


<u>UNIVERSIDAD AUTÓNOMA “TOMAS FRÍAS” CARRERA DE INGENIERÍA DE SISTEMAS</u>				
Estudiante:	José Clemente Huanaco Camata			
Materia:	Arquitectura de computadoras (SIS-522)			
Docente:	Ing. Gustavo A. Puita Choque Univ. Aldrin Roger Perez Miranda			N° Práctica
Auxiliar:				3
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.

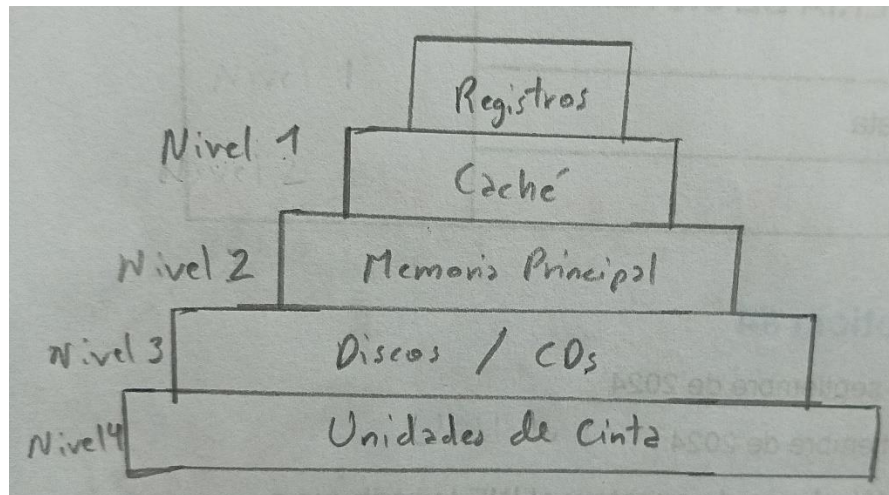
3) ¿Por qué se utiliza la tecnología de Video RAM (VRAM) en los controladores de video de las computadoras y cuál es su función principal? (2 pts)

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

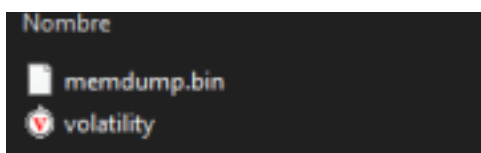
Volatility framework es una completa colección de herramientas open source, escrita en Python bajo licencia GNU, para el análisis de la memoria volátil (RAM). Tiene como objetivo introducir a las personas en las complejas técnicas de extracción de artefactos digitales de imágenes de memoria volátil (RAM),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

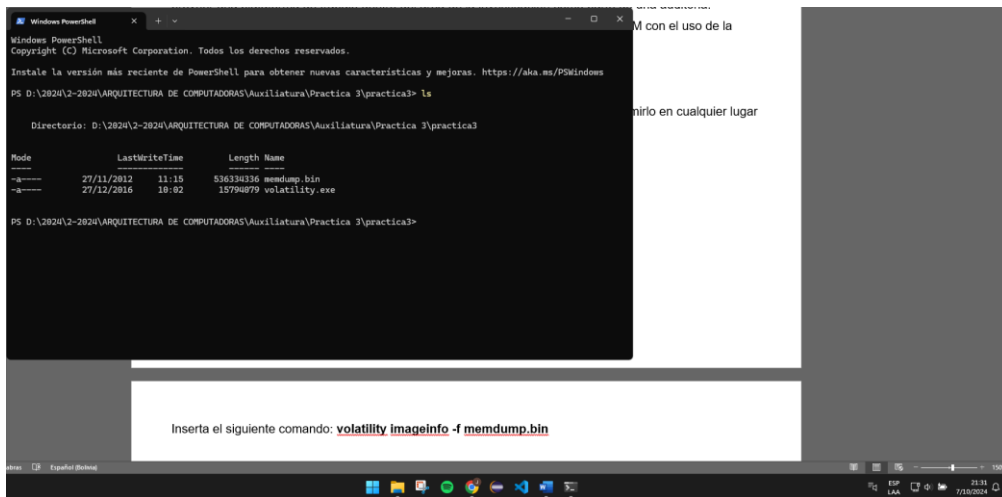
Descarga el archivo comprimido "practica3" de la plataforma Classroom, descomprimirlo en cualquier lugar de tu equipo, los dos archivos deben estar en un mismo lugar.



