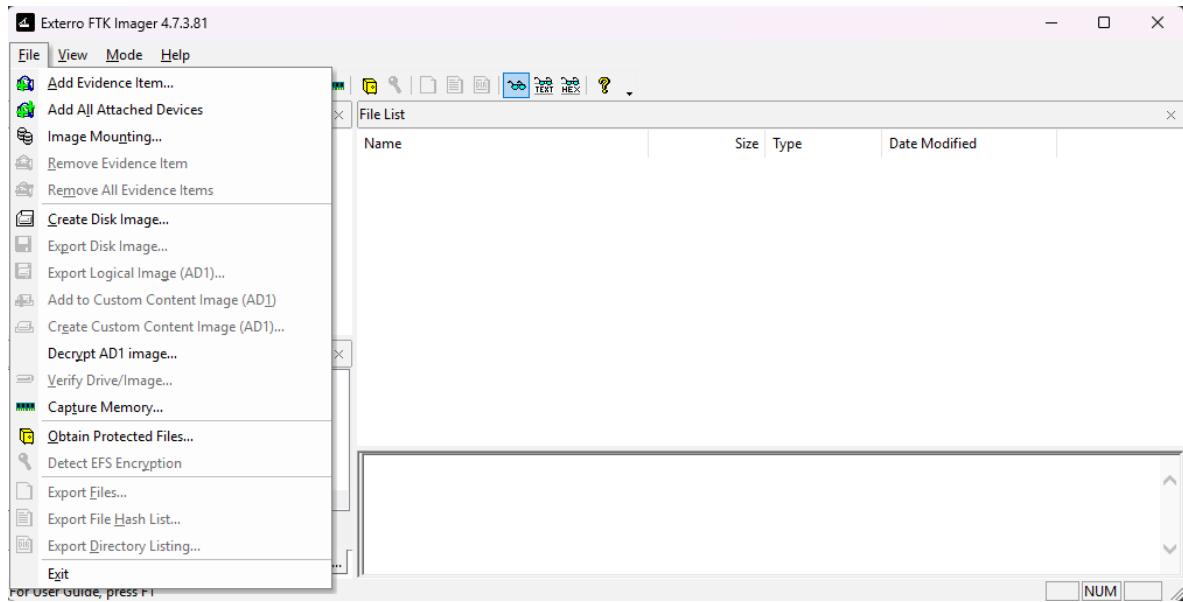
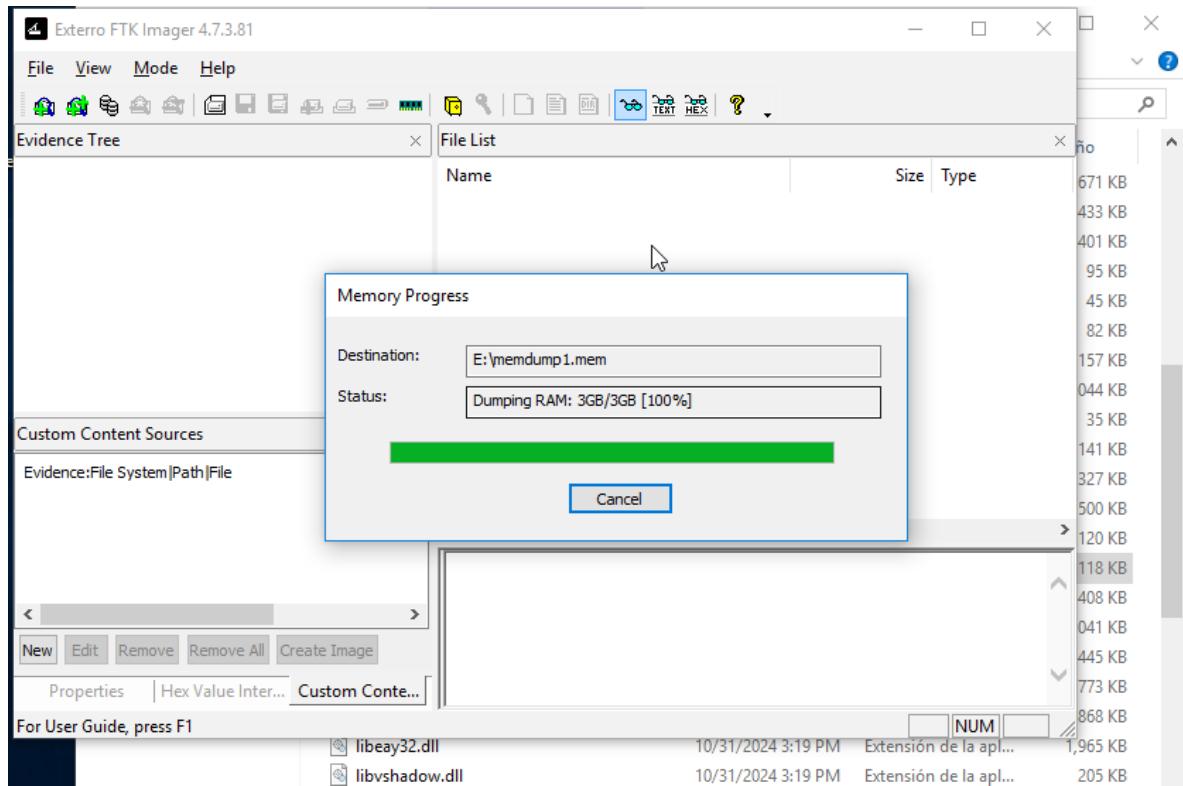


