PRÁCTICA 4: ADQUISICIÓN Y ANÁLISIS DE EVIDENCIAS VOLÁTILES

IZAN NAVARRO LUJAN

IES SERRA PERENXISA

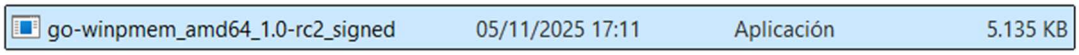
INDICE

1. Configuración Previa:

1) Instalación de Volatility3 para volcados de W11:

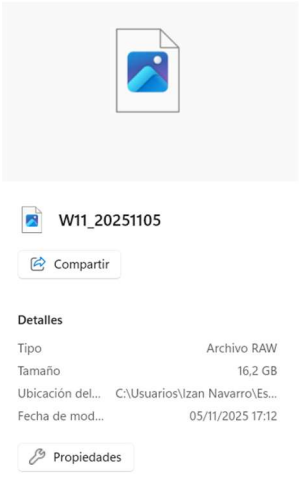

```
An open-source memory forensics framework

options:
  -h, --help            Show this help message and exit, for specific plugin options use 'vol.py <pluginname> --help'
  -c, --config CONFIG   Load the configuration from a json file
  --parallelism [{processes,threads,off}]
                        Enables parallelism (defaults to off if no argument given)
  -e, --extend EXTEND   Extend the configuration with a new (or changed) setting
  -p, --plugin-dirs PLUGIN_DIRS
                        Semi-colon separated list of paths to find plugins
  -s, --symbol-dirs SYMBOL_DIRS
                        Semi-colon separated list of paths to find symbols
  -v, --verbosity       Increase output verbosity
  -l, --log LOG         Log output to a file as well as the console
  -o, --output-dir OUTPUT_DIR
                        Directory in which to output any generated files
  -q, --quiet           Remove progress feedback
  -f, --file FILE       Shorthand for --single-location=file:// if single-location is not defined
  --write-config        Write configuration JSON file out to config.json
  --save-config SAVE_CONFIG
                        Save configuration JSON file to a file
  --clear-cache         Clears out all short-term cached items
  --cache-path CACHE_PATH
                        Change the default path (C:\Users\Izan Navarro\AppData\Roaming\volatility3) used to store the
```

2) Descargar la aplicación WinPmen para obtener una copia de la memoria RAM del equipo:



Ahora realizamos la copia con este comando SIEMPRE ENTRANDO COMO ADMINISTRADOR EN EL CMD:

```
C:\Users\Izan Navarro\Downloads> go-winpmem_amd64_1.0-rc2_signed.exe acquire W11_20251105
```



El tamaño del archivo debe de coincidir con el de la RAM de tu equipo.

3) Instalamos Python3 para poder utilizar volatility3:

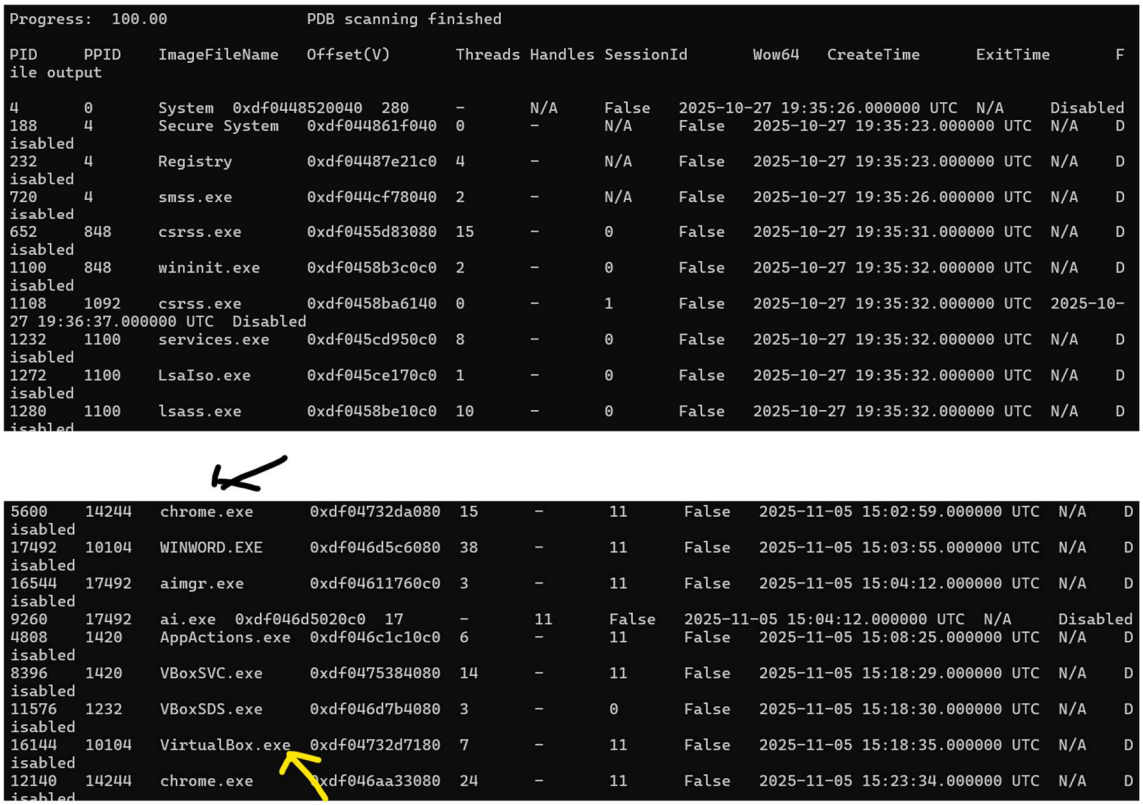
```
C:\Users\Izan Navarro>python --version
Python 3.13.7
```