Ejemplo:

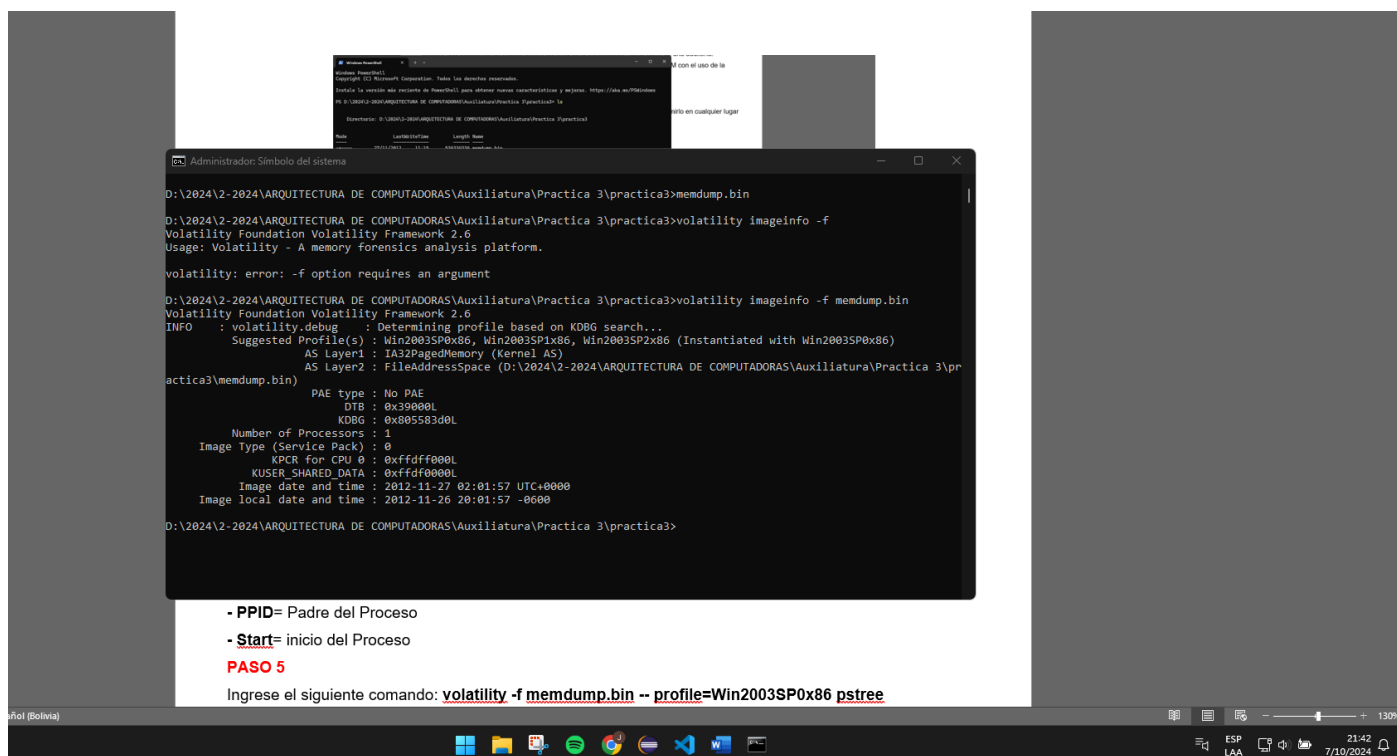
PASO 2

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**



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: Símbolo del sistema
IA32PagedMemoryPae: No valid DTB found
IA32PagedMemory: No valid DTB found
OSXPmemELF: ELF Header signature invalid
FileAddressSpace: Must be first Address Space
ArmAddressSpace: No valid DTB found

D:\2024\2-2024\ARQUITECTURA DE COMPUTADORAS\Auxiliatura\Practica 3\practica3>volatility -f memdump.bin -- profile=Win2003SP0x86 pslist
Volatility Foundation Volatility Framework 2.6
No suitable address space mapping found
Tried to open image as:
MachOAddressSpace: mac: need base
LimeAddressSpace: lime: need base
WindowsHiberFileSpace32: No base Address Space
WindowsCrashDumpSpace64BitMap: No base Address Space
VMWareMetaAddressSpace: No base Address Space
WindowsCrashDumpSpace64: No base Address Space
HPAKAddressSpace: No base Address Space
VirtualBoxCoreDumpElf64: No base Address Space
VMWareAddressSpace: No base Address Space
QemuCoreDumpElf: No base Address Space
WindowsCrashDumpSpace32: No base Address Space
Win10AMD64PagedMemory: No base Address Space
WindowsAMD64PagedMemory: No base Address Space
LinuxAMD64PagedMemory: No base Address Space
AMD64PagedMemory: No base Address Space
IA32PagedMemoryPae: No base Address Space
IA32PagedMemory: No base Address Space
OSXPmemELF: No base Address Space
MachOAddressSpace: MachO Header signature invalid
LimeAddressSpace: Invalid lime header signature
WindowsHiberFileSpace32: No xpress signature found
WindowsCrashDumpSpace64BitMap: Header signature invalid
VMWareMetaAddressSpace: VMWare metadata file is not available
WindowsCrashDumpSpace64: Header signature invalid
HPAKAddressSpace: Invalid magic found
VirtualBoxCoreDumpElf64: ELF Header signature invalid
VMWareAddressSpace: Invalid VMware signature: 0xf00ff53
QemuCoreDumpElf: ELF Header signature invalid
WindowsCrashDumpSpace32: Header signature invalid
Win10AMD64PagedMemory: Incompatible profile WinXPSP2x86 selected
WindowsAMD64PagedMemory: Incompatible profile WinXPSP2x86 selected
LinuxAMD64PagedMemory: Incompatible profile WinXPSP2x86 selected
AMD64PagedMemory: Incompatible profile WinXPSP2x86 selected
IA32PagedMemoryPae: No valid DTB found
IA32PagedMemory: No valid DTB found
OSXPmemELF: ELF Header signature invalid
FileAddressSpace: Must be first Address Space
ArmAddressSpace: No valid DTB found
```

(DESDE AQUÍ EL RESTO DE COMANDOS NO ME FUNCIONARON)

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: Símbolo del sistema
OSXPmemELF: ELF Header signature invalid
FileAddressSpace: Must be first Address Space
ArmAddressSpace: No valid DTB found

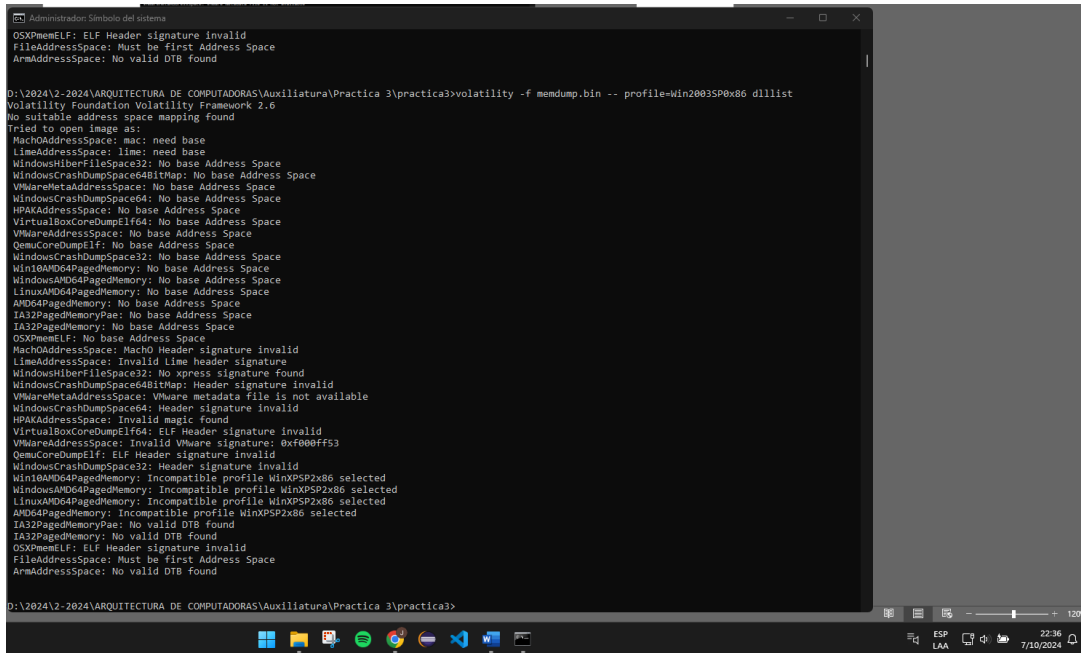
D:\2024\2-2024\ARQUITECTURA DE COMPUTADORAS\Auxiliatura\Practica 3\practica3>volatility -f memdump.bin -- profile=Win2003SP0x86 pstree
Volatility Foundation Volatility Framework 2.6
No suitable address space mapping found
Tried to open image as:
MachOAddressSpace: mac: need base
LimeAddressSpace: lime: need base
WindowsHiberFileSpace32: No base Address Space
WindowsCrashDumpSpace64BitMap: No base Address Space
VMWareMetaAddressSpace: No base Address Space
WindowsCrashDumpSpace64: No base Address Space
HPAKAddressSpace: No base Address Space
VirtualBoxCoreDumpElf64: No base Address Space
VMWareAddressSpace: No base Address Space
QemuCoreDumpElf: No base Address Space
WindowsCrashDumpSpace32: No base Address Space
Win10AMD64PagedMemory: No base Address Space
WindowsAMD64PagedMemory: No base Address Space
LinuxAMD64PagedMemory: No base Address Space
AMD64PagedMemory: No base Address Space
IA32PagedMemoryPae: No base Address Space
IA32PagedMemory: No base Address Space
OSXPmemELF: No base Address Space
MachOAddressSpace: MachO Header signature invalid
LimeAddressSpace: Invalid lime header signature
WindowsHiberFileSpace32: No xpress signature found
WindowsCrashDumpSpace64BitMap: Header signature invalid
WindowsCrashDumpSpace64: Header signature invalid
HPAKAddressSpace: Invalid magic found
VirtualBoxCoreDumpElf64: ELF Header signature invalid
VMWareAddressSpace: Invalid VMware signature: 0xf00ff53
QemuCoreDumpElf: ELF Header signature invalid
WindowsCrashDumpSpace32: Header signature invalid
Win10AMD64PagedMemory: Incompatible profile WinXPSP2x86 selected
WindowsAMD64PagedMemory: Incompatible profile WinXPSP2x86 selected
LinuxAMD64PagedMemory: Incompatible profile WinXPSP2x86 selected
AMD64PagedMemory: Incompatible profile WinXPSP2x86 selected
IA32PagedMemoryPae: No valid DTB found
IA32PagedMemory: No valid DTB found
OSXPmemELF: ELF Header signature invalid
FileAddressSpace: Must be first Address Space
ArmAddressSpace: No valid DTB found

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

- **pstree** muestra los procesos de manera más ordenada.

PASO 6

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



