TP04: Suspected e-mails Analysis

1. Before we begin

In this **Practice**, we'll download an HDD of a compromised computer and analyse a suspected email extracted from it.

2. What we'll learn

- ⊡ How to use FTK imager to explore a hard disk image files and folders.
- ⊡ How to extract an OST file using FTK imager.
- ⊡ How to display an OST file contents with help of Kernel OST viewer tool.

3. FTK imager [1]

FTK Imager is a FREE data preview and imaging tool used to acquire electronic evidence for a digital forensic analysis by creating copies of computer data, RAM and HDD, without making changes to the original evidence.

4. OST file

An OST file (.ost) is an offline folder file in Microsoft Outlook. Offline folders make it possible for the user to work offline and then to synchronize changes with the Exchange server the next time they connect. The ability to work offline is useful in environments with limited or unreliable connectivity. OST stands for Offline Storage Table.

5. How to use FTK imager to explore an HDD image and recuperate important files

L'email[2] est un des **vecteurs les plus utilisés** par les attaquants pour transmettre un logiciel malveillant. Vous avez surement déjà reçu un email contenant une facture à payer ou vous informant que vous avez été sélectionné pour toucher l'héritage d'une personne très riche ? Ce type d'email est fréquent et la plupart du temps exploite **le vecteur humain.**

En forensic, l'analyse des emails peut être fastidieuse car on se retrouve souvent à analyser et trier des centaines voire des milliers d'emails.

Récupérer un email pour l'analyser

Le stockage des emails avec Outlook

[1] https://d1kpmuwb7gvu1i.cloudfront.net/AccessData_FTK_Imager_4.7.1.exe

[2] L'envoi d'email malveillant est une **technique de social engineering,** c'est-à-dire qu'il n'exploite pas une faille logicielle mais une **faille humaine**.

Avec **Outlook,** les emails sont stockés dans un **fichier PST.** Chaque compte de messagerie que vous avez configuré dans Outlook reçoit sa propre **base de données** sous la forme d'un fichier PST (*Personal Storage Table*), où les courriers électroniques, les éléments de calendrier, les contacts et les rappels sont tous stockés.

Les données d'un fichier PST peuvent ou non être **compressées** et **chiffrés**, en fonction de vos paramètres.

Vous pouvez également remarquer des fichiers avec une **extension .ost** dans votre dossier de données Outlook. Les fichiers OST ont le même format que PST, mais sont généralement utilisés comme stockage **temporaire hors connexion** de courriers électroniques pour les serveurs Exchange et les hôtes de messagerie Web tels que **Gmail** et **Outlook.com**.

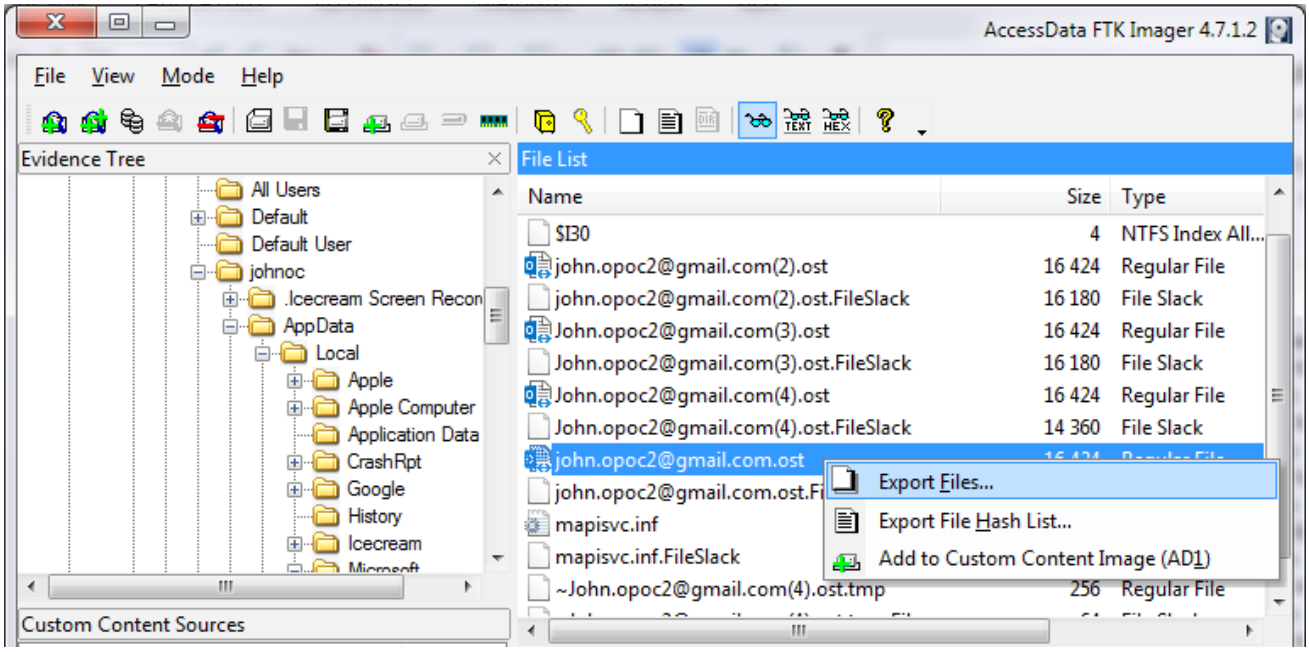
L'idée est que vous pouvez toujours interagir avec les messages stockés dans le fichier OST lorsque vous êtes **déconnecté** du serveur de messagerie (par exemple, lorsque vous n'avez pas Internet), puis lorsque vous vous reconnectez au serveur à nouveau, Outlook synchronise tout.