2. Ejercicio 1:

En este apartado deberás obtener la siguiente información a partir del volcado de memoria obtenido. En cada apartado deberán responder anotando el comando utilizado y la captura de pantalla con la información obtenida. Adjunta también un enlace compartido que apunte a tu volcado de memoria.

• Apartado a: Obtener los procesos en ejecución

Para este apartado, ejecutaremos el comando “python vol.py -f ‘C:\Users\Izan Navarro\Desktop\CIBERSEGURIDAD\CE_Ciberseguridad\ANALISIS_FORENSE\VOLCADO_RAM\W11_20251105.raw’ windows.pslist” y nos debería salir un esquema de procesos como el siguiente:



```
Progress:  100.00               PDB scanning finished

PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        F
ile output

4       0       System  0xdf04485200040  280     -       N/A     False   2025-10-27 19:35:26.000000 UTC  N/A     Disabled
188     4       Secure System   0xdf044861f040  0       -       N/A     False   2025-10-27 19:35:23.000000 UTC  N/A     D
isabled
232     4       Registry        0xdf04487e21c0  4       -       N/A     False   2025-10-27 19:35:23.000000 UTC  N/A     D
isabled
720     4       smss.exe        0xdf044cf78040  2       -       N/A     False   2025-10-27 19:35:26.000000 UTC  N/A     D
isabled
652     848     csrss.exe       0xdf0455d83080  15      -       0       False   2025-10-27 19:35:31.000000 UTC  N/A     D
isabled
1100    848     wininit.exe     0xdf0458b3c0c0  2       -       0       False   2025-10-27 19:35:32.000000 UTC  N/A     D
isabled
1108    1092    csrss.exe       0xdf0458ba6140  0       -       1       False   2025-10-27 19:35:32.000000 UTC  2025-10-
27 19:36:37.000000 UTC  Disabled
1232    1100    services.exe    0xdf045cd950c0  8       -       0       False   2025-10-27 19:35:32.000000 UTC  N/A     D
isabled
1272    1100    LsaIso.exe      0xdf045ce170c0  1       -       0       False   2025-10-27 19:35:32.000000 UTC  N/A     D
isabled
1280    1100    lsass.exe       0xdf0458be10c0  10      -       0       False   2025-10-27 19:35:32.000000 UTC  N/A     D
isabled
```



```
5600    14244   chrome.exe      0xdf04732da080  15      -       11      False   2025-11-05 15:02:59.000000 UTC  N/A     D
isabled
17492   10104   WINWORD.EXE     0xdf046d5c6080  38      -       11      False   2025-11-05 15:03:55.000000 UTC  N/A     D
isabled
16544   17492   aimgr.exe       0xdf04611760c0  3       -       11      False   2025-11-05 15:04:12.000000 UTC  N/A     D
isabled
9260    17492   ai.exe  0xdf046d5020c0  17      -       11      False   2025-11-05 15:04:12.000000 UTC  N/A     Disabled
4808    1420    AppActions.exe  0xdf046c1c10c0  6       -       11      False   2025-11-05 15:08:25.000000 UTC  N/A     D
isabled
8396    1420    VBoxSVC.exe     0xdf0475384080  14      -       11      False   2025-11-05 15:18:29.000000 UTC  N/A     D
isabled
11576   1232    VBoxSDS.exe     0xdf046d7b4080  3       -       0       False   2025-11-05 15:18:30.000000 UTC  N/A     D
isabled
16144   10104   VirtualBox.exe  0xdf04732d7180  7       -       11      False   2025-11-05 15:18:35.000000 UTC  N/A     D
isabled
12140   14244   chrome.exe      0xdf046aa33080  24      -       11      False   2025-11-05 15:23:34.000000 UTC  N/A     D
isabled
```

