

# PRÁCTICA 4: ADQUISICIÓN Y ANÁLISIS DE EVIDENCIAS VOLÁTILES

IZAN NAVARRO LUJAN

IES SERRA PERENXISA

pag.1

# INDICE

1. Configuración Previa:.....	2
2. Ejercicio 1:.....	3
3. Ejercicio 2:.....	5

# 1. Configuración Previa:


## 1) Instalación de Volatility3 para volcados de W11:

 volatility3-2.26.2-py3-none-any.whl	sha256:a39964e2c752cf64fe0b3d9a53a8...		1.33 MB	Sep 25
 Source code (zip)				Sep 25
 Source code (tar.gz)				Sep 25

```
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:

 go-winpmem_amd64_1.0-rc2_signed	05/11/2025 17:11	Aplicación	5.135 KB
---	------------------	------------	----------

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.

W11\_20251105

Compartir

Detalles

Tipo Archivo RAW  
Tamaño 16,2 GB  
Ubicación del... C:\Usuarios\Izan Navarro\Escritorio  
Fecha de mod... 05/11/2025 17:12

Propiedades

## 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
file output										
4	0	System	0xdf0448520040 280	-	N/A	False	2025-10-27 19:35:26.000000 UTC	N/A	Disabled	D
188	4	Secure System	0xdf044861f040 0	-	N/A	False	2025-10-27 19:35:23.000000 UTC	N/A	N/A	D
232	4	Registry	0xdf04487e21c0 4	-	N/A	False	2025-10-27 19:35:23.000000 UTC	N/A	N/A	D
720	4	smss.exe	0xdf044cf78040 2	-	N/A	False	2025-10-27 19:35:26.000000 UTC	N/A	N/A	D
652	848	csrss.exe	0xdf0455d83080 15	-	0	False	2025-10-27 19:35:31.000000 UTC	N/A	N/A	D
1100	848	wininit.exe	0xdf0458b3c0c0 2	-	0	False	2025-10-27 19:35:32.000000 UTC	N/A	N/A	D
1108	1092	csrss.exe	0xdf0458ba6140 0	-	1	False	2025-10-27 19:35:32.000000 UTC	2025-10-		
1232	1100	services.exe	0xdf045cd950c0 8	-	0	False	2025-10-27 19:35:32.000000 UTC	N/A	N/A	D
1272	1100	LsaIso.exe	0xdf045ce170c0 1	-	0	False	2025-10-27 19:35:32.000000 UTC	N/A	N/A	D
1280	1100	lsass.exe	0xdf0458be10c0 10	-	0	False	2025-10-27 19:35:32.000000 UTC	N/A	N/A	D
<div>⬅</div>										
5600	14244	chrome.exe	0xdf04732da080 15	-	11	False	2025-11-05 15:02:59.000000 UTC	N/A	N/A	D
17492	10104	WINWORD.EXE	0xdf046d5c6080 38	-	11	False	2025-11-05 15:03:55.000000 UTC	N/A	N/A	D
16544	17492	aimgr.exe	0xdf04611760c0 3	-	11	False	2025-11-05 15:04:12.000000 UTC	N/A	N/A	D
9260	17492	ai.exe	0xdf046d5020c0 17	-	11	False	2025-11-05 15:04:12.000000 UTC	N/A	Disabled	D
4808	1420	AppActions.exe	0xdf046c1c10c0 6	-	11	False	2025-11-05 15:08:25.000000 UTC	N/A	N/A	D
8396	1420	VBoxSVC.exe	0xdf0475384080 14	-	11	False	2025-11-05 15:18:29.000000 UTC	N/A	N/A	D
11576	1232	VBoxSDS.exe	0xdf046d7b4080 3	-	0	False	2025-11-05 15:18:30.000000 UTC	N/A	N/A	D
16144	10104	VirtualBox.exe	0xdf04732d7180 7	-	11	False	2025-11-05 15:18:35.000000 UTC	N/A	N/A	D
12140	14244	chrome.exe	0xdf046aa33080 24	-	11	False	2025-11-05 15:23:34.000000 UTC	N/A	N/A	D

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

Para poder mostrar las relaciones en forma de árbol la terminal evalúa 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.

```

diskVolume3\Program Files\Oracle\VirtualBox\VirtualBoxVM.exe - - - - -
3912 8100 VirtualBoxVM.exe 0xdf046dc4f080 0 8 - False 2025-11-04 16:20:17.000000 UTC 2025-11-04 17:32:15.000000 UTC \Device\Hard
diskVolume3\Program Files\Oracle\VirtualBox\VirtualBoxVM.exe - - - - -
5968 6972 csrss.exe 0xdf0470ba90c0 14 - 11 False 2025-11-05 12:16:42.000000 UTC N/A \Device\HarddiskVolume3\Windows\Syst
em32\csrss.exe %SystemRoot%\system32\csrss.exe ObjectDirectory=Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 S
erverDll=winssrv:UserServerDllInitialization,3 ServerDll=ssssrv,4 ProfileControl=Off MaxRequestThreads=16 C:\WINDOWS\System32\csrss.exe
2976 6972 winlogon.exe 0xdf046cbb80c0 4 - 11 False 2025-11-05 12:16:42.000000 UTC N/A \Device\HarddiskVolume3\Windows\Syst
em32\winlogon.exe C:\WINDOWS\System32\Winlogon.exe -SpecialSession C:\WINDOWS\System32\Winlogon.exe
647 2976 fontdrvhost.exe 0xdf04646b8080 5 - 11 False 2025-11-05 12:16:42.000000 UTC N/A \Device\HarddiskVolume3\Windows\Syst
em32\fontdrvhost.exe "fontdrvhost.exe" C:\WINDOWS\System32\fontdrvhost.exe
4804 2976 userinit.exe 0xdf04773d0800 0 - 11 False 2025-11-05 14:58:24.000000 UTC 2025-11-05 14:58:47.000000 UTC \Device\Hard
diskVolume3\Windows\System32\userinit.exe - - - - -
1104 14804 explorer.exe 0xdf04709ab0c0 99 - 11 False 2025-11-05 14:58:24.000000 UTC N/A \Device\HarddiskVolume3\Wind
ows\explorer.exe C:\WINDOWS\Explorer.EXE C:\WINDOWS\Explorer.EXE
9400 10104 SecurityHealth 0xdf0462c020c0 1 - 11 False 2025-11-05 14:58:29.000000 UTC N/A \Device\HarddiskVolume3\Wind
ows\System32\SecurityHealthSystray.exe "C:\WINDOWS\System32\SecurityHealthSystray.exe" C:\Windows\System32\SecurityHealthSystray.exe
12224 10104 OneDrive.exe 0xdf046f7790c0 29 - 11 False 2025-11-05 14:58:33.000000 UTC N/A \Device\HarddiskVolume3\Prog
ram Files\Microsoft OneDrive\OneDrive.exe "C:\Program Files\Microsoft OneDrive\OneDrive.exe" /background C:\Program Files\Microsoft OneDrive\OneDrive
.exe
14244 10104 chrome.exe 0xdf0473be4080 46 - 11 False 2025-11-05 14:58:32.000000 UTC N/A \Device\HarddiskVolume3\Prog
ram Files\Google\Chrome\Application\chrome.exe "C:\Program Files\Google\Chrome\Application\chrome.exe" C:\Program Files\Google\Chrome\Application\c
hrome.exe
12032 14244 chrome.exe 0xdf0473beb080 19 - 11 False 2025-11-05 14:58:32.000000 UTC N/A \Device\HarddiskVolume3\Prog
ram Files\Google\Chrome\Application\chrome.exe "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.Netw
orkService --lang=es --service-sandbox-type=none --no-pre-read-main-dll --metrics-shmem-handle=2148,i,967429308541179060,31811772716275129,524288 --field-t
rial-handle=1928,i,2484569480599283980,9412392914594627782,262144 --variations-seed-version=20251104-170857.604000 --mojo-platform-channel-handle=2144 /pref
etch=13 C:\Program Files\Google\Chrome\Application\chrome.exe
1776 14244 chrome.exe 0xdf04613c0800 11 - 11 False 2025-11-05 14:58:32.000000 UTC N/A \Device\HarddiskVolume3\Prog
ram Files\Google\Chrome\Application\chrome.exe "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=storage.mojom.Stor
ageService --lang=es --service-sandbox-type=service --no-pre-read-main-dll --metrics-shmem-handle=2328,i,13178237951925193892,5925377773258657446,524288 --f
ield-trial-handle=1928,i,2484569480599283980,9412392914594627782,262144 --variations-seed-version=20251104-170857.604000 --mojo-platform-channel-handle=2344 /p
refetch=13 C:\Program Files\Google\Chrome\Application\chrome.exe
13968 14244 chrome.exe 0xdf04638970c0 13 - 11 False 2025-11-05 16:09:27.000000 UTC N/A \Device\HarddiskVolume3\Prog
ram Files\Google\Chrome\Application\chrome.exe "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --origin-trial-disabled-features=Can
vasTextNg WebAssemblyCustomDescriptors --no-pre-read-main-dll --video-capture-use-gpu-memory-buffer --lang=es --device-scale-factor=1.25 --num-raster-thread
s=4 --enable-main-frame-before-activation --renderer-client-id=136 --time-ticks-at-unix-epoch=1761593662385978 --launch-time-ticks=765385331242 --metrics-s
hmem-handle=9404,i,14878695280543111261,4484337735206409860,2097152 --field-trial-handle=1928,i,2484569480599283980,9412392914594627782,262144 --variations-
seed-version=20251104-170857.604000 --mojo-platform-channel-handle=9020 /prefetch=1 C:\Program Files\Google\Chrome\Application\chrome.exe
6424 14244 chrome.exe 0xdf04759bb080 23 - 11 False 2025-11-05 16:06:46.000000 UTC N/A \Device\HarddiskVolume3\Prog
ram Files\Google\Chrome\Application\chrome.exe "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --extension-process --init-isolate-a
s-foreground --origin-trial-disabled-features=CanvasTextNg WebAssemblyCustomDescriptors --no-pre-read-main-dll --video-capture-use-gpu-memory-buffer --lang=

```

- 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\_RA**  
**M\W11\_20251105.raw" windows.dllicst”.**

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

-chrome.exe:

```

13668 chrome.exe 0x7ff8ccb90000 0x177000 CRYPT32.dll C:\WINDOWS\System32\CRYPT32.dll 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8cc150000 0xd7000 OLEAUT32.dll C:\WINDOWS\System32\OLEAUT32.dll 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8cc0e0000 0xa3000 msvcrt_wins.dll C:\WINDOWS\System32\msvcrt_wins.dll 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8cc0a0000 0x37b000 combase.dll C:\WINDOWS\System32\combase.dll 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8cd710000 0x7f000 WINTRUST.dll C:\WINDOWS\System32\WINTRUST.dll 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8cc3e0000 0x35000 WINMM.dll C:\WINDOWS\System32\WINMM.dll 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8cd9a0000 0x242000 dbghelp.dll C:\WINDOWS\System32\dbghelp.dll 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8cc320000 0x34000 IPHLPAPI.dll C:\WINDOWS\System32\IPHLPAPI.dll 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8ccbf0000 0x2b000 USERENV.dll C:\WINDOWS\System32\USERENV.dll 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8cd930000 0xd000 Secur32.dll C:\WINDOWS\System32\Secur32.dll 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8cd50a000 0x11f000 WINHTTP.dll C:\WINDOWS\System32\WINHTTP.dll 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8cd7db000 0x267000 DWrite.dll C:\WINDOWS\System32\DWrite.dll 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8cd4bc000 0x23000 dhcpcsvc.DLL C:\WINDOWS\System32\dhcpcsvc.DLL 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8cd3c2000 0xb1000 WINSPOOL.DRV C:\WINDOWS\System32\WINSPOOL.DRV 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8cdcf2000 0xf2000 shcore.dll C:\WINDOWS\System32\shcore.dll 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8cd710000 0x57000 cfmgr32.dll C:\WINDOWS\System32\cfmgr32.dll 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8cd770000 0xa000 DPAPI.dll C:\WINDOWS\System32\DPAPI.dll 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8cdcb0000 0x49000 SSPICLI.DLL C:\WINDOWS\System32\SSPICLI.DLL 6 2025-11-05 16:09:27.000000 UTC Disabled
13668 chrome.exe 0x7ff8cd2b0000 0x13000 MSASN1.dll C:\WINDOWS\System32\MSASN1.dll 6 2025-11-05 16:09:27.000000 UTC Disabled

```

-ms-teams.exe:

```

14060 ms-teams.exe 0x7ff8c4610000 0x8e000 編譯-u004u編譯-u 6 2025-11-05 14:58:38.000000 UTC Disabled
14060 ms-teams.exe 0x7ff8c5560000 0x22000 - - 6 2025-11-05 14:58:38.000000 UTC Disabled
14060 ms-teams.exe 0x7ff8bd470000 0x17000 - - 6 2025-11-05 14:58:38.000000 UTC Disabled
14060 ms-teams.exe 0x7ff8ad2a0000 0x38000 - - 6 2025-11-05 14:58:38.000000 UTC Disabled
14060 ms-teams.exe 0x7ff8c7b70000 0x230000 windowscodecs.dll C:\Windows\System32\windowscodecs.dll 6 2025-11-05 14:58:38.000000 U
TC Disabled
14060 ms-teams.exe 0x7ff8c40e0000 0x15c000 wpnapps.dll C:\Windows\System32\wpnapps.dll 6 2025-11-05 14:58:38.000000 UTC Disabled
14060 ms-teams.exe 0x7ff8c7600000 0xb40000 policymanager.dll C:\WINDOWS\SYSTEM32\policymanager.dll 6 2025-11-05 14:58:38.000000 UTC Disa
bled
14060 ms-teams.exe 0x7ff8b2350000 0x1d000 - - 6 2025-11-05 14:58:38.000000 UTC Disabled
14060 ms-teams.exe 0x7ff88ceb0000 0x2c000 Webview2Loader.dll C:\Program Files\WindowsApps\MSTeams_25275.2601.4002.2815_x64_x-wwwekby3d8bbwe\WebView
2Loader.dll 6 2025-11-05 14:58:38.000000 UTC Disabled
14060 ms-teams.exe 0x7ff8a1b0000 0x597000 EmbeddedBrowserWebView.dll C:\Program Files (x86)\Microsoft\EdgeWebView\Application\141.0.3537.
90\EmbeddedBrowserWebView.dll 6 2025-11-05 14:58:38.000000 UTC Disabled
14060 ms-teams.exe 0x7ff8b1db0000 0x29000 - - 6 2025-11-05 14:58:38.000000 UTC Disabled
14060 ms-teams.exe 0x7ff8b77f0000 0x47000 - - 6 2025-11-05 14:58:38.000000 UTC Disabled
14060 ms-teams.exe 0x7ff8a4fa0000 0x5d000 capauthz.dll C:\WINDOWS\SYSTEM32\capauthz.dll 6 2025-11-05 14:58:38.000000 UTC Disabled
14060 ms-teams.exe 0x7ff8c9310000 0x9f000 -1 2025-11-05 14:58:38.000000 UTC Disabled
14060 ms-teams.exe 0x7ff8b7980000 0xc5000 twinui.appcore.dll C:\WINDOWS\System32\twinui.appcore.dll 6 2025-11-05 14:58:38.000000 UTC Disa
bled
14060 ms-teams.exe 0x7ff8ae040000 0x38000 Windows.Management.Workplace.dll C:\Windows\System32\Windows.Management.Workplace.dll 6 2025
