

# [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 à la place de 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

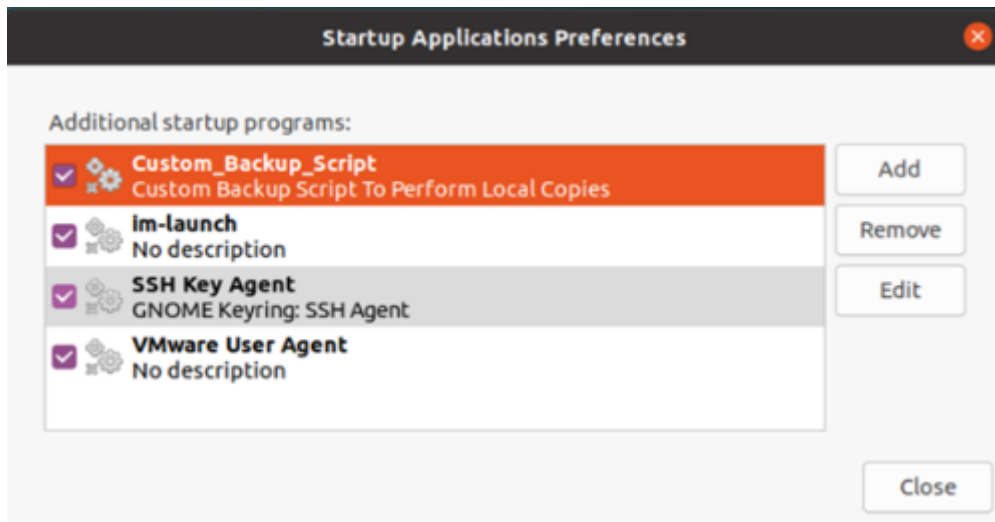
Ces fichiers de profil sont en réalité des scripts bash qui s'exécutent au démarrage de la session de l'utilisateur, ils sont exécutés dans l'ordre suivant :

- **/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 :



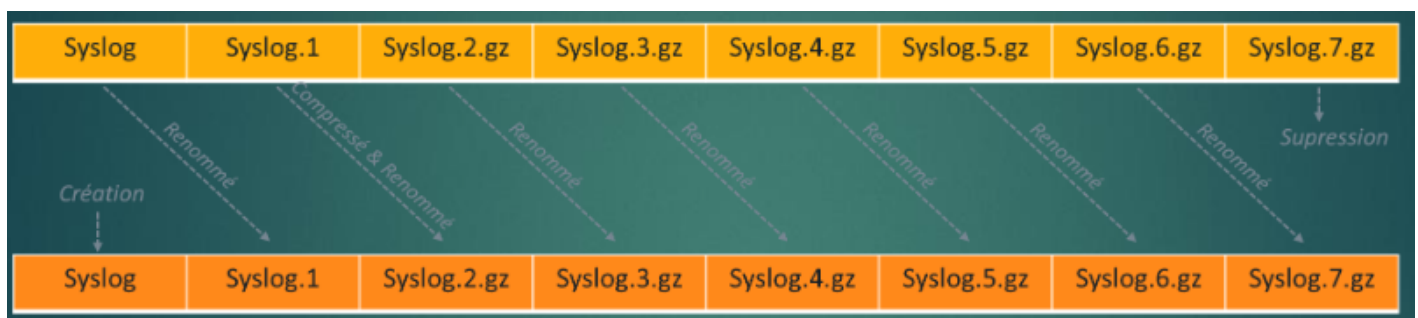
Vous pouvez les retrouver à l'emplacement ~/.config/autostart/ .

## 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 la 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 commandes 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 où 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** :

```
<bookmark href="file:///home/nachivel/Downloads/virtualbox-6.1_6.1.34-150636.1-Ubuntu-jammy_and64.deb" added="2022-06-10T09:56:40Z" modified="2022-06-10T09:56:40Z"
visited="1969-12-31T23:59:59Z">
  <info>
    <metadata owner="http://freedesktop.org">
      <mime:mime-type type="application/vnd.debian.binary-package"/>
      <bookmark:applications>
        <bookmark:application name="Firefox" exec="&apos;firefox %u&apos;" modified="2022-06-10T09:56:40Z" count="1"/>
      </bookmark:applications>
    </metadata>
  </info>
</bookmark>
```

Il s'agit d'un fichier "xml" contenant le nom des fichiers accédés avec l'interface graphique. Il inclut 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 profils 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 :

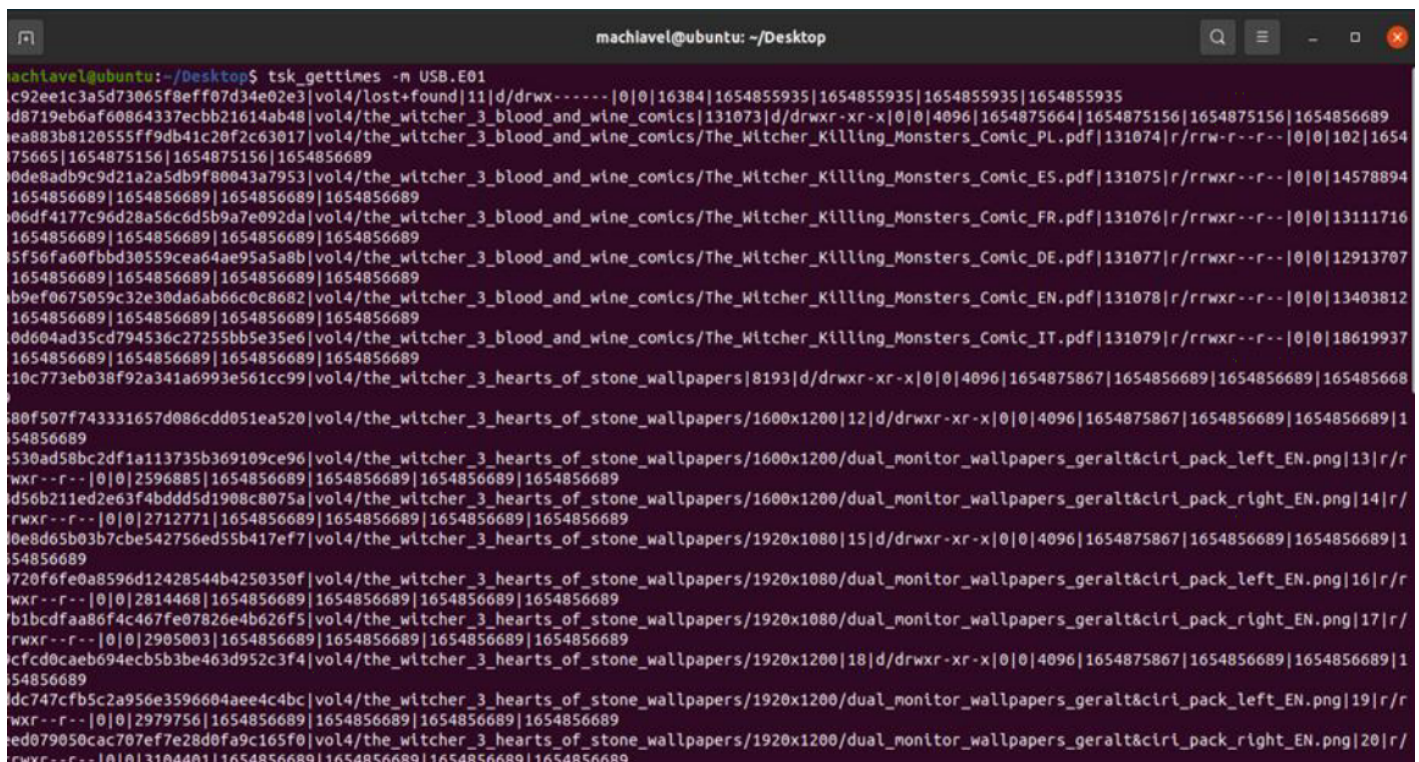
**MD5|nom|inode|mode\_en\_chaine|UID|GID|taille|atime|mtime|ctime|crtme .**

