Forensics

Plan

- Acquisition et préservation de données
- Un mot sur les systèmes de fichiers (FS) ainsi que leurs spécificités
- Exploration des images de FS (montage, exploration, analyse de traces logicielles)
- Analyse de la RAM
- Analyse de paquets réseaux

Acquisition et préservation de données

Assurer l’intégrité de l’image système

La majorité de l’information pertinente est volatile

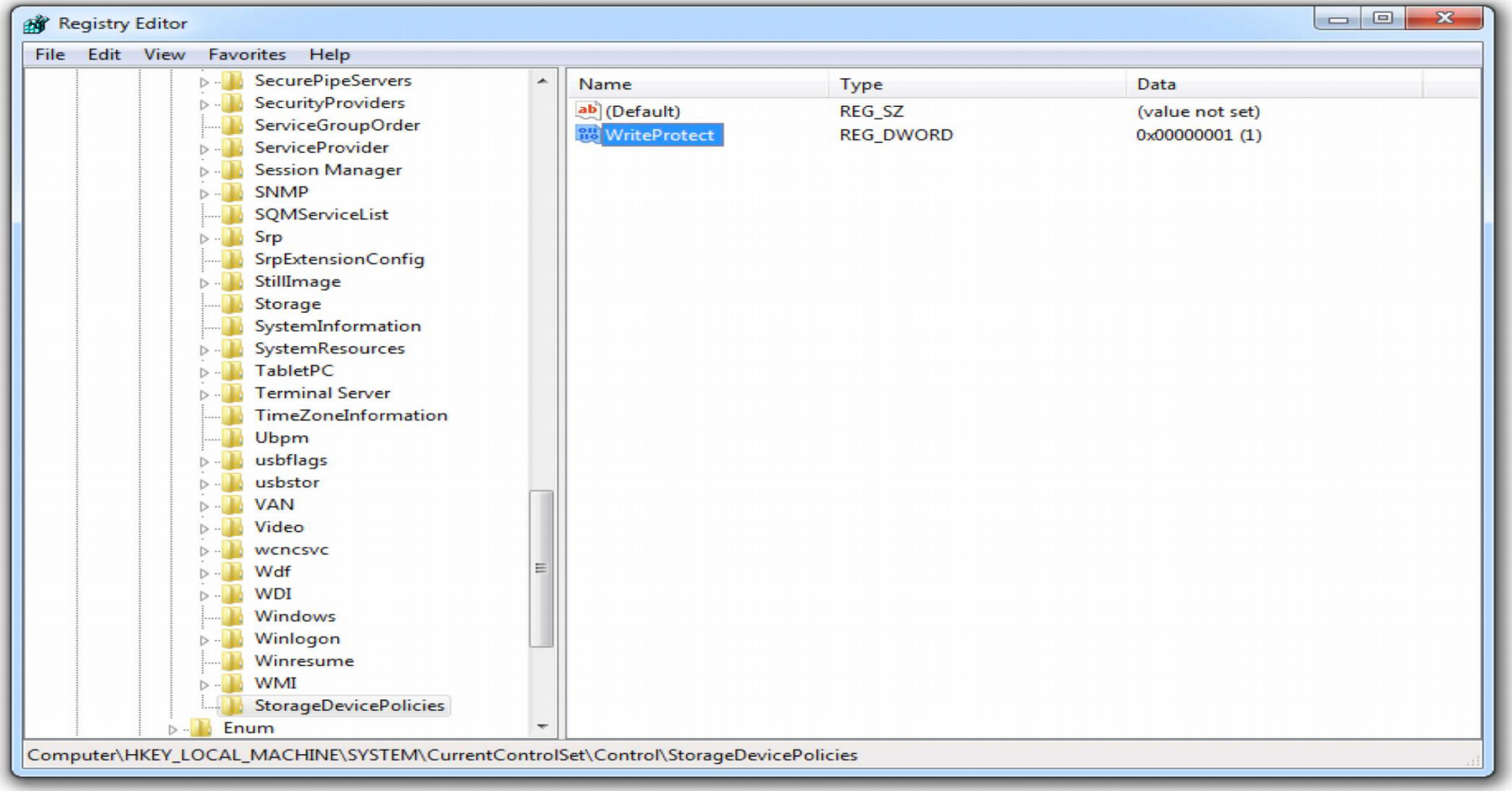
→ Prévenir toute écriture sur le media qui contient le système suspecté (on veut qu’il reste identique dans le temps). On recours pour cela à des **write blockers**

- Matériel
- Logiciel

Write blocker logiciel : procédure pour Windows

- Regedit
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
- Créer une nouvelle clé (de type StorageDevicePolicies)
- select “New” and then “DWORD (32-bit) Value
- Change the name from “New Value #1” to “WriteProtect”
- 0

Write blocker logiciel : procédure pour Windows



Procédure sur Linux

On pourrait croire que mount -o ro /dev/sda1 /mnt/sda1/ suffit mais il n’y a aucune garantie

- Un patch kernel qui revient souvent

Phase d’acquisition (édition d’une copie identique destinée au forensics)

Le media peut être déconnecté de la machine

→ connexion à un Write blocker sur une machine de confiance

Le media ne peut pas être déconnecté de la machine

→ live USB

→ réseau

Comment s’assurer de l’identité de la copie

Utiliser des logiciels de copie bit-à-bit

- EnCase
- FTK
- dd

Comparaison de deux hashs

- Hash du media d’origine
- Hash de l’image

La question du format de la copie

- E01 – Expert Witness compressed format, which is used by Guidance Software and often called the EnCase evidence file format.
- Ex01 – A new variation of the E01 format introduced by Guidance Software, which offers encryption and compression options. This was released with version 7 of EnCase.
- SMART – a file format to work with a software utility for Linux.
- dd/RAW – An exact copy of the media. The destination that holds the resultant dd file must be larger than the media being acquired.
- AFF – Advanced Forensics Format, which works well with Autopsy and The Sleuth Kit.
- AFF4 – a redesign of AFF.
- ProDiscover Image File Format – for use with ProDiscover.

Création de notre image (sous linux)

Nous allons nous servir de dc3dd

dc3dd n’est jamais plus qu’un dd custom. Même logique dans les commandes :

```
dc3dd if=/dev/sdc1 of=usb1_evidence_image.img hash=sha256
log=usb1_evidence.log
```

documentation

tutoriel

Un mot sur les systèmes de fichiers

Identification des méthodes pertinentes pour chaque système de fichier

- Organisation des données
- Type de métadonnées
- Journalisation

  → on ne peut seulement se fier à l’arborescence des dossiers créés par l’utilisateur ou le système

  → besoin d’outils spécifiques

La journalisation

La **journalisation** est ce qui dote un FS d'une tolérance à la panne ou de la possibilité d'un débranchement à chaud. Elle est assuré par l'existence d'un journal référençant les opérations d'écriture

Quelques systèmes de fichiers journalisés :

- Ext3, ext4 (linux)
- BFS, UFS, ZFS (autres UNIX)
- NTFS (Windows)
- HFS + (OSX)

Quelques systèmes de fichiers non journalisés :

- FAT 16, FAT32
- ext2
- exFAT

Quelques outils d’analyse des FS

- fsstat (Sleuth_Kit)
- Appliquons le sur notre image

Exploration des images de FS

Scan :montage de l’image vulnérable

Les solutions windowsiennes

- OSF Mount
- FTK Imager

Les solutions linuxiennes

- libewf (pour les EWF-S01 SMART et EWF-E01 EnCase) ewf-tools
- Support natif des dd RAW source
- Affuse Pour les AFF

Outils d’analyse et exploration des images

Open source

- SleuthKit et Autopsy
- DFF

Propriétaires

- Blackbag
- EnCase
- Cellbrite

Que chercher exactement ?

Du côté des fichiers

- Fichiers supprimés
- Méta-données
- Type (et éventuelle manipulation de ces derniers)

Traces logicielles

- Historique des navigateurs
- Fichiers journaux systèmes
- Fichiers journaux logiciels
- Base de registre Windows
- Entêtes d’emails
- Fichiers d’hibernation (Win) et swap (Linux)

l’analyse d’un registre (Win)

- C:\Windows\system32\config\default
- C:\Windows\system32\config\SAM
- C:\Windows\system32\config\SECURITY
- C:\Windows\system32\config\software
- C:\Windows\system32\config\system
- C:\Users\username\NTUSER.DAT

  → sont loadés en mémoire pour devenir (HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG)

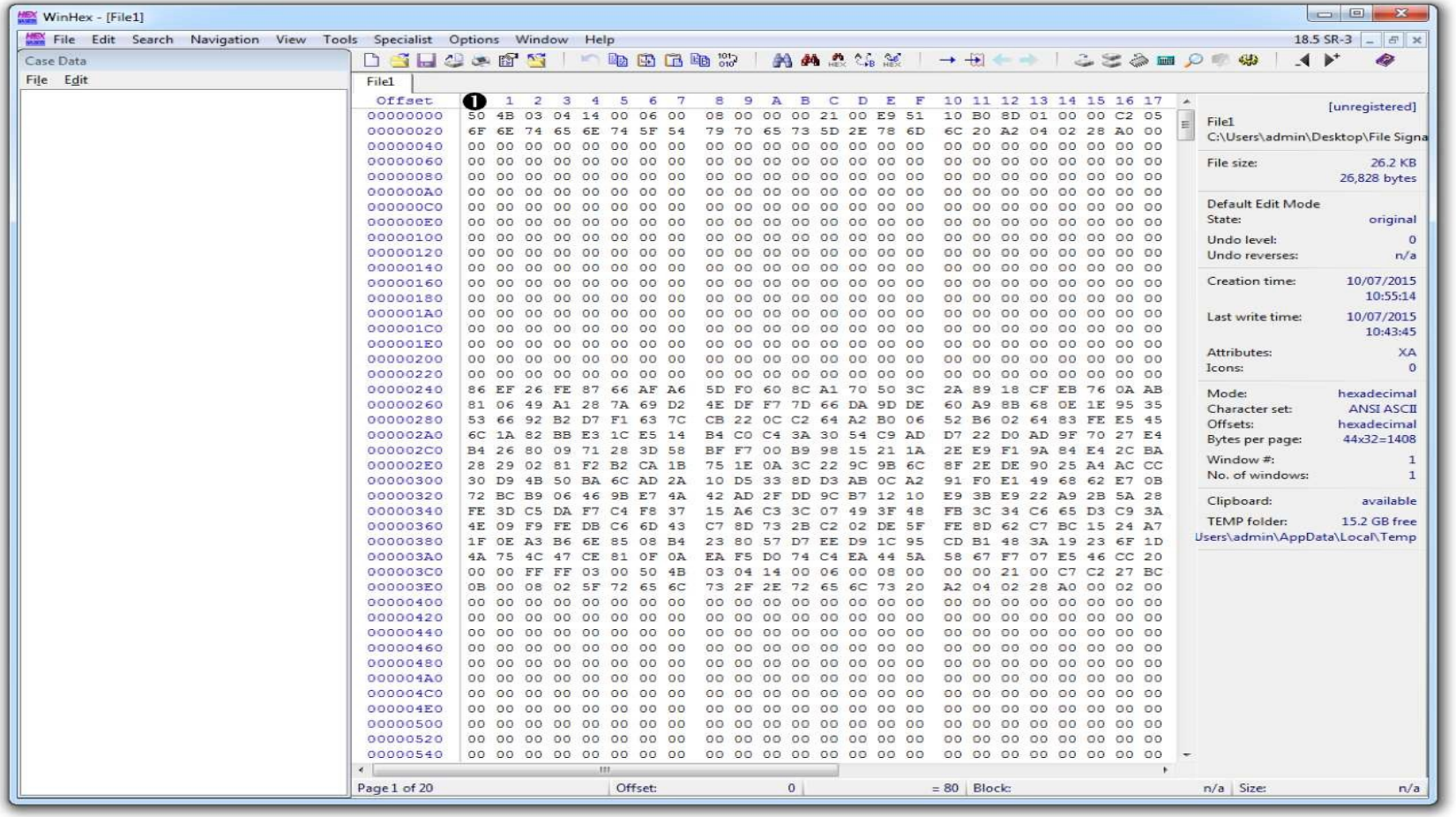
Analyse des signatures de fichiers

Magic numbers : ensemble de caractères (ou constante) qui désigne un format de fichier dans le header (reliquat du passé)

Pourquoi vouloir les analyser ?

- Changement d’extension par le hacker
- Fichier corrompu
- Etc etc

Analyse des signatures de fichiers



Analyse des signatures de fichiers

De quel genre de fichier 50 4B 03 04 14 00 06 00 est il le header ?

une ressource

Analyse des méta-données des fichiers suspects

Vous donne :

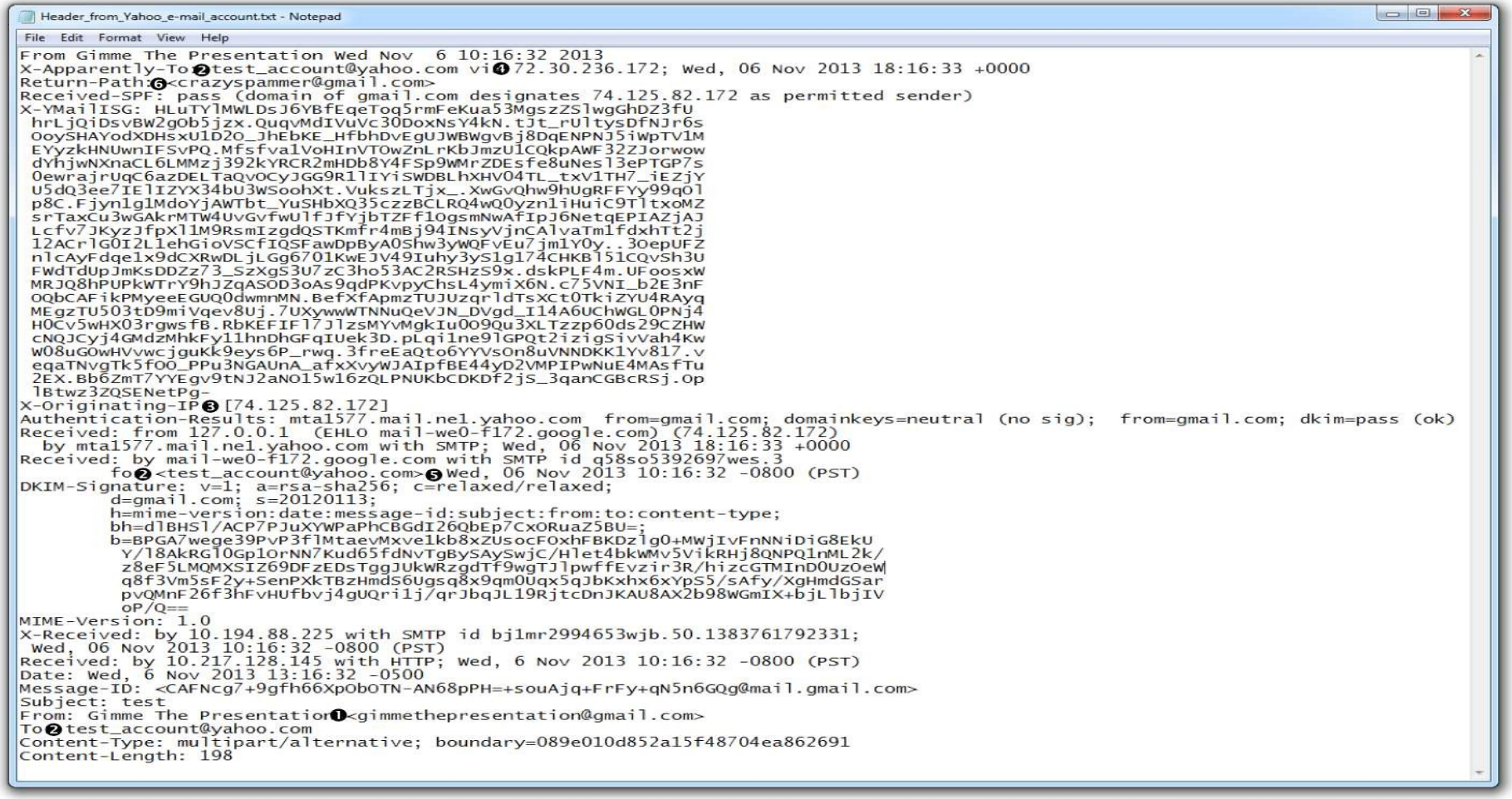
- l’os
- l’application
- l’utilisateur

Dans le cas des appareils photos et téléphones

- Modèle
- Lentille
- Focale
- Coordonnées GPS (et oui !!!!)

Analysez ces deux fichiers

Analyse de headers de mail


Header_from_Yahoo_e-mail_account.txt - Notepad

File Edit Format View Help

```
From Gimme The Presentation Wed Nov  6 10:16:32 2013
X-Apparently-To❷test_account@yahoo.com vi❹72.30.236.172; Wed, 06 Nov 2013 18:16:33 +0000
Return-Path:❻<crazyspammer@gmail.com>
Received-SPF: pass (domain of gmail.com designates 74.125.82.172 as permitted sender)
X-YMailISG: HLuTYlMWLDsJ6YBfEqeToq5rmFeKua53MgszZSlwgGhDZ3fU
 hrLjQiDsvBW2gOb5jzx.QuqvMdIVuVc30DoxNsY4kN.tJt_rUltysDfNJr6s
 OoySHAYodXDHsxU1D2O_JhEbkE_HfbhDvEgUJWBWgvBj8DqENPNJ5iWpTV1M
 EYyzkHNUwnIFSvPQ.MfsfvalVoHInVTOwZnLrKbJmzUlCQkpAWF32ZJorwow
 dYhjwNXnaCL6LMMzj392kYRCR2mHDb8Y4FSp9WMrZDEsfe8uNesl3ePTGP7s
 OewrajrUqC6azDELTaQvOCyJGG9R1lIYiSWDBLhXHVO4TL_txV1TH7_iEZjY
 U5dQ3ee7IElIZYX34bU3WSoohXt.VukszLTjx_.XwGvQhw9hUgRFFYy99qOl
 p8C.Fjyn1g1MdoYjAWTbt_YuSHbXQ35czzBCLRQ4wQ0yzn1iHuiC9TltxoMZ
 srTaxCu3wGAkrMTW4UvGvfwUlfJfYjbTZFf1OgsmNwAfIpJ6NetqEPIAZjAJ
 Lcfv7JKyzJfpXl1M9RsmIzgdQSTKmfr4mBj94INsyVjnCAlvaTm1fdxhTt2j
 12ACrlG0I2L1ehGioVSCfIQSFawDpByA0Shw3yWQFvEu7jm1Y0y..3OepUFZ
 nlcAyFdqe1x9dCXRwDLjLGg6701KwEJv49Iuhy3yS1g174CHKBl51CQvSh3U
 FWdTdUpJmKsDDZz73_SzXgS3U7zC3ho53AC2RSHzS9x.dskPLF4m.UFoosxW
 MRJQ8hPUPkWTrY9hJZqASOD3oAs9qdPKvpyChsL4ymiX6N.c75VNI_b2E3nF
 OQbCAFikPMyeeEGUQOdwmnMN.BefXfApmzTUJUzqrldTsXCt0TkiZYU4RAyq
 MEgzTU503tD9miVqev8Uj.7UXywwWTNNuQeVJN_DVgd_I14A6UChWGLOPNj4
 HOCv5wHX03rgwsfB.RbKEFIFl7JlzsMYvMgkIuOO9Qu3XLTzzp60ds29CZHW
 cNQJCyj4GMdzMhkFyl1hnDhGFqIUek3D.pLqi1ne9lGPQt2izigSivVah4Kw
 W08uGOwHVvwcjguKk9eys6P_rwq.3freEaQto6YYVsOn8uVNNDKK1Yv817.v
 eqaTNvgTk5fOO_PPu3NGAUnA_afxXvyWJAIpfBE44yD2VMPIPwNuE4MAsfTu
 2EX.Bb6ZmT7YYEgv9tNJ2aNO15w16zQLPNUKbCDKDf2jS_3qanCGBcRSj.Op
 lBtwz3ZQSENetPg-
X-Originating-IP❸[74.125.82.172]
Authentication-Results: mta1577.mail.ne1.yahoo.com  from=gmail.com; domainkeys=neutral (no sig);  from=gmail.com; dkim=pass (ok)
Received: from 127.0.0.1  (EHLO mail-we0-f172.google.com) (74.125.82.172)
  by mta1577.mail.ne1.yahoo.com with SMTP; Wed, 06 Nov 2013 18:16:33 +0000
Received: by mail-we0-f172.google.com with SMTP id q58so5392697wes.3
        fo❷<test_account@yahoo.com>❺Wed, 06 Nov 2013 10:16:32 -0800 (PST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20120113;
        h=mime-version:date:message-id:subject:from:to:content-type;
        bh=dlBHSl/ACP7PJuXYWPaPhCBGdI26QbEp7CxORuaZ5BU=;
        b=BPGA7wege39PvP3flMtaevMxve1kb8xZUsocFOxhFBKDzlgO+MWjIvFnNNiDiG8EkU
         Y/l8AkRGlOGp1OrNN7Kud65fdNvTgBySAySwjC/Hlet4bkWMv5ViKRHj8QNPQ1nML2k/
         z8eF5LMQMXSIZ69DFzEDsTggJUkWRzgdTf9wgTJlpwffEvzir3R/hizcGTMInDOUzOeW
         q8f3Vm5sF2y+SenPXkTBzHmdS6Ugsq8x9qmOUqx5qJbKxhx6xYpS5/sAfy/XgHmdGSar
         pvQMnF26f3hFvHUfbvj4gUQri1j/qrJbqJL19RjtcDnJKAU8AX2b98WGmIX+bjLlbjIV
         oP/Q==
MIME-Version: 1.0
X-Received: by 10.194.88.225 with SMTP id bj1mr2994653wjb.50.1383761792331;
 Wed, 06 Nov 2013 10:16:32 -0800 (PST)
Received: by 10.217.128.145 with HTTP; Wed, 6 Nov 2013 10:16:32 -0800 (PST)
Date: Wed, 6 Nov 2013 13:16:32 -0500
Message-ID: <CAFNcg7+9gfh66XpObOTN-AN68pPH=+souAjq+FrFy+qN5n6GQg@mail.gmail.com>
Subject: test
From: Gimme The Presentation❶<gimmethepresentation@gmail.com>
To❷test_account@yahoo.com
Content-Type: multipart/alternative; boundary=089e010d852a15f48704ea862691
Content-Length: 198
```

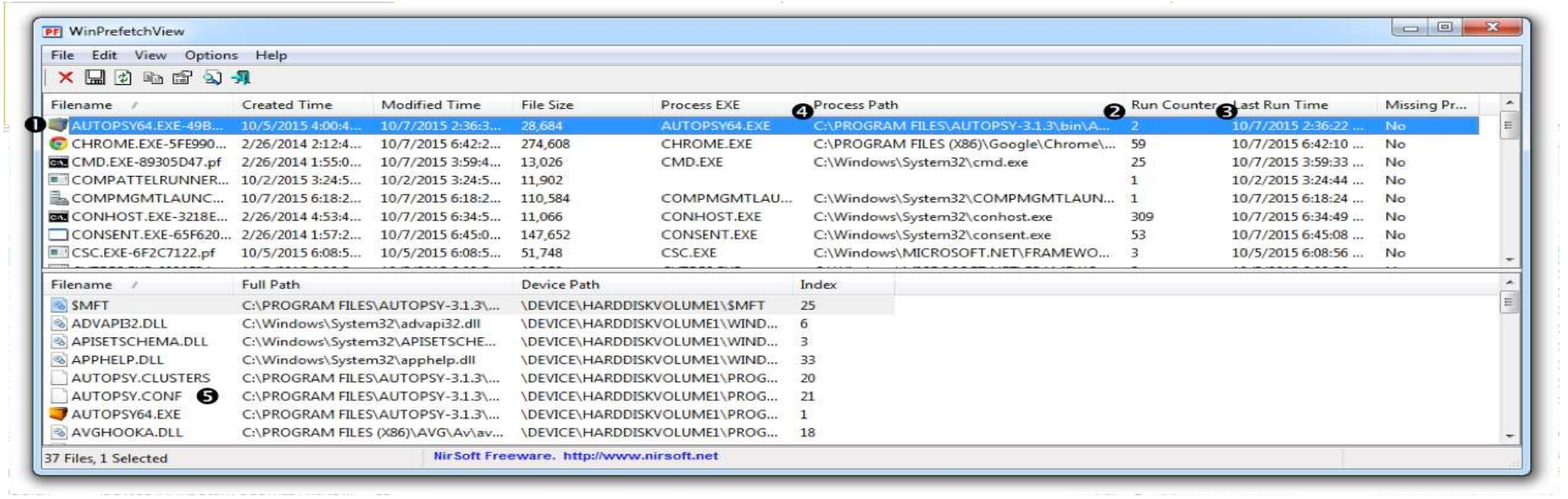
Le cas spécifique des prefetch files

- Windows Xp et versions suivantes
- Au premier lancement d’une application, détermination des fichiers lus (ou non)
- Ces infos sont conservées dans C:\Windows\Prefetch (par défaut)
- Au lancement suivant, Win se fie au .pf de l’application

Anatomie d’un .pf

- Nom et emplacement de l’exécutable
- Liste des fichiers (.dll, notamment) devant être lus dans les 10 secondes qui suivent sont lancement
- Nombre de fois que l’application a été lancée
- Date et heure de la dernière utilisation

Anatomie d’un .pf



File Carving

En cas de métadonnées absente, système de fichiers corrompus ou données compromettantes effacées, il demeure tout de même possible de récupérer ces infos : le **carving**

- FTK Imager (propriétaire)
- Carver Recovery (propriétaire)
- Foremost (open source)
- scalpel (open source)

Monter l’image sur une VM

Why would you do such a thing ?!?

Analyser un partition en **état de stase** est une chose, observer un système **en action** en est une autre

Solution windowsienne

FTK imager + virtualbox
procédure

Procédure linuxienne

idéalement, partir de RAW pour les convertir en vdi

(travailler avec d’autre format d’image à l’air cauchemardesque)

Analyse de la RAM

Gardez à l’esprit qu’une machine en **veille prolongée** est en veille parce que le contenu de sa RAM a été dumpé en SWAP

Premiers pas avec Volatility

La première étape consiste toujours à identifier le système :

```
volatility -f chemin.dmp imageinfo
```

...pour renseigner ce paramètre à chaque commande

```
volatility -f chemin.dmp –profile=Win7SP0x86 plugin
```

Ressources générales

Sources d’images

- https://www.cfreds.nist.gov/
- https://www.forensicfocus.com/images-and-challenges

Forensics sur Linux

- https://linuxleo.com/