
Creando una Trayectoria Profesional en Seguridad Digital

Laboratorio 4: Introducción al Análisis Forense

Agosto, 2021

Índice

1. Laboratorio 4	3
1.1. Laboratorio 4A	3
1.2. Laboratorio 4B	6
1.3. Laboratorio 4C	9
1.4. Laboratorio 4D	9

1. Laboratorio 4

Acerca del Laboratorio 4

Objetivo: en este laboratorio se realizará la adquisición forense y análisis de un volcado de memoria RAM de un sistema operativo Windows.

Requerimientos: Máquina Virtual con Sistema Operativo Kali Linux o Sistema Operativo Windows anfitrión, con la herramienta de análisis forense *volatility* instalada

1.1. Laboratorio 4A

Nota: Las instrucciones son las mismas para ambos sistemas operativos, Python es un lenguaje independiente a la arquitectura.

1. Descargue el volcado de memoria RAM `memdump.mem.zip` de la carpeta de la nube [Laboratorio 4](#). Descomprima y arrastre el volcado a su maquina virtual con S.O. Kali Linux o en su S.O Windows, si desea hacerlo en su equipo anfitrión.

En el sistema operativo Kali Linux:

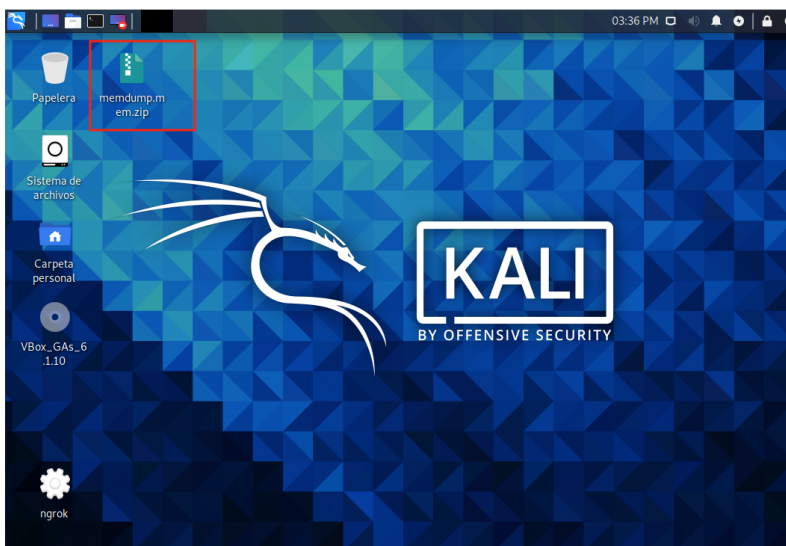


Figura 1:

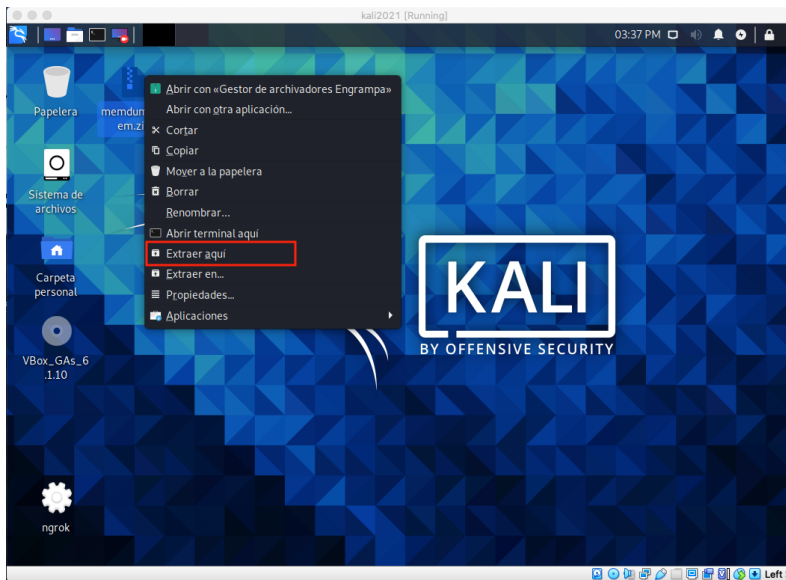


Figura 2:

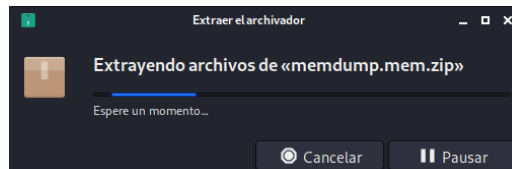


Figura 3:

2. Diríjase a la carpeta donde instaló volatility3. Despliegue la información del sistema operativo donde se realizó la captura de memoria RAM `memdump.mem`. Es importante identificar el directorio donde extrajo dicha captura

```
python3 vol.py -f /home/kali/Escritorio/memdump.mem/memdump.mem  
windows.info
```

, donde la opción `-f` recibe como argumento la locación de la captura y el argumento `windows.info` muestra el resultado de la información



1.1 Laboratorio 4A

```
Volatility 3 Framework 1.0.1
Progress: 100.00 PDB scanning finished
Variable Value
Kernel Base 0xf80002857000
DTB 0x187000
Symbols file:///home/kali/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/DAD0B889360E450292977378F364B110-1.json.xz
Is64Bit True
IsPAE False
Primary 0 WindowsIntel32e
Memory Layer 1 FileLayer
KdDebuggerDataBlock 0xf80002a3a120
NTBuildLab 7601.24214.amd64fre.win7sp1_ldr_
CSDVersion 1
KdVersionBlock 0xf80002a3a0e8
Major/Minor 15.7601
MachineType 34404
KeNumberProcessors 1
SystemTime 2021-04-18 22:33:16
NtSystemRoot C:\Windows
NtProductType NtProductWinNt
NtMajorVersion 6
NtMinorVersion 1
PE MajorOperatingSystemVersion 6
PE MinorOperatingSystemVersion 1
PE Machine 34404
PE TimeDateStamp Thu Aug 2 02:18:10 2018
```

Figura 4:

- ¿Qué versión del sistema operativo Windows es aquel donde se realizó la captura?
- ¿Qué arquitectura del sistema operativo Windows es aquella donde se realizó la captura?
- ¿Qué service pack se utilizó en la versión del sistema operativo Windows ?

3. Liste los procesos que el usuario estaba ejecutando en ese momento.

```
python3 vol.py -f /home/kali/Escritorio/memdump.mem/memdump.mem
windows.pslist
```

, donde el argumento windows.pslist muestra la lista de procesos



1.2 Laboratorio 4B

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
4	0	System	0xfa800cc0040 81	524	N/A	False	2021-04-18 23:29:11.000000	N/A	Disabled	
272	4	smss.exe	0xfa8001df6920 2	29	N/A	False	2021-04-18 23:29:11.000000	N/A	Disabled	
340	332	csrss.exe	0xfa80026cb060 9	379	0	False	2021-04-18 23:29:12.000000	N/A	Disabled	
388	332	wininit.exe	0xfa80026d75c0 4	80	0	False	2021-04-18 23:29:12.000000	N/A	Disabled	
400	380	csrss.exe	0xfa8000cc5800 7	239	1	False	2021-04-18 23:29:12.000000	N/A	Disabled	
440	380	winlogon.exe	0xfa80026b4580 5	116	1	False	2021-04-18 23:29:12.000000	N/A	Disabled	
484	388	services.exe	0xfa80026d9b00 8	183	0	False	2021-04-18 23:29:12.000000	N/A	Disabled	
500	388	lsass.exe	0xfa80027f1b00 7	486	0	False	2021-04-18 23:29:12.000000	N/A	Disabled	
508	388	lsass.exe	0xfa8002804b00 10	147	0	False	2021-04-18 23:29:12.000000	N/A	Disabled	
608	484	svchost.exe	0xfa800286f060 11	351	0	False	2021-04-18 23:29:13.000000	N/A	Disabled	
672	484	VBoxService.exe	0xfa800288c8e0 12	125	0	False	2021-04-18 23:29:13.000000	N/A	Disabled	
728	484	svchost.exe	0xfa80028a29b0 6	246	0	False	2021-04-18 23:29:13.000000	N/A	Disabled	
780	484	svchost.exe	0xfa80028d9b00 18	384	0	False	2021-04-18 23:29:13.000000	N/A	Disabled	
908	484	svchost.exe	0xfa800293a860 22	447	0	False	2021-04-18 23:29:13.000000	N/A	Disabled	
948	484	svchost.exe	0xfa800297a710 36	484	0	False	2021-04-18 23:29:13.000000	N/A	Disabled	
992	484	svchost.exe	0xfa800295bb00 33	752	0	False	2021-04-18 23:29:13.000000	N/A	Disabled	
1088	780	audiogd.exe	0xfa8001c34370 5	126	0	False	2021-04-18 23:29:13.000000	N/A	Disabled	
1104	484	svchost.exe	0xfa80029d2060 16	351	0	False	2021-04-18 23:29:14.000000	N/A	Disabled	
1200	484	spoolsv.exe	0xfa8002a153f0 14	270	0	False	2021-04-18 23:29:14.000000	N/A	Disabled	
1236	484	svchost.exe	0xfa8002a2fb00 19	321	0	False	2021-04-18 23:29:14.000000	N/A	Disabled	
1332	484	svchost.exe	0xfa8002a095f0 10	148	0	False	2021-04-18 23:29:15.000000	N/A	Disabled	
1420	484	svchost.exe	0xfa8002b12900 26	299	0	False	2021-04-18 23:29:15.000000	N/A	Disabled	
1848	484	taskhost.exe	0xfa80025b78e0 11	220	1	False	2021-04-18 23:29:17.000000	N/A	Disabled	
1900	908	dwm.exe	0xfa8002b29290 5	75	1	False	2021-04-18 23:29:17.000000	N/A	Disabled	
1912	1884	explorer.exe	0xfa8002c1cb00 27	758	1	False	2021-04-18 23:29:17.000000	N/A	Disabled	
1320	1912	VBoxTray.exe	0xfa8002c51b00 14	144	1	False	2021-04-18 23:29:17.000000	N/A	Disabled	
904	1912	notepad.exe	0xfa8002918b00 1	66	1	False	2021-04-18 23:29:21.000000	N/A	Disabled	
1984	484	SearchIndexer.exe	0xfa8002d03060 15	1629	0	False	2021-04-18 23:29:24.000000	N/A	Disabled	
1268	1984	SearchProtocolHost.exe	0xfa8002d9ab00 6	311	0	False	2021-04-18 23:29:25.000000	N/A	Disabled	
2852	1984	SearchFilterHost.exe	0xfa8001cd2a50 4	92	0	False	2021-04-18 23:29:25.000000	N/A	Disabled	
2288	1912	mspaint.exe	0xfa8002e445f0 6	134	1	False	2021-04-18 23:29:28.000000	N/A	Disabled	
2320	484	svchost.exe	0xfa8002da85f0 7	108	0	False	2021-04-18 23:29:28.000000	N/A	Disabled	
2428	1912	notepad.exe	0xfa8002e525f0 1	65	1	False	2021-04-18 23:30:06.000000	N/A	Disabled	
2612	1912	bandera_siete.exe	0xfa8002b19330 27	465	1	False	2021-04-18 23:30:12.000000	N/A	Disabled	