```
Administrador: Símbolo del sistema
OSXPneumELF: ELF Header signature invalid
FileAddressSpace: Must be first Address Space
ArmAddressSpace: No valid DTB found

D:\2024\2-2024\ARQUITECTURA DE COMPUTADORAS\Auxiliatura\Practica 3\practica3>volatility -f memdump.bin -- profile=Win2003SP0x86 dlllist
Volatility Foundation Volatility Framework 2.6
No suitable address space mapping found
Tried to open image as:
MachAddressSpace: mach: need base
LimeAddressSpace: lime: need base
WindowsHiberFileSpace32: No base Address Space
WindowsCrashDumpSpace64BitMap: No base Address Space
VMWareMetaAddressSpace: No base Address Space
WindowsCrashDumpSpace64: No base Address Space
HPAAddressSpace: No base Address Space
VirtualBoxCoreDumpElf64: No base Address Space
VMWareAddressSpace: No base Address Space
QemuCoreDumpElf: No base Address Space
WindowsCrashDumpSpace32: No base Address Space
Win10AMD64PagedMemory: No base Address Space
WindowsAMD64PagedMemory: No base Address Space
LinuxAMD64PagedMemory: No base Address Space
AMD64PagedMemory: No base Address Space
IA32PagedMemoryPae: No base Address Space
IA32PagedMemory: No base Address Space
OSXPneumELF: No base Address Space
MachAddressSpace: MachO Header signature invalid
LimeAddressSpace: Invalid Lime header signature
WindowsHiberFileSpace32: No xpress signature found
WindowsCrashDumpSpace64BitMap: Header signature invalid
VMWareMetaAddressSpace: VMWare metadata file is not available
WindowsCrashDumpSpace64: Header signature invalid
HPAAddressSpace: Invalid magic found
VirtualBoxCoreDumpElf64: ELF Header signature invalid
VMWareAddressSpace: Invalid VMWare signature: 0xf000ff53
QemuCoreDumpElf: ELF Header signature invalid
WindowsCrashDumpSpace32: Header signature invalid
Win10AMD64PagedMemory: Incompatible profile WinXPS2x86 selected
WindowsAMD64PagedMemory: Incompatible profile WinXPS2x86 selected
LinuxAMD64PagedMemory: Incompatible profile WinXPS2x86 selected
AMD64PagedMemory: Incompatible profile WinXPS2x86 selected
IA32PagedMemoryPae: No valid DTB found
IA32PagedMemory: No valid DTB found
OSXPneumELF: ELF Header signature invalid
FileAddressSpace: Must be first Address Space
ArmAddressSpace: No valid DTB found

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

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

Preguntas de verificación del laboratorio

- ¿Qué hora inicia el proceso explorer.exe?
- ¿Qué hora inicia el proceso svchost.exe?
- ¿Cuál es el nombre del proceso PID: 420?
- ¿Cuál es el nombre del proceso PID: 932?

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

$= 0,00048828125 \text{ Terabytes}$)