-11-05 14:58:38.000000 UTC Disabled

```

- 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\_RA**  
**M\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	0xdf04487e21c0	4	-	N/A	False	2025-10-27 19:35:23.000000 UTC	N/A	Disabled
7160	9800	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	0xdf0457d804c0	4	-	0	False	2025-10-27 19:35:33.000000 UTC	N/A	Disabled
4212	1232	svchost.exe	0xdf0457e909c0	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	3808	taskhost.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
8040	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	svchost.exe	0xdf04592310c0	5	-	0	False	2025-10-27 19:35:33.000000 UTC	N/A	Disabled
1640	1232	svchost.exe	0xdf04593a00c0	5	-	0	False	2025-10-27 19:35:33.000000 UTC	N/A	Disabled
1580	1232	svchost.exe	0xdf0459c4020c0	10	-	0	False	2025-10-27 19:35:33.000000 UTC	N/A	Disabled
2148	1232	svchost.exe	0xdf0459d48f0c0	6	-	0	False	2025-10-27 19:35:33.000000 UTC	N/A	Disabled
2132	1232	svchost.exe	0xdf0459d990c0	3	-	0	False	2025-10-27 19:35:33.000000 UTC	N/A	Disabled
2692	1232	svchost.exe	0xdf0459f7b10c0	10	-	0	False	2025-10-27 19:35:33.000000 UTC	N/A	Disabled
2384	1232	svchost.exe	0xdf0459f808c0	7	-	0	False	2025-10-27 19:35:33.000000 UTC	N/A	Disabled
3192	1232	svchost.exe	0xdf0459fc820c0	3	-	0	False	2025-10-27 19:35:33.000000 UTC	N/A	Disabled
3680	1232	svchost.exe	0xdf0459fc80c0	4	-	0	False	2025-10-27 19:35:34.000000 UTC	N/A	Disabled
3448	1232	svchost.exe	0xdf0459bd770c0	7	-	0	False	2025-10-27 19:35:34.000000 UTC	N/A	Disabled
1384	1232	SearchIndexer.exe	0xdf0459c3db080	0	-	0	False	2025-10-27 19:35:46.000000 UTC	2025-11-02 15:11:31.000000 UTC	Disabled
15480	11204	msiexec.exe	0xdf0459c7170c0	0	-	4	True	2025-10-31 11:06:53.000000 UTC	2025-10-31 11:06:54.000000 UTC	Disabled
15252	11204	msiexec.exe	0xdf0459c8100c0	0	-	4	True	2025-10-31 11:14:36.000000 UTC	2025-10-31 11:14:37.000000 UTC	Disabled
