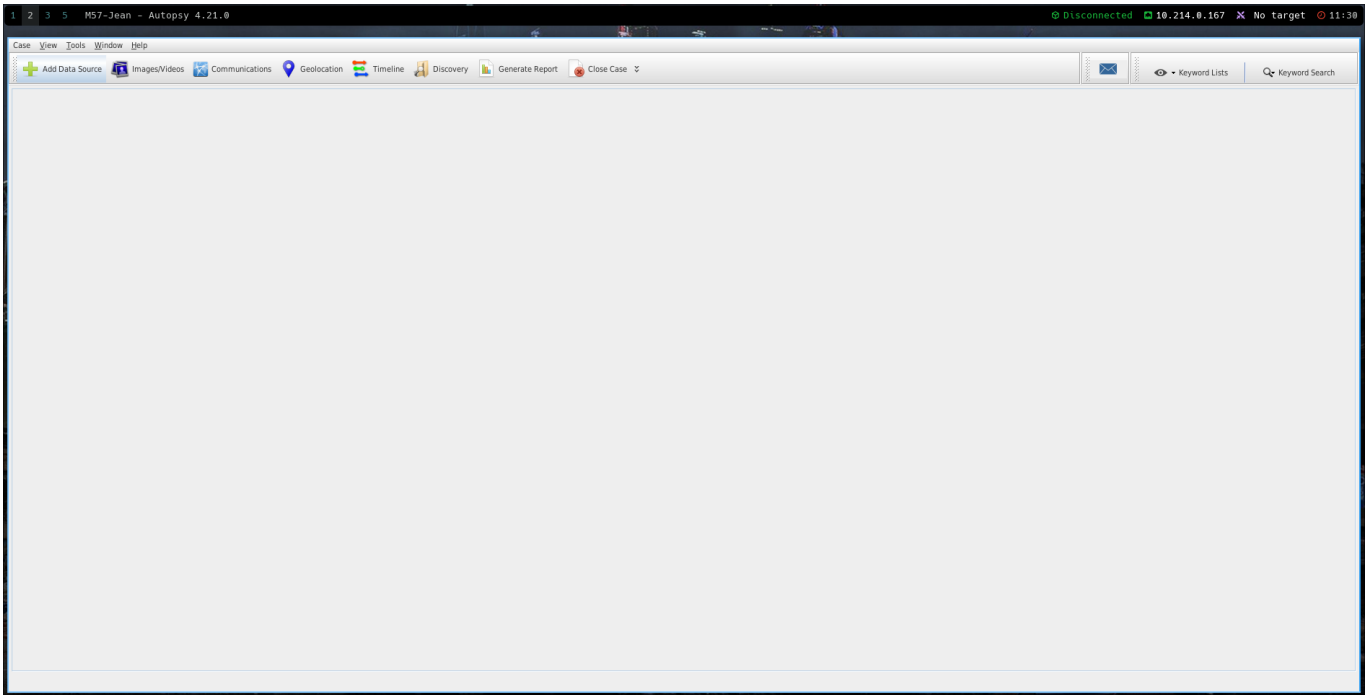
On lance autopsy (depuis le répertoire où ce dernier a été installé):

```
./autopsy --no-splash
```