Cela signifie que vos données seront stockées dans un fichier PST si vous utilisez un compte POP3 ou IMAP standard, ou un compte Exchange pour lequel **le stockage hors connexion n'est pas configuré**. Gmail, Outlook.com et les autres hôtes de messagerie Web obtiendront un fichier OST. Les comptes Exchange peuvent même utiliser à la fois un fichier OST pour un accès hors connexion et un fichier PST pour la sauvegarde des données.

Pour **extraire les fichiers OST et PST** il est possible de se rendre dans le répertoire suivant :

```
C:\users\johnoc\AppData\Local\Microsoft\Outlook
```

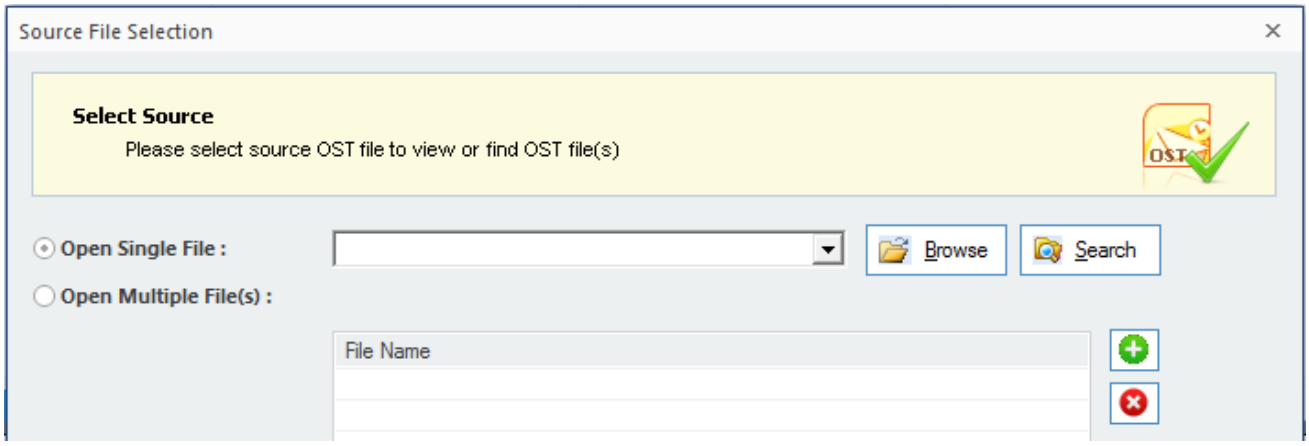
Nous récupérons ici notre fichier à l'aide de FTK Imager :