12276	11204	msiexec.exe	0xdf0459ca1f0c0	0	-	4	True	2025-10-31 11:14:26.000000 UTC	2025-10-31 11:14:27.000000 UTC	Disabled
1232	1100	services.exe	0xdf0459cd950c0	8	-	0	False	2025-10-27 19:35:32.000000 UTC	N/A	Disabled
1272	1100	lsass.exe	0xdf0459ce170c0	1	-	0	False	2025-10-27 19:35:32.000000 UTC	N/A	Disabled
1420	1232	svchost.exe	0xdf0459d30080	22	-	0	False	2025-10-27 19:35:33.000000 UTC	N/A	Disabled
1452	1100	fontdrvhost.exe	0xdf0459d12080	5	-	0	False	2025-10-27 19:35:33.000000 UTC	N/A	Disabled
12280	1420	MicrosoftStart	0xdf0459d532080	0	-	2	False	2025-10-29 15:14:29.000000 UTC	2025-10-29 19:44:24.000000 UTC	Disabled
12104	1420	WidgetService.exe	0xdf0459d582080	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=winssrv	UserServerDllInitialization,3 ServerDll=ssssrv,4 ProfileControl=Off MaxRequestThreads=16
1100	wininit.exe	wininit.exe
1108	csrss.exe	-
1232	services.exe	C:\WINDOWS\system32\services.exe
1272	lsass.exe	??C:\WINDOWS\system32\lsass.exe -KeyGuard
1200	lsass.exe	C:\WINDOWS\system32\lsass.exe
1420	svchost.exe	C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
1452	fontdrvhost.exe	"fontdrvhost.exe"
1468	WUDFHost.exe	"C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:\UMDFCommunicationPorts\WUDF\Ho
stProcess-b123f740-5303-404e-b803-de24e77f3e3b	-SystemEventPortName:	UMDFCommunicationPorts\WUDF\HostProcess-e073ee2b-83e1-4074-b611-3ca531a7533f -IoCancelE
ventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-deed4895-f33a-4937-bd1f-0acda5d1f24c	-NonStateChangingEventPortName:	UMDFCommunicationPorts\WUDF\HostP
rocess-d08f5a5e-338c-4111-af11-70bbdb062d3a	-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).

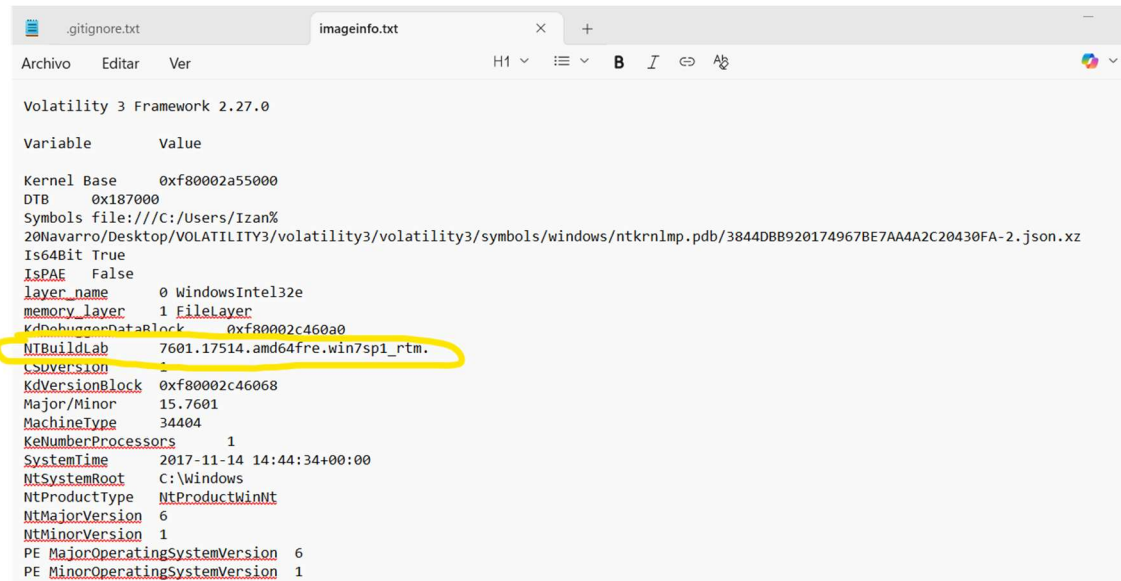
Fases de la investigación:

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  B  I  A

Volatility 3 Framework 2.27.0

Variable      Value

Kernel Base   0xf80002a55000
DTB           0x187000
Symbols file:  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
KDBGHeaderDataBlock  0xf80002c460a0
NTBuildLab    7601.17514.amd64fre.win7sp1_rtm.
CSVersion     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\VOLCA DO\_RAM\dump.mem’ windows.pslist”

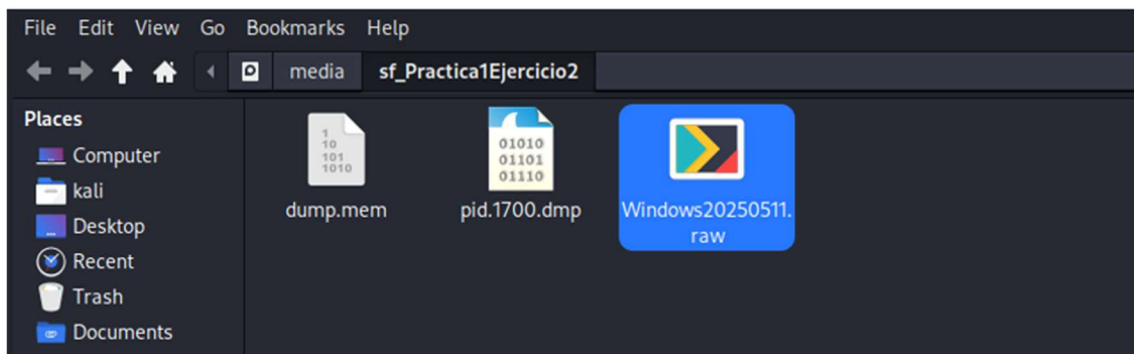
PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
4	0	System	0xfa8000ca0890 91	543	N/A	False	2017-11-14 14:21:02.000000 UTC	N/A	Disabled	
260	4	smss.exe	0xfa8001c1ba40 2	29	N/A	False	2017-11-14 14:21:02.000000 UTC	N/A	Disabled	
344	332	csrss.exe	0xfa8002a07060 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	lsass.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	0xfa8002f25d30 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	VGAAuthService.exe	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	0xfa800380ff60 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	0xfa80043ea4d0 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
0x10000 0x43b9000 0x1000 0x0 pid.1700.dmp
0x11000 0x161ef000 0x1000 0x1000 pid.1700.dmp
0x20000 0x1a8d000 0x1000 0x2000 pid.1700.dmp
0x30000 0x914e000 0x1000 0x3000 pid.1700.dmp
0x40000 0x1f80f000 0x1000 0x4000 pid.1700.dmp
0x79000 0x240f7000 0x1000 0x5000 pid.1700.dmp
0x7a000 0x2bc37000 0x1000 0x6000 pid.1700.dmp
0x7b000 0x2d37f000 0x1000 0x7000 pid.1700.dmp
0x7c000 0x9b7f000 0x1000 0x8000 pid.1700.dmp
0x7d000 0x3817f000 0x1000 0x9000 pid.1700.dmp
0x7e000 0x2cde9000 0x1000 0xa000 pid.1700.dmp
0x7f000 0x65e8000 0x1000 0xb000 pid.1700.dmp
0x80000 0x199a7000 0x1000 0xc000 pid.1700.dmp
0x81000 0x1dfa6000 0x1000 0xd000 pid.1700.dmp
0x82000 0xefa5000 0x1000 0xe000 pid.1700.dmp
0x83000 0xb764000 0x1000 0xf000 pid.1700.dmp
0x84000 0xc663000 0x1000 0x10000 pid.1700.dmp
0x85000 0x103e2000 0x1000 0x11000 pid.1700.dmp
0x86000 0x23f21000 0x1000 0x12000 pid.1700.dmp
0x87000 0x3c613000 0x1000 0x13000 pid.1700.dmp
0x88000 0x1e412000 0x1000 0x14000 pid.1700.dmp
0x89000 0x19941000 0x1000 0x15000 pid.1700.dmp
0x8a000 0x2462c000 0x1000 0x16000 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:

