Forensic

- [Forensic] Volweb
- [Windows]
  - [Forensic] Artefacts
- [Linux]
  - [Forensic] Collecte de données
  - [Forensic] Artefacts
  - [Forensic] Montage d'une image
  - [Forensic] Récupération de masterkey LUKS dans la ram
- [Réseau]
  - [Forensic] TShark
  - [Forensic] Analyse IPs / domaines
  - [Forensic] NetworkMiner
  - [Forensic] A-Packets

[Forensic] Volweb

Introduction

Cet outil est une interface web (GUI) à Volatility 3 qui permet de faire de l'analyse de mémoire de manière plus conviviale qu'en CLI en volatility de manière traditionnelle.



Installation

Docker

Tout d'abord, clonez le dépôt de volweb :

```
git clone https://github.com/k1nd0ne/VolWeb
```

Faite une copie du **.env.example** puis remplacez localhost par votre IP pour être accessible sur le réseau :

```
cp .env.example .env
```

```
CSRF_TRUSTED_ORIGINS=http://<IP>:3000
```

Puis lancez la stack :

```
docker compose up -d
```

Vous pouvez désormais vous connecter sur l'interface**http://<IP>:3000** avec les identifiants **admin/password** ou **user/password** .

[Windows]

[Windows]

[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
```

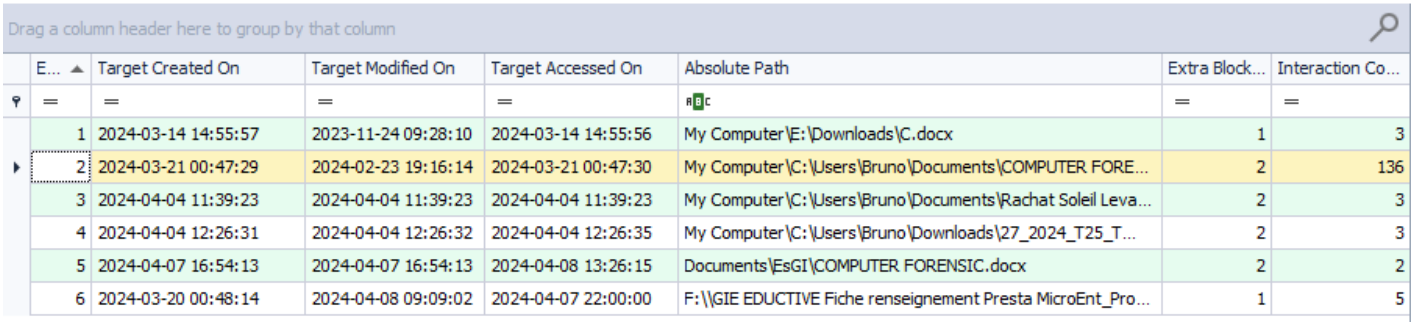
Jumplists

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

[Linux]

[Linux]

[Forensic] Collecte de données

Introduction

Avant votre analyse, il vous faudra collecter les données de votre disque ou votre périphérique. Vous pouvez effectuer une copie physique avec un bloqueur d'écriture de disque mais aussi lancer une distribution en live tel que **Tsurugi Linux** ou **Paladin Linux** pour monter les périphériques en lecture seule.

DD

```
sudo dd if=/dev/sdX of=tmp/myusb.raw bs=512M status=progress
```

Ou pour créer une image d'un système distant :

```
ssh root@192.168.122.33 "dd if=/dev/sda bs=512M" | dd of=/root/vm-debian.dd bs=512M
```

EWF Tools

Cette suite d'outils sur Linux permet de faire une copie bit à bit de votre périphérique au format E01.

Pour cela, lancez **ewfacquire** :

```
ewfacquire /dev/sd<X>
```

> Tout un tas de question vous sera posé. Laissez par défaut pour la plupart mais faite en sorte de n'avoir qu'un seul segment si possible (c'est plus pratique après pour ne pas à avoir à gérer plusieurs fichiers).

Vous pouvez afficher les informations de votre nouveau conteneur :

```
ewfinfo myusb.E01
```

Vous pouvez aussi vérifier l'intégrité de votre conteneur :

```
ewfverify myusb.E01
```

[Linux]

[Forensic] Artefacts

Introduction

De nombreux artefacts sont consultables sur les systèmes Linux pour effectuer une analyse forensique.

