INTRODUCTION À L'INVESTIGATION NUMERIQUE

LE PROF

- Laurent Clévy (@lorenz02472)
- Informatique Forensique depuis 2013
- Coordination des analyses Forensique et Malware chez Thales depuis 2015
- Giac Certified Forensic Analyst (GCFA) depuis 2013,
  GREM (Malware reversing) depuis 2015
- Auteur de plusieurs articles MISC sur le forensic et l'analyse de malware
- Cours d'analyse forensique à l'AFTI (master 2) entre 2015 et 2019.

ORGANISATION DU COURS

- 9h30-11h30 : cours
- 12h30-17h30 : TDs et évaluations
  - 12h30 : TD1
  - 13h50 : Evaluation TD1
  - 14h10 : pause de 30mn
  - 14h40 : TD2
  - 16h10 : Evaluation TD2
  - 16h30 : Synthèse
  - 17h30 : envoi de la synthèse

AGENDA

- Principe de l'analyse forensique
- Analyse des métadonnées disques (aperçu, NTFS)
  - Données temporelles NTFS
  - Génération d'une timeline
- Analyse forensique système Windows (aperçu)
  - Registre
  - Journaux (etvx)
  - Preuves d'exécution (aperçu) : prefetch
- Traces applicatives (navigation Web)
- Rédiger un rapport

PRINCIPES DE L'ANALYSE FORENSIQUE

INFO(RMATIQUE) (FO)RENSIQUE

- Est une science
  - Reproductible
  - Méthodique
  - Argumenté
- Un art
  - Il n'y a pas de recette miracle
  - Discipline naissante (15 à 20 ans)
  - Repose beaucoup sur le savoir faire et la bonne utilisations des outils

QUELLES DONNÉES ANALYSER?

L'activité numérique crée de nombreuses traces:

- Sur l'appareil utilisé
  - Par l'application, le système d'exploitation, les « middleware », le système de fichiers…
- Sur le réseau
  - L'accès GSM/3G/LTE, le Proxy, le NAT, le Firewall…
- Sur le serveur distant
  - Serveur de publicité, le serveur de login, le serveur de données statique (images), données dynamiques…

OBJECTIFS DE L'INFORENSIQUE

Reconstituer une scène de crime numérique

- Victime (gère un site Web)

  Déterminer comment un site Web a été attaqué, le parcours de l'attaquant, quelles données ont fuitées

- Attaquant

  Prouver que la machine du suspect est celle qui a été utilisée et de quelle manière

Corréler les données et dates des 2 ensembles de données ci-dessus

Corréler les événements entre plusieurs sources techniques: le système de fichier, les journaux systèmes, les journaux applicatifs, le journal AV, les journaux proxy et FW

EXEMPLES DE CONTEXTE

Réponse à incident

Activité suspectes détectée

- Grâce au SOC (Security Operations Center)
  - Un PC bureautique se met à faire du TOR…
- Un signalement client
- Un disque plein

Expertise numérique légale

Une machine / un téléphone à analyser

INFORENSIQUE, DÉFINITION

Définition

- Investigation numérique légale
- Computer forensics

- "*Computer forensics is equivalent of surveying a crime scene or performing an autopsy on a victim*". {*Source: James Borek 2001*}

Digital Forensic Science

« The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations. » [DFRWS2001]

PRINCIPES FONDAMENTAUX

Préservation des preuves

- Tracer les intervenants, les dates, la pose et l'examen des sceaux numériques
- Ne pas polluer les preuves: toujours travailler sur une copie quand cela est possible

Pouvoir expliquer et prouver sa démarche

- Comment une information a été obtenue
- Démontrer les conclusions obtenues
- Expliquer les doutes restants
- Importance d'un rapport de qualité (20 à 30% du temps passé)

Permettre une contre-expertise

Confidentialité des résultats!

ETAPES D'UNE INVESTIGATION

1. Identification
   - Détecter/identifier l'événement/crime numérique
2. Préservation
   - Préserver la chaîne de preuve
3. Collection
   - Récupérer les données et les preuves
4. Filtrage, Triage et pré-analyse des données
5. Analyse des preuves
6. Présentation des résultats (rapport d'analyse)

TYPES DE COLLECTE

Live

- En utilisant la machine elle-même
- Peut être perturbé par un rootkit (qui cache des fichiers ou processus au système et donc l'outil de collecte!)
- Exemples de collecte Live:
  - Dump mémoire (y compris les malware décompressés en mémoire)
  - Liste des sessions ouvertes, des processus en cours, des fichiers ouverts, des connections réseaux, avec un EDR…
  - Dump Registre, Journaux et MFT (métadonnées NTFS)
  - Copies d'écrans

