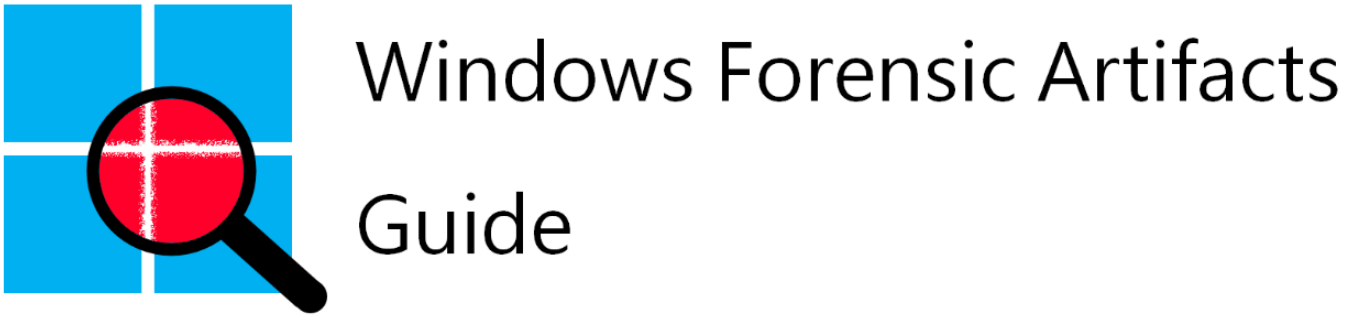
[Windows]

- [Forensic] Artefacts

[Forensic] Artefacts

Introduction

Différents artefacts sont intéressants selon ce que vous cherchez. Beaucoup passent par la base de registre, certains sont des prefetchs, des shell links etc ou même des journaux d'évènements.



Cheat-sheet

Ruches (registres)

Ruches	Chemin	Description
SAM	C:\Windows\System32\config\SAM	Base SAM (Contient la base des utilisateurs)
SOFTWARE	C:\Windows\System32\config\SOFTWARE	Contient les informations des logiciels installés sur la machine.
SECURITY	C:\Windows\System32\config\SECURITY	

SYSTEM	C:\Windows\System32\config\SYSTEM	
NTUSER	C:\Users\<YOUR_USER>\NTUSER.DAT	Contient les informations utilisateurs.
USRCLASS	C:\Users\<YOUR_USER>\USRCLASS.dat	

Registres

Registres	Description
SOFTWARE\Microsoft\Windows NT\CurrentVersion	Contient toutes les informations systèmes (comme systeminfo). Inclut le Product Name (OS), EditionID, DisplayVersion (version), InstallDate (date de dernière maj), SystemRoot.
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Uninstall	Logiciels installés sur le postes (avec un uninstaller).
SYSTEM\CurrentControlSet\Control\ComputerName\ OU System\ControlSet001\Control\ComputerName\ComputerName\	Nom de l'ordinateur.
SYSTEM\CurrentControlSet\Control\TimeZoneInformation OU SYSTEM\ControlSet001\Control\TimeZoneInformation\	Fuseau horaires.
SYSTEM\CurrentControlSet\Control\Windows OU SYSTEM\ControlSet001\Control\Windows\	Dernière extinction du système.
SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList	Contient une sous-clé par utilisateur avec toutes les infos utilisateurs.
SAM\Domains\Account\Users	Dernier login et changement de mot de passe.
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run	Démarrage automatique (Si clé "Start"=2 alors activé)
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce	Démarrage automatique (Si clé "Start"=2 alors activé)
SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Démarrage automatique (Si clé "Start"=2 alors activé)
SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Démarrage automatique (Si clé "Start"=2 alors activé)
SYSTEM\CurrentControlSet\Services	Démarrage automatique (Si clé "Start"=2 alors activé)