Figura 5:

- ¿Qué procesos estaba utilizando al momento de la captura?
- ¿Se puede identificar una bandera dentro de los procesos?

Identifique el PID del proceso mspaint.exe ya que se utilizará más adelante

1.2. Laboratorio 4B

4. En un análisis forense es importante localizar el registro hive del S.O. Windows. Liste los registros y muestre los llaves

```
python3 vol.py -f /home/kali/Escritorio/memdump.mem/memdump.mem  
windows.registry.hivelist
```

, donde el argumento windows.registry.hivelist muestra las llaves y registros el hivelist

1.2 Laboratorio 4B

```
0xf8a00000f010 Disabled
0xf8a000024010 \REGISTRY\MACHINE\SYSTEM Disabled
0xf8a00004f010 \REGISTRY\MACHINE\HARDWARE Disabled
0xf8a0000e6010 \SystemRoot\System32\Config\DEFAULT Disabled
0xf8a0007d1010 \SystemRoot\System32\Config\SECURITY Disabled
0xf8a0007eb010 \SystemRoot\System32\Config\SOFTWARE Disabled
0xf8a001301010 \Device\HarddiskVolume1\Boot\BCD Disabled
0xf8a0016e3010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT Disabled
0xf8a001795010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT Disabled
0xf8a001ac3010 \??\C:\System Volume Information\Syscache.hve Disabled
0xf8a001c51010 \??\C:\Users\pruebas\ntuser.dat Disabled
0xf8a001c921f0 \??\C:\Users\pruebas\AppData\Local\Microsoft\Windows\UsrClass.dat Disabled
0xf8a004011010 \SystemRoot\System32\Config\SAM Disabled
```

Figura 6:

Se ha encontrado la llave del registro SAM. **¿Será posible listar los usuarios con los valores de este registro?** Con el valor *offset* de memoria virtual, es decir con la dirección de memoria donde esta alojada la SAM, liste sus llaves y valores de manera recursiva y filtre la palabra *Users* con la herramienta *grep*

```
python3 vol.py -f /home/kali/Escritorio/memdump.mem/memdump.mem
windows.registry.printkey
--offset 0xf8a00421e010
--key SAM
--recurse
| grep "Users"
```