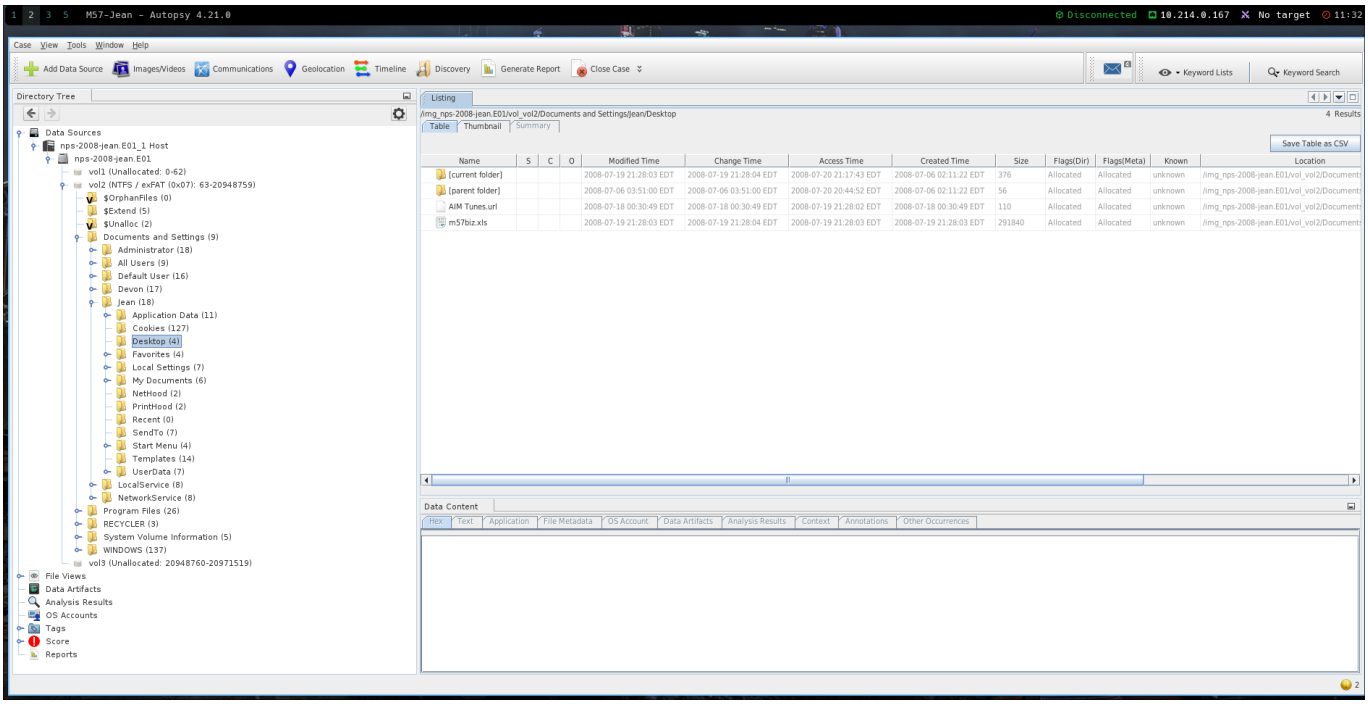
Ensuite, on crée une nouvelle enquête



On arrive sur la page suivante



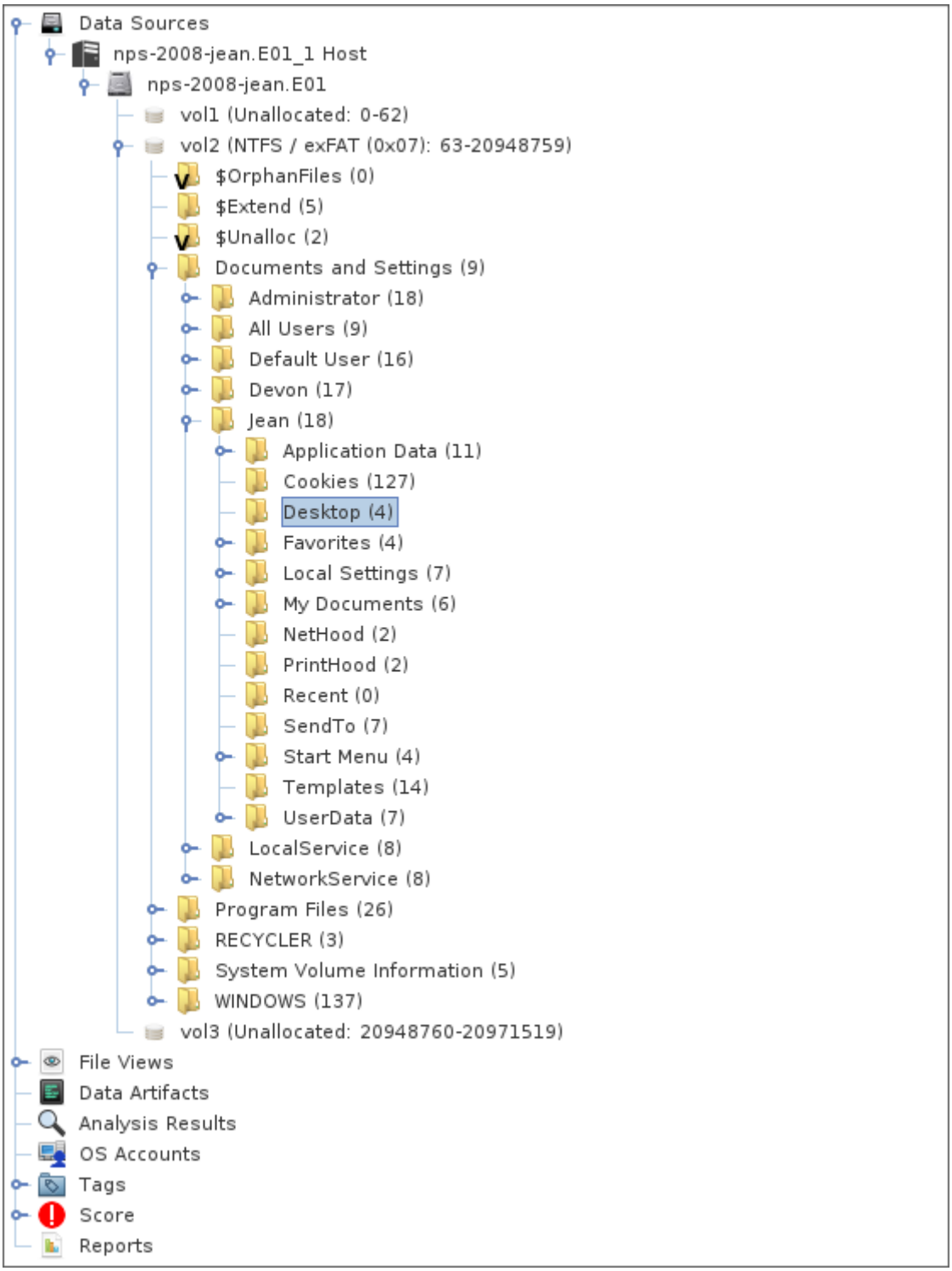