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	Fichiers récents : Sous-clé contenant les 20 dernières entrées pour chaque type de fichiers, en format binaire. Folder : les 30 derniers répertoires.
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU	Dernières application exécutées.
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU	Sous clés contenant le nom des 20 derniers fichiers enregistrés, par extensions.
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery	Recherches entrées par l'utilisateur dans l'explorateur, en unicode.
NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	Seulement les commandes valides entrées dans l'invite RUN (WIN+R).
NTUSER.DAT\Control Panel\Desktop	Chemin du fond d'écran de l'utilisateur
SYSTEM\CurrentControlSet\Enum\USBSTOR	Périphériques USB branchés. (FriendlyName=Nom, ClassGUID=Identifiant Unique)
SOFTWARE\Microsoft\Windows Portable\Devices\Devices	Une clé par périphérique, avec le FriendlyName.
SYSTEM\MountedDevices	Lettre de périphérique avec identifiant.
SOFTWARE\Microsoft\Windows\Search\VolumeInfoCache	Une clé par périphérique, avec le Volume Label.
SAM\SAM\Domains\Account\Users\Names	Liste des utilisateurs du système.
SAM\SAM\Domains\Account\Users\RID Manager	La clé F stocke les dates de connexion sur les utilisateurs et la clé V stocke les noms d'utilisateurs par SID.

Shell Links

Vous pouvez retrouver vos shell links à l'emplacement suivant :

```
%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\
```

Vous pouvez traiter vos shell links avec l'outil d'Eric Zemmour :

```
LECmd.exe –f your-shell-link.lnk
```

Jumplists

Vous pouvez retrouver vos jumplists à l'emplacement suivant :

```
%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
```

```
%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations
```

Vous pouvez traiter vos jumplists avec l'outil d'Eric Zimmerman **JumpListExplorer** :

Drag a column header here to group by that column

	E...	Target Created On	Target Modified On	Target Accessed On	Absolute Path	Extra Block...	Interaction Co...
	=	=	=	=	=	=	=
	1	2024-03-14 14:55:57	2023-11-24 09:28:10	2024-03-14 14:55:56	My Computer\E:\Downloads\C.docx	1	3
▸	2	2024-03-21 00:47:29	2024-02-23 19:16:14	2024-03-21 00:47:30	My Computer\C:\Users\Bruno\Documents\COMPUTER FORE...	2	136
	3	2024-04-04 11:39:23	2024-04-04 11:39:23	2024-04-04 11:39:23	My Computer\C:\Users\Bruno\Documents\Rachat Soleil Leva...	2	3
	4	2024-04-04 12:26:31	2024-04-04 12:26:32	2024-04-04 12:26:35	My Computer\C:\Users\Bruno\Downloads\27_2024_T25_T...	2	3
	5	2024-04-07 16:54:13	2024-04-07 16:54:13	2024-04-08 13:26:15	Documents\EsGI\COMPUTER FORENSIC.docx	2	2
	6	2024-03-20 00:48:14	2024-04-08 09:09:02	2024-04-07 22:00:00	F:\\GIE EDUCTIVE Fiche renseignement Presta MicroEnt_Pro...	1	5

Thumbcaches

Vous pouvez retrouver vos thumbcaches à l'emplacement suivant :

```
%userprofile%\AppData\Local\Microsoft\Windows\Explorer
```

Pour avoir les chemins dans Thumbcache Viewer il vous faudra extraire aussi cette base :

```
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db
```

> Il y a plusieurs entrées tels que thumbcache_32.db, thumbcache_96.db, thumbcache_256.db . Prenez les toutes si possible.

> Vous pouvez traiter vos jumplists avec l'outil **Thumbcache Viewer**.

Volumes Shadow Copies (VSC / VSS)

Les VSC sont stockées dans le dossier "**System Volume Information**" à la racine de votre volume (ex: *C:*).

Pour lister vos shadow copies (dans un cmd avec les privilèges administrateurs) :

```
vssadmin.exe list shadows /for=C:
```

> Vous pouvez monter vos VSC avec un logiciel comme**Arsenal Image Mounter** avec un cache en écriture.