Offline

- Disque, copie intégrale.
- Pas d'interférence avec le système potentiellement infecté

METADONNÉES DISQUE (NTFS)

NIVEAUX D'ABSTRACTION D'UN SYSTÈME DE FICHIERS

1. Niveau physique (SSD*, HDD, VMDK, VHDX, EWF)
2. Volume logiques (LVM, option)
3. Niveau logique: partitions (décrit dans la MBR ou GPT)
4. Niveau données: cluster/block= Groupe de secteurs
5. Système de fichiers (NTFS, FAT, EXT4): métadonnées
6. Fichiers et répertoires

*https://articles.forensicfocus.com/2016/04/20/ssd-and-emmc-forensics-2016/

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-vhdx

PRINCIPE DE FONCTIONNEMENT

Au début du niveau N, on a les informations pour gérer le niveau N+1

- N=0 : au début d'un disque physique (premier secteurs et suivants), on a la MBR ou GPT, qui contiennent la table des partitions (utilisée par le BIOS ou UEFI)
- N= 1 ou 2: au début d'une partition, on a les informations pour gérer le système de fichiers, des pointeurs vers une table ou un arbre de métadonnées

Une partition NTFS commence avec une VBR, qui contient les caractéristiques du système de fichiers et un pointeur vers la MFT

- http://ntfs.com/ntfs-partition-boot-sector.htm

FORENSIC À PARTIR D'UNE IMAGE DISQUE

- Image : capture secteur par secteur du niveau « physique », pour ne rien manquer : SSD, HDD, VMDK, VHDX
- Accès au logiciel de démarrage : MBR, EFI
- Accès aux partitions
  - Il faut parfois la clé Bitlocker ou LUKS pour déchiffrer
- Accès aux partitions ou à l'espace cachés du système
- Accès aux fichiers effacés (espace libre, mais pas remis à zéro)
- Format le plus courant : EWF/.E01/Encase
  - https://connect.ed-diamond.com/misc/misc-117/description-du-format-de-stockage-forensique-encase-ewf

METADONNÉES NTFS

- $MFT : Master File Table
  - Attribut $I30 : index des répertoires
- $UsnJrnl : journal des données
- $LogFile : journal des métadonnées

```
98693-128-3 c/$Extend/$UsnJrnl:$J
```

```
2-128-1   c/$LogFile
2-48-2    c/$LogFile ($FILE_NAME)
```

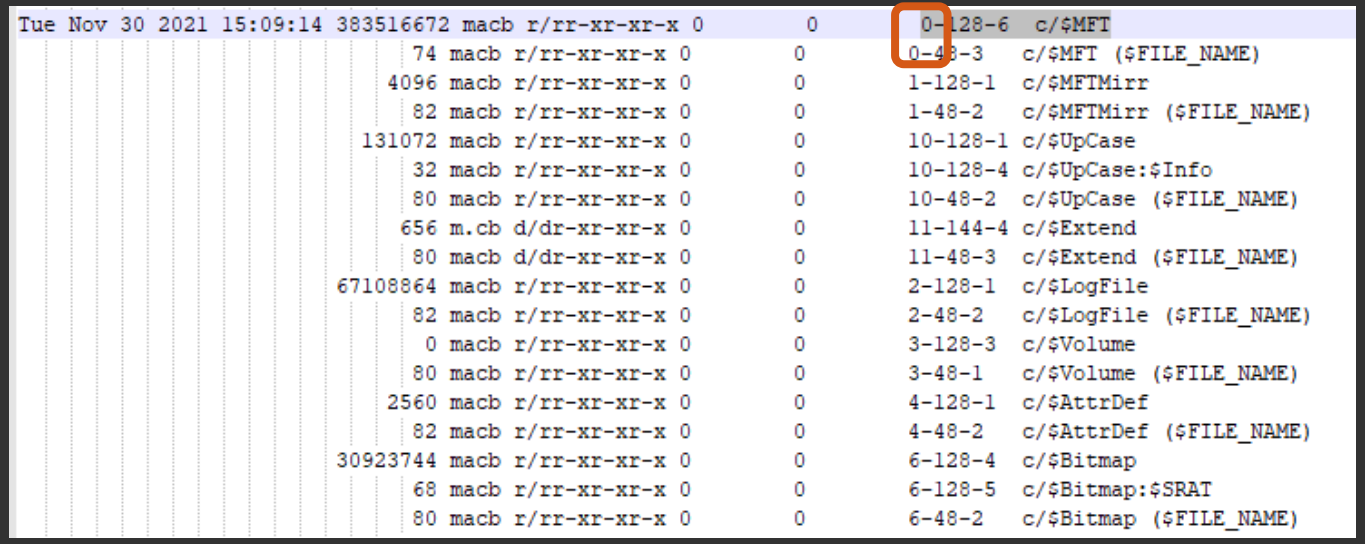
https://learn.microsoft.com/fr-fr/windows-server/administration/windows-commands/fsutil-usn