On clique en haut à gauche pour ajouter l'image disque sur "Add Data Source"



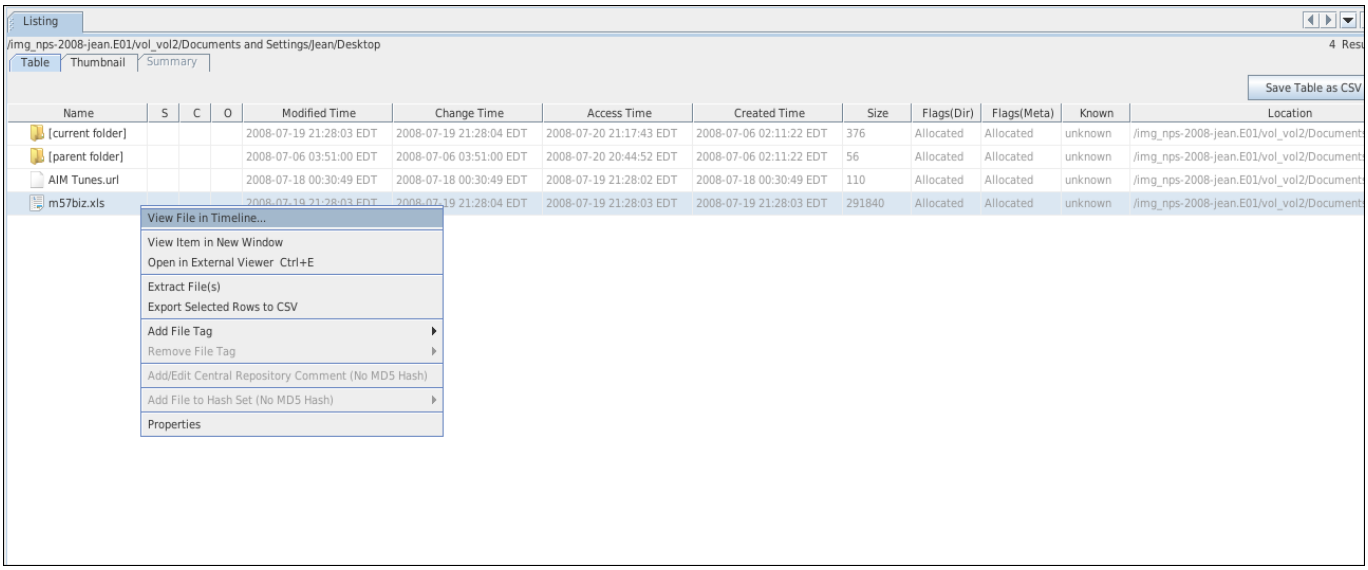
L'image disque a bien été chargée, on peut passer à l'analyse des données.