Vous pouvez aussi monter vos VSC avec la commande suivante :

```
mklink /d <mount point> \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopyXXX\
```

> Cette opération va créer un lien symbolique vers votre volume shadow copie mais nécessitera les privilèges administrateurs pour y accéder.

Un solution alternative consiste à utiliser l'outil **VSCMount.exe** de la suite Zimmerman pour monter votre VSC :

```
.\VSCMount.exe --dl C --mp C:\Users\MalDev\Documents\VSC-mount
```

> Ici, on monte tous les VSCs du lecteur **C** dans le répertoire **C:\Users\MalDev\Documents\VSC-mount** .

SRUM

Il s'agit des fichiers qui stockent les métriques des ressources utilisées sur le système. Vous pouvez avoir des informations comme :

- Les applications exécutées.
- La quantité de données transférées,
- Les périodes d'activité du système.

La base de données SRU est stockée à l'emplacement suivant :

```
C:\Windows\System32\SRU\SRUDB.dat
```

Combiné à la ruche SOFTWARE, vous allez pouvoir l'analyser avec l'outil d'Eric Zimmerman :

```
SrumECmd.exe -f SRUDB.dat -r SOFTWARE --csv SRUM_export
```

AMCache

Stocke des informations sur les applications exécutées notamment leur hashs (non disponible dans les prefetchs).

Voici l'emplacement de l'AMCache :

```
C:\Window\AppCompat\Programs\Amcache.hve
```

Vous allez pouvoir l'analyser avec l'outil d'Eric Zimmerman **AmcacheParser :**

```
AmcacheParser.exe -f Amcache.hve --csv <dst>
```

Il se peut que le fichier ruche Amcache.hve soit endommagé. Dans ce cas, vous pouvez le réparer avec **hvexsh** sous Linux.

Pour l'installer :

```
apt install -y libhivex-bin
```

Puis :

```
hivexsh -w amcache.hve
> commit
> quit
```

Prefetch

Le nom de chaque fichier prefetch est composé du nom de l'application concernée, suivi de **8** caractères représentant le hash du chemin d'exécution, puis de l'extension PF (ex: **GKAPE.EXE-FA3D288B.pf**).

Voici l'emplacement des fichiers prefetch :

```
C:\Windows\Prefetch
```

A savoir qu'il est possible de brute force le hash du prefetch pour retrouver le chemin de l'application :

- https://github.com/harelsegev/prefetch-hash-cracker

Vous pouvez analyser vos prefetch avec l'outil d'Eric Zimmerman :

```
PECmd.exe -d <dir_with_prefetchs> --csv <dst>
```

ShellBags

Les fichiers **ShellBags** sont des artefacts Windows stockés dans le registre et utilisés par l'Explorateur Windows pour mémoriser les préférences d'affichage des dossiers (taille, position, mode d'affichage, etc.). En **forensic**, ils sont précieux pour reconstituer l'historique des accès aux

répertoires, y compris ceux qui ont été supprimés.

Ils sont récupérables depuis le registre suivant :

- **HKEY_USERS{SID}\Software\Microsoft\Windows\Shell\Bags**
- **HKEY_USERS{SID}\Software\Microsoft\Windows\Shell\BagMRU**

Vous pouvez explorer les shellbags depuis le logiciel ShellBags Explorer (SBE) de la suite Zimmerman.

Corbeille

La corbeille se situe à la racine du volume dans un répertoire caché nommé **$Recycle.Bin** notamment dans :

```
C:\$Recycle.Bin
```

> Chaque sous-répertoire, nommé après le **SID** de chaque utilisateur et contient les fichiers de l'utilisateur qui les a supprimés.

> Le nom original du fichier est modifié, (**6** random characters + extension) mais peut être retrouvé en étudiant la **$MFT**, ainsi que les métadonnées d'un fichier d'information.

