Forensic

- Les bases du computer forensic
- Memory forensic (Volatility)

Les bases du computer forensic

DÉFINITION DU FORENSIC

Le forensic, ou criminalistique numérique, est une discipline qui consiste à collecter, analyser et préserver des preuves numériques afin de les utiliser dans des enquêtes judiciaires ou techniques. Cela inclut l'étude des disques durs, systèmes de fichiers, réseaux, et tout autre support numérique.

PRINCIPES FONDAMENTAUX DU FORENSIC

1 - **Identification** : Processus visant à déterminer l'individualité d'une personne ou d'un objet en reliant des traces ou des preuves à une identité connue. Cela inclut l'analyse des empreintes digitales, des données biométriques, des fichiers numériques, ou des objets physiques pour établir un lien avec une personne ou un événement spécifique.
2- **Saisie** : Collecte méthodique et sécurisée des preuves numériques ou physiques tout en garantissant leur intégrité. Cela inclut l'utilisation de techniques et outils spécialisés pour capturer les données sans les altérer, comme la création d'images forensiques de disques ou la confiscation de matériel lors d'une perquisition.
3- **Analyse** : Examen approfondi des données collectées afin d'identifier, interpréter et comprendre les preuves. Cela peut inclure la recherche de métadonnées, l'extraction d'informations cachées, la reconstruction d'événements ou la détection d'activités suspectes dans les journaux système.
4- **Rapport** : Documentation claire et détaillée des résultats obtenus lors de l'enquête, incluant les méthodes utilisées, les conclusions tirées et les preuves présentées. Le rapport doit être compréhensible pour un public non technique (comme les jurés), tout en respectant les standards légaux et scientifiques. En computer forensic on parle de deux types d'extractions (une extraction est un enregistrement de l'appareil tel qu'il est à un instant donné).

Principe d'extraction d'un support matériel

Ça consiste à copier le disque dur d'un support physique (SSD, disque SATA etc..) ou d'un PC, Mac. L'opération se fait avec un bloqueur d'écriture. Il existe des bloqueurs d'écriture matériel sur lesquelles on branche directement nos disques dur internes grâce à des adaptateurs et des bloqueurs d’écritures logiciel qui se brancheront sur le pc directement et bloquant qui contrôlent et filtrent les commandes d'entrée-sortie envoyées au support de stockage

Il existe deux types d'extractions :

Extraction physique :

C'est une copie bit à bit de l'ensemble d'un apprareil (pc ou mobile)
en format ewf (Expert Witness Format) .E01, .E02, est un format empêchant l'écriture par défaut, read only

Extraction Logique :

Une extraction que d'un ensembles de données visées
en format AFF(Advanced Forensic Format)

OUTILS ET TECHNIQUES UTILISÉS EN FORENSIC

OUTILS DE BASE

- **dd** : Utilisé pour créer une image brute d'un disque ou d'une partition.
  - Exemple : `dd if=/dev/sda of=/path/to/image.img bs=4M`
- **hash (md5sum, sha256sum)** : Génération de hash pour vérifier l'intégrité des fichiers.
  - Exemple : `md5sum image.img`
- **strings** : Extraction de chaînes de caractères lisibles dans un fichier ou une image disque.
  - Exemple : `strings image.img | grep "password"`

OUTILS AVANCÉS

- **Autopsy** : Interface graphique pour l'analyse forensic basée sur The Sleuth Kit.
- **The Sleuth Kit (TSK)** : Collection d'outils en ligne de commande pour analyser les systèmes de fichiers.
- **Volatility** : Analyse forensic de la mémoire vive (RAM).
- **Wireshark** : Analyseur de paquets réseau pour examiner les communications réseau.
- **FTK Imager** : Création d'images disque et analyse forensic.
- **Forensic Explorer** : Naviguer dans les fichiers de l'image, analyses de metadata etc...
- **https://exif.tools** : Outils en ligne permettant d'accéder au meta-données
- **Les bloqueurs d'écriture**
- **Kape** : Outils permettant de faire de la captures de log/artefacts ciblés (navigateur, registre etc..) pourrait s'aparenté à une extraction logique. Peut être utlisé quand on manque de matériel pour une extration logique rapide
- **JumpList Explorer** (permet de naviguer entre les informations des jumplists utilisateurs)

LES SYTÈMES D'EXPLOITATION

Certaines distributions linux contenant des outils dédié aux analyses forensics

- **Tsurugi**
- **Paladin**

TYPES DE PREUVES NUMÉRIQUES

1. **DISQUES DURS INTERNES ET PARTITIONS** :
   - Analyse des systèmes de fichiers (FAT32, NTFS, ext4).
   - Recherche de fichiers supprimés ou cachés.
   - Exemple d'outil : `testdisk` pour récupérer des partitions perdues.
2. **MÉMOIRE VIVE (RAM)** :
   - Extraction d'informations volatiles comme les processus en cours ou les clés de chiffrement.
   - Utilisation d'outils comme Volatility.
3. **MÉDIAS AMOVIBLES** :
   - Clés USB, cartes SD, disques externes ou internes
   - Vérification des métadonnées et récupération des fichiers supprimés.

COMMANDES UTILES EN FORENSIC

CRÉATION D'IMAGE DISQUE

- `dd if=/dev/sdX of=/path/to/image.img bs=4M` : Crée une copie brute du disque.
- `dcfldd` : Version améliorée de dd avec génération automatique de hash.

Autres commandes utilse

- `vssadmin.exe list shadows /for=C:` permet de lister les Volumes Shadows Copy d'une machine windows

PRINCIPAUX ARTEFACTS WINDOWS

1- Base de registre
2- Shell link files (.lnk)
3- JumpLists
4- ThumbCaches
5- Volumes Shadow Copies (VSC/VSS)
6- Corbeille
7- Journaux des événements (EVTX)
8- SRUM (System Resource Usage Monitor)
9- Amcache
10- Prefetch
11- Navigateurs internet

Quelques Exemples de récoltes d'information sur l'extraction d'une image

- L'Amcache.hve est un fichier de registre Windows qui stocke des informations sur l'exécution des programmes (il peut contenir les noms et versions des applications exécutées, les chemins d'exécution des fichiers. Les horodatages de création et de dernière modification. Les hashs SHA-1 des fichiers exécutables. Ces informations persistent même après la suppression des applications, ce qui en fait un outil précieux pour retracer l'activité d'un système).

  Les amcaches se trouvent dans `C:\Windows\AppCompat\Programs\Amcache.hve`

  La commande pour extraire des données du hve est `.\AmcacheParser.exe -f C:\Users\Student\Desktop\Artefacts\Amcache\Amcache.hve --csv C:\Users\Student\Desktop\Artefacts\Amcache-out`

- Les thumbcaches sont des fichiers système Windows qui stockent des miniatures d'images, de vidéos et d'autres types de fichiers, permettant un affichage rapide des aperçus dans l'explorateur et pouvant conserver des traces de fichiers supprimés, ce qui en fait une source précieuse pour les investigations forensiques.

  On trouves dans `C:\Users$$Nom d'utilisateur]\AppData\Local\Microsoft\Windows\Explorer`

  L'outil ***thumbcaches viewer*** permets de les visualiser.

- Les "compounds" (ou fichiers composés) sont des fichiers qui contiennent d'autres fichiers ou structures de données intégrés. Un exemple courant est le format de fichier OLE (Object Linking and Embedding) utilisé par Microsoft Office. Ces fichiers peuvent contenir plusieurs types de données, comme du texte, des images, et des métadonnées, tous encapsulés dans une seule structure de fichier. L'analyse des compounds est importante en forensique car ils peuvent cacher des informations cruciales ou des preuves dans leurs structures complexes.

- Prefetch (il sert à enregistrer les librairies dont à besoin un programme en s'exécutant)

  Situé dans `%root\Windows\Prefetch`

  `PECmd.exe -d 'repertoire'` permet de voir le nombre d'exécution de l'application, la dernière exécution, date de création, modification etc..., enregistre les dates et certaines infos des huits dernières exécution de l'application.

- Corbeille (permet de voir certains des fichiers supprimé avec le SID de l'utilisateur)

  On trouve les infos dans \Root$Recycle.Bin (on aura deux identifiant le $I et le $R)

- Les EVTX (ce sont les journaux, les plus important sont les journeaux de sécurité systèmes et applications)

  Principalement dans `\Root\System32\winevt\Logs. Sur Forensic explorer, sur l'onglet *Artefacts* ensuite la partie *Log events* on peut importer les logs de l'image et naviguer dedans. On peut filtrer par code d'évenement bien connus pour windows, sur la partie EventID. Et sur EventData on peut rajouter un filtre sur une donnée pour plus de précision.

- Jumplist (Les Jump Lists sont une fonctionnalité de Windows introduite avec Windows 7, permettant aux utilisateurs d'accéder rapidement aux fichiers, dossiers et tâches récemment ou fréquemment utilisés associés à des applications spécifiques)

  `\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\` ou `\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations`

  Le logicel Jumplist explorer nous permet d'analyser ces jumplist et donc de voir certains fichiers/dossier qui ont été ouvert avec certaines applications. Ou de chercher une application par son ID.