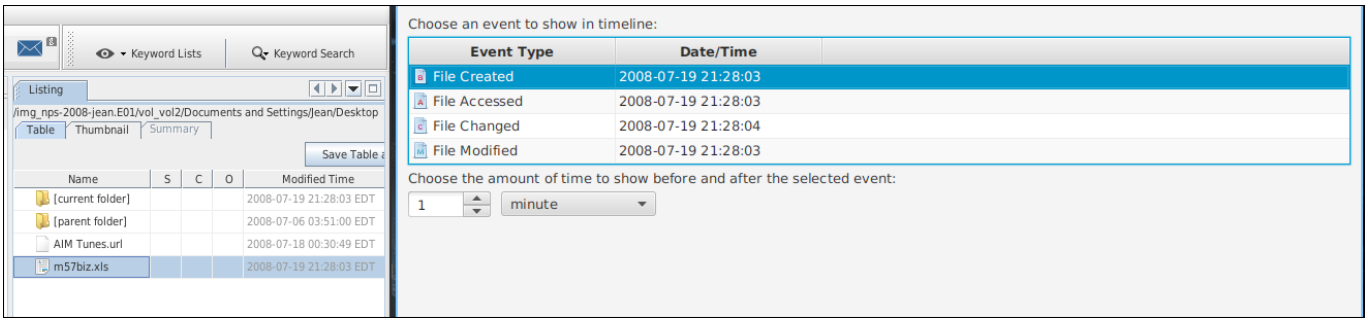
1. Quand es-ce que Jean à crée la feuille de calcul ?

En me balandant dans les dossiers de l'images disque, j'arrive sur le bureau de Jean où la feuille de calcul est disponible.



Pour avoir les informations temporelles du fichier on peut faire un clique droit et cliquer sur "View file in timeline" :

