
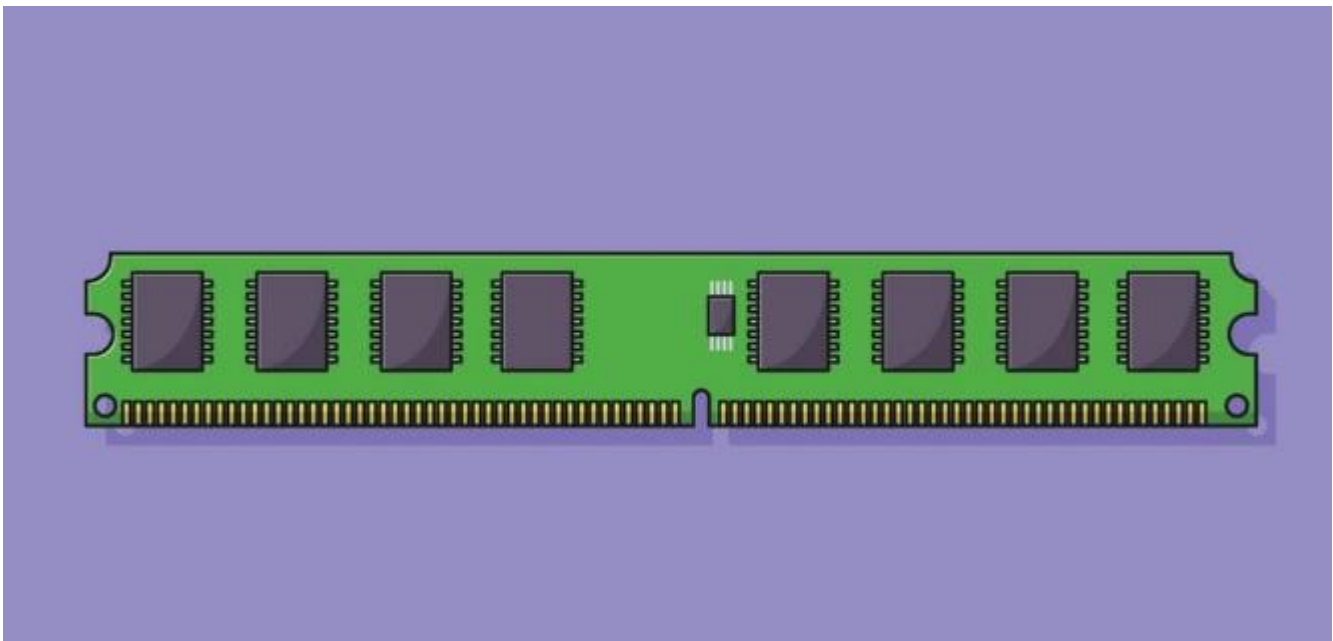


<u>UNIVERSIDAD AUTÓNOMA “TOMAS FRÍAS”</u> <u>CARRERA DE INGENIERÍA DE SISTEMAS</u>			
Nombre	Univ. Luis Daniel Acuña Oyola		
Materia:	Arquitectura de computadoras (SIS-522)		
Docente:	Ing. Gustavo A. Puita Choque		N° Práctica
Auxiliar:	Univ. Aldrin Roger Perez Miranda		3
Fecha publicación:	23/09/2024		
Fecha de entrega:	07/10/2024		
Grupo:	1	Sede:	Potosí



### **PARTE TEÓRICA (50 pts)**

- 1) **¿CUÁL ES LA DIFERENCIA FUNDAMENTAL ENTRE UNA MEMORIA RAM Y UNA MEMORIA ROM EN TERMINOS DE ACCESIBILIDAD Y VOLATILIDAD? (2 pts)**

La **RAM** es volátil (se pierde los datos cuando se apaga la PC) y de acceso aleatorio, mientras que la **ROM** es no volátil (no se pierde los datos cuando se apaga la PC) y es de acceso de solo lectura.

- 2) **¿QUÉ VENTAJAS Y DESVENTAJAS PRESENTAN LAS MEMORIAS ESTÁTICAS Y DINÁMICAS EN TÉRMINOS DE VELOCIDAD, DENSIDAD Y COSTO? (2 pts)**

**Ventajas:**

**ESTÁTICAS:** La velocidad de acceso es alta, para retener los datos solo necesita estar energizada, son más fáciles de diseñar.

**DINÁMICAS:** Mayor densidad y capacidad, menor costo por bit, menor consumo de potencia.

**Desventajas:**

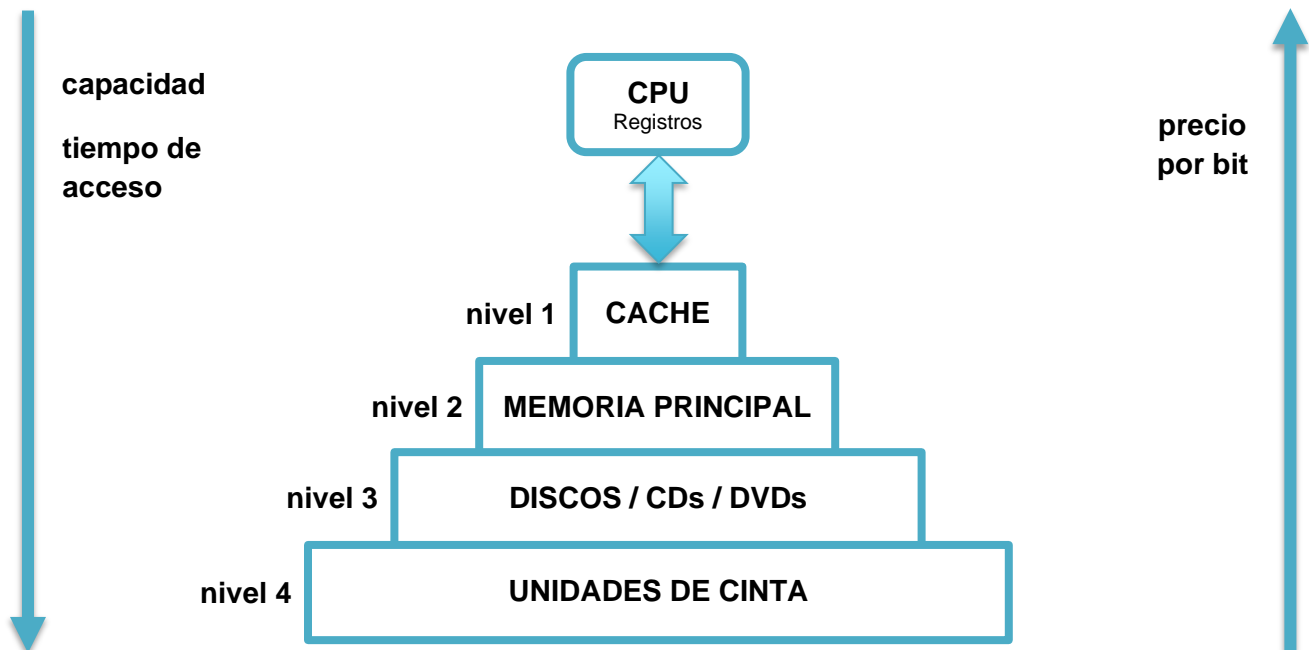
**ESTÁTICAS:** Menor capacidad, debido a que cada celda de almacenamiento requiere mas transistores, mayor costo por bit, mayor consumo de potencia.

**DINÁMICAS:** La velocidad de acceso es baja, necesita recarga de la información almacenada para retenerla (refresco), diseño complejo.

3) ¿POR QUÉ SE UTILIZA LA TECNOLOGÍA DE VIDEO RAM (VRAM) EN LOS CONTROLADORES DE VIDEO DE LAS COMPUTADORAS Y CUÁL ES SU FUNCIÓN PRINCIPAL? (2 pts)

**Porque** su tecnología de "doble puerta" permite realizar lecturas y escrituras al mismo tiempo en diferentes direcciones y su **función principal** es mantener un refresco constante en el monitor mientras el procesador gráfico actualiza la información, mejorando así el rendimiento y la calidad de la imagen.

4) DIBUJA UN DIAGRAMA QUE REPRESENTA LA JERARQUÍA DE MEMORIA EN UN SISTEMA INFORMÁTICO TÍPICO Y ETIQUETA CADA NIVEL CON EL TIPO CORRESPONDIENTE DE MEMORIA. (2 pts)



5) ¿QUÉ DIFERENCIAS EXISTEN ENTRE LA MEMORIA CACHÉ L1, L2 Y L3 EN TÉRMINOS DE TAMAÑO, VELOCIDAD Y PROXIMIDAD AL PROCESADOR? (2 pts)

- **L1:** Es la más pequeña, pero la más rápida, ubicada directamente en el núcleo del procesador y esta cercanía al núcleo permite un acceso casi instantáneo a los datos más críticos.
- **L2:** Más grande que L1, pero más lenta. Generalmente está también dentro del núcleo o muy cerca, almacenando datos usados frecuentemente.
- **L3:** Es la más grande, más lenta comparada con L1 y L2 y se comparte entre todos los núcleos del procesador, actuando como un último nivel de almacenamiento rápido antes de recurrir a la RAM.

## 6) RESOLVER EL SIGUIENTE LABORATORIO PASO A PASO CON CAPTURAS PROPIAS MOSTRANDO SU BARRA DE TAREAS DE SU PC. (40 pts)

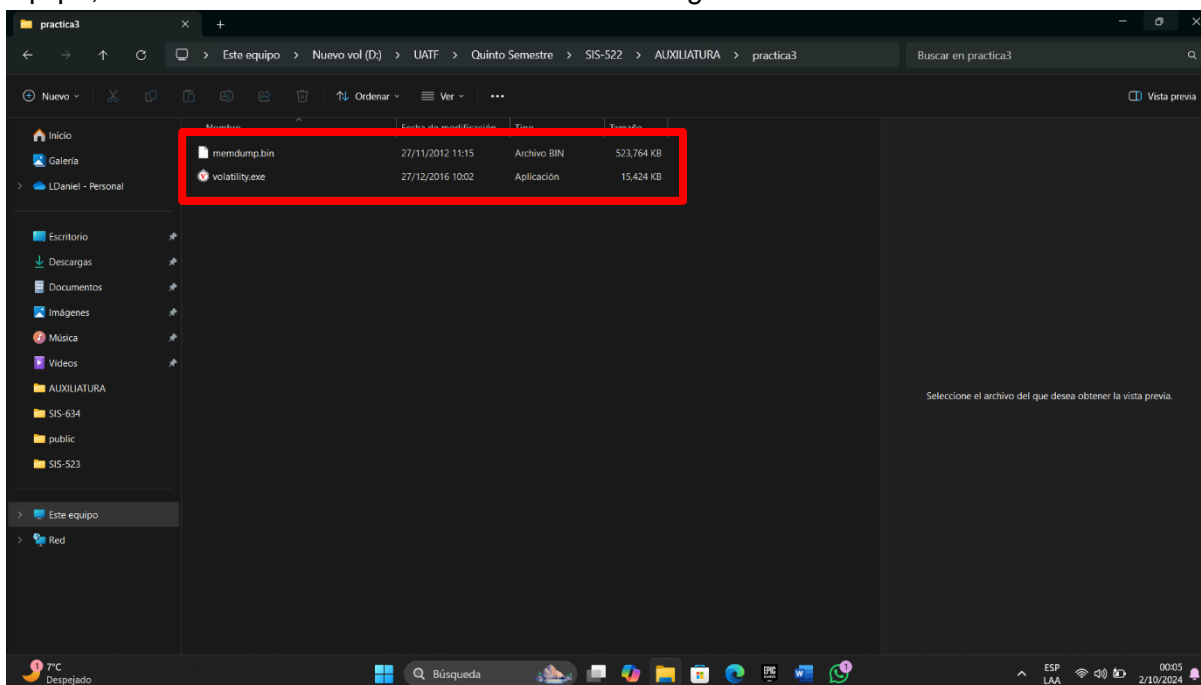
### ANALISIS DE MEMORIA RAM CON VOLATILITY

**Objetivo General.** - Realizar el análisis de auditoría de una imagen de memoria RAM con el uso de la herramienta Volatility. Se analizará una memoria ya capturada.

#### PORTE 1

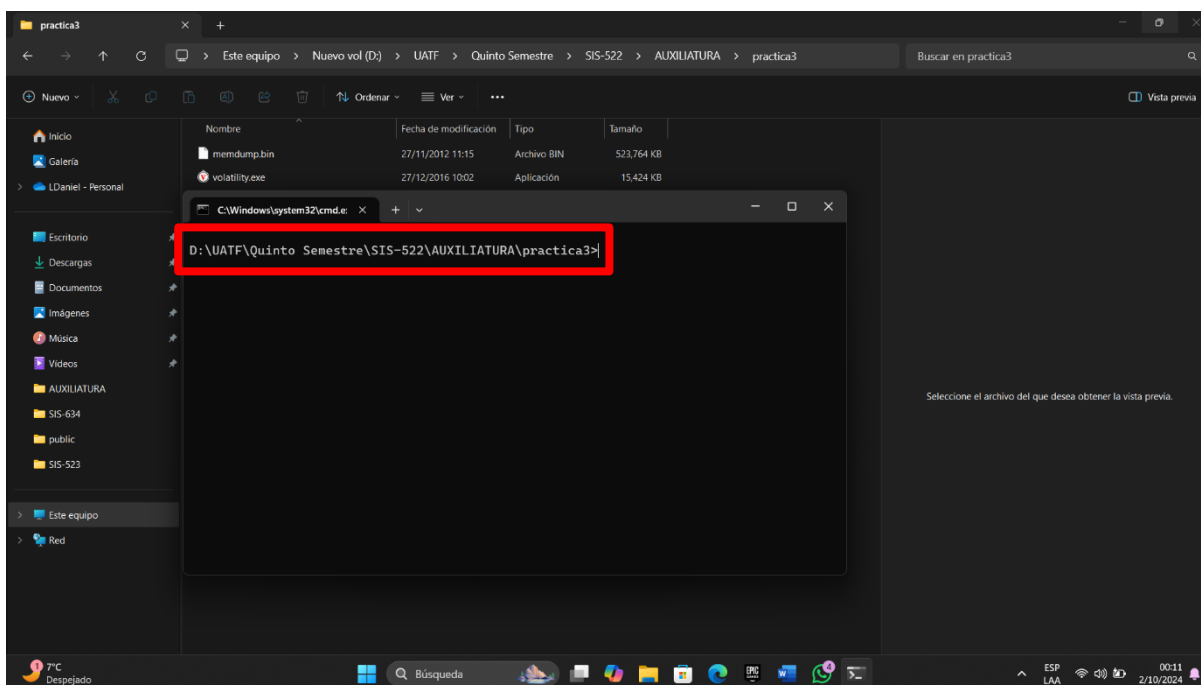
##### **PASO 1:**

Descarga el archivo comprimido “practica3” de la plataforma Classroom, descomprimirlo en cualquier lugar de tu equipo, los dos archivos deben estar en un mismo lugar.



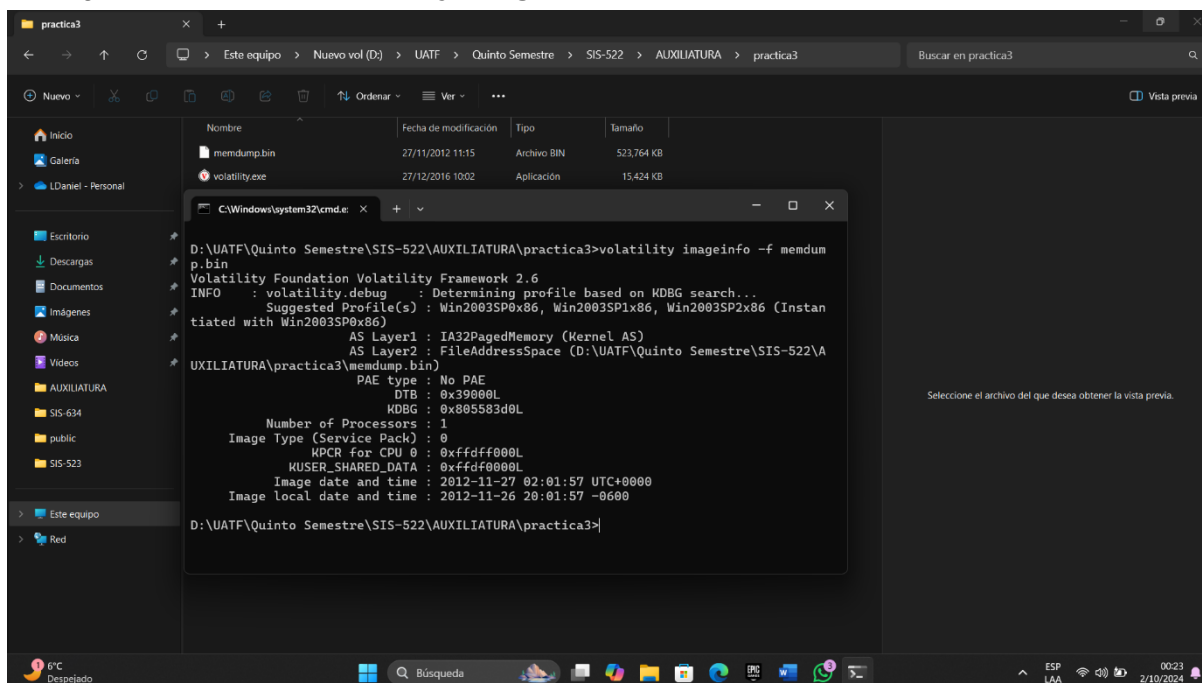
##### **PASO 2:**

Ingresa hasta la dirección donde están los dos archivos mediante el Símbolo de Sistema (cmd).



### PASO 3:

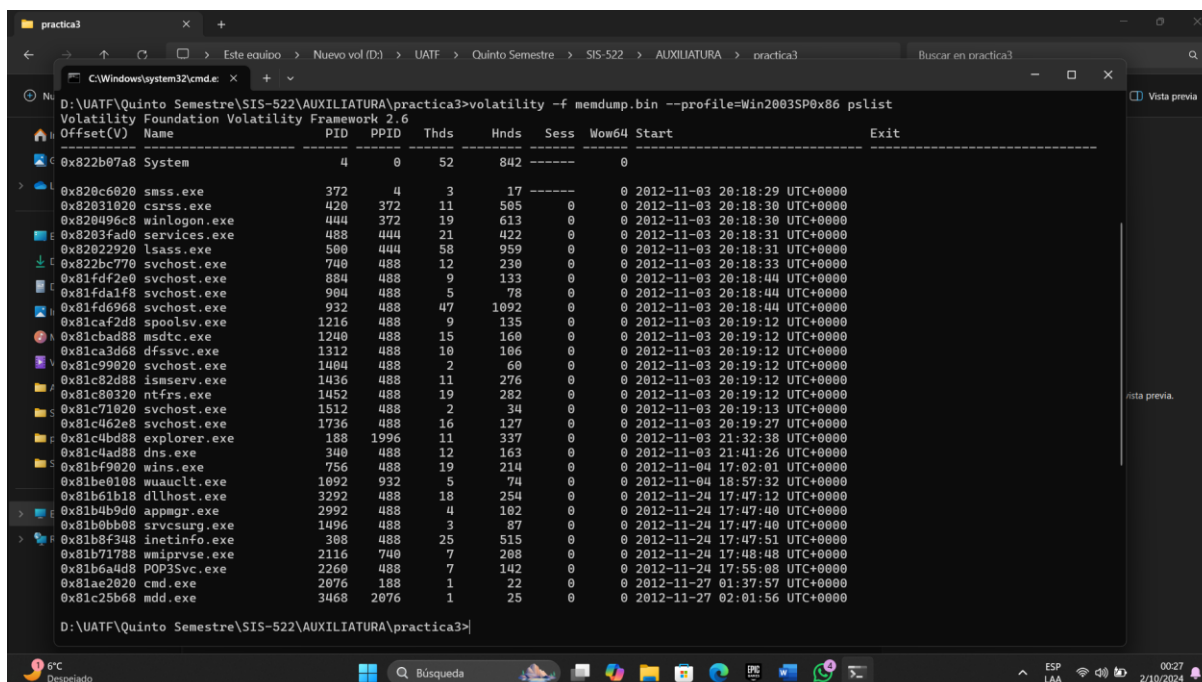
Inserta el siguiente comando: “**volatility imageinfo -f memdump.bin**”.



En la imagen se puede observar las características de la memoria, sobre todo el perfil sugerido “Win8SP0x64”, el cual nos permitirá realizar las demás instrucciones.

### PASO 4:

Ingresa el siguiente comando: “**volatility -f memdump.bin --profile=Win2003SP0x86 pslist**”.

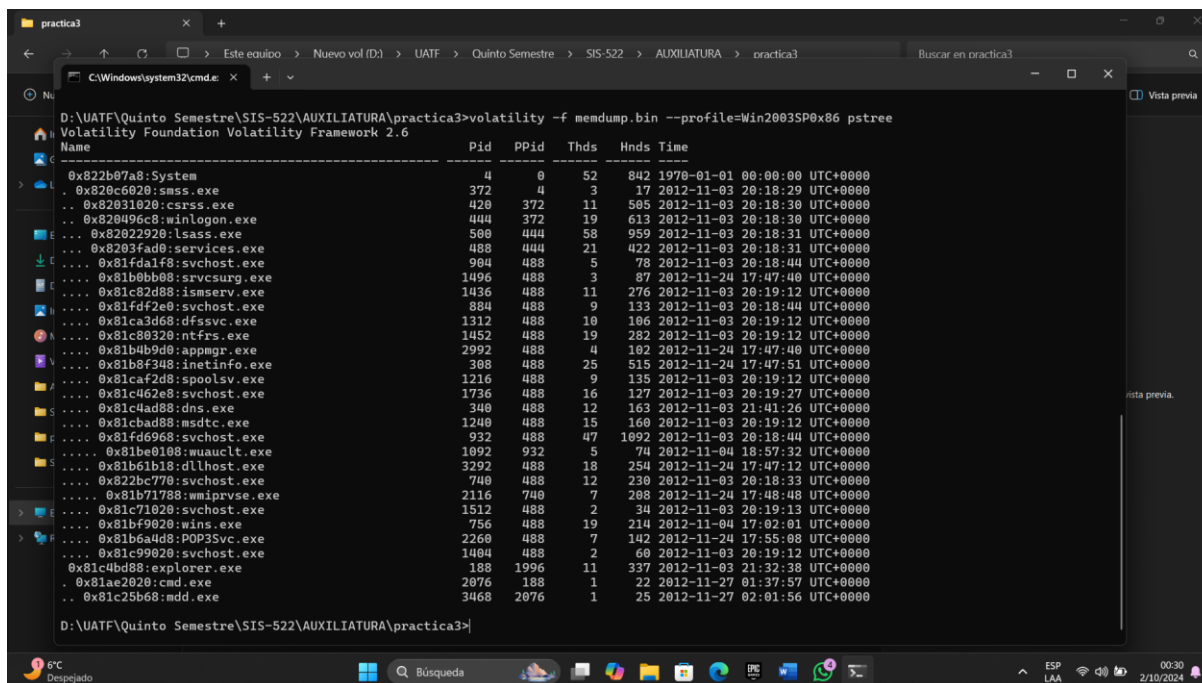


La imagen nos muestra los nombres de los procesos que se estaban ejecutando además de:

- **PID** = Identificador del proceso.
- **PPID** = Padre del Proceso.
- **Start** = inicio del Proceso.

## PASO 5:

Ingresa el siguiente comando: “volatility -f memdump.bin --profile=Win2003SP0x86 pstree”.

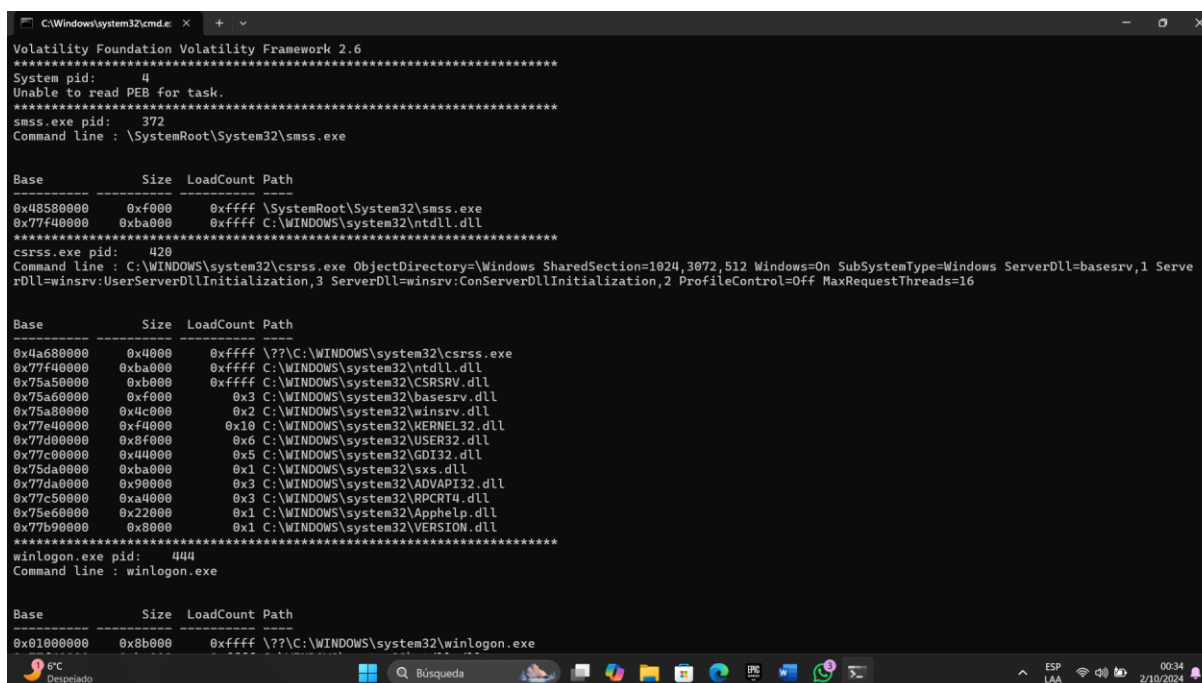


```
D:\UATF\Quinto Semestre\SIS-522\AUXILIATURA\practica3>volatility -f memdump.bin --profile=Win2003SP0x86 pstree
Volatility Foundation Volatility Framework 2.6
Name                                     Pid  PPid  Thds  Hnds  Time
-----
0x822b07a8: System                      4     0    52    842  1970-01-01 00:00:00 UTC+0000
0x820c6020: smss.exe                   372     4     3     17  2012-11-03 20:18:29 UTC+0000
0x82031020: csrss.exe                   420    372    11    505  2012-11-03 20:18:30 UTC+0000
0x820496c8: winlogon.exe                444    372    19    613  2012-11-03 20:18:30 UTC+0000
0x82022920: lsass.exe                   500    444    58    959  2012-11-03 20:18:31 UTC+0000
0x8203fad0: services.exe                488    444    21    422  2012-11-03 20:18:31 UTC+0000
0x81fdaf18: svchost.exe                 904    488     5     78  2012-11-03 20:18:44 UTC+0000
0x81b0bb08: smss.exe                   1496    488     3     87  2012-11-24 17:47:40 UTC+0000
0x81c82d88: iiserv.exe                 1436    488    11    276  2012-11-03 20:19:12 UTC+0000
0x81fd2a0: svchost.exe                 884    488     9    133  2012-11-03 20:18:44 UTC+0000
0x81ca3d68: dfssvc.exe                 1312    488    10    106  2012-11-03 20:19:12 UTC+0000
0x81c80320: ntfrs.exe                   1452    488    19    282  2012-11-03 20:19:12 UTC+0000
0x81b4b9d0: appmgr.exe                 2992    488     4    102  2012-11-24 17:47:40 UTC+0000
0x81b8f348: inetinfo.exe               308    488    25    515  2012-11-24 17:47:51 UTC+0000
0x81caf2d8: spoolsv.exe                1216    488     9    135  2012-11-03 20:19:12 UTC+0000
0x81c462e8: svchost.exe                1736    488    16    127  2012-11-03 20:19:27 UTC+0000
0x81c4ad88: dns.exe                    340    488    12    163  2012-11-03 21:41:26 UTC+0000
0x81cbad88: msdtc.exe                 1240    488    15    160  2012-11-03 20:19:12 UTC+0000
0x81fd6968: svchost.exe               932    488    47   1092  2012-11-03 20:18:44 UTC+0000
0x81be0108: wuaucnt.exe                1092    932     5     74  2012-11-04 18:57:32 UTC+0000
0x81b61b18: dlhst.exe                 3292    488    18    254  2012-11-24 17:47:12 UTC+0000
0x822bc770: svchost.exe                740    488    12    230  2012-11-03 20:18:33 UTC+0000
0x81b71788: wmiiprv.exe                2116    740     7    208  2012-11-24 17:48:48 UTC+0000
0x81c71020: svchost.exe                1512    488     2     34  2012-11-03 20:19:13 UTC+0000
0x81bf9020: wins.exe                   756    488    19    214  2012-11-04 17:02:01 UTC+0000
0x81b6a4d8: POP3Svc.exe               2260    488     7    142  2012-11-24 17:55:08 UTC+0000
0x81c99020: svchost.exe               1404    488     2     60  2012-11-03 20:19:12 UTC+0000
0x81c4bd88: explorer.exe               188   1996    11    337  2012-11-03 21:32:38 UTC+0000
0x81ae2020: cmd.exe                    2076    188     1     22  2012-11-27 01:37:57 UTC+0000
0x81c25b68: mdd.exe                    3468   2076     1     25  2012-11-27 02:01:56 UTC+0000
```