13cubed: https://www.youtube.com/watch?v=_qElVZJqlGY

MASTER FILE TABLE

Table des métadonnées NTFS, créée lors de l'initialisation de la partition

- ici : 30/11/2021 15h09
- Filename : $MFT
- Contient une entrée pour elle-même : entrée numéro 0 (zéro)
  - L'index dans la MFT, c'est la première colonne dans 0-128-6, 0-48-3, 1-128-1, 1-48-2, 10-128-1 …



```
Tue Nov 30 2021 15:09:14 383516672 macb r/rr-xr-xr-x 0        0         0-128-6  c/$MFT
                              74 macb r/rr-xr-xr-x 0          0         0-48-3   c/$MFT ($FILE_NAME)
                            4096 macb r/rr-xr-xr-x 0          0         1-128-1  c/$MFTMirr
                              82 macb r/rr-xr-xr-x 0          0         1-48-2   c/$MFTMirr ($FILE_NAME)
                          131072 macb r/rr-xr-xr-x 0          0         10-128-1 c/$UpCase
                              32 macb r/rr-xr-xr-x 0          0         10-128-4 c/$UpCase:$Info
                              80 macb r/rr-xr-xr-x 0          0         10-48-2  c/$UpCase ($FILE_NAME)
                             656 m.cb d/dr-xr-xr-x 0          0         11-144-4 c/$Extend
                              80 macb d/dr-xr-xr-x 0          0         11-48-3  c/$Extend ($FILE_NAME)
                        67108864 macb r/rr-xr-xr-x 0          0         2-128-1  c/$LogFile
                              82 macb r/rr-xr-xr-x 0          0         2-48-2   c/$LogFile ($FILE_NAME)
                               0 macb r/rr-xr-xr-x 0          0         3-128-3  c/$Volume
                              80 macb r/rr-xr-xr-x 0          0         3-48-1   c/$Volume ($FILE_NAME)
                            2560 macb r/rr-xr-xr-x 0          0         4-128-1  c/$AttrDef
                              82 macb r/rr-xr-xr-x 0          0         4-48-2   c/$AttrDef ($FILE_NAME)
                        30923744 macb r/rr-xr-xr-x 0          0         6-128-4  c/$Bitmap
                              68 macb r/rr-xr-xr-x 0          0         6-128-5  c/$Bitmap:$SRAT
                              80 macb r/rr-xr-xr-x 0          0         6-48-2   c/$Bitmap ($FILE_NAME)
```

STRUCTURE GÉNÉRALE DE LA MASTER FILE TABLE

- Table
  - Entrée #0 (MFT)
    - Entête « FILE »
    - Attributs
    - Attributs
    - …
  - Entrée #1
    - Entête « FILE »
    - Attributs
    - Attributs
    - …

  …

https://www.ntfs.com/ntfs-mft.htm

STRUCTURE GÉNÉRALE DE LA MASTER FILE TABLE

- Table
  - Entrée #0 (MFT)
    - Entête « FILE »
    - Attributs
    - Attributs
    - …
  - Entrée #1
    - Entête « FILE »
    - Attributs
    - Attributs
    - …

  …

https://www.ntfs.com/ntfs-mft.htm

NTFS: CHAQUE ENTRÉE POSSÈDE DES ATTRIBUTS

Type	Nom	Description
0x10	**$Standard_information**	Horodatage, flags
0x20	$Attribute_List	Lorsqu'il y a trop d'attributs pour une seule entrée (1k) de la MFT
0x30	**$File_Name**	Répertoire parent, horodatage, taille, flags et nom
0x40	$Object_Id	Nom du volume, version de NTFS, dirty flag
0x50	$Security_Descriptor	Info de sécurité et ACLs
0x60	$Volume_Name	
0x70	$Volume_Information	Version NTFS et drapeau
0x80	**$Data**	Contenu du fichiers
0x90	**$Index_Root**	Entête de l'index
0xa0	**$Index_Allocation**	Contenu de l'index
0xb0	$Bitmap	Allocation de l'index
0xc0	$Reparse_Point	Extensions NTFS. Utilisé pour les soft et hard links, les points de montages.
0x100	$Logged_Util_Stream	Contenu pour le journal ou les clés de chiffrement

ATTRIBUTS NTFS

2 sources d'horodatage:

- Attribut $STANDARD_INFORMATION (0x10/16)
- Attribut $FILE_NAME (0x30/48)

Attribut $DATA (0x80/128)

0-128-6 : $DATA
0-48-3 : $FILENAME

```
0-128-6   c/$MFT
0-48-3    c/$MFT ($FILE_NAME)
```

```
>istat -o 673792 f:\2600\ewf\disk.E01 104521
MFT Entry Header Values:
Entry: 104521        Sequence: 3
$LogFile Sequence Number: 438547939
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 1588  (S-1-5-21-2722385413-3376392337-3178984373-1000)
Last User Journal Update Sequence Number: 22648280
Created:        2022-10-20 09:29:46.714795700 (Paris, Madrid (heure d
File Modified:     2022-10-31 10:25:22.064067100 (Paris, Madrid)
MFT Modified:   2022-10-31 10:25:22.064067100 (Paris, Madrid)
Accessed:       2022-10-31 10:25:22.392014000 (Paris, Madrid)

$FILE_NAME Attribute Values:
Flags: Archive
Name: History
Parent MFT Entry: 104517        Sequence: 3
Allocated Size: 0       Actual Size: 0
Created:        2022-10-20 09:29:46.714795700 (Paris, Madrid (heure d
File Modified:     2022-10-20 09:29:46.714795700 (Paris, Madrid (heure d
MFT Modified:      2022-10-20 09:29:46.714795700 (Paris, Madrid (heure d
Accessed:    2022-10-20 09:29:46.714795700 (Paris, Madrid (heure d

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-2)   Name: N/A   Resident   size: 80
Type: $DATA (128-3)   Name: N/A   Non-Resident   size: 196608  init_size: 192512
2518127 59010 59011 59012 59013 34725 34726 34727
34728 34729 34730 34731 34732 34733 34734 34735
34736 34737 34738 34739 34740 34741 34742 34743
34744 34745 92882 92883 92884 92885 92886 123418
123419 258950 258951 260898 123369 123370 85293 3242064
3242065 3242066 3242067 3242068 3242069 3242070 3242071 3242072
```

HORODATAGE « MACB »

- M = File Modified
- A = Accessed
- C = MFT Modified (Change)
- B = Created (Birth)

```
$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 1588  (S-1-5-21-2722385413-3376392337-3178984373-1000)
Last User Journal Update Sequence Number: 22648280
Created:        2022-10-20 09:29:46.714795700 (Paris, Madrid (heure d
File Modified:     2022-10-31 10:25:22.064067100 (Paris, Madrid)
MFT Modified:   2022-10-31 10:25:22.064067100 (Paris, Madrid)
Accessed:       2022-10-31 10:25:22.392014000 (Paris, Madrid)
```

B = date de création du fichier sur ce volume (copie ou installation)

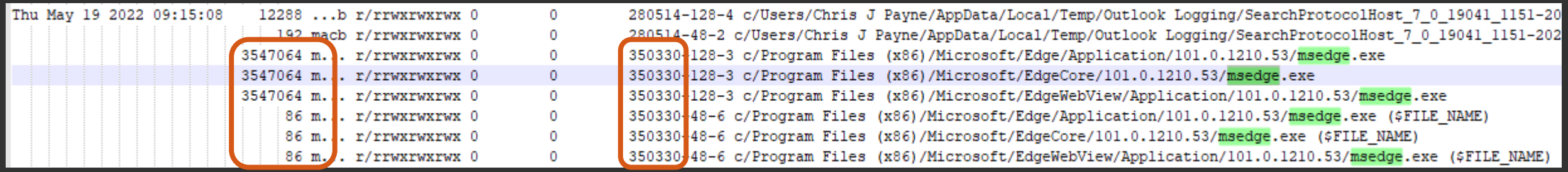
M = date de modification du contenu (compilation pour un binaire)

13Cubed : https://www.youtube.com/watch?v=OTea54BelTg

HORODATAGE « MACB » : EXEMPLE « M »

B = date de <u>création</u> du fichier sur ce volume (copie ou installation)