On différencie deux types de fichiers :

$R*** . ***	Fichier original
$I*** . ***	Information sur le fichier

Journaux d'évènements (EVTX)

Les journaux des événements Windows, enregistrent les activités du système tels que:

• Les ouvertures de programmes

• Les interactions utilisateurs

• Les modifications systèmes

• Les périphériques installés

• Les démarrages et extinctions

• Les logons et logoffs

Ils sont localisés dans :

```
C:\Windows\System32\winevt\Logs
```

On distingue 5 types d'évènements :

Types d'évènements	Descriptions
Error	L'évènement occasionne une erreur
Warning	L'évènement s'est bien déroulé, mais une erreur pourrait survenir dans le futur.
Information	Indique un évènement réussi
Audit Success	L'action surveillée par les politiques d'audit s'est bien déroulée
Audit failure	L'action surveillée par les politiques d'audit ne s'est pas bien déroulée

On distingue 3 catégories de journaux :

- **Sécurité** : Enregistre les tentatives de connexion, les changements de politiques de sécurité, l'accès aux ressources etc.
- **Système** : Enregistre les notifications au noyau, les informations des pilotes de périphériques etc.
- **Application** : Enregistre les erreurs d'application, les avertissements et les autres messages générés par les applications.

Voici quelques code d'évènements qui vous seront intéressants :

Codes	Descriptions
4624	Succès de connexion
4625	Echec de connexion
4648	Tentative de connexion avec des identifiants explicites.
4672	Attribution de privilèges spéciaux lors d'une ouverture de session.
1102	Effacement du journal des événements (Sécurité, Système, Application).
4720	Création d'un compte utilisateur.
4726	Suppression d'un compte utilisateur.

4728	Un utilisateur a été ajouté à un groupe de sécurité globale.
4732	Un utilisateur a été ajouté à un groupe de sécurité local.
4756	Un membre a été ajouté à un groupe de sécurité universel.
4776	La validation du compte utilisateur a été tentée.
4946	Un changement a été effectué dans le pare-feu Windows.
7045	Un service a été installé dans le système.

Pour chercher un code particulier :

- https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/
- https://andreafortuna.org/2019/06/12/windows-security-event-logs-my-own-cheatsheet/

Éric Zimmerman a développé un outil pour traiter les logs EVTX et les exporter dans un fichier CSV ce qui peut être beaucoup plus facile à traiter :

```
EvtxECmd.exe -d <EVTX_DIR> --csv <Output_DIR>
```

Navigateurs internet

Voici les emplacements des différents profiles de navigateur :

Navigateurs	**Chemins**
Edge	/AppData/Local/Microsoft/Edge/User Data/Default/
Firefox	/AppData/Roaming/Mozilla/Firefox/Profiles/
Chrome	/AppData/Local/Google/Chrome/User Data/Default/
Chromium	/AppData/Local/Chromium/User Data/Default/
Brave	/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/
Opera	/AppData/Roaming/Opera Software/Opera Stable/
Vivaldi	/AppData/Local/Vivaldi/User Data/Default/

360 Speed	/AppData/Local/360chrome/Chrome/User Data/Default/
QQ	/AppData/Local/Tencent/QQBrowser/User Data/Default/
Yandex	/AppData/Local/Yandex/YandexBrowser/User Data/Default/
CocCoc	/AppData/Local/CocCoc/Browser/User Data/Default/

Voici 2 outils pour extraire toutes les informations des navigateurs :

- https://github.com/moonD4rk/HackBrowserData
- https://www.nirsoft.net/utils/browsing_history_view

Quelques exemples de données intéressantes à récupérer :

Types de données	**Fichiers**
Historique de téléchargement	places.sqlite ou History
Favoris	bookmarks.json ou Bookmarks
Identifiants	logins.json ou Login Data
Auto-completions	formhistory.sqlite ou Web Data ou Shortcuts ou Login Data