About me…

Marcos Fuentes Martínez

@_N4rr34n6_ | N4rr34n6@protonmail.com

- Especialista en Tecnologías de la Información y Comunicaciones
- Experto en Derecho Tecnológico e Informática Forense por la Unex
- Ex autor en ‘Follow the White Rabbit’, (https://www.fwhibbit.es)

Generación y visualización de líneas de tiempo

Algo atrevido

Marcos Fuentes Martínez | @_N4rr34n6_

PATRONATO DE CULTURA AYUNTAMIENTO DE GUADALAJARA
HoneyCON By HoneySec

¿Líneas de tiempo?

Follow The White Rabbit

- *Sobre las líneas de tiempo: El límite, tu imaginación*

https://www.fwhibbit.es/sobre-las-lineas-de-tiempo-el-limite-tu-imaginacion

- *¿Qué ha pasado? El ABC del MACB*

https://www.fwhibbit.es/que-ha-pasado-el-abc-del-macb

Visualización de una lista de eventos en **orden cronológico**

Ordenar cronológicamente **toda actividad** de un Sistema

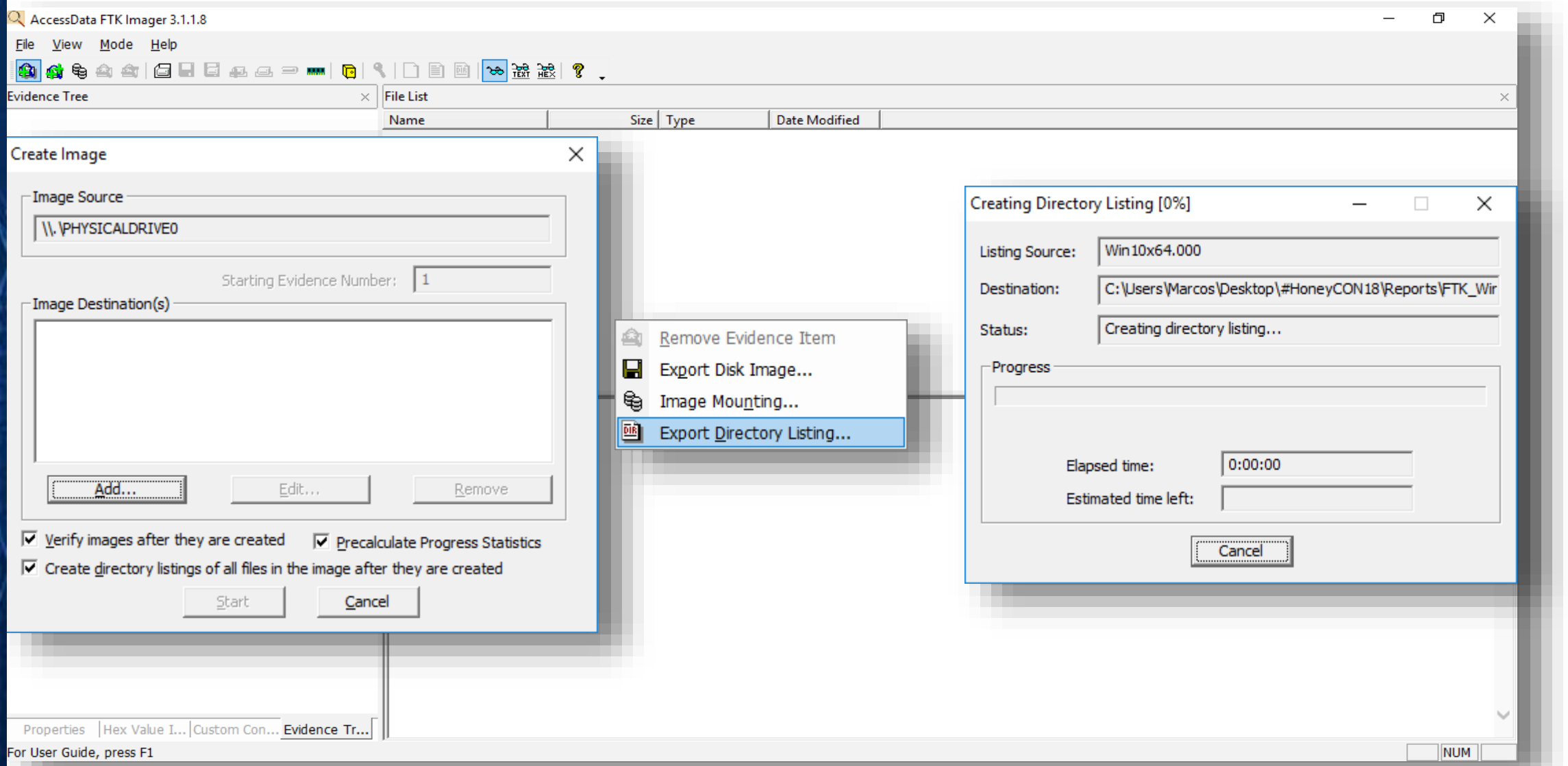
Algo ha pasado, en un momento determinado, en un fichero en concreto

Modificado, **A**ccedido, **C**ambiado, **B** Creado, **Deleted**

‘**$Standard Information**’ | ‘**$File_Name**’

FTK, (Forensic ToolKit)

http://accessdata.com/product-download/ftk-imager-lite-version-3.1.1



Crea listados de directorios de todos los archivos de la imagen

FTK, (Forensic ToolKit)

http://accessdata.com/product-download/ftk-imager-lite-version-3.1.1

	A	B	C	D	E	F	G
1	Filename	Full Path	Size (bytes)	Created	Modified	Accessed	Is Deleted
2	[root]	NONAME [NTFS]\[root]\	56	2016-Jul-16 06:04:24.614482 UTC	2017-Oct-20 20:26:10.002389 UTC	2017-Oct-20 20:26:10.002389 UTC	no
3	[unallocated space]	NONAME [NTFS]\[unallocated space]\	0				no
4	[orphan]	NONAME [NTFS]\[orphan]\	0				no
5	file system slack	NONAME [NTFS]\file system slack	3584				no
6	backup boot sector	NONAME [NTFS]\backup boot sector	512				no
7	$I30	NONAME [NTFS]\[root]\$I30	4096	2016-Jul-16 06:04:24.614482 UTC	2017-Oct-20 20:26:10.002389 UTC	2017-Oct-20 20:26:10.002389 UTC	no
8	$TXF_DATA	NONAME [NTFS]\[root]\$TXF_DATA	56	2016-Jul-16 06:04:24.614482 UTC	2017-Oct-20 20:26:10.002389 UTC	2017-Oct-20 20:26:10.002389 UTC	no
9	$AttrDef	NONAME [NTFS]\[root]\$AttrDef	2560	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	no
10	$BadClus	NONAME [NTFS]\[root]\$BadClus\	0	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	no
11	$Bitmap	NONAME [NTFS]\[root]\$Bitmap	639296	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	no
12	$Boot	NONAME [NTFS]\[root]\$Boot	8192	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	no
13	$Extend	NONAME [NTFS]\[root]\$Extend\	656	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	no
14	$LogFile	NONAME [NTFS]\[root]\$LogFile	29868032	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	no
15	$MFT	NONAME [NTFS]\[root]\$MFT	96731136	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	no
16	$MFTMirr	NONAME [NTFS]\[root]\$MFTMirr	4096	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	no
17	$Recycle.Bin	NONAME [NTFS]\[root]\$Recycle.Bin\	608	2016-Jul-16 11:47:47.967567 UTC	2017-Oct-20 20:26:10.040628 UTC	2017-Oct-20 20:26:10.040628 UTC	no
18	$Secure	NONAME [NTFS]\[root]\$Secure\	56	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	no
19	$UpCase	NONAME [NTFS]\[root]\$UpCase\	131072	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	no
20	$Volume	NONAME [NTFS]\[root]\$Volume	0	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	2017-Oct-18 19:21:08.205814 UTC	no
21	@Please_Read_Me@.txt	NONAME [NTFS]\[root]\@Please_Read_Me@.txt	933	2017-Oct-20 20:26:10.002389 UTC	2017-Oct-20 20:26:09.923531 UTC	2017-Oct-20 20:26:10.002389 UTC	no
22	@WanaDecryptor@.exe	NONAME [NTFS]\[root]\@WanaDecryptor@.exe	245760	2017-Oct-20 20:26:10.002389 UTC	2017-May-12 00:22:56 UTC	2017-Oct-20 20:26:10.002389 UTC	no
23	Archivos de programa	NONAME [NTFS]\[root]\Archivos de programa\	92	2017-Oct-18 18:38:43.048199 UTC	2017-Oct-18 18:38:43.048199 UTC	2017-Oct-18 18:38:43.048199 UTC	no
24	bootmgr	NONAME [NTFS]\[root]\bootmgr	384322	2016-Jul-16 12:58:18.186536 UTC	2016-Jul-16 11:43:00.546257 UTC	2016-Jul-16 22:42:58.098700 UTC	no
25	BOOTNXT	NONAME [NTFS]\[root]\BOOTNXT	1	2016-Jul-16 12:58:19.874034 UTC	2016-Jul-16 11:43:00.546257 UTC	2016-Jul-16 22:42:58.395593 UTC	no

Crea listados de directorios de todos los archivos de la imagen

FTK, (Forensic ToolKit)

http://accessdata.com/product-download/ftk-imager-lite-version-3.1.1

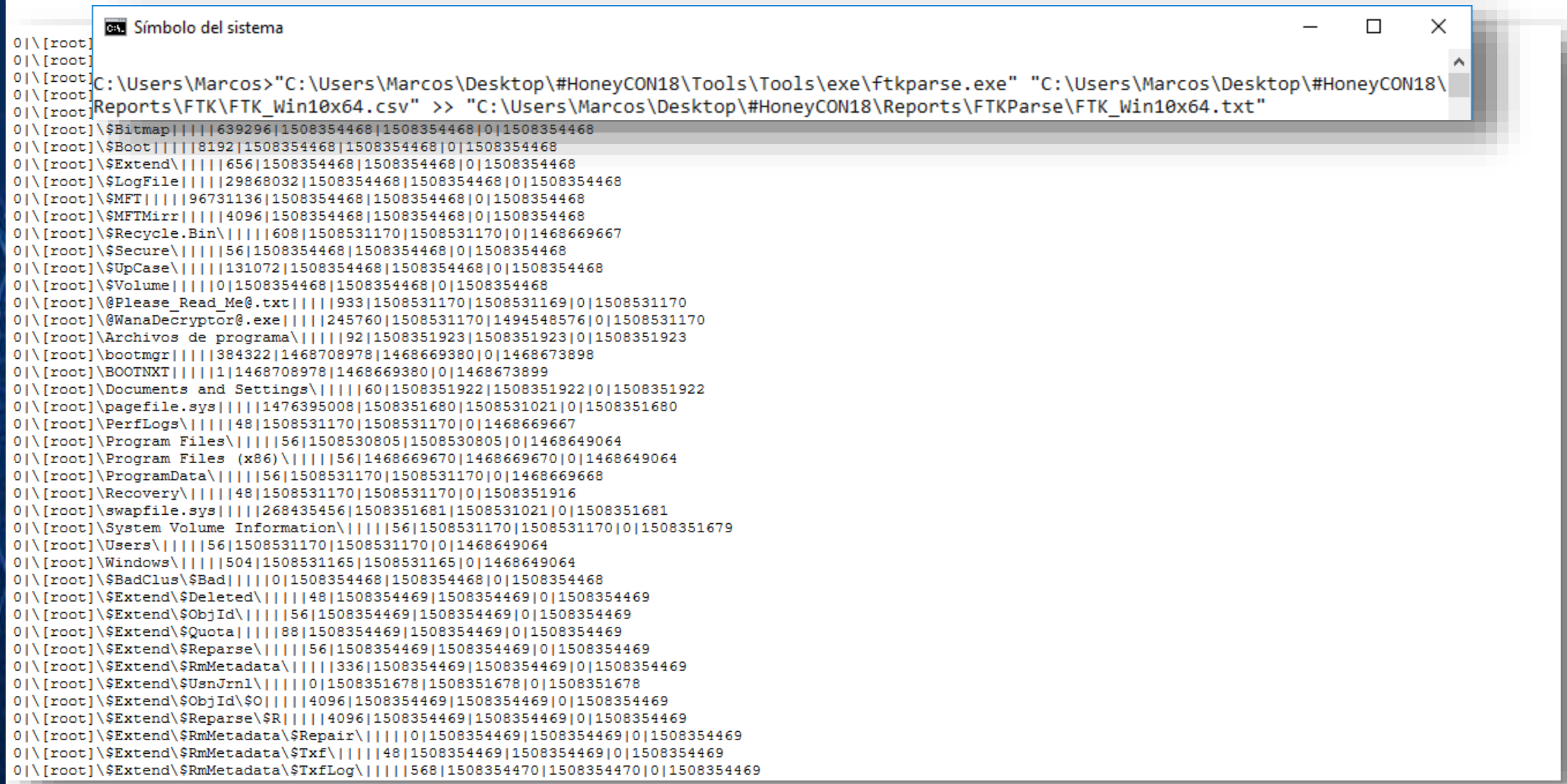
	A	B	C	D	E	F	G
1	Filename	Full Path	Size (bytes)	Created	Modified	Accessed	Is Deleted
2	[root]	NONAME [NTFS]\[root]\	56	2016-Jul-16 06:04:24.614482 UTC	2017-Oct-20 20:26:10.002389 UTC	2017-Oct-20 20:26:10.002389 UTC	no
3	[unallocated space]	NONAME [NTFS]\[unallocated space]\	0				no
4	[orphan]	NONAME [NTFS]\[orphan]\	0				no
5	file system slack	NONAME [NTFS]\file system slack	3584				no
6	backup boot sector	NONAME [NTFS]\backup boot sector	512				no

	A	B	C	D	E	F	G
1	Filename	Full Path	Size (bytes)	Created	Modified	Accessed	Is Deleted
2	#CONPilar - Logo02.jpg	NONAME [NTFS]\[root]\Users\Marcos\Downl	17544	2017-Oct-19 20:02:42.960369 UTC	2017-Feb-16 04:52:38 UTC	2017-Oct-19 20:02:42.960369 UTC	no
3	#CONPilar - Logo02.jpg.WNCRY	NONAME [NTFS]\[root]\Users\Marcos\Downl	17832	2017-Oct-19 20:02:42.960369 UTC	2017-Feb-16 04:52:38 UTC	2017-Oct-19 20:02:42.960369 UTC	no
4	#CONPilar17 - Logo01.png	NONAME [NTFS]\[root]\Users\Marcos\Downl	32796	2017-Oct-19 20:02:45.798571 UTC	2017-Jan-30 11:36:12 UTC	2017-Oct-19 20:02:45.798571 UTC	no
5	#CONPilar17 - Logo01.png.WNCRY	NONAME [NTFS]\[root]\Users\Marcos\Downl	33080	2017-Oct-19 20:02:45.798571 UTC	2017-Jan-30 11:36:12 UTC	2017-Oct-19 20:02:45.798571 UTC	no
6	$$.cdf-ms	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	3180	2016-Jul-16 06:04:27.911619 UTC	2016-Jul-16 22:47:45.848473 UTC	2016-Jul-16 22:47:45.848473 UTC	no
7	$$_addins_2452dff8cb692cdd.cdf-ms	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	632	2016-Jul-16 11:47:49.670688 UTC	2016-Jul-16 11:45:34.858454 UTC	2016-Jul-16 11:45:34.858454 UTC	no
8	$$_appcompat_appraiser_33781004	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	576	2016-Jul-16 11:47:49.655065 UTC	2016-Jul-16 11:45:34.842830 UTC	2016-Jul-16 11:45:34.842830 UTC	no
9	$$_appcompat_appraiser_telemetry	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	588	2016-Jul-16 11:47:49.655065 UTC	2016-Jul-16 11:45:34.858454 UTC	2016-Jul-16 11:45:34.858454 UTC	no
10	$$_appcompat_programs_99c7f419b	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	572	2016-Jul-16 11:47:49.655065 UTC	2016-Jul-16 11:45:34.842830 UTC	2016-Jul-16 11:45:34.842830 UTC	no
11	$$_apppatch_1143992cbbbebcab.cdf	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	2952	2016-Jul-16 11:47:49.655065 UTC	2016-Jul-16 22:39:43.635168 UTC	2016-Jul-16 22:39:43.635168 UTC	no
12	$$_apppatch_apppatch64_e39bab3b	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	1996	2016-Jul-16 11:47:49.655065 UTC	2016-Jul-16 11:45:34.842830 UTC	2016-Jul-16 11:45:34.842830 UTC	no
13	$$_apppatch_custom_2adff76bea48	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	592	2016-Jul-16 11:47:49.655065 UTC	2016-Jul-16 11:45:34.842830 UTC	2016-Jul-16 11:45:34.842830 UTC	no
14	$$_apppatch_custom_custom64_121	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	600	2016-Jul-16 11:47:49.655065 UTC	2016-Jul-16 11:45:34.842830 UTC	2016-Jul-16 11:45:34.842830 UTC	no
15	$$_apppatch_en-us_098dc872781ael	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	640	2016-Jul-16 22:39:52.416880 UTC	2016-Jul-16 22:39:43.635168 UTC	2016-Jul-16 22:39:43.635168 UTC	no
16	$$_apppatch_es-es_098dc7be781ae	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	664	2016-Jul-16 22:39:52.416880 UTC	2016-Jul-16 22:39:43.635168 UTC	2016-Jul-16 22:39:43.635168 UTC	no
17	$$_appreadiness_b6ba89081e320d8	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	584	2016-Jul-16 11:47:49.655065 UTC	2016-Jul-16 11:45:34.842830 UTC	2016-Jul-16 11:45:34.842830 UTC	no
18	$$_bcastdvr_fab1ebc0dbf2dacb.cdf-	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	756	2016-Jul-16 11:47:49.655065 UTC	2016-Jul-16 11:45:34.842830 UTC	2016-Jul-16 11:45:34.842830 UTC	no
19	$$_bitlockerdiscoveryvolumeconter	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	8968	2016-Jul-16 22:45:52.248589 UTC	2016-Jul-16 22:45:46.013939 UTC	2016-Jul-16 22:45:46.013939 UTC	no
20	$$_boot_40104b85a18bfcb2.cdf-ms	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	664	2016-Jul-16 11:47:49.561313 UTC	2016-Jul-16 22:39:43.635168 UTC	2016-Jul-16 22:39:43.635168 UTC	no
21	$$_boot_dvd_efi_de3c4ceb52549e1	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	652	2016-Jul-16 11:47:49.655065 UTC	2016-Jul-16 11:45:34.842830 UTC	2016-Jul-16 11:45:34.842830 UTC	no
22	$$_boot_dvd_efi_en-us_8245c3aed	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	680	2016-Jul-16 11:47:49.655065 UTC	2016-Jul-16 11:45:34.842830 UTC	2016-Jul-16 11:45:34.842830 UTC	no
23	$$_boot_dvd_pcat_de3c62295de3e2	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	884	2016-Jul-16 11:47:49.655065 UTC	2016-Jul-16 22:39:43.635168 UTC	2016-Jul-16 22:39:43.635168 UTC	no
24	$$_boot_dvd_pcat_es-es_80af5830f	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	656	2016-Jul-16 22:39:52.416880 UTC	2016-Jul-16 22:39:43.635168 UTC	2016-Jul-16 22:39:43.635168 UTC	no
25	$$_boot_efi_0f890f82be247f42.cdf-r	NONAME [NTFS]\[root]\Windows\WinSxS\Fil	964	2016-Jul-16 11:47:49.608188 UTC	2016-Jul-16 11:45:34.811578 UTC	2016-Jul-16 11:45:34.811578 UTC	no

Crea listados de directorios de todos los archivos de la imagen

FTK parse

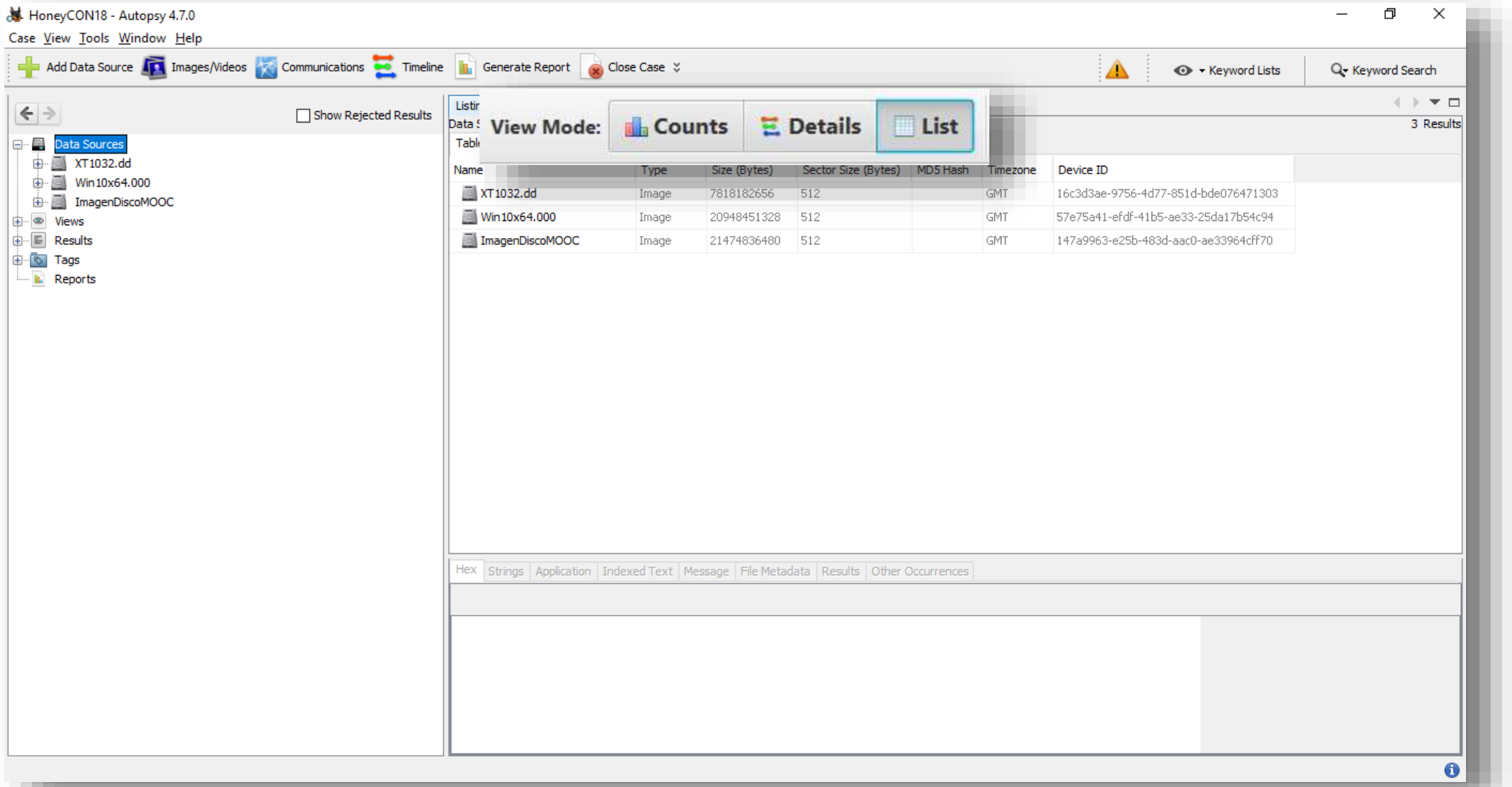
https://github.com/keydet89/Tools



Parsea la salida '.csv' del "Export Directory Listing" de FTK Imager al formato de cuerpo TSK

Autopsy

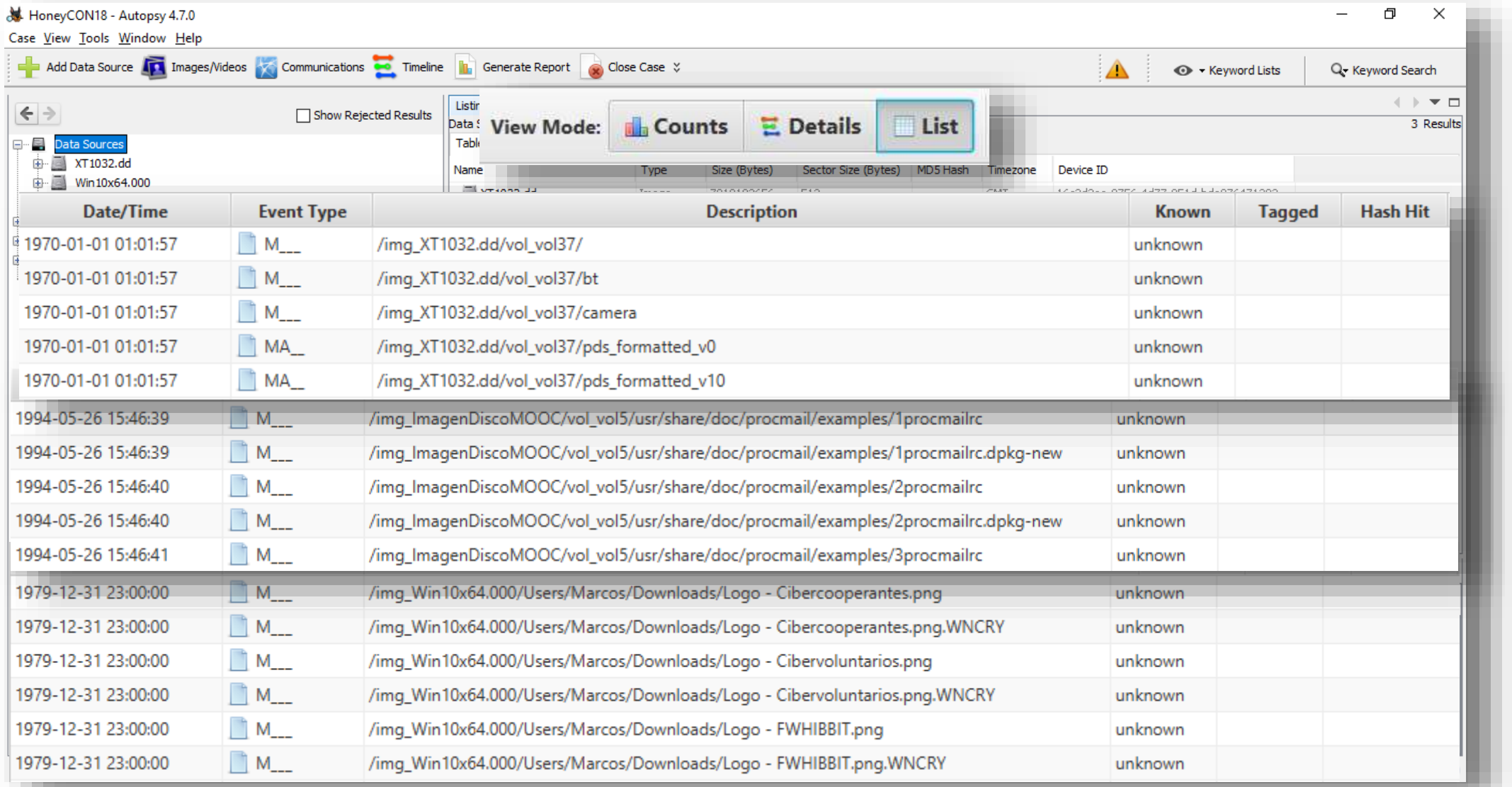
https://www.sleuthkit.org/autopsy/download.php



Tiene tres modos de visualización dentro de la misma herramienta

Autopsy

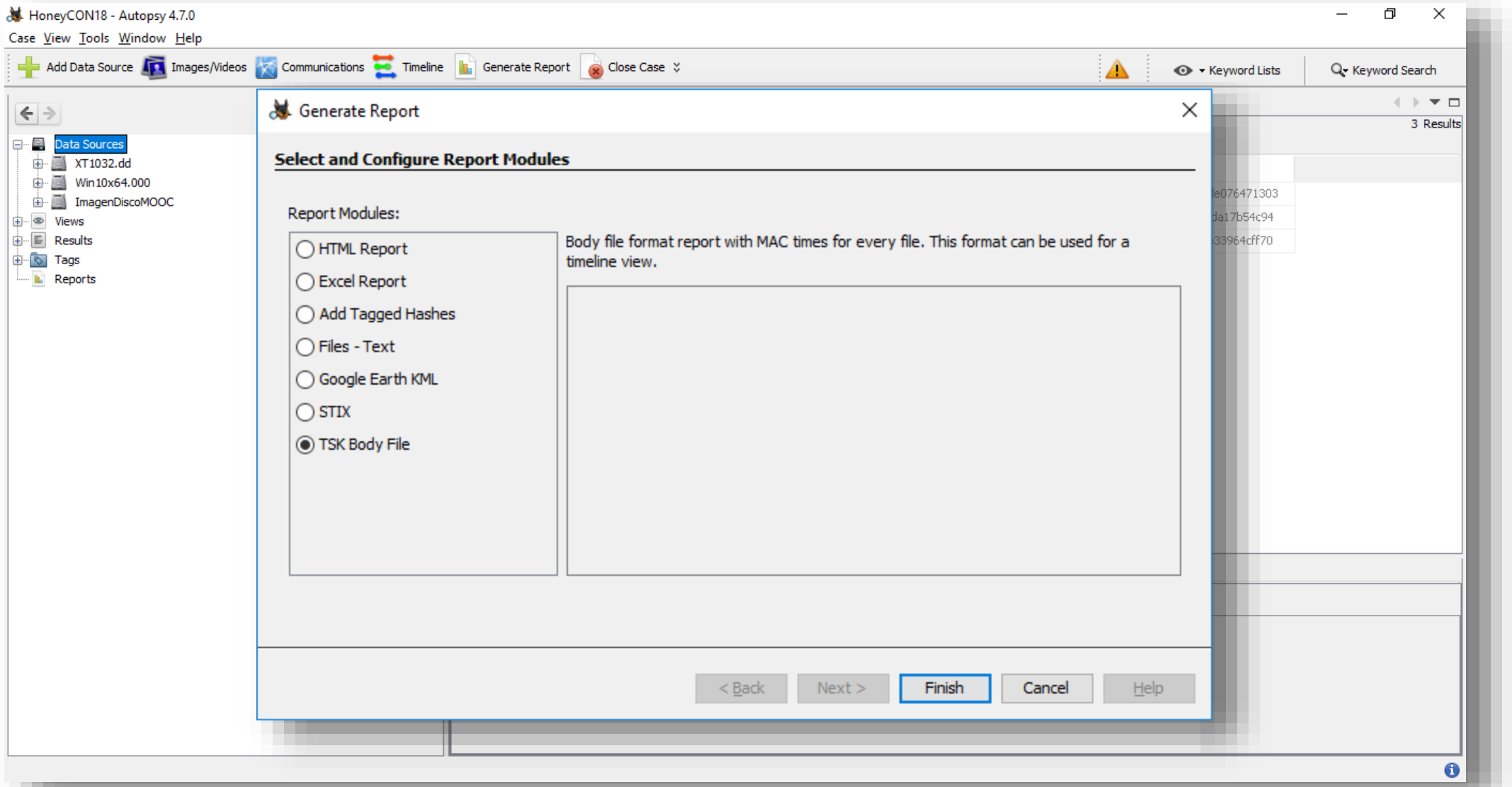
https://www.sleuthkit.org/autopsy/download.php



Tiene tres modos de visualización dentro de la misma herramienta

Autopsy

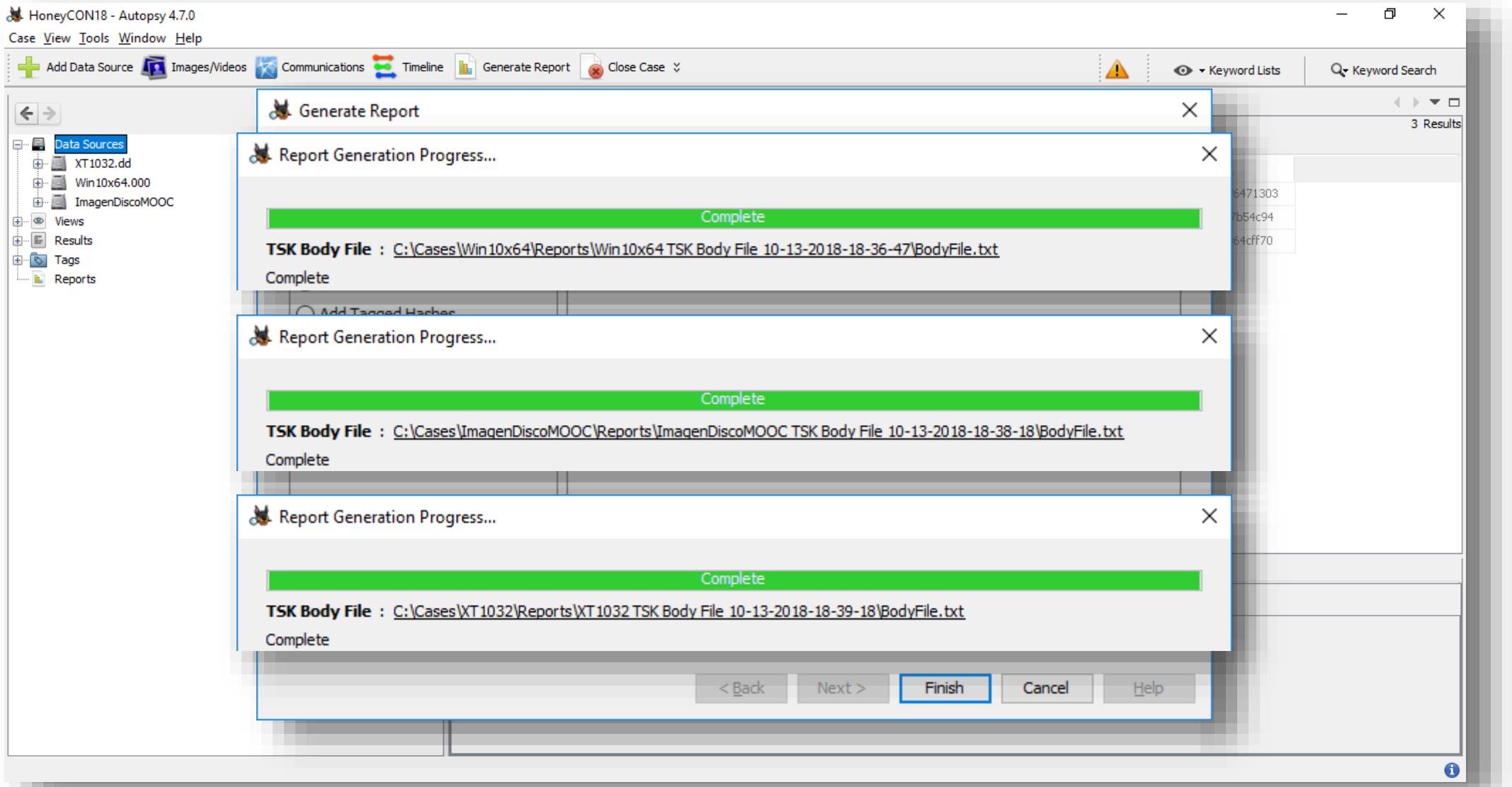
https://www.sleuthkit.org/autopsy/download.php



Crea un reporte de formato de archivo de cuerpo con tiempos MACB para cada archivo

Autopsy

https://www.sleuthkit.org/autopsy/download.php

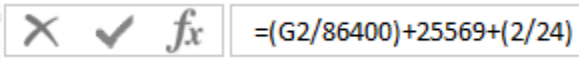


Crea un reporte de formato de archivo de cuerpo con tiempos MACb para cada archivo