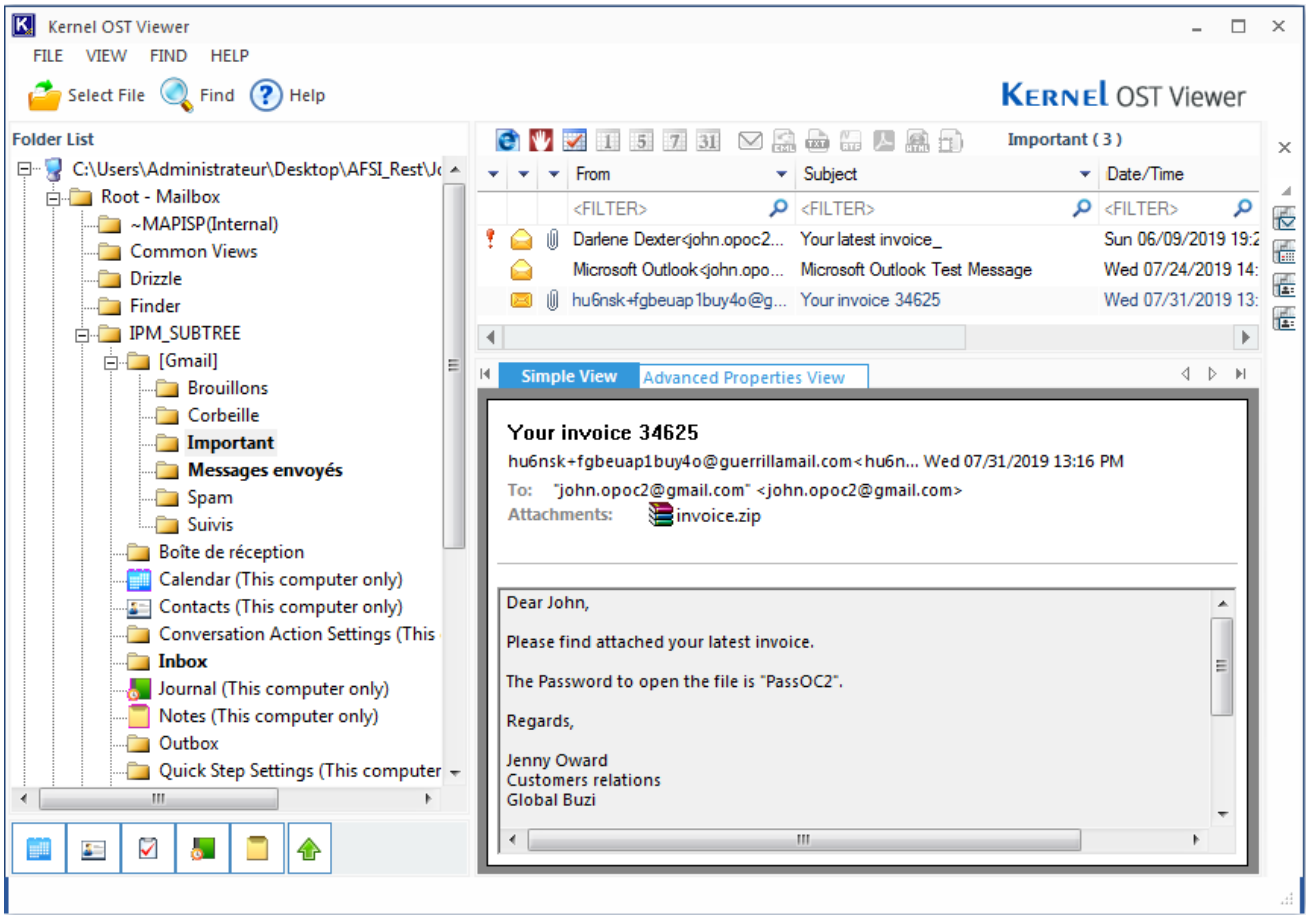
Pour ouvrir ce type de fichier vous pouvez utiliser un simple OST V**iewer.** Il existe de nombreux outils de forensic que vous pouvez également utiliser mais ils ne sont pas gratuits.

6. Display an OST/PST file contents with help of Kernel OST viewer tool

Kernel OST Viewer is a valuable software available free of cost to a business and an individual user. It scans the corrupt, damaged, and inaccessible OST file and open a complete mailbox, exactly like the Outlook application. It will open emails with their complete body and attachments as well as contacts, calendars, meetings, appointments, drafts, sent items, deleted items, etc.



Une fois que le fichier OST est chargé, nous pouvons explorer la boite email :



Nous pouvons voir ici qu'un email a été reçu provenant d'un adresse **@guerrillamail.com** qui est un fournisseur d'email temporaire en ligne. Par ailleurs nous pouvons voir également le contenu de l'email ainsi que sa pièce jointe **invoice.zip**.

Il est également possible d'extraire cet email (OST Viewer complete version), vous obtiendrez alors un fichier avec l'extension .**msg**.

Pour analyser un fichier PST/OST il sera également possible d'utiliser **pffexport** . Pour installer **pffexport** il faudra rentrer la commande suivante sur la machine Linux.

```
~$ sudo apt install pff-tools
```

Analyser l'en-tête et récupérer une pièce jointe

Nous venons d'extraire un email pour l'analyser. Un entête email est composé de plusieurs informations qui peuvent être utile pour l'analyse forensic.

From	**Champs indiquant l'émetteur de l'email.**
Subject	Champs indiquant le sujet de l'email
Date	indique la date et l'heure de l'email
To	L'adresse qui recoit l'email
Return-Path	L'adresse de retour pour l'option Reply To
Received	liste de tous les serveurs traversés par le message pour atteindre le destinataire.
Mime-Version	MIME (Multipurpose Internet Mail Extensions) est une norme Internet qui étend le format du courrier électronique.
Content-Type	En règle générale, cela vous indiquera le format du message, tel que HTML ou texte brut.
Message-id	Chaîne unique attribuée par le système de messagerie lors de la création du message.
Message Body	Le contenu de l'email ainsi que la piece jointe.

Pour obtenir ces informations il faudra d'abord installer la bibliothèque libemail pour Outlook :

```
~$ sudo apt install libemail-outlook-message-perl libemail-sender-perl
```

Et ensuite convertir le .MSG en fichier EML.

```
~$ msgconvert ./invoice.msg
```

Cette commande va générer un fichier .**eml,** il sera ensuite possible de lire l'entête avec un éditeur de texte.

```
(venv) labeni@labeni-hp-pavilion-g6-notebook-pc:~$ cat invoice.eml
Date: Wed, 31 Jul 2019 12:16:12 +0000
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="17013625211.E9C8bCA.8400"
Content-Transfer-Encoding: 7bit
Subject: Your invoice 34625
From: hu6nsk+fgbeuap1buy4o@guerrillamail.com
To: "john.opoc2@gmail.com" <john.opoc2@gmail.com>
Message-Id: <543bbcc75ae0202f89fe5fcb408d235ae031@guerrillamail.com>
Delivered-To: john.opoc2@gmail.com
Received: by 2002:ab0:2a01:0:0:0:0:0 with SMTP id o1csp6133066uar;
 Wed, 31 Jul 2019 05:16:13 -0700 (PDT)
Received: from mail.guerrillamail.com ([2607:5300:60:689e::])        by
 mx.google.com with ESMTPS id l29si41498316qtk.192.2019.07.31.05.16.12
 for <john.opoc2@gmail.com>        (version=TLS1_3
 cipher=AEAD-AES256-GCM-SHA384 bits=256/256);        Wed, 31 Jul 2019 05:16:13
 -0700 (PDT)
Received: by 167.114.101.158 with HTTP; Wed, 31 Jul 2019 12:16:12 +0000
X-Google-Smtp-Source:
 APXvYqyRjPOInApk2ZEt17RG0kgKDavpSqUIs5+qODhTBMwhU6jCkAhZHXV3uRje9X5X4hYHtXvP
X-Received: by 2002:ac8:354d:: with SMTP id
 z13mr88242321qtb.340.1564575373191;        Wed, 31 Jul 2019 05:16:13 -0700
 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1564575373; cv=none;        d=google.com;
 s=arc-20160816;
 b=r0fDMNaKbbNL6ow9Y+ba2TEjGILfcOrZFGo3wTXnO+XEct3SuhcoXKE+T2HhpiVCbL
 U4MLNSQzA0gpRbMQP7akgQD3zRuFRcaA0hm97+cQWoYCTeKkNT7znI/CXpuNI9nDwpNA
 8nCbP2Bbh7CLdYW6VyOEFDUWNe9eH5Dgij06YZT326TEIJYdIoaR4jrtcDR28sBj+Yjy
 VE+8yj2OOKNB07mODYaYxIwRgAmIPJekfnZS9W9PA8041q+hP3WeIX4tg5raLAY1JB/k
 7Fbbs78a3TV9JtNzzx5k4YMFlJiYDnrY1iEmTOH5Zj41gs3+dLYU0a1Y2nntFjQ5qW5A
 VHfQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com;
```

Nous retrouvons ici nos éléments de l'en-tête email. Nous pouvons identifier les éléments suivant:

- L'email a été envoyé le **31 juillet 2019 a 12h16**
- L'objet de l'email est : "**Your invoice 34625**"
- L'adresse émettrice est **hu6nsk+fgbeuap1buy4o@guerrillamail.com**
- L'adresse receveur est **john.opoc2@gmail.com**
- Une pièce jointe appelé **invoice.zip** est présente.

En descendant un peu plus vous trouverez du texte encodé en base 64. Ce morceau en base64 correspond à la pièce jointe de l'email.

Base64 est un encodage utilisé pour l'échange de données sur internet. Il suffit de copier/coller cette base64 dans un fichier pour pouvoir ensuite le décoder :

```
~$ base64 -d pj.b64 >> invoice
```

Un fichier nommé **invoice.zip** sera créé. En ouvrant ce fichier correspondant à la pièce jointe avec le mot de passe mentionné dans l'email, nous nous retrouvons avec 2 fichiers : **`invoice.pdf & invoice.docm`**