


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

PARTE TEÓRICA (50 pts)

1) ¿Cuál es la diferencia fundamental entre una memoria RAM y una memoria ROM en términos de accesibilidad y volatilidad? (2 pts)

R. En accesibilidad, la RAM permite la lectura y la escritura de información, mientras que la ROM solo permita la lectura, de ahí su nombre Read Only Memory o memoria de solo lectura. ✓

En términos de volatilidad, la RAM es volátil ya que necesita de energía eléctrica para funcionar, mientras que la ROM no es volátil o sea no necesita electricidad y guarda la información cuando el equipo se apaga

2) ¿Qué ventajas y desventajas presentan las memorias estáticas y dinámicas en términos de velocidad, densidad y costo? (2 pts)

R. Las memorias estáticas tienen las ventajas de que: son más rápidas ya que no necesitan actualizaciones constantes, también son más estables al no necesitar refrescar sus datos, y también no consumen mucha energía al no realizar ciclos de refresco. Las desventajas que poseen serian que: tienen menos densidad o sea que ocupan más espacio físico por bit almacenado, también estas memorias son más caras. ✓

Las memorias dinámicas tienen la ventaja de que tienen mejor densidad de almacenamiento, ya que pueden almacenar más en la misma cantidad de espacio físico, y además que sus costos son más bajos comparados a las estáticas. Sus desventajas serian que tienen menor velocidad, y que tienen un mayor consumo de energía.

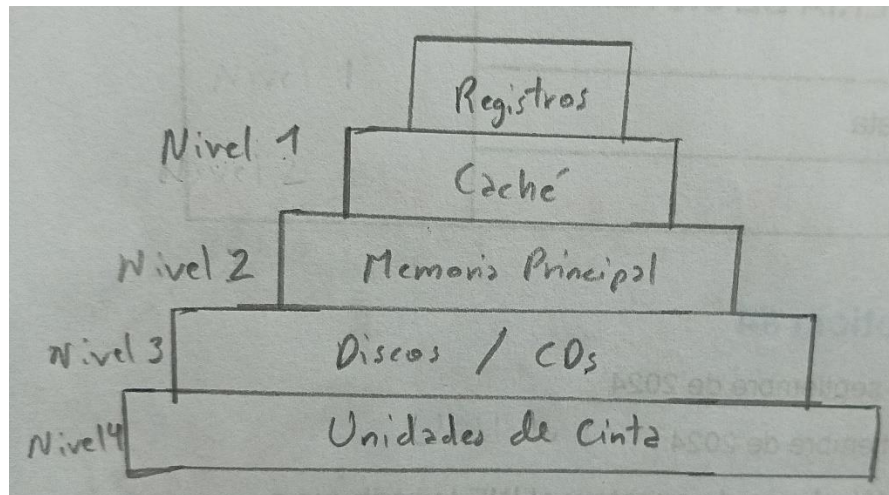
3) ¿Por qué se utiliza la tecnología de Video RAM (VRAM) en los controladores de video de las computadoras y cuál es su función principal? (2 pts)

R. Porque tiene un mayor rendimiento en el procesamiento gráfico, además que también se puede acceder a ellas de forma simultánea. La función principal de la VRAM es actuar como buffer de cuadros para almacenar información relacionada con los gráficos como: las texturas, mapas de bits, información del color de pixeles; asegurando de esta manera una representación gráfica fluida y de alta calidad. ✓

4) Dibuja un diagrama que represente la jerarquía de memoria en un sistema informático típico y

etiqueta cada nivel con el tipo correspondiente de memoria. (2 pts)

R.



5) ¿Qué diferencias existen entre la memoria caché L1, L2 y L3 en términos de tamaño, velocidad y proximidad al procesador? (2 pts)

R. La diferencia entre las tres memorias caché con referente al tamaño es que L1 es más pequeño (16 KB - 128 KB), L2 tiene más capacidad (256 KB - 1 MB), y L3 es más grande (2 MB - 30+ MB). Con referente a velocidad: L1 es más rápida, L2 tiene velocidad intermedia y L3 es más lenta. Y la proximidad al procesador sería lo siguiente: L1 está en el núcleo, L2 está cerca del núcleo y L3 está compartida entre núcleos.



