**Manipulación de una fuente de evidencia no volátil en Linux**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **2**

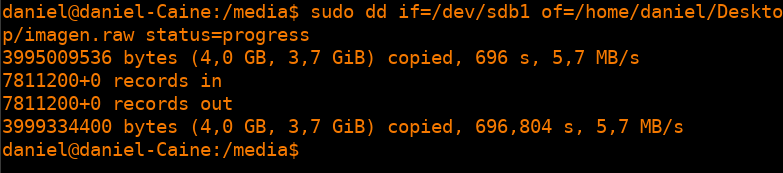
[**2. Linux**](#_g59i8ewd3ed3) **2**

[**2.1dd y Photorec:**](#_5d38uxjyswtl) **3**

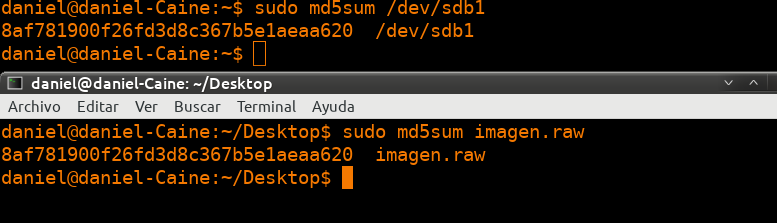
# **2. Linux**

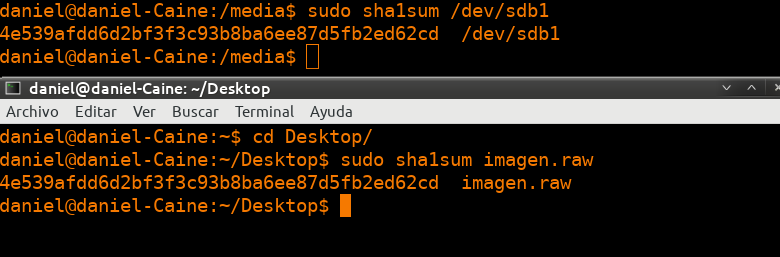
### **2.1dd y Photorec:**

Obtener, con el comando dd, la imagen del dispositivo físico en formato RAW



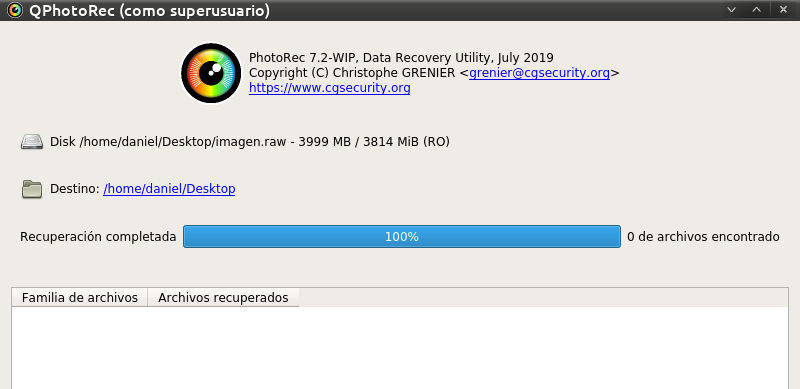
Comprobar la integridad de la imagen realizada, obteniendo los códigos md5 y sha1 del dispositivo original y de la imagen extraída.





Recuperar todos los archivos (también los borrados) de la imagen obtenida en el punto anterior.

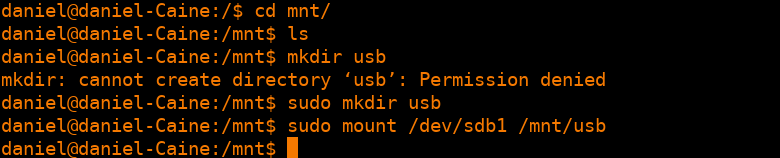
Mostrar, entre otras, captura del número de archivos recuperados de cada tipo que ofrece photorec

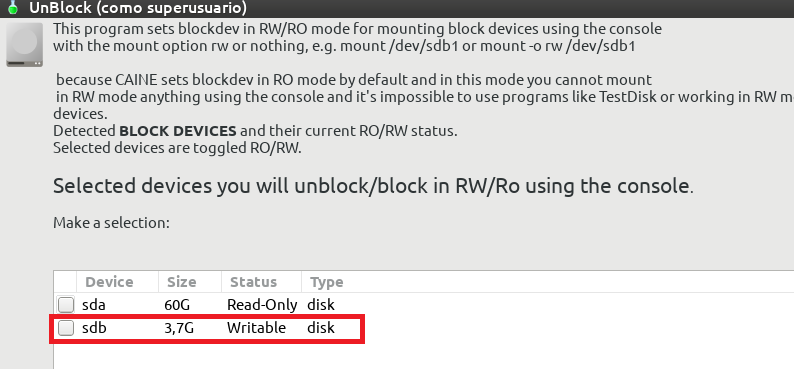


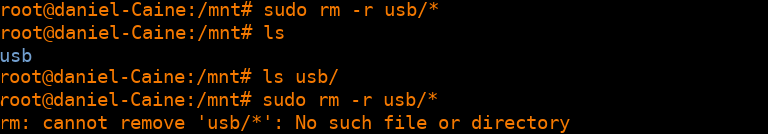
Borrar el contenido del dispositivo con el comando rm de Linux. Para ello tendrá que:

Montar el dispositivo con el comando mount o mediante la aplicación Mounter.

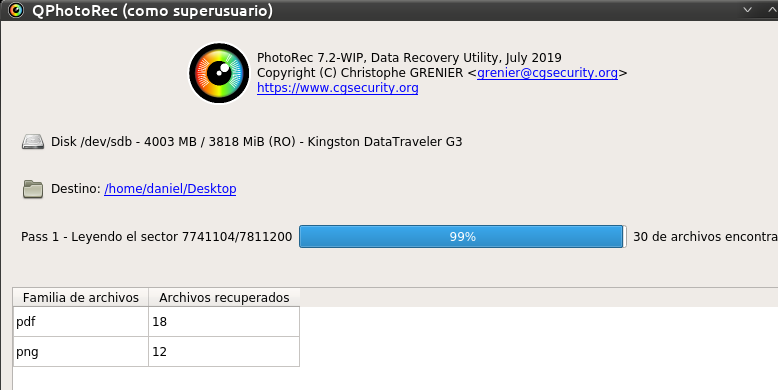
Asegurar que el dispositivo está en modo escritura, mediante la aplicación UnBlock



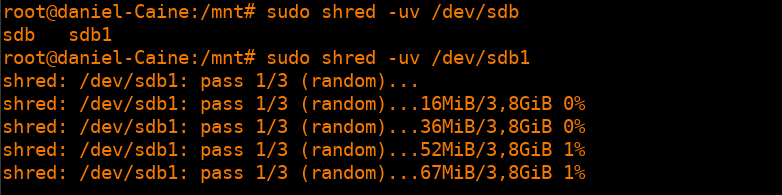




Recuperar la información del dispositivo físico tras el borrado con rm y mostrar captura de archivos recuperados esta vez. Comparar este dato con el anteriormente obtenido.

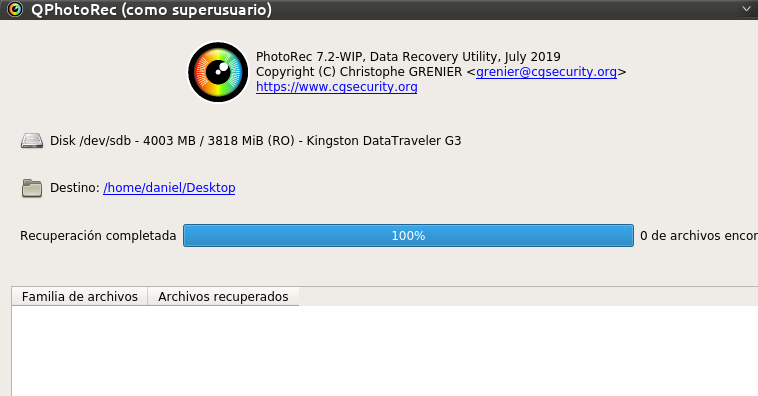


Hacer un borrado a bajo nivel del dispositivo con el comando shred (han de realizarse 3 pasadas de contenido aleatorio)



Verificar que el borrado de datos a bajo nivel ha sido efectivo.

Mostrar, entre otras, captura del número de archivos recuperados de cada tipo que ofrece photorec



Restaurar, con el comando dd, la imagen obtenida en el paso 1 en el dispositivo físico y verificar que contiene toda la información original.