Volcado de memoria con volatility3

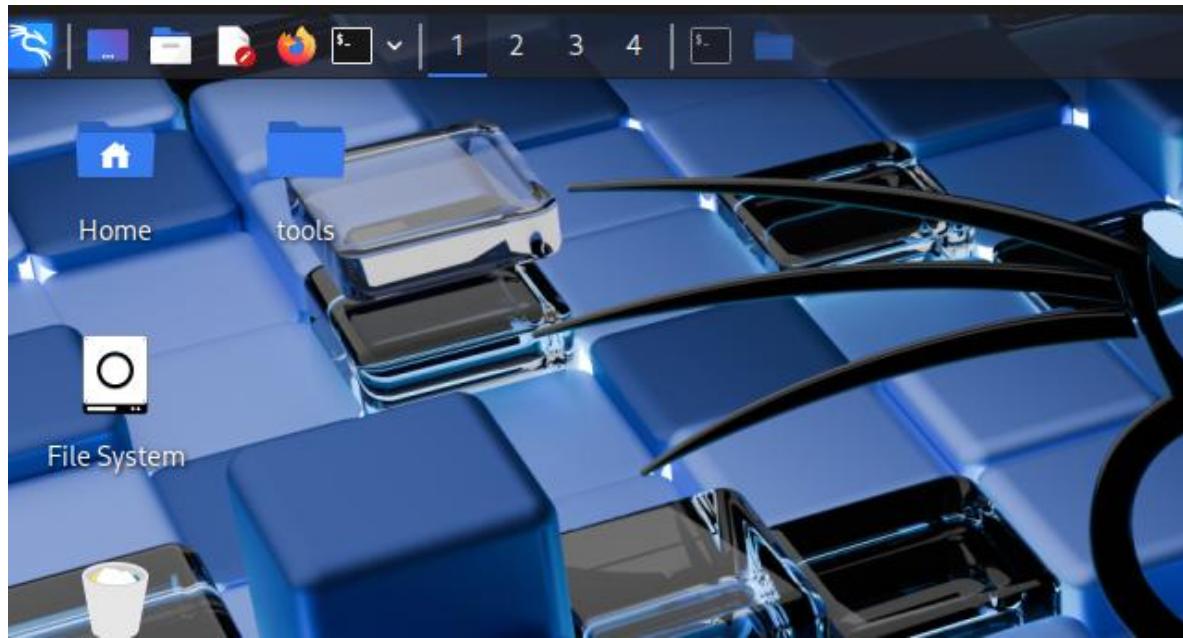
Paso 1: Ejecutamos el programa FKT Imager y Capturamos la memoria



