1 ASIX

**MÒDUL 16: CIBERSEGURETAT I HACKING ÈTIC**

ACTIVITAT 3: Anàlisi Forense

línea horizontal

# 



**Alumne**: Daniel Mascarilla del Olmo

**Professor**: Sergi Andrés

**Curs**: 1 ASIX

**Centre**: Jaume Viladoms

**ÍNDEX**

[**Exercici 1 – Imatge forense d’un disc des de Windows 3**](#_kc11eg7rqqxv)

[a. Connecta un pendrive i copia-hi unes quantes imatges de diferents formats (jpg, png...) i algun fitxer PDF. 3](#_7mc6cwownb1a)

[b. Esborra del pendrive les dades que has copiat en l’apartat anterior. 3](#_4703ku2ksl1i)

[c. Fes una còpia bit a bit (clonació/copia forense) del pendrive 4](#_8ssj3q63gn5r)

[d. Mostra quin és el Hash de la còpia creada (recorda que pot ser SHA1, SHA2, MD5...). 9](#_8pr54f6i1c75)

[**Exercici 2 – Recuperar dades esborrades des de Linux 11**](#_3fgyjagblytw)

[a. Des de Linux agafa la còpia forense del Pendrive 11](#_37ugbp7m3puh)

[b. Dins de Kali ves a l’apartat de les Eines Forenses (Forensics) → I tria el programa à Scalpel 11](#_se0lewspvtud)

[c. Recupera els fitxers esborrats (recorda que dins la carpeta /etc/scalpel/scalpel.conf hi ha definits els formats dels fitxers que Scalpel sap recuperar) descomenta tots aquells formats que vols trobar. Executa la següent comanda per a recuperar-los: scalpel -c /etc/scalpel/scalpel.conf -o /root/Desktop/rec /ruta/copiaForense.raw 12](#_g0ccmthd2sdd)

[d. Comprova que el programa ha pogut recuperar els fitxers anteriors... i segurament altres fitxers què havies esborrat anteriorment del pendrive. 14](#_b805wbm68i1e)

[**Exercici 3 – Imatge forense des de Linux 15**](#_c7eh45gpjtvp)

[a. Utilitza la eina GuyImager per a fer una còpia bit a bit d’un disc des de Kali Linux (pots fer-ho amb un pendrive o amb un disc dur petit que hagis afegit a Kali). 15](#_ikvaeqz0cr6n)

[b. Un cop tinguis la còpia feta, calcula el seu Hash amb l’eina → sha256sum 18](#_hvl3ssgzls81)

[**Exercici 4 – Volcar memòria RAM de sistema Windows 19**](#_eo7fyuh2nn6b)

[**Exercici 5 – Anàlisi de memòria RAM des de Kali Linux amb Volatility 21**](#_hdtezmep0038)

[a. Per a instal·lar Volatility: 21](#_ab42ttyl9td9)

[b. Per veure el perfil (o profile) de la teva RAM pots executar: 22](#_99mq2cit1iyv)

[c. Busca on apareix la connexió reversa què ha fet la teva màquina víctima cap a la màquina atacant a partir de la imatge de la RAM. 23](#_i5sl3647gsx3)

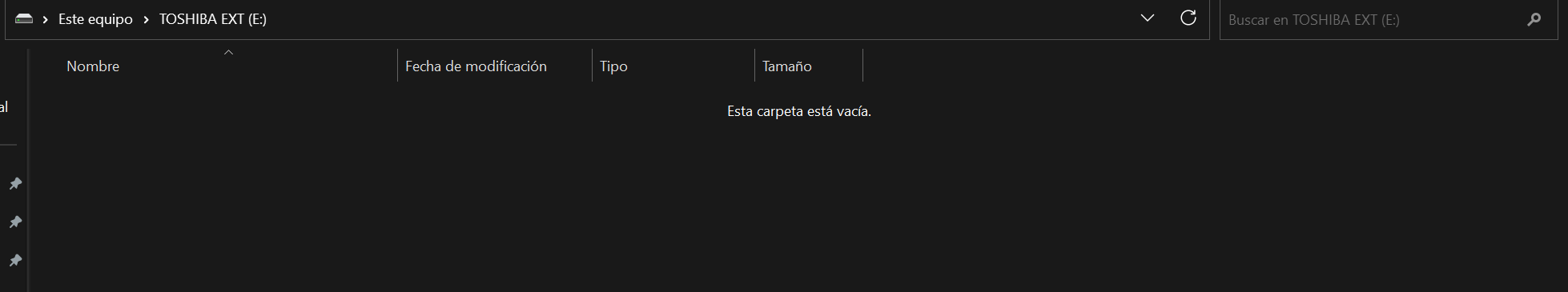
[d. Fes un volcat dels Hashes dels usuaris i passwords. 24](#_t1570ol5wp4b)

# Exercici 1 – Imatge forense d’un disc des de Windows

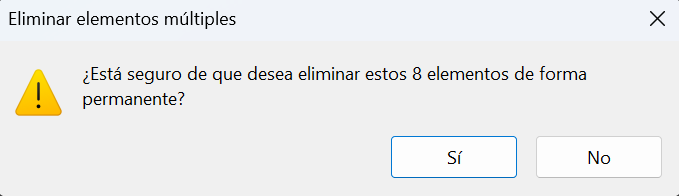
#### a. Connecta un pendrive i copia-hi unes quantes imatges de diferents formats (jpg, png...) i algun fitxer PDF.



#### b. Esborra del pendrive les dades que has copiat en l’apartat anterior.

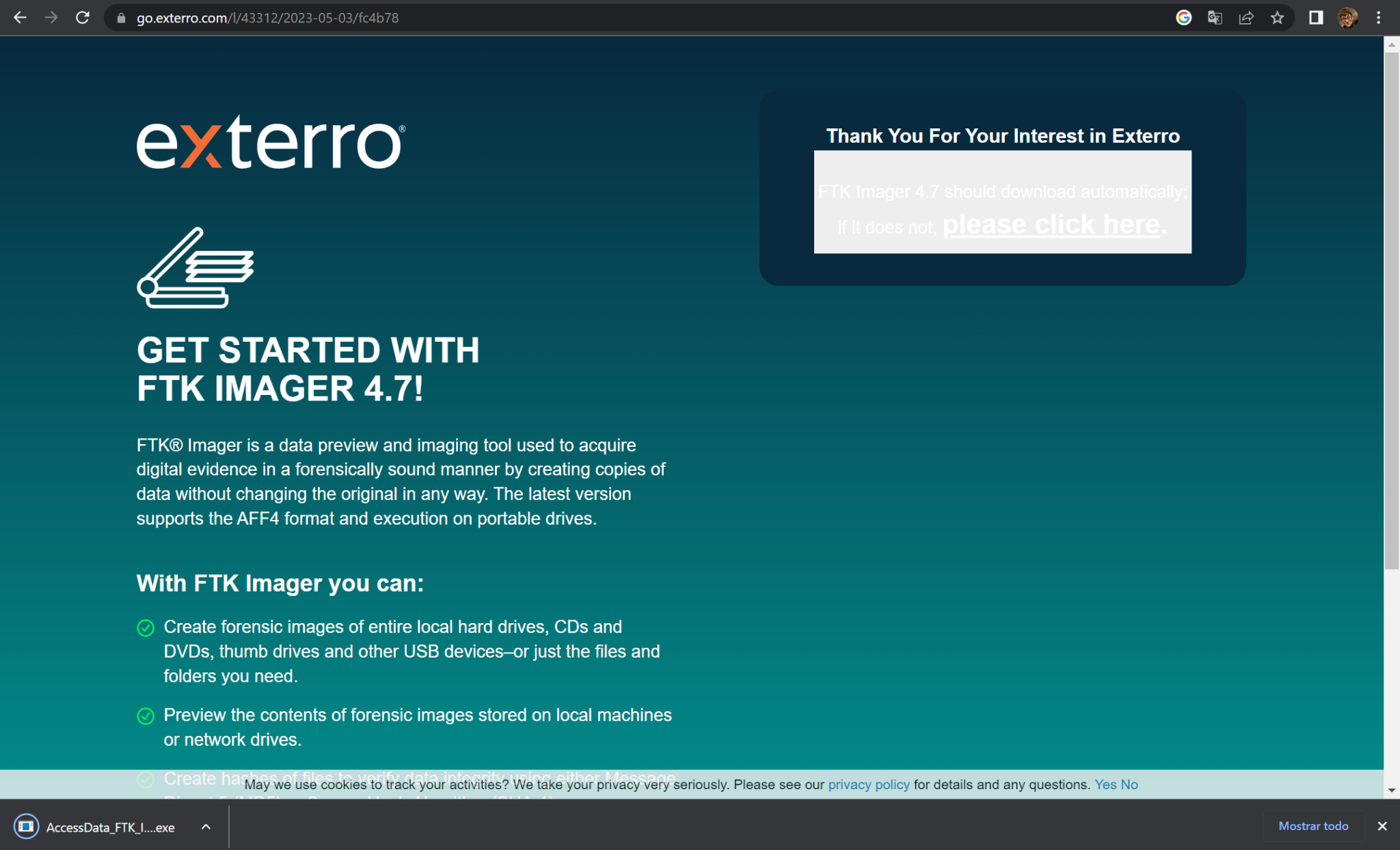


Vaciamos la papelera de reciclaje:

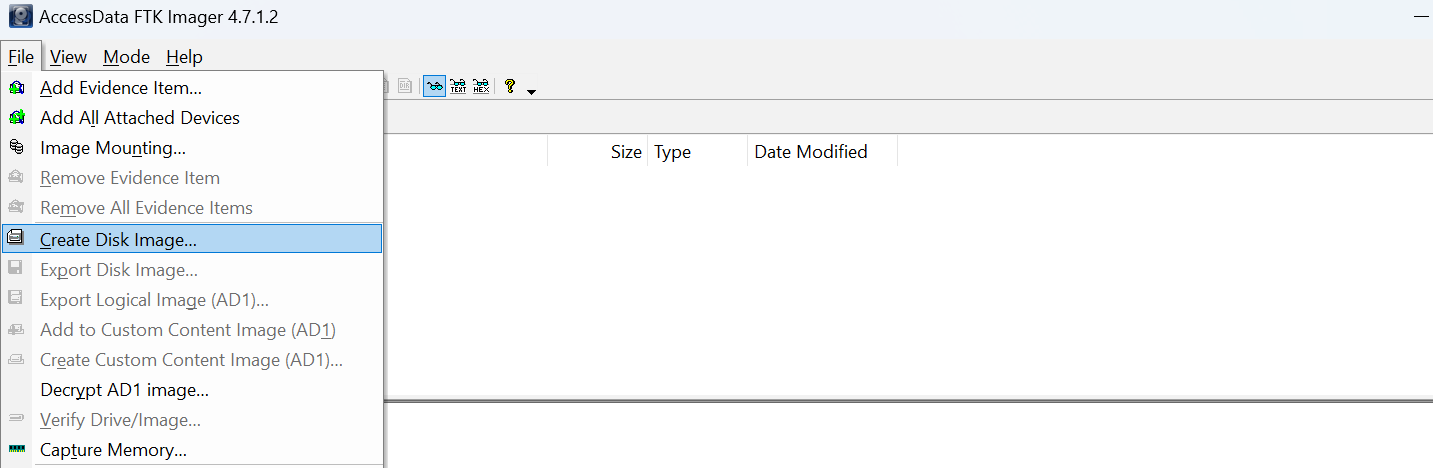


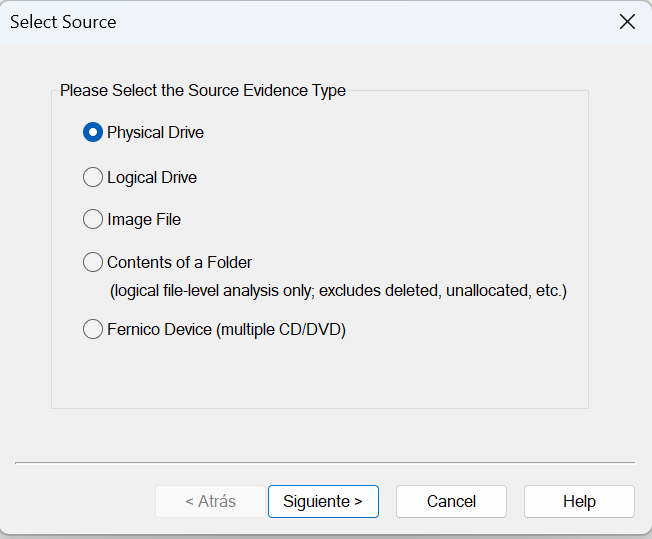
#### 

#### c. Fes una còpia bit a bit (clonació/copia forense) del pendrive

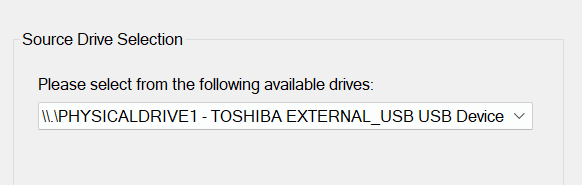


Una vez descargado, le daremos a File y Create Disk Image…

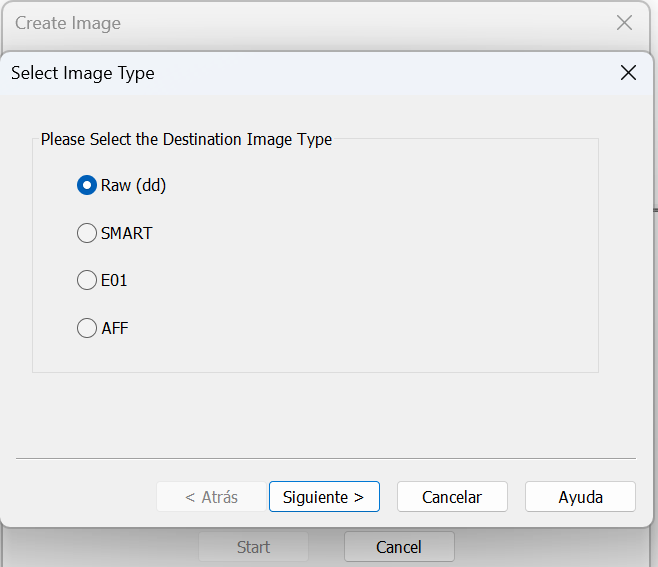


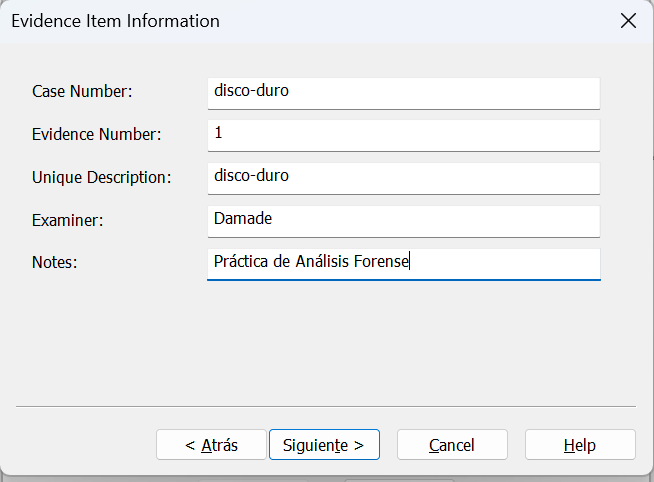


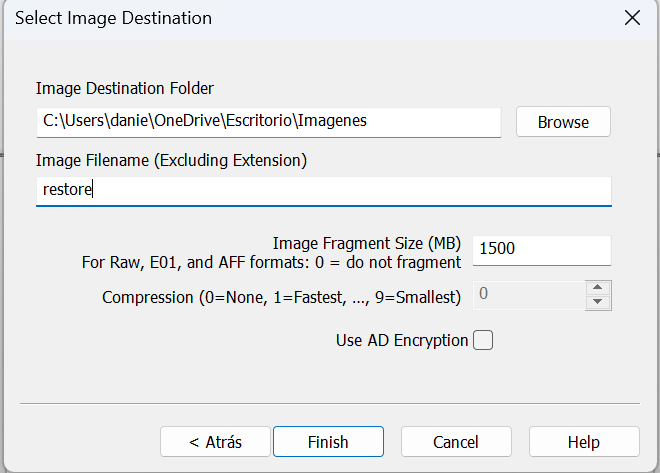
Seleccionamos el disco duro / pen drive:



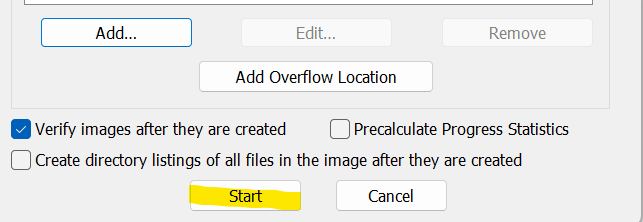
Le daremos clic a Add:



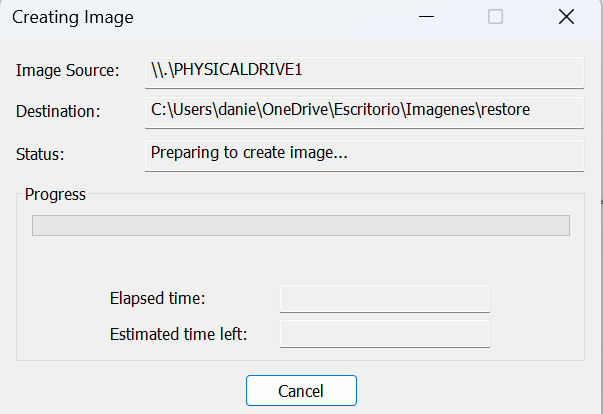




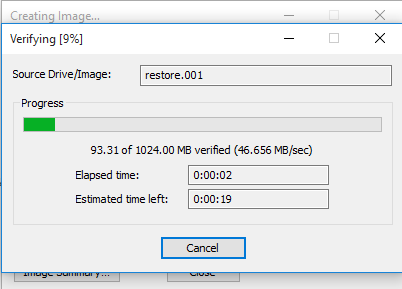
Le daremos a Finish:



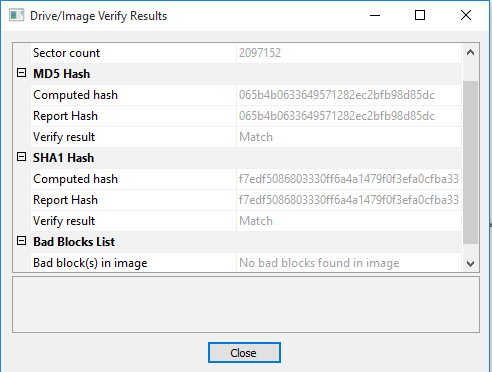
Y le daremos a start.



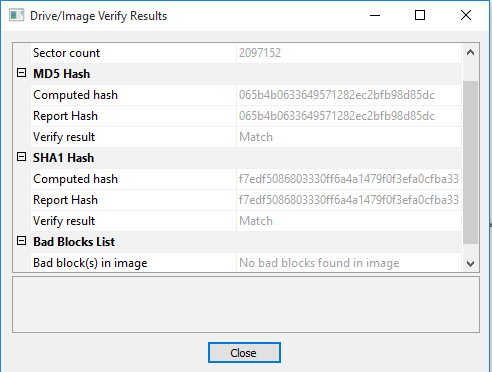
Empezará a crearmos la imagen.



(ATENCIÓN, he continuado haciéndolo en una máquina virtual porque en la máquina física me consumía todo el espacio que podía)

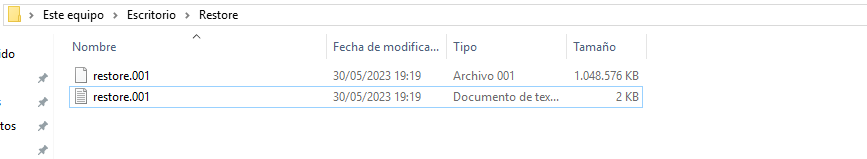


#### d. Mostra quin és el Hash de la còpia creada (recorda que pot ser SHA1, SHA2, MD5...).



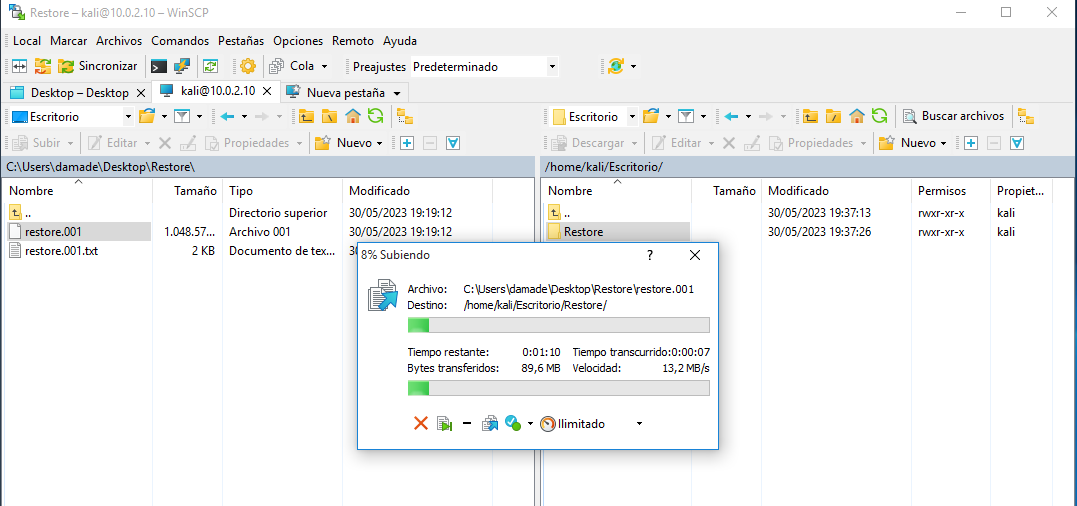
MD5: 065b4b0633649571282ec2bfb98d85dc

SHA1: f7edf5086803330ff6a4a1479f0f3efa0cfba33a

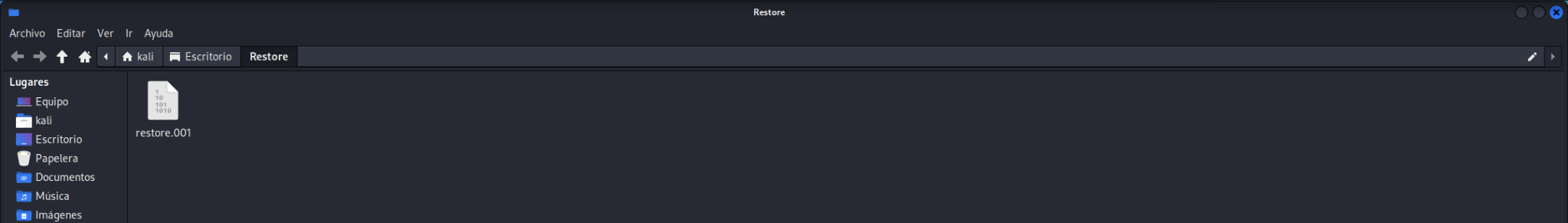


# Exercici 2 – Recuperar dades esborrades des de Linux

#### a. Des de Linux agafa la còpia forense del Pendrive

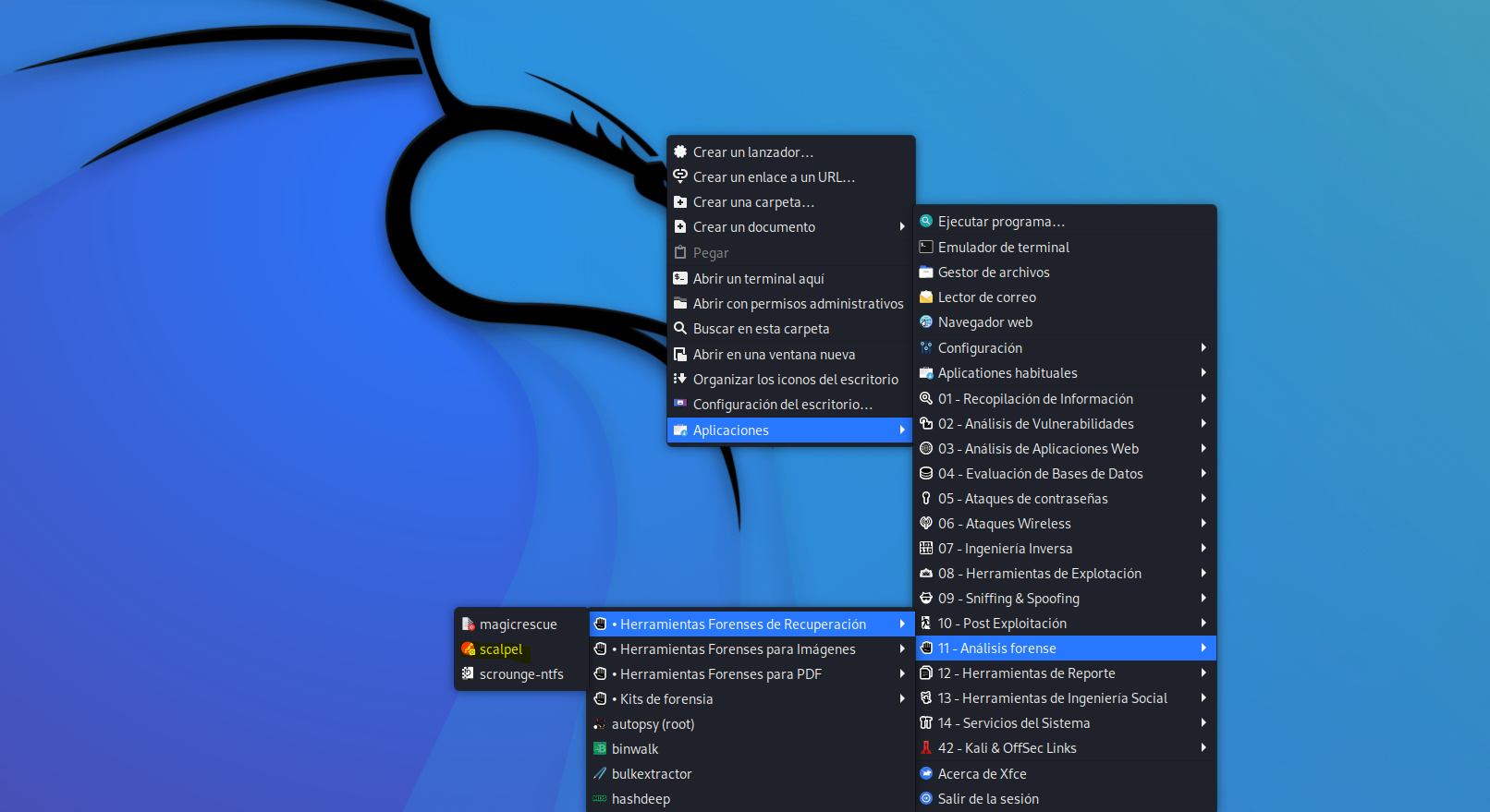


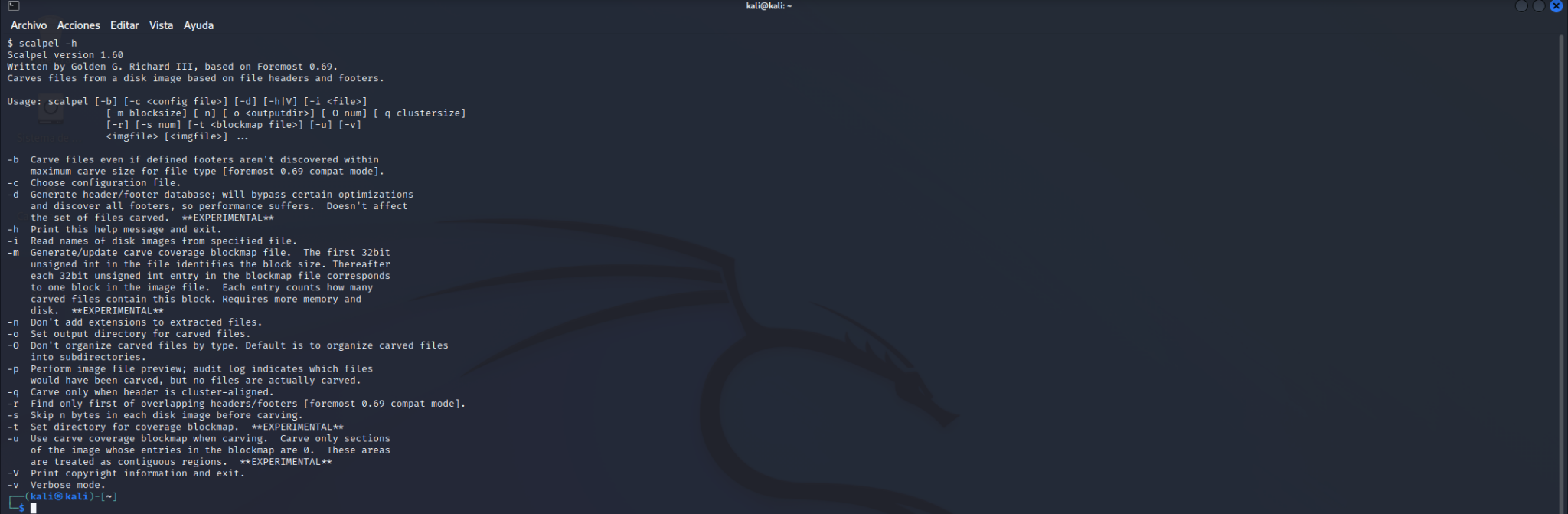
Pasamos el archivo mediante winscp.



#### b. Dins de Kali ves a l’apartat de les Eines Forenses (Forensics) → I tria el programa à Scalpel

Abrimos el scalpel:

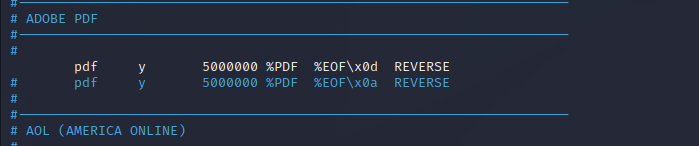


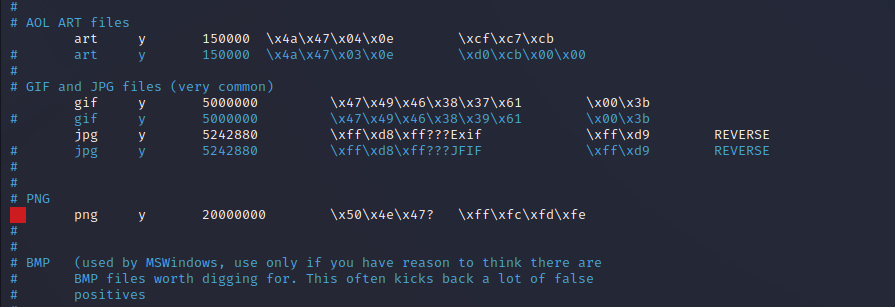


#### c. Recupera els fitxers esborrats (recorda que dins la carpeta /etc/scalpel/scalpel.conf hi ha definits els formats dels fitxers que Scalpel sap recuperar) descomenta tots aquells formats que vols trobar. Executa la següent comanda per a recuperar-los: scalpel -c /etc/scalpel/scalpel.conf -o /root/Desktop/rec /ruta/copiaForense.raw

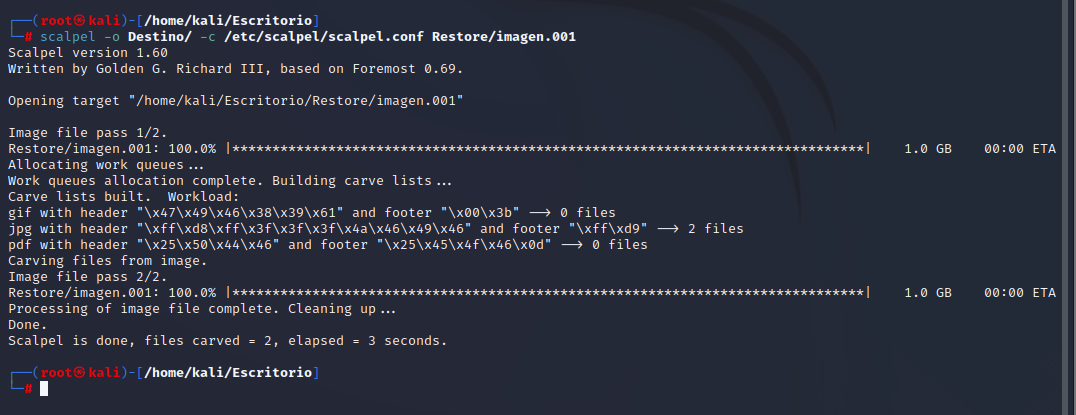
Modificamos el archivo scalpel.conf



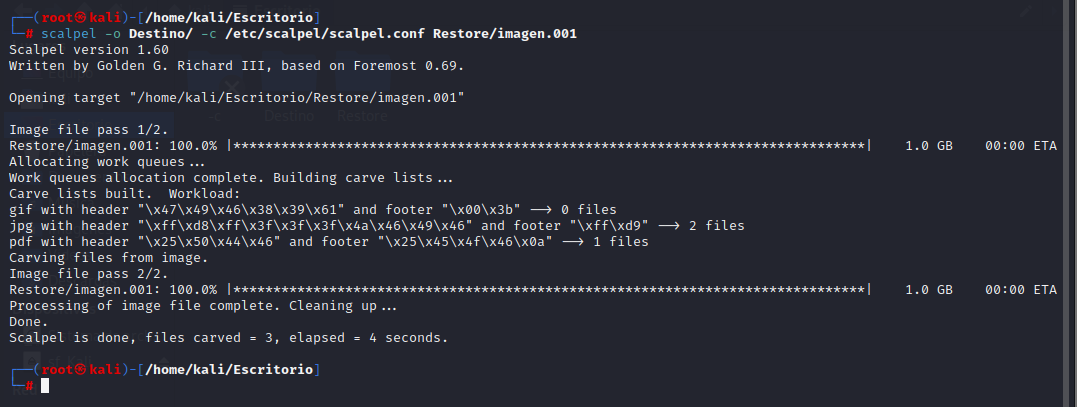




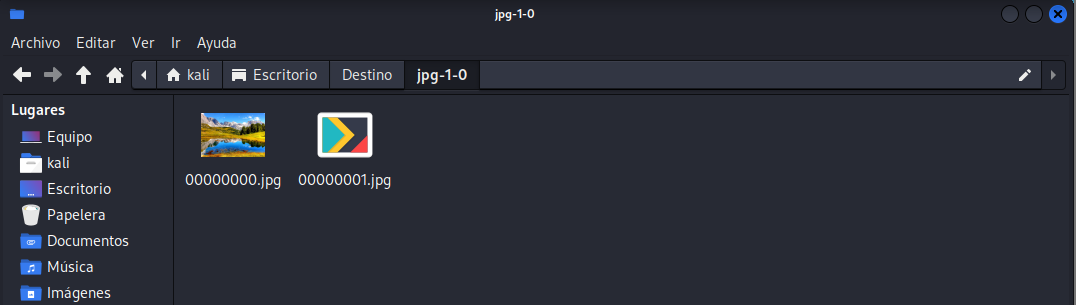
Ahora ejecutaremos el comando:

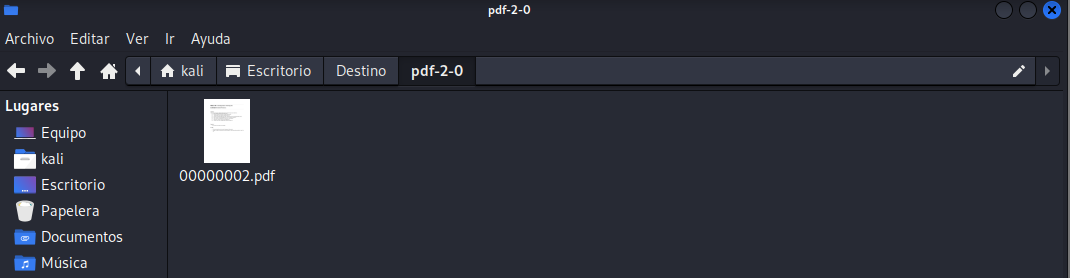


Solo me ha puesto las imagenes jpg, modificaré el scalpel.conf otra vez y volveré a intentar



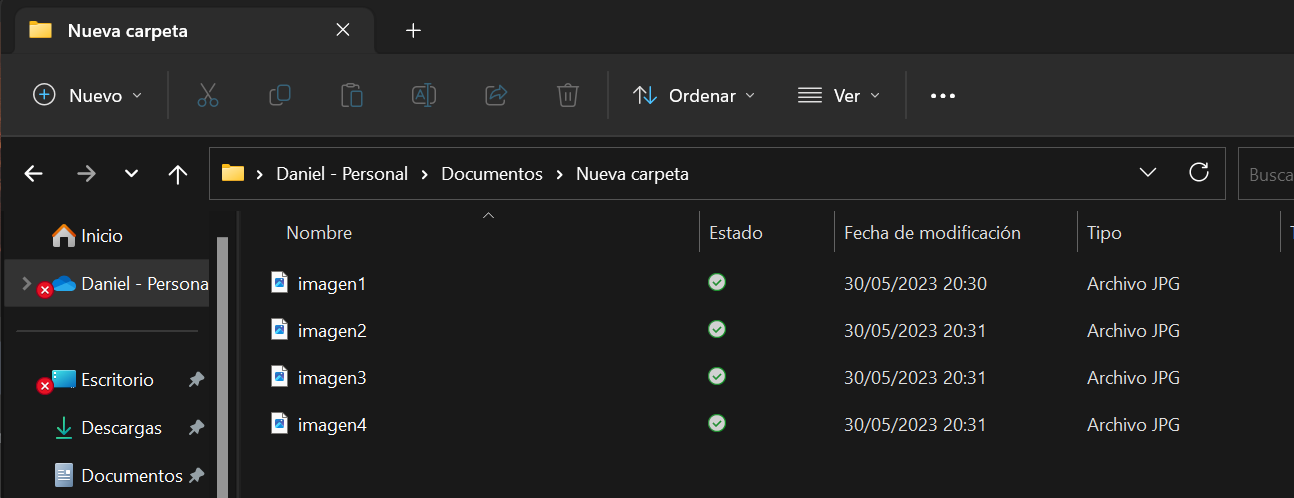
#### d. Comprova que el programa ha pogut recuperar els fitxers anteriors... i segurament altres fitxers què havies esborrat anteriorment del pendrive.



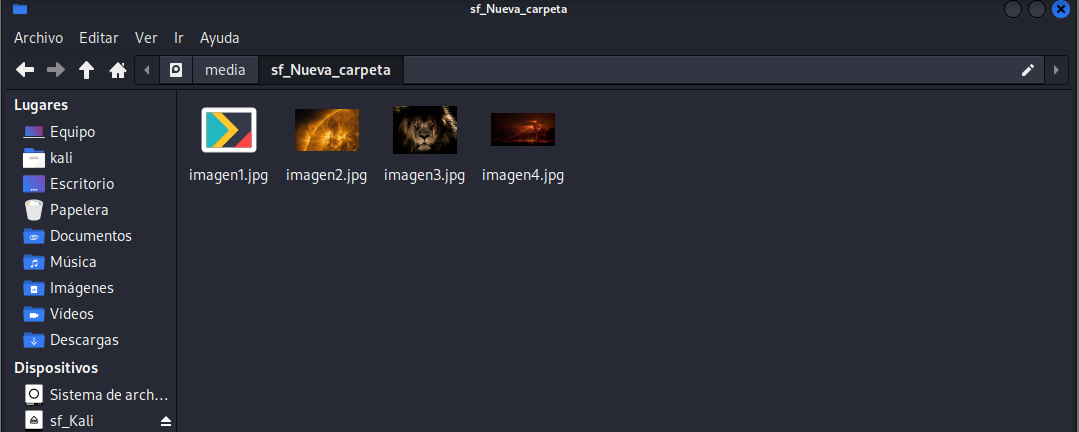


# Exercici 3 – Imatge forense des de Linux

#### a. Utilitza la eina GuyImager per a fer una còpia bit a bit d’un disc des de Kali Linux (pots fer-ho amb un pendrive o amb un disc dur petit que hagis afegit a Kali).

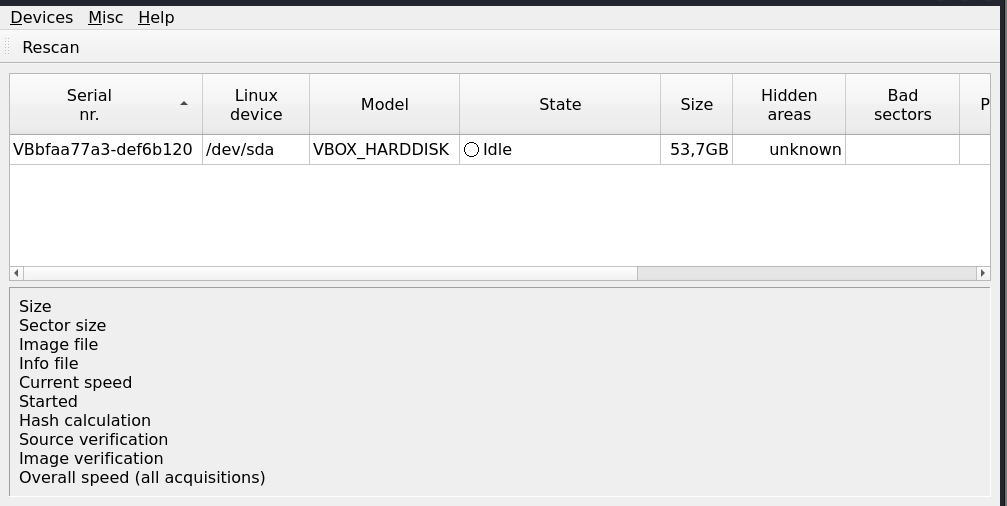


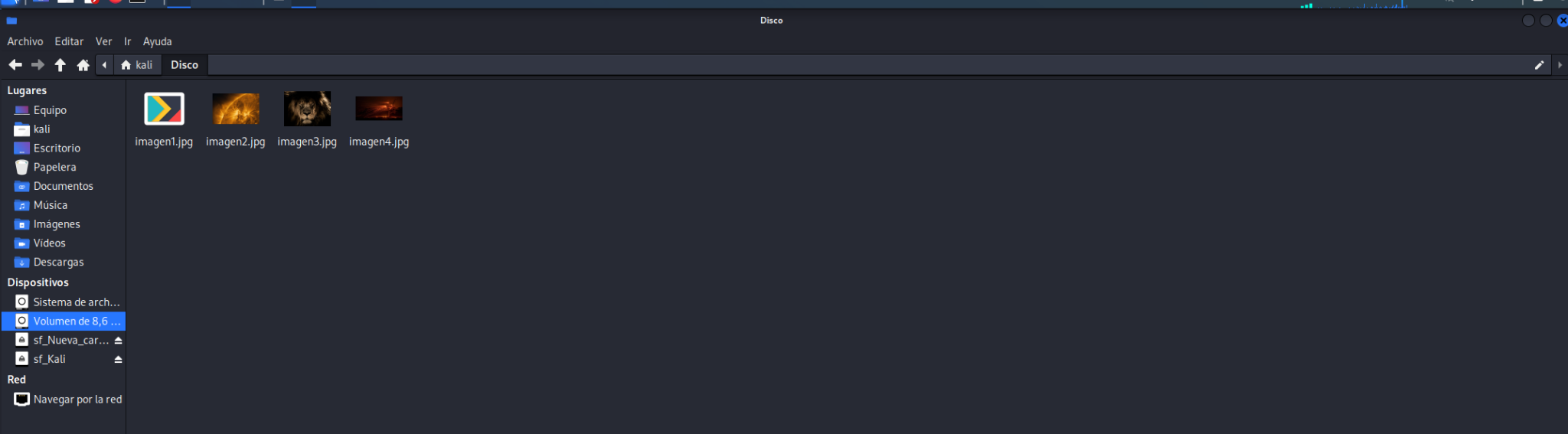
En una carpeta compartida pondremos archivos:



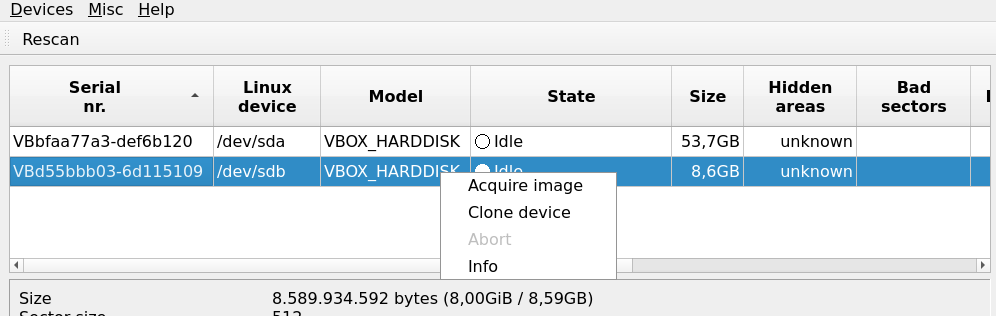
Entramos en el guymanager



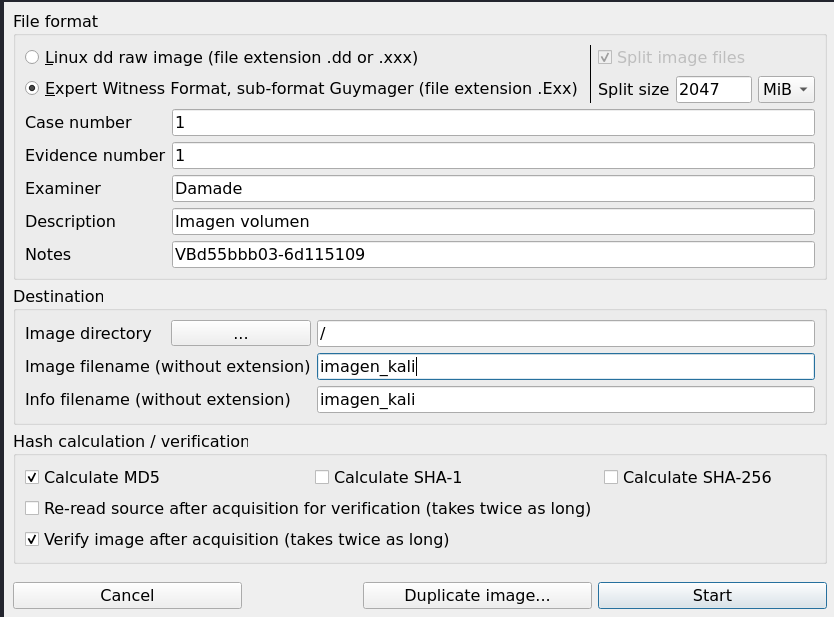




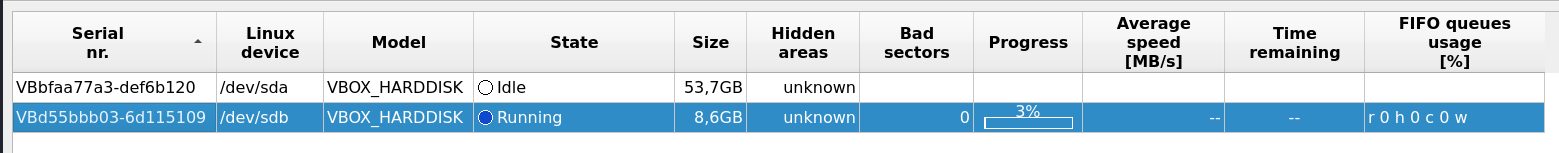
Pasamos los archivos a un volumen nuevo.



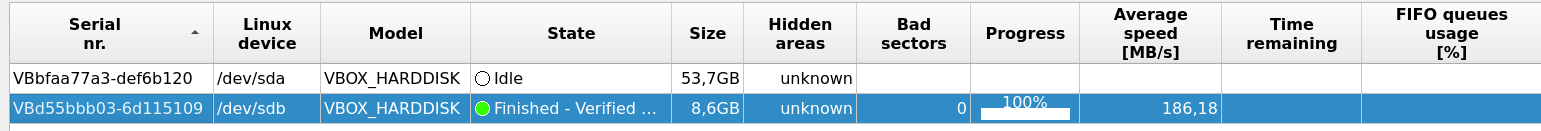
Le damos a acquire image



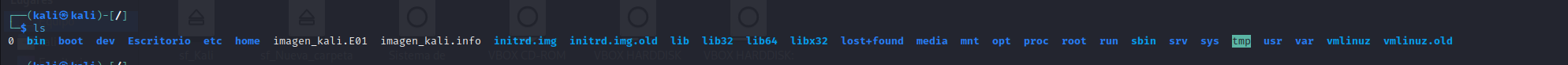
Finalmente le daremos a start



Vemos la barra de progreso

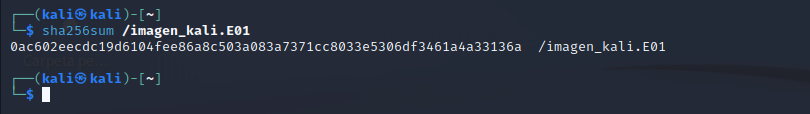


Finalizado



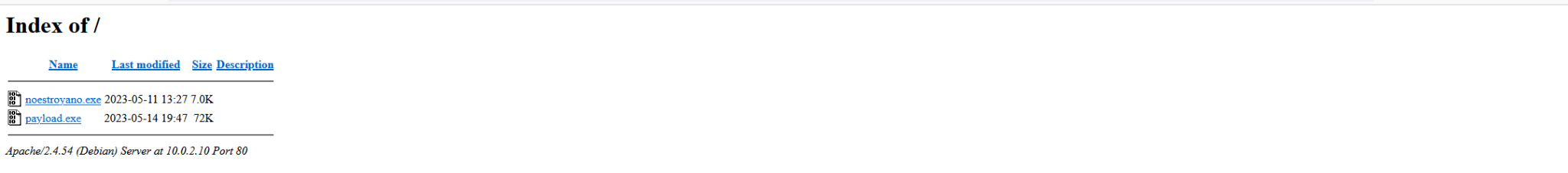
Se nos ha generado como podemos ver en el archivo imagen\_kali.E01

#### b. Un cop tinguis la còpia feta, calcula el seu Hash amb l’eina → sha256sum



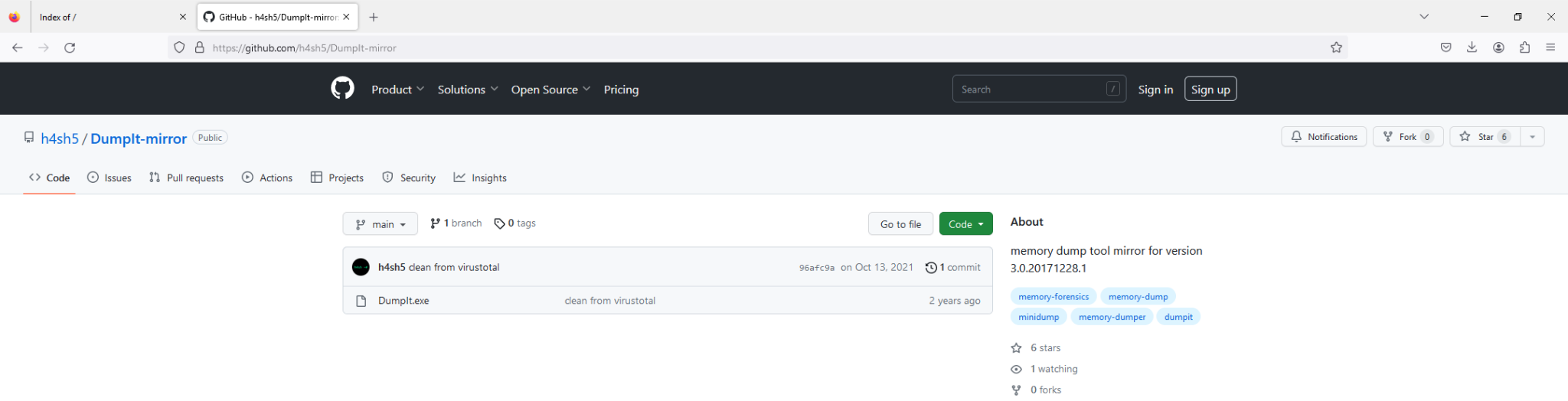
# Exercici 4 – Volcar memòria RAM de sistema Windows

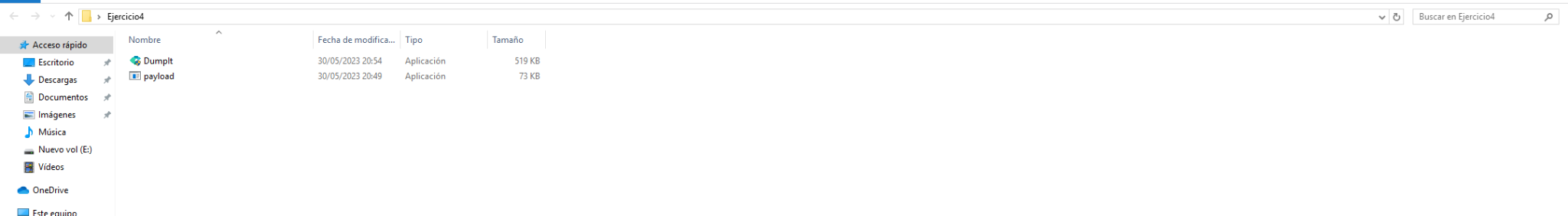
Descargamos un payload que ya hemos usado



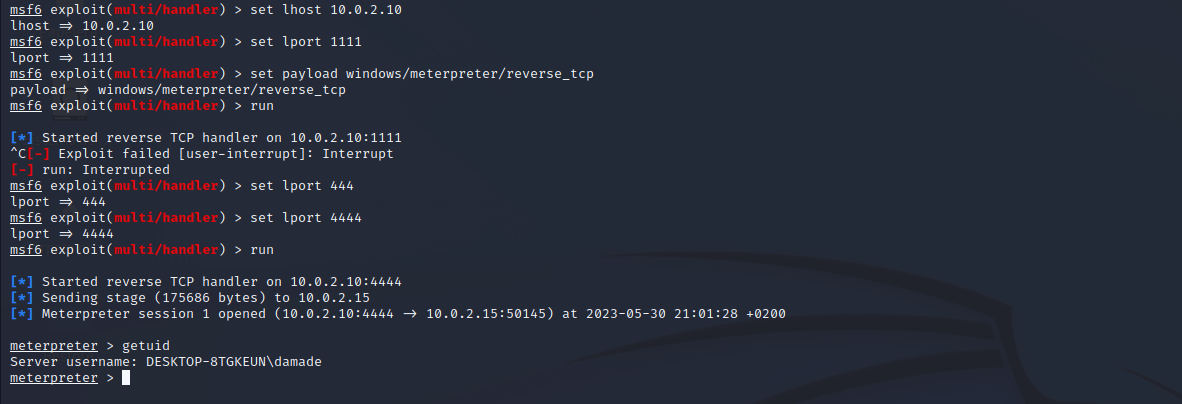
En mi caso payload.exe

Descargaremos tambien DumpIt

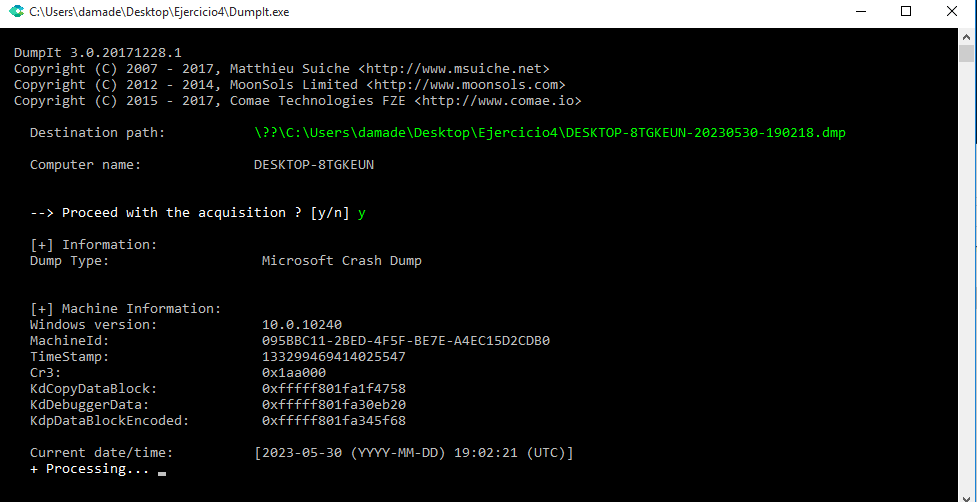




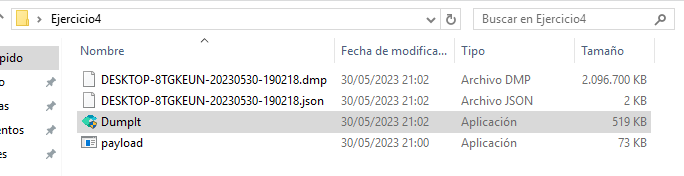
En el kali ejecutamos el msfconsole y configuramos todo



Ejecutamos el dumpit



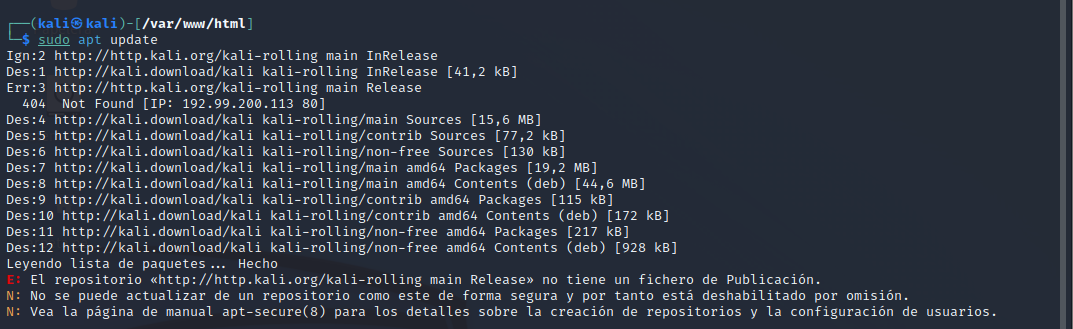
Se nos ha creado las imagenes:



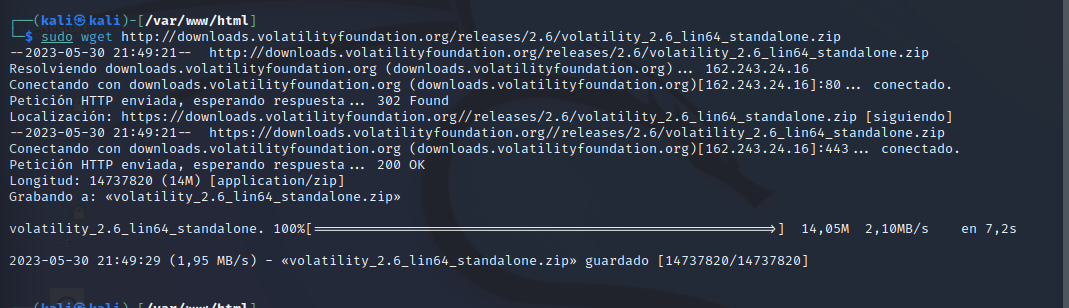
# Exercici 5 – Anàlisi de memòria RAM des de Kali Linux amb Volatility

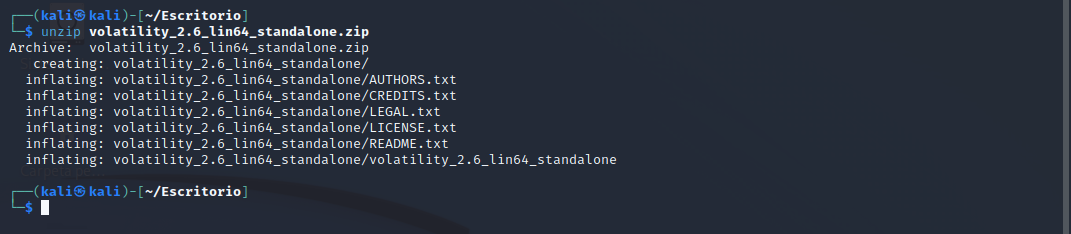
#### a. Per a instal·lar Volatility:

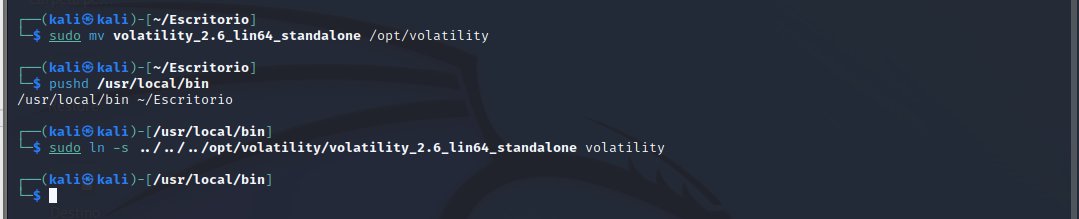
Haremos un apt update



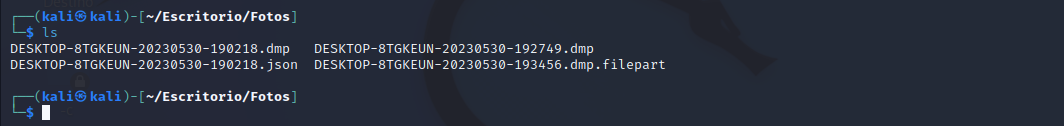
Seguidamente descargaremos de internet el zip de volatility:

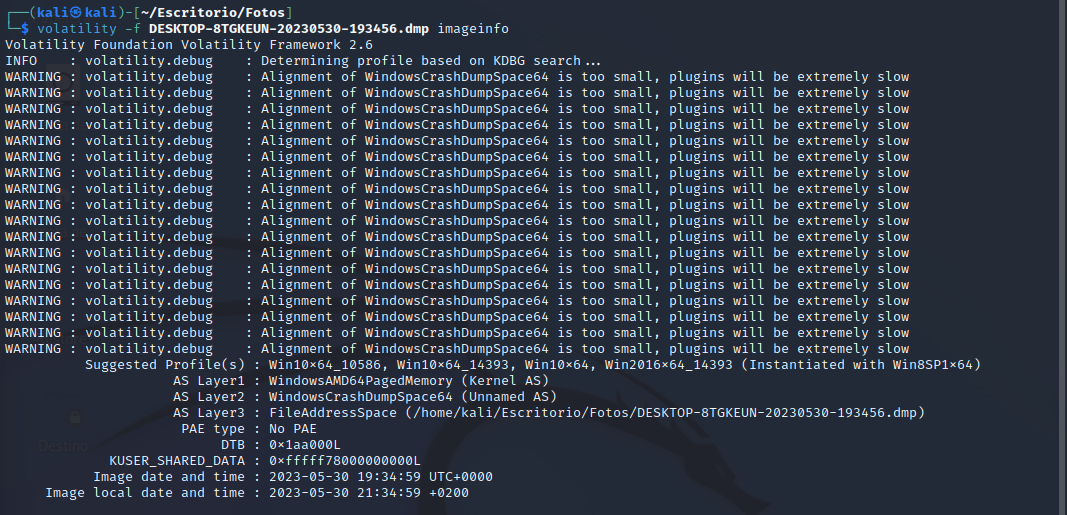




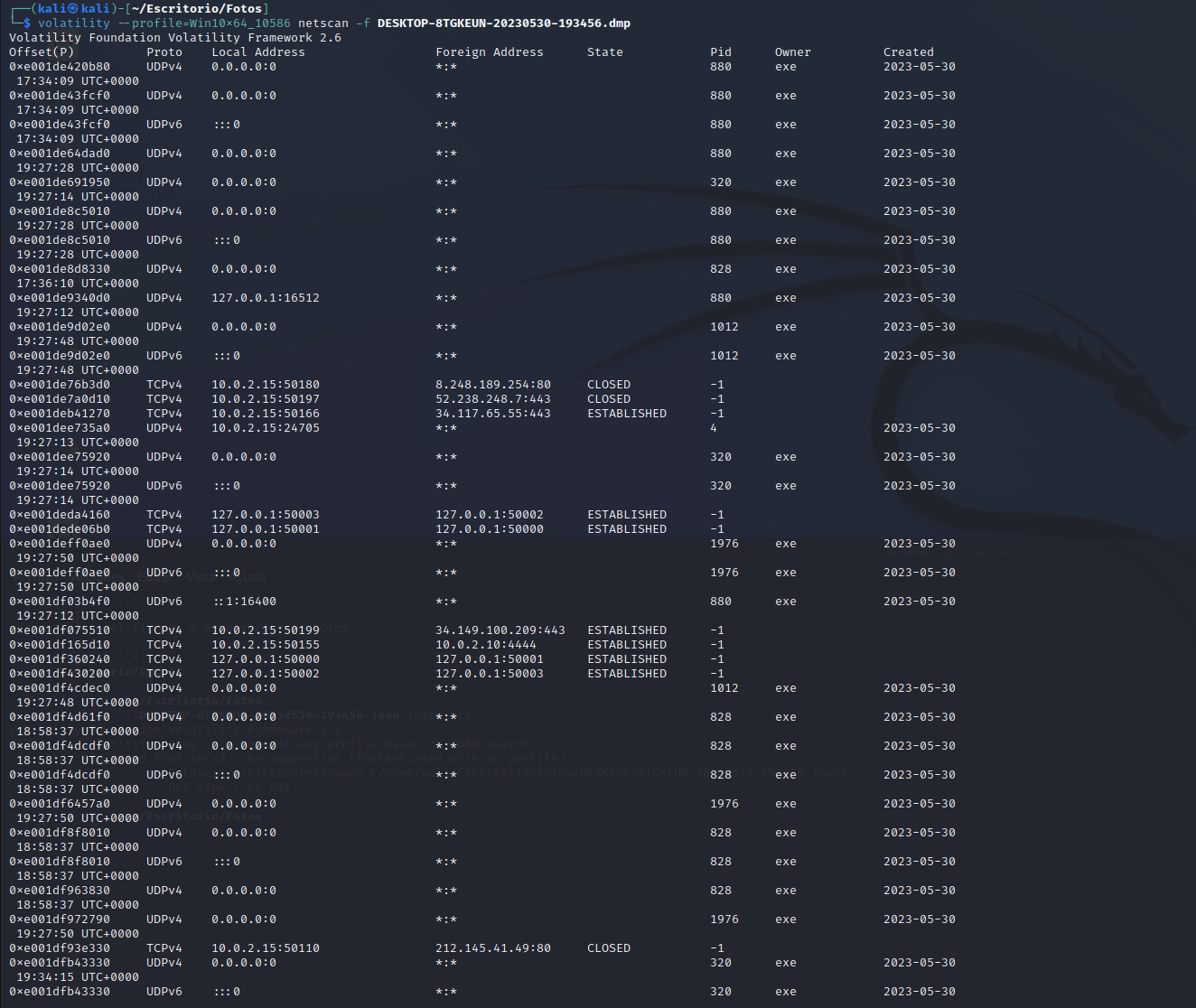


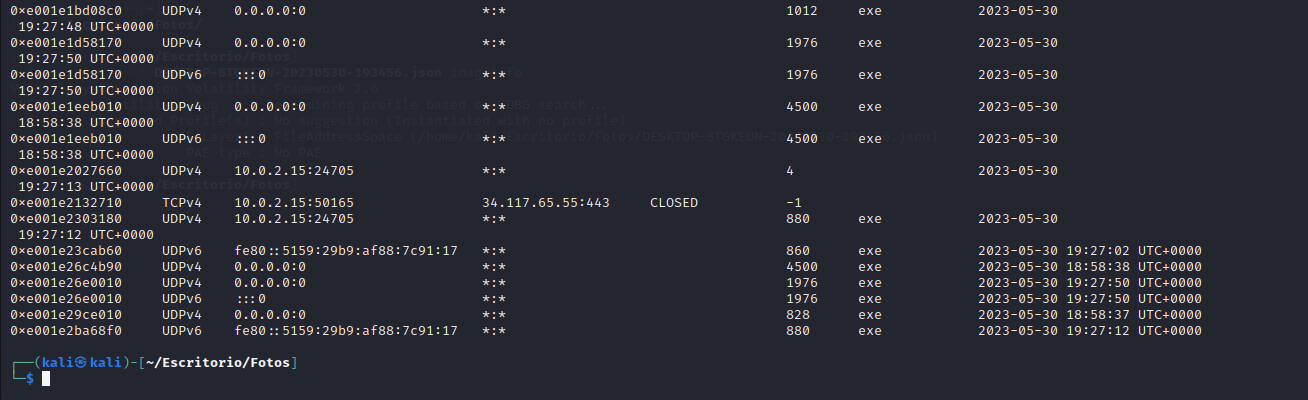
#### b. Per veure el perfil (o profile) de la teva RAM pots executar:



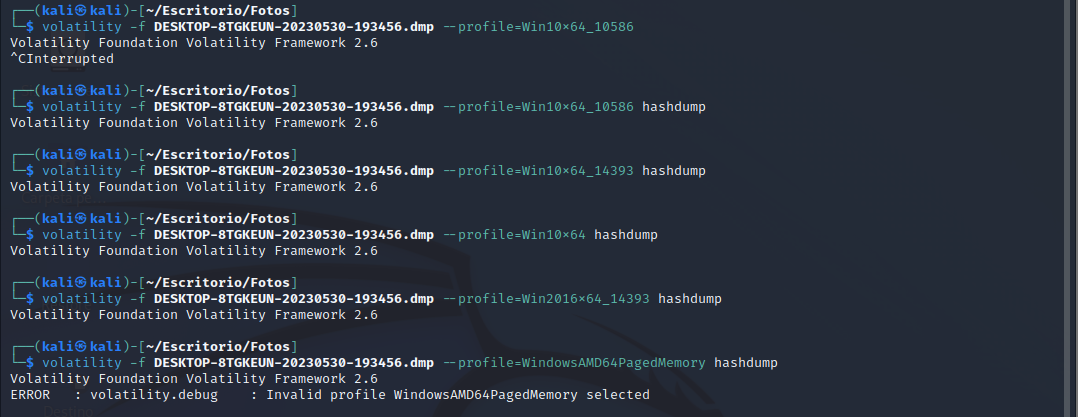


#### c. Busca on apareix la connexió reversa què ha fet la teva màquina víctima cap a la màquina atacant a partir de la imatge de la RAM.





#### d. Fes un volcat dels Hashes dels usuaris i passwords.



No ha funcionat com a tal.