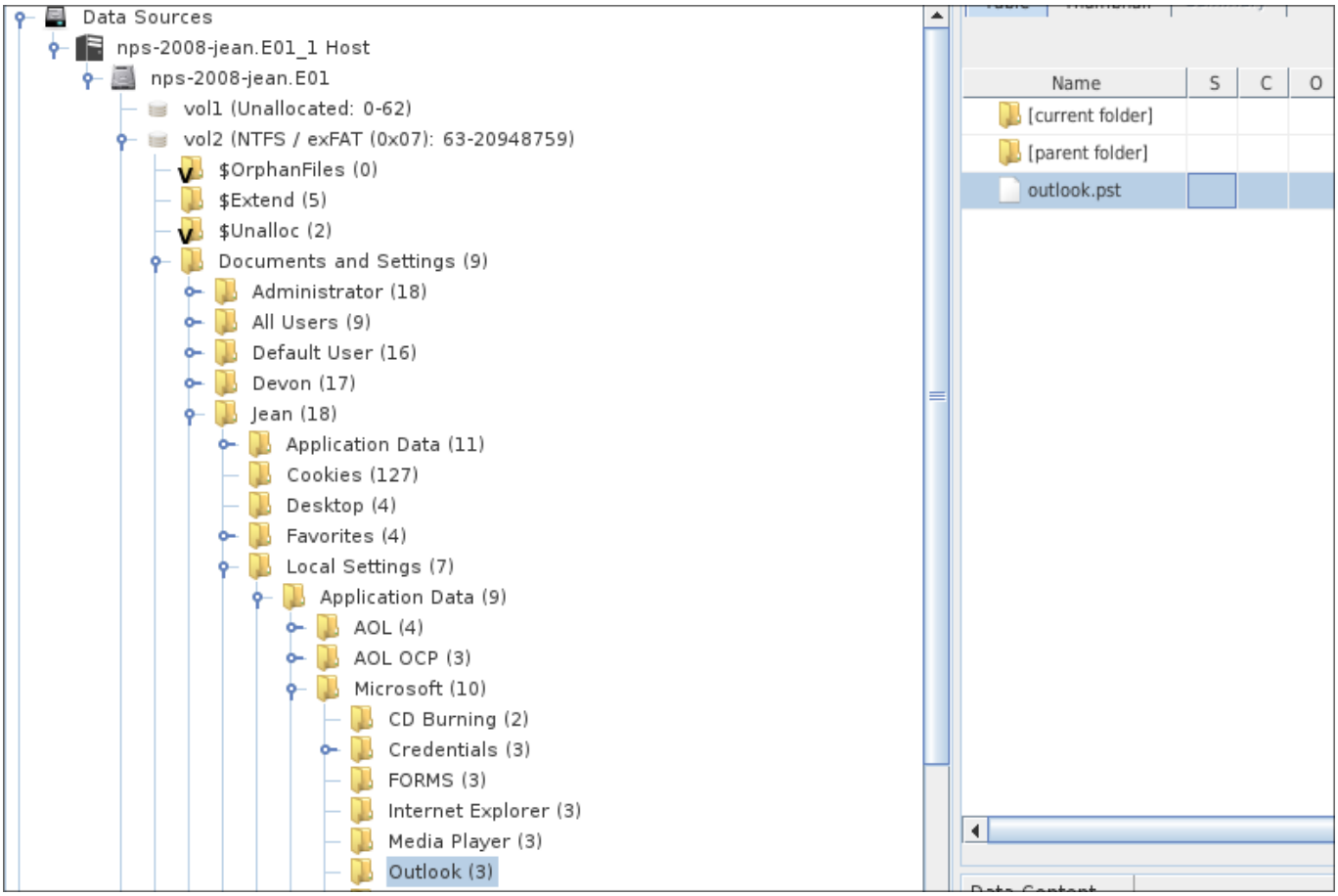




On peut donc noter que le fichier a été crée le **19 Juillet 2088**.

2. Comment l'information est-elle passée de son ordinateur au site web du concurrent ?

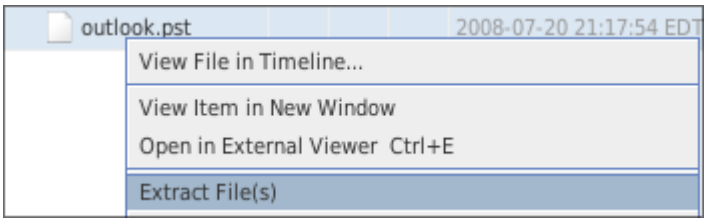
En se balandant dans les dossiers du disque de Jean, je trouve dans les données d'application un dossier "Outlook" contenant les emails envoyés et reçu par Jean :



C'est un fichier .pst "Personal Storage Table" utilisé par Outlook, utilisant une machine sous Linux, je ne peux pas installer Outlook pour visualiser le contenu du fichier un faut donc trouver un logiciel pour l'ouvrir sous Linux.