Les répertoires pertinant à vérifier

`C:\Windows\System32\config\` : Ruches système (SAM, SOFTWARE, SECURITY, SYSTEM)
`C:\Users<UserName>\` : Ruches utilisateur (NTUSER.DAT, USRCLASS.dat)
`C:\Users<UserName>\AppData\Roaming\Microsoft\Windows\Recent\` : Fichiers .lnk
`C:\Users<UserName>\AppData\Local\Microsoft\Windows\Explorer\` : ThumbCache
`C:\Windows\System32\winevt\Logs\` : Journaux d'événements
`C:\Windows\System32\sru\SRUDB.dat` : SRUM
`C:\Windows\AppCompat\Programs\Amcache.hve` : Amcache
`C:\Windows\Prefetch\` : Fichiers Prefetch
`C:\$Recycle.Bin\` : Information sur les fichiers supprimés

RUCHE SOFTWARE

- **Software\Microsoft\Windows NT\Current Version** : Informations sur le système : nom du produit, version affichée, propriétaire enregistré, date et heure d'installation, répertoire système.
- **Software\Microsoft\Windows NT\Current Version\ProfileList** : SID des utilisateurs humains.
- **Software\Microsoft\Windows\Current Version\Uninstall** : Liste des applications installées (ex. version de VLC, présence du sous-système Linux).

- **Software\Microsoft\Windows Portable Devices** : Numéro de série des périphériques connectés (ex. PCULOCKER).
- **Software\Microsoft\Windows Search\VolumeInfoCache** : Lettre de lecteur et nom convivial (Friendly Name) des volumes.

RUCHE SYSTEM

- **System\ControlSet001\Control\ComputerName\ComputerName** : Nom de l'ordinateur.
- **System\ControlSet001\Control\TimeZoneInformation** : Fuseau horaire configuré sur l'appareil.
- **System\ControlSet001\Control\Windows** : Date et heure de la dernière extinction.

RUCHE SAM

- **SAM\SAM\Domains\Account\Users\Names** : Liste des utilisateurs créés et leurs RID ; vérification des utilisateurs supprimés.
- **SAM\SAM\Domains\Account\Users\RID Manager** : Informations hexadécimales : dernier logon réussi, dernier changement de mot de passe, création du compte, nombre de connexions.

RUCHE NTUSER

- **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs** : Liste des fichiers récemment ouverts (ex. fichiers MP3 ou TXT).
- **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavedMRU** : Liste des fichiers enregistrés récemment.
- **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU** : Dernières commandes exécutées via "Run".
- **NTUSER.DAT\Control Panel\Desktop** : Nom du fichier utilisé comme fond d'écran.

AUTRES ARTEFACTS WINDOWS

- **%USERPROFILE%\AppData Roaming Microsoft Windows Recent AutomaticDestinations/CustomDestinations** : JumpLists : historique des fichiers ouverts par application.
- **%SystemRoot%\System32\sru SRUDB.dat** : Informations sur l'utilisation des ressources système (SRUM).

Les datas des principaux navigateurs d'une image Windows:

L'historique de navigation (certains historiques, et favoris des navigateurs de rechercher peuvent être retrouvés. Les databases sqlite stocké sur l'image peuvent aussi être consultés.)

Sur Forensic explorer en accédant à l'onglet *Artefacts* sur la partie processus en déroulant on peut

afficher les processus liée au navigateur de recherches.

Ils se trouvent tous dans `C:\Users<UserName>\AppData`

- Microsoft Edge : `"/AppData/Local/Microsoft/Edge/User Data/Default/"`
- Firefox : `"/AppData/Roaming/Mozilla/Firefox/Profiles/"`
- Google 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/`

Quelques exemples de données:

- L'historique et les téléchargements : “places.sqlite” ou “History”
- Les favoris : "bookmarks.json" ou “Bookmarks”
- Les identifiants : “logins.json” ou “Login Data”
- Les auto-completion :
  - “formhistory.sqlite”
  - “Web Data”
  - "Shortcuts”
  - “Login Data”

Memory forensic (Volatility)

Volatility est un outils permettant d'analyser les dumps de ram.

Installation

Pour l'installer il faut cloner le repo github : `git clone https://github.com/volatilityfoundation/volatility3.git`

Utilisation

Installer les dépendances :

- `pip3 install -r requirements.txt`

Vérfier l'installation :

- `python3 vol.py -h`

Commandes de base

Attention certaines commandes peuvent changer selon votre version de volatility, ces commandes fonctionnent avec volatility 3, mais peuvent changées entre temps.

Lister les procéssus actifs :

- `python3 vol.py -f <dump_memoire> windows.pslist`

ou selon la version

- `volatility --profile=Win10x64 -f <chemin_vers_le_dump> pslist`

Extraire un processus suspect :

- `python3 vol.py -f <dump_memoire> windows.dumpfiles --pid <PID>`

Lister tous les fichiers présents ou référencés en mémoire :

- `python3 vol.py -f <dump_memoire> filescan`

Extraire un fichier du dump :

- `python3 vol.py -f dump.raw windows.dumpfiles --physaddr <offset>`