M = date de modification <u>du contenu</u> (compilation pour un binaire)



```
Thu May 19 2022 09:15:08    12288 ...b r/rrwxrwxrwx 0       0       280514-128-4 c/Users/Chris J Payne/AppData/Local/Temp/Outlook Logging/SearchProtocolHost_7_0_19041_1151-20
                              192 macb r/rrwxrwxrwx 0       0       280514-48-2 c/Users/Chris J Payne/AppData/Local/Temp/Outlook Logging/SearchProtocolHost_7_0_19041_1151-202
                          3547064 m... r/rrwxrwxrwx 0       0       350330-128-3 c/Program Files (x86)/Microsoft/Edge/Application/101.0.1210.53/msedge.exe
                          3547064 m... r/rrwxrwxrwx 0       0       350330-128-3 c/Program Files (x86)/Microsoft/EdgeCore/101.0.1210.53/msedge.exe
                          3547064 m... r/rrwxrwxrwx 0       0       350330-128-3 c/Program Files (x86)/Microsoft/EdgeWebView/Application/101.0.1210.53/msedge.exe
                               86 m... r/rrwxrwxrwx 0       0       350330-48-6 c/Program Files (x86)/Microsoft/Edge/Application/101.0.1210.53/msedge.exe ($FILE_NAME)
                               86 m... r/rrwxrwxrwx 0       0       350330-48-6 c/Program Files (x86)/Microsoft/EdgeCore/101.0.1210.53/msedge.exe ($FILE_NAME)
                               86 m... r/rrwxrwxrwx 0       0       350330-48-6 c/Program Files (x86)/Microsoft/EdgeWebView/Application/101.0.1210.53/msedge.exe ($FILE_NAME)
```

M = date de compilation de msedge.exe = 19/05/2022 9h15m08

3547064 = filesize (attribut $DATA, -128-)

350330 = numéro d'entrée dans la MFT

HORODATAGE « MACB » : EXEMPLE « BIRTH »

B = date de <u>création</u> du fichier sur ce volume (copie ou installation)

M = date de modification <u>du contenu</u> (compilation pour un binaire)

```
Tue May 24 2022 08:44:20      544 m... d/drwxrwxrwx 0        0        318025-144-1 c/Program Files (x86)/Microsoft/EdgeCore/101.0.1210.53/Notifications
                              288 m... d/drwxrwxrwx 0        0        318354-144-1 c/Program Files (x86)/Microsoft/EdgeCore/101.0.1210.53/PdfPreview
...
                          3547064 ...b r/rrwxrwxrwx 0        0        350330-128-3 c/Program Files (x86)/Microsoft/Edge/Application/101.0.1210.53/msedge.exe
                          3547064 ...b r/rrwxrwxrwx 0        0        350330-128-3 c/Program Files (x86)/Microsoft/EdgeCore/101.0.1210.53/msedge.exe
                          3547064 ...b r/rrwxrwxrwx 0        0        350330-128-3 c/Program Files (x86)/Microsoft/EdgeWebView/Application/101.0.1210.53/msedge.exe
```

B = date de copie du binaire sur le volume (MAJ) = 24/05/2022 8h44m20

350330 = numéro d'entrée dans la MFT

TIMELINE NTFS: DELETED

- Les fichiers effacés sont juste marqués comme tels, mais les données ne sont pas remises à zéro

```
65536 mac. -/rrwxrwxrwx 0        0        61266-128-3 c/Windows/System32/sru/SRU03E57.log (deleted)
   90 mac. -/rrwxrwxrwx 0        0        61266-48-17 c/Windows/System32/sru/SRU03E57.log ($FILE_NAME) (deleted)
```

- On peut tenter d'extraire l'entrée 61266 et retrouver le contenu du fichier !

TIMELINE: RÉSUMÉ

- Chercher les événements « Birth » : installation d'un malware
- Chercher les événements « content Modification » : modification d'un journal ou d'une configuration (.ssh/authorized_keys)
- Permet dans certain cas
  - de retrouver le fait qu'un fichier a été effacé
  - en retrouver le contenu
- Souvent on peut suivre un téléchargement, une exécution (.lnk, .pf), une détection AV (.etvx) …

OUTILLAGE : THE SLEUTH KIT

- Niveau physique (mm pour medium)
  - mmls disk.e01 ou disk.vmdk : liste les partitions, début et tailles en secteurs
- Niveau partition (f pour filesystem)
  - fls : liste les entrées (métadonnées) du système de fichier
  - fsstat : stats sur le système de fichier
  - Il faut indiquer le début de la partition avec l'option -o
- Niveau métadonnées (i pour inode)
  - icat : extrait le contenu d'un fichier
  - istat : stats sur une entrée (fichier ou répertoire)

THE SLEUTH KIT : QUELQUES EXEMPLES

- mmls disk.e01
  - Résultat : la partition pertinente commence au secteur 2048
- fls -o 2048 disk.e01
  - Résultat : l'entrée $MFT porte l'index 0 (zéro)
- icat -o 2048 disk.e01 0 > $MFT.bin