• Apartado b: Mostrar las relaciones entre procesos en forma de árbol

Para poder mostrar las relaciones en forma de árbol la terminal evalua los niveles con asteriscos *, pasando de la primera rama (*), a diferentes subramas (**, ***, ****) y así dar a entender la estructura de árbol.

Se podría exportar el resultado de esta terminal a un fichero .csv, .json o pretty pero como me está dando algunos errores, lo muestro directamente por consola y así mejor.

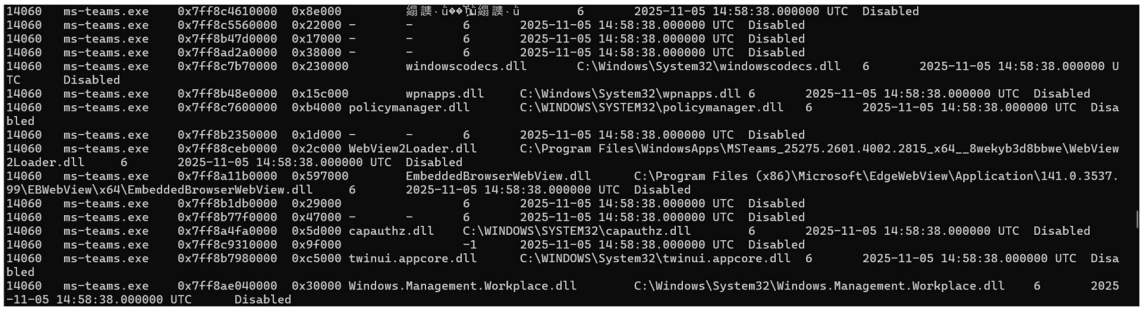
• Apartado c: Listar las librerías dll cargadas por los procesos

Para mostrar las Dlls cargadas en cada proceso ejecutamos el siguiente comando: **“python vol.py -f "C:\Users\Izan Navarro\Desktop\CIBERSEGURIDAD\CE_Ciberseguridad\ANALISIS_FORENSE\VOLCADO_RAM\W11_20251105.raw" windows.dlllist”.**

Este nos mostrará una estructura como está de cada uno de los procesos de la memoria RAM:

-chrome.exe:

-ms-teams.exe:



• Apartado d: Encontrar procesos escondidos en los procesos que está listando

Para mostrar los procesos escondidos/ocultos de los procesos de la RAM usaremos el siguiente comando. **“python vol.py -f "C:\Users\Izan Navarro\Desktop\CIBERSEGURIDAD\CE_Ciberseguridad\ANALISIS_FORENSE\VOLCADO_RAM\W11_20251105.raw" windows.psscan”.**