- pstree muestra los procesos de manera más ordenada.

## PASO 6:

Ingresa el siguiente comando: “volatility -f memdump.bin --profile=Win2003SP0x86 dlllist”.



```
Volatility Foundation Volatility Framework 2.6
*****
System pid: 4
Unable to read PEB for task.
*****
smss.exe pid: 372
Command line : \SystemRoot\System32\smss.exe

Base          Size  LoadCount Path
-----
0x48580000    0x0000    0xffff \SystemRoot\System32\smss.exe
0x77f40000    0xba0000    0xffff C:\WINDOWS\system32\ntdll.dll

csrss.exe pid: 420
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemType=Windows ServerDll=basesrv,1 Serve
rDll=win32srv:UserServerDllInitialization,3 ServerDll=win32srv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16

Base          Size  LoadCount Path
-----
0x4a680000    0x4000    0xffff C:\WINDOWS\system32\csrss.exe
0x77f40000    0xba0000    0xffff C:\WINDOWS\system32\ntdll.dll
0x75a50000    0xb000    0xffff C:\WINDOWS\system32\CSRSRV.dll
0x75a60000    0xf000    0x3 C:\WINDOWS\system32\basesrv.dll
0x75a70000    0x4000    0x2 C:\WINDOWS\system32\win32srv.dll
0x77e40000    0xf000    0x10 C:\WINDOWS\system32\USER32.dll
0x77d00000    0x8f000    0x6 C:\WINDOWS\system32\USER32.dll
0x77c00000    0x4000    0x5 C:\WINDOWS\system32\GDI32.dll
0x75da0000    0xba0000    0x1 C:\WINDOWS\system32\sxs.dll
0x77da0000    0x90000    0x3 C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000    0xa000    0x3 C:\WINDOWS\system32\RPCRT4.dll
0x75e60000    0x22000    0x1 C:\WINDOWS\system32\Apphelp.dll
0x77b90000    0x8000    0x1 C:\WINDOWS\system32\VERSION.dll

winlogon.exe pid: 444
Command line : winlogon.exe

Base          Size  LoadCount Path
-----
0x01000000    0xb000    0xffff C:\WINDOWS\system32\winlogon.exe
```

- Dlllist Identifica las librerías del sistema que se están utilizando.

## PREGUNTAS DE VERIFICACIÓN DEL LABORATORIO

¿QUÉ HORA INICIA EL PROCESO EXPLORER.EXE?

0x81c462e8	svchost.exe	1736	488	16	127	0	0	2012-11-03 20:19:27 UTC+0000
0x81c4bd88	explorer.exe	188	1996	11	337	0	0	2012-11-03 21:32:38 UTC+0000
0x81c4ad88	dns.exe	340	488	12	163	0	0	2012-11-03 21:41:26 UTC+0000

## ¿QUÉ HORA INICIA EL PROCESO SVCHOST.EXE?

0x82022920	lsass.exe	500	444	58	959	0	0	2012-11-03 20:18:31 UTC+0000
0x822bc770	svchost.exe	740	488	12	230	0	0	2012-11-03 20:18:33 UTC+0000
0x81fdf2e0	svchost.exe	884	488	9	133	0	0	2012-11-03 20:18:44 UTC+0000
0x81fda1f8	svchost.exe	904	488	5	78	0	0	2012-11-03 20:18:44 UTC+0000
0x81fd6968	svchost.exe	932	488	47	1092	0	0	2012-11-03 20:18:44 UTC+0000
0x81caf2d8	spoolsv.exe	1216	488	9	135	0	0	2012-11-03 20:19:12 UTC+0000
0x81cbad88	msdtc.exe	1240	488	15	160	0	0	2012-11-03 20:19:12 UTC+0000
0x81ca3d68	dfssvc.exe	1312	488	10	106	0	0	2012-11-03 20:19:12 UTC+0000
0x81c99020	svchost.exe	1404	488	2	60	0	0	2012-11-03 20:19:12 UTC+0000
0x81c82d88	ismserv.exe	1436	488	11	276	0	0	2012-11-03 20:19:12 UTC+0000
0x81c80320	ntfrs.exe	1452	488	19	282	0	0	2012-11-03 20:19:12 UTC+0000
0x81c71020	svchost.exe	1512	488	2	34	0	0	2012-11-03 20:19:13 UTC+0000
0x81c462e8	svchost.exe	1736	488	16	127	0	0	2012-11-03 20:19:27 UTC+0000
0x81c4bd88	explorer.exe	188	1996	11	337	0	0	2012-11-03 21:32:38 UTC+0000

## ¿CUÁL ES EL NOMBRE DEL PROCESO PID: 420?

0x820c6020	smss.exe	372	4	3	17	-----	0	2012-11-03 20:18:29 UTC+0000
0x82031020	csrss.exe	420	372	11	505	0	0	2012-11-03 20:18:30 UTC+0000
0x820496c8	winlogon.exe	444	372	19	613	0	0	2012-11-03 20:18:30 UTC+0000

## ¿CUÁL ES EL NOMBRE DEL PROCESO PID: 932?

0x81fda1f8	svchost.exe	904	488	5	78	0	0	2012-11-03 20:18:44 UTC+0000
0x81fd6968	svchost.exe	932	488	47	1092	0	0	2012-11-03 20:18:44 UTC+0000
0x81caf2d8	spoolsv.exe	1216	488	9	135	0	0	2012-11-03 20:19:12 UTC+0000

## PARTE PRÁCTICA (50 pts)

- 1) DETERMINA CUÁNTOS BITS EN TOTAL PUEDE ALMACENAR UNA MEMORIA RAM DE 128K X 4 (5 pts)

$$128 * 2^{10} * 4 = 524288 \text{ bits.}$$

- 2) ¿CUÁNTOS BITS PUEDE ALMACENAR UNA MEMORIA DE 10G X 16? (5 pts)

$$10 * 2^{30} * 16 = 171798691840 \text{ bits.}$$

- 3) ¿CUANTAS LOCALIDADES DE MEMORIA SE PUEDE DIRECCIONAR CON 32 LÍNEAS DE DIRECCIÓN? (5 pts)

$$2^{32} = 4294967296 \text{ localidades.}$$

- 4) ¿CUÁNTAS LOCALIDADES DE MEMORIA SE PUEDEN DIRECCIONAR CON 1024 LÍNEAS DE DIRECCIÓN? (5 pts)

$$2^{1024} = 1,7976931349 \times 10^{308} \text{ localidades.}$$

- 5) ¿CUÁNTAS LOCALIDADES DE MEMORIA SE PUEDEN DIRECCIONAR CON 64 LÍNEAS DE DIRECCIÓN? (5 pts)

$$2^{64} = 1,8446744074 \times 10^{19} \text{ localidades.}$$

- 6) ¿CUÁNTAS LÍNEAS DE DIRECCIÓN SE NECESITAN PARA UNA MEMORIA ROM DE 512M x 8? (5 pts)

$$n = \frac{\ln(512 * 2^{20})}{\ln(2)} = 29 \text{ lineas.}$$

- 7) ¿CUÁNTAS LÍNEAS DE DIRECCIÓN SE NECESITAN PARA UNA MEMORIA ROM DE 128M x 128? (5 pts)

$$n = \frac{\ln(128 * 2^{20})}{\ln(2)} = 27 \text{ lineas.}$$

- 8) ¿CUÁNTOS BITS EN TOTAL PUEDE ALMACENAR UNA MEMORIA RAM 128M x 4?, DE ÉL RESULTADO GIGABYTES (5 pts)

$$128 * 2^{20} * 4 = 536870912 / (8 * 2^{30}) = 0,0625 \text{ gigabytes.}$$

9) ¿CUÁNTOS BITS EN TOTAL PUEDE ALMACENAR UNA MEMORIA RAM 64M x 64?, DE ÉL RESULTADO EN TERAS (5 pts)

$$64 * 2^{20} * 64 = 4294967296 / (8 * 2^{40}) = 0,00048828125 \text{ terabytes.}$$

10) ¿CUÁNTOS BITS EN TOTAL PUEDE ALMACENAR UNA MEMORIA RAM 64M x 64?, DE ÉL RESULTADO EN TERABYTES (5 pts)

$$64 * 2^{20} * 64 = 4294967296 / (8 * 2^{40}) = 0,00048828125 \text{ terabytes.}$$