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

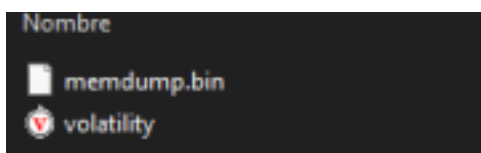
Volatility framework es una completa colección de herramientas open source, escrita en Python bajo licencia GNU, para el análisis de la memoria volátil (RAM). Tiene como objetivo introducir a las personas en las complejas técnicas de extracción de artefactos digitales de imágenes de memoria volátil (RAM), y proveer una plataforma de trabajo dentro del área de la investigación como parte de una auditoria.

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.

PARTE 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.



Ejemplo:



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**

```
Administrador: C:\Windows\System32\cmd.exe
Microsoft Windows [Versión 10.0.22631.4317]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\System32>cd

D:\>cd "D:\2024\2-2024\ARQUITECTURA DE COMPUTADORAS\Auxiliatura\Practica 3\practica3"

D:\2024\2-2024\ARQUITECTURA DE COMPUTADORAS\Auxiliatura\Practica 3\practica3>volatility imageinfo -f memdump.bin
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win2003SP0x86, Win2003SP1x86, Win2003SP2x86 (Instantiated with Win2003SP0x86)
AS Layer1 : IA32PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (D:\2024\2-2024\ARQUITECTURA DE COMPUTADORAS\Auxiliatura\Practica 3\practica3\memdump.bin)
PAE type : No PAE
DTB : 0x39000L
KDBG : 0x805583d0L
Number of Processors : 1
Image Type (Service Pack) : 0
KPCR for CPU 0 : 0xffdf000L
KUSER_SHARED_DATA : 0xffdf000L
Image date and time : 2012-11-27 02:01:57 UTC+0000
Image local date and time : 2012-11-26 20:01:57 -0600

D:\2024\2-2024\ARQUITECTURA DE COMPUTADORAS\Auxiliatura\Practica 3\practica3>volatility -f memdump.bin --profile=Win2003SP0x86 pslist
```

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

Ingrese el siguiente comando: **volatility -f memdump.bin --profile=Win2003SP0x86 pslist**

```
Administrador: C:\Windows\System32\cmd.exe

Number of Processors : 1
Image Type (Service Pack) : 0
KPCR for CPU 0 : 0xffdf000L
KUSER_SHARED_DATA : 0xffdf000L
Image date and time : 2012-11-27 02:01:57 UTC+0000
Image local date and time : 2012-11-26 20:01:57 -0600

D:\2024\2-2024\ARQUITECTURA DE COMPUTADORAS\Auxiliatura\Practica 3\practica3>volatility -f memdump.bin --profile=Win2003SP0x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit
-----
0x822b07a8 System 4 0 52 842 ----- 0
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
0x8203fad0 services.exe 488 444 21 422 0 0 2012-11-03 20:18:31 UTC+0000
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 mscsc.exe 1240 488 15 160 0 0 2012-11-03 20:19:12 UTC+0000
0x81ca3d68 dfsvc.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
0x81c4ad88 dns.exe 340 488 12 163 0 0 2012-11-03 21:41:26 UTC+0000
0x81bf9020 wins.exe 756 488 19 214 0 0 2012-11-04 17:02:01 UTC+0000
0x81be0108 wuauclt.exe 1092 932 5 74 0 0 2012-11-04 18:57:32 UTC+0000
0x81b61b18 dllhost.exe 3292 488 18 254 0 0 2012-11-24 17:47:12 UTC+0000
0x81b4b9d0 appmgr.exe 2992 488 4 102 0 0 2012-11-24 17:47:40 UTC+0000
0x81b0bb08 srvcsvrg.exe 1496 488 3 87 0 0 2012-11-24 17:47:40 UTC+0000
0x81b0f240 inetinfo.exe 300 488 25 515 0 0 2012-11-24 17:47:51 UTC+0000
0x81b71788 wmiiprsv.exe 2116 740 7 208 0 0 2012-11-24 17:48:48 UTC+0000
0x81b6a4d8 POP3Svc.exe 2260 488 7 142 0 0 2012-11-24 17:55:08 UTC+0000
0x81ae2020 cmd.exe 2076 188 1 22 0 0 2012-11-27 01:37:57 UTC+0000
0x81c25b68 mdd.exe 3468 2076 1 25 0 0 2012-11-27 02:01:56 UTC+0000

D:\2024\2-2024\ARQUITECTURA DE COMPUTADORAS\Auxiliatura\Practica 3\practica3>
```