Exploitation du fichier outlook.pst

Dans une premier temps, il faut extraire le fichier vers la machine linux:



Une fois le fichier extrait sur ma machine, j'installe le logiciel **evolution** qui me permet de lire ce type de fichier sous Linux.

```
sudo apt install evolution evolution-plugins
```

Une fois le fichier chargé, je remarque qu'il y a de nombreux mail d'alertes Google qui envoie un mail à Jean quand du contenu est susceptible de l'interessés sur Internet. Après vérification aucun de ces mails ne contient de phising. Il y a également quelques mail de newsletter dans sa boîte de réception.

Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	07/07/2008 10:39
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	07/07/2008 17:36
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	07/07/2008 19:50
NPR Song of the Day <newsletters@n.npr.org>	Hear Wolf Parade's "California Dreamer"	07/07/2008 21:06
NPR Music Notes <newsletters@n.npr.org>	Summer Music Preview	07/07/2008 21:17
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	07/07/2008 21:39
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	07/07/2008 22:14
NPR's All Songs Considered <allsongs@n.npr.org>	The Best CDs of 2008 (So Far), Plus Fleet Foxes Live	07/07/2008 23:37
NPR News & Notes <newsletters@n.npr.org>	Black Conservatives Conflicted Over Obama	07/07/2008 23:48
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	08/07/2008 01:35
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	08/07/2008 09:32
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	08/07/2008 11:40
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	08/07/2008 12:19
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	08/07/2008 14:44
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	08/07/2008 14:56
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	08/07/2008 15:40
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	08/07/2008 18:12
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	08/07/2008 19:03
NPR Song of the Day <newsletters@n.npr.org>	Hear Sloan's "Believe In Me"	08/07/2008 19:35
NPR News & Notes <newsletters@n.npr.org>	Hill Harper, Gabrielle Union On Mentoring Young Girls	08/07/2008 23:12
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	09/07/2008 01:42
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	09/07/2008 02:45
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	09/07/2008 05:53
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	09/07/2008 08:52
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	09/07/2008 10:14
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	09/07/2008 12:35

Après avoir enlevés ces mails, il ne reste plus que les mails de Jean avec les autres membres de la société.

De	Objet	Date
Jean User <jean@m57.biz>	test test test	06/07/2008 09:48
Jean User <jean@m57.biz>	let's try again	06/07/2008 09:48
jean@m57.biz	this is what I was talking about	06/07/2008 09:55
AlisonM57 <alison@m57.biz>	RE: this is what I was talking about	06/07/2008 21:25
AlisonM57 <alison@m57.biz>	By the way...	06/07/2008 21:25
AlisonM57 <alison@m57.biz>	business plan	06/07/2008 21:25
AlisonM57 <alison@m57.biz>	RE: This is what I was talking about	06/07/2008 21:28
alex <alex@m57.biz>	financial plans	20/07/2008 01:32
alex <alex@m57.biz>	FW: CNN.com Daily Top 10	20/07/2008 01:32
alex <alex@m57.biz>	FW: This Week in Health	20/07/2008 01:32
alex <alex@m57.biz>	FW: Obama makes first trip to Afghanistan	20/07/2008 01:32
alex <alex@m57.biz>	FW: The CNN Political Ticker PM, Friday, July 18, 2008	20/07/2008 01:32
alex <alex@m57.biz>	RE: which email address are you using?	20/07/2008 01:33
alex <alison@m57.biz>	RE: which email address are you using?	20/07/2008 01:43
alex <alison@m57.biz>	programmers	20/07/2008 01:43
alison@m57.biz	background checks	20/07/2008 01:39

Répondre Répondre au groupe Faire suivre

De: AlisonM57 <alison@m57.biz>
À: jean@m57.biz
Objet: RE: this is what I was talking about
Date: Sun, 6 Jul 2008 20:25:11 +0100 (*06/07/2008 21:25:11*)

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.