Autopsy

https://www.sleuthkit.org/autopsy/download.php

```
|/img_Win10x64.000/|5|dr-xr-xr-x|0|0|56|1508531170|1508531170|1508531170|1468649064
|/img_Win10x64.000/$AttrDef|4|rr-xr-xr-x|48|0|2560|1508354468|1508354468|1508354468|1508354468
|/img_Win10x64.000/$BadClus|8|rr-xr-xr-x|0|0|0|1508354468|1508354468|1508354468|1508354468
|/img_Win10x64.000/$BadClus:$Bad|8|rr-xr-xr-x|0|0|20948447232|1508354468|1508354468|1508354468|1508354468
|/img_Win10x64.000/$Bitmap|6|rr-xr-xr-x|0|0|639296|1508354468|1508354468|1508354468|1508354468
|/img_Win10x64.000/$Boot|7|rr-xr-xr-x|48|0|8192|1508354468|1508354468|1508354468|1508354468
|/img_Win10x64.000/$Extend|11|dr-xr-xr-x|0|0|656|1508354468|1508354468|1508354468|1508354468
|/img_Win10x64.000/$Extend/$Deleted|24|dr-xr-xr-x|0|0|48|1508354469|1508354469|1508354469|1508354469
|/img_Win10x64.000/$Extend/$ObjId|26|rr-xr-xr-x|0|0|0|1508354469|1508354469|1508354469|1508354469
|/img_Win10x64.000/$Extend/$Quota|25|rr-xr-xr-x|0|0|0|1508354469|1508354469|1508354469|1508354469
|/img_Win10x64.000/$Extend/$Reparse|27|rr-xr-xr-x|0|0|0|1508354469|1508354469|1508354469|1508354469
|/img_Win10x64.000/$Extend/$RmMetadata|28|dr-xr-xr-x|0|0|336|1508354469|1508354469|1508354469|1508354469
|/img_Win10x64.000/$Extend/$RmMetadata/$Repair|29|rr-xr-xr-x|0|0|0|1508354469|1508354469|1508354469|1508354469
|/img_Win10x64.000/$Extend/$RmMetadata/$Repair:$Config|29|rr-xr-xr-x|0|0|8|1508354469|1508354469|1508354469|1508354469
|/img_Win10x64.000/$Extend/$RmMetadata/$Repair:$Corrupt|29|rr-xr-xr-x|0|0|8388608|1508354469|1508354469|1508354469|1508354469
|/img_Win10x64.000/$Extend/$RmMetadata/$Repair:$Verify|29|rr-xr-xr-x|0|0|1048576|1508354469|1508354469|1508354469|1508354469
|/img_Win10x64.000/$Extend/$RmMetadata/$Txf|31|dr-xr-xr-x|0|0|48|1508354469|1508354469|1508354469|1508354469
|/img_Win10x64.000/$Extend/$RmMetadata/$TxfLog|30|dr-xr-xr-x|0|0|568|1508354470|1508354470|1508354470|1508354469
|/img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$Tops|32|rr-xr-xr-x|0|0|100|1508354469|1508354469|1508354469|1508354469
|/img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$Tops:$T|32|rr-xr-xr-x|0|0|1048576|1508354469|1508354469|1508354469|1508354469
|/img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$TxfLog.blf|33|rrwxrwxrwx|0|0|65536|1508354470|1508531211|1508531211|1508354470
|/img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$TxfLogContainer00000000000000000001|34|rrwxrwxrwx|0|0|10485760|1508354470|1508531211|1508531211|1508354470
|/img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$TxfLogContainer00000000000000000002|35|rrwxrwxrwx|0|0|10485760|1508354470|1508355258|1508355258|1508354470
|/img_Win10x64.000/$Extend/$UsnJrnl:$J|45993|rr-xr-xr-x|0|0|9819416|1508351678|1508351678|1508351678|1508351678
|/img_Win10x64.000/$Extend/$UsnJrnl:$Max|45993|rr-xr-xr-x|0|0|32|1508351678|1508351678|1508351678|1508351678
|/img_Win10x64.000/$LogFile|2|rr-xr-xr-x|0|0|29868032|1508354468|1508354468|1508354468|1508354468
|/img_Win10x64.000/$MFT|0|rr-xr-xr-x|0|0|96731136|1508354468|1508354468|1508354468|1508354468
|/img_Win10x64.000/$MFTMirr|1|rr-xr-xr-x|0|0|4096|1508354468|1508354468|1508354468|1508354468
|/img_Win10x64.000/$Recycle.Bin|58|dr-xr-xr-x|0|0|608|1508531170|1508531170|1508531170|1468669667
|/img_Win10x64.000/$Recycle.Bin/S-1-5-21-3930698692-3150784357-1811628781-1000|90887|dr-xr-xr-x|0|0|152|1508531170|1508531170|1508531170|1508352359
|/img_Win10x64.000/$Recycle.Bin/S-1-5-21-3930698692-3150784357-1811628781-1000/desktop.ini|90888|rr-xr-xr-x|0|0|129|1508352359|1508352359|1508352359|1508352359
|/img_Win10x64.000/$Recycle.Bin/S-1-5-21-3930698692-3150784357-1811628781-1001|92013|dr-xr-xr-x|0|0|152|1508531170|1508531170|1508531170|1508352394
|/img_Win10x64.000/$Recycle.Bin/S-1-5-21-3930698692-3150784357-1811628781-1001/desktop.ini|92014|rr-xr-xr-x|0|0|129|1508352394|1508352394|1508352394|1508352394
|/img_Win10x64.000/$Secure:$SDS|9|rr-xr-xr-x|0|0|1027440|1508354468|1508354468|1508354468|1508354468
|/img_Win10x64.000/$UpCase|10|rr-xr-xr-x|0|0|131072|1508354468|1508354468|1508354468|1508354468
|/img_Win10x64.000/$UpCase:$Info|10|rr-xr-xr-x|0|0|32|1508354468|1508354468|1508354468|1508354468
|/img_Win10x64.000/$Volume|3|rr-xr-xr-x|0|0|0|1508354468|1508354468|1508354468|1508354468
|/img_Win10x64.000/@Please_Read_Me@.txt|93956|rrwxrwxrwx|0|0|933|1508531170|1508531169|1508531169|1508531170
|/img_Win10x64.000/@WanaDecryptor@.exe|93957|rrwxrwxrwx|0|0|245760|1508531170|1494548576|1508531167|1508531170
|/img_Win10x64.000/Archivos de programa|90249|dr-xr-xr-x|0|0|48|1508351923|1508351923|1508351923|1508351923
|/img_Win10x64.000/bootmgr|19984|r--x--x--x|0|0|384322|1468708978|1468669380|1508354480|1468673898
|/img_Win10x64.000/BOOTNXT|19980|rr-xr-xr-x|0|0|1|1468708978|1468669380|1508354480|1468673899
|/img_Win10x64.000/Documents and Settings|90237|dr-xr-xr-x|0|0|48|1508351922|1508351922|1508351922|1508351922
```



=(G2/86400)+25569+(2/24)

Autopsy

https://www.sleuthkit.org/autopsy/download.php

```
|/img_Win10x64.000/|5|dr-xr-xr-x|0|0|56|1508531170|1508531170|1508531170|1468649064
|/img_Win10x64.000/$AttrDef|4|rr-xr-xr-x|48|0|2560|1508354468|1508354468|1508354468|1508354468
|/img_Win10x64.000/$BadClus|8|rr-xr-xr-x|0|0|0|1508354468|1508354468|1508354468|1508354468
```

=(G2/86400)+25569+(2/24)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Path	Inode	Mode	UID	GID	Size	Atime	Access	Mtime	Modified	Ctime	Changed	Crtime	Birth
2	/img_Win10x64.000/Program Files/WindowsApps/	25074	rrwxrwxrwx	0	0	1096	1468709462	17-7-16 0:51	1468709462	17-7-16 0:51	1508351812	18-10-17 20:36	1468709462	17-7-16 0:51
3	/img_Win10x64.000/Program Files/WindowsApps/	23313	rrwxrwxrwx	0	0	281	1468709402	17-7-16 0:50	1468709402	17-7-16 0:50	1508351798	18-10-17 20:36	1468709402	17-7-16 0:50
4	/img_Win10x64.000/Program Files/WindowsApps/	27590	rrwxrwxrwx	0	0	2204	1468709473	17-7-16 0:51	1468709473	17-7-16 0:51	1508351831	18-10-17 20:37	1468709473	17-7-16 0:51
5	/img_Win10x64.000/ProgramData/Microsoft/Wind	89675	----------	0	0	0	0	1-1-70 2:00	0	1-1-70 2:00	0	1-1-70 2:00	0	1-1-70 2:00
6	/img_Win10x64.000/Users/Marcos/AppData/Local/	93352	drwxrwxrwx	0	0	312	1508531173	20-10-17 22:26	1508531173	20-10-17 22:26	1508531173	20-10-17 22:26	1508353269	18-10-17 21:01
7	/img_Win10x64.000/Users/Marcos/AppData/Local/	90934	drwxrwxrwx	0	0	280	1508531173	20-10-17 22:26	1508531173	20-10-17 22:26	1508531173	20-10-17 22:26	1508352359	18-10-17 20:45
8	/img_Win10x64.000/Windows/servicing/Packages/	36593	rrwxrwxrwx	0	0	1089	1468708602	17-7-16 0:36	1468679642	16-7-16 16:34	1508354762	18-10-17 21:26	1468708602	17-7-16 0:36
9	/img_Win10x64.000/Windows/assembly/NativeIm	30298	rrwxrwxrwx	0	0	120160	1468709516	17-7-16 0:51	1468676922	16-7-16 15:48	1508354632	18-10-17 21:23	1468709516	17-7-16 0:51
10	/img_Win10x64.000/Windows/Fonts/vga775.fon	31507	rrwxrwxrwx	0	0	5168	1468669349	16-7-16 13:42	1468669349	16-7-16 13:42	1508354677	18-10-17 21:24	1468669349	16-7-16 13:42
11	/img_Win10x64.000/Windows/ImmersiveControlP	32106	rrwxrwxrwx	0	0	1512	1468669360	16-7-16 13:42	1468669360	16-7-16 13:42	1508354695	18-10-17 21:24	1468669360	16-7-16 13:42
12	/img_Win10x64.000/Windows/INF/c_keyboard.inf	32386	rrwxrwxrwx	0	0	1402	1468669313	16-7-16 13:41	1468669313	16-7-16 13:41	1508354696	18-10-17 21:24	1468669313	16-7-16 13:41
13	/img_Win10x64.000/Windows/InfusedApps/Packag	21839	rrwxrwxrwx	0	0	27648	1468709330	17-7-16 0:48	1468709330	17-7-16 0:48	1508351780	18-10-17 20:36	1468709330	17-7-16 0:48
14	/img_Win10x64.000/Windows/InfusedApps/Packag	23374	rrwxrwxrwx	0	0	221	1468709403	17-7-16 0:50	1468709403	17-7-16 0:50	1508351798	18-10-17 20:36	1468709403	17-7-16 0:50
15	/img_Win10x64.000/Windows/Microsoft.NET/asse	33456	rrwxrwxrwx	0	0	497936	1468669435	16-7-16 13:43	1468669435	16-7-16 13:43	1508354729	18-10-17 21:25	1468669435	16-7-16 13:43
16	/img_Win10x64.000/Windows/System32/DriverSto	50199	rrwxrwxrwx	0	0	67584	1468669318	16-7-16 13:41	1468669318	16-7-16 13:41	1508355001	18-10-17 21:30	1468669318	16-7-16 13:41
17	/img_Win10x64.000/Windows/System32/he-IL/ms	52620	rrwxrwxrwx	0	0	5120	1468669347	16-7-16 13:42	1468669347	16-7-16 13:42	1508355021	18-10-17 21:30	1468669347	16-7-16 13:42
18	/img_Win10x64.000/Windows/System32/CatRoot/	40770	rrwxrwxrwx	0	0	9731	1468668986	16-7-16 13:36	1468648717	16-7-16 7:58	1508354774	18-10-17 21:26	1468668986	16-7-16 13:36
19	/img_Win10x64.000/Windows/SystemApps/Contac	56001	rrwxrwxrwx	0	0	3032	1468709257	17-7-16 0:47	1468709257	17-7-16 0:47	1508355080	18-10-17 21:31	1468709257	17-7-16 0:47
20	/img_Win10x64.000/Windows/SysWOW64/en-US/	61148	rrwxrwxrwx	0	0	20992	1468708747	17-7-16 0:39	1468708747	17-7-16 0:39	1508355164	18-10-17 21:32	1468708747	17-7-16 0:39
21	/img_Win10x64.000/Windows/SysWOW64/tasksch	60348	rrwxrwxrwx	0	0	566600	1468669381	16-7-16 13:43	1468669381	16-7-16 13:43	1508355152	18-10-17 21:32	1468669381	16-7-16 13:43
22	/img_Win10x64.000/Windows/WinSxS/amd64_mdi	32520	rrwxrwxrwx	0	0	105140	1468669313	16-7-16 13:41	1468669313	16-7-16 13:41	1508354700	18-10-17 21:25	1468669313	16-7-16 13:41
23	/img_Win10x64.000/Windows/WinSxS/amd64_mic	45726	rrwxrwxrwx	0	0	46592	1468709140	17-7-16 0:45	1468709140	17-7-16 0:45	1508354856	18-10-17 21:27	1468669400	16-7-16 13:43
24	/img_Win10x64.000/Windows/WinSxS/amd64_mic	52827	rrwxrwxrwx	0	0	199008	1468669354	16-7-16 13:42	1468669354	16-7-16 13:42	1508355029	18-10-17 21:30	1468669354	16-7-16 13:42
25	/img_Win10x64.000/Windows/WinSxS/amd64_mic	50573	rrwxrwxrwx	0	0	52224	1468669341	16-7-16 13:42	1468669341	16-7-16 13:42	1508355008	18-10-17 21:30	1468669341	16-7-16 13:42

```
|/img_Win10x64.000/@WanaDecryptor@.exe|93957|rrwxrwxrwx|0|0|245760|1508531170|1494548576|1508531167|1508531170
|/img_Win10x64.000/Archivos de programa|90249|dr-xr-xr-x|0|0|48|1508351923|1508351923|1508351923|1508351923
|/img_Win10x64.000/bootmgr|19984|r--x--x--x|0|0|384322|1468708978|1468669380|1508354480|1468673898
|/img_Win10x64.000/BOOTNXT|19980|rr-xr-xr-x|0|0|1|1468708978|1468669380|1508354480|1468673899
|/img_Win10x64.000/Documents and Settings|90237|dr-xr-xr-x|0|0|48|1508351922|1508351922|1508351922|1508351922
```

=(G2/86400)+25569+(2/24)

Bodyfile

https://github.com/keydet89/Tools

Símbolo del sistema

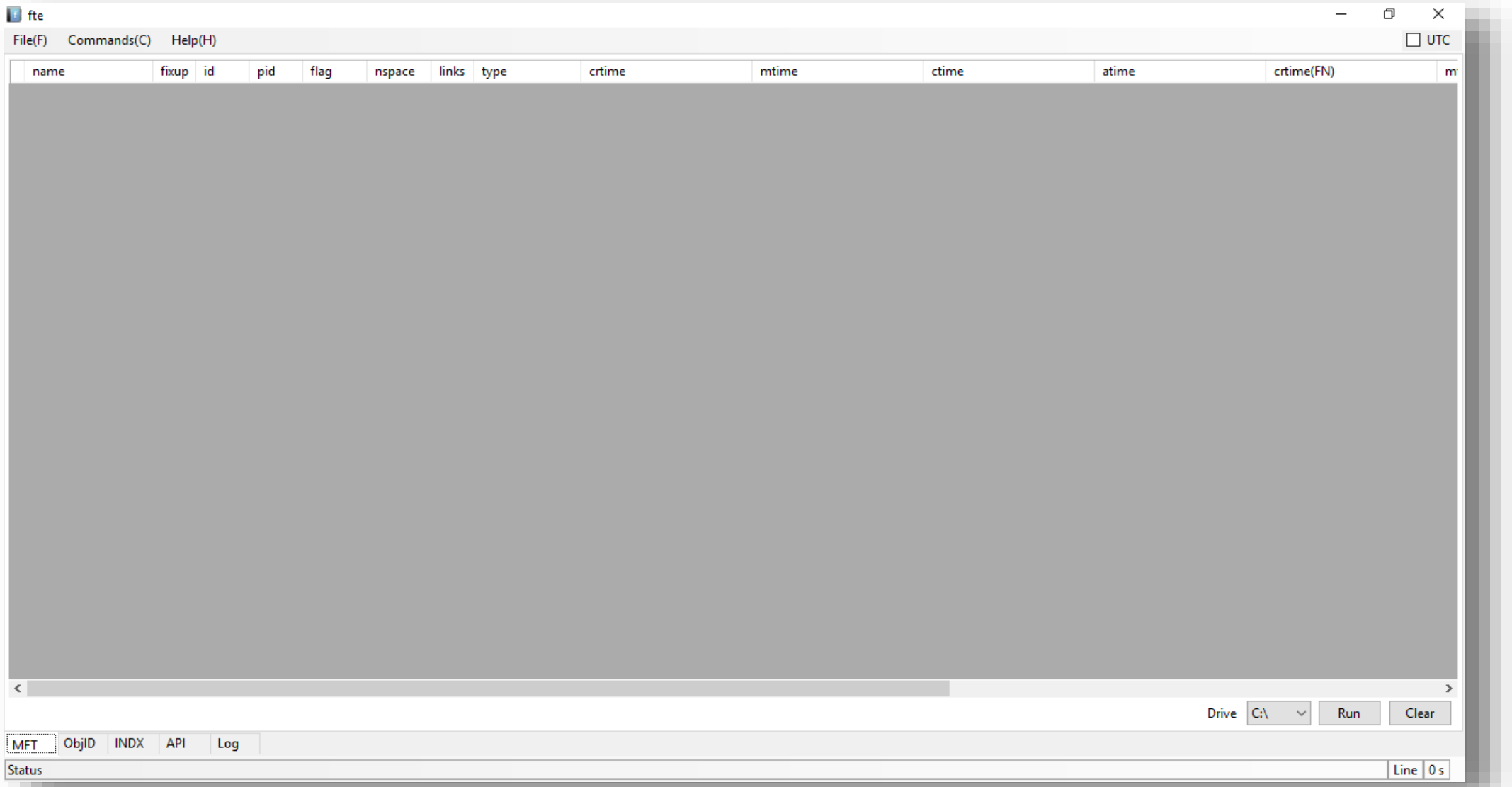
```
C:\Users\Marcos>"C:\Users\Marcos\Desktop\#HoneyCON18\Tools\Tools\exe\bodyfile.exe" -f "C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Autopsy\Win10x64_BodyFile.txt" >> "C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Bodyfile\Win10x64_BodyFile.txt"
```

```
1508354468|FILE|||MACB [656] /img_Win10x64.000/$Extend
1508354469|FILE|||MACB [48] /img_Win10x64.000/$Extend/$Deleted
1508354469|FILE|||MACB [0] /img_Win10x64.000/$Extend/$ObjId
1508354469|FILE|||MACB [0] /img_Win10x64.000/$Extend/$Quota
1508354469|FILE|||MACB [0] /img_Win10x64.000/$Extend/$Reparse
1508354469|FILE|||MACB [336] /img_Win10x64.000/$Extend/$RmMetadata
1508354469|FILE|||MACB [0] /img_Win10x64.000/$Extend/$RmMetadata/$Repair
1508354469|FILE|||MACB [8] /img_Win10x64.000/$Extend/$RmMetadata/$Repair:$Config
1508354469|FILE|||MACB [8388608] /img_Win10x64.000/$Extend/$RmMetadata/$Repair:$Corrupt
1508354469|FILE|||MACB [1048576] /img_Win10x64.000/$Extend/$RmMetadata/$Repair:$Verify
1508354469|FILE|||MACB [48] /img_Win10x64.000/$Extend/$RmMetadata/$Txf
1508354470|FILE|||MAC. [568] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog
1508354469|FILE|||...B [568] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog
1508354469|FILE|||MACB [100] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$Tops
1508354469|FILE|||MACB [1048576] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$Tops:$T
1508531211|FILE|||M.C. [65536] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$TxfLog.blf
1508354470|FILE|||.A.B [65536] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$TxfLog.blf
1508531211|FILE|||M.C. [10485760] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$TxfLogContainer00000000000000000001
1508354470|FILE|||.A.B [10485760] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$TxfLogContainer00000000000000000001
1508355258|FILE|||M.C. [10485760] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$TxfLogContainer00000000000000000002
1508354470|FILE|||.A.B [10485760] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$TxfLogContainer00000000000000000002
1508351678|FILE|||MACB [9819416] /img_Win10x64.000/$Extend/$UsnJrnl:$J
1508351678|FILE|||MACB [32] /img_Win10x64.000/$Extend/$UsnJrnl:$Max
1508354468|FILE|||MACB [29868032] /img_Win10x64.000/$LogFile
1508354468|FILE|||MACB [96731136] /img_Win10x64.000/$MFT
1508354468|FILE|||MACB [4096] /img_Win10x64.000/$MFTMirr
1508531170|FILE|||MAC. [608] /img_Win10x64.000/$Recycle.Bin
1468669667|FILE|||...B [608] /img_Win10x64.000/$Recycle.Bin
1508531170|FILE|||MAC. [152] /img_Win10x64.000/$Recycle.Bin/S-1-5-21-3930698692-3150784357-1811628781-1000
1508352359|FILE|||...B [152] /img_Win10x64.000/$Recycle.Bin/S-1-5-21-3930698692-3150784357-1811628781-1000
1508352359|FILE|||MACB [129] /img_Win10x64.000/$Recycle.Bin/S-1-5-21-3930698692-3150784357-1811628781-1000/desktop.ini
1508531170|FILE|||MAC. [152] /img_Win10x64.000/$Recycle.Bin/S-1-5-21-3930698692-3150784357-1811628781-1001
1508352394|FILE|||...B [152] /img_Win10x64.000/$Recycle.Bin/S-1-5-21-3930698692-3150784357-1811628781-1001
1508352394|FILE|||MACB [129] /img_Win10x64.000/$Recycle.Bin/S-1-5-21-3930698692-3150784357-1811628781-1001/desktop.ini
1508354468|FILE|||MACB [1027440] /img_Win10x64.000/$Secure:$SDS
1508354468|FILE|||MACB [131072] /img_Win10x64.000/$UpCase
```

Abre un archivo generado por 'fls.exe‘ y lo traduce al formato de Timeline de 5 campos

fte

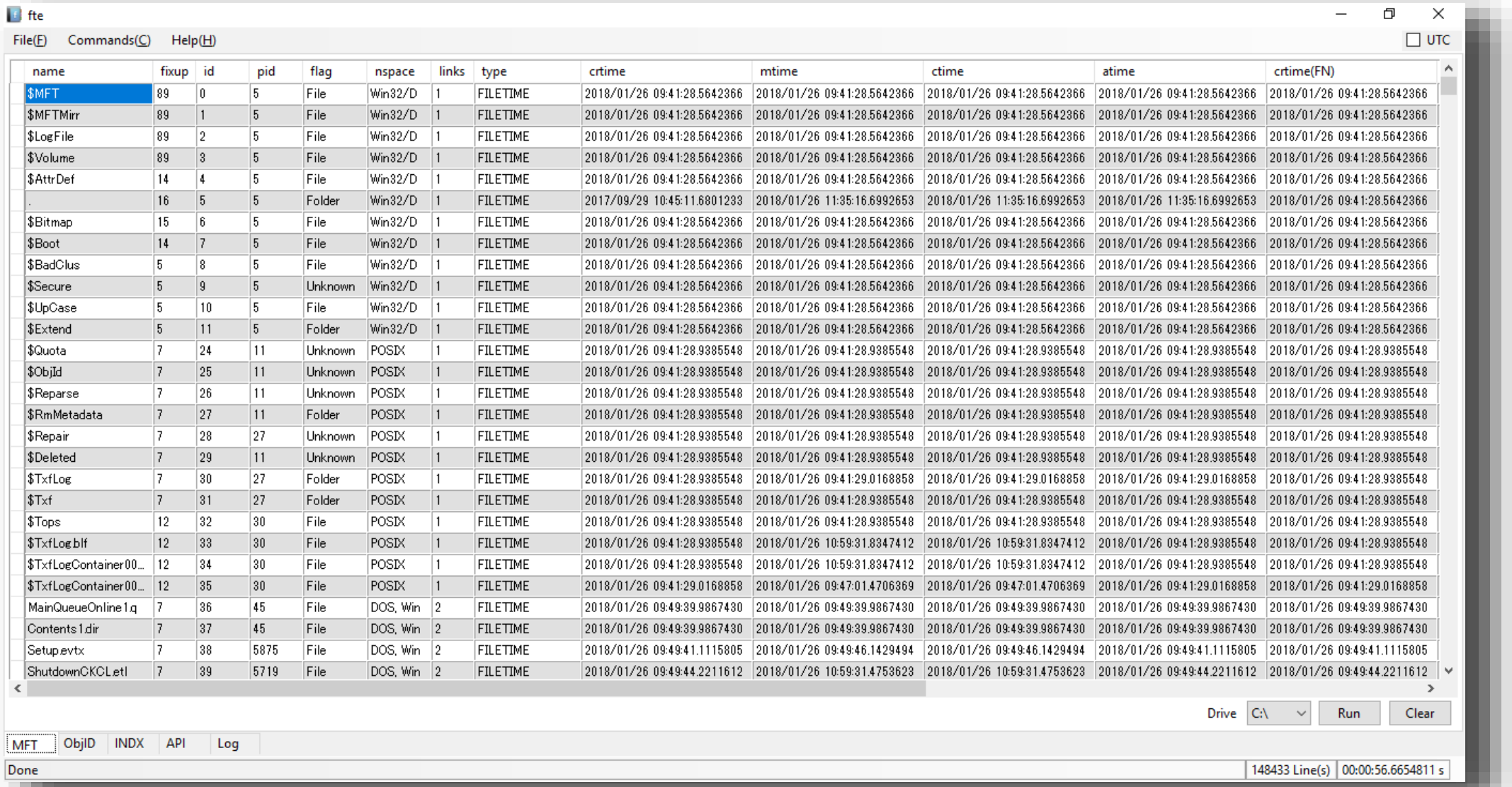
https://www.kazamiya.net/fte



Obtiene, del fichero 'MFT', marcas de tiempo precisas y varias informaciones sobre NTFS

fte

https://www.kazamiya.net/fte



name	fixup	id	pid	flag	nspace	links	type	crtime	mtime	ctime	atime	crtime(FN)
$MFT	89	0	5	File	Win32/D	1	FILETIME	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366
$MFTMirr	89	1	5	File	Win32/D	1	FILETIME	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366
$LogFile	89	2	5	File	Win32/D	1	FILETIME	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366
$Volume	89	3	5	File	Win32/D	1	FILETIME	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366
$AttrDef	14	4	5	File	Win32/D	1	FILETIME	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366
.	16	5	5	Folder	Win32/D	1	FILETIME	2017/09/29 10:45:11.6801233	2018/01/26 11:35:16.6992653	2018/01/26 11:35:16.6992653	2018/01/26 11:35:16.6992653	2018/01/26 09:41:28.5642366
$Bitmap	15	6	5	File	Win32/D	1	FILETIME	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366
$Boot	14	7	5	File	Win32/D	1	FILETIME	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366
$BadClus	5	8	5	File	Win32/D	1	FILETIME	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366
$Secure	5	9	5	Unknown	Win32/D	1	FILETIME	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366
$UpCase	5	10	5	File	Win32/D	1	FILETIME	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366
$Extend	5	11	5	Folder	Win32/D	1	FILETIME	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366	2018/01/26 09:41:28.5642366
$Quota	7	24	11	Unknown	POSIX	1	FILETIME	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548
$ObjId	7	25	11	Unknown	POSIX	1	FILETIME	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548
$Reparse	7	26	11	Unknown	POSIX	1	FILETIME	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548
$RmMetadata	7	27	11	Folder	POSIX	1	FILETIME	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548
$Repair	7	28	27	Unknown	POSIX	1	FILETIME	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548
$Deleted	7	29	11	Unknown	POSIX	1	FILETIME	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548
$TxfLog	7	30	27	Folder	POSIX	1	FILETIME	2018/01/26 09:41:28.9385548	2018/01/26 09:41:29.0168858	2018/01/26 09:41:29.0168858	2018/01/26 09:41:29.0168858	2018/01/26 09:41:28.9385548
$Txf	7	31	27	Folder	POSIX	1	FILETIME	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548
$Tops	12	32	30	File	POSIX	1	FILETIME	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548
$TxfLog.blf	12	33	30	File	POSIX	1	FILETIME	2018/01/26 09:41:28.9385548	2018/01/26 10:59:31.8347412	2018/01/26 10:59:31.8347412	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548
$TxfLogContainer00...	12	34	30	File	POSIX	1	FILETIME	2018/01/26 09:41:28.9385548	2018/01/26 10:59:31.8347412	2018/01/26 10:59:31.8347412	2018/01/26 09:41:28.9385548	2018/01/26 09:41:28.9385548
$TxfLogContainer00...	12	35	30	File	POSIX	1	FILETIME	2018/01/26 09:41:29.0168858	2018/01/26 09:47:01.4706369	2018/01/26 09:47:01.4706369	2018/01/26 09:41:29.0168858	2018/01/26 09:41:29.0168858
MainQueueOnline1.q	7	36	45	File	DOS, Win	2	FILETIME	2018/01/26 09:49:39.9867430	2018/01/26 09:49:39.9867430	2018/01/26 09:49:39.9867430	2018/01/26 09:49:39.9867430	2018/01/26 09:49:39.9867430
Contents1.dir	7	37	45	File	DOS, Win	2	FILETIME	2018/01/26 09:49:39.9867430	2018/01/26 09:49:39.9867430	2018/01/26 09:49:39.9867430	2018/01/26 09:49:39.9867430	2018/01/26 09:49:39.9867430
Setup.evtx	7	38	5875	File	DOS, Win	2	FILETIME	2018/01/26 09:49:41.1115805	2018/01/26 09:49:46.1429494	2018/01/26 09:49:46.1429494	2018/01/26 09:49:41.1115805	2018/01/26 09:49:41.1115805
ShutdownCKCL.etl	7	39	5719	File	DOS, Win	2	FILETIME	2018/01/26 09:49:44.2211612	2018/01/26 10:59:31.4753623	2018/01/26 10:59:31.4753623	2018/01/26 09:49:44.2211612	2018/01/26 09:49:44.2211612

Obtiene, del fichero 'MFT', marcas de tiempo precisas y varias informaciones sobre NTFS

fte

https://www.kazamiya.net/fte

```
name|fixup|id|pid|flag|nspace|links|type|crtime|mtime|ctime|atime|crtime(FN)|mtime(FN)|ctime(FN)|atime(FN)|remark
$MFT|89|0|5|File|Win32/DOS|1|FILETIME|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26
09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
$MFTMirr|89|1|5|File|Win32/DOS|1|FILETIME|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26
09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
$LogFile|89|2|5|File|Win32/DOS|1|FILETIME|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26
09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
$Volume|89|3|5|File|Win32/DOS|1|FILETIME|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26
09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
$AttrDef|14|4|5|File|Win32/DOS|1|FILETIME|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26
09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
.|16|5|5|Folder|Win32/DOS|1|FILETIME|2017/09/29 10:45:11.6801233|2018/01/26 11:35:16.6992653|2018/01/26 11:35:16.6992653|2018/01/26 11:35:16.6992653|2018/01/26
09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366| cr  <  fcr  =  fm  =  fc  =  fa  <  m  =  c  =  a
$Bitmap|15|6|5|File|Win32/DOS|1|FILETIME|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26
09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
$Boot|14|7|5|File|Win32/DOS|1|FILETIME|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26
09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
$BadClus|5|8|5|File|Win32/DOS|1|FILETIME|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26
09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
$Secure|5|9|5|Unknown|Win32/DOS|1|FILETIME|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26
09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
$UpCase|5|10|5|File|Win32/DOS|1|FILETIME|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26
09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
$Extend|5|11|5|Folder|Win32/DOS|1|FILETIME|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26
09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
$Quota|7|24|11|Unknown|POSIX|1|FILETIME|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26
09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
$ObjId|7|25|11|Unknown|POSIX|1|FILETIME|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26
09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
$Reparse|7|26|11|Unknown|POSIX|1|FILETIME|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26
09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
$RmMetadata|7|27|11|Folder|POSIX|1|FILETIME|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26
09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
$Repair|7|28|27|Unknown|POSIX|1|FILETIME|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26
09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
$Deleted|7|29|11|Unknown|POSIX|1|FILETIME|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26
09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
$TxfLog|7|30|27|Folder|POSIX|1|FILETIME|2018/01/26 09:41:28.9385548|2018/01/26 09:41:29.0168858|2018/01/26 09:41:29.0168858|2018/01/26 09:41:29.0168858|2018/01/26
09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548| cr  =  fcr  =  fm  =  fc  =  fa  <  m  =  c  =  a
$Txf|7|31|27|Folder|POSIX|1|FILETIME|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26
09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
$Tops|12|32|30|File|POSIX|1|FILETIME|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26
09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548|2018/01/26 09:41:28.9385548| cr  =  m  =  c  =  a  =  fcr  =  fm  =  fc  =  fa
```

Obtiene, del fichero ‘MFT’, marcas de tiempo precisas y varias informaciones sobre NTFS

fte

https://www.kazamiya.net/fte

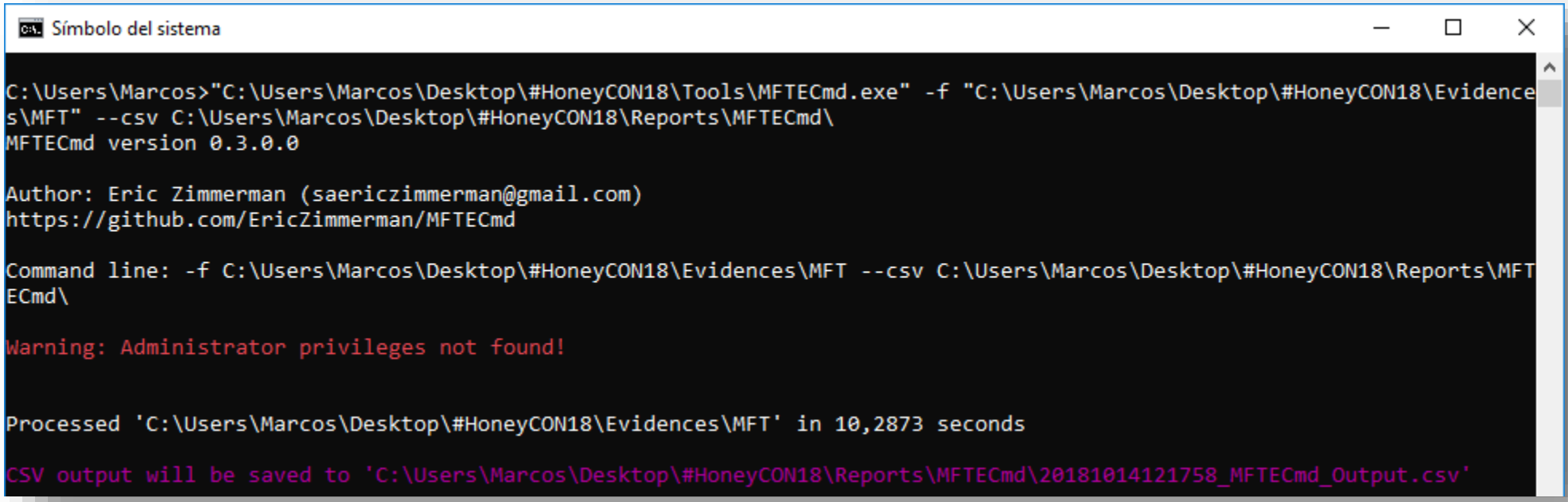
```
name|fixup|id|pid|flag|nspace|links|type|crtime|mtime|ctime|atime|crtime(FN)|mtime(FN)|ctime(FN)|atime(FN)|remark
$MFT|89|0|5|File|Win32/DOS|1|FILETIME|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26
09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366| cr = m = c = a = fcr = fm = fc = fa
$MFTMirr|89|1|5|File|Win32/DOS|1|FILETIME|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26
09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366| cr = m = c = a = fcr = fm = fc = fa
$LogFile|89|2|5|File|Win32/DOS|1|FILETIME|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26
09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366| cr = m = c = a = fcr = fm = fc = fa
$Volume|89|3|5|File|Win32/DOS|1|FILETIME|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26
09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366| cr = m = c = a = fcr = fm = fc = fa
$AttrDef|14|4|5|File|Win32/DOS|1|FILETIME|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26 09:41:28.5642366|2018/01/26
```