```
remnux@remnux:~$ cat /etc/os-release
NAME="Ubuntu"
VERSION="14.04.2 LTS, Trusty Tahr"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 14.04.2 LTS"
VERSION_ID="14.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
```

Artefacts

Liste d'artefacts

Artefacts	Descriptions
/etc/*-release	Informations sur l'OS et les numéros de version
/etc/issue	Informations sur l'OS et les numéros de version
/etc/issue.net	Informations sur l'OS et les numéros de version
/etc/timezone	Fuseau horaire
/etc/localtime	Fuseau horaire

/etc/passwd	Comptes utilisateurs
/etc/group	Groupes et membres
/etc/shadow	Mots de passe hashés des comptes utilisateurs
/etc/sudoers | /etc/sudoers.d	Politiques sudo
/etc/fstab	Points de montages automatiques
/etc/hostname	Nom d'hôte de la machine
/etc/hosts	Résolution des noms de domaine
/etc/network/interfaces	Configuration réseau
/etc/resolv.conf	Configuration DNS
/var/lib/networkmanager/internal	Dernière IP attribuée au système
/var/lib/networkmanager/NetworkManager.state	Etat actuel du réseau, du wifi et de l'accès à internet sur le système
/var/lib/networkmanager/seen-bssids	Enregistre les BSSID wifi vus, mais pas nécessairement connectés
/var/lib/networkmanager/timestamps	Enregistre les baux DHCP
/var/lib/dpkg/status	Journaux d'évènements du gestionnaire de paquets DPKG (Debian / Ubuntu)
/var/lib/dpkg/status	Journaux d'évènements du gestionnaire de paquets RPM (Redhat)
/var/lib/pacman/local	Journaux d'évènements du gestionnaire de paquets PACMAN (Arch Linux)
/var/log/apt/history.log	Journaux d'évènements de ce qui a été installé avec le gestionnaire de paquets APT (Debian / Ubuntu)
/var/log/apt/term.log	Enregistre les sorties de terminal des commandes d'installations avec APT (Debian / Ubuntu)
/var/log/yum.log*	Contient les dates d'installation des paquets (Redhat)
/var/log/dnf.log*	Contient les dates d'installation des paquets dans un format difficile à lire (Redhat)

/var/log/dpkg.log*	Journaux d'évènements pour les paquets installés manuellement avec le gestionnaire de paquets DPKG (Debian / Ubuntu)
/var/log/auth.log	Connexions utilisateurs.
/var/log/btmp	Connexions échouées des utilisateurs.
/var/log/faillog	Connexions échouées des utilisateurs.
/var/log/dmesg	Périphériques matériels détectés par le kernel au démarrage.
/var/log/journal/*	Logs systèmes et services (remplaçant de syslog)
/var/log/lastlog	Dernières connexions pour chaque utilisateur.
/var/log/syslog	Logs systèmes et services.
/var/log/wtmp | /var/log/utmp	Connexions réussies des utilisateurs.

Date d'installation du système

La méthode la plus sûre est de chercher la date de création du système de fichiers, en utilisant la commande suivante pour **EXT4** :

```
tune2fs –l /dev/sdb2 | grep -i "created"
```

Et la commande suivante pour **BTRFS** :

```
btrfs subvol show /mnt/evidence/| grep -i "creation time"
```

Dernières extinctions

```
last -f /var/log/wtmp | grep shutdown
```

$PATH

Le $PATH contient les chemins vers tous les binaires exécutables. Vous pouvez afficher les chemins (*chroot* requis) :

```
echo $PATH
```

Vous pouvez aussi récupérer tous les binaires (applications), avec la commande suivante (*chroot* requis) :

```
for i in $(echo $PATH | tr -s ":" "\n"); do find $i/ -type f; done > apps.txt
```

Démarrages automatiques

Systemd

Vous pouvez consulter tous les fichiers **.service** ou **.target** ou **.socket** contenus dans les répertoires suivants :

- **/etc/systemd/system/**
- **/usr/lib/systemd/system**
- **/lib/systemd/system/**

> Vous pouvez consulter les logs systemd dans le fichier **/var/log/syslog** .

Init

Sur les vieux systèmes, init était utilisé et non systemd. Les scripts exécutés au démarrage avec init sont situés dans **/etc/init.d** .

Cron

Les tâches crontab peuvent être vérifiées dans les répertoires suivants :

- **/etc/crontab/**
- **/var/spool/cron/crontabs/**

De plus, les tâches propres aux utilisateurs peuvent être consultées avec la commande suivante (*chroot* requis) :

```
crontab -l
```

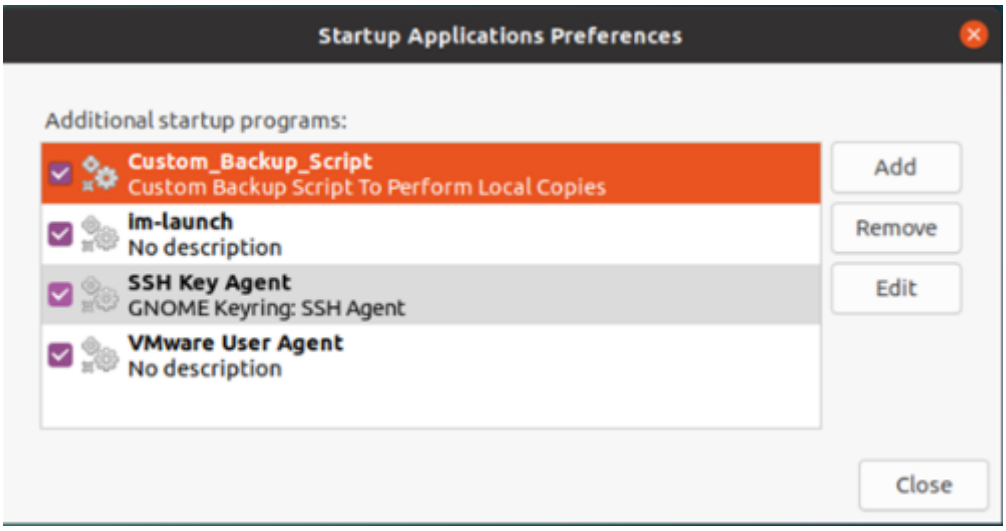
Profils shells

Ces fichiers de profil sont en réalité des scripts bash qui s'exécutent au démarrage de la session de l'utilisateur, ils sont exécutés dans l'ordre suivant :

- **/etc/profile**
- **~/.bash_profile**
- **~/.bash_login**
- **~/.profile**

GUI Startup Manager

Sur les environnements de bureau traditionnels (Gnome, KDE, XFCE), il est possible de configurer des applications de démarrage :



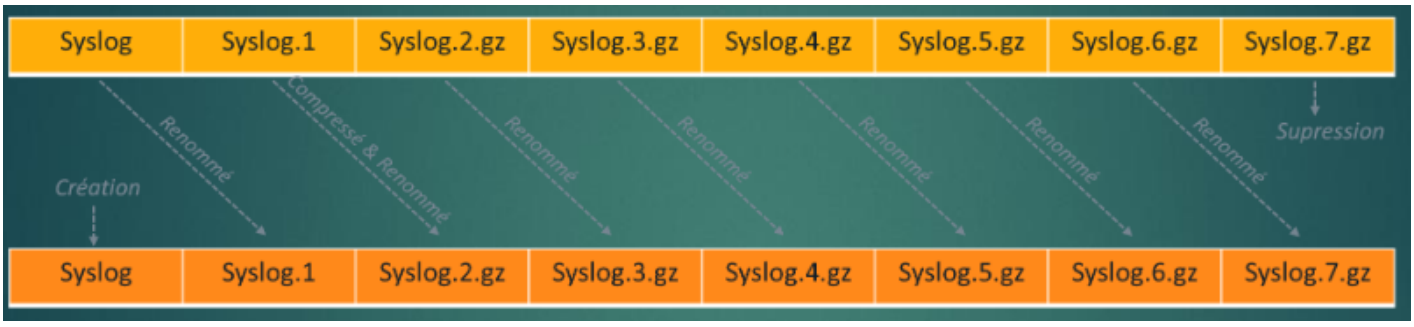
> Vous pouvez les retrouver à l'emplacement **~/.config/autostart/** .

Logrotate

La configuration de Logrotate est disponible via le fichier **/etc/logrotate.conf** ou dans le dossier **/etc/logrotate.d/** . Voici la configuration par défaut :

- weekly : rotation hebdomadaire.
- rotate 4 : conserve 4 cycle de rotation.
- create : un nouveau fichier vide après chaque rotation.

Voici un schéma explicatif du fonctionnement de Logrotate :



> Une tâche cron exécute quotidiennement logrotate, celle-ci est disponible à cet emplacement **/etc/cron.daily/logrotate** .

>

> Les status et horodatages des rotations sont disponible à cet emplacement **/var/lib/logrotate/status** .

Journaux d'évènements

> Les logs au format texte sont en train d'être remplacés par des fichiers de base de données sur les systèmes Linux, ce qui les rend plus difficile à consulter.

Vous pouvez afficher les logins réussis avec l'horodatage pour les utilisateurs du système avec la commande suivante :

```
lastlog |pr -2 -t -s | column -t
```

Vous pouvez afficher les dernières connexions de l'utilisateur courant avec la commande suivante :

```
last -F
```

Vous pouvez consulter les logs d'un système distant avec **journalctl** :