Paso 2: Configuramos la captura de memoria

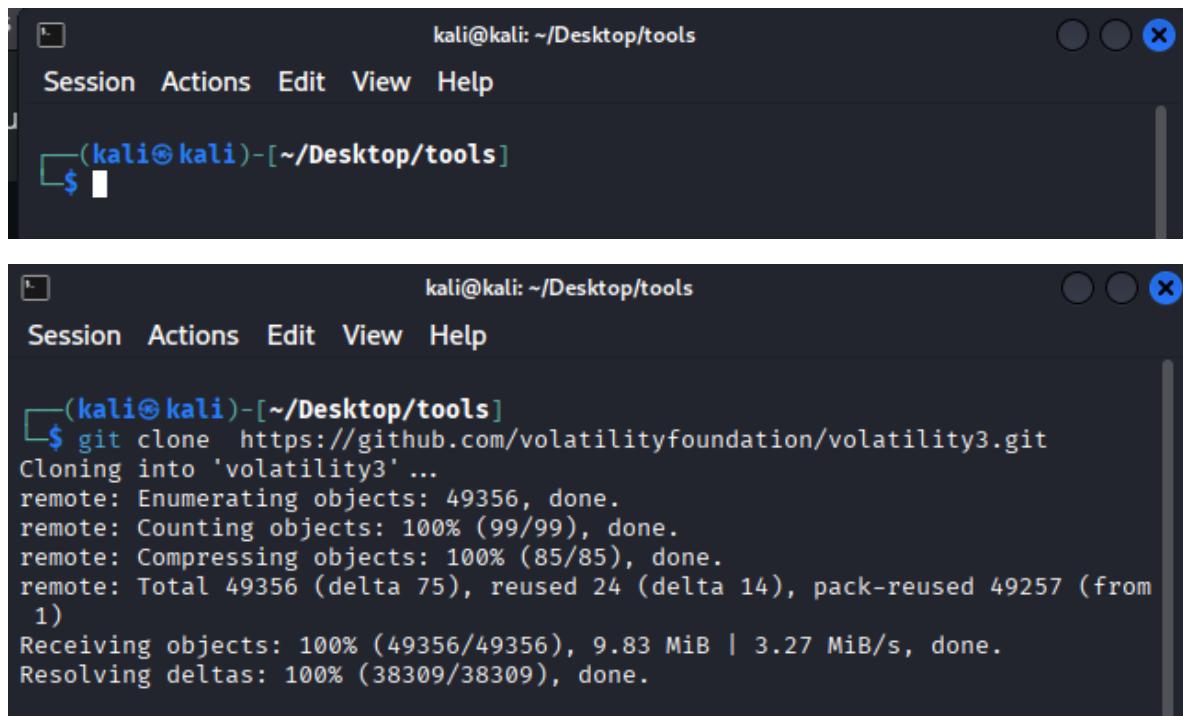


Paso 3: creamos una carpeta tools



Paso 4: Descargamos volatility 3 y clonamos el repositorio de volatility en la carpeta tools

```
git clone https://github.com/volatilityfoundation/volatility3.git
```



```
kali@kali: ~/Desktop/tools
Session Actions Edit View Help
(kali㉿kali)-[~/Desktop/tools]
$ git clone https://github.com/volatilityfoundation/volatility3.git
Cloning into 'volatility3' ...
remote: Enumerating objects: 49356, done.
remote: Counting objects: 100% (99/99), done.
remote: Compressing objects: 100% (85/85), done.
remote: Total 49356 (delta 75), reused 24 (delta 14), pack-reused 49257 (from 1)
Receiving objects: 100% (49356/49356), 9.83 MiB | 3.27 MiB/s, done.
Resolving deltas: 100% (38309/38309), done.
```

Paso 5: verificamos la versión de Python

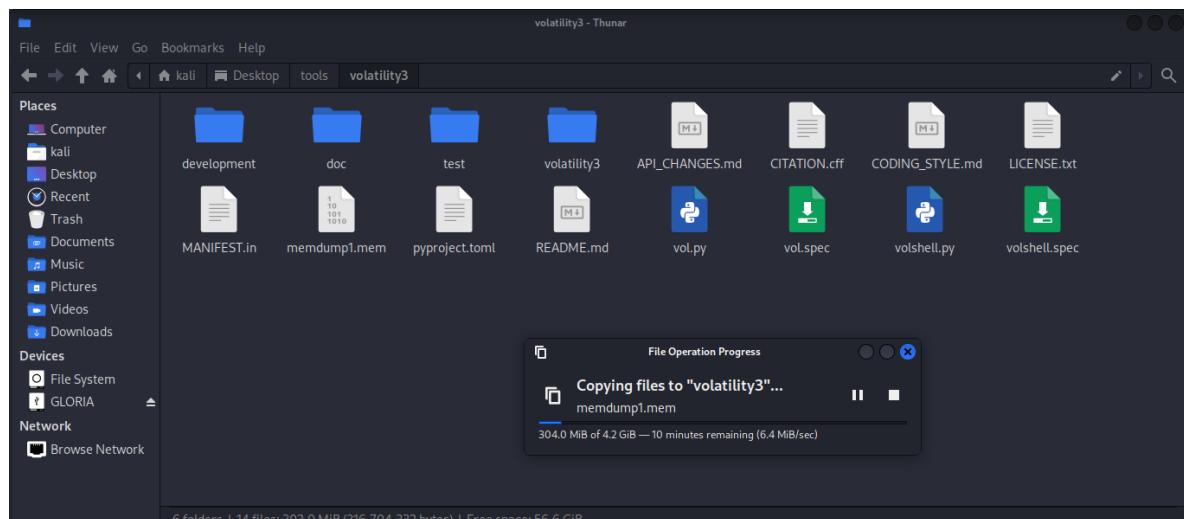
```
python3 –versión
```

```
(kali㉿kali)-[~/Desktop/tools/volatility3]
$ python --version
Python 3.13.7
```

Paso 6: instalamos plugin pendientes

```
(kali㉿kali)-[~/Desktop/tools/volatility3]
$ pip install --user -e ".[full]"
```

Paso 7: copiamos las imágenes que hicimos en la memoria dentro de la carpeta de tools



Paso 8: obtenemos el sh256 de la imagen

```
(kali㉿kali)-[~/Desktop/tools/volatility3]
$ sha256sum memdump1.mem
ec15ada1bc8a50789b07517c5138404215bf93ae3febe6a3e6ceae08661f6795  memdump1.me
m
```

Paso 9: hacemos el proceso de clonado de Windows moviéndonos hasta la carpeta symbols

```
(kali㉿kali)-[~/Tools/volatility3/volatility3/symbols]
$ wget https://downloads.volatilityfoundation.org/volatility
3/symbols/windows.zip
```

Paso 10: obtener la información de la imagen

```
(kali㉿kali)-[~/Desktop/tools/volatility3]
$ python3 vol.py -f memdump1.mem windows.info.Info
```

```
kali@kali: ~/Desktop/tools/volatility3
Session Actions Edit View Help
Volatility 3 Framework 2.27.0
Progress: 100.00          PDB scanning finished
Variable      Value
Kernel Base      0xf803d581e000
DTB      0x1aa000
Symbols jar:file:/home/kali/Desktop/tools/volatility3/volatility3/symbols/windows.zip!windows!ntkrnlmp.pdb/F7971FB6AA7E450C98D65942-1.json.xz
Is64Bit True
IsPAE  False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf803d5ae2dc0
Major/Minor     15.10586
MachineType    34404
KeNumberProcessors 1
SystemTime      2025-12-01 04:14:34+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNT
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine      34404
PE TimeStamp     Wed Feb 24 05:48:00 2016
(kali㉿kali)-[~/Desktop/tools/volatility3]
$
```

Paso 11: obtenemos todos los procesos que se estaba ejecutando

```
(kali㉿kali)-[~/Desktop/tools/volatility3]
$ python3 vol.py -f memdump1.mem windows.pslist.PsList
```

Session Actions Edit View Help								
3340	820	taskhostw.exe	0xe0003f897340	8	-	1	False	
2025-12-01	03:59:47.000000	UTC	N/A	Disabled				
3748	568	dllhost.exe	0xe000414b57c0	7	-	1	False	
2025-12-01	04:00:15.000000	UTC	N/A	Disabled				
3108	480	NisSrv.exe	0xe00040f1a7c0	6	-	0	False	
2025-12-01	04:00:34.000000	UTC	N/A	Disabled				
3496	248	smss.exe	0xe000415217c0	0	-	2	False	
2025-12-01	04:00:46.000000	UTC	2025-12-01 04:00:46.000000	UTC	Disabled			
3672	3496	csrss.exe	0xe0004152f080	12	-	2	False	
2025-12-01	04:00:46.000000	UTC	N/A	Disabled				
3260	3496	winlogon.exe	0xe0003f0ac7c0	6	-	2	False	
2025-12-01	04:00:46.000000	UTC	N/A	Disabled				
4044	3260	dwm.exe	0xe000412a47c0	12	-	2	False	2025-
12-01	04:00:46.000000	UTC	N/A	Disabled				
3564	1704	OneDrive.exe	0xe000413c77c0	21	-	1	True2	
025-12-01	04:00:47.000000	UTC	N/A	Disabled				
4700	820	sihost.exe	0xe0004056d7c0	14	-	2	False	
2025-12-01	04:01:01.000000	UTC	N/A	Disabled				
4728	820	taskhostw.exe	0xe0003f8b57c0	11	-	2	False	
2025-12-01	04:01:02.000000	UTC	N/A	Disabled				
4736	820	MicrosoftEdgeU	0xe000405a97c0	6	-	0	True2	
025-12-01	04:01:02.000000	UTC	N/A	Disabled				
4912	568	RuntimeBroker.	0xe0003e65c080	13	-	2	False	
2025-12-01	04:01:05.000000	UTC	N/A	Disabled				
5008	3260	userinit.exe	0xe0003f7387c0	0	-	2	False	
2025-12-01	04:01:06.000000	UTC	2025-12-01 04:01:32.000000	UTC	Disabled			
5052	5008	explorer.exe	0xe0003f9c67c0	57	-	2	False	
2025-12-01	04:01:07.000000	UTC	N/A	Disabled				

Paso 12: Conocer los hashes de la contraseña de Windows

```
(kali㉿kali)-[~/Desktop/tools/volatility3]
$ python3 vol.py -f memdump1.mem windows.hashdump.Hashdump
```

```
(venv)kali㉿kali: ~/Desktop/tools/volatility3
Session Actions Edit View Help
/home/kali/Desktop/tools/volatility3/volatility3/framework/deprecation.py:28:
  FutureWarning: This API (volatility3.plugins.windows.registry.hashdump.Hashdump.run) will be removed in the first release after 2026-09-25. This plugin has been renamed, please call volatility3.plugins.windows.registry.hashdump.Hashdump rather than volatility3.plugins.windows.hashdump.Hashdump.
  warnings.warn(
User      rid      lmhash      nthash
/home/kali/Desktop/tools/volatility3/volatility3/framework/deprecation.py:105
: FutureWarning: This plugin (volatility3.plugins.windows.hashdump.Hashdump) has been renamed and will be removed in the first release after 2026-09-25. Please ensure all method calls to this plugin are replaced with calls to volatility3.plugins.windows.registry.hashdump.Hashdump
  warnings.warn(
Administrador      500      aad3b435b51404eeaad3b435b51404ee      c8b73f1ce6137
29ad779aabc722fd575
Invitado      501      aad3b435b51404eeaad3b435b51404ee      31d6cf0d16ae
931b73c59d7e0c089c0
DefaultAccount      503      aad3b435b51404eeaad3b435b51404ee      31d6cf0d16ae
931b73c59d7e0c089c0
vboxuser      1000      aad3b435b51404eeaad3b435b51404ee      c8b73f1ce6137
29ad779aabc722fd575
itachi      1001      aad3b435b51404eeaad3b435b51404ee      209c6174da490caeb422f
3fa5a7ae634
(venv)–(kali㉿kali)–[~/Desktop/tools/volatility3]
```

Paso 13: desciframos la contraseña usando los hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
aad3b435b51404eeaad3b435b51404ee	LM	
209c6174da490caeb422f3fa5a7ae634	NTLM	admin

Color Codes: Green Exact match, Yellow Partial match, Red Not found.