


<div>UNIVERSIDAD AUTÓNOMA “TOMAS FRÍAS”</div> <div>CARRERA DE INGENIERÍA DE SISTEMAS</div>				
Materia:	Arquitectura de computadoras (SIS-522)			
Docente:	Ing. Gustavo A. Puita Choque			
Auxiliar:	Univ. Aldrin Roger Perez Miranda			
23/09/2024	Fecha publicación			
07/10/2024	Fecha de entrega			
Grupo:	1	Sede	Potosí	<div>Nº Práctica</div> <div>3</div>

Parte teórica

1. ¿Cuál es la diferencia fundamental entre una memoria RAM y una memoria ROM en términos de accesibilidad y volatilidad?

R. que la memoria RAM almacena datos temporalmente y la ROM lo hace permanentemente

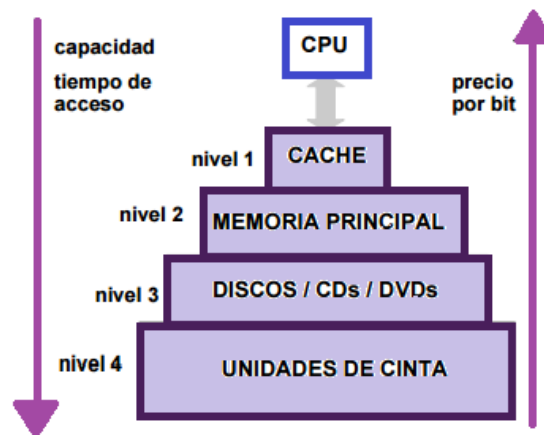
2. ¿Qué ventajas y desventajas presentan las memorias estáticas y dinámicas en términos de velocidad, densidad y costo?

Memoria	Ventajas	Desventajas
Estática	<ul style="list-style-type: none"> La velocidad de acceso es alta Para retener los datos solo necesita estar energizada Son fáciles de diseñar 	<ul style="list-style-type: none"> Menor capacidad debido a que cada celda de almacenamiento requiere más transistores Mayor costo por bit Mayor consumo de potencia
Dinámica	<ul style="list-style-type: none"> Mayor densidad y capacidad Menor costo por bit Menor consumo por potencia 	<ul style="list-style-type: none"> La velocidad de acceso es baja Necesita recarga de la información. Almacenamiento 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?

R. Para poder mantener el refresco de la información en el monitor a una velocidad constante a la misma vez que el programa actualiza la información a desplegar en la pantalla.

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.



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

Caché L1: es el nivel más básico, la más cercana al procesador y la más rápida. También es la que menos capacidad tiene

Caché L2: es un nivel intermedio que presenta un buen equilibrio entre capacidad, cercanía y velocidad.

Caché L3: posiciona en un nivel inferior a la anterior tanto en cercanía como en velocidad, pero tiene una capacidad mucho mayor

Laboratorio

6. Resolver el siguiente laboratorio paso a paso con capturas propias mostrando su barra de tareas de su pc

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.

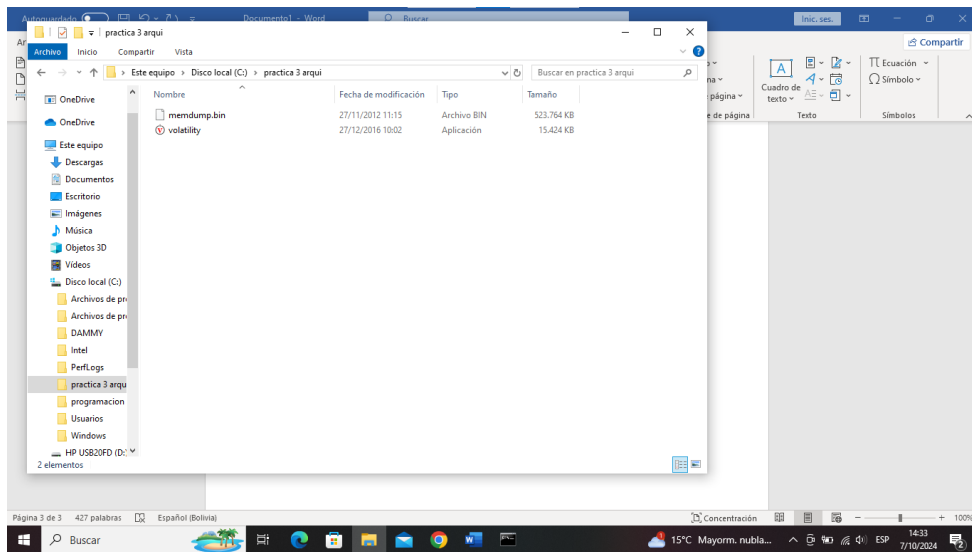
Objetivo General. - Realizar el análisis de auditoría de una imagen de memoria RAM con el uso de la herramienta Volatility.

Se analizará una memoria ya capturada.

PARTE 1

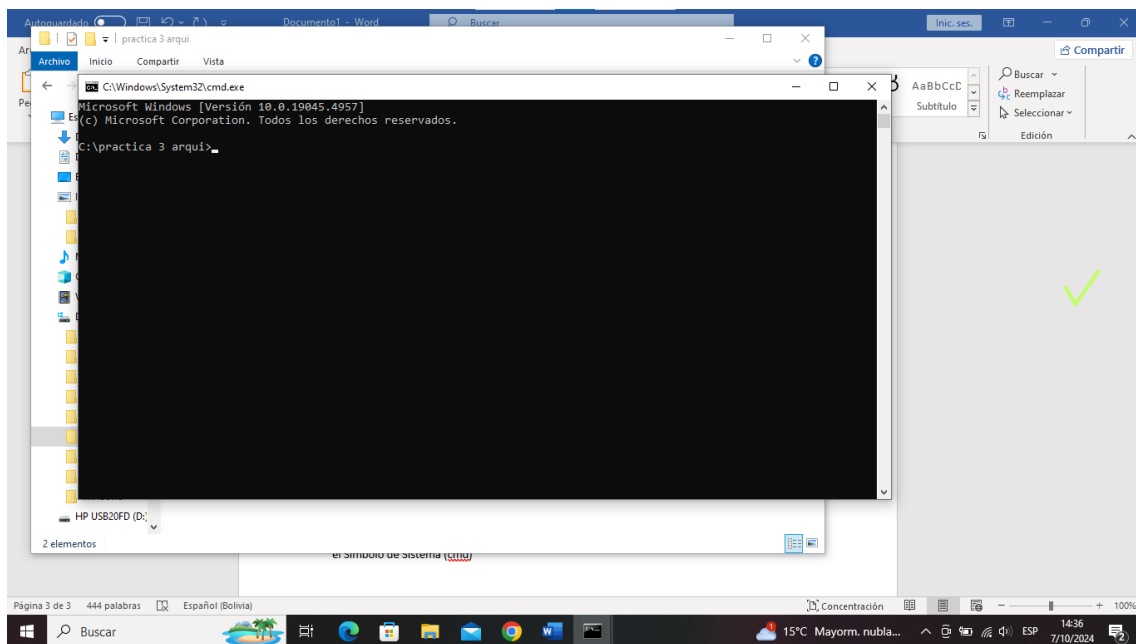
PASO 1

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.



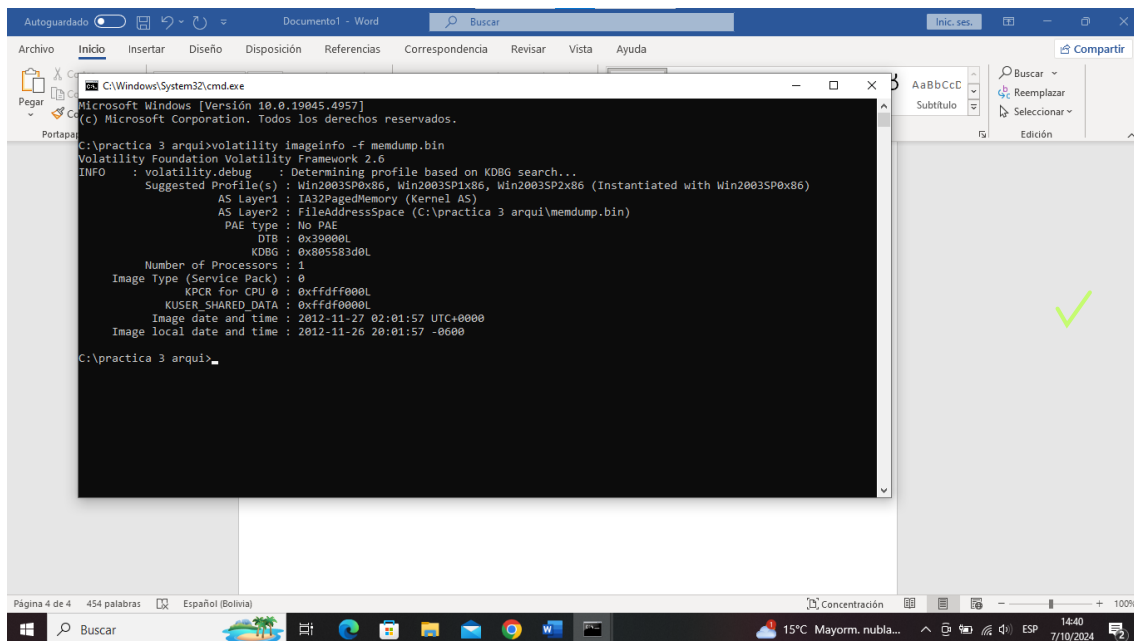
PASO 2

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



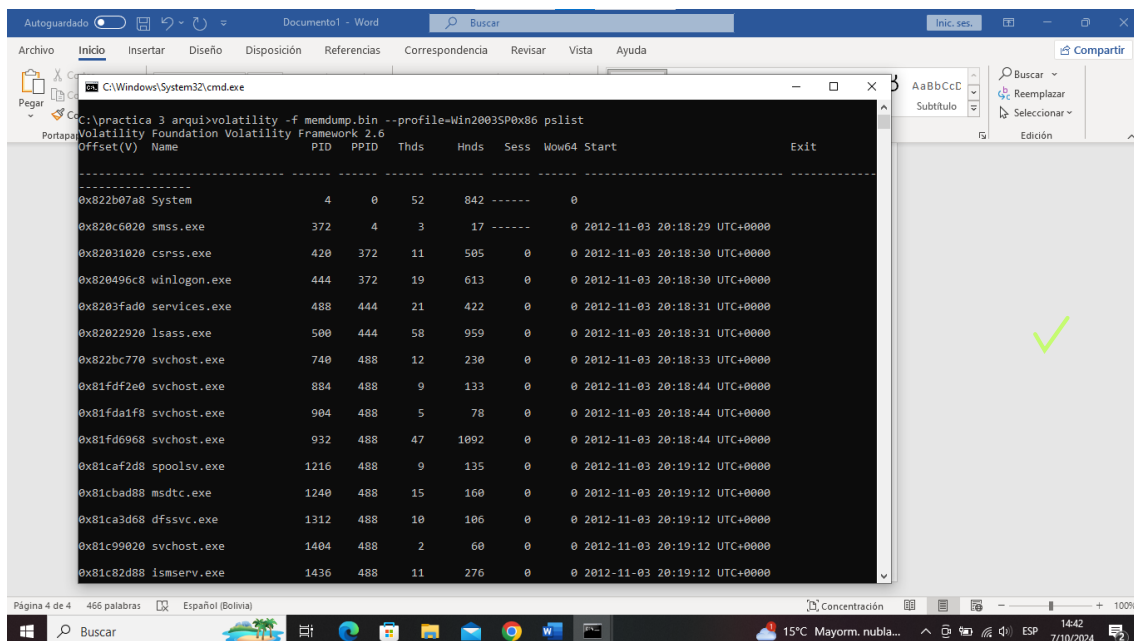
PASO 3

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



PASO 4

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



PASO 5

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

```

C:\Windows\System32\cmd.exe
C:\practica 3\arquib>volatility -f memdump.bin --profile=Win2003SP0x86 pstree
Volatility Foundation Volatility Framework 2.6
-----
Pid      PPID     Tids     Hnds     Time
-----
0x822b7a8: System
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
0x81b0b008: svcsrv.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
0x81fd2e0: 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: ntfsn.exe     1452     488     19     282 2012-11-03 20:19:12 UTC+0000
0x81b4b0d0: appmgr.exe    2992     488      4     102 2012-11-24 17:47:40 UTC+0000
0x81b8f4d0: 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
0x81fd60b0: svchost.exe     932     488     47    1092 2012-11-03 20:18:44 UTC+0000
0x81be0188: wuaucit.exe   1092     932      5      74 2012-11-04 18:57:32 UTC+0000
0x81b1b18: dllhost.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: wmiprvse.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
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
C:\practica 3\arquib>

```

PASO 6

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

```

C:\Windows\System32\cmd.exe
C:\practica 3\arquib>volatility -f memdump.bin --profile=Win2003SP0x86 dlllist
Volatility Foundation Volatility Framework 2.6
-----
System pid: 4
Unable to read PEB for task.
-----
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 ServerDll=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\CSRSSRV.dll
0x75a60000 0xf000 0x3 C:\WINDOWS\system32\basesrv.dll
0x75a80000 0x4c00 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

```

Preguntas de verificación del laboratorio

¿Qué hora inicia el proceso explorer.exe?

explorer.exe 188 1996 11 337 0 0 2012-11-03 21:32:38 UTC+0000

¿Qué hora inicia el proceso svchost.exe?

svchost.exe 740 488 12 230 0 0 2012-11-03 20:18:33 UTC+0000

¿Cuál es el nombre del proceso PID: 420?



csrss.exe

¿Cuál es el nombre del proceso PID: 932?



svchost.exe

Parte Practica

1) Determina cuántos bits en total puede almacenar una memoria

RAM de 128K x 4

$$128 \times 1024 = 131072$$



tamaño de palabra → 4

$$131072 \times 4 = 524288$$

R. se pueden almacenar 524288 bits

2) ¿Cuántos bits puede almacenar una memoria de 10G x 16?

$$10 \times 1024^3 = 1.073741824 \times 10^{10}$$

$$1.073741824 \times 16 = 1.717986918 \times 10^{11}$$

R. se pueden almacenar $1.717986918 \times 10^{11}$ bits



3) Cuántas localidades de memoria se puede direccionar con 32

líneas de dirección.

$$2^n = \# \text{ de localidades}$$

$$n = 32 \quad 2^{32} = 42949667296$$



R. 42949667296 localidades de memoria

4) ¿Cuántas localidades de memoria se pueden direccionar con

1024 líneas de dirección?

$$2^n = \# \text{ de localidades}$$

$$n = 1024 \quad 2^{1024} = 1.7976931348623157 \times 10^{308}$$



R. $1.7976931348623157 \times 10^{308}$ localidades de memoria

5) ¿Cuántas localidades de memoria se pueden direccionar con 64 líneas de dirección?

$$2^n = \# \text{ de localidades}$$

$$n = 64 \quad 2^{64} = 1.844674407 \times 10^{19}$$



R. $1.844674407 \times 10^{19}$ localidades de memoria

6) Cuántas líneas de dirección se necesitan para una memoria ROM de 512M x 8.

$$n=? \quad 512 \times 1024^2 = 536870912$$

$$n=29 \quad 2^{29} = 536870912$$



R. se necesitan 29 líneas de dirección

7) ¿Cuántas líneas de dirección se necesitan para una memoria ROM de 128M x 128?

$$n=? \quad 128 \times 1024^2 = 134217728$$

$$n=27 \quad 2^{27} = 134217728$$



R. se necesitan 27 líneas de dirección

8) ¿Cuántos bits en total puede almacenar una memoria RAM 128M x 4, de él resultado gigabytes?

$$n=27 \quad \text{tamaño de palabra} \rightarrow 4$$

$$128 \times 1024^2 = 134217728$$

$$134217728 \times 4 = 536870912 \text{ bits}$$

$$536870912 \div 1024 = 524288 \text{ kb}$$

$$524288 \div 1024 = 512 \text{ M}$$

$$512 \div 1024 = 0.5 \text{ G}$$

0,0625

R. se pueden almacenar 0.5 gigabytes



9) ¿Cuántos bits en total puede almacenar una memoria RAM 64M x 64, de él resultado en teras?

$$n=26 \quad 64 \times 1024^2 = 67108864$$

$$67108864 \times 64 = 4294967296 \text{ bits}$$

$$4294967296 \div 1024 = 4194304 \text{ kb}$$

$$4194304 \div 1024 = 4096 \text{ M}$$

$$4096 \div 1024 = 4 \text{ G}$$

$$4 \div 1024 = 0.003906 \text{ T}$$

0,00048828125

R. se pueden almacenar 0.003906 T



10) ¿Cuántos bits en total puede almacenar una memoria RAM 64M x 64, de él resultado en terabytes?

$$n=26 \quad 64 \times 1024^2 = 67108864$$

$$67108864 \times 64 = 4294967296 \text{ bits}$$

$$4294967296 \div 1024 = 4194304 \text{ kb}$$

$$4194304 \div 1024 = 4096 \text{ M}$$

$$4096 \div 1024 = 4 \text{ G}$$

$$4 \div 1024 = 0.003906 \text{ T} \quad 0,00048828125$$

R. se pueden almacenar 0.003906 T 