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

Ingrese el siguiente comando: **volatility -f memdump.bin --profile=Win2003SP0x86 pstree**

```
Administrador: C:\Windows\System32\cmd.exe
0x81b6a4d8 POP3Svc.exe 2260 488 7 142 0 0 2012-11-24 17:55:08 UTC+0000
0x81ae2020 cmd.exe 2076 188 1 22 0 0 2012-11-27 01:37:57 UTC+0000
0x81c25b68 mdd.exe 3468 2076 1 25 0 0 2012-11-27 02:01:56 UTC+0000

D:\2024\2-2024\ARQUITECTURA DE COMPUTADORAS\Auxiliatura\Practica 3\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 2012-11-01 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
0x81fdaf8: 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
0x81c2d08: smss.exe 1436 488 11 276 2012-11-03 20:19:12 UTC+0000
0x81fd72e0: svchost.exe 884 488 9 133 2012-11-03 20:18:44 UTC+0000
0x81ca3d68: dfsvc.exe 1312 488 10 106 2012-11-03 20:19:12 UTC+0000
0x81c00320: ntfs.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: msdte.exe 1240 488 15 160 2012-11-03 20:19:12 UTC+0000
0x81fd6068: svchost.exe 932 488 47 1002 2012-11-03 20:18:44 UTC+0000
0x81be8108: wuaucit.exe 1092 932 5 74 2012-11-04 18:57:32 UTC+0000
0x81b61b18: dlhost.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: wmlprvse.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: wlns.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
0x81c4b08: explorer.exe 108 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

D:\2024\2-2024\ARQUITECTURA DE COMPUTADORAS\Auxiliatura\Practica 3\practica3>
```

- pstree muestra los procesos de manera más ordenada.

PASO 6

Ingrese el siguiente comando: **volatility -f memdump.bin --profile=Win2003SP0x86 dlllist**

```
Administrador: C:\Windows\System32\cmd.exe
D:\2024\2-2024\ARQUITECTURA DE COMPUTADORAS\Auxiliatura\Practica 3\practica3>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 0xf000 0xffff \SystemRoot\System32\smss.exe
0x77f40000 0xba00 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 Se
rverDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16

Base Size LoadCount Path
-----
0x4a680000 0x4000 0xffff \??\C:\WINDOWS\system32\csrss.exe
0x77f40000 0xba00 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\winsrv.dll
0x77e40000 0xf400 0x10 C:\WINDOWS\system32\KERNEL32.dll
0x77d00000 0x8f00 0x6 C:\WINDOWS\system32\USER32.dll
0x77c00000 0x4400 0x5 C:\WINDOWS\system32\GDI32.dll
0x75da0000 0xba00 0x1 C:\WINDOWS\system32\sxs.dll
0x77da0000 0x9000 0x3 C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa400 0x3 C:\WINDOWS\system32\RPCRT4.dll
0x75e60000 0x2200 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
-----
0x81000000 0x8b00 0xffff \??\C:\WINDOWS\system32\winlogon.exe
0x77f40000 0xba00 0xffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf400 0xffff C:\WINDOWS\system32\kernel32.dll
0x77b00000 0x5400 0xffff C:\WINDOWS\system32\usercr.dll
0x77da0000 0x9000 0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa400 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77d00000 0x8f00 0xffff C:\WINDOWS\system32\USER32.dll
0x77c00000 0x4400 0xffff C:\WINDOWS\system32\GDI32.dll
0x75970000 0xba00 0xffff C:\WINDOWS\system32\USERENV.dll
0x75810000 0x7000 0xffff C:\WINDOWS\system32\WDdeApi.dll
0x761b0000 0x9800 0xffff C:\WINDOWS\system32\CRYPT32.dll
0x76190000 0x1200 0xffff C:\WINDOWS\system32\MSASN1.dll
0x76f50000 0x1300 0xffff C:\WINDOWS\system32\Secur32.dll
0x76c00000 0x1000 0xffff C:\WINDOWS\system32\WINSTA.dll
0x71c40000 0x5300 0xffff C:\WINDOWS\system32\NETAPI32.dll
0x75800000 0x9000 0xffff C:\WINDOWS\system32\PROFMAP.dll
0x76b20000 0xf000 0xffff C:\WINDOWS\system32\REGAPI.dll
0x71c00000 0x1800 0xffff C:\WINDOWS\system32\WS2_32.dll
0x71bf0000 0x8000 0xffff C:\WINDOWS\system32\WS2HELP.dll
```

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

Preguntas de verificación del laboratorio

¿Qué hora inicia el proceso explorer.exe?

Inicia: 2012-11-03 21:32:38 UTC+0000



¿Qué hora inicia el proceso svchost.exe?

En mi caso hay siete procesos con ese nombre iniciando cada uno en estos tiempos:

2012-11-03 20:18:44 UTC+0000

2012-11-03 20:18:44 UTC+0000

2012-11-03 20:19:27 UTC+0000

2012-11-03 20:18:44 UTC+0000

2012-11-03 20:18:33 UTC+0000

2012-11-03 20:19:13 UTC+0000

2012-11-03 20:19:12 UTC+0000



¿Cuál es el nombre del proceso PID: 420?

Tiene el nombre de: csrss.exe



¿Cuál es el nombre del proceso PID: 932?

Tiene el nombre de: svchost.exe



PARTE PRÁCTICA (50 pts)

- 1) Determina cuántos bits en total puede almacenar una memoria RAM de 128K x 4 (5 pts)
- 2) ¿Cuántos bits puede almacenar una memoria de 10G x 16? (5 pts)
- 3) Cuántas localidades de memoria se puede direccionar con 32 líneas de dirección. (5 pts)
- 4) ¿Cuántas localidades de memoria se pueden direccionar con 1024 líneas de dirección? (5 pts)
- 5) ¿Cuántas localidades de memoria se pueden direccionar con 64 líneas de dirección? (5 pts)
- 6) Cuántas líneas de dirección se necesitan para una memoria ROM de 512M x 8. (5 pts)
- 7) ¿Cuántas líneas de dirección se necesitan para una memoria ROM de 128M x 128? (5 pts)
- 8) ¿Cuántos bits en total puede almacenar una memoria RAM 128M x 4, de él resultado gigabytes? (5 pts)
- 9) ¿Cuántos bits en total puede almacenar una memoria RAM 64M x 64, de él resultado en teras? (5 pts)
- 10) ¿Cuántos bits en total puede almacenar una memoria RAM 64M x 64, de él resultado en terabytes? (5 pts)

Ejercicios

1) $K=1024$ $128(1024) \times 4 = 524288 \text{ bits}$ ✓

2) $G=1024^3$ $10(1024^3) \times 16 = 171798691840 \text{ bits}$ ✓

3) $2^n = ? \Rightarrow 2^{32} = 4294967296 \text{ localidades}$ ✓

4) $2^n = ? \Rightarrow 2^{1024} = 1,7976931349 \times 10^{308} \text{ localidades}$ ✓

5) $2^n = ? \Rightarrow 2^{65} = 18446744073709551616 \text{ localidades}$ ✓

6) $2^n = 512M \Rightarrow n = \frac{\ln(512M)}{\ln(2)} \Rightarrow n = \frac{\ln(512 \times 1024^2)}{\ln(2)} = 29 \text{ líneas de dirección}$ ✓

7) $n = \frac{\ln(128M)}{\ln(2)} \Rightarrow n = \frac{\ln(128 \times 1024^2)}{\ln(2)} = 27 \text{ líneas de dirección}$ ✓

8) $128M \times 4 \Rightarrow 128(1024^2) \times 4 = 536870912 \text{ bits} \Rightarrow \frac{536870912}{8}$

$= 67108864 \text{ bytes} \Rightarrow \frac{67108864}{1024^3} = 0,0625 \text{ Gigabytes}$ ✓

9) $64(1024^2) \times 64 = 4294967296 \text{ bits} \Rightarrow \frac{4294967296}{8} = 536870912 \text{ bytes}$

$\frac{536870912}{1024^4} = 0,00048828125 \text{ Teras}$ ✓

10) $64(1024^3) \times 64 = \frac{4294967296}{8} = \frac{536870912}{1024^4}$

$= 0,00048828125 \text{ Terabytes}$ ✓