On remarque un mail d'Alison demandant à Jean de lui envoyer la feuille de calcul, elle qui disait pourtant "n'avoir jamais demandé à Jean cette feuille de calcul".

alison@m57.biz	background checks	20/07/2008 01:39
alex <alison@m57.biz>	RE: background checks	20/07/2008 01:50
alex <alison@m57.biz>	RE: CNN.com Daily Top 10	20/07/2008 01:50

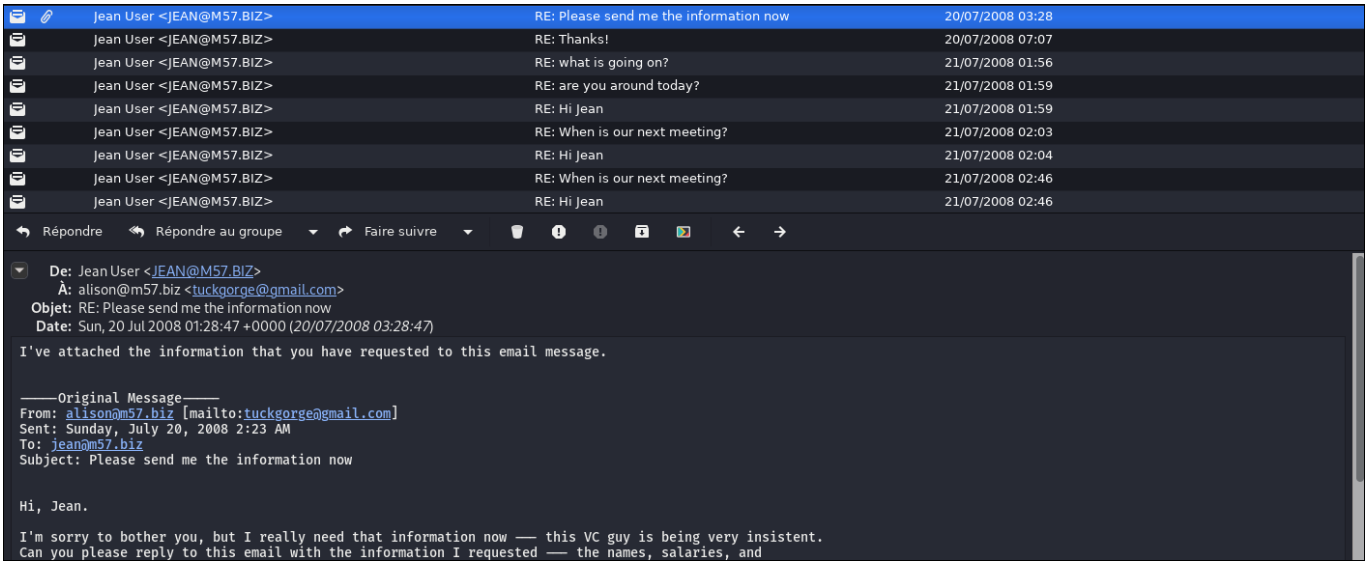
Répondre Répondre au groupe Faire suivre

De: alison@m57.biz
À: jean@m57.biz
Objet: background checks
Date: Sat, 19 Jul 2008 16:39:57 -0700 (PDT) (*20/07/2008 01:39:57*)

```
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.)
```

On peut donc penser que soit Alison a menti ou alors son identité à été usurpé.

Dans le mail où Jean envoie la feuille de calcul, on remarque que l'identité d'Alison à été usurpé depuis le début:



En effet, on remarque que le destinataire de l'email est `alison\@m57.biz <tuckgorge\@gmail.com>` ce qui signifie que Jean parle en fait avec un certain tuckgorge@gmail.com et cette personne à récupérer la feuille de calcul en changenant son nom par l'email d'Alison. Jean pensait donc qu'il parlait à Alision mais ce n'est pas le cas.

Jean à reçu 2 mails avec l'adresse email usurpé d'Alison est ne s'est pas rendu compte du problème.

On peut donc penser que si la feuille de calcul s'est retrouvé chez un concurrent, c'est à cause dun certain tuckgorge@gmail.com qui a peut-être revendu la feuille de calcul ou bien fait partie du groupe concurrent.

3. Qui d'autre dans l'entreprise est impliqué ?

Personne d'autres dans l'entreprise n'est impliqué, l'identité d'Alison à été usurpé dans le but de récupérer des informations confidentielles sur les autres employés de la boîte, en l'occurence ici Jean.