Este mostrará una estructura como la siguiente de cada uno de los procesos ocultos:

```
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

188     4       Secure System   0xdf044861f040  0       -       N/A     False   2025-10-27 19:35:23.000000 UTC  N/A     Disabled
232     4       Registry        0xdf044487e21c0 4       -       N/A     False   2025-10-27 19:35:23.000000 UTC  N/A     Disabled
7160    9000    cncmd.exe       0xdf044c909080  1       -       11      False   2025-11-05 14:58:45.000000 UTC  N/A     Disabled
720     4       smss.exe        0xdf044cf78040  2       -       N/A     False   2025-10-27 19:35:26.000000 UTC  N/A     Disabled
652     848     csrss.exe       0xdf0455d83080  15      -       0       False   2025-10-27 19:35:31.000000 UTC  N/A     Disabled
2928    1232    amdfendrsr.exe  0xdf0457d840c0  4       -       0       False   2025-10-27 19:35:33.000000 UTC  N/A     Disabled
4212    1232    svchost.exe     0xdf0457e090c0  4       -       0       False   2025-10-27 19:35:34.000000 UTC  N/A     Disabled
5812    11204   msiexec.exe     0xdf0457e3b0c0  0       -       4       True    2025-10-31 11:14:52.000000 UTC  2025-10-31 11:14:53.000000 UTC  Disabled
10972   3008    taskhostw.exe   0xdf0458ac90c0  0       -       0       False   2025-10-29 15:14:23.000000 UTC  2025-10-29 15:14:29.000000 UTC  Disabled
1100    848     wininit.exe     0xdf0458b3c0c0  2       -       0       False   2025-10-27 19:35:32.000000 UTC  N/A     Disabled
1108    1092    csrss.exe       0xdf0458ba6140  0       -       1       False   2025-10-27 19:35:32.000000 UTC  2025-10-27 19:36:37.000000 UTC  Disabled
1280    1100    lsass.exe       0xdf0458be10c0  10      -       0       False   2025-10-27 19:35:32.000000 UTC  N/A     Disabled
12892   1232    svchost.exe     0xdf0458f6c080  12      -       0       False   2025-10-29 15:22:40.000000 UTC  N/A     Disabled
4420    1232    svchost.exe     0xdf0459b740c0  6       -       0       False   2025-10-27 19:35:34.000000 UTC  N/A     Disabled
8840    11204   msiexec.exe     0xdf0459ea10c0  0       -       4       True    2025-10-31 11:12:47.000000 UTC  2025-10-31 11:12:47.000000 UTC  Disabled
1468    1232    WUDFHost.exe    0xdf045b2310c0  5       -       0       False   2025-10-27 19:35:33.000000 UTC  N/A     Disabled
1640    1232    svchost.exe     0xdf045b3e00c0  5       -       0       False   2025-10-27 19:35:33.000000 UTC  N/A     Disabled
1580    1232    svchost.exe     0xdf045b4020c0  10      -       0       False   2025-10-27 19:35:33.000000 UTC  N/A     Disabled
2148    1232    svchost.exe     0xdf045b48f0c0  6       -       0       False   2025-10-27 19:35:33.000000 UTC  N/A     Disabled
2132    1232    svchost.exe     0xdf045b4990c0  3       -       0       False   2025-10-27 19:35:33.000000 UTC  N/A     Disabled
2692    1232    svchost.exe     0xdf045b7b10c0  10      -       0       False   2025-10-27 19:35:33.000000 UTC  N/A     Disabled
2384    1232    svchost.exe     0xdf045b8980c0  7       -       0       False   2025-10-27 19:35:33.000000 UTC  N/A     Disabled
3192    1232    svchost.exe     0xdf045bc820c0  3       -       0       False   2025-10-27 19:35:33.000000 UTC  N/A     Disabled
3680    1232    svchost.exe     0xdf045bc8c0c0  4       -       0       False   2025-10-27 19:35:34.000000 UTC  N/A     Disabled
3448    1232    svchost.exe     0xdf045bd770c0  7       -       0       False   2025-10-27 19:35:34.000000 UTC  N/A     Disabled
1384    1232    SearchIndexer.  0xdf045c3db080  0       -       0       False   2025-10-27 19:35:46.000000 UTC  2025-11-02 15:11:31.000000 UTC  Disabled
15480   11204   msiexec.exe     0xdf045c7170c0  0       -       4       True    2025-10-31 11:06:53.000000 UTC  2025-10-31 11:06:54.000000 UTC  Disabled
15252   11204   msiexec.exe     0xdf045c8100c0  0       -       4       True    2025-10-31 11:14:36.000000 UTC  2025-10-31 11:14:37.000000 UTC  Disabled
12276   11204   msiexec.exe     0xdf045ca1f0c0  0       -       4       True    2025-10-31 11:14:26.000000 UTC  2025-10-31 11:14:27.000000 UTC  Disabled
1232    1100    services.exe    0xdf045cd950c0  8       -       0       False   2025-10-27 19:35:32.000000 UTC  N/A     Disabled
1272    1100    LsaIso.exe      0xdf045ce170c0  1       -       0       False   2025-10-27 19:35:32.000000 UTC  N/A     Disabled
1420    1232    svchost.exe     0xdf045d3d3080  22      -       0       False   2025-10-27 19:35:33.000000 UTC  N/A     Disabled
1452    1100    fontdrvhost.ex  0xdf045d412080  5       -       0       False   2025-10-27 19:35:33.000000 UTC  N/A     Disabled
12280   1420    MicrosoftStart  0xdf045d532080  0       -       2       False   2025-10-29 15:14:29.000000 UTC  2025-10-29 19:44:24.000000 UTC  Disabled
12104   1420    WidgetService.  0xdf045d582080  0       -       2       False   2025-10-29 15:14:28.000000 UTC  2025-10-29 19:44:24.000000 UTC  Disabled
```

• Apartado e: Muestra los argumentos introducidos por la línea de comandos

Muestra qué programas se estaban ejecutando y con qué argumentos (por ejemplo, si alguien lanzó un script, un comando sospechoso o un malware con parámetros específicos).. con el comando: **“python vol.py -f ‘C:\Users\Izan Navarro\Desktop\CIBERSEGURIDAD\CE_Ciberseguridad\ANALISIS_FORENSE\VOLCADO_RAM\W11_20251105.raw’ windows.cmdline”.**

```
PID     Process Args

4       System  -
188     Secure System   -
232     Registry        -
720     smss.exe        \SystemRoot\System32\smss.exe
652     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=bas
esrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
1100    wininit.exe     wininit.exe
1108    csrss.exe       -
1232    services.exe    C:\WINDOWS\system32\services.exe
1272    LsaIso.exe      \??\C:\WINDOWS\system32\lsaiso.exe -KeyGuard
1280    lsass.exe       C:\WINDOWS\system32\lsass.exe
1420    svchost.exe     C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
1452    fontdrvhost.ex  "fontdrvhost.exe"
1468    WUDFHost.exe    "C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:\UMDFCommunicationPorts\WUDF\Ho
stProcess-b123f740-5303-444e-b803-de24e77fce3b -SystemEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-e073ee2b-83e1-4074-b611-3ca531a7533f -IoCancelE
ventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-deed4895-f33a-4937-bdf1-0acda5d1f24c -NonStateChangingEventPortName:\UMDFCommunicationPorts\WUDF\HostP
rocess-d08f5a5e-338c-4111-af11-70bbdb6c2d3a -LifetimeId:a5e84c90-e7fc-4ff9-8f19-ac834d5eeb9d -DeviceGroupId:WudfDefaultDevicePool -HostArg:0
1580    svchost.exe     C:\WINDOWS\system32\svchost.exe -k RPCSS -p
1640    svchost.exe     C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p -s LSM
1804    svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s HvHost
1860    svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -s BTAGService
1872    svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalService -p -s BthAvctpSvc
1888    svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalService -p -s bthserv
1112    svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
688     svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
824     svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalService -p -s nsi
2084    svchost.exe     C:\WINDOWS\System32\svchost.exe -k netprofm -p -s netprofm
```

3. Ejercicio 2:

En una empresa han despedido a un trabajador por acceder a un documento pdf confidencial para el que no tenía autorización. El trabajador intentó borrar las evidencias, pero el informático de la empresa pudo obtener el volcado de la memoria RAM y desde la dirección nos piden que intentemos encontrar el documento pdf que tenía abierto en el momento del volcado y reportar su contenido (una contraseña).

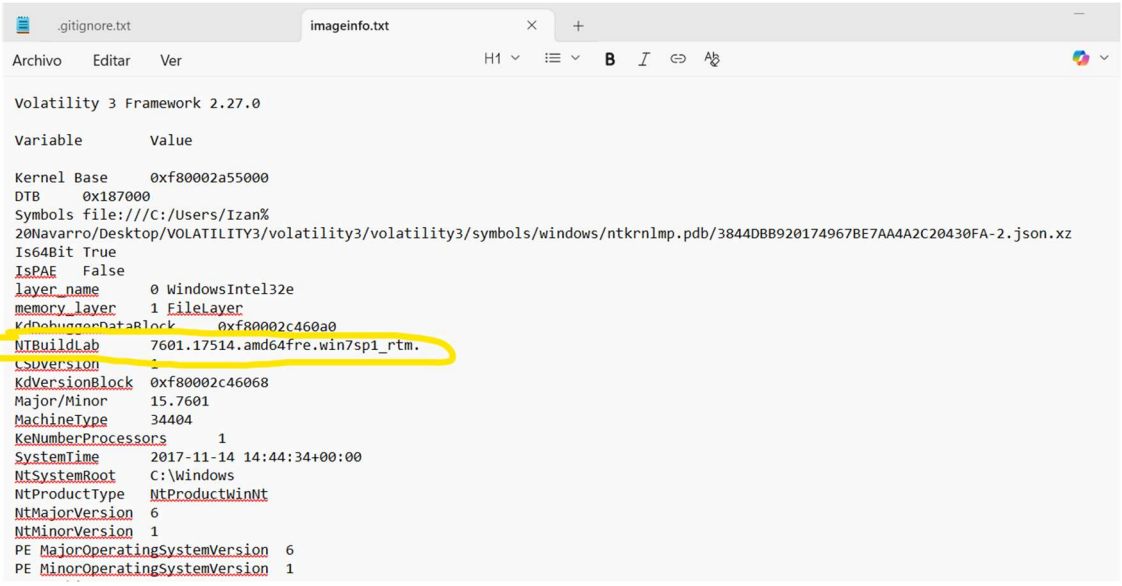
Fases de la investigación:

1. Obtención del perfil que se debe utilizar para analizar el volcado de memoria.

1) Primero genero un fichero .txt con la información obtenida mediante “Windows.info”:

```
C:\Users\Izan Navarro\Desktop\VOLATILITY3\volatility3>python vol.py -f "C:\Users\Izan Navarro\Desktop\CIBERSEGURIDAD\CE_
Ciberseguridad\ANALISIS_FORENSE\VOLCADO_RAM\dump.mem" windows.info > imageinfo.txt
```

2) Entro dentro del fichero .txt, en este caso, “imageinfo.txt” y observamos que está hecho desde un “W7_amd64free”:



.gitignore.txt imageinfo.txt

Archivo Editar Ver H1

```
Volatility 3 Framework 2.27.0

Variable        Value

Kernel Base     0xf80002a55000
DTB     0x187000
Symbols file:///C:/Users/Izan%
20Navarro/Desktop/VOLATILITY3/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/3844DBB920174967BE7AA4A2C20430FA-2.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdDebuggerDataBlock     0xf80002c460a0
NTBuildLab      7601.17514.amd64fre.win7sp1_rtm.
CSDVersion      1
KdVersionBlock  0xf80002c46068
Major/Minor     15.7601
MachineType     34404
KeNumberProcessors      1
SystemTime      2017-11-14 14:44:34+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  6
NtMinorVersion  1
PE MajorOperatingSystemVersion  6
PE MinorOperatingSystemVersion  1
```

2. Obtención de los procesos abiertos

Para obtener la información de los procesos abiertos ejecutaremos el siguiente comando **“python vol.py -f ‘C:\Users\Izan Navarro\Desktop\CIBERSEGURIDAD\CE_Ciberseguridad\ANALISIS_FORENSE\VOLCADO_RAM\dump.mem’ windows.pslist”**

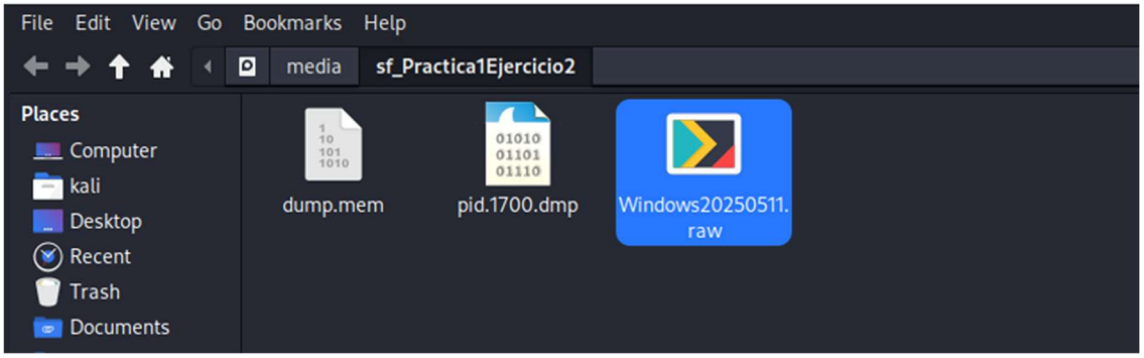
PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
4	0	System	0xfa8000ca0890	91	543	N/A	False	2017-11-14 14:21:02.000000 UTC	N/A	Disabled
260	4	smss.exe	0xfa8001c1ba40	2	29	N/A	False	2017-11-14 14:21:02.000000 UTC	N/A	Disabled
344	332	csrss.exe	0xfa8002a07060	9	360	0	False	2017-11-14 14:21:05.000000 UTC	N/A	Disabled
396	332	wininit.exe	0xfa8002bb99e0	3	74	0	False	2017-11-14 14:21:06.000000 UTC	N/A	Disabled
408	388	csrss.exe	0xfa8002bbb9e0	12	358	1	False	2017-11-14 14:21:06.000000 UTC	N/A	Disabled
456	388	winlogon.exe	0xfa8002c48580	3	110	1	False	2017-11-14 14:21:06.000000 UTC	N/A	Disabled
504	396	services.exe	0xfa8002c6db30	7	217	0	False	2017-11-14 14:21:06.000000 UTC	N/A	Disabled
512	396	lsass.exe	0xfa8002c7d9e0	6	556	0	False	2017-11-14 14:21:06.000000 UTC	N/A	Disabled
524	396	lsm.exe	0xfa8002c8ab30	9	148	0	False	2017-11-14 14:21:07.000000 UTC	N/A	Disabled
640	504	svchost.exe	0xfa8002dce970	10	356	0	False	2017-11-14 14:21:11.000000 UTC	N/A	Disabled
704	504	vmacthlp.exe	0xfa8002df8b30	3	54	0	False	2017-11-14 14:21:11.000000 UTC	N/A	Disabled
736	504	svchost.exe	0xfa8002e19b30	7	278	0	False	2017-11-14 14:21:11.000000 UTC	N/A	Disabled
784	504	svchost.exe	0xfa8002e4fb30	19	462	0	False	2017-11-14 14:21:11.000000 UTC	N/A	Disabled
888	504	svchost.exe	0xfa8002eddb30	21	474	0	False	2017-11-14 14:21:12.000000 UTC	N/A	Disabled
916	504	svchost.exe	0xfa8002f255d0	34	920	0	False	2017-11-14 14:21:12.000000 UTC	N/A	Disabled
360	504	svchost.exe	0xfa8002f6eb30	14	315	0	False	2017-11-14 14:21:12.000000 UTC	N/A	Disabled
844	504	svchost.exe	0xfa8002fb4200	15	380	0	False	2017-11-14 14:21:13.000000 UTC	N/A	Disabled
1072	504	spoolsv.exe	0xfa8002c8c060	12	322	0	False	2017-11-14 14:21:13.000000 UTC	N/A	Disabled
1104	504	svchost.exe	0xfa8002cf7060	18	309	0	False	2017-11-14 14:21:13.000000 UTC	N/A	Disabled
1384	504	VGAuthService.	0xfa80030b5b30	3	88	0	False	2017-11-14 14:21:16.000000 UTC	N/A	Disabled
1416	504	vmtoolsd.exe	0xfa80030d8580	9	292	0	False	2017-11-14 14:21:16.000000 UTC	N/A	Disabled
1440	504	ManagementAgen	0xfa8003102830	10	88	0	False	2017-11-14 14:21:16.000000 UTC	N/A	Disabled
1672	504	svchost.exe	0xfa80031ddb30	6	93	0	False	2017-11-14 14:21:18.000000 UTC	N/A	Disabled
1900	888	dwm.exe	0xfa80035d39e0	5	146	1	False	2017-11-14 14:21:21.000000 UTC	N/A	Disabled
1960	640	WmiPrvSE.exe	0xfa800380f6f0	10	197	0	False	2017-11-14 14:21:21.000000 UTC	N/A	Disabled
1336	504	taskhost.exe	0xfa80031de060	9	175	1	False	2017-11-14 14:21:21.000000 UTC	N/A	Disabled
1324	1892	explorer.exe	0xfa80038a7b30	38	888	1	False	2017-11-14 14:21:22.000000 UTC	N/A	Disabled
1956	504	msdtc.exe	0xfa8003908770	12	142	0	False	2017-11-14 14:21:22.000000 UTC	N/A	Disabled
2328	1324	vmtoolsd.exe	0xfa8003672150	6	207	1	False	2017-11-14 14:21:24.000000 UTC	N/A	Disabled
3000	1324	chrome.exe	0xfa8003d91b30	36	887	1	False	2017-11-14 14:21:42.000000 UTC	N/A	Disabled
3012	3000	chrome.exe	0xfa8003d909e0	7	77	1	False	2017-11-14 14:21:42.000000 UTC	N/A	Disabled
2240	3000	chrome.exe	0xfa800d3ea4d0	2	58	1	False	2017-11-14 14:21:44.000000 UTC	N/A	Disabled
2352	504	svchost.exe	0xfa8003e457a0	5	72	0	False	2017-11-14 14:21:44.000000 UTC	N/A	Disabled
2500	3000	chrome.exe	0xfa8003eb06a0	15	193	1	False	2017-11-14 14:21:46.000000 UTC	N/A	Disabled
2968	640	dllhost.exe	0xfa80041ff280	7	195	1	False	2017-11-14 14:21:59.000000 UTC	N/A	Disabled