, donde el argumento *windows.registry.printkey* lista los valores de la llave de registro, *--offset* recibe como argumento el valor de la memoria virtual donde se encuentra el registro SAM, la opción *-key* recibe como argumento el nombre de la llave, *-recurse* realiza una búsqueda recursiva de valores en la SAM y *grep "User"* filtra la palabra deseada. Localice a los tres usuarios que residen en ese sistema operativo. Si la SAM permite almacenar en memoria RAM las credenciales de acceso **¿Podrán exportarse en texto plano sus contraseñas?**

```
*** 2021-04-11 03:00:03.000000 0xf8a004011010 Key \SystemRoot\System32\Config\SAM\SAM\Domains\Account\Users\Names\Administrator (Default) ** False
*** 2021-04-11 02:59:49.000000 0xf8a004011010 REG_UNKNOWN \SystemRoot\System32\Config\SAM\SAM\Domains\Account\Users\Names\Administrator
*** 2021-04-11 03:00:03.000000 0xf8a004011010 Key \SystemRoot\System32\Config\SAM\SAM\Domains\Account\Users\Names\Guest (Default) ** False
*** 2021-04-11 02:59:49.000000 0xf8a004011010 REG_UNKNOWN \SystemRoot\System32\Config\SAM\SAM\Domains\Account\Users\Names\Guest
*** 2021-04-11 03:00:03.000000 0xf8a004011010 Key \SystemRoot\System32\Config\SAM\SAM\Domains\Account\Users\Names\pruebas (Default) ** False
*** 2021-04-11 03:00:03.000000 0xf8a004011010 REG_UNKNOWN \SystemRoot\System32\Config\SAM\SAM\Domains\Account\Users\Names\pruebas
*** 2021-04-11 03:00:03.000000 0xf8a004011010 REG_NONE \SystemRoot\System32\Config\SAM\SAM\Domains\Account\Users\Names\pruebas (Default) ** False
*** 2021-04-11 03:00:03.000000 0xf8a004011010 REG_BINARY \SystemRoot\System32\Config\SAM\SAM\Domains\Account\Users\Names\pruebas (Default) ** False
```

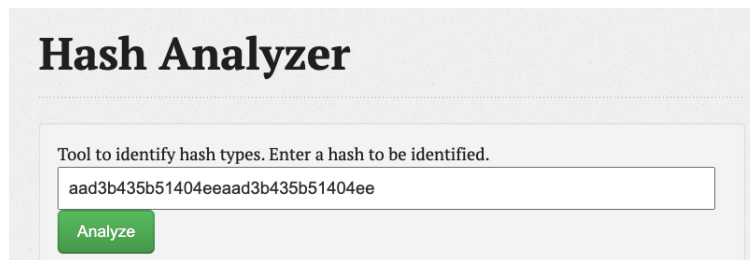
Figura 7:

- La SAM es conocida por almacenar contraseñas mediante un *hash* codificado con el algoritmo md5, para versiones de Windows 7 ≤. Utilice el comando *windows.hashdump* para recuperar los *hashes* de las contraseñas. Puede consultar el tipo de *hash* en la herramienta [Hash Analyzer](#)

```
python3 vol.py -f /home/kali/Escritorio/memdump.mem  
windows.hashdump
```

```
Administrator 500 aad3b435b51404eeaad3b435b51404ee 10eca58175d4228eco1516787086e824  
Guest 501 aad3b435b51404eeaad3b435b51404ee 31d6cfe0d1eae931b73c59d7e0c089c0  
pruebas 1000 aad3b435b51404eeaad3b435b51404ee 32ed87bdb5fdc5e9cba88547376818d4
```

Figura 8:

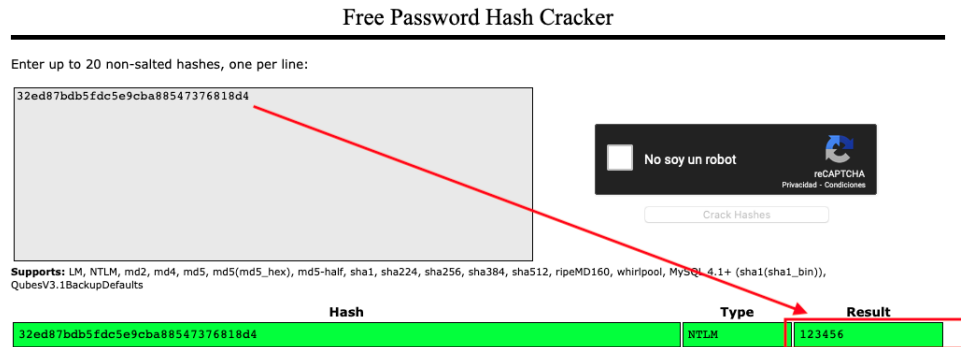


Hash Analyzer

Tool to identify hash types. Enter a hash to be identified.