	A	B	C	D	E	F	G	H	I	J
1	name	fixup	id	pid	flag	nspace	links	type	crtime	mtime
2	css	5	796	795	Folder	Win32/DOS	1	FILETIME	2017/09/30 16:44:28.1043331	2017/09/30 16:44
3	amd64_microsoft-windows-e..-protocol-host-peer_31bf3856ad364e35_10.0.16299.15_none_	9	9216	6704	Folder	DOS, Win32	2	FILETIME	2017/09/29 15:42:06.7512504	2017/09/29 15:42
4	amd64_microsoft-windows-m..nsettings.resources_31bf3856ad364e35_10.0.16299.15_es-es_	7	10801	6704	Folder	DOS, Win32	2	FILETIME	2017/09/30 16:40:22.5355543	2017/09/30 16:40
5	amd64_microsoft-windows-w..cywmdmapi.resources_31bf3856ad364e35_10.0.16299.15_es-	7	13710	6704	Folder	DOS, Win32	2	FILETIME	2017/09/30 16:40:18.6815117	2017/09/30 16:40
6	wow64_adobe-flash-for-windows_31bf3856ad364e35_10.0.16299.15_none_58e0ba4b0f14c8	6	16762	6704	Folder	DOS, Win32	2	FILETIME	2017/09/29 15:41:23.1071072	2017/09/29 15:41
7	TIPRES~1.MUI	2	21512	13231	File	DOS	3	FILETIME	2017/09/29 15:41:54.0939790	2017/09/29 15:41
8	AppxBlockMap.xml	4	22568	2397	File	POSIX	2	FILETIME	2017/09/30 16:43:54.1954557	2017/09/30 16:43
9	Undo.png	4	23704	458	File	POSIX	2	FILETIME	2017/09/30 16:45:52.1371518	2017/09/30 16:45
10	RoundedFreehand3D.mp4	4	23875	475	File	POSIX	2	FILETIME	2017/09/30 16:45:52.4591640	2017/09/30 16:45
11	OneConnectAppList.scale-100.png	4	24916	2631	File	POSIX	2	FILETIME	2017/09/30 16:43:17.6332049	2017/09/30 16:43
12	SkypeMedTile.scale-125_contrast-white.png	4	25376	2693	File	POSIX	2	FILETIME	2017/09/30 16:43:24.7868738	2017/09/30 16:43
13	MSFT_PackageManagementSource.strings.psd1	3	31049	14253	File	DOS, Win32	2	FILETIME	2017/09/30 16:40:11.5644648	2017/09/30 16:40
14	resource.xml	3	31450	11663	File	POSIX	2	FILETIME	2017/09/30 16:40:12.3664717	2017/09/30 16:40
15	bootmgr.efi.mui	2	32145	1953	File	POSIX	3	FILETIME	2017/09/29 15:41:52.9376348	2017/09/29 15:41
16	MICROS~1.DLL	3	34547	14719	File	DOS	3	FILETIME	2017/09/30 16:40:19.7265163	2017/09/30 16:40
17	SYSTEM~1.DLL	2	35249	16415	File	DOS	3	FILETIME	2017/09/29 15:43:08.2093248	2017/09/29 15:43
18	CbsMsg.dll.mui	3	37139	4526	File	POSIX	3	FILETIME	2017/09/30 16:40:04.9953960	2017/09/30 16:40
19	shutdown.exe	5	44179	4559	File	Win32/DOS	2	FILETIME	2017/09/29 15:41:45.8901923	2017/09/29 15:41
20	WinSyncProviders.dll	2	45044	4559	File	POSIX	3	FILETIME	2017/09/29 15:41:44.6400918	2017/09/29 15:41
21	Wwanpref.dll	4	45255	4559	File	POSIX	2	FILETIME	2017/09/29 15:42:08.1576131	2017/09/29 15:42
22	spaceport.sys.mui	3	46227	15541	File	Win32	3	FILETIME	2017/09/30 16:40:05.8994028	2017/09/30 16:40
23	CNBXAQPIPELINECONFIG.XML	3	47237	5132	File	POSIX	3	FILETIME	2017/09/29 15:41:05.1369092	2017/09/29 15:41
24	hpbxmmw81.gpd	2	47615	5149	File	POSIX	3	FILETIME	2017/09/29 15:41:07.0901924	2017/09/29 15:41
25	CheckNetIsolation.exe.mui	3	48715	5399	File	POSIX	5	FILETIME	2017/09/30 16:40:10.6344322	2017/09/30 16:40

Obtiene, del fichero ‘MFT’, marcas de tiempo precisas y varias informaciones sobre NTFS

MFTECmd

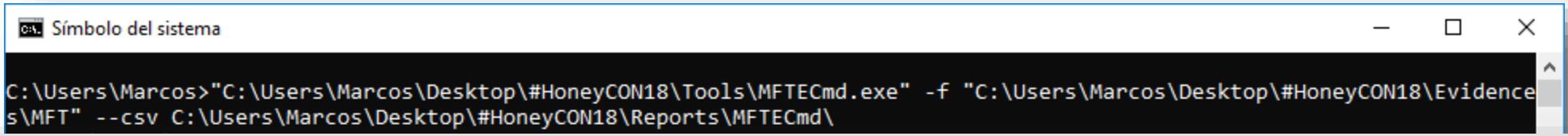
https://ericzimmerman.github.io/



Parsea, en línea de comandos, el fichero ‘MFT’ y puede exportar directamente en ‘.csv’

MFTECmd

https://ericzimmerman.github.io/



	A
1	EntryNumber,SequenceNumber,InUse,ParentEntryNumber,ParentSequenceNumber,ParentPath,FileName,Extension,FileSize,ReferenceCount,ReparseTarget,IsDirectory,HasAds,IsAds,SI<FN,uSecZeros,Copied,SiFl
2	0,1,True,5,5,.,$MFT,,94109696,1,,False,False,False,False,False,False,Hidden|System,DosWindows,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,
3	1,1,True,5,5,.,$MFTMirr,,4096,1,,False,False,False,False,False,False,Hidden|System,DosWindows,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,
4	2,2,True,5,5,.,$LogFile,,23085056,1,,False,False,False,False,False,False,Hidden|System,DosWindows,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.56423
5	3,3,True,5,5,.,$Volume,,0,1,,False,False,False,False,False,False,Hidden|System,DosWindows,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,0,1(
6	4,4,True,5,5,.,$AttrDef,,2560,1,,False,False,False,False,False,False,Hidden|System,DosWindows,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,(
7	5,5,True,5,5,.,.,,0,1,,True,False,False,True,False,False,Hidden|System,DosWindows,2017-09-29 08:45:11.6801233,2018-01-26 08:41:28.5642366,2018-01-26 10:35:16.6992653,2018-01-26 08:41:28.5642366,2018-01-26 10:3
8	6,6,True,5,5,.,$Bitmap,,473888,1,,False,False,False,False,False,False,Hidden|System,DosWindows,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366
9	7,7,True,5,5,.,$Boot,,8192,1,,False,False,False,False,False,False,Hidden|System,DosWindows,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,0,0
10	8,8,True,5,5,.,$BadClus,,0,1,,False,True,False,False,False,False,Hidden|System,DosWindows,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,0,83
11	8,8,True,5,5,.,$BadClus:$Bad,,15528357888,1,,False,False,True,False,False,False,Hidden|System,DosWindows,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41
12	9,9,True,5,5,.,$Secure,,1382740,1,,False,True,False,False,False,False,Hidden|System|IsIndexView,DosWindows,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:
13	9,9,True,5,5,.,$Secure:$SDS,,1382740,1,,False,False,True,False,False,False,Hidden|System|IsIndexView,DosWindows,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-
14	10,10,True,5,5,.,$UpCase,,131072,1,,False,True,False,False,False,False,Hidden|System,DosWindows,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.56423
15	10,10,True,5,5,.,$UpCase:$Info,,32,1,,False,False,True,False,False,False,Hidden|System,DosWindows,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642
16	11,11,True,5,5,.,$Extend,,0,1,,True,False,False,False,False,False,Hidden|System,DosWindows,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,0,1
17	24,1,True,11,11,.\$Extend,$Quota,,0,1,,False,False,False,False,False,False,Hidden|System|Archive|IsIndexView,Posix,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01
18	25,1,True,11,11,.\$Extend,$ObjId,,0,1,,False,False,False,False,False,False,Hidden|System|Archive|IsIndexView,Posix,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01
19	26,1,True,11,11,.\$Extend,$Reparse,,0,1,,False,False,False,False,False,False,Hidden|System|Archive|IsIndexView,Posix,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-
20	27,1,True,11,11,.\$Extend,$RmMetadata,,0,1,,True,False,False,False,False,False,Hidden|System,Posix,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.938
21	28,1,True,27,1,.\$Extend\$RmMetadata,$Repair,,0,1,,False,True,False,False,False,False,Hidden|System|Archive,Posix,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01
22	28,1,True,27,1,.\$Extend\$RmMetadata,$Repair:$Config,,8,1,,False,False,True,False,False,False,Hidden|System|Archive,Posix,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,
23	28,1,True,27,1,.\$Extend\$RmMetadata,$Repair:$Corrupt,,8388608,1,,False,False,True,False,False,False,Hidden|System|Archive,Posix,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9
24	28,1,True,27,1,.\$Extend\$RmMetadata,$Repair:$Verify,,1048576,1,,False,False,True,False,False,False,Hidden|System|Archive,Posix,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.93
25	29,1,True,11,11,.\$Extend,$Deleted,,0,1,,True,False,False,False,False,False,Hidden|System,Posix,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,,2018-01-26 08:41:28.9385548,

Parsea, en línea de comandos, el fichero ‘MFT’ y puede exportar directamente en ‘.csv’

MFTECmd

https://ericzimmerman.github.io/

Símbolo del sistema

```
C:\Users\Marcos>"C:\Users\Marcos\Desktop\#HoneyCON18\Tools\MFTECmd.exe" -f "C:\Users\Marcos\Desktop\#HoneyCON18\Evidence
s\MFT" --csv C:\Users\Marcos\Desktop\#HoneyCON18\Reports\MFTECmd\
```

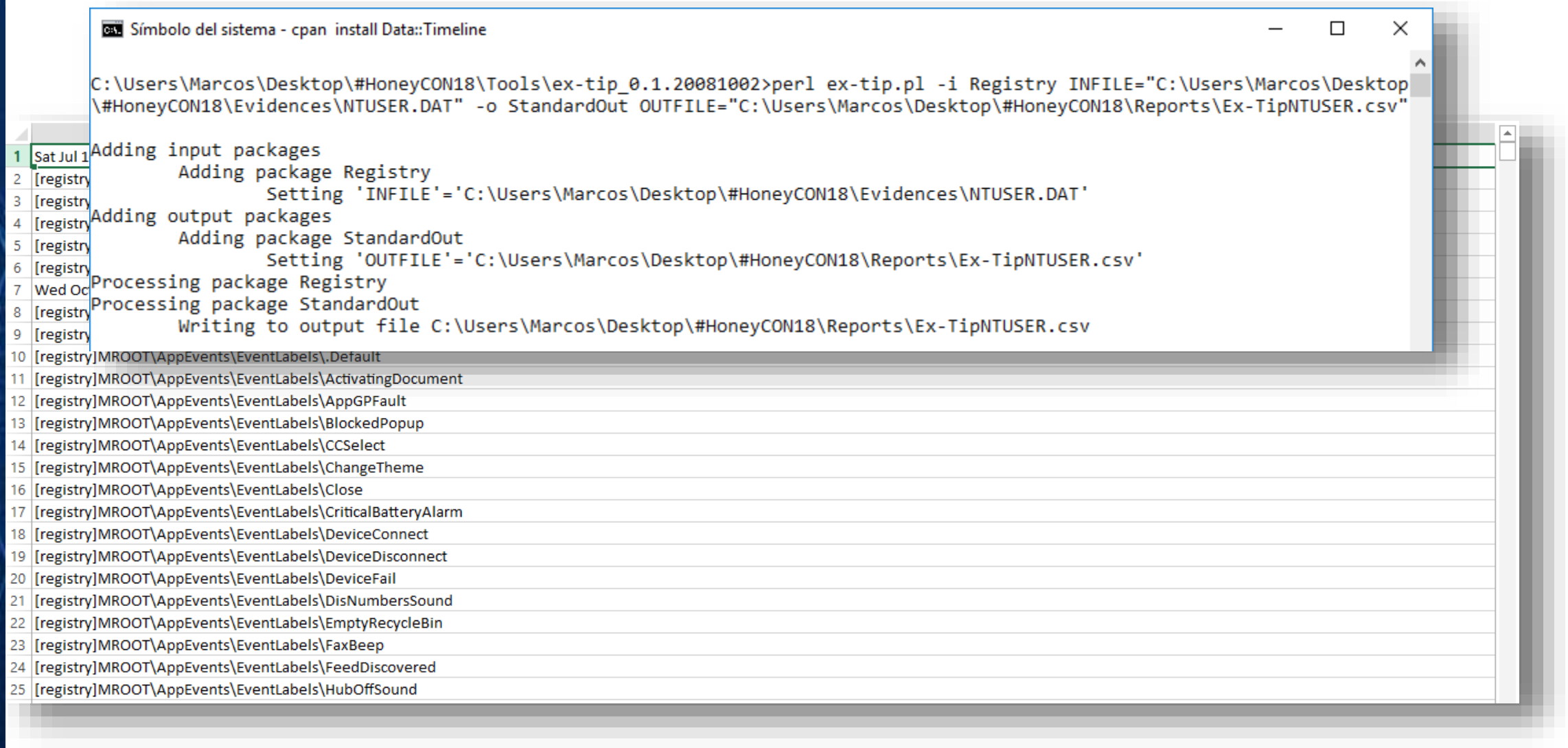
	A
1	EntryNumber,SequenceNumber,InUse,ParentEntryNumber,ParentSequenceNumber,ParentPath,FileName,Extension,FileSize,ReferenceCount,ReparseTarget,IsDirectory,HasAds,IsAds,SI<FN,uSecZeros,Copied,SiFl
2	0,1,True,5,5,.,$MFT,,94109696,1,,False,False,False,False,False,False,Hidden|System,DosWindows,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,,2018-01-26 08:41:28.5642366,

	A	B	C	D	E	F	
1	EntryNumber	SequenceNumber	InUse	ParentEntryNumber	ParentSequenceNumber	ParentPath	FileName
2	15847	1	True	6704	1	.\Windows\WinSxS	amd64_windows-id
3	22727	1	True	290	1	.\Program Files\WindowsApps\Microsoft.Messaging_3.32.15001.0_x64__8wekyb3d8bbwe\T	en-US.Messaging.cc
4	22931	1	True	330	1	.\Program Files\WindowsApps\DeletedAllUserPackages\Microsoft.MicrosoftSolitaireCollec	SplashScreen.scale-
5	27257	1	True	729	1	.\Program Files\WindowsApps\Microsoft.WindowsCamera_2017.727.20.0_x64__8wekyb3d8	WindowsCameraAp
6	30883	1	True	3186	1	.\Windows\InfusedApps\Packages\Microsoft.ZuneVideo_10.17063.24021.0_x64__8wekyb3d	FileExtension.targe
7	31192	1	True	1208	1	.\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Functions\Assertions	Contain.Tests.ps1
8	31639	1	True	1498	1	.\Users\Default\AppData\Local\Microsoft\Windows\WinX\Group3	04 - Disk Manageme
9	32201	1	True	1973	1	.\Windows\Boot\Fonts	msjh_boot.ttf
10	32508	1	True	10901	1	.\Windows\WinSxS\amd64_microsoft-windows-maintenancediagnostic_31bf3856ad364e35_	RS_UserDiagnosticH
11	33565	1	True	6959	1	.\Windows\WinSxS\amd64_dual_c_media.inf_31bf3856ad364e35_10.0.16299.15_none_8a89	c_media.inf
12	34153	1	True	15190	1	.\Windows\WinSxS\amd64_netfx4-_dataperfcounters_ini_b03f5f7f11d50a3a_4.0.15522.0_nc	_DataPerfCounters_
13	36255	1	True	14708	1	.\Windows\WinSxS\amd64_netfx4-legacy_web_h..rust_config_default_b03f5f7f11d50a3a_4	legacy.web_hightru
14	42166	1	True	4559	1	.\Windows\System32	drvstore.dll
15	43442	1	True	15900	1	.\Windows\WinSxS\amd64_windows.networking.vpn.nethost_31bf3856ad364e35_10.0.162	NetHost.exe
16	44340	1	True	13066	1	.\Windows\WinSxS\amd64_microsoft-windows-sxs-store_31bf3856ad364e35_10.0.16299.15	sxsstore.dll
17	44613	1	True	4559	1	.\Windows\System32	user32.dll
18	45495	1	True	19119	1	.\Windows\WinSxS\wow64_microsoft-windows-p..rgraphing.resources_31bf3856ad364e35_	p2p-mesh.mfl
19	47779	1	True	5174	1	.\Windows\System32\DriverStore\FileRepository\prnms005.inf_amd64_34c0896eae1bf8d0\	MSxpsPCL6-pipelin
20	48343	1	True	14324	1	.\Windows\WinSxS\amd64_microsoft.windows.c..-controls.resources_6595b64144ccf1df_5.	comctl32.dll.mui
21	50416	1	True	17750	1	.\Windows\WinSxS\wow64_microsoft-windows-font-fms.resources_31bf3856ad364e35_10.	fms.dll.mui
22	51378	1	True	21009	1	.\Windows\WinSxS\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_5.82.	comctl32.dll.mui
23	54712	1	True	5938	1	.\Windows\SystemApps\Microsoft.Windows.AddSuggestedFoldersToLibraryDialog_cw5n1h	AppxBlockMap.xml
24	58278	1	True	18857	1	.\Windows\WinSxS\wow64_microsoft-windows-msvcp110_31bf3856ad364e35_10.0.16299.1	msvcp110_win.dll
25	58685	1	True	6232	1	.\Windows\SysWOW64	RpcRtRemote.dll

Parsea, en línea de comandos, el fichero 'MFT' y puede exportar directamente en '.csv'

ExTip

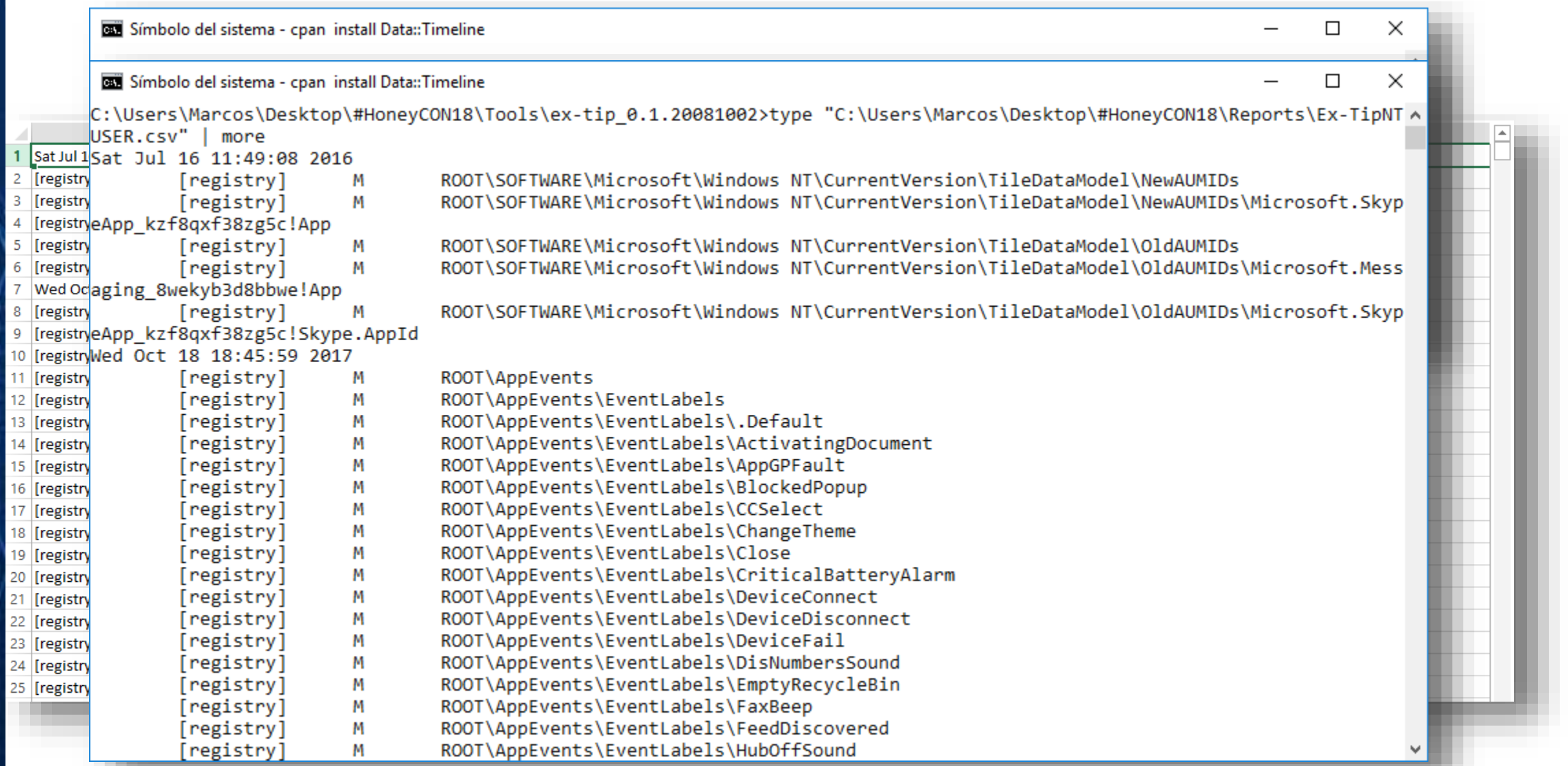
https://sourceforge.net/projects/ex-tip/



Prueba de concepto que emula la funcionalidad ‘mactime’, de TSK, sobre el Registro

ExTip

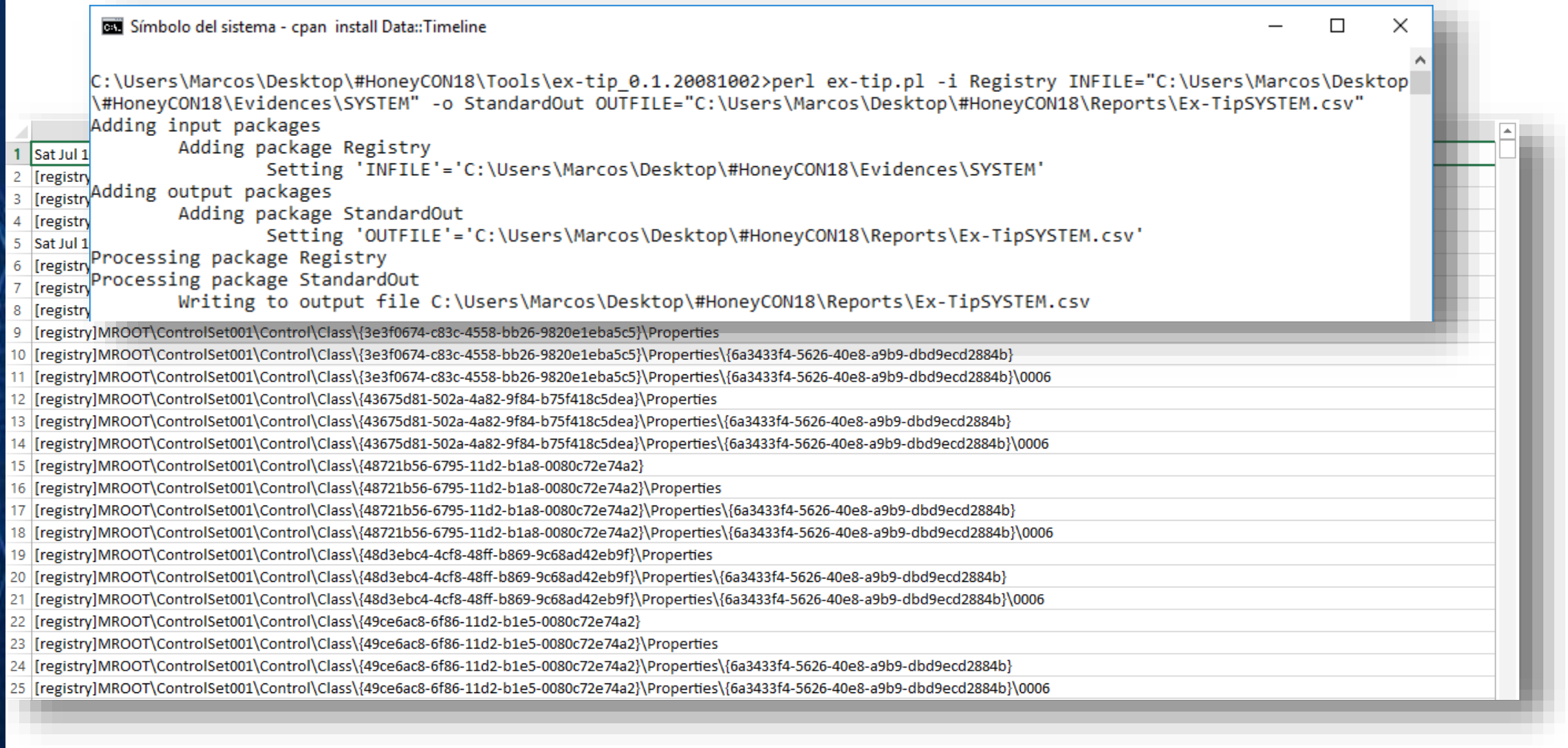
https://sourceforge.net/projects/ex-tip/



Prueba de concepto que emula la funcionalidad ‘mactime’, de TSK, sobre el Registro

ExTip

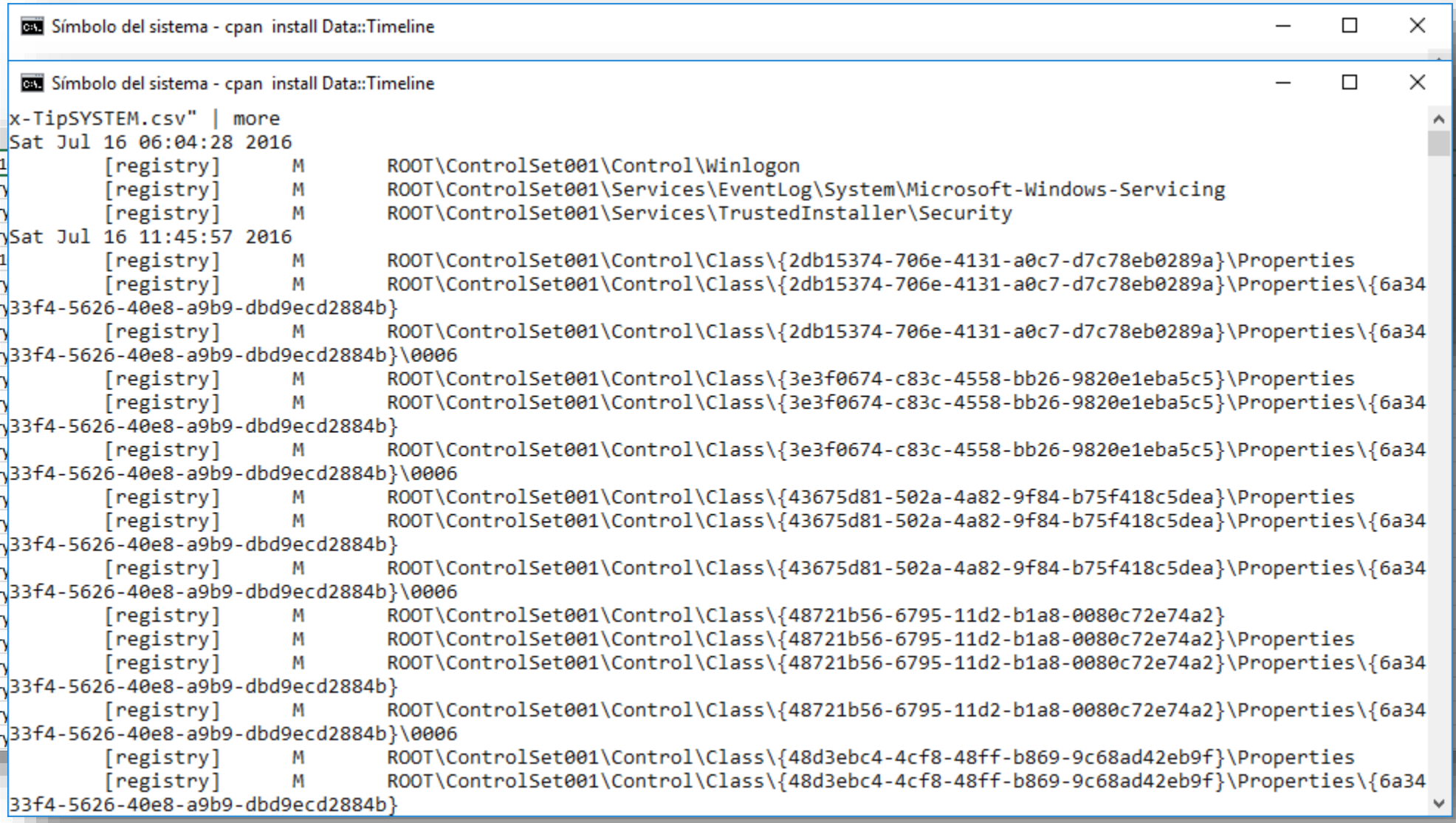
https://sourceforge.net/projects/ex-tip/



Prueba de concepto que emula la funcionalidad ‘mactime’, de TSK, sobre el Registro

ExTip

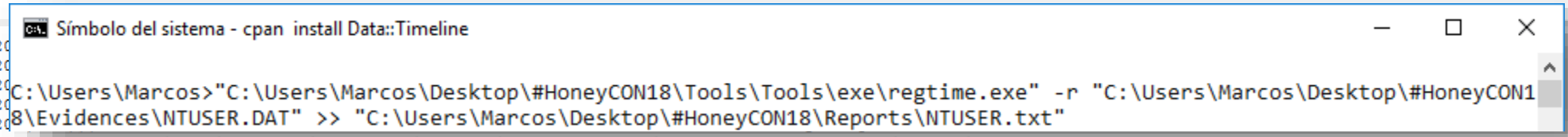
https://sourceforge.net/projects/ex-tip/



Prueba de concepto que emula la funcionalidad ‘mactime’, de TSK, sobre el Registro

Regtime

https://github.com/keydet89/Tools

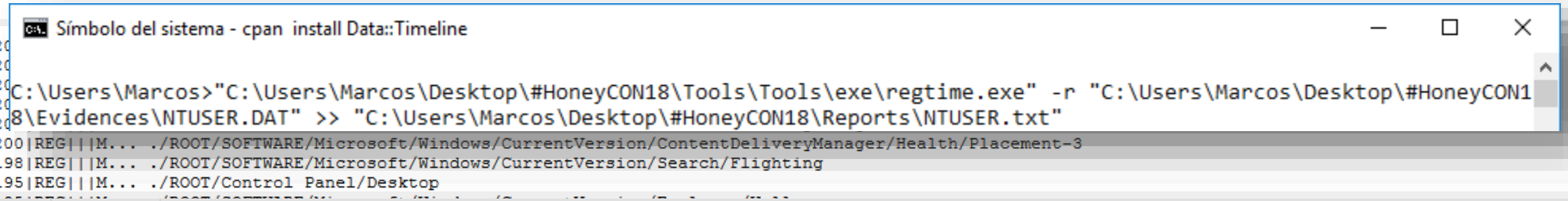



```
1508531200|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/ContentDeliveryManager/Health/Placement-3
1508531198|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Search/Flighting
1508531195|REG|||M... ./ROOT/Control Panel/Desktop
1508531195|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/Wallpapers
1508531192|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows NT/CurrentVersion/AppCompatFlags/Compatibility Assistant/Store
1508531163|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/Connections
1508531163|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Search/RecentApps
1508531163|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Search/RecentApps/{14E94377-B8B5-4791-B791-731E3915B1E4}
1508531162|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Security and Maintenance/Checks/{852FB1F8-5CC6-4567-9C0E-7C330F8807C2}.check.100
1508531162|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Security and Maintenance/Checks/{852FB1F8-5CC6-4567-9C0E-7C330F8807C2}.check.101
1508531161|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/ContentDeliveryManager/Health/Placement-10
1508531160|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer
1508531159|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/ContentDeliveryManager/Health/Placement-1
1508531156|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/Modules/NavPane
1508531152|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Search
1508531149|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows NT/CurrentVersion/Devices
1508531149|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows NT/CurrentVersion/PrinterPorts
1508531146|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/UserAssist/{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}/Count
1508531146|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Search/RecentApps/{C47CB463-C976-4256-8F2A-074500315F7A}
1508531144|REG|||M... ./ROOT/SOFTWARE/Piriform/CCleaner
1508531138|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/FileExts
1508531133|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/CIDSizeMRU
1508531130|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32
1508531130|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/LastVisitedPidlMRULegacy
1508531103|REG|||M... ./ROOT/SOFTWARE/Microsoft/Internet Explorer
1508531103|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/RecentDocs
1508531074|REG|||M... ./ROOT/SOFTWARE/Microsoft/Internet Explorer/Main
1508531074|REG|||M... ./ROOT/SOFTWARE/Microsoft/Internet Explorer/Main/WindowsSearch
1508531074|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/5.0/Cache/Extensible Cache
1508531074|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows Search/ProcessedSearchRoots
1508531074|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows Search/ProcessedSearchRoots/0004
1508531055|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Run
1508531053|REG|||M... ./ROOT/SOFTWARE/Microsoft
1508531048|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Search/RecentApps/{4BD5D865-FBBF-4837-A12C-BDB4BDEF35A4}
1508531039|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/CD Burning/Drives/Volume{5ed1a5e8-b43b-11e7-9c07-806e6f6e6963}
1508531039|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/CD Burning/StagingInfo/Volume{5ed1a5e8-b43b-11e7-9c07-806e6f6e6963}
1508531039|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/HomeGroup
1508531029|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/PushNotifications
```

Analiza uno, o varios, archivos del Registro y genera una línea de tiempo en formato 'TLN'

Regtime

https://github.com/keydet89/Tools



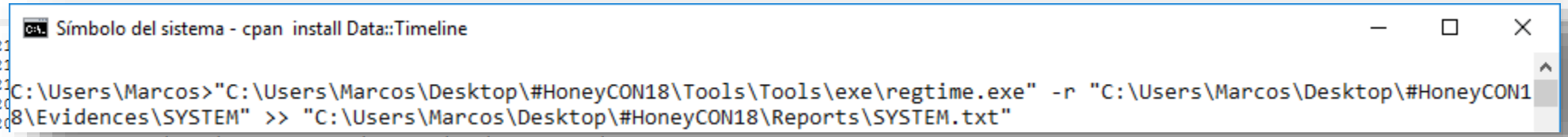

```
1508531200|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/ContentDeliveryManager/Health/Placement-3
1508531198|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Search/Flighting
1508531195|REG|||M... ./ROOT/Control Panel/Desktop
```

	A	B	C
1	Columna1	Columna2	Columna5
2	1508353227	REG	M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Authentication/LogonUI/Notifications/BackgroundCapability/S-1-15-2-1288279408-4010470124-2163985056-447644096-19460
3	1508352375	REG	M... ./ROOT/AppEvents/Schemes/Apps/.Default/CriticalBatteryAlarm/.Current
4	1508352381	REG	M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/FileExts/.gif/UserChoice
5	1508352359	REG	M... ./ROOT/AppEvents/Schemes/Apps/.Default/Notification.Looping.Call2
6	1508353304	REG	M... ./ROOT/SOFTWARE/Microsoft/Unified Store
7	1508352381	REG	M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/FileExts/.swf/OpenWithList
8	1508352359	REG	M... ./ROOT/SOFTWARE/Microsoft/CTF/SortOrder/AssemblyItem
9	1508352370	REG	M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/DeviceAccess/Global/{E5323777-F976-4f5b-9B55-B94699C46E44}
10	1508352381	REG	M... ./ROOT/SOFTWARE/Microsoft/Windows/Roaming/OpenWith/FileExts/.orf
11	1508353238	REG	M... ./ROOT/SOFTWARE/Policies/Microsoft/SystemCertificates/Disallowed/CRLs
12	1508352387	REG	M... ./ROOT/SOFTWARE/Microsoft/Speech_OneCore/Isolated/ohDO1Sgy3MzgdEgEb4WYfDS4eikKwN2EBJ1Cyr7HTF0/HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Speech_OneCore/Spee
13	1508352376	REG	M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/DeviceAccess/S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194
14	1508531025	REG	M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/BackgroundAccessApplications/Microsoft.XboxIdentityProvider_8wekyb3d8bbwe
15	1508353307	REG	M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Security and Maintenance/Checks/{2374911B-B114-42FE-900D-54F95FEE92E5}.check.100
16	1508352381	REG	M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/FileExts/.amr/UserChoice
17	1508352359	REG	M... ./ROOT/AppEvents/Schemes/Apps/.Default/Notification.Looping.Alarm10/.Current
18	1508352371	REG	M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/UserAssist/{B267E3AD-A825-4A09-82B9-EEC22AA3B847}/Count
19	1508352381	REG	M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/FileExts/.png
20	1508352359	REG	M... ./ROOT/Control Panel/PowerCfg/PowerPolicies/3
21	1508353239	REG	M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Authentication/LogonUI/Notifications/BackgroundCapability/S-1-15-2-2246530975-808720366-1776470054-230329187-415322
22	1508352374	REG	M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Authentication/LogonUI/Notifications/BackgroundCapability/S-1-15-2-1861897761-1695161497-2927542615-642690995-32784
23	1508352381	REG	M... ./ROOT/SOFTWARE/Microsoft/Windows/Roaming/OpenWith/FileExts/.mkv
24	1508352359	REG	M... ./ROOT/SOFTWARE/Policies/Power/PowerSettings
25	1508352377	REG	M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Authentication/LogonUI/Notifications/BackgroundCapability/S-1-15-2-350187224-1905355452-1037786396-3028148496-26241

Analiza uno, o varios, archivos del Registro y genera una línea de tiempo en formato 'TLN'

Regtime

https://github.com/keydet89/Tools

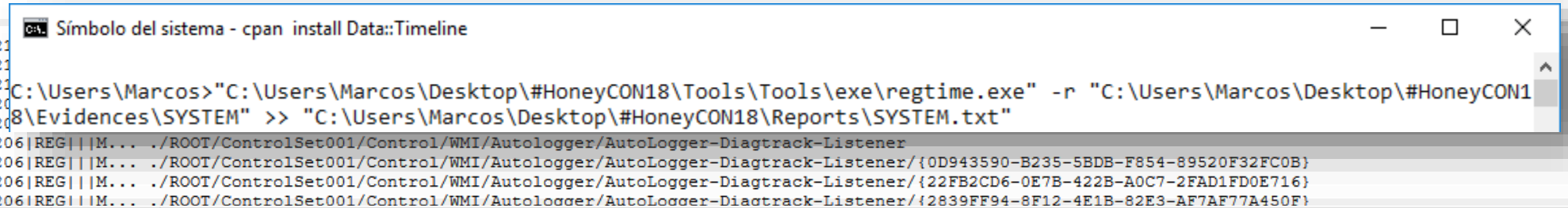



```
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener/{0D943590-B235-5BDB-F854-89520F32FC0B}
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener/{22FB2CD6-0E7B-422B-A0C7-2FAD1FD0E716}
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener/{2839FF94-8F12-4E1B-82E3-AF7AF77A450F}
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener/{331C3B3A-2005-44C2-AC5E-77220C37D6B4}
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener/{4F50731A-89CF-4782-B3E0-DCE8C90476BA}
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener/{53B78FC6-E359-453E-89FE-A5F4E5FF4AF3}
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener/{5ECB0BAC-B930-47F5-A8A4-E8253529EDB7}
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener/{96F4A050-7E31-453C-88BE-9634F4E02139}
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener/{976A8310-986E-4640-8BFB-7736EE6D9B65}
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener/{9DFC8457-4D69-44C7-8FCD-192290702A89}
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener/{A0B6BE33-B959-50C3-3C92-8451B6F965C3}
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener/{A19FDC69-A626-5289-BE4D-1F508A8C9A3B}
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener/{BA84F32B-8AF2-5006-F147-5030CDD7F22D}
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener/{DBE9B383-7CF3-4331-91CC-A3CB16A3B538}
1508531206|REG|||M... ./ROOT/ControlSet001/Enum/SWD/MSDAS/{ce958e9a-424f-4c88-86f4-11314821e75a}/Properties/{83da6326-97a6-4088-9453-a1923f573b29}/0067
1508531206|REG|||M... ./ROOT/ControlSet001/Services
1508531206|REG|||M... ./ROOT/ControlSet001/Services/Winmgmt/Parameters
1508531204|REG|||M... ./ROOT/ControlSet001/Control/Diagnostics/Performance
1508531192|REG|||M... ./ROOT/ControlSet001/Services/VSS/Diag
1508531183|REG|||M... ./ROOT/ControlSet001/Control/Session Manager
1508531173|REG|||M... ./ROOT/ControlSet001/Control/DeviceContainers/{00000000-0000-0000-FFFF-FFFFFFFFFFFF}/Properties/{3464f7a4-2444-40b1-980a-e0903cb6d912}/0008
1508531173|REG|||M... ./ROOT/ControlSet001/Control/DeviceContainers/{00000000-0000-0000-FFFF-FFFFFFFFFFFF}/Properties/{78c34fc8-104a-4aca-9ea4-524d52996e57}/0069
1508531173|REG|||M... ./ROOT/ControlSet001/Control/DeviceContainers/{0a568158-2954-f19c-89f3-03acaee1f85e}/Properties/{3464f7a4-2444-40b1-980a-e0903cb6d912}
1508531173|REG|||M... ./ROOT/ControlSet001/Control/DeviceContainers/{0a568158-2954-f19c-89f3-03acaee1f85e}/Properties/{3464f7a4-2444-40b1-980a-e0903cb6d912}/0008
1508531173|REG|||M... ./ROOT/ControlSet001/Control/DeviceContainers/{0a568158-2954-f19c-89f3-03acaee1f85e}/Properties/{78c34fc8-104a-4aca-9ea4-524d52996e57}/0069
1508531173|REG|||M... ./ROOT/ControlSet001/Control/DeviceContainers/{5ed1a5f0-b43b-11e7-9c07-806e6f6e6963}/Properties/{3464f7a4-2444-40b1-980a-e0903cb6d912}/0008
1508531173|REG|||M... ./ROOT/ControlSet001/Control/DeviceContainers/{5ed1a5f0-b43b-11e7-9c07-806e6f6e6963}/Properties/{78c34fc8-104a-4aca-9ea4-524d52996e57}/0069
1508531173|REG|||M... ./ROOT/ControlSet001/Control/DeviceContainers/{ca0e9e80-3e97-fcac-730a-8cb080fa2581}/Properties/{3464f7a4-2444-40b1-980a-e0903cb6d912}
1508531173|REG|||M... ./ROOT/ControlSet001/Control/DeviceContainers/{ca0e9e80-3e97-fcac-730a-8cb080fa2581}/Properties/{3464f7a4-2444-40b1-980a-e0903cb6d912}/0008
1508531173|REG|||M... ./ROOT/ControlSet001/Control/DeviceContainers/{ca0e9e80-3e97-fcac-730a-8cb080fa2581}/Properties/{78c34fc8-104a-4aca-9ea4-524d52996e57}/0069
1508531173|REG|||M... ./ROOT/ControlSet001/Control/DeviceContainers/{d397268a-724c-b4ef-d641-c9234ba2948b}/Properties/{3464f7a4-2444-40b1-980a-e0903cb6d912}
1508531173|REG|||M... ./ROOT/ControlSet001/Control/DeviceContainers/{d397268a-724c-b4ef-d641-c9234ba2948b}/Properties/{3464f7a4-2444-40b1-980a-e0903cb6d912}/0008
1508531173|REG|||M... ./ROOT/ControlSet001/Control/DeviceContainers/{d397268a-724c-b4ef-d641-c9234ba2948b}/Properties/{78c34fc8-104a-4aca-9ea4-524d52996e57}/0069
1508531173|REG|||M... ./ROOT/ControlSet001/Control/DeviceContainers/{ed17222b-f1c7-537f-9546-745658ade2e3}/Properties/{3464f7a4-2444-40b1-980a-e0903cb6d912}
1508531173|REG|||M... ./ROOT/ControlSet001/Control/DeviceContainers/{ed17222b-f1c7-537f-9546-745658ade2e3}/Properties/{3464f7a4-2444-40b1-980a-e0903cb6d912}/0008
1508531173|REG|||M... ./ROOT/ControlSet001/Control/DeviceContainers/{ed17222b-f1c7-537f-9546-745658ade2e3}/Properties/{78c34fc8-104a-4aca-9ea4-524d52996e57}/0069
1508531165|REG|||M... ./ROOT/ControlSet001/Services/awtojqiopxvsxgg941
```

Analiza uno, o varios, archivos del Registro y genera una línea de tiempo en formato 'TLN'

Regtime

https://github.com/keydet89/Tools



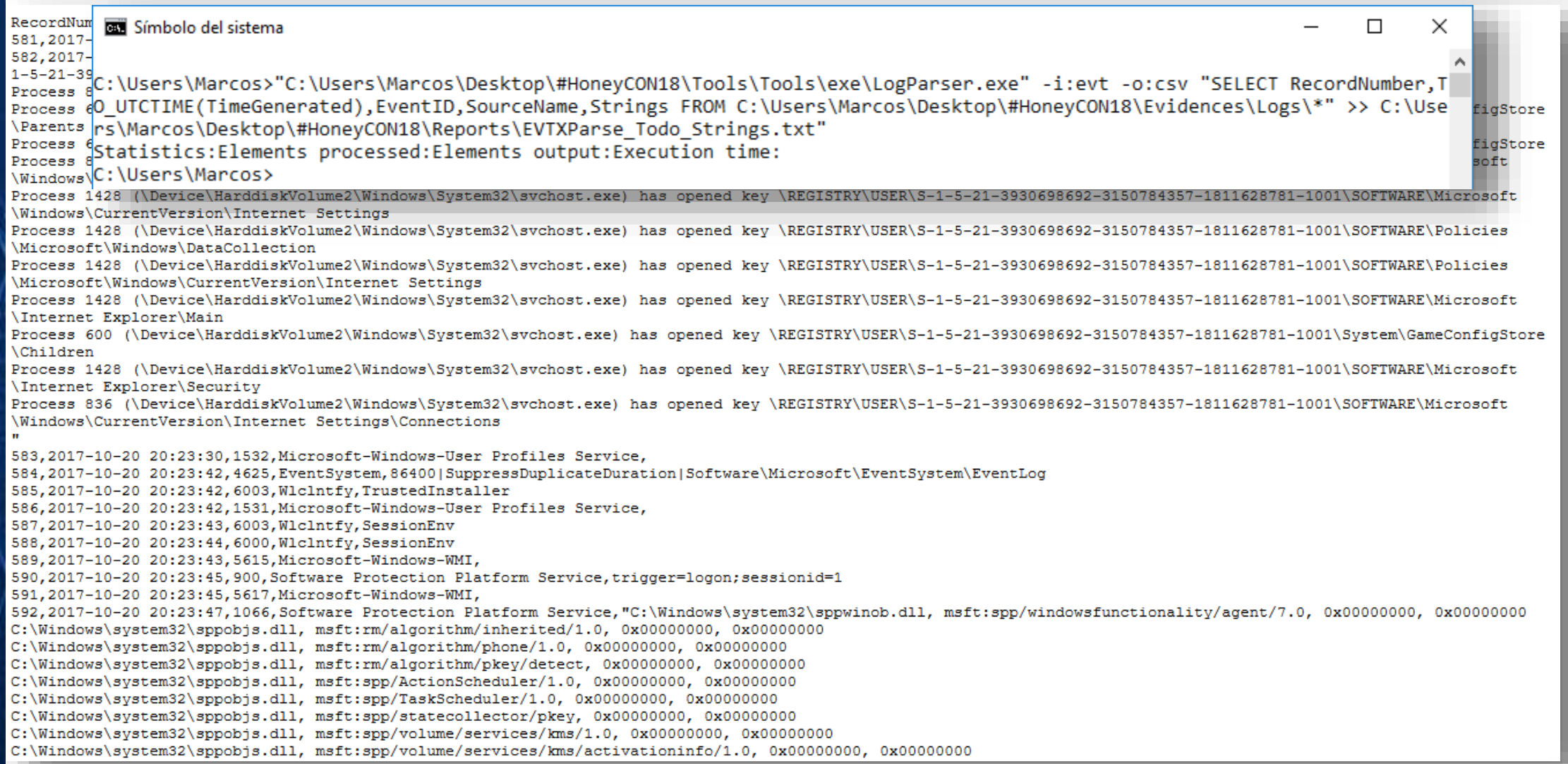

```
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener/{0D943590-B235-5BDB-F854-89520F32FC0B}
1508531206|REG|||M... ./ROOT/ControlSet001/Control/WMI/Autologger/AutoLogger-Diagtrack-Listener/{22FB2CD6-0E7B-422B-A0C7-2FAD1FD0E716}
```

	A	B	C
1	Columna1	Columna2	Columna5
2	1468669626	REG	M... ./ROOT/DriverDatabase/DeviceIds/PCI/VEN_103C&DEV_10ED
3	1468669709	REG	M... ./ROOT/ControlSet001/Control/Power/PowerSettings/F15576E8-98B7-4186-B944-EAFA664402D9/DefaultPowerSchemeValues
4	1468669657	REG	M... ./ROOT/DriverDatabase/DriverPackages/vsmraid.inf_amd64_3d2bbc45931b8232/Configurations/vsmraid/Services/vsmraid/Parameters
5	1468669646	REG	M... ./ROOT/DriverDatabase/DriverPackages/hidirkbd.inf_amd64_8c1605d359765877/Descriptors/HID/IrDeviceV2&COL05
6	1508351679	REG	M... ./ROOT/ControlSet001/Enum/USB/VID_80EE&PID_0021/5&18f54cb7&0&1/Properties/{80497100-8c73-48b9-aad9-ce387e19c56e}
7	1468669626	REG	M... ./ROOT/DriverDatabase/DeviceIds/PCI/VEN_1000&DEV_0091
8	1468669709	REG	M... ./ROOT/ControlSet001/Control/Power/PowerSettings/7516b95f-f776-4464-8c53-06167f40cc99/FBD9AA66-9553-4097-BA44-ED6E9D65EAB8/DefaultPowerSchemeValues/8c5e7fda-e8bf
9	1468669657	REG	M... ./ROOT/DriverDatabase/DriverPackages/ndisvirtualbus.inf_amd64_d43186f4226299a9/Descriptors/ROOT
10	1468669646	REG	M... ./ROOT/DriverDatabase/DriverInfFiles/compositebus.inf
11	1468669710	REG	M... ./ROOT/ControlSet001/Control/NetDiagFx/Microsoft/HostDLLs/WPPTrace/HelperClasses/wireless_dbg/Providers/{2DD11DE3-FDDE-4DA9-B57A-AF6585F74233}
12	1468669709	REG	M... ./ROOT/Setup/Service Reporting API/Baselines/2.0/1
13	1468669733	REG	M... ./ROOT/ControlSet001/Services/vmicvmsession/TriggerInfo/0
14	1468669709	REG	M... ./ROOT/ControlSet001/Control/Power/PowerSettings/54533251-82be-4824-96c1-47b60b740d00/be337238-0d82-4146-a960-4f3749d470c7
15	1468669626	REG	M... ./ROOT/DriverDatabase/DeviceIds/PCI/VEN_1000&DEV_0059&SUBSYS_000D15D9
16	1468669710	REG	M... ./ROOT/ControlSet001/Control/NetDiagFx/Microsoft/HostDLLs/WPPTrace/HelperClasses/WirelessDisplay/Providers/{00000002-0dc9-401d-b9b8-05e4eca4977e}
17	1468669657	REG	M... ./ROOT/DriverDatabase/DriverPackages/mshdc.inf_amd64_67bad2c7196330b6/Descriptors/PCI/VEN_8086&DEV_24DB
18	1508351687	REG	M... ./ROOT/ControlSet001/Enum/DISPLAY/Default_Monitor/1&8713bca&0&UID0/Properties/{a8b865dd-2e3d-4094-ad97-e593a70c75d6}/0006
19	1468669620	REG	M... ./ROOT/DriverDatabase/DeviceIds/USB/VID_04B4&PID_4C67
20	1468669709	REG	M... ./ROOT/ResourcePolicyStore/ResourceSets/PolicySets/DefaultPPLE
21	1468669733	REG	M... ./ROOT/ControlSet001/Services/Spooler
22	1468669656	REG	M... ./ROOT/DriverDatabase/DriverPackages/stexstor.inf_amd64_fefc1160d15aa667/Descriptors/PCI/VEN_105A&DEV_8760&SUBSYS_4262105A
23	1468669626	REG	M... ./ROOT/DriverDatabase/DeviceIds/*PNP0A06
24	1468669709	REG	M... ./ROOT/ControlSet001/Control/Power/PowerSettings/54533251-82be-4824-96c1-47b60b740d00/619b7505-003b-4e82-b7a6-4dd29c300972/DefaultPowerSchemeValues/381b4222-f694
25	1468669657	REG	M... ./ROOT/ControlSet001/Services/EventLog/System/usbser

Analiza uno, o varios, archivos del Registro y genera una línea de tiempo en formato 'TLN'

Log Parser

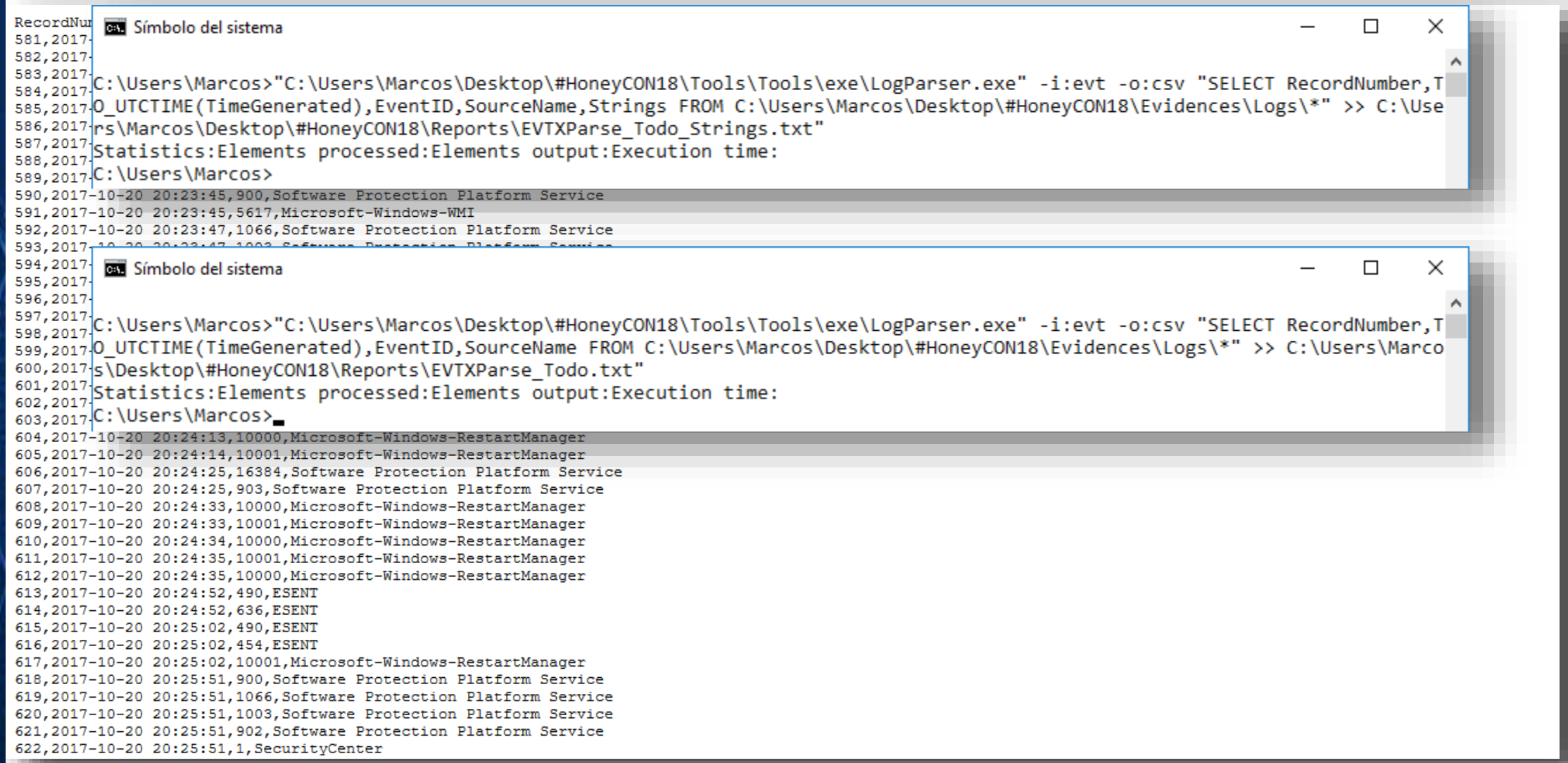
https://github.com/keydet89/Tools



Analiza los registros de eventos desde los archivos '.evtx'

Log Parser

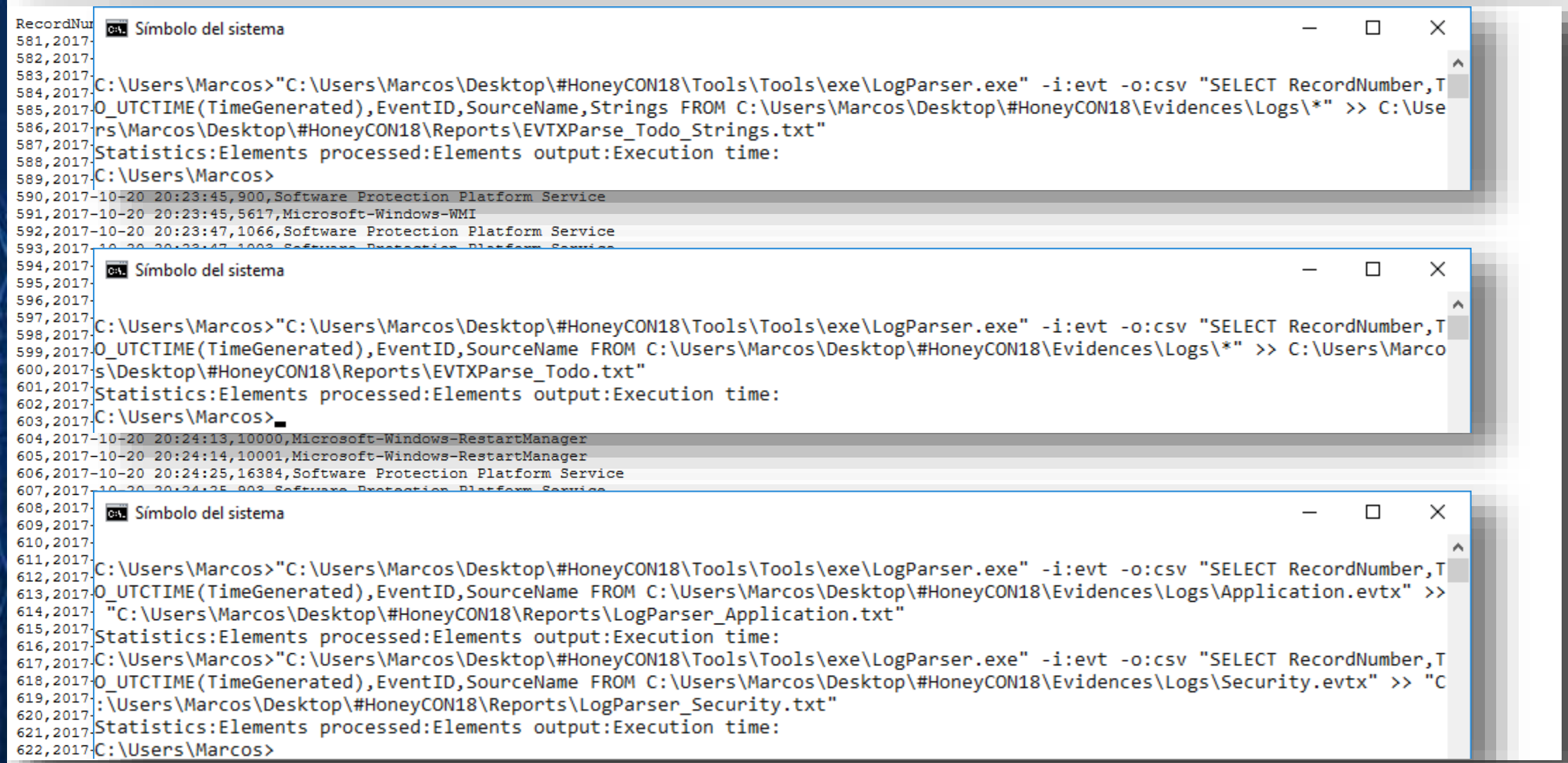
https://github.com/keydet89/Tools



Analiza los registros de eventos desde los archivos '.evtx'

Log Parser

https://github.com/keydet89/Tools



Analiza los registros de eventos desde los archivos '.evtx'

Log Parser

https://github.com/keydet89/Tools

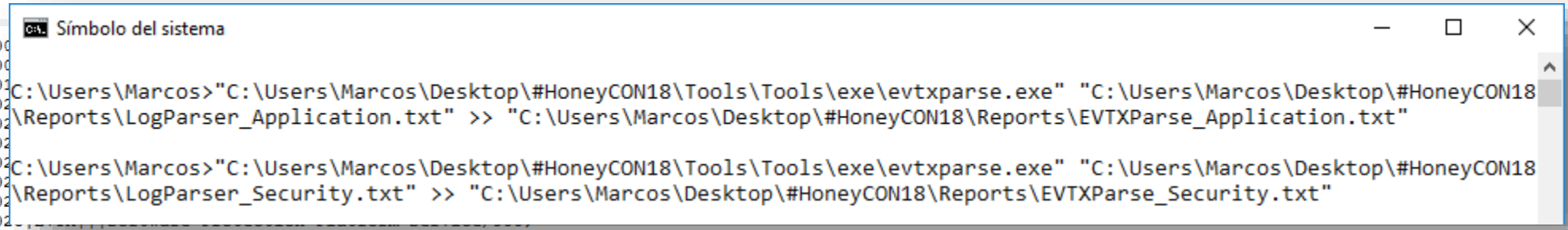
	A	B	C	D	E
1	RecordNumber	TO_UTCTIME(TimeGenerated)	EventID	SourceName	Strings
2	123	18/10/2017 19:00	227	Microsoft-Windows-AppReadiness	Marcos|install::Microsoft.WindowsMaps_8wekyb3d8bbwe|3
3	315	20/10/2017 20:23	200	Microsoft-Windows-DeviceSetupManager	
4	29990	20/10/2017 20:25	175	Microsoft-Windows-Diagnosis-DPS	{1196801C-0A0F-4D3D-9276-012F44DB15AB}|{265CC810-2DDD-43B1-A96E-
5	183	19/10/2017 20:01	5313	Microsoft-Windows-GroupPolicy	Directiva de grupo local
6	265	18/10/2017 18:46	62144	Microsoft-Windows-Shell-Core	Microsoft.BingWeather_8wekyb3d8bbwe|Instalando|0
7	564	18/10/2017 19:19	62171	Microsoft-Windows-Shell-Core	0|InitializeBrowserSsoCookie
8	22	19/			ndows\AppRepository\StateRepos
9	188	18/			01C}|@{Microsoft.ZuneMusic_3.6.
10	37	18/			E9C}|DESKTOP-JCDAIV9||824|Unk
11	536	18/			
12	4	18/			
13	1061	18/			soft.DesktopAppInstaller_1.5.2600
14	329	18/			entication::UserHostAuthenticatic
15	167	18/			nit found: EmojiMFU (fMarkDefau
16	30711	20/			5AB}|{40A03229-41E0-4F8C-8FD8-6
17	29586	20/			5AB}|{249C9718-AB8B-4073-864F-5
18	111	18/			8bbwe
19	9	18/			
20	192	18/			nt_cw5n1h2txyewy|0|0.6518007
21	94	18/			entication::UserHostAuthenticatic
22	432	18/			
23	1209	18/			L.3.23901.0_x64__8wekyb3d8bbwe
24	307	18/			="IDCRL" version="1.0"/><Authent
25	30307	20/			5AB}|{36EAFD13-5471-4295-829D-5

	A	B	C	D
1	RecordNumber	TO_UTCTIME(TimeGenerated)	EventID	SourceName
2	211	19/10/2017 20:02	3052	Microsoft-Windows-PushNotifications-Platform
3	586	18/10/2017 18:37	447	Microsoft-Windows-AppXDeployment-Server
4	996	18/10/2017 18:46	822	Microsoft-Windows-AppXDeployment-Server
5	30663	20/10/2017 20:25	175	Microsoft-Windows-Diagnosis-DPS
6	286	18/10/2017 18:47	6067	Microsoft-Windows-SettingSync
7	1357	18/10/2017 18:46	613	Microsoft-Windows-AppXDeployment-Server
8	90	18/10/2017 18:39	375	Microsoft-Windows-ApplicationResourceManagementSystem
9	1955	18/10/2017 19:00	8106	Microsoft-Windows-AppXDeployment-Server
10	30097	20/10/2017 20:25	175	Microsoft-Windows-Diagnosis-DPS
11	164	18/10/2017 19:21	5325	Microsoft-Windows-GroupPolicy
12	1396	18/10/2017 18:46	813	Microsoft-Windows-AppXDeployment-Server
13	221	18/10/2017 18:36	613	Microsoft-Windows-AppXDeployment-Server
14	193	19/10/2017 20:01	5340	Microsoft-Windows-GroupPolicy
15	295	18/10/2017 19:19	6115	Microsoft-Windows-LiveId
16	29817	20/10/2017 20:25	175	Microsoft-Windows-Diagnosis-DPS
17	627	19/10/2017 20:01	62171	Microsoft-Windows-Shell-Core
18	31194	20/10/2017 20:25	175	Microsoft-Windows-Diagnosis-DPS
19	293	20/10/2017 20:23	8001	Microsoft-Windows-GroupPolicy
20	588	20/10/2017 20:24	2028	Microsoft-Windows-LiveId
21	263	18/10/2017 18:36	613	Microsoft-Windows-AppXDeployment-Server
22	1783	18/10/2017 19:00	603	Microsoft-Windows-AppXDeployment-Server
23	797	18/10/2017 18:46	303	Microsoft-Windows-AppReadiness
24	478	18/10/2017 18:36	613	Microsoft-Windows-AppXDeployment-Server
25	1751	18/10/2017 19:00	10000	Microsoft-Windows-AppXDeployment-Server

Analiza los registros de eventos desde los archivos '.evtx'

EVTX Parse

https://github.com/keydet89/Tools

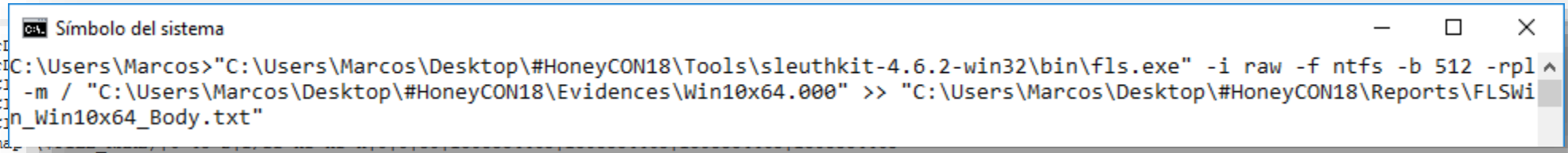



```
1508531025|EVTX|||Microsoft-Windows-WMI/5617;
1508531027|EVTX|||Software Protection Platform Service/1066;
1508531027|EVTX|||Software Protection Platform Service/1003;
1508531027|EVTX|||Software Protection Platform Service/902;
1508531032|EVTX|||Software Protection Platform Service/1003;
1508531032|EVTX|||Software Protection Platform Service/1003;
1508531032|EVTX|||Software Protection Platform Service/8198;
1508531034|EVTX|||Windows Error Reporting/1001;
1508531034|EVTX|||Windows Error Reporting/1001;
1508531034|EVTX|||ESENT/102;
1508531034|EVTX|||ESENT/105;
1508531034|EVTX|||ESENT/326;
1508531035|EVTX|||Windows Search Service/1003;
1508531053|EVTX|||Microsoft-Windows-RestartManager/10000;
1508531054|EVTX|||Microsoft-Windows-RestartManager/10001;
1508531065|EVTX|||Software Protection Platform Service/16384;
1508531065|EVTX|||Software Protection Platform Service/903;
1508531073|EVTX|||Microsoft-Windows-RestartManager/10000;
1508531073|EVTX|||Microsoft-Windows-RestartManager/10001;
1508531074|EVTX|||Microsoft-Windows-RestartManager/10000;
1508531075|EVTX|||Microsoft-Windows-RestartManager/10001;
1508531075|EVTX|||Microsoft-Windows-RestartManager/10000;
1508531092|EVTX|||ESENT/490;
1508531092|EVTX|||ESENT/636;
1508531102|EVTX|||ESENT/490;
1508531102|EVTX|||ESENT/454;
1508531102|EVTX|||Microsoft-Windows-RestartManager/10001;
1508531151|EVTX|||Software Protection Platform Service/900;
1508531151|EVTX|||Software Protection Platform Service/1066;
1508531151|EVTX|||Software Protection Platform Service/1003;
1508531151|EVTX|||Software Protection Platform Service/902;
1508531151|EVTX|||SecurityCenter/1;
1508531153|EVTX|||SecurityCenter/15;
```

Parsea la salida del comando LogParser

TSK, (The SleuthKit)

https://www.sleuthkit.org/sleuthkit/download.php

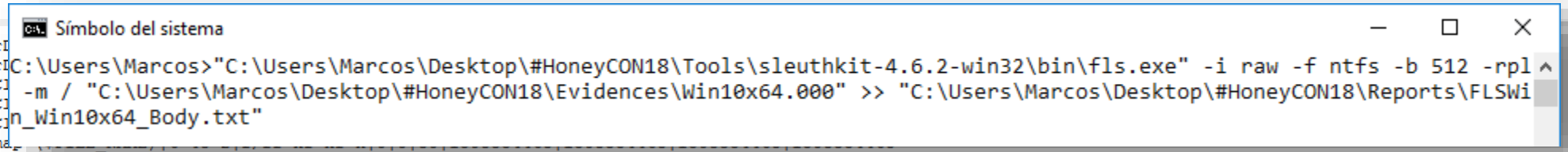


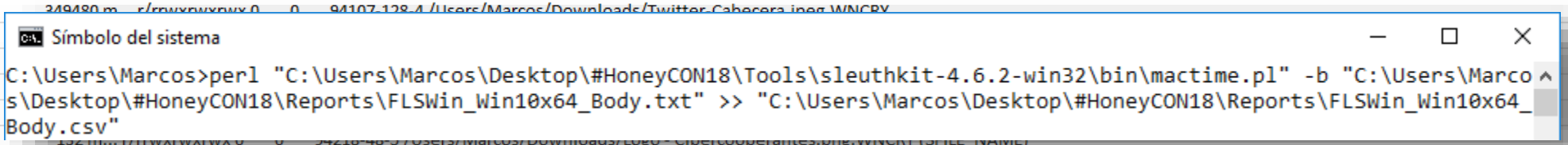

```
0|/$Bitmap|6-128-4|r/rr-xr-xr-x|0|0|639296|1508354468|1508354468|1508354468|1508354468
0|/$Boot ($FILE_NAME)|7-48-2|r/rr-xr-xr-x|48|0|76|1508354468|1508354468|1508354468|1508354468
0|/$Boot|7-128-1|r/rr-xr-xr-x|48|0|8192|1508354468|1508354468|1508354468|1508354468
0|/$Extend ($FILE_NAME)|11-48-3|d/dr-xr-xr-x|0|0|80|1508354468|1508354468|1508354468|1508354468
0|/$Extend|11-144-4|d/dr-xr-xr-x|0|0|656|1508354468|1508354468|1508354468|1508354468
0|/$Extend/$Deleted ($FILE_NAME)|24-48-1|d/dr-xr-xr-x|0|0|82|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$Deleted|24-144-2|d/dr-xr-xr-x|0|0|48|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$ObjId ($FILE_NAME)|26-48-1|r/rr-xr-xr-x|0|0|78|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$ObjId:$O|26-144-5|r/rr-xr-xr-x|0|0|56|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$Quota ($FILE_NAME)|25-48-1|r/rr-xr-xr-x|0|0|78|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$Quota:$O|25-144-3|r/rr-xr-xr-x|0|0|88|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$Quota:$Q|25-144-2|r/rr-xr-xr-x|0|0|208|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$Reparse ($FILE_NAME)|27-48-1|r/rr-xr-xr-x|0|0|82|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$Reparse:$R|27-144-5|r/rr-xr-xr-x|0|0|56|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$RmMetadata ($FILE_NAME)|28-48-1|d/dr-xr-xr-x|0|0|88|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$RmMetadata|28-144-2|d/dr-xr-xr-x|0|0|336|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$RmMetadata/$Repair ($FILE_NAME)|29-48-1|r/rr-xr-xr-x|0|0|80|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$RmMetadata/$Repair|29-128-4|r/rr-xr-xr-x|0|0|0|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$RmMetadata/$Repair:$Config|29-128-2|r/rr-xr-xr-x|0|0|8|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$RmMetadata/$Repair:$Corrupt|29-128-6|r/rr-xr-xr-x|0|0|8388608|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$RmMetadata/$Repair:$Verify|29-128-8|r/rr-xr-xr-x|0|0|1048576|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$RmMetadata/$Txf ($FILE_NAME)|31-48-1|d/dr-xr-xr-x|0|0|74|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$RmMetadata/$Txf|31-144-2|d/dr-xr-xr-x|0|0|48|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$RmMetadata/$TxfLog ($FILE_NAME)|30-48-1|d/dr-xr-xr-x|0|0|80|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$RmMetadata/$TxfLog|30-144-2|d/dr-xr-xr-x|0|0|568|1508354470|1508354470|1508354470|1508354469
0|/$Extend/$RmMetadata/$TxfLog/$Tops ($FILE_NAME)|32-48-1|r/rr-xr-xr-x|0|0|76|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$RmMetadata/$TxfLog/$Tops|32-128-2|r/rr-xr-xr-x|0|0|100|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$RmMetadata/$TxfLog/$Tops:$T|32-128-4|r/rr-xr-xr-x|0|0|1048576|1508354469|1508354469|1508354469|1508354469
0|/$Extend/$RmMetadata/$TxfLog/$TxfLog.blf ($FILE_NAME)|33-48-2|r/rrwxrwxrwx|0|0|88|1508354470|1508354470|1508354470|1508354470
0|/$Extend/$RmMetadata/$TxfLog/$TxfLog.blf|33-128-1|r/rrwxrwxrwx|0|0|65536|1508354470|1508531211|1508531211|1508354470
0|/$Extend/$RmMetadata/$TxfLog/$TxfLogContainer00000000000000000001 ($FILE_NAME)|34-48-2|r/rrwxrwxrwx|0|0|138|1508354470|1508354470|1508354470|1508354470
0|/$Extend/$RmMetadata/$TxfLog/$TxfLogContainer00000000000000000001|34-128-1|r/rrwxrwxrwx|0|0|10485760|1508354470|1508531211|1508531211|1508354470
0|/$Extend/$RmMetadata/$TxfLog/$TxfLogContainer00000000000000000002 ($FILE_NAME)|35-48-2|r/rrwxrwxrwx|0|0|138|1508354470|1508354470|1508354470|1508354470
0|/$Extend/$RmMetadata/$TxfLog/$TxfLogContainer00000000000000000002|35-128-1|r/rrwxrwxrwx|0|0|10485760|1508354470|1508355258|1508355258|1508354470
0|/$Extend/$UsnJrnl ($FILE_NAME)|45993-48-1|r/rr-xr-xr-x|0|0|82|1508351678|1508351678|1508351678|1508351678
0|/$Extend/$UsnJrnl:$J|45993-128-3|r/rr-xr-xr-x|0|0|9819416|1508351678|1508351678|1508351678|1508351678
0|/$Extend/$UsnJrnl:$Max|45993-128-10|r/rr-xr-xr-x|0|0|32|1508351678|1508351678|1508351678|1508351678
```

Lista los archivos y los nombres de directorios en un sistema de archivos

TSK, (The SleuthKit)

https://www.sleuthkit.org/sleuthkit/download.php






```
0|/$AttrDef|4-128-4|r/rr-xr-xr-x|0|0|2560|1508354468|1508354468|1508354468|1508354468
0|/$BadClus|8-128-2|r/rr-xr-xr-x|0|0|0|1508354468|1508354468|1508354468|1508354468
0|/$BadClus:$Bad|8-128-1|r/rr-xr-xr-x|0|0|639296|1508354468|1508354468|1508354468|1508354468
0|/$Bitmap|6-128-4|r/rr-xr-xr-x|0|0|639296|1508354468|1508354468|1508354468|1508354468
0|/$Boot (($FILE_NAME)|7-48-2|r/rr-xr-xr-x|48|0|76|1508354468|1508354468|1508354468|1508354468
0|/$Boot|7-128-1|r/rr-xr-xr-x|48|0|8192|1508354468|1508354468|1508354468|1508354468
```

	A
1	Mon Dec 31 1979 23:00:00 349186 m... r/rrwxrwxrwx 0 0 93738-128-1 /Users/Marcos/Downloads/Twitter-Cabecera.jpeg
2	43504 m... r/rrwxrwxrwx 0 0 93739-128-1 /Users/Marcos/Downloads/Twitter-Perfil.jpeg
3	31790 m... r/rrwxrwxrwx 0 0 93749-128-1 /Users/Marcos/Downloads/Logo - Cibercooperantes.png
4	22028 m... r/rrwxrwxrwx 0 0 93750-128-1 /Users/Marcos/Downloads/Logo - Cibervoluntarios.png
5	51221 m... r/rrwxrwxrwx 0 0 93751-128-1 /Users/Marcos/Downloads/Logo - FWHIBBIT.png
6	349480 m... r/rrwxrwxrwx 0 0 94107-128-4 /Users/Marcos/Downloads/Twitter-Cabecera.jpeg.WNCRY
7	
8	
9	
10	
11	
12	22312 m... r/rrwxrwxrwx 0 0 94219-128-4 /Users/Marcos/Downloads/Logo - Cibervoluntarios.png.WNCRY
13	132 m... r/rrwxrwxrwx 0 0 94219-48-5 /Users/Marcos/Downloads/Logo - Cibervoluntarios.png.WNCRY ($FILE_NAME)
14	51512 m... r/rrwxrwxrwx 0 0 94220-128-4 /Users/Marcos/Downloads/Logo - FWHIBBIT.png.WNCRY
15	116 m... r/rrwxrwxrwx 0 0 94220-48-5 /Users/Marcos/Downloads/Logo - FWHIBBIT.png.WNCRY ($FILE_NAME)
16	Fri Dec 31 1999 23:00:00 3197106 ma.b r/rrwxrwxrwx 0 0 94296-128-3 /ProgramData/awtojqiopxvsxgg941/TaskData/Tor/libeay32.dll
17	719217 ma.b r/rrwxrwxrwx 0 0 94297-128-4 /ProgramData/awtojqiopxvsxgg941/TaskData/Tor/libevent-2-0-5.dll
18	417759 ma.b r/rrwxrwxrwx 0 0 94298-128-4 /ProgramData/awtojqiopxvsxgg941/TaskData/Tor/libevent_core-2-0-5.dll
19	411369 ma.b r/rrwxrwxrwx 0 0 94299-128-4 /ProgramData/awtojqiopxvsxgg941/TaskData/Tor/libevent_extra-2-0-5.dll
20	523262 ma.b r/rrwxrwxrwx 0 0 94300-128-4 /ProgramData/awtojqiopxvsxgg941/TaskData/Tor/libgcc_s_sjlj-1.dll
21	92599 ma.b r/rrwxrwxrwx 0 0 94301-128-3 /ProgramData/awtojqiopxvsxgg941/TaskData/Tor/libssp-0.dll
22	711459 ma.b r/rrwxrwxrwx 0 0 94302-128-3 /ProgramData/awtojqiopxvsxgg941/TaskData/Tor/ssleay32.dll
23	3098624 ma.b r/rrwxrwxrwx 0 0 94303-128-3 /ProgramData/awtojqiopxvsxgg941/TaskData/Tor/tor.exe
24	107520 ma.b r/rrwxrwxrwx 0 0 94304-128-3 /ProgramData/awtojqiopxvsxgg941/TaskData/Tor/zlib1.dll
25	3098624 m... r/rrwxrwxrwx 0 0 94305-128-1 /ProgramData/awtojqiopxvsxgg941/TaskData/Tor/taskhsvc.exe

Lista los archivos y los nombres de directorios en un sistema de archivos

TSK, (The SleuthKit)

https://www.sleuthkit.org/sleuthkit/download.php

	A
1	Date,Size,Type,Mode,UID,GID,Meta,File Name
2	Mon Dec 31 1979 23:00:00,349186,m...,r/rrwxrwxrwx,0,0,93738-128-1,"/Users/Marcos/Downloads/Twitter-Cabecera.jpeg"
3	Mon Dec 31 1979 23:00:00,43504,m...,r/rrwxrwxrwx,0,0,93739-128-1,"/Users/Marcos/Downloads/Twitter-Perfil.jpeg"
4	Mon Dec 31 1979 23:00:00,31790,m...,r/rrwxrwxrwx,0,0,93749-128-1,"/Users/Marcos/Downloads/Logo - Cibercooperantes.png"
5	Mon Dec 31 1979 23:00:00,22028,m...,r/rrwxrwxrwx,0,0,93750-128-1,"/Users/Marcos/Downloads/Logo - Cibervoluntarios.png"
6	Mon Dec 31 1979 23:00:00,51221,m...,r/rrwxrwxrwx,0,0,93751-128-1,"/Users/Marcos/Downloads/Logo - FWHIBBIT.png"
7	Mon Dec 31 1979 23:00:00,349480,m...,r/rrwxrwxrwx,0,0,94107-128-4,"/Users/Marcos/Downloads/Twitter-Cabecera.jpeg.WNCRY"
8	Mon Dec 31 1979 23:00:00,120,m...,r/rrwxrwxrwx,0,0,94107-48-5,"/Users/Marcos/Downloads/Twitter-Cabecera.jpeg.WNCRY ($FILE_NAME)"
9	Mon Dec 31 1979 23:00:00,43784,m...,r/rrwxrwxrwx,0,0,94109-128-4,"/Users/Marcos/Downloads/Twitter-Perfil.jpeg.WNCRY"
10	Mon Dec 31 1979 23:00:00,116,m...,r/rrwxrwxrwx,0,0,94109-48-5,"/Users/Marcos/Downloads/Twitter-Perfil.jpeg.WNCRY ($FILE_NAME)"
11	Mon Dec 31 1979 23:00:00,32072,m...,r/rrwxrwxrwx,0,0,94218-128-4,"/Users/Marcos/Downloads/Logo - Cibercooperantes.png.WNCRY"
12	Mon Dec 31 1979 23:00:00,132,m...,r/rrwxrwxrwx,0,0,94218-48-5,"/Users/Marcos/Downloads/Logo - Cibercooperantes.png.WNCRY ($FILE_NAME)"
13	Mon Dec 31 1979 23:00:00,22312,m...,r/rrwxrwxrwx,0,0,94219-128-4,"/Users/Marcos/Downloads/Logo - Cibervoluntarios.png.WNCRY"
14	Mon Dec 31 1979 23:00:00,132,m...,r/rrwxrwxrwx,0,0,94219-48-5,"/Users/Marcos/Downloads/Logo - Cibervoluntarios.png.WNCRY ($FILE_NAME)"
15	Mon Dec 31 1979 23:00:00,51512,m...,r/rrwxrwxrwx,0,0,94220-128-4,"/Users/Marcos/Downloads/Logo - FWHIBBIT.png.WNCRY"
16	Mon Dec 31 1979 23:00:00,116,m...,r/rrwxrwxrwx,0,0,94220-48-5,"/Users/Marcos/Downloads/Logo - FWHIBBIT.png.WNCRY ($FILE_NAME)"
17	Fri Dec 31 1999 23:00:00,3197106,ma.b,r/rrwxrwxrwx,0,0,94296-128-3,"/ProgramData/awtojqiopxvsxgg941/TaskData/Tor/libeay32.dll"
18	Fri Dec 31 1999 23:00:00,719217,ma.b,r/rrwxrwxrwx,0,0,94297-128-4,"/ProgramData/awtojqiopxvsxgg941/TaskData/Tor/libevent-2-0-5.dll"
19	Fri Dec 31 1999 23:00:00,417759,ma.b,r/rrwxrwxrwx,0,0,94298-128-4,"/ProgramData/awtojqiopxvsxgg941/TaskData/Tor/libevent_core-2-0-5.dll"
20	Fri Dec 3
21	Fri Dec 3
22	Fri Dec 3
23	Fri Dec 3
24	Fri Dec 3
25	Fri Dec 3

Símbolo del sistema

```
C:\Users\Marcos>perl "C:\Users\Marcos\Desktop\#HoneyCON18\Tools\sleuthkit-4.6.2-win32\bin\mactime.pl" -d -b "C:\Users\Ma
rcos\Desktop\#HoneyCON18\Reports\FLSWin_Win10x64_Body.txt" >> "C:\Users\Marcos\Desktop\#HoneyCON18\Reports\FLSWin_Window
s10x64_Delimited.csv"
```

18							
19	411369	ma.b	r/rrwxrwxrwx	0	0	94299-128-4	/ProgramData/awtojqiopxvsxgg941/TaskData/Tor/libevent_extra-2-0-5.dll
20	523262	ma.b	r/rrwxrwxrwx	0	0	94300-128-4	/ProgramData/awtojqiopxvsxgg941/TaskData/Tor/libgcc_s_sjlj-1.dll
21	92599	ma.b	r/rrwxrwxrwx	0	0	94301-128-3	/ProgramData/awtojqiopxvsxgg941/TaskData/Tor/libssp-0.dll
22	711459	ma.b	r/rrwxrwxrwx	0	0	94302-128-3	/ProgramData/awtojqiopxvsxgg941/TaskData/Tor/ssleay32.dll
23	3098624	ma.b	r/rrwxrwxrwx	0	0	94303-128-3	/ProgramData/awtojqiopxvsxgg941/TaskData/Tor/tor.exe
24	107520	ma.b	r/rrwxrwxrwx	0	0	94304-128-3	/ProgramData/awtojqiopxvsxgg941/TaskData/Tor/zlib1.dll
25	3098624	m...	r/rrwxrwxrwx	0	0	94305-128-1	/ProgramData/awtojqiopxvsxgg941/TaskData/Tor/taskhsvc.exe

Lista los archivos y los nombres de directorios en un sistema de archivos

TSK, (The SleuthKit)

https://www.sleuthkit.org/sleuthkit/download.php

	A
1	Date,Size,Type,Mode,UID,GID,Meta,File Name
2	Mon Dec 31 1979 23:00:00,349186,m...,r/rrwxrwxrwx,0,0,93738-128-1,"/Users/Marcos/Downloads/Twitter-Cabecera.jpeg"
3	Mon Dec 31 1979 23:00:00,43504,m...,r/rrwxrwxrwx,0,0,93739-128-1,"/Users/Marcos/Downloads/Twitter-Perfil.jpeg"
4	Mon Dec 31 1979 23:00:00,31790,m...,r/rrwxrwxrwx,0,0,93749-128-1,"/Users/Marcos/Downloads/Logo - Cibercooperantes.png"
5	Mon Dec 31 1979 23:00:00,22028,m...,r/rrwxrwxrwx,0,0,93750-128-1,"/Users/Marcos/Downloads/Logo - Cibervoluntarios.png"
6	Mon Dec 31 1979 23:00:00,51221,m...,r/rrwxrwxrwx,0,0,93751-128-1,"/Users/Marcos/Downloads/Logo - FWHIBBIT.png"
7	Mon Dec 31 1979 23:00:00,349480,m...,r/rrwxrwxrwx,0,0,94107-128-4,"/Users/Marcos/Downloads/Twitter-Cabecera.jpeg.WNCRY"

	A	B	C	D	E	F	G	
1	Date	Size	Type	Mode	UID	GID	Meta	File Name
2	Sat Jul 16 2016 08:04:24	56	...b	d/drwxrwxrwx	0	0	14865-144-12	/Windows/WinSxS/Manifests
3	Sat Jul 16 2016 08:04:27	374112	ma.b	r/rrwxrwxrwx	0	0	47936-128-4	/Windows/WinSxS/amd64_microsoft-windows-d..gement-winproviders_31bf3856ad364e35_10.0.14393.0_none_e4c225
4	Sat Jul 16 2016 08:24:46	13653	m...	r/rrwxrwxrwx	0	0	36057-128-8	/Windows/servicing/Packages/Microsoft-Client-License-Platform-Package~31bf3856ad364e35~amd64~~10.0.14393.0.ca
5	Sat Jul 16 2016 11:31:30	24392	m...	r/rrwxrwxrwx	0	0	40888-128-8	/Windows/System32/CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/Microsoft-Windows-Multilingual-windows-Pa
6	Sat Jul 16 2016 11:46:17	9416	m...	r/rrwxrwxrwx	0	0	42122-128-8	/Windows/servicing/Packages/Microsoft-Windows-SecConfig-Package~31bf3856ad364e35~amd64~~10.0.14393.0.cat
7	Sat Jul 16 2016 13:36:29	1587	.a.b	r/rrwxrwxrwx	0	0	42108-128-4	/Windows/servicing/Packages/Microsoft-Windows-SearchEngine-Client-Package-base~31bf3856ad364e35~amd64~~10.
8	Sat Jul 16 2016 13:38:07	131	...b	r/rrwxrwxrwx	0	0	76540-128-1	/Windows/WinSxS/Manifests/amd64_microsoft-windows-o..-winsock-deployment_31bf3856ad364e35_10.0.14393.0_n
9	Sat Jul 16 2016 13:40:29	109	ma..	r/rrwxrwxrwx	0	0	77064-128-1	/Windows/WinSxS/Manifests/amd64_microsoft-windows-powershell-preloc_31bf3856ad364e35_10.0.14393.0_none_f6
10	Sat Jul 16 2016 13:42:13	87040	ma.b	r/rrwxrwxrwx	0	0	53489-128-4	/Windows/System32/ro-RO/msimsg.dll.mui
11	Sat Jul 16 2016 13:42:14	17408	ma.b	r/rrwxrwxrwx	0	0	45521-128-3	/Windows/WinSxS/amd64_microsoft-windows-ktmutil_31bf3856ad364e35_10.0.14393.0_none_b5fe639917db7cd7/ktm
12	Sat Jul 16 2016 13:42:17	6144	ma.b	r/rrwxrwxrwx	0	0	45711-128-4	/Windows/System32/microsoft-windows-storage-tiering-events.dll
13	Sat Jul 16 2016 13:42:19	577536	ma.b	r/rrwxrwxrwx	0	0	46532-128-4	/Windows/System32/RMActivate.exe
14	Sat Jul 16 2016 13:42:24	384	ma.b	d/drwxrwxrwx	0	0	12073-144-1	/Windows/WinSxS/amd64_microsoft-windows-synchost_31bf3856ad364e35_10.0.14393.0_none_96f5789413450b4a
15	Sat Jul 16 2016 13:42:30	70000	ma.b	r/rrwxrwxrwx	0	0	31259-128-3	/Windows/Fonts/app950.fon
16	Sat Jul 16 2016 13:42:39	60928	ma.b	r/rrwxrwxrwx	0	0	48251-128-3	/Windows/WinSxS/amd64_microsoft-windows-rasbase-core_31bf3856ad364e35_10.0.14393.0_none_5f5ae511dacc1cfa/
17	Sat Jul 16 2016 13:42:40	152	ma.b	d/drwxrwxrwx	0	0	11014-144-1	/Windows/WinSxS/amd64_microsoft-windows-printing-oleprn_31bf3856ad364e35_10.0.14393.0_none_a89b47d575f543
18	Sat Jul 16 2016 13:43:14	1315	ma.b	r/rrwxrwxrwx	0	0	57009-128-4	/Windows/WinSxS/amd64_microsoft-windows-c..ssets.icons.cortana_31bf3856ad364e35_10.0.14393.0_none_323e6ef9c
19	Sat Jul 16 2016 13:43:50	19968	ma.b	r/rrwxrwxrwx	0	0	46474-128-4	/Windows/WinSxS/amd64_microsoft-windows-recoverycenter-core_31bf3856ad364e35_10.0.14393.0_none_3860cb0b7
20	Sat Jul 16 2016 13:45:36	317	ma..	r/rrwxrwxrwx	0	0	34549-128-1	/Windows/Microsoft.NET/Framework64/v4.0.30319/ASP.NETWebAdminFiles/App_Data/GroupedProviders.xml
21	Sat Jul 16 2016 14:37:51	4289938	.a..	r/rrwxrwxrwx	0	0	66685-128-4	/Windows/WinSxS/Backup/wow64_microsoft-windows-directui_31bf3856ad364e35_10.0.14393.0_none_eebf097a39a96
22	Sat Jul 16 2016 21:54:56	9417	m...	r/rrwxrwxrwx	0	0	37484-128-8	/Windows/servicing/Packages/Microsoft-OneCore-NowPlayingSessionManager-shell-Package~31bf3856ad364e35~amd
23	Sun Jul 17 2016 00:38:00	261	...b	r/rrwxrwxrwx	0	0	74857-128-1	/Windows/WinSxS/Manifests/amd64_microsoft-windows-idctrls.resources_31bf3856ad364e35_10.0.14393.0_es-es_f77
24	Sun Jul 17 2016 00:38:10	462	ma..	r/rrwxrwxrwx	0	0	84270-128-4	/Windows/WinSxS/Manifests/wow64_microsoft-windows-n..-security.resources_31bf3856ad364e35_10.0.14393.0_es-e
25	Sun Jul 17 2016 00:38:21	437	...b	r/rrwxrwxrwx	0	0	82824-128-1	/Windows/WinSxS/Manifests/msil_wsatconfig.resources_b03f5f7f11d50a3a_4.0.14305.0_es-es_2d320b30497722e5.man

Lista los archivos y los nombres de directorios en un sistema de archivos

Plaso

https://github.com/log2timeline/plaso/releases

Símbolo del sistema - "C:\Users\Marcos\Desktop\#HoneyCON18\Tools\plaso-20170930-amd64\psteal.exe" -o l2tcsv --source C:\Users\Marcos\Deskto...

```
C:\Users\Marcos>"C:\Users\Marcos\Desktop\#HoneyCON18\Tools\plaso-20170930-amd64\psteal.exe" -o l2tcsv --source C:\Users\
Marcos\Desktop\#HoneyCON18\Evidences\ImagenDiscoMOOC -w C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Plaso_Linux_Psteal.c
sv
```

	A
1	date,time,timezone,MACB,source,sourcetype,type,user,host,short,desc,version,filename,inode,notes,format,extra
2	12/30/1899,00:00:00,UTC,M...,PLSRecall,PL/SQL Developer Recall file,Content Modification Time,SH NAME
3	tcpd \- access control ,team-0002,541611054 SH NAMEtcpd \- access control facility for internet services.SH DE...,Sequence number: 541611054 Username: SH NAMEtcpd \- access control Database name: facility for ir
4	01/01/1970,00:00:00,UTC,M...,FILE,GZIP Content Modification Time,Content Modification Time,-,team-0002,/usr/share/man/man3/Perl4::CoreLibs.3pm.gz,GZIP:/usr/share/man/man3/Perl4::CoreLibs.3pm.gz Type: fil
5	01/01/1970,00:00:00,UTC,M...,FILE,GZIP Content Modification Time,Content Modification Time,-,team-0002,/usr/share/man/man1/smtp-sink.1.gz,GZIP:/usr/share/man/man1/smtp-sink.1.gz Type: file,2,GZIP:/usr/sha
6	01/01/1970,00:00:00,UTC,M...,FILE,GZIP Content Modification Time,Content Modification Time,-,team-0002,/usr/share/man/man1/setfacl.1.gz,GZIP:/usr/share/man/man1/setfacl.1.gz Type: file,2,GZIP:/usr/share/ma
7	01/01/1970,00:00:00,UTC,M...,FILE,GZIP Content Modification Time,Content Modification Time,-,team-0002,/usr/share/man/man3/DBI::ProfileDumper::Apache.3pm.gz,GZIP:/usr/share/man/man3/DBI::ProfileDump
8	01/01/1970,00:00:00,UTC,M...,FILE,GZIP Content Modification Time,Content Modification Time,-,team-0002,/usr/share/doc/liblogging-stdlog0/changelog.Debian.gz,GZIP:/usr/share/doc/liblogging-stdlog0/changelog
9	01/01/1970,00:00:00,UTC,M...,FILE,GZIP Content Modification Time,Content Modification Time,-,team-0002,/usr/share/i18n/charmaps/TIS-620.gz,GZIP:/usr/share/i18n/charmaps/TIS-620.gz Type: file,2,GZIP:/usr/shar
10	01/01/1970,00:00:00,UTC,M...,FILE,GZIP Content Modification Time,Content Modification Time,-,team-0002,/usr/share/man/man7/systemd.journal-fields.7.gz,GZIP:/usr/share/man/man7/systemd.journal-fields.7.gz
630833	10/11/2016,06:39:05,UTC,M...,LOG,Log File,Content Modification Time,-,team-0002,[CRON pid: 7554] pam_unix(cron:session): session closed for user root,[CRON pid: 7554] pam_unix(cron:session): session close
630834	10/11/2016,06:40:01,UTC,M...,LOG,Log File,Content Modification Time,-,team-0002,[CRON pid: 7642] (www-data) CMD (php --define suhosin.memory_limit=512M /usr...,[CRON pid: 7642] (www-data) CMD (php -
630835	10/11/2016,06:40:01,UTC,M...,LOG,Log File,Content Modification Time,-,team-0002,[CRON pid: 7641] pam_unix(cron:session): session opened for user www-data by...,[CRON pid: 7641] pam_unix(cron:session): s
630836	10/11/2016,06:40:02,UTC,M...,LOG,Log File,Content Modification Time,-,team-0002,[CRON pid: 7641] pam_unix(cron:session): session closed for user www-data,[CRON pid: 7641] pam_unix(cron:session): sessior
630837	10/11/2016,06:45:01,UTC,M...,LOG,Log File,Content Modification Time,-,team-0002,[CRON pid: 7648] (www-data) CMD (php --define suhosin.memory_limit=512M /usr...,[CRON pid: 7648] (www-data) CMD (php -
630838	10/11/2016,06:45:01,UTC,M...,LOG,Log File,Content Modification Time,-,team-0002,[CRON pid: 7647] pam_unix(cron:session): session opened for user www-data by...,[CRON pid: 7647] pam_unix(cron:session): s
630839	10/11/2016,06:45:02,UTC,M...,LOG,Log File,Content Modification Time,-,team-0002,[CRON pid: 7647] pam_unix(cron:session): session closed for user www-data,[CRON pid: 7647] pam_unix(cron:session): sessior
630840	10/11/2016,06:50:01,UTC,M...,LOG,Log File,Content Modification Time,-,team-0002,[CRON pid: 7654] (www-data) CMD (php --define suhosin.memory_limit=512M /usr...,[CRON pid: 7654] (www-data) CMD (php -
630841	10/11/2016,06:50:01,UTC,M...,LOG,Log File,Content Modification Time,-,team-0002,[CRON pid: 7653] pam_unix(cron:session): session closed for user www-data,[CRON pid: 7653] pam_unix(cron:session): sessior
630842	10/11/2016,06:50:01,UTC,M...,LOG,Log File,Content Modification Time,-,team-0002,[CRON pid: 7653] pam_unix(cron:session): session opened for user www-data by...,[CRON pid: 7653] pam_unix(cron:session): s

Super línea de tiempo de todas las cosas

Plaso

https://github.com/log2timeline/plaso/releases

```
Símbolo del sistema - "C:\Users\Marcos\Desktop\#HoneyCON18\Tools\plaso-20170930-amd64\psteal.exe"  -o l2tcsv --source C:\Users\Marcos\Deskto...

C:\Users\Marcos>"C:\Users\Marcos\Desktop\#HoneyCON18\Tools\plaso-20170930-amd64\psteal.exe" -o l2tcsv --source C:\Users\
Marcos\Desktop\#HoneyCON18\Evidences\ImagenDiscoMOOC -w C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Plaso_Linux_Psteal.c
sv
```

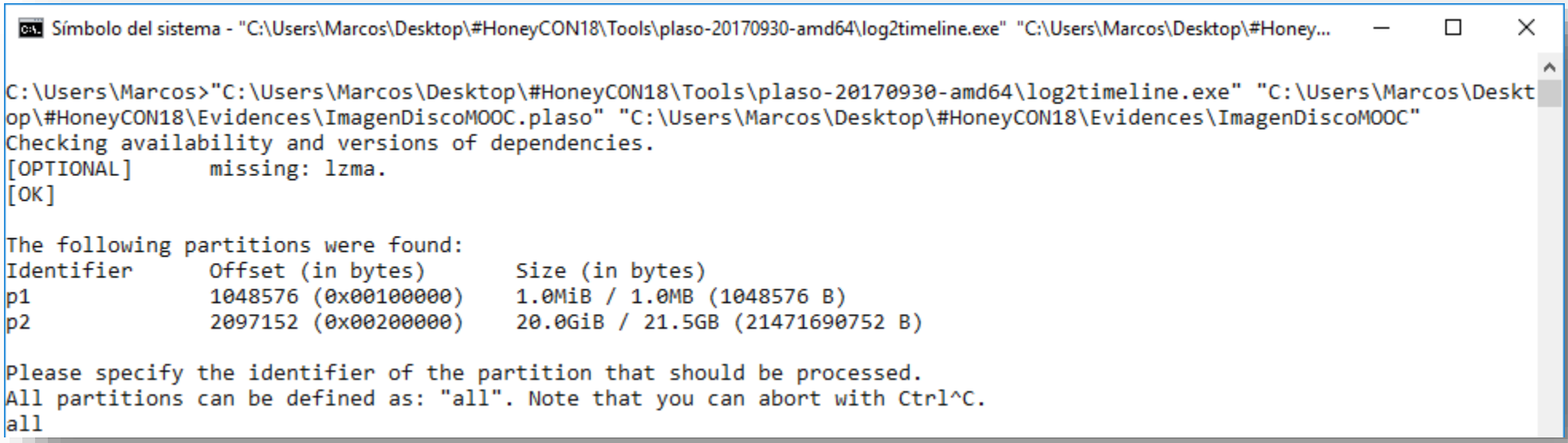
	A
1	date,time,timezone,MACB,source,sourcetype,type,user,host,short,desc,version,filename,inode,notes,format,extra

	A	B	C	D	E	F	G	H	I	J
1	date	time	timezone	MACB	source	sourcetype	type	user	host	short
2	01/01/1970	0:00:00	UTC	M...	FILE	GZIP Content Modification Time	Content Modification Time	-	team-0002	/usr/share/doc/libdatrie1/changelog.Debian.gz
3	01/01/1970	0:00:00	UTC	M...	FILE	GZIP Content Modification Time	Content Modification Time	-	team-0002	/usr/share/man/man1/euca-describe-instance-types.1.g
4	08/07/2013	2:31:22	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/usr/share/doc/cacti/html/advanced_topics.html
5	07/16/2014	18:03:20	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/usr/share/locale/ms/LC_MESSAGES/nano.mo
6	09/17/2014	17:11:27	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/usr/share/terminfo/d/d413-unix-sr
7	09/26/2014	15:06:53	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/usr/share/perl5/CPAN/Meta/Spec.pm
8	10/05/2014	15:16:07	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/usr/share/doc/fakeroot/copyright
9	10/08/2014	23:23:31	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/usr/share/man/man1/euscale-set-desired-capacity.1.g
10	11/08/2014	16:24:03	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/lib/xtables/libxt_bpf.so
11	05/02/2016	22:45:13	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/usr/share/man/man8/update-alternatives.8.gz
12	07/05/2016	18:15:44	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/usr/share/zoneinfo/right/Poland
13	09/03/2016	9:59:28	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/lib/modules/3.16.0-4-686-pae/kernel/drivers/video/fb
14	09/03/2016	21:01:53	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/usr/share/i18n/charmaps/ISO-8859-15.gz
15	09/05/2016	6:20:33	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/usr/lib/i386-linux-gnu/gconv/ISO8859-6.so
16	09/19/2016	12:34:50	UTC	..C.	FILE	UNKNOWN Metadata Modification Time	Metadata Modification Time	-	team-0002	/usr/share/zoneinfo/Etc/GMT-13
17	09/19/2016	12:34:51	UTC	..C.	FILE	UNKNOWN Metadata Modification Time	Metadata Modification Time	-	team-0002	/usr/share/zoneinfo/posix/America/Metlakatla
18	09/19/2016	12:35:27	UTC	...B	FILE	UNKNOWN Creation Time	Creation Time	-	team-0002	/var/lib/dpkg/info/debian-archive-keyring.conffiles
19	09/19/2016	12:37:07	UTC	...B	FILE	UNKNOWN Creation Time	Creation Time	-	team-0002	/lib/modules/3.16.0-4-686-pae/kernel/net/netfilter/xt_
20	09/19/2016	12:37:34	UTC	...B	FILE	UNKNOWN Creation Time	Creation Time	-	team-0002	/lib/modules/3.16.0-4-686-pae/kernel/drivers/media/i2
21	09/19/2016	12:37:42	UTC	..C.	FILE	UNKNOWN Metadata Modification Time	Metadata Modification Time	-	team-0002	/lib/modules/3.16.0-4-686-pae/kernel/sound/pci/snd-e
22	09/19/2016	12:37:42	UTC	..C.	FILE	UNKNOWN Metadata Modification Time	Metadata Modification Time	-	team-0002	/lib/modules/3.16.0-4-686-pae/kernel/drivers/hid/hid-t
23	09/19/2016	12:38:56	UTC	...B	FILE	UNKNOWN Creation Time	Creation Time	-	team-0002	/usr/share/consolefonts/Greek-Terminus16.psf.gz
24	09/19/2016	12:42:32	UTC	..C.	FILE	UNKNOWN Metadata Modification Time	Metadata Modification Time	-	team-0002	/usr/share/perl/5.20.2/Module/Build/Version.pm
25	09/19/2016	12:44:16	UTC	...B	FILE	UNKNOWN Creation Time	Creation Time	-	team-0002	/usr/share/terminfo/n/news31-a

Super línea de tiempo de todas las cosas

Plaso

https://github.com/log2timeline/plaso/releases



Super línea de tiempo de todas las cosas

Plaso

https://github.com/log2timeline/plaso/releases

Símbolo del sistema

```
C:\Users\Marcos>"C:\Users\Marcos\Desktop\#HoneyCON18\Tools\plaso-20170930-amd64\psort.exe" "C:\Users\Marcos\Desktop\#Hon
eyCON18\Evidences\ImagenDiscoMOOC.plaso" -w "C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Plaso_ImagenDiscoMOOC.csv"
2018-10-13 13:14:44,980 [WARNING] (MainProcess) PID:4896 <psort_tool> Appending to an already existing storage file.
2018-10-13 13:14:49,214 [INFO] (MainProcess) PID:4896 <zip_file> Finished filling event heap, added 3777 events
Processing completed.
```

Símbolo del sistema

```
C:\Users\Marcos>"C:\Users\Marcos\Desktop\#HoneyCON18\Tools\plaso-20170930-amd64\psort.exe" -o l2ttln "C:\Users\Marcos\De
sktop\#HoneyCON18\Evidences\ImagenDiscoMOOC.plaso" -w "C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Plaso_ImagenDiscoMOOC
_l2ttln.csv"
2018-10-13 17:13:10,325 [WARNING] (MainProcess) PID:10432 <psort_tool> Appending to an already existing storage file.
2018-10-13 17:13:12,061 [INFO] (MainProcess) PID:10432 <zip_file> Finished filling event heap, added 3777 events
Processing completed.
```

Símbolo del sistema

```
C:\Users\Marcos>"C:\Users\Marcos\Desktop\#HoneyCON18\Tools\plaso-20170930-amd64\psort.exe" -o tln "C:\Users\Marcos\Deskt
op\#HoneyCON18\Evidences\ImagenDiscoMOOC.plaso" -w "C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Plaso_ImagenDiscoMOOC_tl
n.csv"
2018-10-13 17:44:03,525 [WARNING] (MainProcess) PID:12520 <psort_tool> Appending to an already existing storage file.
```

Símbolo del sistema

```
C:\Users\Marcos>"C:\Users\Marcos\Desktop\#HoneyCON18\Tools\plaso-20170930-amd64\psort.exe" -o dynamic  "C:\Users\Marcos\
Desktop\#HoneyCON18\Evidences\ImagenDiscoMOOC.plaso" "select date,time,macb,source.sourcetype,type,short,desc,user,filen
ame,inode" -w "C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Plaso_ImagenDiscoMOOC_dynamic.csv"
2018-10-13 18:05:47,368 [WARNING] (MainProcess) PID:10932 <psort_tool> Appending to an already existing storage file.
2018-10-13 18:05:50,726 [INFO] (MainProcess) PID:10932 <zip_file> Finished filling event heap, added 3777 events
Processing completed.
```

Super línea de tiempo de todas las cosas

Plaso

https://github.com/log2timeline/plaso/releases

Símbolo del sistema

```
C:\Users\Marcos>"C:\Users\Marcos\Desktop\#HoneyCON18\Tools\plaso-20170930-amd64\psort.exe" "C:\Users\Marcos\Desktop\#Hon
eyCON18\Evidences\ImagenDiscoMOOC.plaso" -w "C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Plaso_ImagenDiscoMOOC.csv"
```

	A	B	C	D	E
1	Time	Sourc	Host	Use	Description
2	1476082362	LOG	team-0002	-	2016-10-10T06:52:42+00:00; Content Modification Time; [postfix/pickup, pid: 13287] A4A4520CC7: uid=0 from=<root>
3	1475419830	FILE	team-0002	-	2016-10-02T14:50:30.896000+00:00; Creation Time; TSK:/usr/src/linux-headers-3.16.0-4-686-pae/include/config/net/vendor/smsc.h Type: file
4	1476080616	LOG	team-0002	-	2016-10-10T06:23:36+00:00; Content Modification Time; [postfix/pickup, pid: 13287] warning: maildrop/A6BE8209BC: error writing 362C720CC5: queue file write error
5	1475384944	LOG	team-0002	-	2016-10-02T05:09:04+00:00; Content Modification Time; [postfix/smtp, pid: 11142] 2D23821D01: to=<root@mooc-hacking-team-xxx.mondragon.edu>, orig_to=<root>, relay
6	1476087520	LOG	team-0002	-	2016-10-10T08:18:40+00:00; Content Modification Time; [postfix/pickup, pid: 13680] warning: maildrop/BADC820BC5: error writing D7E5120CCE: queue file write error
7	1476127619	FILE	team-0002	-	2016-10-10T19:26:59.828000+00:00; Last Access Time; TSK:/usr/share/doc/e2fslibs/copyright Type: file
8	1474289130	FILE	team-0002	-	2016-09-19T12:45:30.977593+00:00; Metadata Modification Time; TSK:/usr/include/python2.7/Imaging.h Type: file
9	1476040262	LOG	team-0002	-	2016-10-09T19:11:02+00:00; Content Modification Time; [postfix/pickup, pid: 9817] 1E64320B5B: uid=0 from=<root>
10	1476057017	LOG	team-0002	-	2016-10-09T23:50:17+00:00; Content Modification Time; [postfix/pickup, pid: 11637] 3C0D4209BC: uid=0 from=<root>

	A	B	C	D	E	F	G	H	I	J
1	date	time	timezone	MACB	source	sourcetype	type	user	host	short
2	01/01/1970	0:00:00	UTC	M...	FILE	GZIP Content Modification Time	Content Modification Time	-	team-0002	/usr/share/doc/libdatrie1/changelog.Debian.gz
3	01/01/1970	0:00:00	UTC	M...	FILE	GZIP Content Modification Time	Content Modification Time	-	team-0002	/usr/share/man/man1/euca-describe-instance-types.1.gz
4	08/07/2013	2:31:22	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/usr/share/doc/cacti/html/advanced_topics.html
5	07/16/2014	18:03:20	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/usr/share/locale/ms/LC_MESSAGES/nano.mo
6	09/17/2014	17:11:27	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/usr/share/terminfo/d/d413-unix-sr
7	09/26/2014	15:06:53	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/usr/share/perl5/CPAN/Meta/Spec.pm
8	10/05/2014	15:16:07	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/usr/share/doc/fakeroot/copyright
9	10/08/2014	23:23:31	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/usr/share/man/man1/euscale-set-desired-capacity.1.gz
10	11/08/2014	16:24:03	UTC	M...	FILE	UNKNOWN Content Modification Time	Content Modification Time	-	team-0002	/lib/xtables/libxt_bpf.so

```
C:\Users\Marcos>"C:\Users\Marcos\Desktop\#HoneyCON18\Tools\plaso-20170930-amd64\psort.exe" -o dynamic  "C:\Users\Marcos\
Desktop\#HoneyCON18\Evidences\ImagenDiscoMOOC.plaso" "select date,time,macb,source.sourcetype,type,short,desc,user,filen
ame,inode" -w "C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Plaso_ImagenDiscoMOOC_dynamic.csv"
2018-10-13 18:05:47,368 [WARNING] (MainProcess) PID:10932 <psort_tool> Appending to an already existing storage file.
2018-10-13 18:05:50,726 [INFO] (MainProcess) PID:10932 <zip_file> Finished filling event heap, added 3777 events
Processing completed.
```

Super línea de tiempo de todas las cosas

Timeline Color Template

https://blogs.sans.org/computer-forensics/files/2012/01/TIMELINE_COLOR_TEMPLATE.zip

	A	B	C	D	E	F	G	short
1	date	time	timezone	MACB	source	sourcetype	type	short
2	07/16/2016	1:18:30	UTC	M...	REG	UNKNOWN	Content Modification Time	[\SharedPC\Accou
3	07/16/2016	1:41:26	UTC	...B	PE	PE Compilation time	Creation Time	pe_type
4	07/16/2016	1:45:06	UTC	...B	PE	PE Compilation time	Creation Time	pe_type
5	07/16/2016	11:42:21	UTC	M...	FILE	NTFS Content Modification Time	Content Modification Time	/Windows/WinSxS
6	07/16/2016	11:42:38	UTC	MA.B	FILE	NTFS Content Modification Time	Content Modification Time; Creation Time; Last Access Time	/Windows/System
7	07/16/2016	11:42:45	UTC	MA.B	FILE	NTFS Content Modification Time	Content Modification Time; Creation Time; Last Access Time	/Windows/SysWO
8	07/16/2016	11:42:46	UTC	MA.B	FILE	NTFS Content Modification Time	Content Modification Time; Creation Time; Last Access Time	/Windows/SysWO
9	07/16/2016	11:42:50	UTC	MA.B	FILE	NTFS Content Modification Time	Content Modification Time; Creation Time; Last Access Time	/Windows/WinSxS
10	07/16/2016	11:43:08	UTC	MA.B	FILE	NTFS Content Modification Time	Content Modification Time; Creation Time; Last Access Time	/Windows/System32/WmpDui.dll
11	07/16/2016	11:46:30	UTC	...B	FILE	NTFS Creation Time	Creation Time	/Windows/System32/DriverStore/FileRepository/mdmgc
12	07/16/2016	22:48:12	UTC	MA.B	FILE	NTFS Content Modification Time	Content Modification Time; Creation Time; Last Access Time	/Program Files/WindowsApps/microsoft.windowscommu
13	10/18/2017	18:35:09	UTC	..C.	FILE		Metadata Modification Time	sdstor.sys 48304-1 USN_REASON_SECURITY_CHANGE
14	10/18/2017	18:35:41	UTC	..C.	FILE		Metadata Modification Time	setupapi.dev.log 88871-1 USN_REASON_DATA_EXTEND
15	10/18/2017	18:36:11	UTC	..C.	FILE		Metadata Modification Time	resources.pri 21063-1 USN_REASON_SECURITY_CHANGE
16	10/18/2017	18:36:11	UTC	..C.	FILE	NTFS Metadata Modification Time	Metadata Modification Time	/Program Files/WindowsApps/Microsoft.Getstarted_3.11
17	10/18/2017	18:36:38	UTC	..C.	FILE		Metadata Modification Time	OneNotePageSmallTile.scale-150.png 23346-1 USN_REAS
18	10/18/2017	18:36:39	UTC	..C.	FILE	NTFS Metadata Modification Time	Metadata Modification Time	/Program Files/WindowsApps/Microsoft.Office.OneNote
19	10/18/2017	18:36:49	UTC	..C.	FILE		Metadata Modification Time	mu_44x30.png 24736-1 USN_REASON_SECURITY_CHANGE
20	10/18/2017	18:37:00	UTC	..C.	FILE		Metadata Modification Time	microsoft.system.package.metadata 89823-1 USN_REASO
21	10/18/2017	18:37:05	UTC	..C.	FILE		Metadata Modification Time	HxCalendarSmallTile.scale-200.png 26444-1 USN_REASON
22	10/18/2017	18:37:14	UTC	..C.	FILE		Metadata Modification Time	StoreMedTile.scale-100.png 28012-1 USN_REASON_SECUR
23	10/18/2017	18:37:32	UTC	..C.	FILE		Metadata Modification Time	tpmB8BC.tmp 90046-2 USN_REASON_FILE_CREATE USN_R
24	10/18/2017	18:38:47	UTC	..C.	FILE		Metadata Modification Time	CloudStore 90278-1 USN_REASON_BASIC_INFO_CHANGE
25	10/18/2017	18:41:16	UTC	..C.	FILE		Metadata Modification Time	SEARCHINDEXER.EXE-4A6353B9.pf 90662-1 USN_REASON_

	A
1	FILE OPENING
2	WEB HISTORY
3	DELETED DATA
4	EXECUTION
5	DEVICE or USB USAGE
6	FOLDER OPENING
7	LOG FILE

Colorea de un color diferente cada uno de los distintos artefactos conocidos

Timeline Color Template

https://blogs.sans.org/computer-forensics/files/2012/01/TIMELINE_COLOR_TEMPLATE.zip

	A	B	C	D	E	F	G	short
1	date	time	timezone	MACB	source	sourcetype	type	short
2	07/16/2016	1:18:30	UTC	M...	REG	UNKNOWN	Content Modification Time	[\SharedPC\Accou
3	07/16/2016	1:41:26	UTC	...B	PE	PE Compilation time	Creation Time	pe_type
4	07/16/2016	1:45:06	UTC	...B	PE	PE Compilation time	Creation Time	pe_type

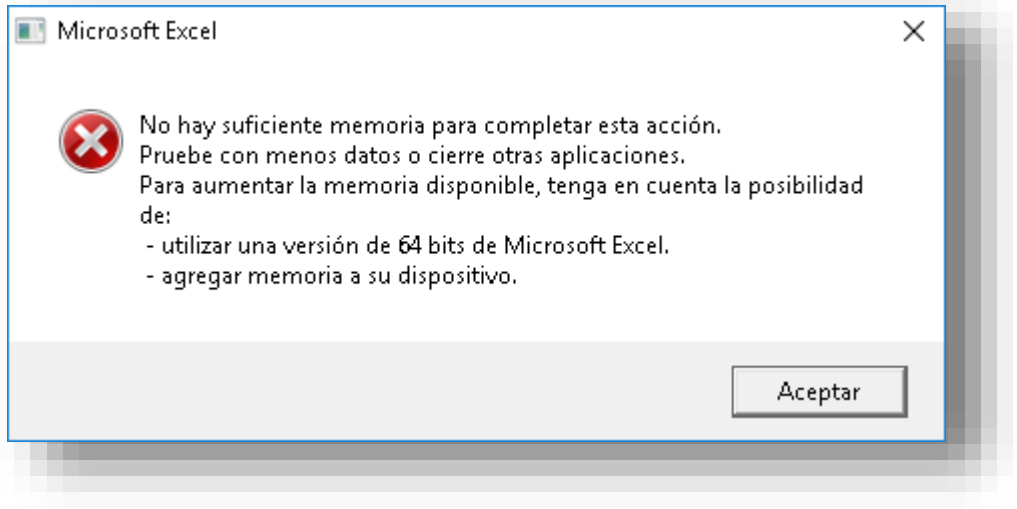
	A
1	FILE OPENING
2	WEB HISTORY
3	DELETED DATA
4	EXECUTION
5	DEVICE or USB USAGE
6	FOLDER OPENING
7	LOG FILE

	A	B	C	D	E	F	G	short
1	date	time	timezone	MACB	source	sourcetype	type	short
187301	10/18/2017	18:37:43	UTC	..C.	FILE		Metadata Modification Time	CiPT0000.002 90
187302	10/18/2017	18:41:28	UTC	..C.	FILE		Metadata Modification Time	CiPT0000.001 89
187303	10/18/2017	18:45:47	UTC	..C.	FILE		Metadata Modification Time	settings.dat 90796-1 USN_REASON_DATA_EXTEND US
187304	10/18/2017	18:46:10	UTC	..C.	FILE		Metadata Modification Time	LocalCache 91095-1 USN_REASON_SECURITY_CHANGE
187305	10/18/2017	18:46:11	UTC	M...	REG	UNKNOWN	Content Modification Time	[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Window
187306	10/18/2017	18:46:21	UTC	M...	REG	UNKNOWN	Content Modification Time	[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Window
187307	10/18/2017	18:46:27	UTC	..C.	FILE		Metadata Modification Time	LocalCache 91787-1 USN_REASON_SECURITY_CHANGE
187308	10/18/2017	18:47:59	UTC	..C.	FILE		Metadata Modification Time	FileSync.Resources.dll 92793-1 USN_REASON_DATA_E
187309	10/18/2017	19:00:30	UTC	..C.	FILE		Metadata Modification Time	VBoxDisp.dll 89775-2 USN_REASON_DATA_EXTEND US
187310	10/18/2017	19:00:39	UTC	M...	REG	UNKNOWN	Content Modification Time	[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Window
187311	10/18/2017	19:02:02	UTC	..C.	FILE		Metadata Modification Time	SET62C.tmp 93631-4 USN_REASON_RENAME_OLD_NAM
187312	10/18/2017	19:02:04	UTC	..C.	FILE		Metadata Modification Time	CONHOST.EXE-1F3E9D7E.pf 92921-1 USN_REASON_DA
187313	10/18/2017	19:21:44	UTC	..C.	FILE		Metadata Modification Time	www.bing[1].xml 91990-1 USN_REASON_DATA_EXTEN
187314	10/18/2017	19:21:54	UTC	..C.	FILE		Metadata Modification Time	dmrc.idx.2 92837-2 USN_REASON_RENAME_NEW_NAM
187315	10/18/2017	19:23:08	UTC	..C.	FILE	NTFS Metadata Modification Time	Metadata Modification Time	/ProgramData/Microsoft/Device Stage/Task/{e35be42
187316	10/18/2017	19:24:56	UTC	..C.	FILE	NTFS Metadata Modification Time	Metadata Modification Time	/Windows/WinSxS/amd64_dual_c_fsinfrastructure.inf
187317	10/18/2017	19:28:27	UTC	..C.	FILE	NTFS Metadata Modification Time	Metadata Modification Time	/Windows/System32/virtdisk.dll
187318	10/18/2017	19:32:03	UTC	..C.	FILE	NTFS Metadata Modification Time	Metadata Modification Time	/Windows/SysWOW64/dimsroam.dll
187319	10/18/2017	19:33:36	UTC	..C.	FILE	NTFS Metadata Modification Time	Metadata Modification Time	/Windows/WinSxS/amd64_microsoft-windows-c..ram
187320	10/18/2017	19:33:36	UTC	..C.	FILE	NTFS Metadata Modification Time	Metadata Modification Time	/Windows/WinSxS/amd64_microsoft-windows-d..ash
187321	10/18/2017	19:33:36	UTC	..C.	FILE	NTFS Metadata Modification Time	Metadata Modification Time	/Windows/WinSxS/amd64_microsoft-windows-d..nt-(
187322	10/18/2017	19:33:36	UTC	..C.	FILE	NTFS Metadata Modification Time	Metadata Modification Time	/Windows/WinSxS/amd64_microsoft-windows-i..migu
187323	10/18/2017	19:33:36	UTC	..C.	FILE	NTFS Metadata Modification Time	Metadata Modification Time	/Windows/WinSxS/amd64_netr28ux.inf_31bf3856ad3(
187324	10/20/2017	20:21:02	UTC	..C.	FILE		Metadata Modification Time	updatestore51b519d5-b6f5-4333-8df6-e74d7c9aead4.x
187325	10/20/2017	20:26:39	UTC	..C.	FILE		Metadata Modification Time	AppCache131530047986645983.txt.~tmp 92873-5 USN_

Colorea de un color diferente cada uno de los distintos artefactos conocidos

Timeline Explorer

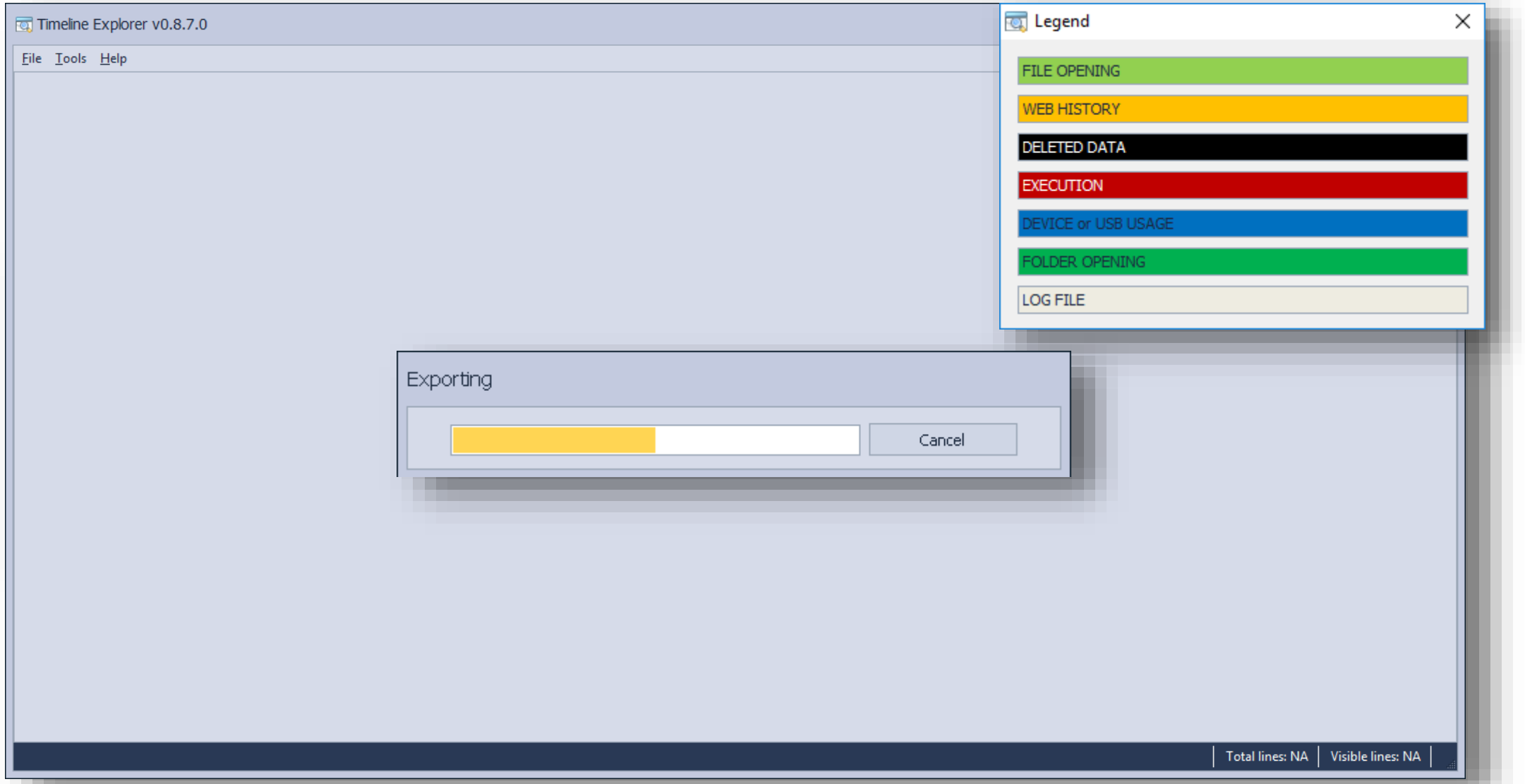
https://ericzimmerman.github.io/



Abre, sin usar Excel, ficheros generados por ‘Mactime’ y ‘Plaso’, además de cualquier ‘.csv’

Timeline Explorer

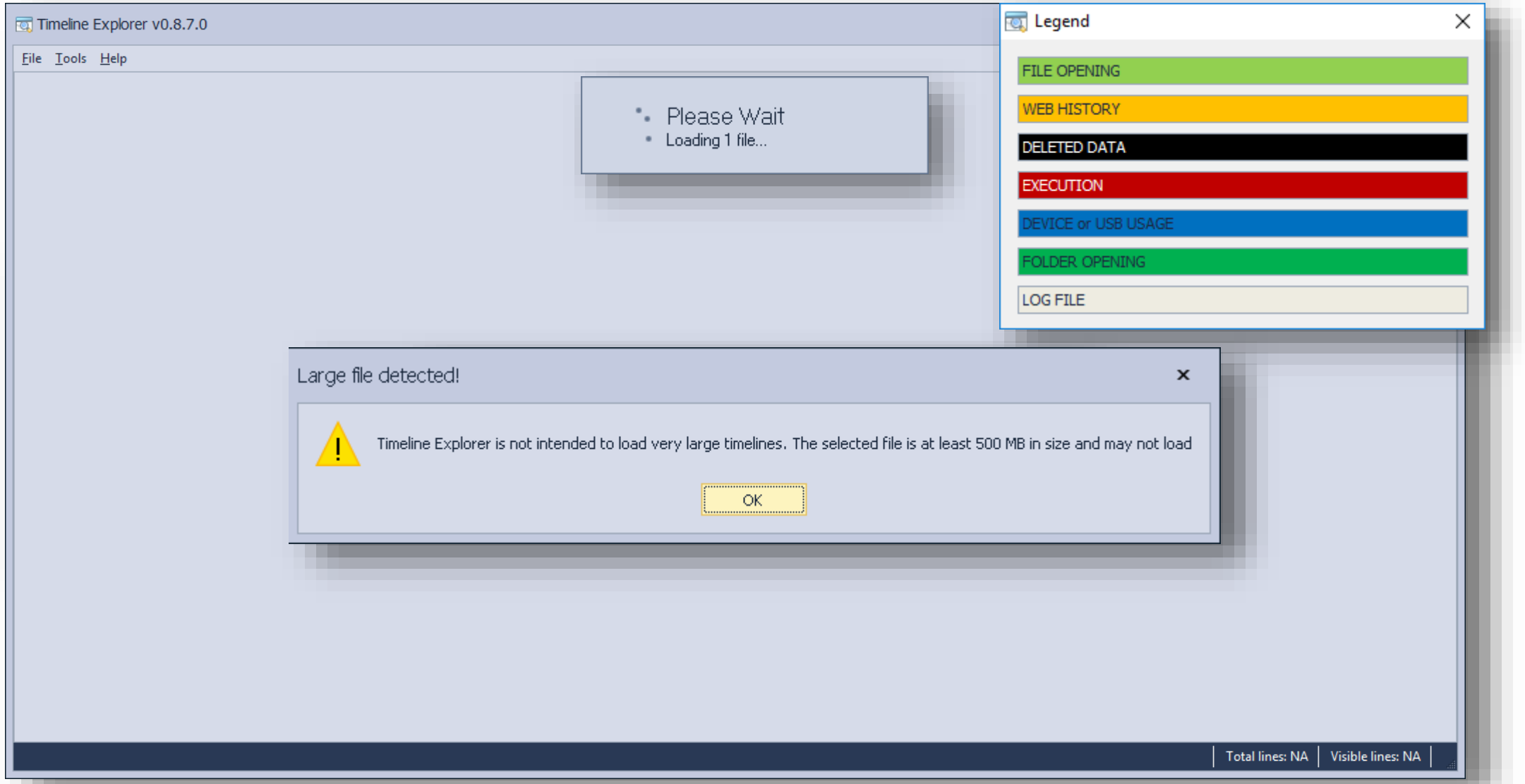
https://ericzimmerman.github.io/



Abre, sin usar Excel, ficheros generados por 'Mactime' y 'Plaso', además de cualquier '.csv'

Timeline Explorer

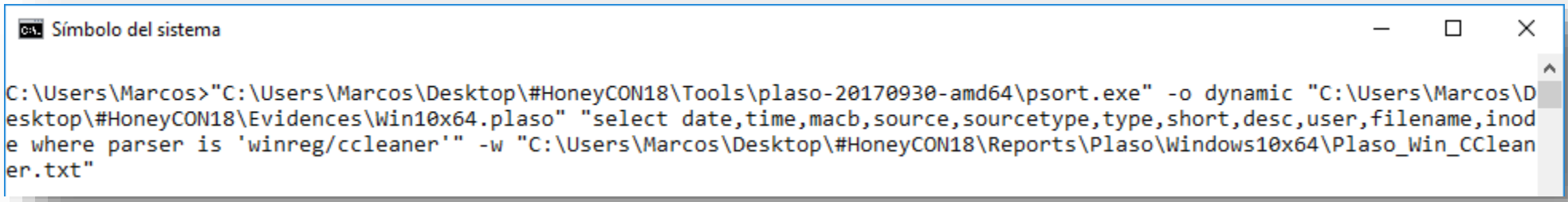
https://ericzimmerman.github.io/

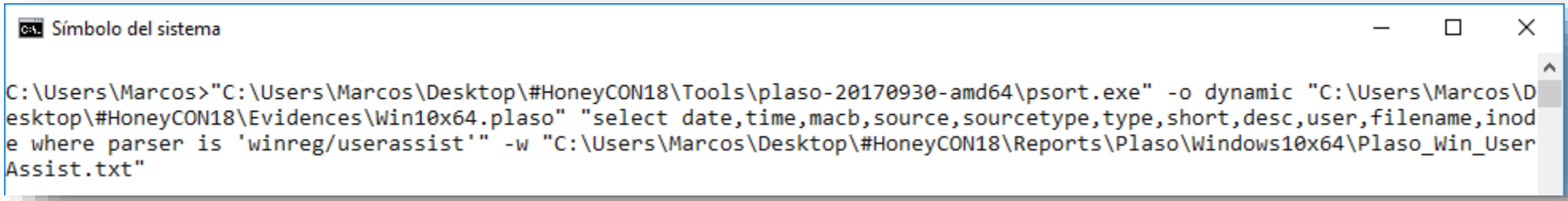


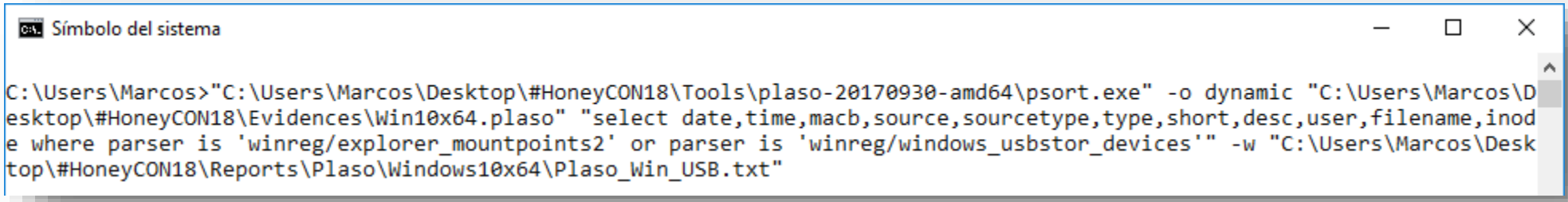
Abre, sin usar Excel, ficheros generados por 'Mactime' y 'Plaso', además de cualquier '.csv'

Plaso

https://github.com/log2timeline/plaso/releases







Super línea de tiempo de todas las cosas

Timeline Explorer

https://ericzimmerman.github.io/

Line	Tag	Timestamp	Source Descr...	Source Name	macb	Inode	Long Description
1		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
2		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
3		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
4		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
5		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
6		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
7		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
8		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
9		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
10		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
11		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
12		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
13		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
14		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
15		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
16		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
17		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
18		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
19		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
20		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C

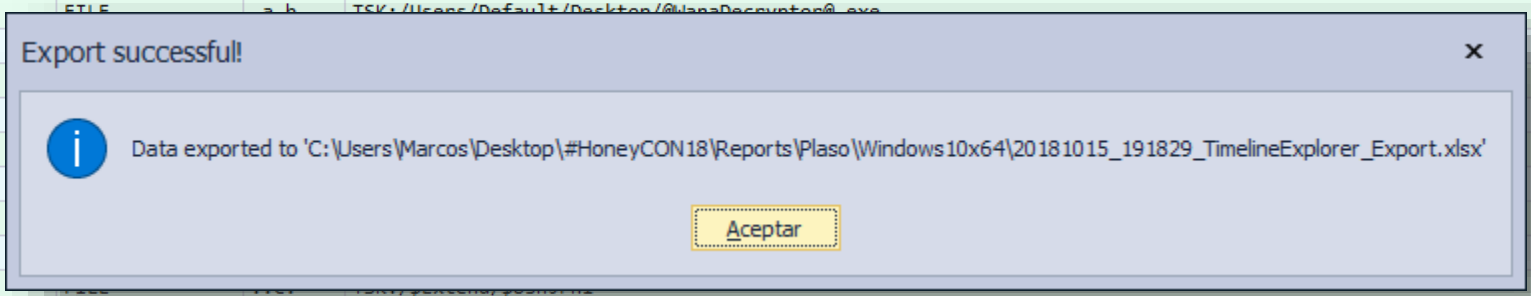
Abre, sin usar Excel, ficheros generados por ‘Mactime’ y ‘Plaso’, además de cualquier ‘.csv’

Timeline Explorer

https://ericzimmerman.github.io/

Line	Tag	Timestamp	Source Descr...	Source Name	macb	Inode	Long Description
1		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
2		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
3		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
4		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
5		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
6		1970-01-01 00:00:00	AppCompatCa...	REG	....	0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C
7		1970-01-01 00:00:00	AppCompatCa...	REG		0	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] C

Timestamp	Source Name	macb	File Name
2017/10/20 20:26:23	FILE	mac.	TSK:/Users/Default/Desktop
2017/10/20 20:26:23	FILE	mac.	TSK:/Users/defaultuser0/Desktop
2017/10/20 20:26:23	FILE	mac.	TSK:/Users/Marcos/Desktop
2017/10/20 20:26:23	FILE	mac.	TSK:/Users/Public/Desktop
2017/10/20 20:26:23	FILE	.a.b	TSK:/Users/Default/Desktop/@WanaDecryptor@.bmp
2017/10/20 20:26:23	FILE	.a.b	TSK:/Users/defaultuser0/Desktop/@WanaDecryptor@.bmp
2017/10/20 20:26:23	FILE	.a.b	TSK:/Users/Marcos/Desktop/@WanaDecryptor@.bmp
2017/10/20 20:26:23	FILE	.a.b	TSK:/Users/Public/Desktop/@WanaDecryptor@.bmp
2017/10/20 20:26:23			
2017/10/20 20:26:23			
2017/10/20 20:26:23			
2017/10/20 20:26:23			
2017/10/20 20:26:23			
2017/10/20 20:26:23			
2017/10/20 20:26:23			
2017/10/20 20:26:23	FILE	..c.	TSK:/$Extend/$UsnJrnl
2017/10/20 20:26:23	FILE	macb	TSK:/Windows/Temp/hibsys.WNCRYT
2017/10/20 20:26:23	REG	m...	TSK:/Windows/System32/config/SYSTEM
2017/10/20 20:26:23	REG	m...	TSK:/Windows/System32/config/SYSTEM



Abre, sin usar Excel, ficheros generados por ‘Mactime’ y ‘Plaso’, además de cualquier ‘.csv’

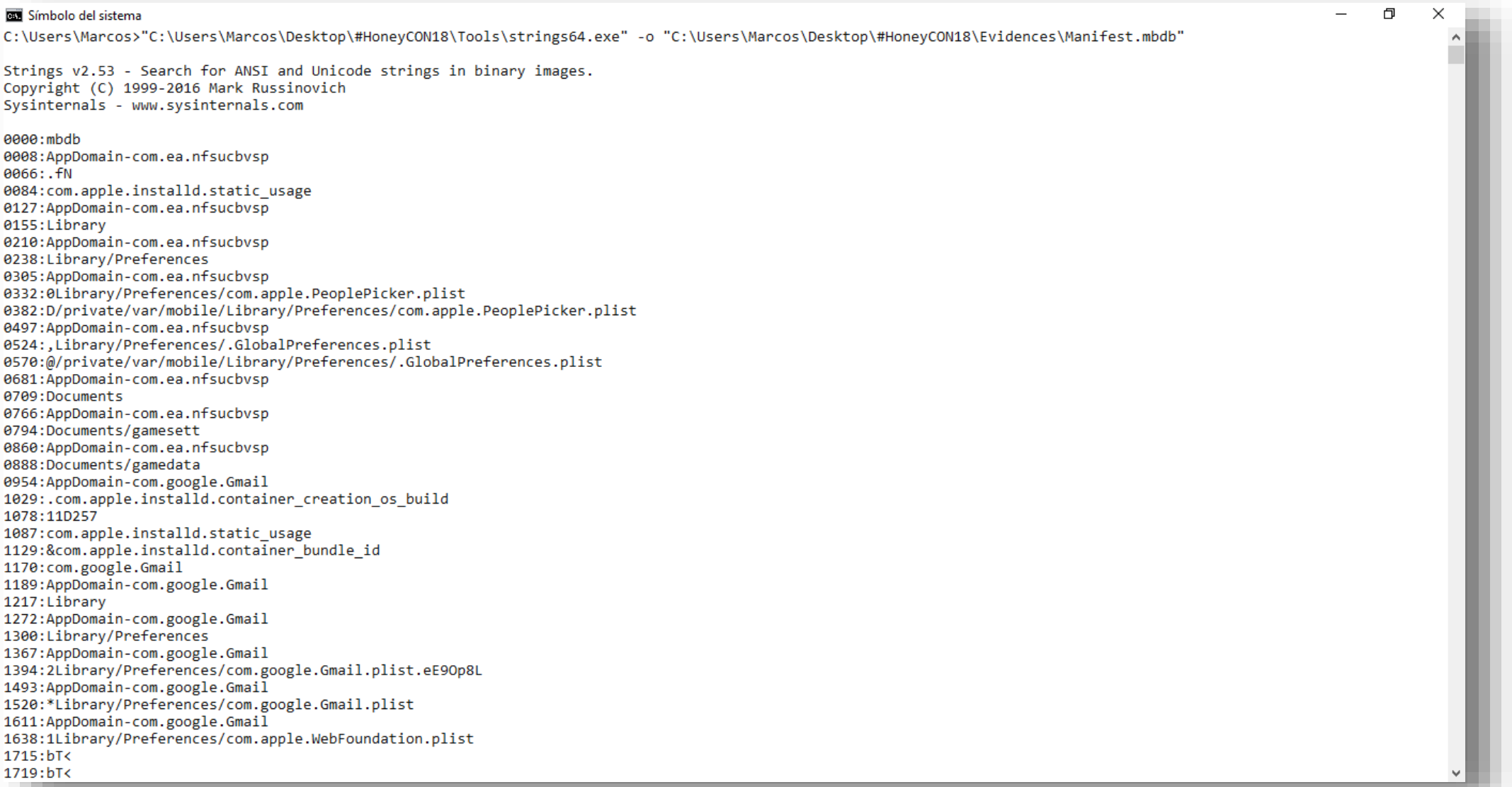
¿Obsesión con las líneas de tiempo?

Una línea de tiempo **siempre** ayudará a entender qué ha pasado en un Sistema

No es algo secundario, irrelevante o sin importancia

ListManifest

https://github.com/aramosf/listManifest



Parsea la base de datos ‘Manifest.mbdb’, generada al realizar un backup de iTunes

ListManifest

https://github.com/aramosf/listManifest

```
root@N4rr34n6: ~/listManifest
root@N4rr34n6:~/listManifest# python listManifest.py /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Evidences/Manifest.mbdb >>
/mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/Manifest.txt
root@N4rr34n6:~/listManifest#
```

```
0000:mbdb
permissions|inode|uid|guid|size|class|mtime|atime|ctime|fileid|domain|application|filename|proprties1|prop2|prop3
drwxr-xr-x|14936082|501|501|0|NSFileProtectionNone|2014-07-14 00:03:10 (DST)|2014-07-14 00:03:10 (DST)|2014-07-14 00:03:10
(DST)|cd1ef41e018b446b9b93445ec8ef88ca6b690b43|CameraRollDomain||Media/PhotoData/Thumbnails/V2/DCIM/107APPLE/IMG_7434.JPG
drwxr-xr-x|491754|501|501|0|NSFileProtectionNone|2011-12-07 17:37:42 (STD)|2012-01-01 10:59:02 (STD)|2011-12-07 17:37:42
(STD)|030c94ffb72e0c86e5219bcb5fa03bec40a04f95|AppDomain|com.ea.nfsucbvsp||com.apple.installd.static_usage='\x00\xc0\x1d\x08\x00\x00\x00\x00'
drwxr-xr-x|19993608|501|501|0|NSFileProtectionCompleteUntilFirstUserAuthentication|2014-12-25 16:56:08 (STD)|2014-12-25 16:56:08 (STD)|2014-12-25 16:56:05
0305:AppDomain-com.ea.nfsucbvsp
```

	A	B	C	D	E	F	G	H	I	
1	permissions	inode	uid	guid	size	class	mtime	atime	ctime	fileid
2	-rw-r--r--	21667864	501	501	3151	NSFileProtectionCompleteUntilFirstUserAuthentication	2015-02-15 18:11:33 (STD)	2015-02-15 18:11:33 (STD)	2015-02-15 18:11:33 (STD)	5feedecb6b063c335629
3	drwxr-xr-x	19425531	501	501	0	NSFileProtectionCompleteUntilFirstUserAuthentication	2014-12-07 14:25:44 (STD)	2014-12-07 14:25:44 (STD)	2014-12-07 14:25:42 (STD)	7a65187c098a832df1402
4	drwxr-xr-x	18176205	501	501	0	NSFileProtectionCompleteUntilFirstUserAuthentication	2014-10-28 09:22:25 (STD)	2014-10-28 09:22:25 (STD)	2014-10-28 09:21:34 (STD)	b1ee276190fada34d7a6
5	-rw-r--r--	23071418	501	501	11409728	NSFileProtectionNone	2015-04-07 11:25:02 (DST)	2015-04-07 11:25:02 (DST)	2015-04-07 11:24:59 (DST)	b665a745408e5ee8e16e
6	-rw-r--r--	9556129	501	501	53603	NSFileProtectionCompleteUntilFirstUserAuthentication	2013-11-02 17:21:07 (STD)	2014-03-12 16:37:03 (STD)	2013-11-02 17:21:07 (STD)	77b54525db36a6d62a16
7	drwxrwxr-x	1365123	501	501	0	NSFileProtectionNone	2015-03-10 13:51:40 (STD)	2015-03-10 13:51:40 (STD)	2012-03-15 14:22:38 (STD)	3e4a9eaa935cbea36c12
8	-rw-r--r--	24358742	501	501	61958	NSFileProtectionNone	2015-05-16 12:47:09 (DST)	2015-05-16 12:47:09 (DST)	2015-05-16 12:47:09 (DST)	b4744030ec25b42d21c5
9	-rw-r--r--	13553526	501	501	68194	NSFileProtectionCompleteUntilFirstUserAuthentication	2014-05-16 20:43:57 (DST)	2014-05-16 20:43:57 (DST)	2014-05-16 20:43:57 (DST)	0eb3dbee7ffd94381093
10	drwxr-xr-x	14246786	501	501	0	NSFileProtectionNone	2014-06-14 18:10:07 (DST)	2014-06-14 18:10:07 (DST)	2014-06-14 18:10:07 (DST)	6831915f32a13d341986
11	drwxr-xr-x	22948020	501	501	0	NSFileProtectionCompleteUntilFirstUserAuthentication	2015-04-03 13:43:42 (DST)	2015-04-03 13:43:42 (DST)	2015-04-03 13:43:40 (DST)	ce4e7ab06ada618fff968
12	drwxr-xr-x	23470471	501	501	0	NSFileProtectionCompleteUntilFirstUserAuthentication	2015-04-28 08:46:51 (DST)	2015-04-28 08:46:51 (DST)	2015-04-21 21:55:05 (DST)	20d2a0cac24a4d92ed20
13	drwxr-xr-x	20782436	501	501	0	NSFileProtectionCompleteUntilFirstUserAuthentication	2015-01-19 13:00:50 (STD)	2015-01-19 13:00:50 (STD)	2015-01-19 13:00:50 (STD)	a3ff99a6ba90a06fd0adc
14	drwxr-xr-x	15387552	501	501	0	NSFileProtectionNone	2014-08-01 11:45:08 (DST)	2014-08-01 11:45:08 (DST)	2014-08-01 11:45:08 (DST)	cfa4e1293e686e1ecce8
15	drwxr-xr-x	8777252	501	501	0	NSFileProtectionNone	2015-05-14 18:36:29 (DST)	2015-05-14 18:36:29 (DST)	2013-09-23 21:20:58 (DST)	7d879ec02f10ceadbcb1
16	-rw-r--r--	15751265	501	501	3473	NSFileProtectionCompleteUntilFirstUserAuthentication	2014-08-14 19:58:22 (DST)	2014-08-14 19:58:22 (DST)	2014-08-14 19:58:22 (DST)	cfd06d8c14159c32ea525
17	-rw-r--r--	12251700	501	501	53230	NSFileProtectionCompleteUntilFirstUserAuthentication	2014-03-27 00:22:00 (STD)	2014-03-27 00:22:00 (STD)	2014-03-27 00:22:00 (STD)	093f9734f8d755b576203
18	-rw-r--r--	17314561	501	501	26640	NSFileProtectionNone	2014-10-09 06:51:00 (DST)	2014-10-09 06:51:00 (DST)	2014-10-02 23:04:56 (DST)	420a32fac7d8f92b5ab86
19	-rw-r--r--	20991647	501	501	224531	NSFileProtectionCompleteUntilFirstUserAuthentication	2015-01-24 15:38:09 (STD)	2015-01-24 15:38:09 (STD)	2015-01-24 15:38:08 (STD)	c070262f84af717dcad3d
20	-rw-r--r--	21638570	501	501	3209	NSFileProtectionCompleteUntilFirstUserAuthentication	2015-02-14 13:40:44 (STD)	2015-02-14 13:40:44 (STD)	2015-02-14 13:40:44 (STD)	183f2d29840e8202f976

Parsea la base de datos 'Manifest.mbdb', generada al realizar un backup de iTunes

mbdbls.py

https://github.com/obsidianforensics/mbdbls

root@N4rr34n6: ~/mbdbls

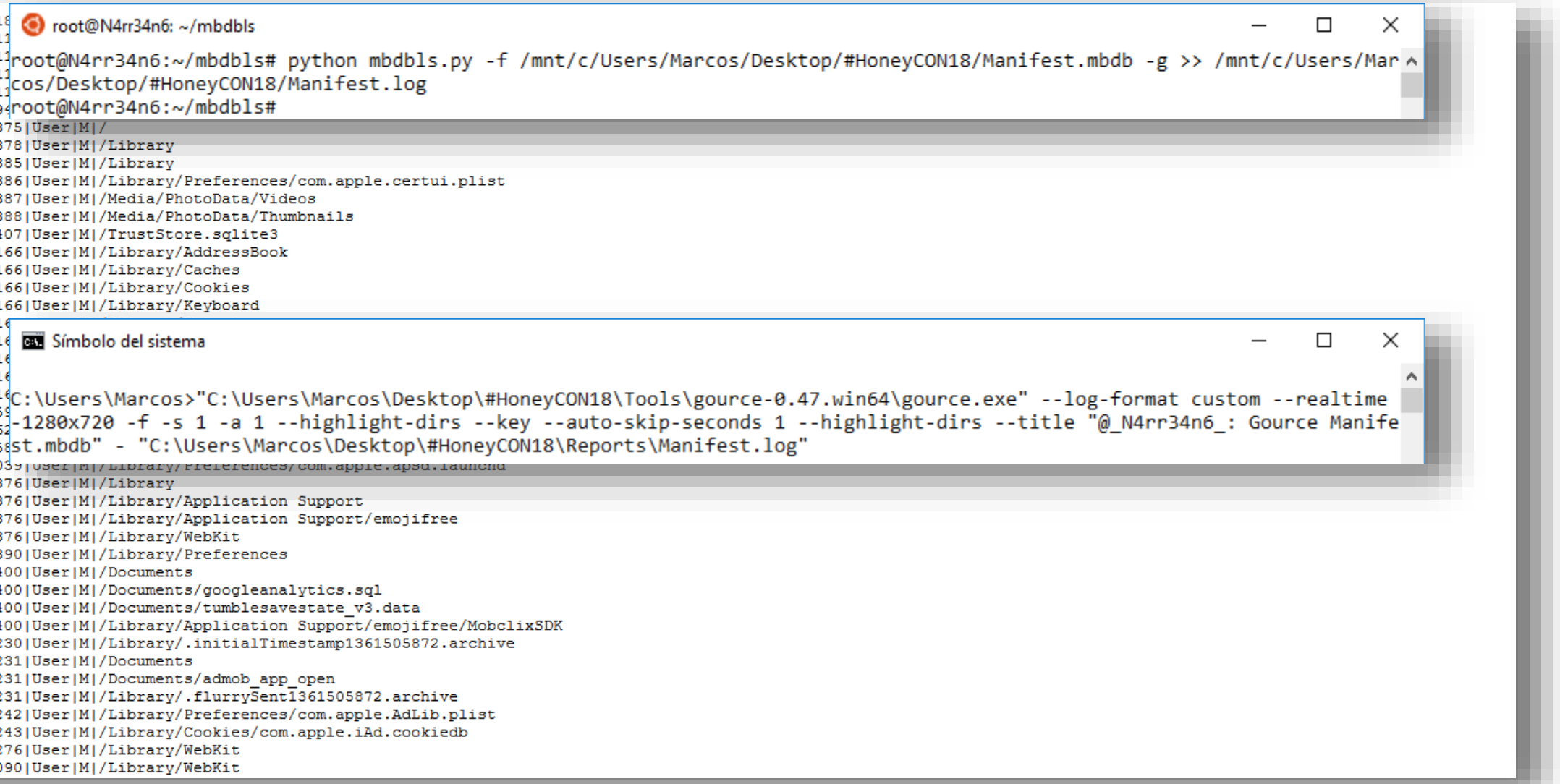
```
root@N4rr34n6:~/mbdbls# python mbdbls.py -f /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Manifest.mbdb -g >> /mnt/c/Users/Mar
cos/Desktop/#HoneyCON18/Manifest.log
root@N4rr34n6:~/mbdbls#
```

```
1297050181|User|M|/
1297051111|User|M|/Library
1297051111|User|M|/Library
1297051111|User|M|/Library/Preferences/com.apple.certui.plist
1297051111|User|M|/Media/PhotoData/Videos
1297051111|User|M|/Media/PhotoData/Thumbnails
1297051111|User|M|/TrustStore.sqlite3
1304052941|User|M|/Library/AddressBook
1309805375|User|M|/
1309805378|User|M|/Library
1309805385|User|M|/Library
1309805386|User|M|/Library/Preferences/com.apple.certui.plist
1309805387|User|M|/Media/PhotoData/Videos
1309805388|User|M|/Media/PhotoData/Thumbnails
1309805407|User|M|/TrustStore.sqlite3
1314675166|User|M|/Library/AddressBook
1314675166|User|M|/Library/Caches
1314675166|User|M|/Library/Cookies
1314675166|User|M|/Library/Keyboard
1314675166|User|M|/Library/Safari
1314675167|User|M|/
1314675167|User|M|/Media
1314675167|User|M|/Media/DCIM
1314675167|User|M|/Media/PhotoData
1315045596|User|M|/Media/Recordings
1315045621|User|M|/
1315049581|User|M|/Library/Caches
1315050039|User|M|/Library/Preferences/com.apple.apsd.launchd
1315050376|User|M|/Library
1315050376|User|M|/Library/Application Support
1315050376|User|M|/Library/Application Support/emojifree
1315050376|User|M|/Library/WebKit
1315050390|User|M|/Library/Preferences
1315050400|User|M|/Documents
1315050400|User|M|/Documents/googleanalytics.sql
1315050400|User|M|/Documents/tumblesavestate_v3.data
1315050400|User|M|/Library/Application Support/emojifree/MobclixSDK
1315060230|User|M|/Library/.initialTimestamp1361505872.archive
1315060231|User|M|/Documents
1315060231|User|M|/Documents/admob_app_open
1315060231|User|M|/Library/.flurrySent1361505872.archive
1315060242|User|M|/Library/Preferences/com.apple.AdLib.plist
1315060243|User|M|/Library/Cookies/com.apple.iAd.cookiedb
1315060276|User|M|/Library/WebKit
1315063090|User|M|/Library/WebKit
```

Parsea archivos Manifest.mbdb procedentes de directorios de copia de seguridad de iTunes

mbdbls.py

https://github.com/obsidianforensics/mbdbls



Parsea archivos Manifest.mbdb procedentes de directorios de copia de seguridad de iTunes

Gource

https://github.com/acaudwell/Gource

Gource

https://github.com/acaudwell/Gource

mbdbls.py

https://github.com/obsidianforensics/mbdbls

gource.exe --log-format custom --realtime -f -1280x720 -s 1 -a 1 --highlight-dirs --key --auto-skip-seconds 1 --highlight-dirs --title “@_N4rr34n6_: Manifest.mbdb” “C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Gource\Manifest.log”

Demo effect? Video 00

Custom Log Format, (Bodyfile)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

root@N4rr34n6: ~

```
root@N4rr34n6:~# sed -e 's/|||MACB/|A|/;s/|||.A.B/|A|/;s/|||.AC./|M|/;s/|||MAC./|M|/;s/|||..C./|M|/;s/|||M..B/|A|/;s/|||...B/|A|/;s/|||M.../|M|/;s/|||MA.B/|A|/;s/|||M.C./|M|/;s/|||.A../|M|/;s/|||MA../|M|/' /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/Bodyfile/Win10x64_BodyFile.txt >> /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/Gource/Win10x64_BodyFile_Gource.log
root@N4rr34n6:~#
```

```
1508354469|FILE|||MACB [48] /img_Win10x64.000/$Extend/$Deleted
1508354469|FILE|||MACB [0] /img_Win10x64.000/$Extend/$ObjId
1508354469|FILE|||MACB [0] /img_Win10x64.000/$Extend/$Quota
1508354469|FILE|||MACB [0] /img_Win10x64.000/$Extend/$Reparse
1508354469|FILE|||MACB [336] /img_Win10x64.000/$Extend/$RmMetadata
1508354469|FILE|||MACB [0] /img_Win10x64.000/$Extend/$RmMetadata/$Repair
1508354469|FILE|||MACB [8] /img_Win10x64.000/$Extend/$RmMetadata/$Repair:$Config
1508354469|FILE|||MACB [8388608] /img_Win10x64.000/$Extend/$RmMetadata/$Repair:$Corrupt
1508354469|FILE|||MACB [1048576] /img_Win10x64.000/$Extend/$RmMetadata/$Repair:$Verify
1508354469|FILE|||MACB [48] /img_Win10x64.000/$Extend/$RmMetadata/$Txf
1508354470|FILE|||MAC. [568] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog
1508354469|FILE|||...B [568] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog
1508354469|FILE|||MACB [100] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$Tops
1508354469|FILE|||MACB [1048576] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$Tops:$T
1508531211|FILE|||M.C. [65536] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$TxfLog.blf
1508354470|FILE|||.A.B [65536] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$TxfLog.blf
1508531211|FILE|||M.C. [10485760] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$TxfLogContainer00000000000000000001
1508354470|FILE|||.A.B [10485760] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$TxfLogContainer00000000000000000001
1508355258|FILE|||M.C. [10485760] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$TxfLogContainer00000000000000000002
1508354470|FILE|||.A.B [10485760] /img_Win10x64.000/$Extend/$RmMetadata/$TxfLog/$TxfLogContainer00000000000000000002
1508351678|FILE|||MACB [9819416] /img_Win10x64.000/$Extend/$UsnJrnl:$J
1508351678|FILE|||MACB [32] /img_Win10x64.000/$Extend/$UsnJrnl:$Max
1508354468|FILE|||MACB [29868032] /img_Win10x64.000/$LogFile
1508354468|FILE|||MACB [96731136] /img_Win10x64.000/$MFT
1508354468|FILE|||MACB [4096] /img_Win10x64.000/$MFTMirr
1508531170|FILE|||MAC. [608] /img_Win10x64.000/$Recycle.Bin
1468669667|FILE|||...B [608] /img_Win10x64.000/$Recycle.Bin
1508531170|FILE|||MAC. [152] /img_Win10x64.000/$Recycle.Bin/S-1-5-21-3930698692-3150784357-1811628781-1000
1508352359|FILE|||...B [152] /img_Win10x64.000/$Recycle.Bin/S-1-5-21-3930698692-3150784357-1811628781-1000
1508352359|FILE|||MACB [129] /img_Win10x64.000/$Recycle.Bin/S-1-5-21-3930698692-3150784357-1811628781-1000/desktop.ini
1508531170|FILE|||MAC. [152] /img_Win10x64.000/$Recycle.Bin/S-1-5-21-3930698692-3150784357-1811628781-1001
1508352394|FILE|||...B [152] /img_Win10x64.000/$Recycle.Bin/S-1-5-21-3930698692-3150784357-1811628781-1001
1508352394|FILE|||MACB [129] /img_Win10x64.000/$Recycle.Bin/S-1-5-21-3930698692-3150784357-1811628781-1001/desktop.ini
1508354468|FILE|||MACB [1027440] /img_Win10x64.000/$Secure:$SDS
1508354468|FILE|||MACB [131072] /img_Win10x64.000/$UpCase
```

Custom Log Format, (Bodyfile)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

root@N4rr34n6: ~

```
root@N4rr34n6:~# sed -e 's/|||MACB/|A|/;s/|||.A.B/|A|/;s/|||.AC./|M|/;s/|||MAC./|M|/;s/|||..C./|M|/;s/|||M..B/|A|/;s/|||
...B/|A|/;s/|||M.../|M|/;s/|||MA.B/|A|/;s/|||M.C./|M|/;s/|||.A../|M|/;s/|||MA../|M|/' /mnt/c/Users/Marcos/Desktop/#Honey
CON18/Reports/Bodyfile/Win10x64_BodyFile.txt >> /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/Gource/Win10x64_BodyFile
_Gource.log
root@N4rr34n6:~#
```

```
1290219418|FILE|A| [37577] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_norwegian.wnry
1290219418|FILE|A| [37580] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_filipino.wnry
1290219418|FILE|A| [37917] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_portuguese.wnry
1290219418|FILE|A| [38377] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_finnish.wnry
1290219418|FILE|A| [38437] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_french.wnry
1290219418|FILE|A| [38483] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_swedish.wnry
1290219418|FILE|A| [39070] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_croatian.wnry
1290219418|FILE|A| [39896] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_polish.wnry
1290219418|FILE|A| [40512] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_czech.wnry
1290219418|FILE|A| [41169] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_latvian.wnry
1290219418|FILE|A| [41391] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_slovak.wnry
1290219418|FILE|A| [42582] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_turkish.wnry
1290219418|FILE|A| [47108] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_russian.wnry
1290219418|FILE|A| [47879] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_bulgarian.wnry
1290219418|FILE|A| [49044] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_greek.wnry
1290219418|FILE|A| [52161] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_romanian.wnry
1290219418|FILE|A| [54359] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_chinese (simplified).wnry
1290219418|FILE|A| [79346] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_chinese (traditional).wnry
1290219418|FILE|A| [81844] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_japanese.wnry
1290219418|FILE|A| [91501] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_korean.wnry
1290219418|FILE|A| [93778] /img_Win10x64.000/ProgramData/awtojqiopxvsxgg941/msg/m_vietnamese.wnry
1458952086|FILE|M| [402396] /img_Win10x64.000/Users/Marcos/Downloads/N4rr34n6.png
1458952086|FILE|M| [402680] /img_Win10x64.000/Users/Marcos/Downloads/N4rr34n6.png.WNCRY
1460537702|FILE|A| [150] /img_Win10x64.000/Users/Marcos/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/LocalState/ConstraintIndex
/Input_{74f757c4-350e-43ad-b70c-a343b2ad6cdc}/apps.schema
1460537702|FILE|A| [162] /img_Win10x64.000/Users/Marcos/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/LocalState/ConstraintIndex
/Input_{74f757c4-350e-43ad-b70c-a343b2ad6cdc}/settings.schema
1460537702|FILE|A| [31582] /img_Win10x64.000/Users/Marcos/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/LocalState/ConstraintIndex
/Input_{74f757c4-350e-43ad-b70c-a343b2ad6cdc}/appsconversions.txt
1460537702|FILE|A| [31582] /img_Win10x64.000/Users/Marcos/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/LocalState/ConstraintIndex
/Input_{74f757c4-350e-43ad-b70c-a343b2ad6cdc}/settingsconversions.txt
1460537702|FILE|A| [31864] /img_Win10x64.000/Users/Marcos/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/LocalState/ConstraintIndex
/Input_{74f757c4-350e-43ad-b70c-a343b2ad6cdc}/appsconversions.txt.WNCRY
1460537702|FILE|A| [31864] /img_Win10x64.000/Users/Marcos/AppData/Local/Packages/Microsoft.Windows.Cortana_cw5n1h2txyewy/LocalState/ConstraintIndex
/Input_{74f757c4-350e-43ad-b70c-a343b2ad6cdc}/settingsconversions.txt.WNCRY
```

Custom Log Format, (Bodyfile)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

gource.exe -f
“C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Gource\Win10x64_BodyFile_Gource_2.log”

Demo effect? Video 01-02

Custom Log Format, (EVTX Parse)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

root@N4rr34n6: ~

```
root@N4rr34n6:~# sed -e 's/|EVTX|/|Application|/;s/|||/|A|/' /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/EVTXParse_Application.txt >> /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/Application_Gource.log
root@N4rr34n6:~# sed -e 's/|EVTX|/|Security|/;s/|||/|A|/' /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/EVTXParse_Security.txt >> /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/Security_Gource.log
root@N4rr34n6:~#
```

```
1508531023|EVTX|||Microsoft-Windows-WMI/5615;
1508531025|EVTX|||Software Protection Platform Service/900;
1508531025|EVTX|||Microsoft-Windows-WMI/5617;
1508531027|EVTX|||Software Protection Platform Service/1066;
1508531027|EVTX|||Software Protection Platform Service/1003;
1508531027|EVTX|||Software Protection Platform Service/902;
1508531032|EVTX|||Software Protection Platform Service/1003;
1508531032|EVTX|||Software Protection Platform Service/1003;
1508531032|EVTX|||Software Protection Platform Service/8198;
1508531034|EVTX|||Windows Error Reporting/1001;
1508531034|EVTX|||Windows Error Reporting/1001;
1508531034|EVTX|||ESENT/102;
1508531034|EVTX|||ESENT/105;
1508531034|EVTX|||ESENT/326;
1508531035|EVTX|||Windows Search Service/1003;
1508531053|EVTX|||Microsoft-Windows-RestartManager/10000;
1508531054|EVTX|||Microsoft-Windows-RestartManager/10001;
1508531065|EVTX|||Software Protection Platform Service/16384;
1508531065|EVTX|||Software Protection Platform Service/903;
1508531073|EVTX|||Microsoft-Windows-RestartManager/10000;
1508531073|EVTX|||Microsoft-Windows-RestartManager/10001;
1508531074|EVTX|||Microsoft-Windows-RestartManager/10000;
1508531075|EVTX|||Microsoft-Windows-RestartManager/10001;
1508531075|EVTX|||Microsoft-Windows-RestartManager/10000;
1508531092|EVTX|||ESENT/490;
1508531092|EVTX|||ESENT/636;
1508531102|EVTX|||ESENT/490;
1508531102|EVTX|||ESENT/454;
1508531102|EVTX|||Microsoft-Windows-RestartManager/10001;
1508531151|EVTX|||Software Protection Platform Service/900;
1508531151|EVTX|||Software Protection Platform Service/1066;
1508531151|EVTX|||Software Protection Platform Service/1003;
1508531151|EVTX|||Software Protection Platform Service/902;
1508531151|EVTX|||SecurityCenter/1;
1508531153|EVTX|||SecurityCenter/15;
```

Custom Log Format, (EVTX Parse)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

```
root@N4rr34n6: ~
root@N4rr34n6:~# sed -e 's/|EVTX|/|Application|/;s/|||/|A|/' /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/EVTXParse_Application.txt >> /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/Application_Gource.log
root@N4rr34n6:~# sed -e 's/|EVTX|/|Security|/;s/|||/|A|/' /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/EVTXParse_Security.txt >> /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/Security_Gource.log
root@N4rr34n6:~#
```

```
1508531020|Security|A|Microsoft-Windows-Security-Auditing/4688;
1508531021|Security|A|Microsoft-Windows-Security-Auditing/4608;
1508531021|Security|A|Microsoft-Windows-Security-Auditing/4624;
1508531021|Security|A|Microsoft-Windows-Security-Auditing/4688;
1508531021|Security|A|Microsoft-Windows-Security-Auditing/4688;
1508531021|Security|A|Microsoft-Windows-Security-Auditing/4688;
1508531021|Security|A|Microsoft-Windows-Security-Auditing/4688;
1508531021|Security|A|Microsoft-Windows-Security-Auditing/4688;
1508531021|Security|A|Microsoft-Windows-Security-Auditing/4688;
1508531021|Security|A|Microsoft-Windows-Security-Auditing/4688;
1508531021|Security|A|Microsoft-Windows-Security-Auditing/4688;
1508531022|Application|A|EventSystem/4625;
1508531022|Application|A|Microsoft-Windows-User Profiles Service/1531;
1508531022|Application|A|Wlclntfy/6003;
1508531022|Security|A|Microsoft-Windows-Security-Auditing/4624;
1508531022|Security|A|Microsoft-Windows-Security-Auditing/4624;
1508531022|Security|A|Microsoft-Windows-Security-Auditing/4624;
1508531022|Security|A|Microsoft-Windows-Security-Auditing/4624;
1508531022|Security|A|Microsoft-Windows-Security-Auditing/4624;
1508531022|Security|A|Microsoft-Windows-Security-Auditing/4624;
1508531022|Security|A|Microsoft-Windows-Security-Auditing/4624;
1508531022|Security|A|Microsoft-Windows-Security-Auditing/4648;
1508531022|Security|A|Microsoft-Windows-Security-Auditing/4672;
1508531022|Security|A|Microsoft-Windows-Security-Auditing/4672;
1508531022|Security|A|Microsoft-Windows-Security-Auditing/4672;
1508531022|Security|A|Microsoft-Windows-Security-Auditing/4672;
1508531022|Security|A|Microsoft-Windows-Security-Auditing/4672;
1508531022|Security|A|Microsoft-Windows-Security-Auditing/4672;
1508531022|Security|A|Microsoft-Windows-Security-Auditing/4672;
1508531022|Security|A|Microsoft-Windows-Security-Auditing/4798;
1508531022|Security|A|Microsoft-Windows-Security-Auditing/4902;
1508531023|Application|A|Microsoft-Windows-WMI/5615;
1508531023|Application|A|Wlclntfy/6003;
1508531023|Security|A|Microsoft-Windows-Security-Auditing/4624;
1508531023|Security|A|Microsoft-Windows-Security-Auditing/4624;
```

Custom Log Format, (EVTX Parse)

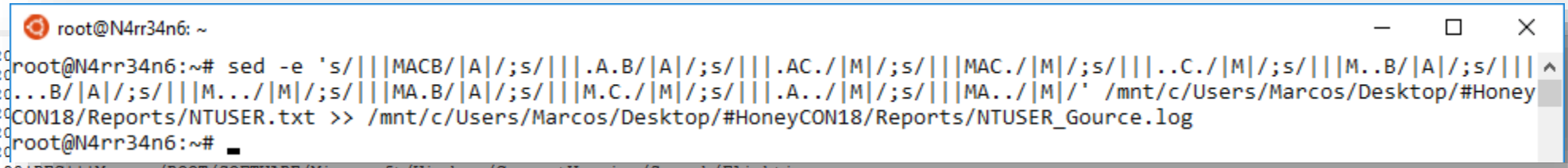
https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

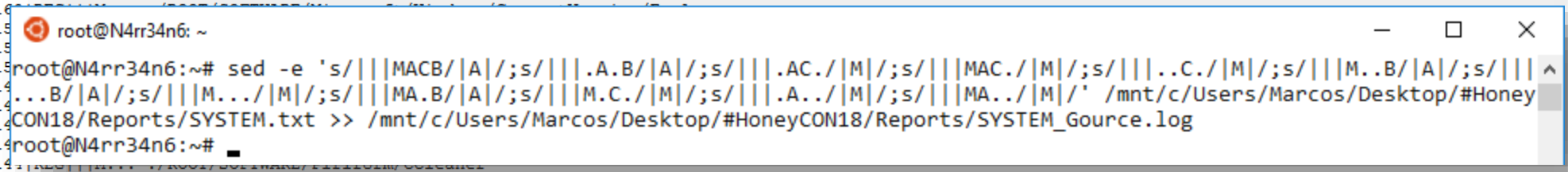
gource.exe -f --log-format custom --realtime -f -1280x720 -s 1 -a 1 --highlight-dirs --key --auto-skip-seconds 1 “C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Gource\Eventos_Gource.log”

Demo effect? Video 02

Custom Log Format, (Regtime)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format






```
1508531198|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Search/Flighting
1508531195|REG|||M... ./ROOT/Control Panel/Desktop
1508531195|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/Wallpapers
1508531192|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows NT/CurrentVersion/AppCompatFlags/Compatibility Assistant/Store
1508531163|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/Connections
1508531163|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Search/RecentApps
1508531163|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Search/RecentApps/{14E94377-B8B5-4791-B791-731E3915B1E4}
1508531162|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Security and Maintenance/Checks/{852FB1F8-5CC6-4567-9C0E-7C330F8807C2}.check.100
1508531162|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Security and Maintenance/Checks/{852FB1F8-5CC6-4567-9C0E-7C330F8807C2}.check.101
1508531161|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/ContentDeliveryManager/Health/Placement-10
1508531138|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/FileExts
1508531133|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/CIDSizeMRU
1508531130|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32
1508531130|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/LastVisitedPidlMRULegacy
1508531103|REG|||M... ./ROOT/SOFTWARE/Microsoft/Internet Explorer
1508531103|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/RecentDocs
1508531074|REG|||M... ./ROOT/SOFTWARE/Microsoft/Internet Explorer/Main
1508531074|REG|||M... ./ROOT/SOFTWARE/Microsoft/Internet Explorer/Main/WindowsSearch
1508531074|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/5.0/Cache/Extensible Cache
1508531074|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows Search/ProcessedSearchRoots
1508531074|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows Search/ProcessedSearchRoots/0004
1508531055|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Run
1508531053|REG|||M... ./ROOT/SOFTWARE/Microsoft
1508531048|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Search/RecentApps/{4BD5D865-FBBF-4837-A12C-BDB4BDEF35A4}
1508531039|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/CD Burning/Drives/Volume{5ed1a5e8-b43b-11e7-9c07-806e6f6e6963}
1508531039|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/CD Burning/StagingInfo/Volume{5ed1a5e8-b43b-11e7-9c07-806e6f6e6963}
1508531039|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/HomeGroup
1508531029|REG|||M... ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/PushNotifications
```

Custom Log Format, (Regtime)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

```
root@N4rr34n6: ~
root@N4rr34n6:~# sed -e 's/|||MACB/|A|/;s/|||.A.B/|A|/;s/|||.AC./|M|/;s/|||MAC./|M|/;s/|||..C./|M|/;s/|||M..B/|A|/;s/|||
...B/|A|/;s/|||M.../|M|/;s/|||MA.B/|A|/;s/|||M.C./|M|/;s/|||.A../|M|/;s/|||MA../|M|/' /mnt/c/Users/Marcos/Desktop/#Honey
CON18/Reports/NTUSER.txt >> /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/NTUSER_Gource.log
root@N4rr34n6:~#
```

```
1508531198|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Search/Flighting
1508531195|REG|M| ./ROOT/Control Panel/Desktop
1508531195|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/Wallpapers
1508531192|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows NT/CurrentVersion/AppCompatFlags/Compatibility Assistant/Store
1508531163|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/Connections
1508531163|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Search/RecentApps
1508531163|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Search/RecentApps/{14E94377-B8B5-4791-B791-731E3915B1E4}
1508531162|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Security and Maintenance/Checks/{852FB1F8-5CC6-4567-9C0E-7C330F8807C2}.check.100
1508531162|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Security and Maintenance/Checks/{852FB1F8-5CC6-4567-9C0E-7C330F8807C2}.check.101
1508531161|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/ContentDeliveryManager/Health/Placement-10
```

```
root@N4rr34n6: ~
root@N4rr34n6:~# sed -e 's/|||MACB/|A|/;s/|||.A.B/|A|/;s/|||.AC./|M|/;s/|||MAC./|M|/;s/|||..C./|M|/;s/|||M..B/|A|/;s/|||
...B/|A|/;s/|||M.../|M|/;s/|||MA.B/|A|/;s/|||M.C./|M|/;s/|||.A../|M|/;s/|||MA../|M|/' /mnt/c/Users/Marcos/Desktop/#Honey
CON18/Reports/SYSTEM.txt >> /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/SYSTEM_Gource.log
root@N4rr34n6:~#
```

```
1508531138|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/FileExts
1508531133|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/CIDSizeMRU
1508531130|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32
1508531130|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/LastVisitedPidlMRULegacy
1508531103|REG|M| ./ROOT/SOFTWARE/Microsoft/Internet Explorer
1508531103|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/RecentDocs
1508531074|REG|M| ./ROOT/SOFTWARE/Microsoft/Internet Explorer/Main
1508531074|REG|M| ./ROOT/SOFTWARE/Microsoft/Internet Explorer/Main/WindowsSearch
1508531074|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Internet Settings/5.0/Cache/Extensible Cache
1508531074|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows Search/ProcessedSearchRoots
1508531074|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows Search/ProcessedSearchRoots/0004
1508531055|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Run
1508531053|REG|M| ./ROOT/SOFTWARE/Microsoft
1508531048|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Search/RecentApps/{4BD5D865-FBBF-4837-A12C-BDB4BDEF35A4}
1508531039|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/CD Burning/Drives/Volume{5ed1a5e8-b43b-11e7-9c07-806e6f6e6963}
1508531039|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/CD Burning/StagingInfo/Volume{5ed1a5e8-b43b-11e7-9c07-806e6f6e6963}
1508531039|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/HomeGroup
1508531029|REG|M| ./ROOT/SOFTWARE/Microsoft/Windows/CurrentVersion/PushNotifications
```

Custom Log Format, (Regtime)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

gource.exe -f --log-format custom --realtime -f -1280x720 -s 1 -a 1 --highlight-dirs --key --auto-skip-seconds 1 --highlight-dirs "C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Gource\Registry_Gource_sort.log"

Demo effect? Video 03

MACTime2Gource

https://github.com/hartek

Mactime2Gource.py - C:\Users\Marcos\Desktop\#HoneyCON18\Tools\Mactime2Gource.py (2.7.15)

File Edit Format Run Options Window Help

```
#!/usr/bin/python3

import sys, datetime, re

def main():
    # Regex to match the lines
    regex_date = "^(\D+\s\D+\s\d+\s\d+\s\d\d:\d\d:\d\d)\s+\d*\s+(....)\s+.+\s\d*\s+\d*\s+\d*.\d*.\d*.\s+(.*)$"
    regex_nodate = "^\s+\d*\s+(....)\s+.+\s\d*\s+\d*\s+\d*.\d*.\d*.\s+(.*)$"

    # Open input file
    filename = sys.argv[1]
    lines = open(filename, "r")

    # Last date detected, to keep control of multiple entries
    date_last = ""

    for line in lines:
        line = line.rstrip()
        #print("Original: " + line)

        # Check if date line or sub-entry, and parse
        matches = re.search(regex_date,line)
        if matches:
            date_last = parse(matches, 1, date_last)
        if not matches:
            matches = re.search(regex_nodate,line)
            date_last = parse(matches, 0, date_last)
        if not matches:
            print("Error in line!")
            exit()

# Parses a line. Offset set to 1 if line with date, 0 if sub-entry.
def parse(matches, offset, date_last):
    # Parse date
    if offset == 1:
        date_match = matches.group(1)
        date = datetime.datetime.strptime(date_match, "%a %b %d %Y %H:%M:%S")
        date_seconds = (date - datetime.datetime(1970,1,1)).total_seconds()
    else:
        date_seconds = date_last
```

Ln: 1 Col: 0

MACTime2Gource

https://github.com/hartek

Mactime2G | Mactime2Gource.py - C:\Users\Marcos\Desktop\#HoneyCON18\Tools\Mactime2Gource.py (2.7.15)

File Edit Format Run Options Window Help

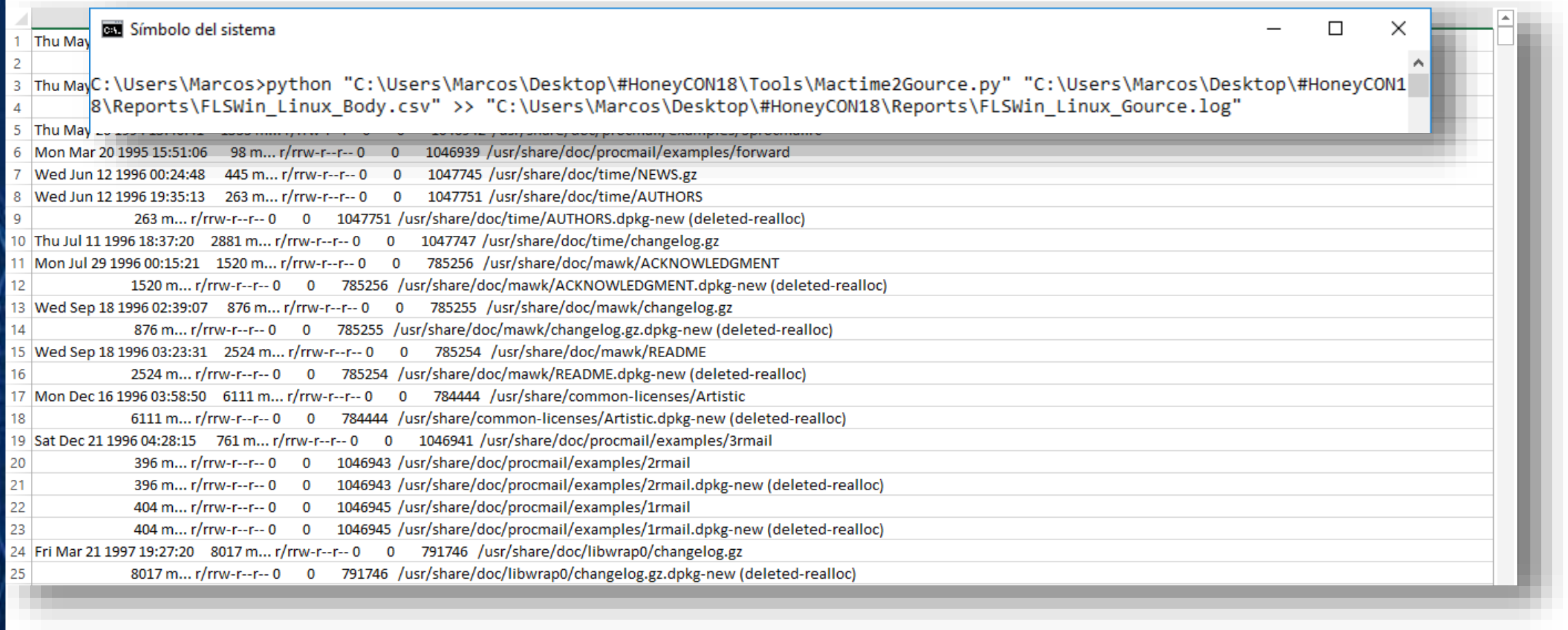
```
#!/usr/bir
import sys

def main()
    # Rege
    regex_
    regex_

    # Oper
    filena
    lines

    # Last
    date_l

    for li
        li
        #p

        #
        ma
        if

        if

        if

# Parses a
def parse(
    # Pars
    if off
        da
        da
        da
    else:
        da

    # Pars
```

```
        date_seconds = (date - datetime.datetime(1970,1,1)).total_seconds()
    else:
        date_seconds = date_last

    # Parse M/A/C/B flag to A/M/D
    macb_match = matches.group(1+offset)
    if re.match("..c.",macb_match):
        macb = 'M'
    elif re.match("m...",macb_match):
        macb = 'M'
    elif re.match("...b",macb_match):
        macb = 'A'
    elif re.match(".a..",macb_match):
        macb = 'M'
    elif re.match("....",macb_match):
        macb = 'D'

    # Parse path
    path = matches.group(2+offset)
    # Was it deleted? Cut and set MACB to D(eleted)
    if path.endswith("(deleted)"):
        path = path[:-10]
        macb = 'D'
        #print(path)
    elif path.endswith("(deleted-realloc)"):
        path = path[:-18]
        macb = 'D'
    # Trim ($FILE_NAME)
    if path.endswith("($FILE_NAME)"):
        path = path[:-13]

    # Print results
    print(str(int(date_seconds)) + "|USER|" + macb + "|" + path)

    # Return last date detected
    return date_seconds


if __name__ == "__main__":
    main()
```

Ln: 1 Col: 0

MACTime2Gource

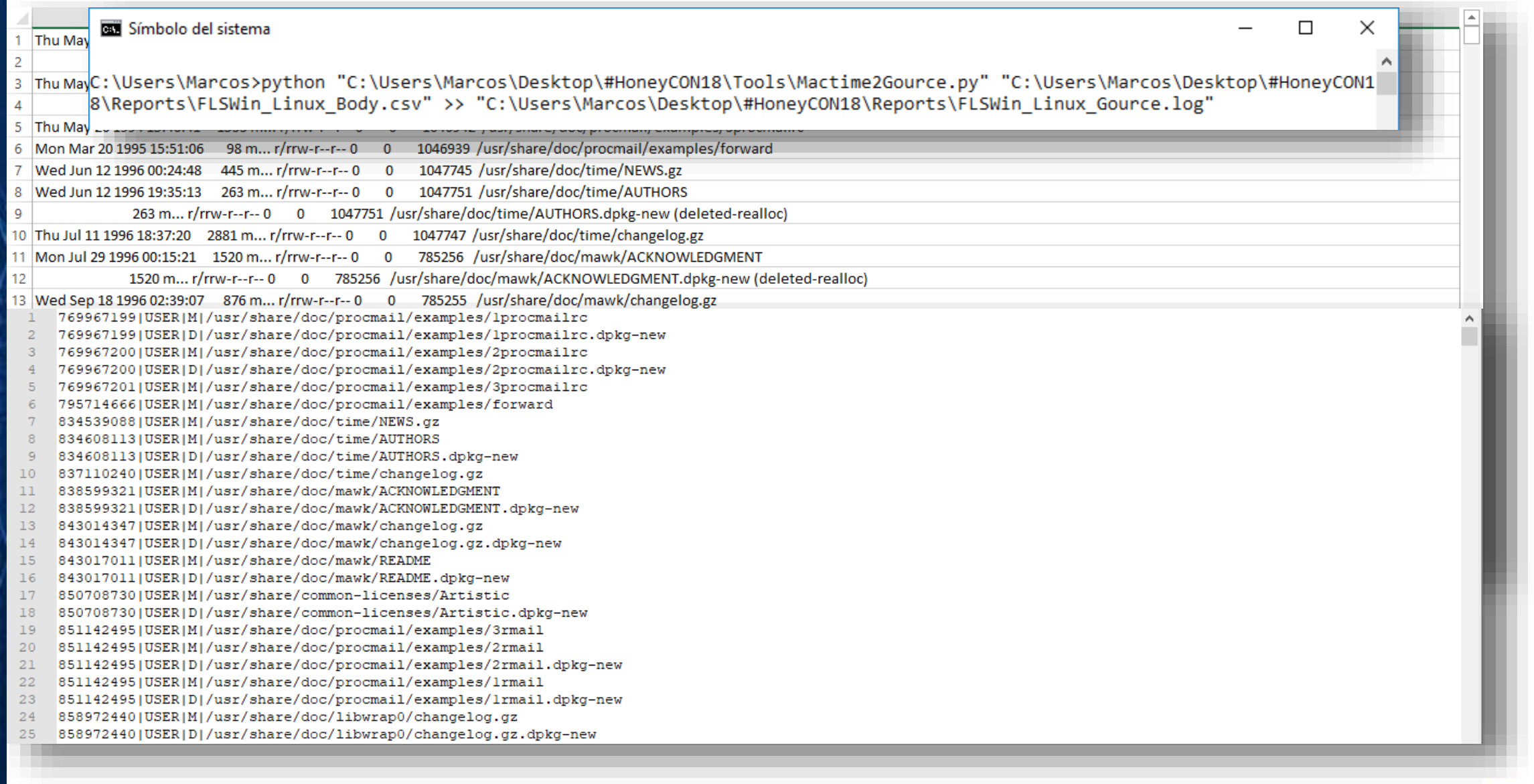
https://github.com/hartek



1	Thu May
2	
3	Thu May
4	
5	Thu May
6	Mon Mar 20 1995 15:51:06 98 m... r/rrw-r--r-- 0 0 1046939 /usr/share/doc/procmail/examples/forward
7	Wed Jun 12 1996 00:24:48 445 m... r/rrw-r--r-- 0 0 1047745 /usr/share/doc/time/NEWS.gz
8	Wed Jun 12 1996 19:35:13 263 m... r/rrw-r--r-- 0 0 1047751 /usr/share/doc/time/AUTHORS
9	263 m... r/rrw-r--r-- 0 0 1047751 /usr/share/doc/time/AUTHORS.dpkg-new (deleted-realloc)
10	Thu Jul 11 1996 18:37:20 2881 m... r/rrw-r--r-- 0 0 1047747 /usr/share/doc/time/changelog.gz
11	Mon Jul 29 1996 00:15:21 1520 m... r/rrw-r--r-- 0 0 785256 /usr/share/doc/mawk/ACKNOWLEDGMENT
12	1520 m... r/rrw-r--r-- 0 0 785256 /usr/share/doc/mawk/ACKNOWLEDGMENT.dpkg-new (deleted-realloc)
13	Wed Sep 18 1996 02:39:07 876 m... r/rrw-r--r-- 0 0 785255 /usr/share/doc/mawk/changelog.gz
14	876 m... r/rrw-r--r-- 0 0 785255 /usr/share/doc/mawk/changelog.gz.dpkg-new (deleted-realloc)
15	Wed Sep 18 1996 03:23:31 2524 m... r/rrw-r--r-- 0 0 785254 /usr/share/doc/mawk/README
16	2524 m... r/rrw-r--r-- 0 0 785254 /usr/share/doc/mawk/README.dpkg-new (deleted-realloc)
17	Mon Dec 16 1996 03:58:50 6111 m... r/rrw-r--r-- 0 0 784444 /usr/share/common-licenses/Artistic
18	6111 m... r/rrw-r--r-- 0 0 784444 /usr/share/common-licenses/Artistic.dpkg-new (deleted-realloc)
19	Sat Dec 21 1996 04:28:15 761 m... r/rrw-r--r-- 0 0 1046941 /usr/share/doc/procmail/examples/3rmail
20	396 m... r/rrw-r--r-- 0 0 1046943 /usr/share/doc/procmail/examples/2rmail
21	396 m... r/rrw-r--r-- 0 0 1046943 /usr/share/doc/procmail/examples/2rmail.dpkg-new (deleted-realloc)
22	404 m... r/rrw-r--r-- 0 0 1046945 /usr/share/doc/procmail/examples/1rmail
23	404 m... r/rrw-r--r-- 0 0 1046945 /usr/share/doc/procmail/examples/1rmail.dpkg-new (deleted-realloc)
24	Fri Mar 21 1997 19:27:20 8017 m... r/rrw-r--r-- 0 0 791746 /usr/share/doc/libwrap0/changelog.gz
25	8017 m... r/rrw-r--r-- 0 0 791746 /usr/share/doc/libwrap0/changelog.gz.dpkg-new (deleted-realloc)

MACTime2Gource

https://github.com/hartek



MACTime2Gource

https://github.com/hartek

Demo MacTime2Gource

MACTime2Gource

https://github.com/hartek

gource.exe --log-format custom --realtime -f -1280x720 -s 1 -a 1 --highlight-dirs --key --auto-skip-seconds 1 --highlight-dirs --title “@_N4rr34n6_: Mactime2Gource.py” “C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Gource\FLSWin_Linux_Gource.log”

Demo effect? Video 06-07

MACTime2Gource

https://github.com/hartek

gource.exe --log-format custom --realtime -f -1280x720 -s 1 -a 1 --highlight-dirs --key --auto-skip-seconds 1 --highlight-dirs --title “@_N4rr34n6_: Mactime2Gource.py” “C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Gource\FLSWin_Win10x64_Gource.log”

Demo effect? Video 04-05

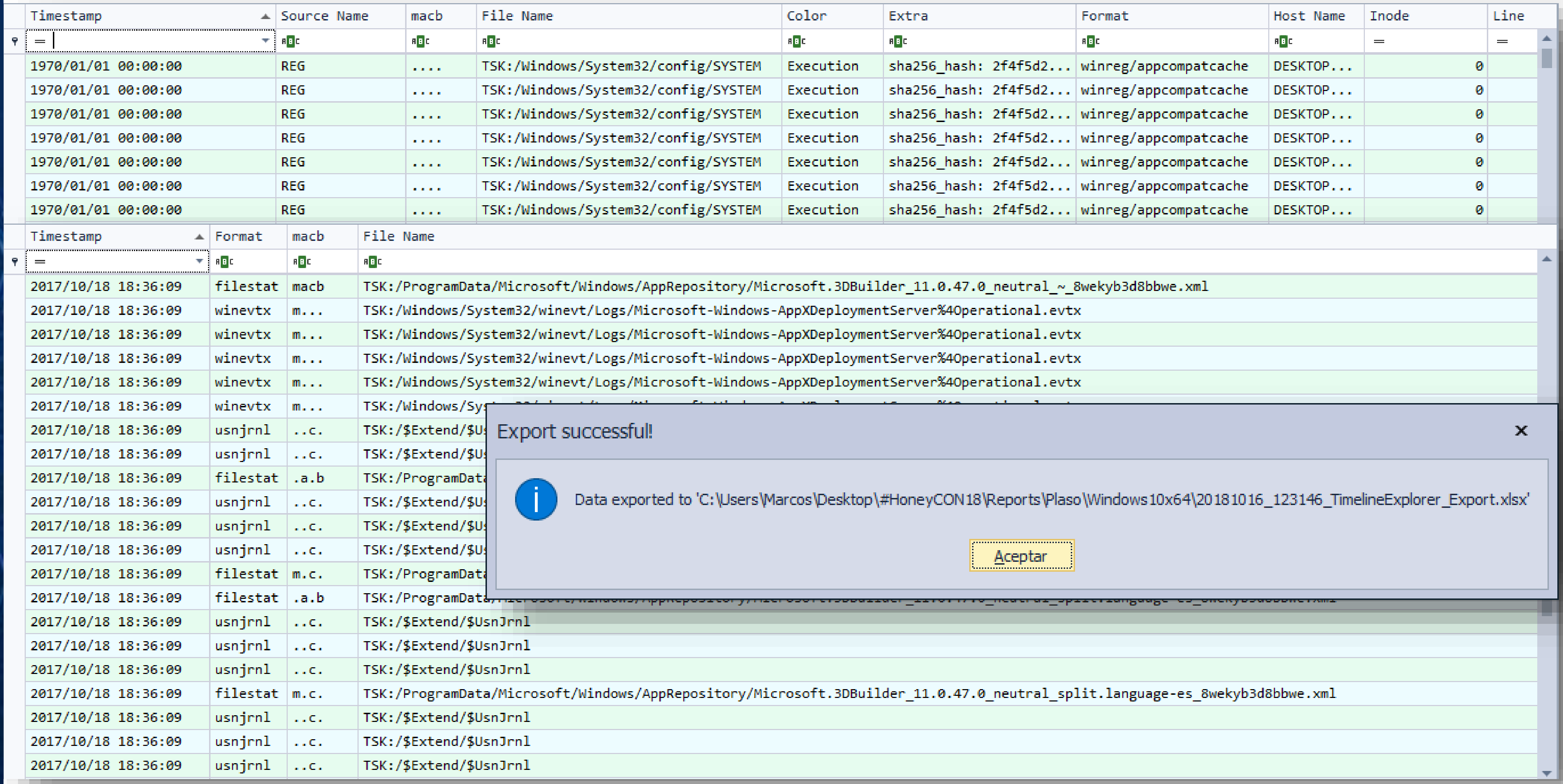
Custom Log Format, (Plaso)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

Timestamp	Source Name	macb	File Name	Color	Extra	Format	Host Name	Inode	Line
=	ABC	ABC	ABC	ABC	ABC	ABC	ABC	=	=
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	
1970/01/01 00:00:00	REG	....	TSK:/Windows/System32/config/SYSTEM	Execution	sha256_hash: 2f4f5d2...	winreg/appcompatcache	DESKTOP...	0	

Custom Log Format, (Plaso)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format



Custom Log Format, (Plaso)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

=(A2-B2)*86400

	C	D	E	
1	Epoch	Format	macb	File Name
2	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
3	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
4	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
5	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
6	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
7	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
8	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
9	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
10	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
11	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
12	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
13	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
14	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
15	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
16	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
17	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
18	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
19	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
20	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
21	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
22	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
23	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
24	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
25	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM

Custom Log Format, (Plaso)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

	C	D	E	
1	Epoch	Format	macb	File Name
2	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
3	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
4	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
5	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
6	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
7	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
8	0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM

=(A2-B2)*86400

```
1   0   winreg/appcompatcache   ....   TSK:/Windows/System32/config/SYSTEM
2   0   winreg/appcompatcache   ....   TSK:/Windows/System32/config/SYSTEM
3   0   winreg/appcompatcache   ....   TSK:/Windows/System32/config/SYSTEM
4   0   winreg/appcompatcache   ....   TSK:/Windows/System32/config/SYSTEM
5   0   winreg/appcompatcache   ....   TSK:/Windows/System32/config/SYSTEM
```

```
814201  1508531211  filestat    m.c.    TSK:/$Extend/$RmMetadata/$TxfLog/$TxfLog.blf
814202  4294967295  pe  m...    TSK:/Users/Marcos/AppData/Local/Microsoft/OneDrive/17.3.6381.0405_1/sqmapi.dll
814203  4294967295  pe  m...    TSK:/Windows/System32/WindowsPowerShell/v1.0/pspluginwkr.dll
814204  4294967295  pe  m...    TSK:/Windows/WinSxS/amd64_microsoft-windows-p..man-pluginworker-v2_31bf3856ad364e35_10.0.14393.0_none_c4eb24a40957ab54/pspluginwkr.dll
814205  4294967295  pe  m...    TSK:/Windows/SysWOW64/WindowsPowerShell/v1.0/pspluginwkr.dll
814206  4294967295  pe  m...    TSK:/Windows/WinSxS/wow64_microsoft-windows-p..man-pluginworker-v2_31bf3856ad364e35_10.0.14393.0_none_cf3fcef63db86d4f/pspluginwkr.dll
814207  4294967295  pe  m...    TSK:/Windows/SysWOW64/mfc40u.dll
814208  4294967295  pe  m...    TSK:/Windows/WinSxS/x86_microsoft-windows-mfc40u_31bf3856ad364e35_10.0.14393.0_none_c468e1fcb3e56cba/mfc40u.dll
814209  4294967295  pe  m...    TSK:/Users/Marcos/AppData/Local/Microsoft/OneDrive/17.3.6381.0405_1/sqmapi.dll
814210  4294967295  pe  m...    TSK:/Windows/System32/WindowsPowerShell/v1.0/pspluginwkr.dll
814211  4294967295  pe  m...    TSK:/Windows/WinSxS/amd64_microsoft-windows-p..man-pluginworker-v2_31bf3856ad364e35_10.0.14393.0_none_c4eb24a40957ab54/pspluginwkr.dll
814212  4294967295  pe  m...    TSK:/Windows/SysWOW64/WindowsPowerShell/v1.0/pspluginwkr.dll
814213  4294967295  pe  m...    TSK:/Windows/WinSxS/wow64_microsoft-windows-p..man-pluginworker-v2_31bf3856ad364e35_10.0.14393.0_none_cf3fcef63db86d4f/pspluginwkr.dll
814214  4294967295  pe  m...    TSK:/Windows/SysWOW64/mfc40u.dll
814215  4294967295  pe  m...    TSK:/Windows/WinSxS/x86_microsoft-windows-mfc40u_31bf3856ad364e35_10.0.14393.0_none_c468e1fcb3e56cba/mfc40u.dll
814216  4294967295  pe  m...    TSK:/Windows/SysWOW64/mfc40u.dll
814217  4294967295  pe  m...    TSK:/Windows/WinSxS/x86_microsoft-windows-mfc40u_31bf3856ad364e35_10.0.14393.0_none_c468e1fcb3e56cba/mfc40u.dll
814218  4294967295  pe  m...    TSK:/Users/Marcos/AppData/Local/Microsoft/OneDrive/17.3.6381.0405_1/sqmapi.dll
814219  4294967295  pe  m...    TSK:/Windows/SysWOW64/mfc40u.dll
814220  4294967295  pe  m...    TSK:/Windows/WinSxS/x86_microsoft-windows-mfc40u_31bf3856ad364e35_10.0.14393.0_none_c468e1fcb3e56cba/mfc40u.dll
814221  4294967295  pe  m...    TSK:/Windows/System32/WindowsPowerShell/v1.0/pspluginwkr.dll
814222  4294967295  pe  m...    TSK:/Windows/WinSxS/amd64_microsoft-windows-p..man-pluginworker-v2_31bf3856ad364e35_10.0.14393.0_none_c4eb24a40957ab54/pspluginwkr.dll
814223  4294967295  pe  m...    TSK:/Windows/SysWOW64/WindowsPowerShell/v1.0/pspluginwkr.dll
814224  4294967295  pe  m...    TSK:/Windows/WinSxS/wow64_microsoft-windows-p..man-pluginworker-v2_31bf3856ad364e35_10.0.14393.0_none_cf3fcef63db86d4f/pspluginwkr.dll
814225  4294967295  pe  m...    TSK:/Users/Marcos/AppData/Local/Microsoft/OneDrive/17.3.6381.0405_1/sqmapi.dll
```

Custom Log Format, (Plaso)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

```
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
0    winreg/appcompatcache    ....    TSK:/Windows/System32/config/SYSTEM
```

Custom Log Format, (Plaso)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

root@N4rr34n6: ~

```
root@N4rr34n6:~# sed -e 's/\tmacb/|A/;s/\t.a.b/|A/;s/\t.ac./|M/;s/\tmac./|M/;s/\t..c./|M/;s/\tm..b/|A/;s/\t...b/|A/;s/\tm.../|M/;s/\tma.b/|A/;s/\tm.c./|M/;s/\t.a../|M/;s/\tma../|M/;s/[.][.][.][.]/D/;s/\t/|/;s/\t/|/;s/\t/|/' /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/Plaso/Windows10x64/Plaso_Windows_1.txt >> /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/Gource/Plaso_Windows_1.log
root@N4rr34n6:~#
```

```
0
0
0
0
0
0
0
0
0	winreg/appcompatcache	....	TSK:/Windows/System32/config/SYSTEM
0	winreg/appcompatcache	....	TSK:/Windows/System32/config
0	winreg/appcompatcache	....	TSK:/Windows/System32/config
0	winreg/appcompatcache	....	TSK:/Windows/System32/config
0	winreg/appcompatcache	....	TSK:/Windows/System32/config
0	winreg/appcompatcache	....	TSK:/Windows/System32/config
0	winreg/appcompatcache	....	TSK:/Windows/System32/config
0	winreg/appcompatcache	....	TSK:/Windows/System32/config
0	winreg/appcompatcache	....	TSK:/Windows/System32/config
0	winreg/appcompatcache	....	TSK:/Windows/System32/config
0	winreg/appcompatcache	....	TSK:/Windows/System32/config
0	winreg/appcompatcache	....	TSK:/Windows/System32/config
0	winreg/appcompatcache	....	TSK:/Windows/System32/config
0	winreg/appcompatcache	....	TSK:/Windows/System32/config
0	winreg/appcompatcache	....	TSK:/Windows/System32/config
0	winreg/appcompatcache	....	TSK:/Windows/System32/config
0	winreg/appcompatcache	....	TSK:/Windows/System32/config
```

```
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
0|winreg/appcompatcache|D|TSK:/Windows/System32/config/SYSTEM
```

Custom Log Format, (Plaso)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

gource.exe --log-format custom --realtime -f -1280x720 -s 1 -a 1 --highlight-dirs --key --auto-skip-seconds 1 --highlight-dirs --title “@_N4rr34n6_: Plaso Windows” --start-date 2017-10-20 “C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Gource\Plaso_Windows_1.log”

Demo effect? Video 09-10-11-12

Custom Log Format, (Plaso)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

=A2&" "&B2

=(A2)*86400

	A	B	C	D	E
1	date	time	MACB	sourcetype	short
2	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/man/man3/Perl4::CoreLibs.3pm.gz
3	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/man/man1/smtp-sink.1.gz
4	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/man/man1/setfacl.1.gz
5	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/man/man3/DBI::ProfileDumper::Apache.3pm.gz
6	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/doc/liblogging-stdlog0/changelog.Debian.gz
7	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/i18n/charmaps/TIS-620.gz
8	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/man/man7/systemd.journal-fields.7.gz
9	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/man/man3/HTML::FormatRTF.3pm.gz
10	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/doc/python-debian/examples/debfile/changelog_head.gz
11	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/man/man8/mount.8.gz
12	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/man/man1/dpkg-deb.1.gz
13	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/doc/texinfo/txirefcard.pdf.gz
14	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/man/man8/sudoreplay.8.gz
15	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/man/man3/HTML::Entities.3pm.gz
16	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/man/man3/HTTP::Status.3pm.gz
17	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/man/pl/man8/shadowconfig.8.gz
18	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/man/man5/os-release.5.gz
19	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/man/man1/prtstat.1.gz
20	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/man/man1/resize-part-image.1.gz
21	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/i18n/charmaps/JIS_C6229-1984-HAND.gz
22	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/i18n/charmaps/IBM874.gz
23	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/info/grub-dev.info.gz
24	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/doc/libnet-ssleay-perl/examples/x509_cert_details.pl.gz
25	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/man/man1/asn1parse.1ssl.gz

Custom Log Format, (Plaso)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

	A	B
1	Time|Source|Host|User|Description	
2	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
3	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
4	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
5	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
6	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
7	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
8	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
9	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
10	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
11	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
12	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
13	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
14	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
15	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
16	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
17	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
18	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
19	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
20	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
21	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
22	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
23	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
24	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time
25	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time

23	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/info/grub-dev.info.gz
24	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/doc/libnet-ssleay-perl/examples/x509_cert_details.pl.gz
25	1970/01/01 00:00:00	1900/01/00 00:00:00	M...	GZIP Content Modification Time	/usr/share/man/man1/asn1parse.1ssl.gz

Custom Log Format, (Plaso)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

root@N4rr34n6: ~

```
root@N4rr34n6:~# sed -e 's/team.*[0-9];//;s/| Content Modification Time;/|M|/;s/| Creation Time;/|A|/;s/| Last Access Time;/|M|/;s/| Metadata Modification Time;/|M|/;s/| Start Time;/|A|/' /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/Plaso/Linux/Plaso_ImagenDiscoMOOC_tln.csv >> /mnt/c/Users/Marcos/Desktop/#HoneyCON18/Reports/Gource/Plaso_Linux_TLN.log
root@N4rr34n6:~#
```

1	Time|So			
2	0|FILE|t			
3	0|FILE|t			
4	0|FILE|t			
5	0|FILE|t			
6	0|FILE|t			
7	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time	GZIP:/usr/share/i18n/charmaps/TIS-620.gz Type: file	
8	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time	GZIP:/usr/share/man/man7/systemd.journal-fields.7.gz Type: file	
9	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time	GZIP:/usr/share/man/man3/HTML::FormatRTF.3pm.gz Type: file	
10	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time	GZIP:/usr/share/doc/python-debian/examples/debfile/changelog_head.gz Type: file	
11	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time	GZIP:/usr/share/man/man8/mount.8.gz Type: file	
12	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time	GZIP:/usr/share/man/man1/dpkg-deb.1.gz Type: file	
13	0|FILE|team-0002|-|1970-01-01T00:00:00+00:00	Content Modification Time	GZIP:/usr/share/doc/texinfo/txirefcard.pdf.gz Type: file	

```
Time|Source|Host|User|Description;;
0|FILE|M| GZIP:/usr/share/man/man3/Perl4::CoreLibs.3pm.gz Type: file
0|FILE|M| GZIP:/usr/share/man/man1/smtp-sink.1.gz Type: file
0|FILE|M| GZIP:/usr/share/man/man1/setfacl.1.gz Type: file
0|FILE|M| GZIP:/usr/share/man/man3/DBI::ProfileDumper::Apache.3pm.gz Type: file
0|FILE|M| GZIP:/usr/share/doc/liblogging-stdlog0/changelog.Debian.gz Type: file
0|FILE|M| GZIP:/usr/share/i18n/charmaps/TIS-620.gz Type: file
0|FILE|M| GZIP:/usr/share/man/man7/systemd.journal-fields.7.gz Type: file
0|FILE|M| GZIP:/usr/share/man/man3/HTML::FormatRTF.3pm.gz Type: file
0|FILE|M| GZIP:/usr/share/doc/python-debian/examples/debfile/changelog_head.gz Type: file
0|FILE|M| GZIP:/usr/share/man/man8/mount.8.gz Type: file
0|FILE|M| GZIP:/usr/share/man/man1/dpkg-deb.1.gz Type: file
0|FILE|M| GZIP:/usr/share/doc/texinfo/txirefcard.pdf.gz Type: file
0|FILE|M| GZIP:/usr/share/man/man8/sudoreplay.8.gz Type: file
0|FILE|M| GZIP:/usr/share/man/man3/HTML::Entities.3pm.gz Type: file
0|FILE|M| GZIP:/usr/share/man/man3/HTTP::Status.3pm.gz Type: file
0|FILE|M| GZIP:/usr/share/man/pl/man8/shadowconfig.8.gz Type: file
0|FILE|M| GZIP:/usr/share/man/man5/os-release.5.gz Type: file
0|FILE|M| GZIP:/usr/share/man/man1/prtstat.1.gz Type: file
0|FILE|M| GZIP:/usr/share/man/man1/resize-part-image.1.gz Type: file
0|FILE|M| GZIP:/usr/share/i18n/charmaps/JIS_C6229-1984-HAND.gz Type: file
0|FILE|M| GZIP:/usr/share/i18n/charmaps/IBM874.gz Type: file
0|FILE|M| GZIP:/usr/share/info/grub-dev.info.gz Type: file
0|FILE|M| GZIP:/usr/share/doc/libnet-ssleay-perl/examples/x509_cert_details.pl.gz Type: file
0|FILE|M| GZIP:/usr/share/man/man1/asn1parse.1ssl.gz Type: file
```

Custom Log Format, (Plaso)

https://github.com/acaudwell/Gource/wiki/Custom-Log-Format

gource.exe" --log-format custom --realtime -f -1280x720 -s 1 -a 1 --highlight-dirs --key --auto-skip-seconds 1 --highlight-dirs --title "@_N4rr34n6_: Plaso Linux" "C:\Users\Marcos\Desktop\#HoneyCON18\Reports\Gource\Plaso_Linux_TLN_EGREP.log" --start-date 2016-10-01 -c 0.20

Demo effect? Video 13

Conclusiones

- La línea de tiempo es un **paso fundamental** de un análisis
- **Multitud de herramientas** para su generación y visualización
- **Todo artefacto** con marcas de tiempo puede ser objeto de ello
- **Ayuda a entender** qué ha pasado
- Buena **referencia**
- El único límite es…

Tu **imaginación**

Muchas gracias por su atención

Lo hizo un mago