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 :



```

machlavel@ubuntu: ~/Desktop
machlavel@ubuntu:~/Desktop$ tsk_gettimes -n USB.E01
c92ee1c3a5d73065f8eff07d34e02e3|vol4/lost+found|11|d|drwx-----|0|0|16384|1654855935|1654855935|1654855935|1654855935
d8719eb6af60864337ecbb21614ab48|vol4/the_witcher_3_blood_and_wine_comics|131073|d|drwxr-xr-x|0|0|4096|1654875156|1654875156|1654856689
ea883b8120555ff9db41c20f2c63017|vol4/the_witcher_3_blood_and_wine_comics/The_Witcher_Killing_Monsters_Comic_PL.pdf|131074|r|rrw-r--r--|0|0|102|1654
75665|1654875156|1654875156|1654856689
0de8adb9c9d21a2a5db9f80043a7953|vol4/the_witcher_3_blood_and_wine_comics/The_Witcher_Killing_Monsters_Comic_ES.pdf|131075|r|rrwxr--r--|0|0|14578894
1654856689|1654856689|1654856689|1654856689
06df4177c96d28a56c6d5b9a7e092da|vol4/the_witcher_3_blood_and_wine_comics/The_Witcher_Killing_Monsters_Comic_FR.pdf|131076|r|rrwxr--r--|0|0|13111716
1654856689|1654856689|1654856689|1654856689
5f56fa60fbbd30559cea64ae95a5a8b|vol4/the_witcher_3_blood_and_wine_comics/The_Witcher_Killing_Monsters_Comic_DE.pdf|131077|r|rrwxr--r--|0|0|12913707
1654856689|1654856689|1654856689|1654856689
b9ef0675059c32e30da6ab66c0c8682|vol4/the_witcher_3_blood_and_wine_comics/The_Witcher_Killing_Monsters_Comic_EN.pdf|131078|r|rrwxr--r--|0|0|13403812
1654856689|1654856689|1654856689|1654856689
0d604ad35cd794536c27255bb5e35e6|vol4/the_witcher_3_blood_and_wine_comics/The_Witcher_Killing_Monsters_Comic_IT.pdf|131079|r|rrwxr--r--|0|0|18619937
1654856689|1654856689|1654856689|1654856689
10c773eb038f92a341a6993e561cc99|vol4/the_witcher_3_hearts_of_stone_wallpapers|8193|d|drwxr-xr-x|0|0|4096|1654875867|1654856689|1654856689|165485668
580f507f743331657d086cdd051ea520|vol4/the_witcher_3_hearts_of_stone_wallpapers|1600x1200|12|d|drwxr-xr-x|0|0|4096|1654875867|1654856689|1654856689|1
54856689
530ad58bc2df1a113735b369109ce96|vol4/the_witcher_3_hearts_of_stone_wallpapers|1600x1200/dual_monitor_wallpapers_geralt&ciri_pack_left_EN.png|13|r/r
wxr--r--|0|0|2596885|1654856689|1654856689|1654856689|1654856689
d56b211ed2e63f4bdd5d1908c8075a|vol4/the_witcher_3_hearts_of_stone_wallpapers|1600x1200/dual_monitor_wallpapers_geralt&ciri_pack_right_EN.png|14|r/r
wxr--r--|0|0|2712771|1654856689|1654856689|1654856689|1654856689
0e8d65b03b7cbe542756ed55b41ef7|vol4/the_witcher_3_hearts_of_stone_wallpapers|1920x1080|15|d|drwxr-xr-x|0|0|4096|1654875867|1654856689|1654856689|1
54856689
720f6fe0a8596d12428544b4250350f|vol4/the_witcher_3_hearts_of_stone_wallpapers|1920x1080/dual_monitor_wallpapers_geralt&ciri_pack_left_EN.png|16|r/r
wxr--r--|0|0|2814468|1654856689|1654856689|1654856689|1654856689
b1bcdfaa86f4c467fe07826e4b626f5|vol4/the_witcher_3_hearts_of_stone_wallpapers|1920x1080/dual_monitor_wallpapers_geralt&ciri_pack_right_EN.png|17|r/r
wxr--r--|0|0|2905003|1654856689|1654856689|1654856689|1654856689
cfcfd0cae694ecb5b3be463d952c3f4|vol4/the_witcher_3_hearts_of_stone_wallpapers|1920x1200|18|d|drwxr-xr-x|0|0|4096|1654875867|1654856689|1654856689|1
54856689
dc747cfb5c2a956e3596604aee4c4bc|vol4/the_witcher_3_hearts_of_stone_wallpapers|1920x1200/dual_monitor_wallpapers_geralt&ciri_pack_left_EN.png|19|r/r
wxr--r--|0|0|2979756|1654856689|1654856689|1654856689|1654856689
ed079050cac707ef7e28d0fa9c165f0|vol4/the_witcher_3_hearts_of_stone_wallpapers|1920x1200/dual_monitor_wallpapers_geralt&ciri_pack_right_EN.png|20|r/r
wxr--r--|0|0|3104401|1654856689|1654856689|1654856689|1654856689

```

Ensuite, il vous faut convertir votre timeline en CSV :

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

Voici à quoi ressemble le fichier CSV généré :

```
machlavel@ubuntu: ~/Desktop
machlavel@ubuntu:~/Desktop$ mactime -b bodyfile -d -i hour timeline_index.csv
Date,Size,Type,Mode,UID,GID,Meta,File Name
Fri Jun 10 2022 03:12:15,16384,macb,d/drwx-----,0,0,11,"vol4/lost+found"
Fri Jun 10 2022 03:24:49,4096,m.cb,d/drwxr-xr-x,0,0,12,"vol4/the_witcher_3_hearts_of_stone_wallpapers/1600x1200"
Fri Jun 10 2022 03:24:49,2596885,macb,r/rwxr--r--,0,0,13,"vol4/the_witcher_3_hearts_of_stone_wallpapers/1600x1200/dual_monitor_wallpapers_geralt&cl
ri_pack_left_EN.png"
Fri Jun 10 2022 03:24:49,4096,...b,d/drwxr-xr-x,0,0,131073,"vol4/the_witcher_3_blood_and_wine_comics"
Fri Jun 10 2022 03:24:49,102,...r/rw-r--r--,0,0,131074,"vol4/the_witcher_3_blood_and_wine_comics/The_Witcher_Killing_Monsters_Comic_PL.pdf"
Fri Jun 10 2022 03:24:49,14578894,macb,r/rwxr--r--,0,0,131075,"vol4/the_witcher_3_blood_and_wine_comics/The_Witcher_Killing_Monsters_Comic_ES.pdf"
Fri Jun 10 2022 03:24:49,13111716,macb,r/rwxr--r--,0,0,131076,"vol4/the_witcher_3_blood_and_wine_comics/The_Witcher_Killing_Monsters_Comic_FR.pdf"
Fri Jun 10 2022 03:24:49,12913707,macb,r/rwxr--r--,0,0,131077,"vol4/the_witcher_3_blood_and_wine_comics/The_Witcher_Killing_Monsters_Comic_DE.pdf"
Fri Jun 10 2022 03:24:49,13403812,macb,r/rwxr--r--,0,0,131078,"vol4/the_witcher_3_blood_and_wine_comics/The_Witcher_Killing_Monsters_Comic_EN.pdf"
Fri Jun 10 2022 03:24:49,18619937,macb,r/rwxr--r--,0,0,131079,"vol4/the_witcher_3_blood_and_wine_comics/The_Witcher_Killing_Monsters_Comic_IT.pdf"
Fri Jun 10 2022 03:24:49,2712771,macb,r/rwxr--r--,0,0,14,"vol4/the_witcher_3_hearts_of_stone_wallpapers/1600x1200/dual_monitor_wallpapers_geralt&cl
ri_pack_right_EN.png"
Fri Jun 10 2022 03:24:49,4096,m.cb,d/drwxr-xr-x,0,0,15,"vol4/the_witcher_3_hearts_of_stone_wallpapers/1920x1080"
Fri Jun 10 2022 03:24:49,2814468,macb,r/rwxr--r--,0,0,16,"vol4/the_witcher_3_hearts_of_stone_wallpapers/1920x1080/dual_monitor_wallpapers_geralt&cl
ri_pack_left_EN.png"
Fri Jun 10 2022 03:24:49,4096,m.cb,d/drwxr-xr-x,0,0,16385,"vol4/the_witcher_3_wallpapers"
Fri Jun 10 2022 03:24:49,2905003,macb,r/rwxr--r--,0,0,17,"vol4/the_witcher_3_hearts_of_stone_wallpapers/1920x1080/dual_monitor_wallpapers_geralt&cl
ri_pack_right_EN.png"
Fri Jun 10 2022 03:24:49,4096,m.cb,d/drwxr-xr-x,0,0,18,"vol4/the_witcher_3_hearts_of_stone_wallpapers/1920x1200"
Fri Jun 10 2022 03:24:49,2979756,macb,r/rwxr--r--,0,0,19,"vol4/the_witcher_3_hearts_of_stone_wallpapers/1920x1200/dual_monitor_wallpapers_geralt&cl
ri_pack_left_EN.png"
Fri Jun 10 2022 03:24:49,3104401,macb,r/rwxr--r--,0,0,20,"vol4/the_witcher_3_hearts_of_stone_wallpapers/1920x1200/dual_monitor_wallpapers_geralt&cl
ri_pack_right_EN.png"
Fri Jun 10 2022 03:24:49,1059660,macb,r/rwxr--r--,0,0,21,"vol4/the_witcher_3_papertoys/Witcher 3 Wild Hunt, The - papertoy Ciri.pdf"
Fri Jun 10 2022 03:24:49,1129666,macb,r/rwxr--r--,0,0,22,"vol4/the_witcher_3_papertoys/Witcher 3 Wild Hunt, The - papertoy Eredin.pdf"
Fri Jun 10 2022 03:24:49,942914,macb,r/rwxr--r--,0,0,23,"vol4/the_witcher_3_papertoys/Witcher 3 Wild Hunt, The - papertoy Geralt.pdf"
Fri Jun 10 2022 03:24:49,905516,macb,r/rwxr--r--,0,0,24,"vol4/the_witcher_3_papertoys/Witcher 3 Wild Hunt, The - papertoy Leshy.pdf"
Fri Jun 10 2022 03:24:49,1054665,macb,r/rwxr--r--,0,0,25,"vol4/the_witcher_3_papertoys/Witcher 3 Wild Hunt, The - papertoy Triss.pdf"
Fri Jun 10 2022 03:24:49,1376352,macb,r/rwxr--r--,0,0,26,"vol4/the_witcher_3_papertoys/Witcher 3 Wild Hunt, The - papertoy Yennefer.pdf"
Fri Jun 10 2022 03:24:49,1119194,macb,r/rwxr--r--,0,0,27,"vol4/the_witcher_3_wallpapers/Witcher 3 Wild Hunt, The - wallpaper 1.jpg"
Fri Jun 10 2022 03:24:49,979349,macb,r/rwxr--r--,0,0,28,"vol4/the_witcher_3_wallpapers/Witcher 3 Wild Hunt, The - wallpaper 2.jpg"
Fri Jun 10 2022 03:24:49,1019487,macb,r/rwxr--r--,0,0,29,"vol4/the_witcher_3_wallpapers/Witcher 3 Wild Hunt, The - wallpaper 3.jpg"
```

## 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>)

Revision #5

Created 8 March 2025 09:39:48 by Elieroc

Updated 12 March 2025 14:15:48 by Elieroc