Figura 9:

Extraiga en texto plano el *hash* del usuario pruebas. Apóyese de la herramienta de fuerza bruta [CrackStation](#). Observe los resultados (la bandera es la contraseña en texto plano).



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
32ed87bdb5fdc5e9cba88547376818d4	NTLM	123456

Figura 10:

1.3. Laboratorio 4C

6. El volcado de memoria al ser una adquisición forense en tiempo real, guarda la información, archivos y datos de los procesos mientras eran ejecutados por el usuario. **¿Se podrán obtener los archivos que estaba modificando el usuario?** Utilice el argumento `windows.filescan` y observe si existe algún archivo en formato `txt` utilizado por el usuario `pruebas`

```
python3 vol.py -f /home/kali/Escritorio/memdump.mem  
windows.filescan  
| grep pruebas  
| grep txt
```

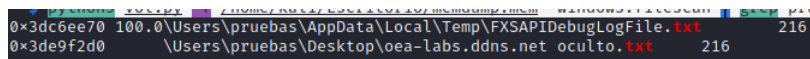


Figura 11:

Observe el nombre del archivo e ingrese a <http://oea-labs.ddns.net/oculto/> para recuperar la bandera.

1.4. Laboratorio 4D

7. Observe el proceso con PID 228 que ejecuta **Microsoft Paint** (`mspaint.exe`). **¿Se podrá visualizar el contenido que fue capturado en tiempo real de un editor de dibujo?** Extraiga los datos del volcado del proceso con el argumento `windows.memmap`.

```
python3 vol.py -f /home/kali/Escritorio/memdump.mem  
windows.memmap  
--pid 2288  
--dump
```

, donde el argumento `-pid` indica el número del PID del proceso y `-dump` que se genere un archivo de volcado del proceso

El proceso puede tardar unos minutos. Identifique el archivo con extensión `dmp`. Renómbralo con extensión `data`

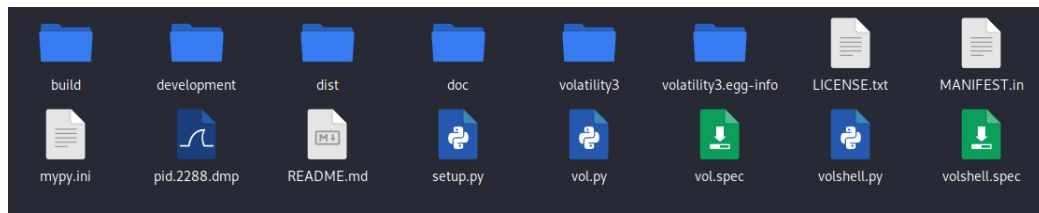


Figura 12:

Instale la herramienta de edición de imágenes `gimp`. Si está en el sistema operativo Kali Linux:

```
$ sudo apt-get install gimp
```

Si está en el S.O. Windows descargue el paquete de instalación desde <https://www.gimp.org/downloads/>

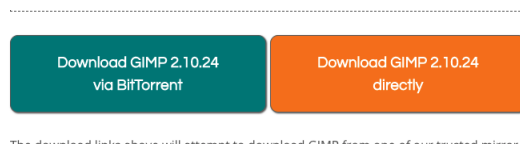


Figura 13:

8. Abra el editor de imágenes `gimp` y arrastre el volcado del proceso. Ajuste los filtros de Desplazamiento a 186323227, de Anchura a 819 y de Altura a 937. Despliegue el contenido del filtro

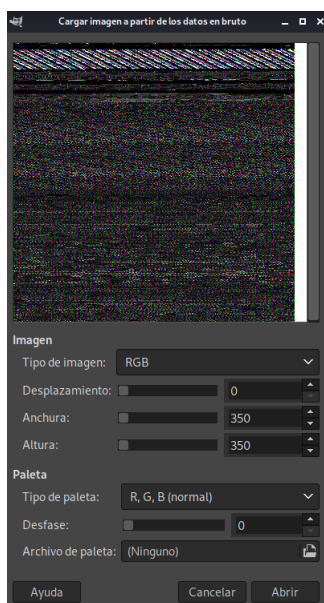


Figura 14:



Figura 15: