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



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

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

[**2. Windows 10**](#_g59i8ewd3ed3) **3**

[**2.1 FTKImager:**](#_5d38uxjyswtl) **3**

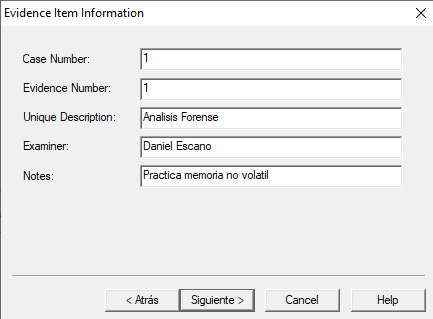
[**2.2 Photorec y Eraser:**](#_5ekabec8xp6e) **5**

# **2. Windows 10**

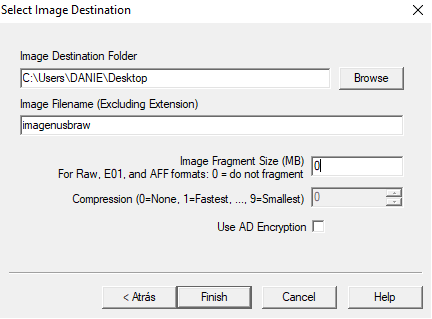
### **2.1 FTKImager:**

Obtener una imagen del dispositivo físico en formato RAW

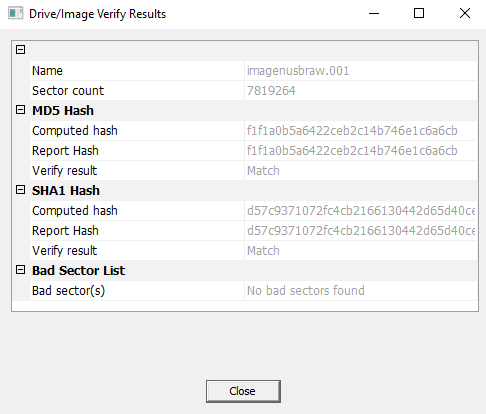
* Completar la información solicitada en el paso "Evidence Item Information" con datos que se ajusten a la actividad

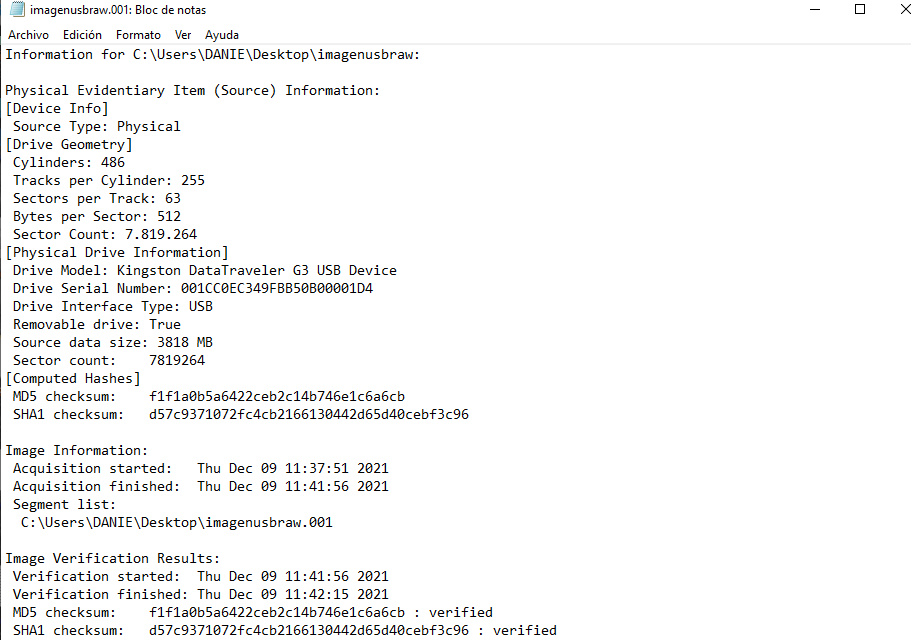


* No fragmentar la imagen generada

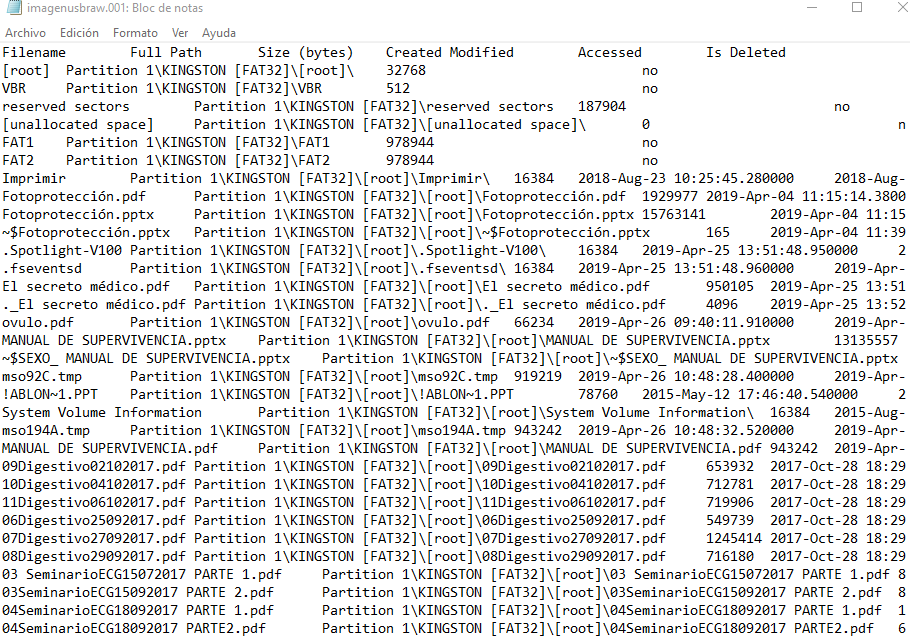


* Mostrar, entre otras, captura del informe de verificación generado tras la creación de la imagen





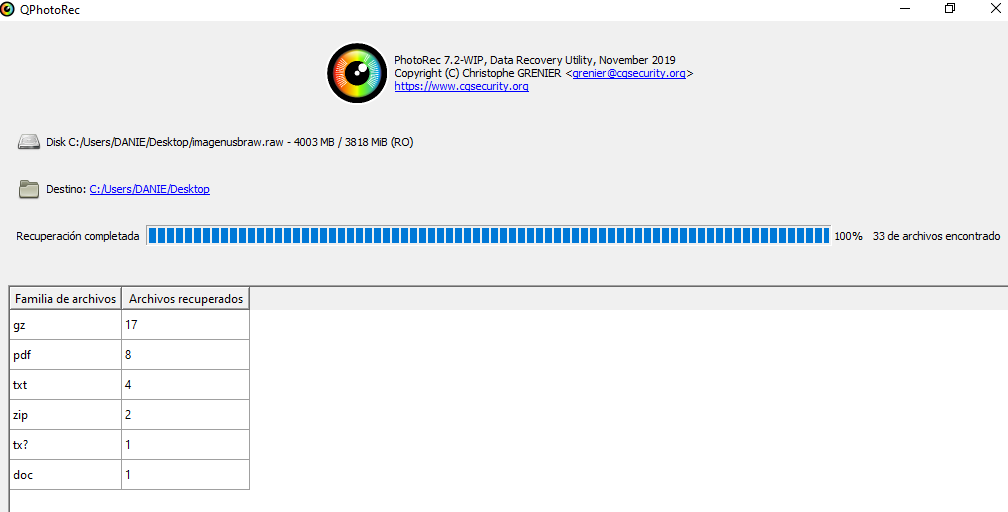
* Mostrar, entre otras, captura del listado de archivos de los directorios de la imagen creada



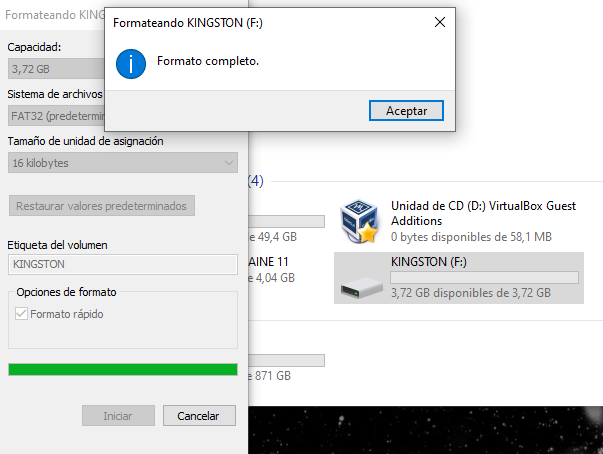
### **2.2 Photorec y Eraser:**

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

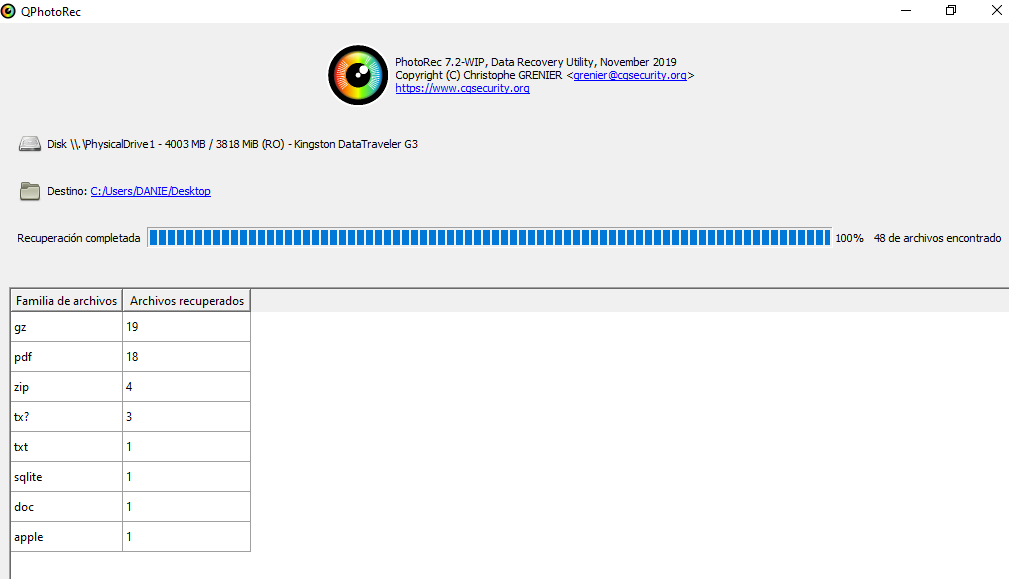


Realizar un formateo rápido del dispositivo físico

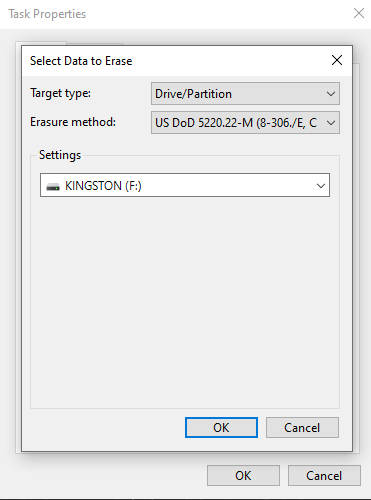


Hacer otra recuperación de archivos, del dispositivo físico, y comprobar la diferencia de archivos recuperados con el paso 2

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

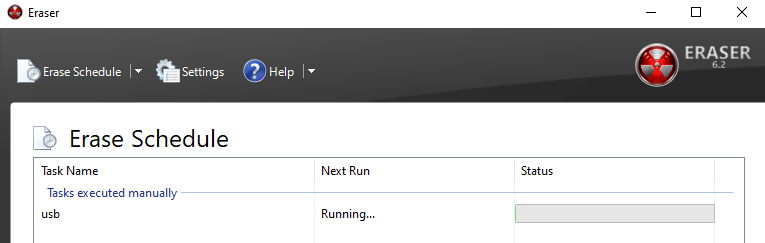


Realizar un borrado a bajo nivel usando el método US DoD 5220.22-M de 7 pasadas con Eraser



Añadir también la captura del log de la tarea de borrado ejecutada, donde se muestre hora de inicio y de fin del proceso.

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