```
journalctl --directory=/mnt/evidence/var/log/journal
```

Voici quelques options pour journalctl :

Commandes	Descriptions
journalctl -o short	Affichage de l'horodatage par défaut [ex: Aug 03 02:43:12]
journalctl -o short-full	Affichage de l'horodatage au format ANSI [ex: Wed 2022-08-03 02:43:12]
journalctl -o short-iso	Affichage de l'horodatage au format ISO [ex:2022-08-03T02:43:12-0700]
journalctl -o short-unix	Affichage de l'horodatage au format Integer [ex: 1659519792.935000]
journalctl -o verbose	Affiche le détail complets des champs
journalctl --no-hostname	Enlève le champ du nom d'hôte pour améliorer la lisibilité
journalctl -a	Affiche l'ensemble des champs des journaux
journalctl -r	Affiche les logs en sens inverse
journalctl --list-boots	Liste les démarrages
journalctl -u <SERVICE>.service	Information sur un service
journalctl _UID=<UID>	Informations sur l'utilisateur (avec son id)
journalctl -k | grep -i USB	Informations kernel sur les périphériques USB

Home

Les répertoires homes des utilisateurs contiennent généralement les artefacts les plus intéressants. Par défaut ils sont situés dans :

- **/home/<USER>** : Pour les utilisateurs
- **/root** : Pour le compte root

Voici des artefacts contenus dans les répertoires home qui pourraient vous intéresser :

Artefacts	Descriptions
.bashrc	Script exécuté à chaque nouvelle session shell. Il contient généralement les configuration du shell, des fonctions, des variables et les alias.
.bash_logout	Script exécuté à chaque fermeture du shell.

Bash_history

Ce fichier est présent dans le home de l'utilisateur et stocke les commande exécutées par celui-ci.

Voici quelques éléments à prendre en considération:

- Il n’enregistre pas les horodatages par défaut (**$HISTTIMEFORMAT**).
- Il peut être manipulé / modifié / supprimé.
- Il ne contient pas les commandes des shells en cours.
- Il peut être situé n’importe ou sur le système (**$HISTFILE**).
- En ajoutant un espace devant la commande, la commande n'est pas enregistrée (**$HISTCONTROL**).
- Le fichier a une taille maximum et un nombre de ligne limité. (**$HISTFILESIZE**) et (**$HISTSIZE**).

Éléments récents

Sur un système avec un environnement de bureau, vous pouvez retrouver l'équivalent des jumplists pour windows via le fichier **~/.local/share/recently-used.xbel** :



Il s'agit d'un fichier “xml” contenant le nom des fichiers accédés avec l'interface graphique. Il inclue d'importantes informations telles que :

- Le nom du programme.
- La date et heure.
- L'emplacement et le nom du fichier.

Corbeille

Sur un système avec un environnement de bureau, vous pouvez retrouver la corbeille à l'emplacement **~/.local/share/Trash** . Cependant, seulement les fichiers supprimés avec l'interface graphique seront présents.

Deux sous répertoires sont à étudier :

- **files/** : Contenant le fichier original.
- **info/** : Contenant les informations de suppression (date et chemin).

Navigateurs internet

Voici les emplacements des profiles utilisateurs selon les navigateurs :

Navigateur	Chemin
Firefox	~/.mozilla/Firefox/
Chrome	~/.config/google-chrome/
Opera	~/.config/opera/
Vivaldi	~/.config/vivaldi/

Timeline

Pour générer une timeline sur les évènements passés sur un système de fichiers, plusieurs solutions s'offrent à vous :

- La super timeline plaso avec **log2timeline** (lente à générer mais très performante).
- La timeline de **sleuthkit** (rapide à générer).

Sleuthkit

Pour générer une timeline avec sleuthkit, commencez par créer un bodyfile :

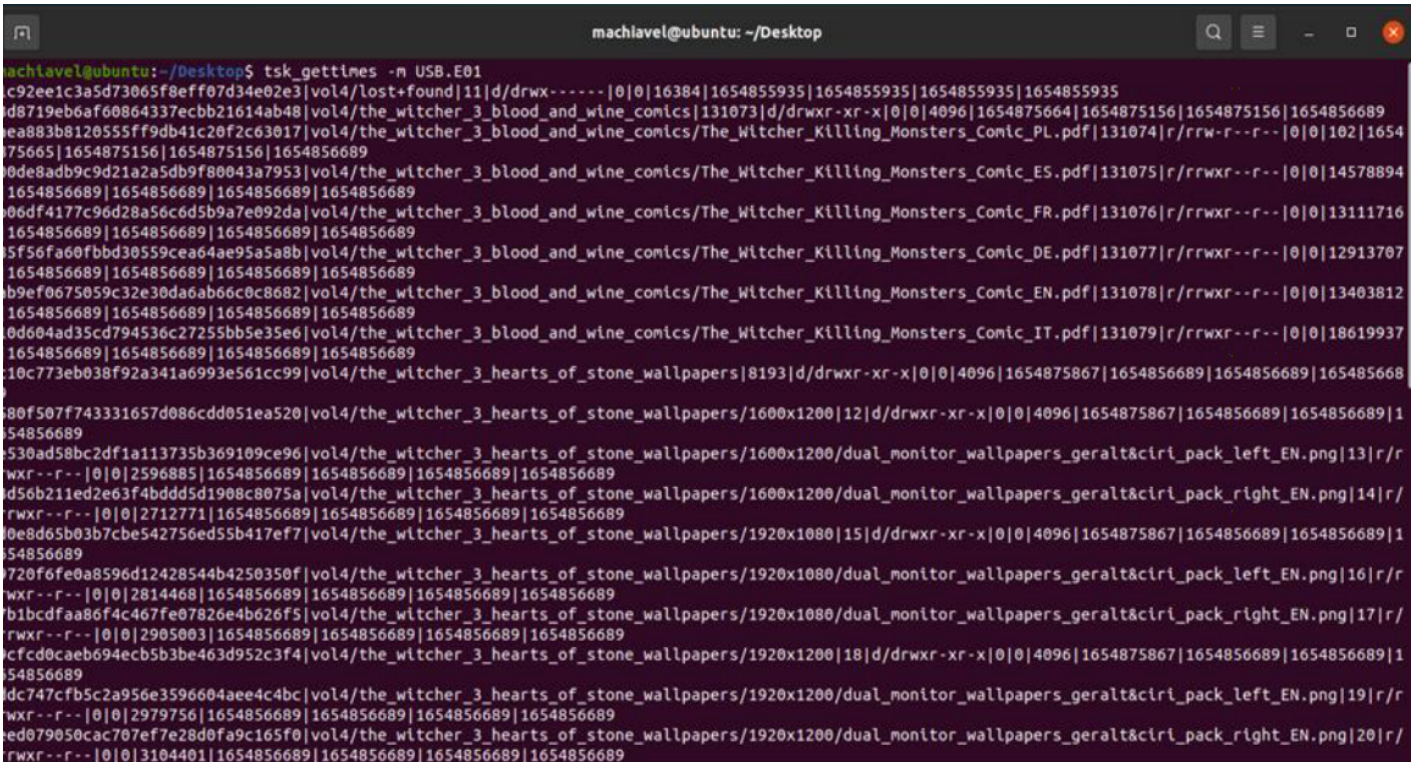
```
tsk_gettimes -m image.E01 > bodyfile
```

Chaque ligne contient les informations suivantes :
MD5|nom|inode|mode_en_chaîne|UID|GID|taille|atime|mtime|ctime|crtime .

Voici le détail des informations :

- **MD5** : MD5 du fichier.
- **nom** : Chemin complet du fichier.
- **inode** : Identifiant unique du fichier dans le système de fichiers.
- **mode** : Permissions UNIX.
- **UID** : Identifiant de l'utilisateur propriétaire du fichier.
- **GID** : Identifiant du groupe propriétaire du fichier.
- **taille** : Taille du fichier.
- **atime** : Heure du dernier accès au fichier.
- **mtime** : Heure de la dernière modification du fichier.
- **ctime** : Heure du dernier changement de métadonnée du fichier.
- **crtime** : Heure de création du fichier.

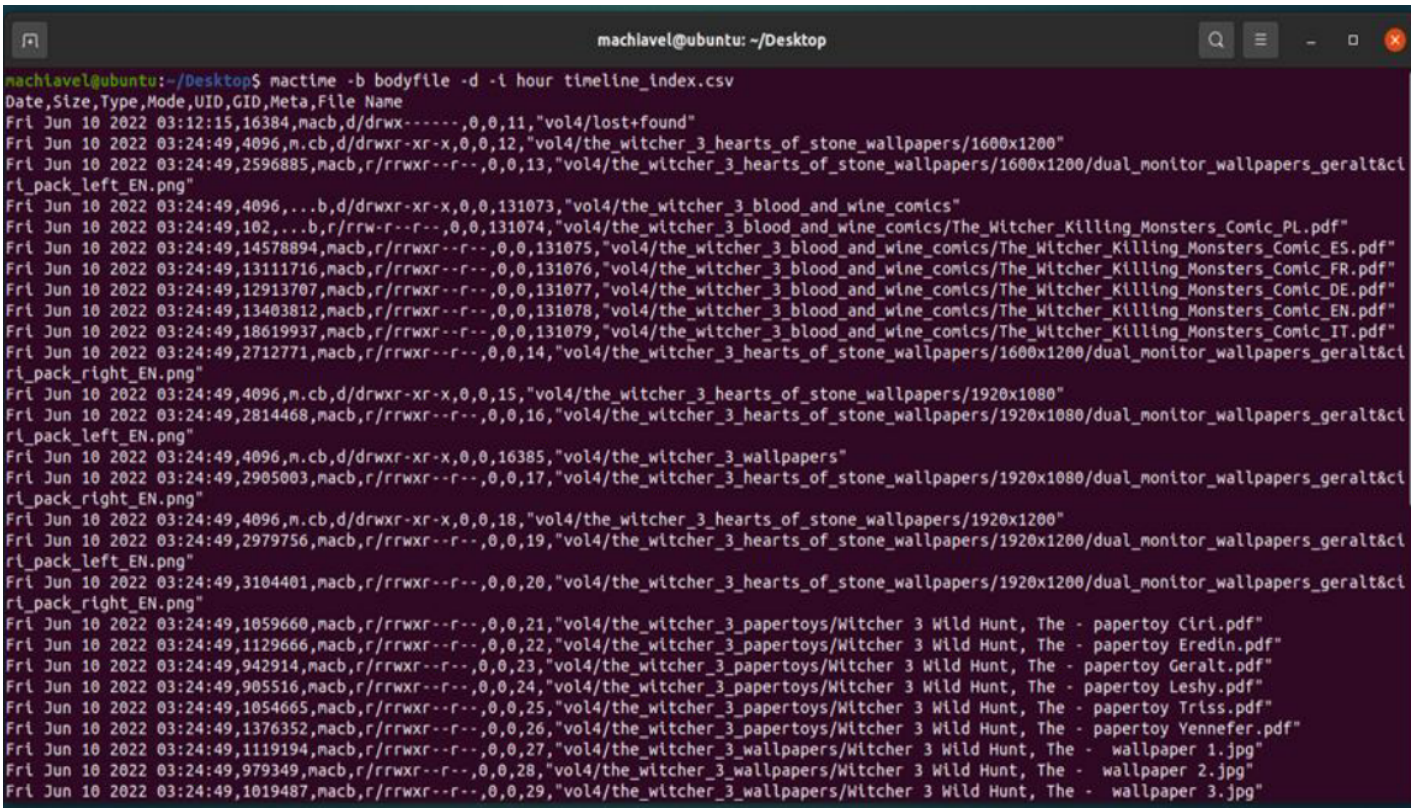
Voici un exemple de ce à quoi ressemble le bodyfile :



Ensuite, il vous faut convertir votre timeline en CSV :

```
mactime -b bodyfile > timeline.csv
```

Voici à quoi ressemble le fichier CSV généré :



Plaso

Tout d'abord créez votre bodyfile :

```
log2timeline.py --storage_file <bodyfile> <image.E01>
```

> Le fichier de sortie est une base de donnée SQLite.

Puis transformez votre bodyfile en timeline :

```
psort -w <timeline> <bodyfile>
```

Visualiseurs

Une fois la timeline générée, il faut utiliser des outils de visualisation pour effectuer une analyse. Pour cela, vous pouvez utiliser :

- **Timesketch** (https://timesketch.org/)
- **Timeline Explorer** (Eric Zimmerman)
- **Glogg** (http://glogg.bonnefon.org/index.html)

[Linux]

[Forensic] Montage d'une image

Introduction

Pour effectuer votre analyse sous Linux, vous aurez besoin d'outils. Vous allez voir comment monter des conteneurs au format E01 (inclus Windows et Linux) et des images faites avec dd.

Manuel

Conteneur EWF (E01)

Tout d'abord, utilisez ewfmount pour monter le disque (installez **ewftools** au préalable) :

```
sudo ewfmount 'windows_or_linux_container.E01' /mnt/ewf/
```

> Cette opération aura pour conséquence de monter le disque dans **/mnt/ewf**, vous pourrez ensuite monter les partitions une à une.

Vous pouvez analyser les partitions avce **fdisk** et relevez à quel secteur commence votre partition pour calculer l'offset :

```
sudo fdisk -l /mnt/ewf/ewf1
```

Utilisez **mount** en saisissant le secteur de début multiplié par la taille de secteur (souvent 512) :