3. Identificar y volcar el proceso objetivo

Vuelco el proceso Objetivo 1700 en un archivo llamado pid.1700.dmp para poder analizarlo posteriormente con el comando **“vol -f dump.mem /ruta/de/envio Windows.memmap - -dump - -pid 1700”**

```
┌──(Windows11)─(jose㉿kali-jose)-[~]
└─$ vol -f /media/sf_Practica1Ejercicio2/dump.mem -o /media/sf_Practica1Ejercicio2 windows.memmap --dump --pid 1700
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Virtual Physical        Size    Offset in File  File output

0×10000 0×43b9000       0×1000  0×0     pid.1700.dmp
0×11000 0×161ef000      0×1000  0×1000  pid.1700.dmp
0×20000 0×1a8d000       0×1000  0×2000  pid.1700.dmp
0×30000 0×914e000       0×1000  0×3000  pid.1700.dmp
0×40000 0×1f80f000      0×1000  0×4000  pid.1700.dmp
0×79000 0×240f7000      0×1000  0×5000  pid.1700.dmp
0×7a000 0×2bc37000      0×1000  0×6000  pid.1700.dmp
0×7b000 0×2d37f000      0×1000  0×7000  pid.1700.dmp
0×7c000 0×9b7f000       0×1000  0×8000  pid.1700.dmp
0×7d000 0×3817f000      0×1000  0×9000  pid.1700.dmp
0×7e000 0×2cde9000      0×1000  0×a000  pid.1700.dmp
0×7f000 0×65e8000       0×1000  0×b000  pid.1700.dmp
0×80000 0×199a7000      0×1000  0×c000  pid.1700.dmp
0×81000 0×1dfa6000      0×1000  0×d000  pid.1700.dmp
0×82000 0×efa5000       0×1000  0×e000  pid.1700.dmp
0×83000 0×b764000       0×1000  0×f000  pid.1700.dmp
0×84000 0×c663000       0×1000  0×10000 pid.1700.dmp
0×85000 0×103e2000      0×1000  0×11000 pid.1700.dmp
0×86000 0×23f21000      0×1000  0×12000 pid.1700.dmp
0×87000 0×3c613000      0×1000  0×13000 pid.1700.dmp
0×88000 0×1e412000      0×1000  0×14000 pid.1700.dmp
0×89000 0×19941000      0×1000  0×15000 pid.1700.dmp
0×8a000 0×2462c000      0×1000  0×16000 pid.1700.dmp
```

Aquí los resultados que me otorga este comando, y con esta imagen ".dmp" puedo analizarla y urgar en los datos que contiene este proceso objetivo.



4. Extraer la información de dicho proceso volcado **(pista, deberás usar herramientas como photorec o foremost para "urgar" dentro de este volcado)**

Con la descarga de foremost cojo y analizo el proceso .dmp para poder observar la información que contiene y lo guardaremos en una carpeta llamada "recovered".

```
┌──(Windows11)─(jose㉿kali-jose)-[~]
└─$ foremost -i /media/sf_Practica1Ejercicio2/pid.1700.dmp -o recovered
Command 'foremost' not found, but can be installed with:
sudo apt install foremost
Do you want to install it? (N/y)y
sudo apt install foremost
[sudo] password for jose:
Installing:
  foremost

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1015
  Download size: 42.5 kB
  Space needed: 104 kB / 56.7 GB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 foremost amd64 1.5.7-11+b2 [42.5 kB]
Fetched 42.5 kB in 1s (73.6 kB/s)
Selecting previously unselected package foremost.
(Reading database ... 417218 files and directories currently installed.)
Preparing to unpack .../foremost_1.5.7-11+b2_amd64.deb ...
Unpacking foremost (1.5.7-11+b2) ...
Setting up foremost (1.5.7-11+b2) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.2) ...
```

Una vez extraída la información almacenada en el proceso 1700.dmp se nos añadirá esta estructura de datos en la carpeta recovered. Entramos dentro de la carpeta pdf y dentro de los archivos tendremos unos pdf's con la clave dentro. Adjunto los datos y estructura de carpetas: