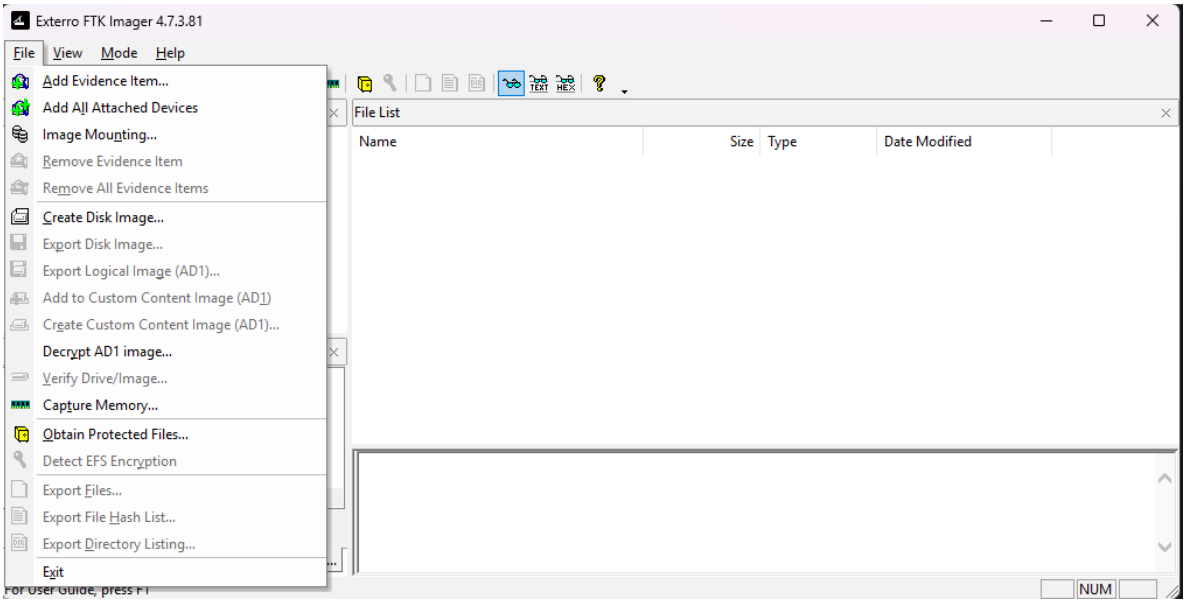
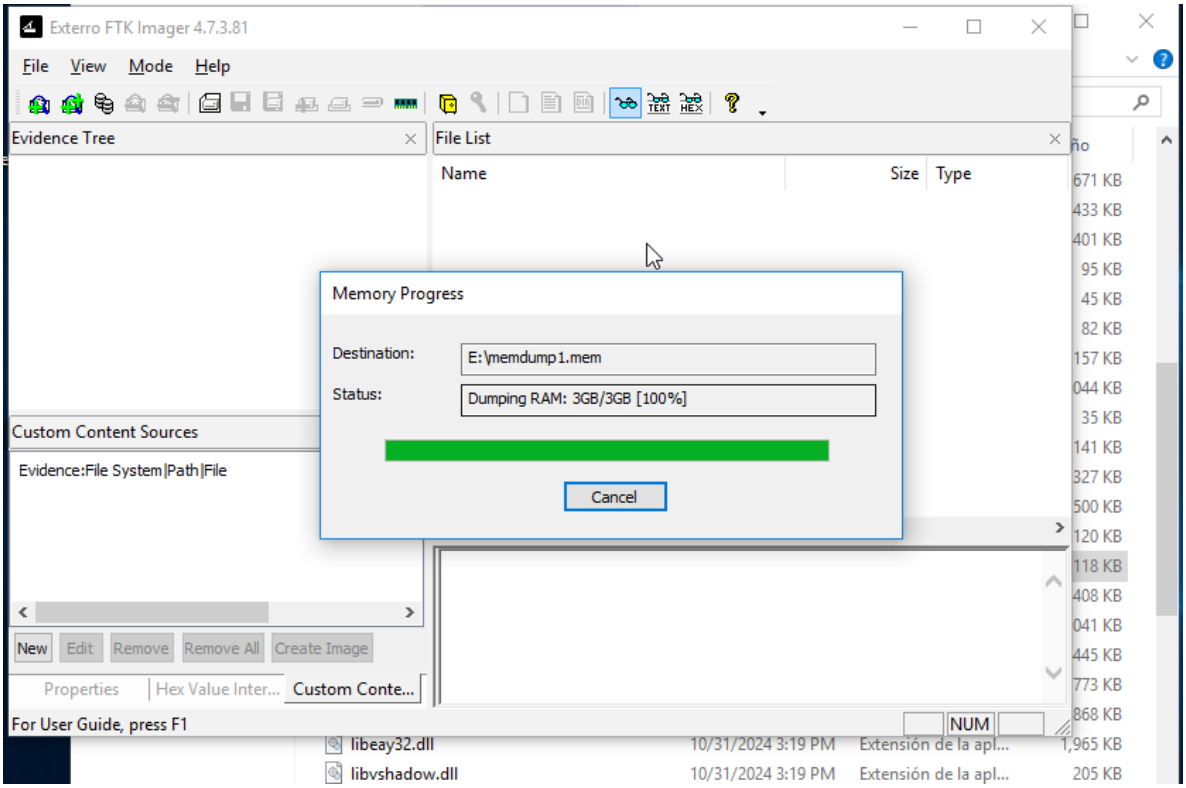
Volcado de memoria con volatility3

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



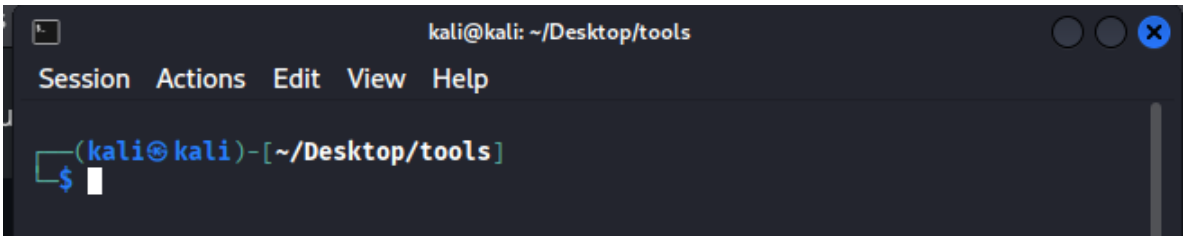
Paso 2: Configuramos la captura de memoria

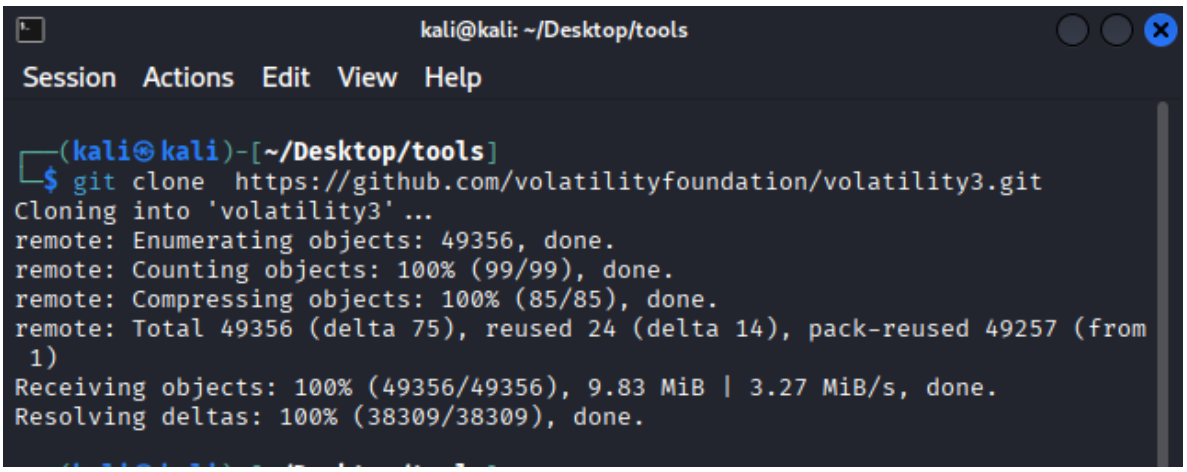


Paso 3: creamos una carpeta tools

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

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





Paso 5: verificamos la versión de Python

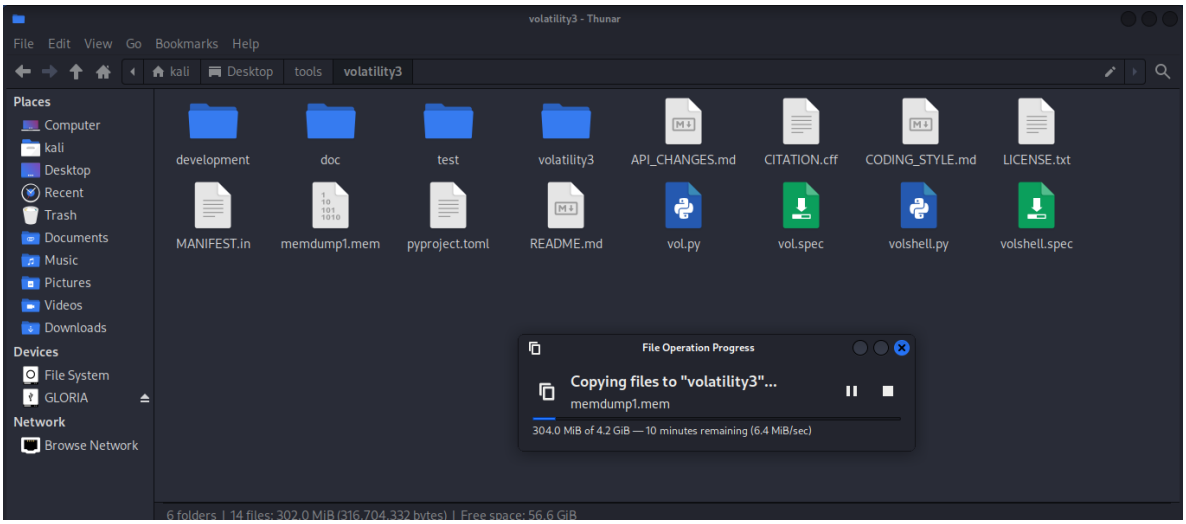
python3 –versión

```
┌──(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

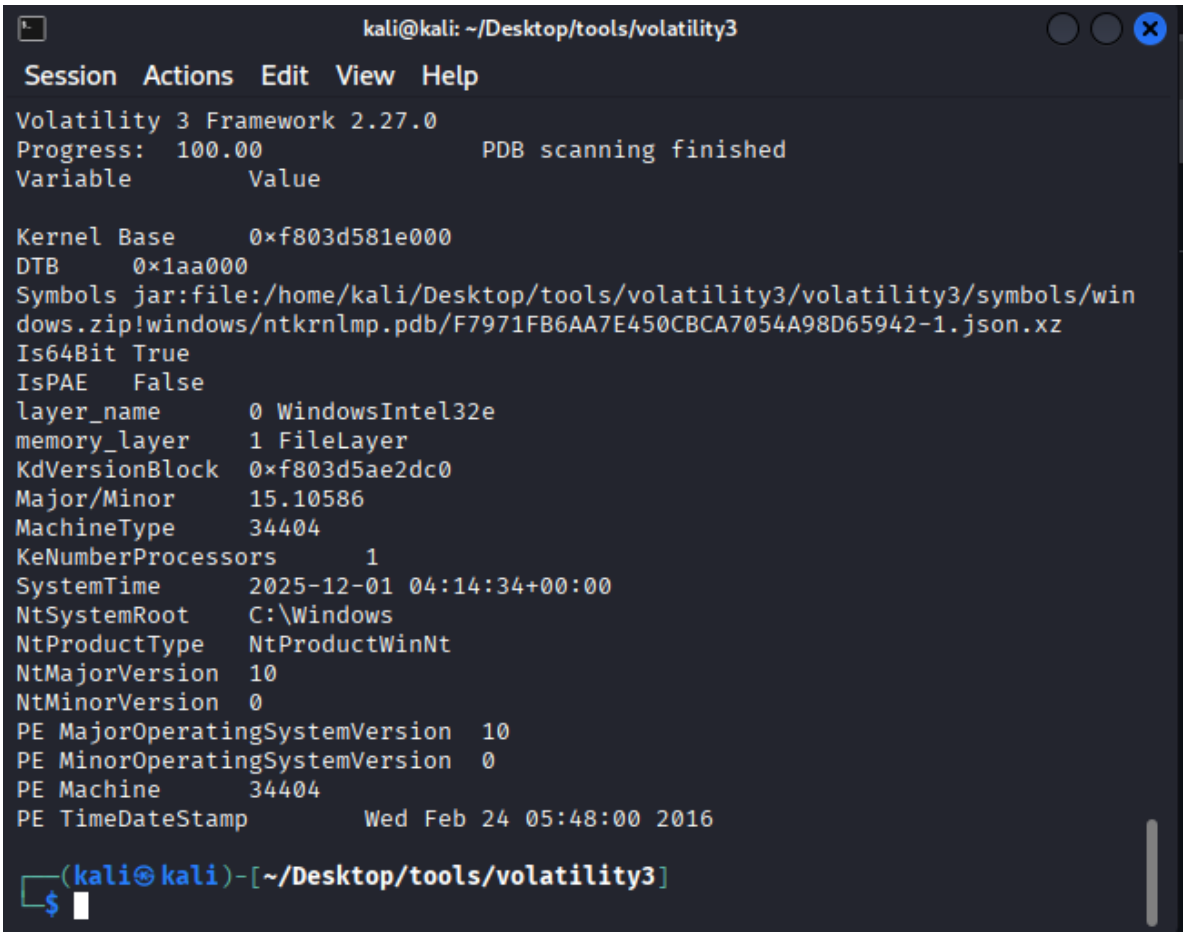
```
┌──(kali㉿kali)-[~/Desktop/tools/volatility3]
└─$ sha256sum memdump1.mem
ec15ada1bc8a50789b07517c5138404215bf93ae3febe6a3e6ceae08661f6795  memdump1.me
m
```

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

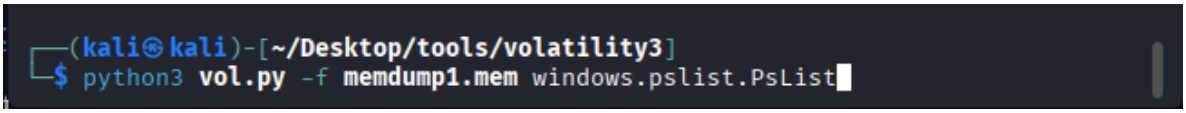
```
┌──(kali㉿kali)-[~/…/Tools/volatility3/volatility3/symbols]
└─$ wget https://downloads.volatilityfoundation.org/volatility
3/symbols/windows.zip
```

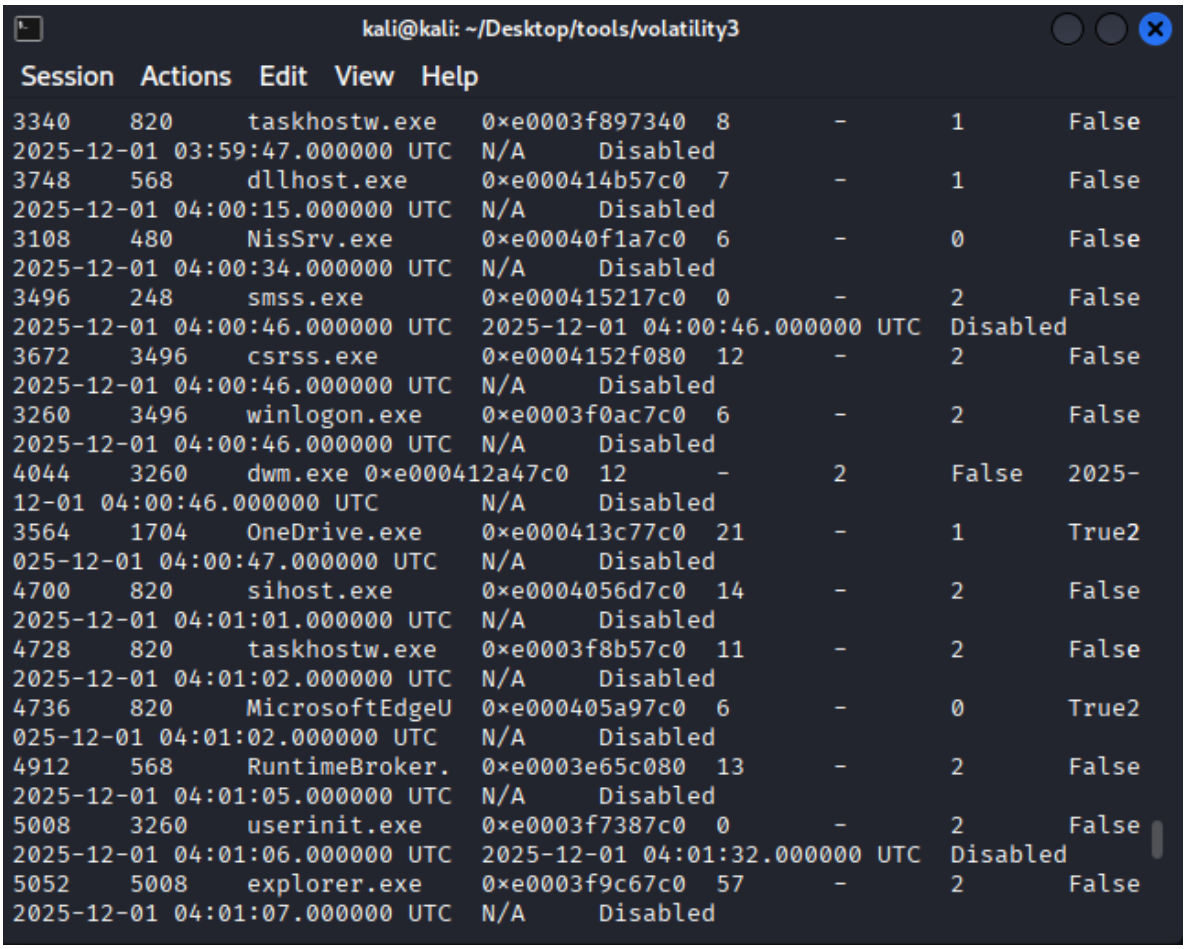
Paso 10: obtener la información de la imagen

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

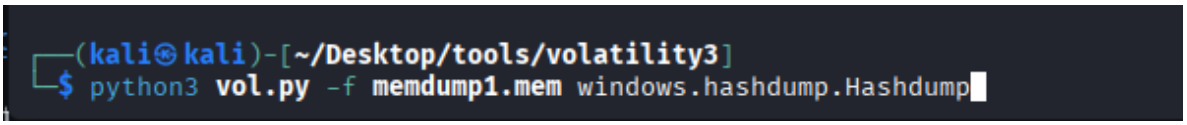


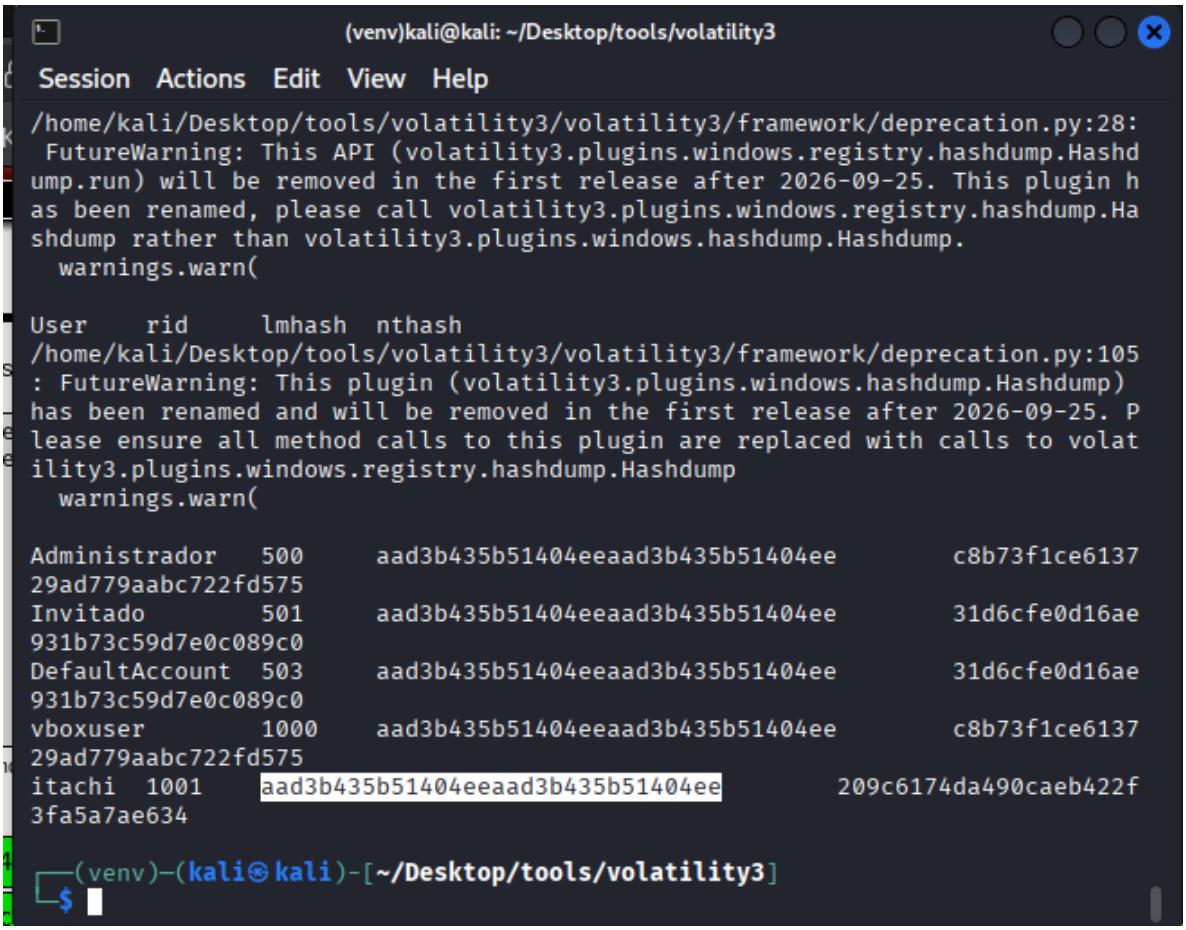
Paso 11: obtenemos todos los procesos que se estaba ejecutando





Paso 12: Conocer los hashes de la contraseña de Windows





Paso 13: desciframos la contraseña usando los hashes