```
sudo mount -o ro,norecovery,offset=$((512*239616)) /mnt/ewf/ewf1 /mnt/evidence/
```

> Cette commande aura pour effet de monter la partition dans **/mnt/evidence** en lecture seule.

Si vous souhaitez utiliser **xmount** pour définir un fichier de cache :

```
sudo xmount --in ewf 'windows.E01' --cache cache.cc --out /mnt/evidence/
```

Si vous souhaitez utiliser **xmount** pour créer un vmdk (VMware) à partir du conteneur :

```
sudo xmount --in ewf 'windows.E01' --cache cache.cc --out vmdk /mnt/c/Users/Elie/Documents/VM/
```

Image DD

Pour monter une image faite avec DD avec une partition de loopback, on peut utiliser **losetup** :

```
sudo losetup -f -P '/media/ewf/Alienware.dd'
```

Pour détacher le périphérique :

```
sudo losetup -d /dev/loop0
```

[Linux]

[Forensic] Récupération de masterkey LUKS dans la ram

Introduction

Cette page présente une méthode pour obtenir une clé de récupération d'une partition chiffrée LUKS (systèmes Linux) à partir de la RAM.

Manuel

Tout d'abord utilisez aeskeyfind pour extraire toutes les clés AES 128 et 256 de l'image de la ram :

```
aeskeyfind 'Kali_5.18.0-kali5-amd64.dmp' > all-aes-keys.txt
```

> Retirez les clés AES 128 bits car seules les clés AES 256 bits sont intéressantes (juxtaposition de deux clés 256 pour faire une clé 512 qui correspond à la taille d'une clé LUKS).

Inversez le sens des clés :

```
tac 'all-aes-keys.txt' | tr -d "\n" | fold -w 128 > KEYS.txt
```

Mettez chaque combinaison de clés dans un fichier MK (MasterKey) :

```
k=1 ; while read i ; do echo $i | xxd -r -p > ./MK$k ; k=$(($k+1)); done < KEYS.txt
```

Testez chaque possible MasterKey sur la partition chiffrée :

```
for i in MK* ; do sudo cryptsetup luksAddKey --master-key-file=$i /dev/loop0p3 ; done
```

> Vous pouvez **echo MK$i** pour afficher le fichier testé.

Puis déverrouillez la partition :

```
sudo cryptsetup luksOpen /dev/loop0p3 BIM
```

[Réseau]

[Réseau]

[Forensic] TShark

Introduction

Cet outil permet d'analyser en ligne de commande des fichiers PCAP un peu à la manière de Wireshark. L'avantage est que vous pouvez utiliser les avantages de bash pour filtrer et effectuer des opérations avancées assez simplement.



Cheat-sheet

IPs connexions sortantes TCP

Si vous souhaitez récupérer les IPs des connexions sortantes TCP en excluant les IPs privées et les IPs appartenant à Akaimai (connexions microsoft légitimes), vous pouvez utiliser la commande suivante :

```
tshark -r 2024-11-26-traffic-analysis-exercise.pcap -T fields -e ip.dst -Y "tcp" | sort -u | grep -Ev "^(10\.|172\.(1[6-9]|2[0-9]|3[0-1])\.|192\.168\.)" | while read ip; do nslookup "$ip" | grep -qi "akamaitechnologies.com" || echo "$ip"; done
```

> Vous pouvez remplacer l'argument -Y "tcp" par **-Y "http"** si vous souhaitez uniquement les connexions HTTP.

IPs connexions entrantes TCP

```
tshark -r 2024-11-26-traffic-analysis-exercise.pcap -T fields -e ip.src -Y "tcp" | grep -E "^(10\.|172\.(1[6-9]|2[0-9]|3[0-1])\.|192\.168\.)" | sort -u
```

> Vous pouvez remplacer l'argument -Y "tcp" par **-Y "http"** si vous souhaitez uniquement les connexions HTTP.

Connexions DNS

```
tshark -r 2024-11-26-traffic-analysis-exercise.pcap -Y "dns.qry.name" -T fields -e dns.qry.name | sort -u
```

Ports de connexion

Pour regarder les ports TCP les plus utilisés :

```
tshark -r 2024-11-26-traffic-analysis-exercise.pcap -T fields -e ip.src -e ip.dst -e tcp.dstport -Y "tcp" | sort -u
```

Pour filtrer selon certains ports spécifiques :

```
tshark -r 2024-11-26-traffic-analysis-exercise.pcap -T fields -e ip.src -e ip.dst -e tcp.dstport -Y "tcp" | sort -u | grep -iE "\s80|\s443|\s88|\s3389\s445"
```

Extraire les fichiers

Pour récupérer tous les fichiers ayant transités via **HTTP** et supprimer les fichiers sans extension (faux-positifs) :

```
tshark -r 2024-11-26-traffic-analysis-exercise.pcap --export-objects "http,extracted_files" && find extracted_files -type f ! -name "*.*" -delete
```

> Les fichiers seront disponibles dans le répertoire ./extracted_files

Scanning

Pour détecter un scan de ports, vous pouvez observer s'il y a un multitude de connexions SYN :

```
tshark -r 2024-11-26-traffic-analysis-exercise.pcap -Y "tcp.flags.syn == 1 and tcp.flags.ack == 0" -T fields -e ip.src -e tcp.dstport | sort | uniq -c | sort -nr | head -20
```

Trouver les fichiers ayant transités par SMB

