

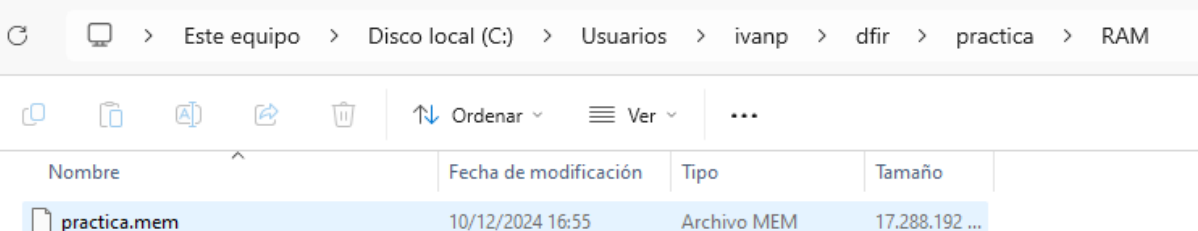
Práctica memoria RAM

- 1) Desde una terminal como administrador ejecutamos el comando:

```
winpmem_mini_x64_rc2.exe C:\Users\ivanp\dfir\practica\RAM\practica.mem
```

```
C:\Users\ivanp\Downloads>winpmem_mini_x64_rc2.exe C:\Users\ivanp\dfir\practica\RAM\practica.mem
WinPmem64
Extracting driver to C:\Users\ivanp\AppData\Local\Temp\pmeF914.tmp
Driver Unloaded.
Loaded Driver C:\Users\ivanp\AppData\Local\Temp\pmeF914.tmp.
Deleting C:\Users\ivanp\AppData\Local\Temp\pmeF914.tmp
The system time is: 15:54:21
Will generate a RAW image
- buffer_size_: 0x1000
CR3: 0x00001AE000
7 memory ranges:
Start 0x00001000 - Length 0x0009F000
Start 0x00100000 - Length 0x09D02000
Start 0x0A000000 - Length 0x00200000
Start 0x0A20E000 - Length 0x00DF2000
Start 0x0B020000 - Length 0xD00BC000
Start 0xDDBFF000 - Length 0x01401000
Start 0x100000000 - Length 0x31F300000
max_physical_memory_ 0x41f30000
Acquisition mode PTE Remapping
```

- 2) Comenzará la adquisición de la memoria y una vez concluida, debemos ver un archivo .mem en la ruta que le hemos pasado con el tamaño de nuestra memoria RAM.



Nombre	Fecha de modificación	Tipo	Tamaño
practica.mem	10/12/2024 16:55	Archivo MEM	17.288.192 ...

- 3) A continuación, ejecutaremos varios comandos con volatility.

En primer lugar, debemos abrir un cmd y situarnos en la carpeta de volatility

```
C:\Users\forensic\Downloads\volatility3-2.8.0\volatility3-2.8.0>
```

A continuación ejecutamos el comando;

```
python vol.py -f C:\Users\forensic\practica\RAM\practica.mem windows.info.Info
```

Con la opción windows.info nos dará el tipo de sistema operativo de la memoria RAM adquirida;

```

Kernel Base      0xf80745400000
DTB              0x1ae000
Symbols file:///C:/Users/forensic/Downloads/volatility3-2.8.0/v
Is64Bit True
IsPAE            False
layer_name       0 WindowsIntel32e
memory_layer     1 FileLayer
KdVersionBlock   0xf80746009998
Major/Minor      15.22621
MachineType      34404
KeNumberProcessors 24
SystemTime       2024-12-10 15:54:33+00:00
NtSystemRoot     C:\WINDOWS
NtProductType    NtProductWinNt
NtMajorVersion   10
NtMinorVersion   0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine       34404
PE TimeDateStamp Sun May 18 00:38:27 2081

```

Otra opción sería ejecutar el comando;

```
python vol.py -f C:\Users\forensic\practica\RAM\practica.mem windows.pslist.PsList
```

Con esta opción, nos listarían los procesos;

```

C:\Users\forensic\Downloads\volatility3-2.8.0\volatility3-2.8.0>python vol.py -f C:\Users\forensic\practica\RAM\practica.mem windows.pslist.PsList
Volatility 3 Framework 2.8.0
Progress: 100.00
PDB scanning finished

```

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
4	0	System	0xcf07a46ff040	351	-	N/A	False	2024-12-04 08:30:09.000000 UTC	N/A	Disabled
276	4	Registry	0xcf07a48e7040	4	-	N/A	False	2024-12-04 08:30:06.000000 UTC	N/A	Disabled
844	4	smss.exe	0xcf07a8c24080	2	-	N/A	False	2024-12-04 08:30:09.000000 UTC	N/A	Disabled
888	980	csrss.exe	0xcf07b17df140	20	-	0	False	2024-12-04 08:30:10.000000 UTC	N/A	Disabled
1128	980	wininit.exe	0xcf07b367b140	2	-	0	False	2024-12-04 08:30:11.000000 UTC	N/A	Disabled
1136	1120	csrss.exe	0xcf07b367d140	0	-	1	False	2024-12-04 08:30:11.000000 UTC	2024-12-04 21:11:40.000000 UTC	Disabled
1204	1128	services.exe	0xcf07b3739140	7	-	0	False	2024-12-04 08:30:11.000000 UTC	N/A	Disabled
1236	1128	lsass.exe	0xcf07b38a20c0	8	-	0	False	2024-12-04 08:30:11.000000 UTC	N/A	Disabled
1352	1204	svchost.exe	0xcf07b39390c0	17	-	0	False	2024-12-04 08:30:12.000000 UTC	N/A	Disabled
1380	1128	fontdrvhost.exe	0xcf07b3943080	5	-	0	False	2024-12-04 08:30:12.000000 UTC	N/A	Disabled