


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

Estudiante: Jefferson Tito Gumiel

CI: 8508426

Enlace a GIT: https://github.com/DevJTG/Practica_3.git

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. Que la memora RAM es de mas facil acceso al procesador y solo retiene información estando energizada mientras la memoria ROM retiene información aun sin tener energia.

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

R. las ventajas de la memoria estatica es su velocidad de acceso, su diseño es sencillo, retiene información estando energizada. Sus desventajas estan en que tienen menor capacidad, mayor costo por bit, consumen mas energia.

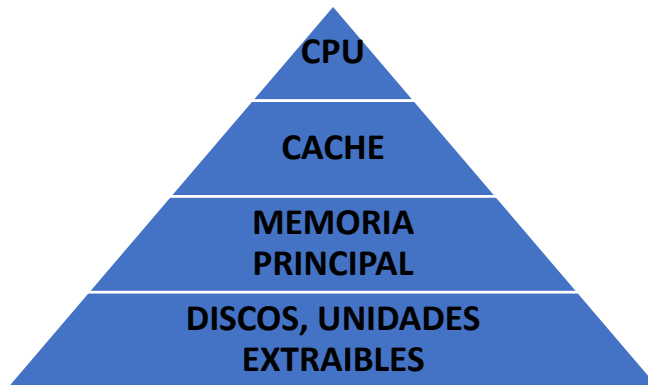
Las ventajas de la memoria dinamica es que tiene mayor capacidad, menor costo por bit, consumo de energia mas eficiente. Sus desventajas estan en su baja velocidad de acceso su diseño es complejo.

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)

R. Para guardar información sobre las imágenes que se van a procesar por la GPU

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. (2pts)

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 principal diferencia entre estos 3 tipos es la velocidad siendo la L1 mas veloz, luego la L2 y la L3 es la mas lenta

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.

CARACTERISTICAS DE LA MEMORIA

```
C:\Windows\System32\cmd.exe
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>cd C:\Users\jef_t\Downloads\practica3

C:\Users\jef_t\Downloads\practica3>volatility imageinfo -f
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.

volatility: error: -f option requires an argument

C:\Users\jef_t\Downloads\practica3>memdump.bin

C:\Users\jef_t\Downloads\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 (C:\Users\jef_t\Downloads\practica3\memdump.bin)
      PAE type : No PAE
      DTB : 0x39000L
      KDBG : 0x805583d0L
      Number of Processors : 1
      Image Type (Service Pack) : 0
      KPCR for CPU 0 : 0xfffff000L
      KUSER_SHARED_DATA : 0xfffff000L
      Image date and time : 2012-11-27 02:01:57 UTC+0000
      Image local date and time : 2012-11-26 20:01:57 -0600

C:\Users\jef_t\Downloads\practica3>
```

LISTA DE PROCESOS

```
C:\Windows\System32\cmd.exe
C:\Users\jef_t\Downloads\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     0      0  2012-11-03 20:18:29 UTC+0000
0x820c6020 smss.exe          372   4     3    17   0     0      0  2012-11-03 20:18:30 UTC+0000
0x82031020 csrss.exe          420  372    11   505   0     0      0  2012-11-03 20:18:30 UTC+0000
0x820496c8 winlogon.exe      444  372    19   613   0     0      0  2012-11-03 20:18:30 UTC+0000
0x8203fad0 services.exe  488  444    21   422   0     0      0  2012-11-03 20:18:31 UTC+0000
0x82022920 lsass.exe        500  444    58   959   0     0      0  2012-11-03 20:18:31 UTC+0000
0x822bc770 svchost.exe      740  488    12   230   0     0      0  2012-11-03 20:18:33 UTC+0000
0x81fdf2e0 svchost.exe        884  488     9   133   0     0      0  2012-11-03 20:18:44 UTC+0000
0x81fda1f8 svchost.exe        904  488     5    78   0     0      0  2012-11-03 20:18:44 UTC+0000
0x81fd6968 svchost.exe        932  488    47  1092   0     0      0  2012-11-03 20:18:44 UTC+0000
0x81caf2d8 spoolsv.exe      1216 488     9   135   0     0      0  2012-11-03 20:19:12 UTC+0000
0x81cbad88 msdtc.exe         1240 488    15   160   0     0      0  2012-11-03 20:19:12 UTC+0000
0x81ca3d68 dfssvc.exe        1312 488    10   106   0     0      0  2012-11-03 20:19:12 UTC+0000
0x81c99020 svchost.exe        1404 488     2    60   0     0      0  2012-11-03 20:19:12 UTC+0000
0x81c82d88 ismserv.exe      1436 488    11   276   0     0      0  2012-11-03 20:19:12 UTC+0000
0x81c80320 ntfrs.exe        1452 488    19   282   0     0      0  2012-11-03 20:19:12 UTC+0000
0x81c71020 svchost.exe      1512 488     2    34   0     0      0  2012-11-03 20:19:13 UTC+0000
0x81c462e8 svchost.exe      1736 488    16   127   0     0      0  2012-11-03 20:19:27 UTC+0000
0x81c4bd88 explorer.exe     188 1996    11   337   0     0      0  2012-11-03 21:32:38 UTC+0000
0x81c4ad88 dns.exe       340  488    12   163   0     0      0  2012-11-03 21:41:26 UTC+0000
0x81bf9020 wins.exe       756  488    19   214   0     0      0  2012-11-04 17:02:01 UTC+0000
0x81be0108 wuauc1t.exe      1092 932     5    74   0     0      0  2012-11-04 18:57:32 UTC+0000
0x81b61b18 dllhost.exe   3292 488    18   254   0     0      0  2012-11-24 17:47:12 UTC+0000
0x81b4b9d0 appmgr.exe   2992 488     4   102   0     0      0  2012-11-24 17:47:40 UTC+0000
0x81b0bb08 srvcurg.exe      1496 488     3    87   0     0      0  2012-11-24 17:47:40 UTC+0000
0x81b8f348 inetinfo.exe       308  488    25   515   0     0      0  2012-11-24 17:47:51 UTC+0000
0x81b71788 wmiiprvse.exe     2116 740     7   208   0     0      0  2012-11-24 17:48:48 UTC+0000
0x81b6a4d8 POP3Svc.exe  2260 488     7   142   0     0      0  2012-11-24 17:55:08 UTC+0000
0x81ae2020 cmd.exe          2076 188     1    22   0     0      0  2012-11-27 01:37:57 UTC+0000
0x81c25b68 mdd.exe           3468 2076     1    25   0     0      0  2012-11-27 02:01:56 UTC+0000
```

LISTA DE PROCESOS ORDENADA

```
C:\Windows\System32\cmd.exe
C:\Users\jef.t\Downloads\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
0x81fdalf8: svchost.exe            904    488     5    78 2012-11-03 20:18:44 UTC+0000
0x81b0bb08: srvcsvr.exe            1496   488     3    87 2012-11-24 17:47:40 UTC+0000
0x81c82d88: ismserv.exe            1436   488    11   276 2012-11-03 20:19:12 UTC+0000
0x81fdf2e0: svchost.exe            884    488     9    13 2012-11-03 20:18:44 UTC+0000
0x81ca3d68: dfssvc.exe             1312   488    10   106 2012-11-03 20:19:12 UTC+0000
0x81c80320: ntrfs.exe             1452   488    19   282 2012-11-03 20:19:12 UTC+0000
0x81b4b9d0: appmgr.exe             2992   488     4    10 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    13 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    16 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: wuaucit.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: wmiiprvse.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    14 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
```

LIBRERIAS QUE SE ESTAN USANDO

```
C:\Windows\System32\cmd.exe
C:\Users\jef.t\Downloads\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  0xfffff \SystemRoot\System32\smss.exe
0x77f40000     0xba000  0xfffff 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 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16

Base          Size  LoadCount Path
-----
0x4a680000     0x4000  0xfffff \??\C:\WINDOWS\system32\csrss.exe
0x77f40000     0xba000  0xfffff C:\WINDOWS\system32\ntdll.dll
0x75a50000     0xb000  0xfffff C:\WINDOWS\system32\CSRSSRV.dll
0x75a60000     0xf000  0x3 C:\WINDOWS\system32\basesrv.dll
0x75a80000     0x4c000  0x2 C:\WINDOWS\system32\winsrv.dll
0x77e40000     0xf4000  0x10 C:\WINDOWS\system32\KERNEL32.dll
0x77d00000     0x8f000  0x6 C:\WINDOWS\system32\USER32.dll
0x77c00000     0x44000  0x5 C:\WINDOWS\system32\GDI32.dll
0x75da0000     0xba000  0x1 C:\WINDOWS\system32\sxs.dll
0x77da0000     0x90000  0x3 C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000     0xa4000  0x3 C:\WINDOWS\system32\RPCRT4.dll
0x75e60000     0x22000  0x1 C:\WINDOWS\system32\Apphelp.dll
0x77b90000     0x8000  0x1 C:\WINDOWS\system32\VERSION.dll
```

Preguntas de verificación del laboratorio

¿Qué hora inicia el proceso explorer.exe?

R. A las 21:32:38

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
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

¿Qué hora inicia el proceso svchost.exe?

R. A las 20:19

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
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

¿Cuál es el nombre del proceso PID: 420?

R. csrss.exe

¿Cuál es el nombre del proceso PID: 932?

R. svchost.exe