```
tshark -r 2024-11-26-traffic-analysis-exercise.pcap -Y "smb2" -T fields -e smb2.filename | sort -u
```

> Vous trouverez aussi des registres modifiés via SMB !

Trouver les fichiers ayant transités par FTP

```
tshark -r 2024-11-26-traffic-analysis-exercise.pcap -Y "ftp.request.command" -T fields -e ftp.request.command -e ftp.request.arg | sort -u
```

Headers HTTP liés à une IP

```
tshark -r 2024-11-26-traffic-analysis-exercise.pcap -Y "ip.src == 194.180.191.64 || ip.dst == 194.180.191.64 && http" -V | grep -E "^[[:space:]]+[A-Za-z-]+:"  | sed '/^[[:space:]]*Host/i\'$'\n'
```

Extraire les mots de passe en clair

```
tshark -r fichier.pcap -Y 'http.authbasic' -T fields -e http.authorization
```

```
tshark -r fichier.pcap -Y 'ftp.request.command == "USER" or ftp.request.command == "PASS"' -T fields -e ftp.request.arg
```

```
tshark -r fichier.pcap -Y 'telnet' -T fields -e telnet.data
```

> Pour extraire des secrets, **NetworkMiner** semble plus performant.

[Réseau]

[Forensic] Analyse IPs / domaines

Introduction

Lors de l'analyse de vos trames, il vous sera utile d'identifier les IPs et les domaines notamment pour déterminer s'ils sont malveillants et s'il s'agit d'un serveur de l'attaquant.



Cheat-sheet

Trouver le provider d'une IP

```
whois <IP> | grep -i "orgname" | cut -f2 -d':' | sed 's/^[[:space:]]*//'
```

Retirer les IPs selon le provider

```
cat ips.txt | while read ip; do if ! whois "$ip" | grep -iE "orgname|role" | grep -iq "microsoft"; then echo "$ip"; fi; done
```

> Vous pouvez filtrer sur **Microsoft** mais aussi **Akamai** ou **Cloudflare** en modifiant le grep. Cela retirera ces IPs de la liste.

> Vous pouvez remplacer le *cat ips.txt* par une commande **tshark** ou autre, cela fonctionnera parfaitement.

Analyse virustotal

Pour analyser une IP :

```
curl -s -X GET "https://www.virustotal.com/api/v3/ip_addresses/194.180.191.64" -H "x-apikey: API_KEY" | jq '.data.attributes.last_analysis_stats'
```

Pour analyser plusieurs IPs :

```
cat ips.txt| while read -r ip; do curl -s -X GET "https://www.virustotal.com/api/v3/ip_addresses/$ip" -H "x-apikey: 1e04da01b0aa70136ef46bfdf8302db049d5dbc78c9bd0f0a6f8cdf59597b6e7" | jq -r --arg ip "$ip" '"\($ip): \(.data.attributes.last_analysis_stats.malicious)"'; done
```

[Réseau]

[Forensic] NetworkMiner

Introduction

Le logiciel **NetworkMiner** est disponible sur Windows et Linux pour analyser les fichiers PCAP. Il permet notamment d'afficher des informations comme les fichiers échangés, les secrets ou autre à travers des sous-menus.



Installation

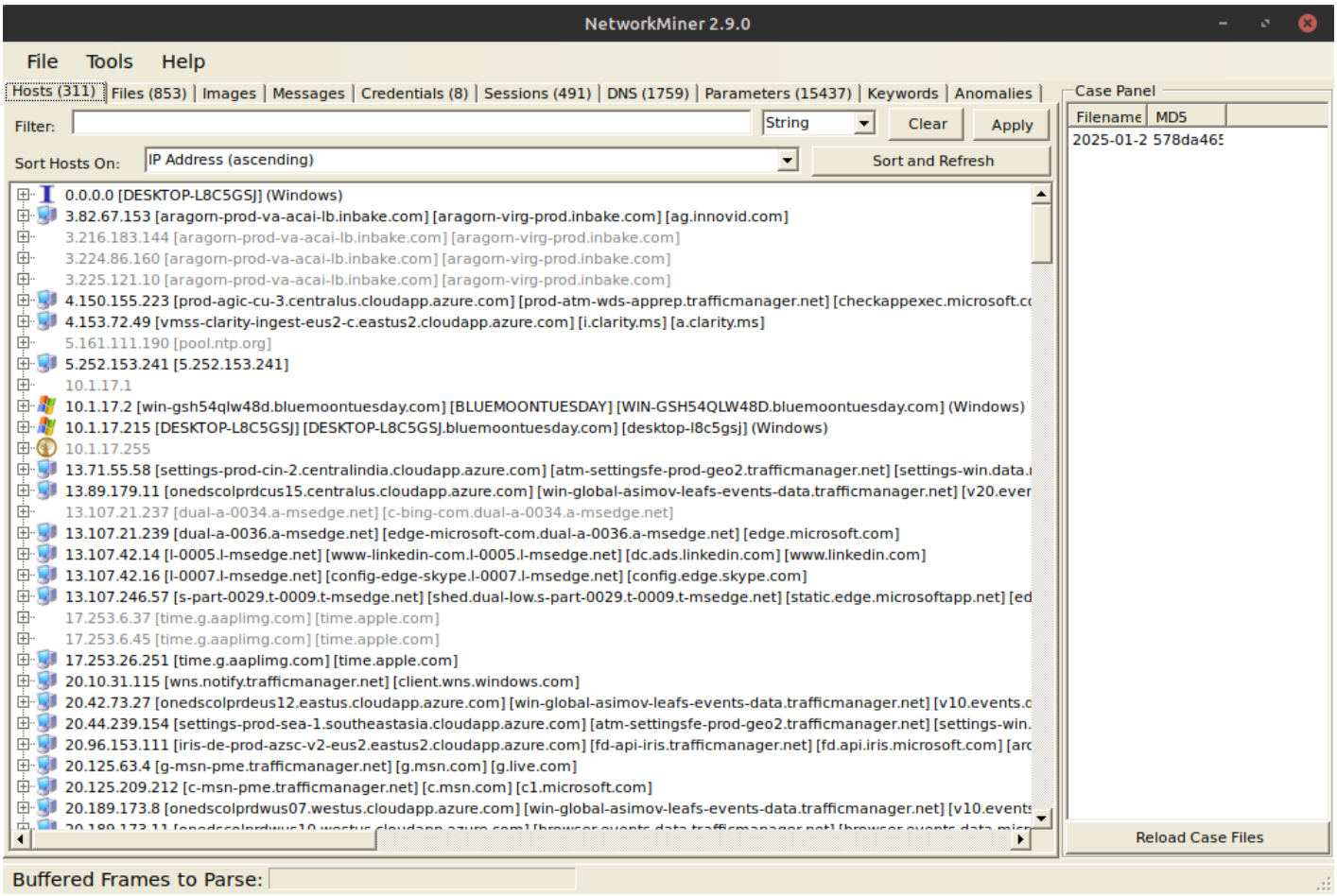
Debian

```
sudo apt install mono-devel && wget https://www.netresec.com/?download=NetworkMiner -O /tmp/nm.zip && sudo unzip /tmp/nm.zip -d /opt/ && cd /opt/NetworkMiner* && sudo chmod +x NetworkMiner.exe && sudo chmod -R go+w AssembledFiles/ && sudo chmod -R go+w Captures/
```

Puis lancez NetworkMiner :

```
cd /opt/NetworkMiner* && mono NetworkMiner.exe --noupdatecheck
```

Interface

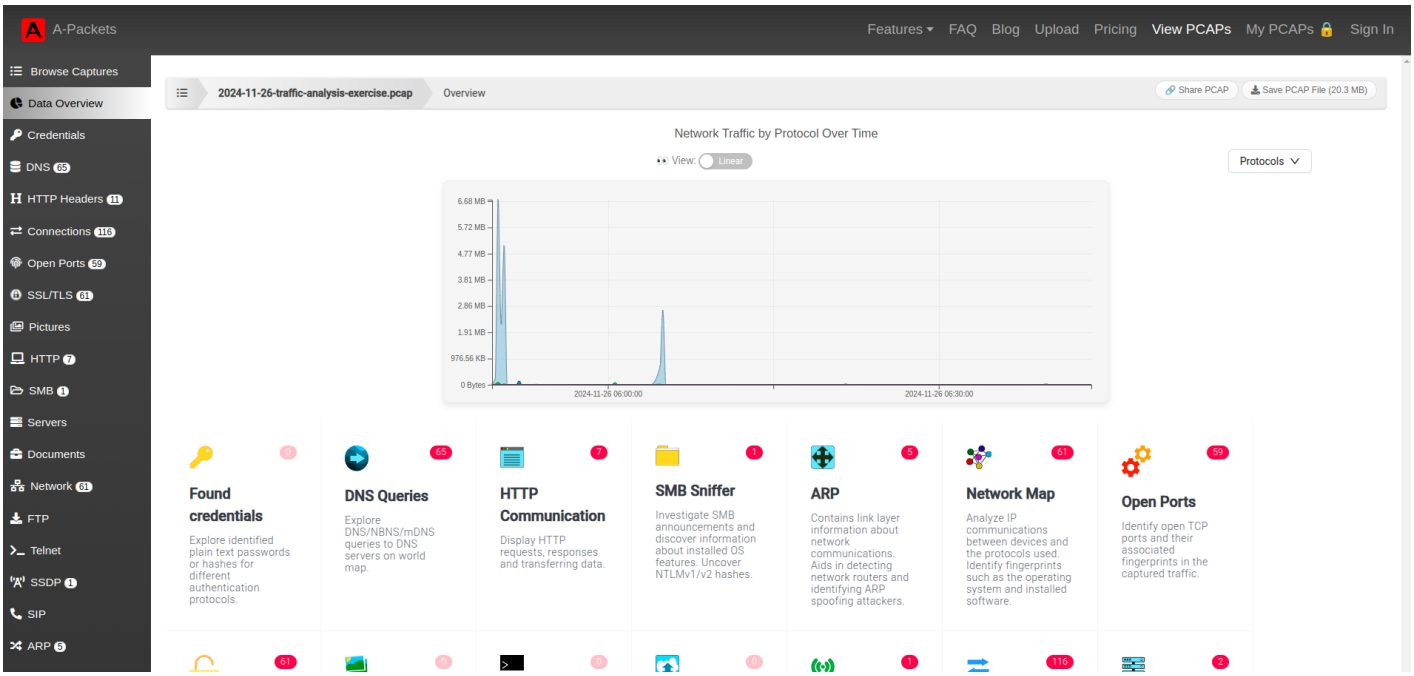


[Réseau]

[Forensic] A-Packets

Introduction

L'outil en ligne **A-Packets** permet d'analyser des fichiers PCAP de moins de **25Mo**. La navigation pour trouver des indicateurs de compromission est très pratique et peut faire gagner énormément de temps pour une investigation contrairement à des outils comme Wireshark.



Lien

- https://apackets.com/