Log2Timeline

Log2Timeline es una herramienta para generar líneas del tiempo forenses para evidencia digital, como imágenes de disco o logs.

Para instalar Log2Timeline en Ubuntu:

sudo apt-get update
sudo apt-get install python-plaso plaso-tools

Esta herramienta consiste en:

- Plaso.py – Que convierte archivos de evidencia en un formato estándar de línea del tiempo.
- Log2timeline.py – Que convierte la línea del tiempo generada en un archivo con formato legible, como CSV.

Generar un archivo plaso Log2Timeline

log2timeline timeline.plaso drive.e01

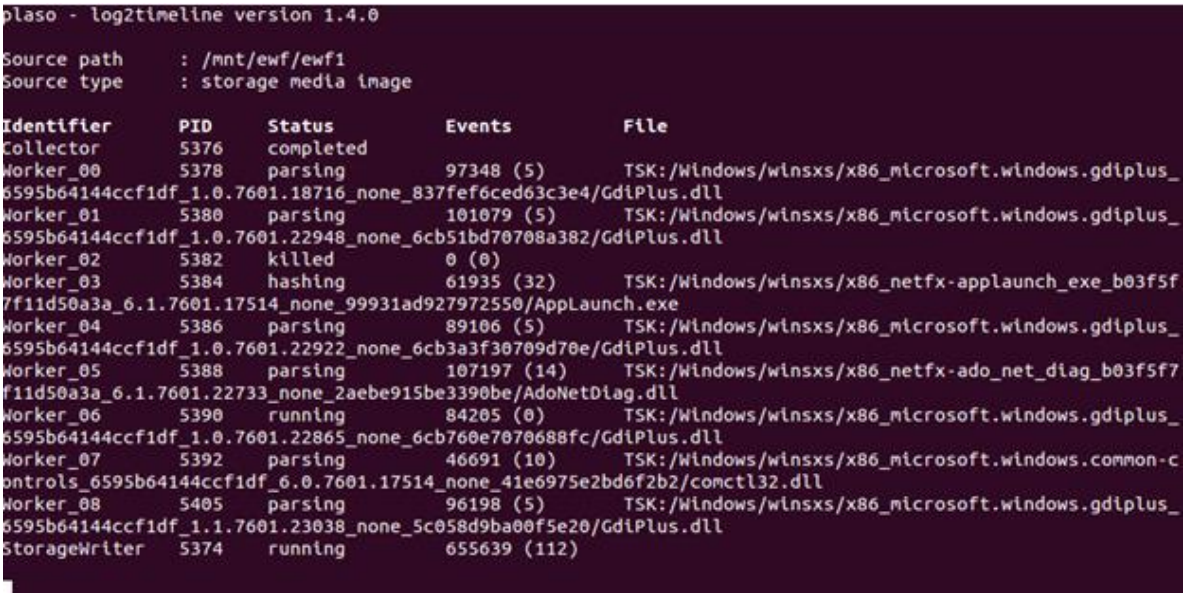
python log2timeline.py timeline.plaso drive.e01

Formatos de salida Log2Timeline

l2tcsv : CSV format used by legacy log2timeline, with 17 fixed fields.
xlsx : Excel Spreadsheet (XLSX) output
l2ttln : Extended TLN 7 field | delimited output.
4n6time_sqlite : Saves the data in a SQLite database, used by the tool 4n6time.
kml : Saves events with geography data into a KML format.
dynamic : Dynamic selection of fields for a separated value output format.
rawpy : "raw" (or native) Python output.
json : Saves the events into a JSON format.
null : Output module that does not output anything.
tln : TLN 5 field | delimited output.
json_line : Saves the events into a JSON line format

Log2Timeline Cheatsheet

https://digital-forensics.sans.org/media/log2timeline_cheatsheet.pdf



```
plaso - log2timeline version 1.4.0

Source path     : /mnt/ewf/ewf1
Source type     : storage media image

Identifier      PID     Status          Events          File
Collector       5376    completed
Worker_00       5378    parsing         97348 (5)       TSK:/Windows/winsxs/x86_microsoft.windows.gdiplus_
6595b64144ccf1df_1.0.7601.18716_none_837fef6ced63c3e4/GdiPlus.dll
Worker_01       5380    parsing         101079 (5)      TSK:/Windows/winsxs/x86_microsoft.windows.gdiplus_
6595b64144ccf1df_1.0.7601.22948_none_6cb51bd70708a382/GdiPlus.dll
Worker_02       5382    killed          0 (0)
Worker_03       5384    hashing         61935 (32)      TSK:/Windows/winsxs/x86_netfx-applaunch_exe_b03f5f
7f11d50a3a_6.1.7601.17514_none_99931ad927972550/AppLaunch.exe
Worker_04       5386    parsing         89106 (5)       TSK:/Windows/winsxs/x86_microsoft.windows.gdiplus_
6595b64144ccf1df_1.0.7601.22922_none_6cb3a3f30709d70e/GdiPlus.dll
Worker_05       5388    parsing         107197 (14)     TSK:/Windows/winsxs/x86_netfx-ado_net_diag_b03f5f7
f11d50a3a_6.1.7601.22733_none_2aebe915be3390be/AdoNetDiag.dll
Worker_06       5390    running         84205 (0)       TSK:/Windows/winsxs/x86_microsoft.windows.gdiplus_
6595b64144ccf1df_1.0.7601.22865_none_6cb760e7070688fc/GdiPlus.dll
Worker_07       5392    parsing         46691 (10)      TSK:/Windows/winsxs/x86_microsoft.windows.common-c
ontrols_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2/comctl32.dll
Worker_08       5405    parsing         96198 (5)       TSK:/Windows/winsxs/x86_microsoft.windows.gdiplus_
6595b64144ccf1df_1.1.7601.23038_none_5c058d9ba00f5e20/GdiPlus.dll
StorageWriter   5374    running         655639 (112)
```