L'entrée zéro de la $MFT est la $MFT

THE SLEUTH KIT : TIMELINE

fls -r -mc -o 2048 > fls_body.txt

-r : récursif

-m : mount point (lecteur c dans l'exemple)

mac_time.pl –b fls_body.txt > fls.txt

ANALYSE FORENSIQUE SYSTÈME (APERÇU)

- Registre
- Journaux (evtx, antivirus)
- Preuves d'exécution : prefetch

REGISTRE WINDOWS (HIVES)

- Registres système
  - %SystemRoot%\System32\Config
    - HKEY_LOCAL_MACHINE (HKLM)
      - System: (C:\Windows\System32\Config\System)
      - Software: (C:\Windows\System32\Config\Software)
      - SAM: (C:\Windows\System32\Config\Sam)
      - Security: (C:\Windows\System32\Config\Security)
    - HKEY_CURRENT_CONFIG (HKCC), points to *HKLM\SYSTEM\CurrentControlSet\CurrentControlSet\HardwareProfiles\Current*
- Registre Utilisateur, HKEY_CURRENT_USER (HKCU)
  - Un par profil utilisateur dans %UserProfile%\NTUSER.DAT
    - C:\Users\laurent\NTUSER.DAT
  - %userprofile%\AppData\Local\Microsoft\Windows\UsrClass.dat (Vista – Win10)
  - %userprofile%\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat (XP & 2003)

UTILISATION DU REGISTRE POUR LE FORENSIC

- Persistence (Run, RunOnce, Autoruns)
- Preuves d'exécution ou d'ouverture de fichiers (MRU, Most Recently Used, UserAssist)
- Traces réseau (NetworkList)
- Traces fichiers (explorateur de fichiers) : ShellBags
- Marqueurs malware
- Stockage malware (fileless)
- Configuration du système, des comptes, des applications…

…

Registry Explorer : https://ericzimmerman.github.io/#!index.md

REGISTRE: OUTILLAGE

- Regripper
- Ecrit en Perl
- Syntaxe (Windows) : rip -r hive -p plugin
- Ruches / hives : system, software, sam, ntuser.dat, usrclass.dat
- Plugins : shellbags, run, …

- https://github.com/keydet89/RegRipper3.0
- https://hexacorn.com/tools/3r.html

JOURNAUX WINDOWS ETVX

Dans c:\windows\system32\winevt\logs

- system.evtx
- security.evtx
- application.evtx
- powershell.evtx
- wmi.evtx
- WindowDefender.evtx
- RDP.evtx

JOURNAUX ETVX : OUTILLAGE

- EvtxCmd converti les .etvx en json ou xml
  -f input
  --csvf output.csv
  --csv output_dir

- https://ericzimmerman.github.io/#!index.md

PREFETCH (.PF)

C'est une preuve d'exécution

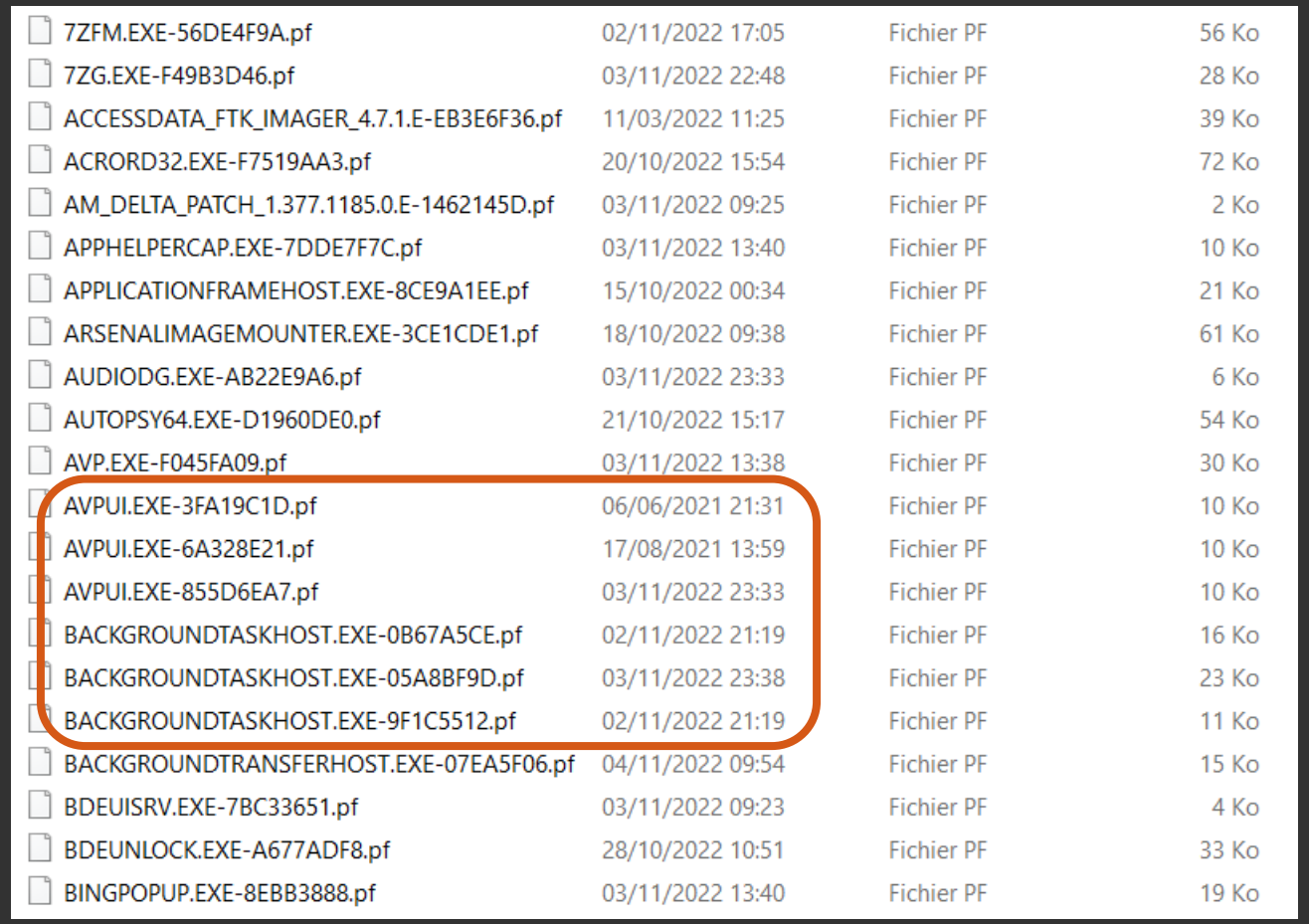
Disponible par défaut sur les workstations, pas les serveurs.

Les fichiers prefetch servent à optimiser le chargement des DLL pour les applications Windows en gardant un cache de la liste de ces DLL et en les pré-chargeant. Effet de bord, cela garde des données sur le nombre et l'horodatage des exécutions

Localisés dans c:\Windows\prefetch

13cubed : https://www.youtube.com/watch?v=f4RAtR_3zcs

PREFETCH (.PF) EXEMPLES



7ZFM.EXE-56DE4F9A.pf	02/11/2022 17:05	Fichier PF	56 Ko
7ZG.EXE-F49B3D46.pf	03/11/2022 22:48	Fichier PF	28 Ko
ACCESSDATA_FTK_IMAGER_4.7.1.E-EB3E6F36.pf	11/03/2022 11:25	Fichier PF	39 Ko
ACRORD32.EXE-F7519AA3.pf	20/10/2022 15:54	Fichier PF	72 Ko
AM_DELTA_PATCH_1.377.1185.0.E-1462145D.pf	03/11/2022 09:25	Fichier PF	2 Ko
APPHELPERCAP.EXE-7DDE7F7C.pf	03/11/2022 13:40	Fichier PF	10 Ko
APPLICATIONFRAMEHOST.EXE-8CE9A1EE.pf	15/10/2022 00:34	Fichier PF	21 Ko
ARSENALIMAGEMOUNTER.EXE-3CE1CDE1.pf	18/10/2022 09:38	Fichier PF	61 Ko
AUDIODG.EXE-AB22E9A6.pf	03/11/2022 23:33	Fichier PF	6 Ko
AUTOPSY64.EXE-D1960DE0.pf	21/10/2022 15:17	Fichier PF	54 Ko
AVP.EXE-F045FA09.pf	03/11/2022 13:38	Fichier PF	30 Ko
AVPUI.EXE-3FA19C1D.pf	06/06/2021 21:31	Fichier PF	10 Ko
AVPUI.EXE-6A328E21.pf	17/08/2021 13:59	Fichier PF	10 Ko
AVPUI.EXE-855D6EA7.pf	03/11/2022 23:33	Fichier PF	10 Ko
BACKGROUNDTASKHOST.EXE-0B67A5CE.pf	02/11/2022 21:19	Fichier PF	16 Ko
BACKGROUNDTASKHOST.EXE-05A8BF9D.pf	03/11/2022 23:38	Fichier PF	23 Ko
BACKGROUNDTASKHOST.EXE-9F1C5512.pf	02/11/2022 21:19	Fichier PF	11 Ko
BACKGROUNDTRANSFERHOST.EXE-07EA5F06.pf	04/11/2022 09:54	Fichier PF	15 Ko
BDEUISRV.EXE-7BC33651.pf	03/11/2022 09:23	Fichier PF	4 Ko
BDEUNLOCK.EXE-A677ADF8.pf	28/10/2022 10:51	Fichier PF	33 Ko
BINGPOPUP.EXE-8EBB3888.pf	03/11/2022 13:40	Fichier PF	19 Ko

Il peut y avoir plusieurs fichiers prefetch pour une application

Les fichiers .pf sont limités en nombre, on ne peut conclure sur l'absence de l'un entre eux, car il peut avoir été effacé par le système ou l'attaquant (mais il y a moyen de retrouver les fichiers effacés)

PREFETCH (.PF) EXEMPLES

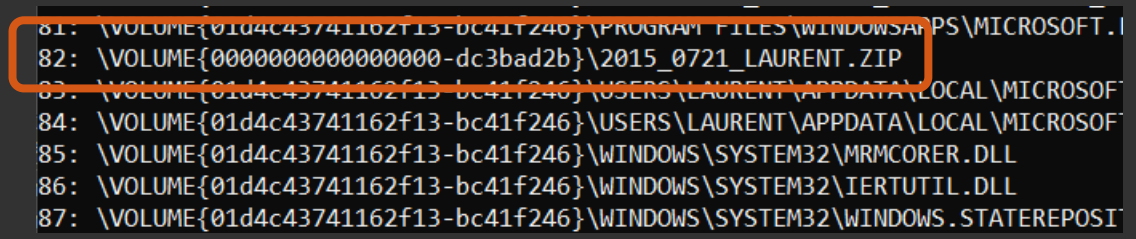
```
C:\_tools\PECmd>PECmd.exe -f c:\Windows\Prefetch\7ZFM.EXE-56DE4F9A.pf
PECmd version 1.4.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -f c:\Windows\Prefetch\7ZFM.EXE-56DE4F9A.pf

Warning: Administrator privileges not found!

Keywords: temp, tmp

Processing 'c:\Windows\Prefetch\7ZFM.EXE-56DE4F9A.pf'

Created on: 2021-03-15 14:32:11
Modified on: 2022-11-02 16:05:50
Last accessed on: 2022-11-04 08:59:56

Executable name: 7ZFM.EXE
Hash: 56DE4F9A
File size (bytes): 287 216
Version: Windows 10

Run count: 95
Last run: 2022-11-02 16:05:42
Other run times: 2022-11-02 15:51:11, 2022-10-26 15:09:59, 2022-10-24 13:13:34, 2022-10-20 13:53:43, 2022-10-13 15:07:29, 2022-10-13 14:33:57, 2022-10-13 14:29:44

Volume information:

#0: Name: \VOLUME{0000000000000000-dc3bad2b} Serial: DC3BAD2B Created: 1601-01-01 00:00:00 Directories: 0 File references: 0
#1: Name: \VOLUME{01d046b484c1f2c0-d485e2c9} Serial: D485E2C9 Created: 2015-02-12 11:10:32 Directories: 0 File references: 0
#2: Name: \VOLUME{01d4c43741162f13-bc41f246} Serial: BC41F246 Created: 2019-02-14 07:31:09 Directories: 23 File references: 83
#3: Name: \VOLUME{01d849bda228b13e-30a25c99} Serial: 30A25C99 Created: 2022-04-06 13:53:02 Directories: 0 File references: 0
#4: Name: \VOLUME{01d8d399a0e13380-6407d68b} Serial: 6407D68B Created: 2022-09-29 00:22:59 Directories: 0 File references: 0
```

Nombre d'exécutions et dates pour ce fichier prefetch.

PREFETCH (.PF) EXEMPLES

Permet parfois de retrouver les fichiers et les volumes liés à l'application !

Ici certainement un stockage externe (commençant par des zéros, lié au système ExFat ?)



TRACES APPLICATIVES

Exemple : Navigation Web

- Historique
- Download
- Cookies
- Cache

Pour Firefox, Chrome, Edge, Internet Explorer

Dans les profils utilisateurs

PAS LE TEMPS DE VOIR EN 1 JOUR

Comment remonter dans le passé (corbeille, shadowcopy)

Les autres preuves d'exécution

Le détail des systèmes de fichiers ExFAT, NTFS et EXT4, des partitions MBR et GPT

Le forensic mémoire (avec Volatility)

Le forensic Android

Le détail des EventId Security à analyser

Plus de détails sur le Registre

…