

Análisis forense

Unidad 1. Actividad 6



28 de NOVIEMbre de 2023

Carlos DÍAZ MONTES

ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

[Ejercicio 1. **¡Error! Marcador no definido.**](#_Toc148985456)

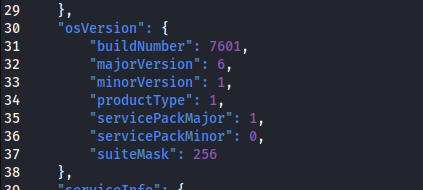
[Ejercicio 2 **¡Error! Marcador no definido.**](#_Toc148985457)

[Ejercicio 3. **¡Error! Marcador no definido.**](#_Toc148985458)

[Ejercicio 4 **¡Error! Marcador no definido.**](#_Toc148985459)

# Cuestiones a resolver

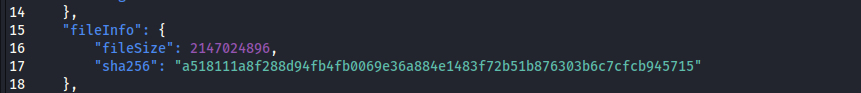
En el Json podemos ver esto:



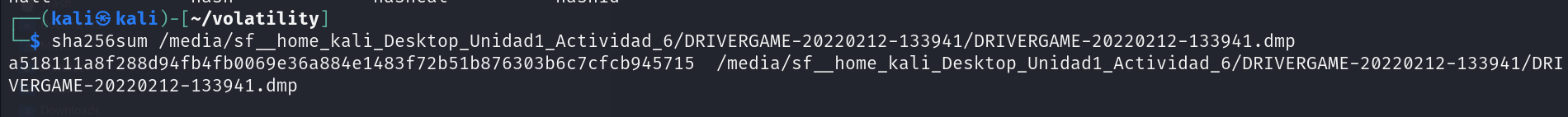
Buscando por internet podemos ver que es un windows 7.

**1. Verifica que los agentes corruptos del FBI no han encontrado y modificado la imagen de memoria para poder invalidarla en un juicio.**

Aquí vemos que esta modificado con sha356:



Y para ver si ha sido modificado hay que hacer un hash:



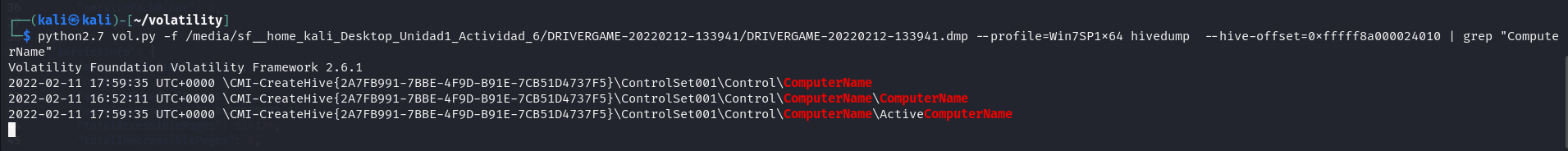
Como vemos la imagen es igual.

**2. Comprueba en el Registro de Windows que la imagen de memoria pertenece al ordenador de Tanner, llamado “DRIVERGAME”.**

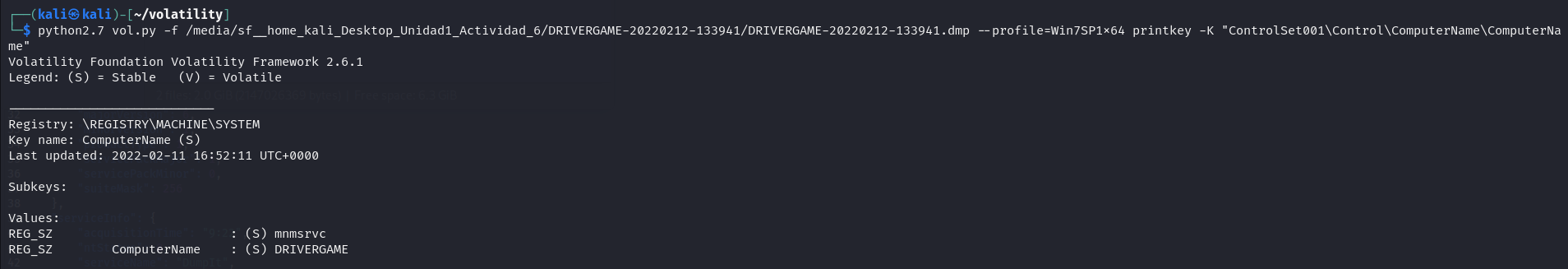
Primero tenemos que usar el hivelist para encontrar el disco virtual de los usuarios:



Ahora usamos hivedump para encontrar donde registra los nombres de usuarios:



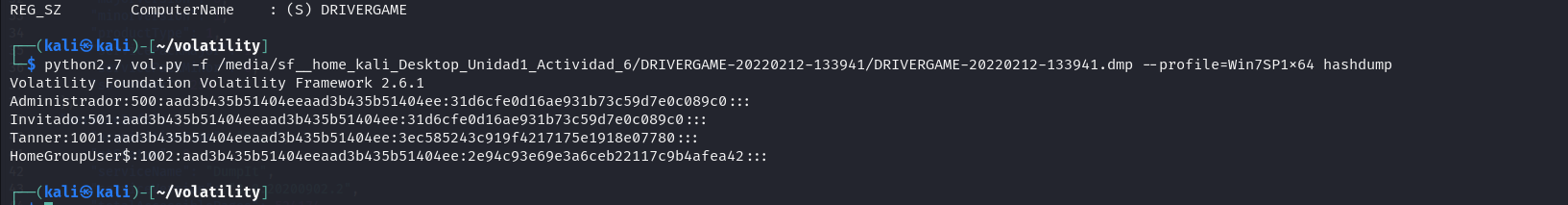
Ahora que sabemos la clave usamos el comando print:



Y ya podemos comprobar que es DRIVERGAME

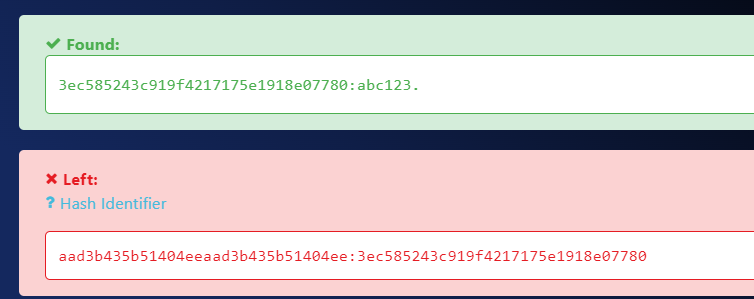
**3. [1,75] Para garantizar que nadie había intervenido el ordenador, comprueba que Tanner es el único usuario que hay en el equipo (aparte de los típicos usuarios por defecto de Windows, tales como “Administrador”, etc.), y obtén su contraseña. Para ésto último, debería bastar con usar uno de esos sitios web que invierten hashes. El comisario ya se ocupará del resto.**

Primero buscamos el hash Lm:



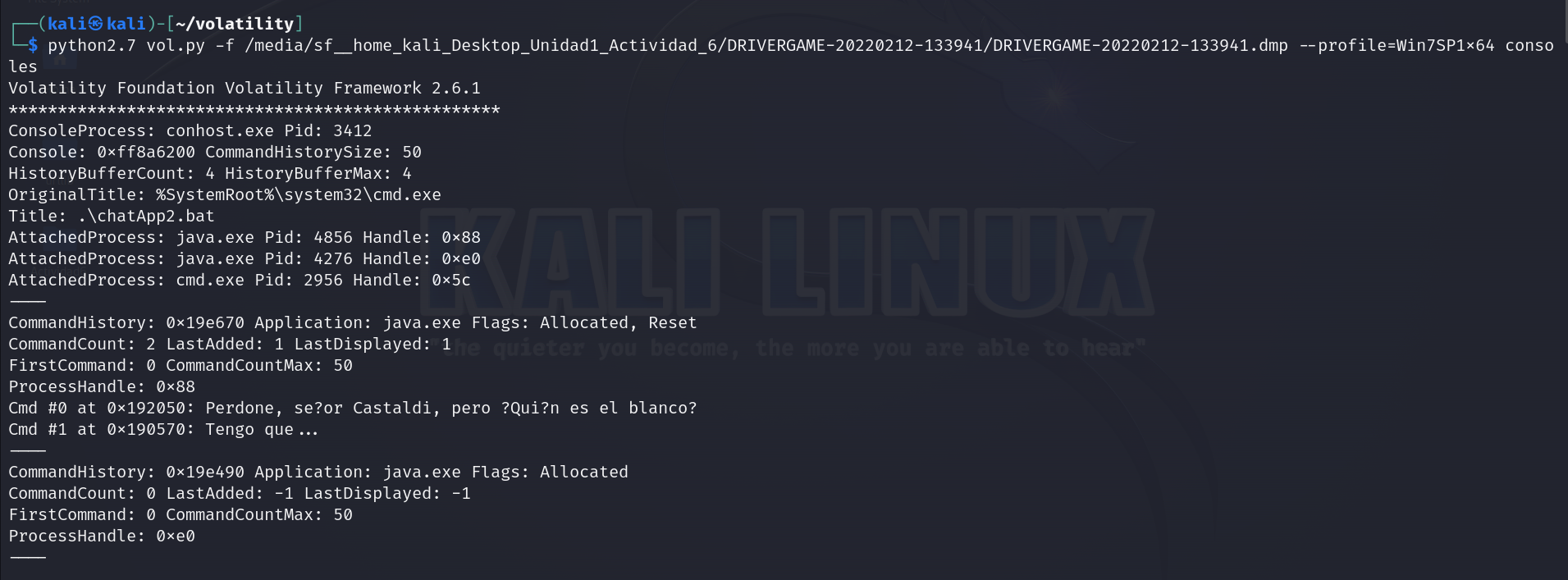
Ahora podemos ver que el único usuario es tanner (más los que crea por defecto windows)

Ahora para poner la contraseña hay que dessencriptador el hash:



**4. Encuentra pruebas de quién es el objetivo del próximo golpe, y de que quien da la orden es el Sr. Castaldi (2 pt por averiguar esto,1 pt por sacar el resto de la conversación).**

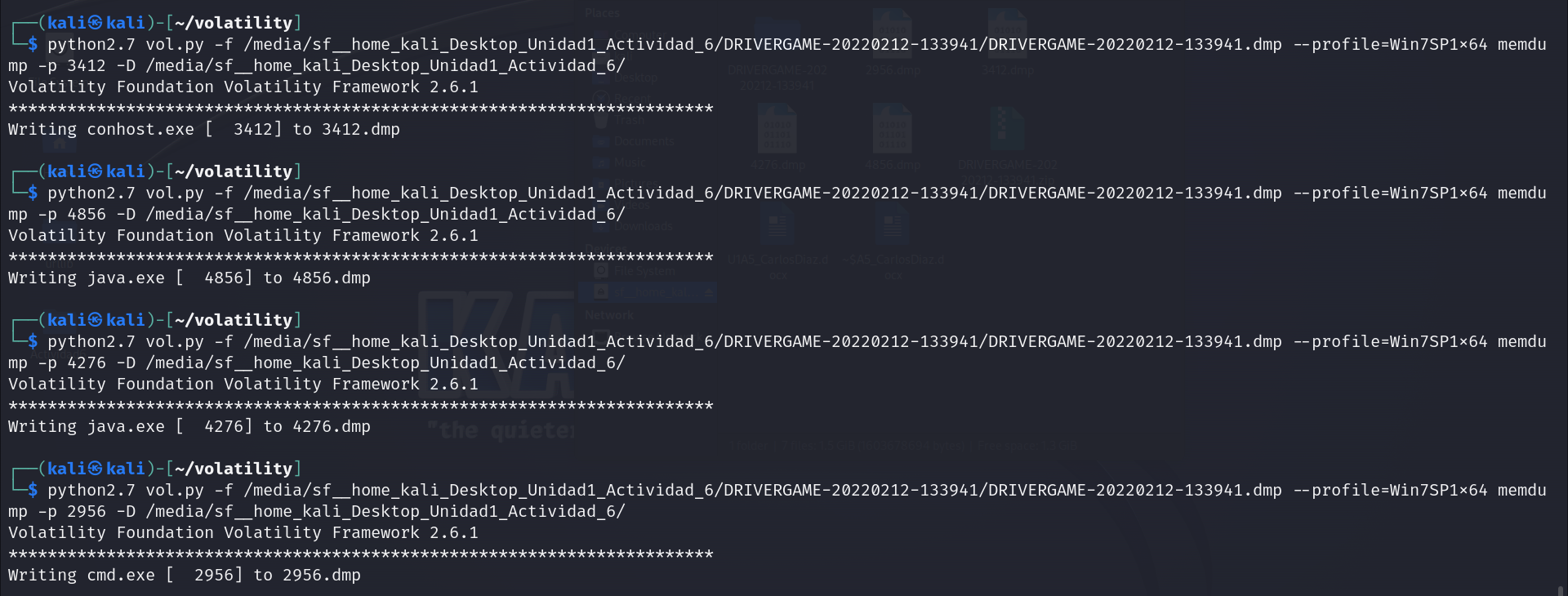
Con el plugin consoles podemos ver las consolas que estaban abiertas.



Después del comando ponemos pstree al final y miramos el 3412, 4856, 4276 y 2956.



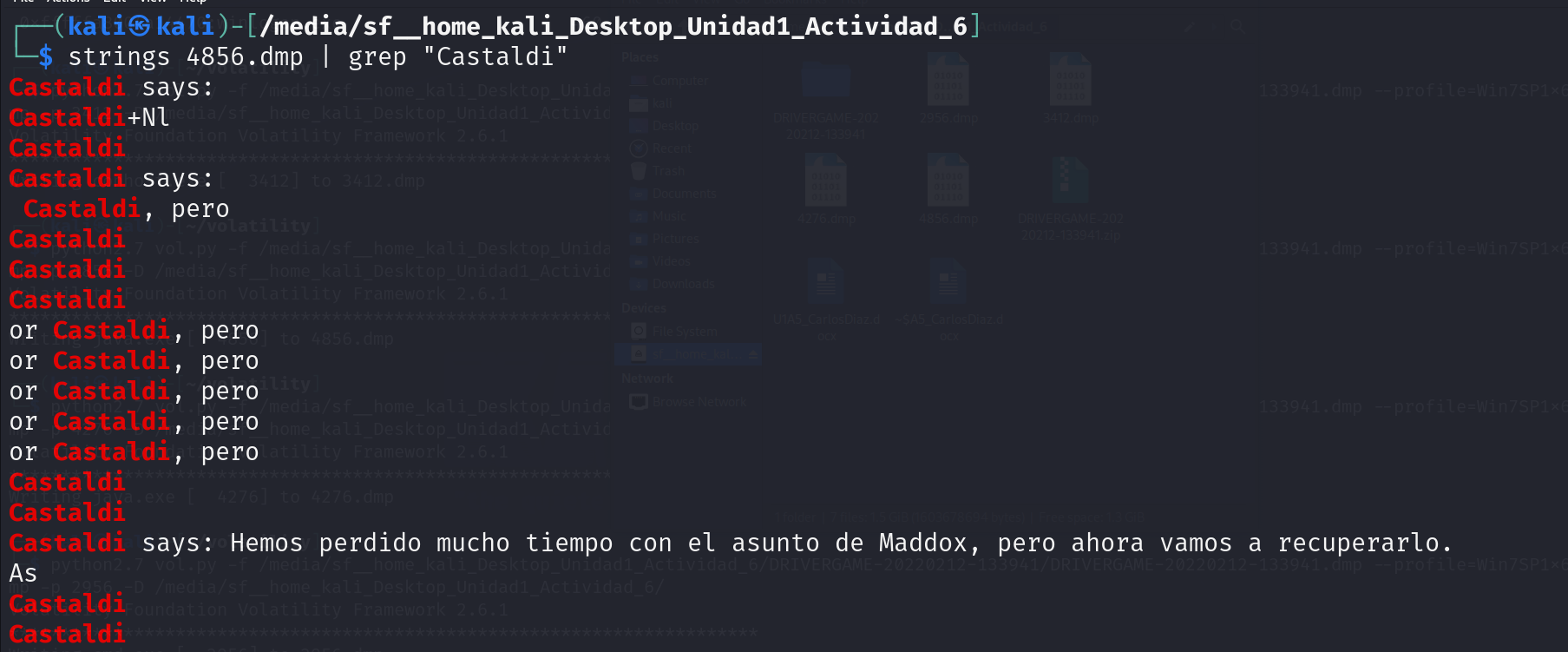
Usamos el comando memdump para descargar los procesos:



Ahora comprobamos cada uno con el comando strings. Primeo el 4276:

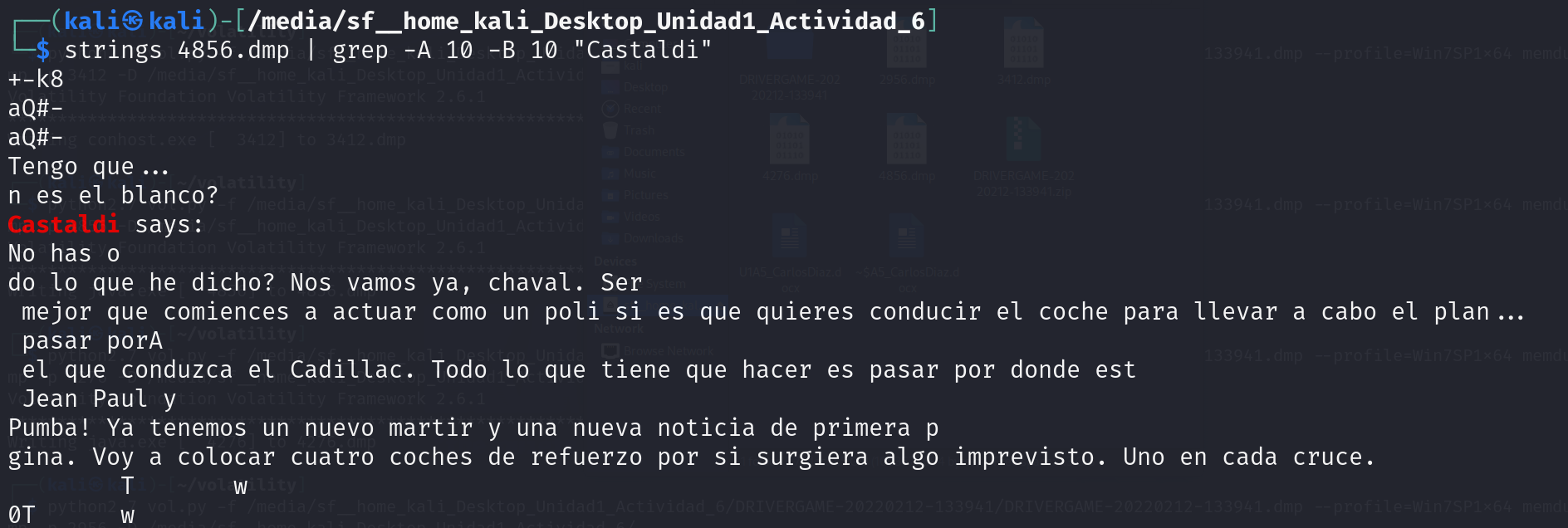


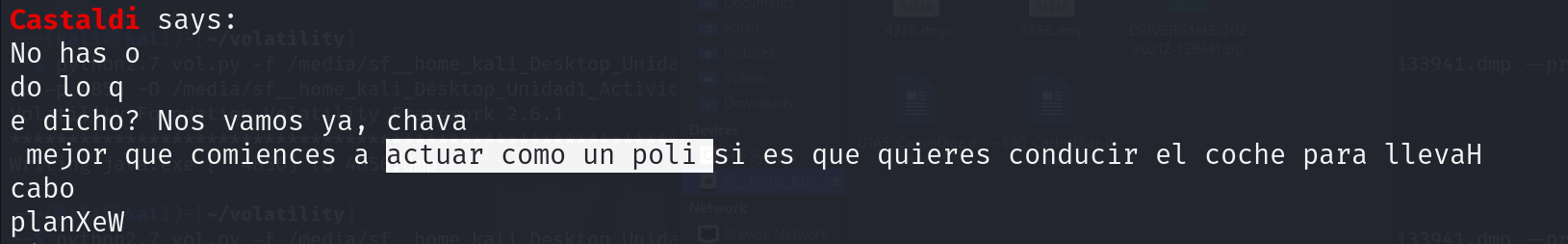
Ahora el 4856:

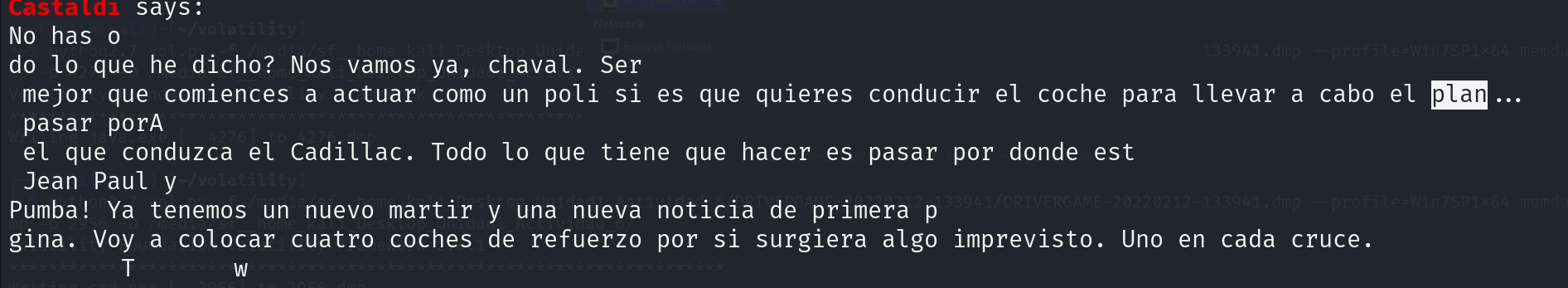


Como vemos con este nos sirve para verlo.

Ahora para ver el contenido completo:

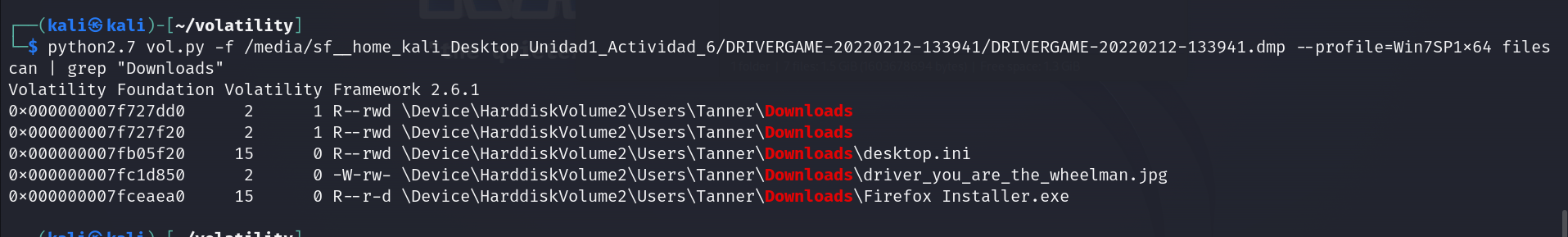




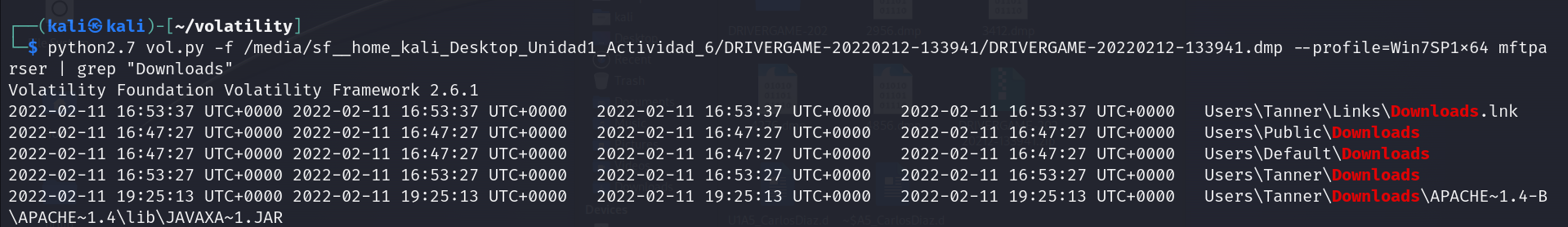


**5. A Tanner le enviaron un archivo con una foto (driver\_you\_are\_the\_wheelman.jpg) que tenía un mensaje escondido con instrucciones. Estamos interesados en saber si las ha recibido y leído. Para ello, encuentra pruebas de que en el directorio de Descargas de Tanner estaba dicho archivo (1,25 pt), y de que en algún momento lo abrió con el Visualizador de Fotos de Windows, también conocido como Windows Photo Viewer (1,5 pt). Nota: no te mates en buscar el mensaje secreto en la imagen, ya que no existe, haz sólo lo que se te pide.**

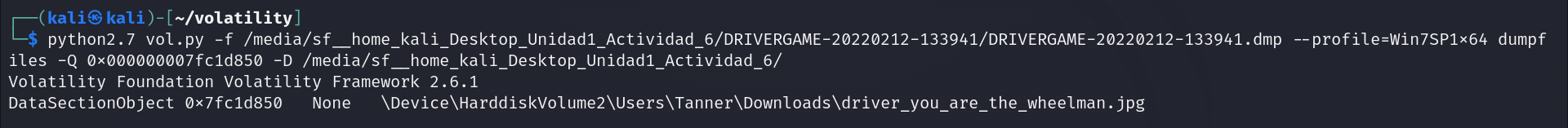
Usando el comando filescan podemos buscarlo, despues usamos grep para simplificar la búsqueda:



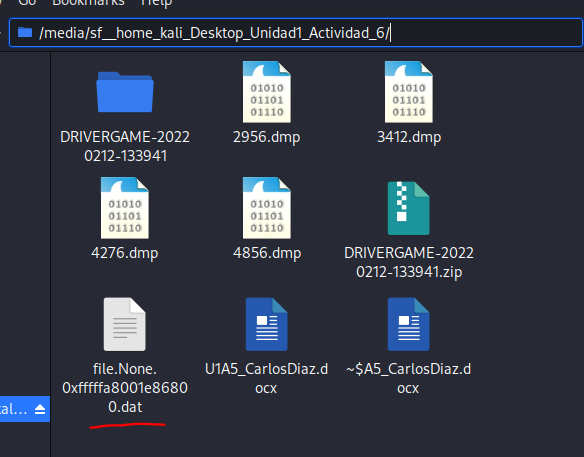
Otra forme de hacerlo es con mftparser



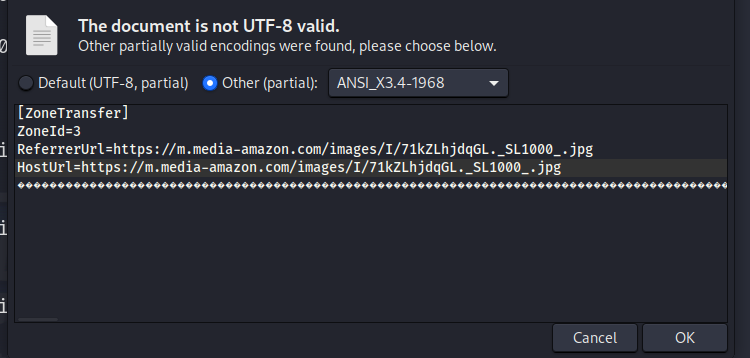
Ahora usamos dumpfiles para extraer los ficheros:



Como vemos en nuestra carpeta compartida, tenemos ahora un .dat:

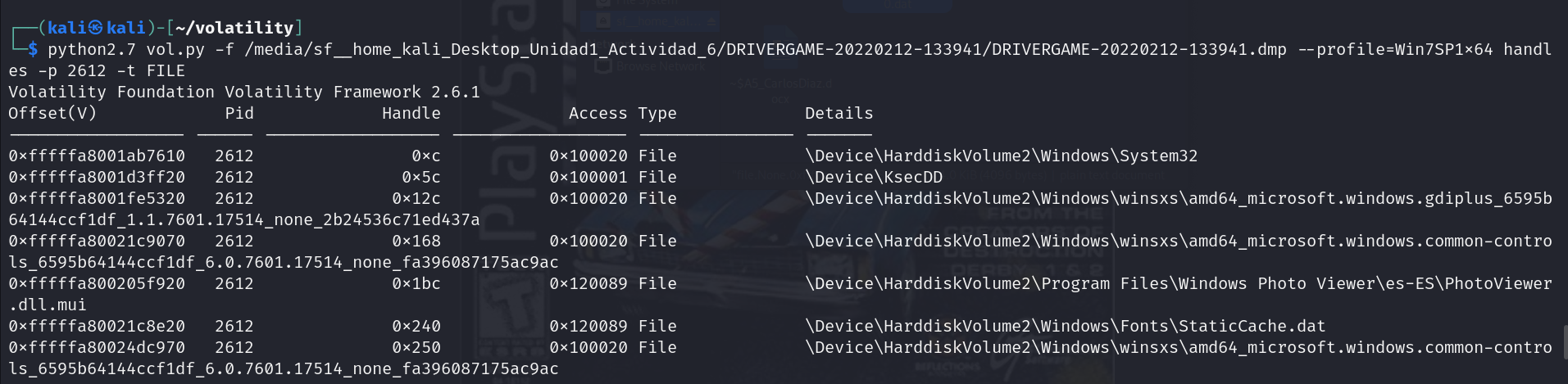


Ahora al abrirlo nos saldrá un enlace y podremos ver la imagen:

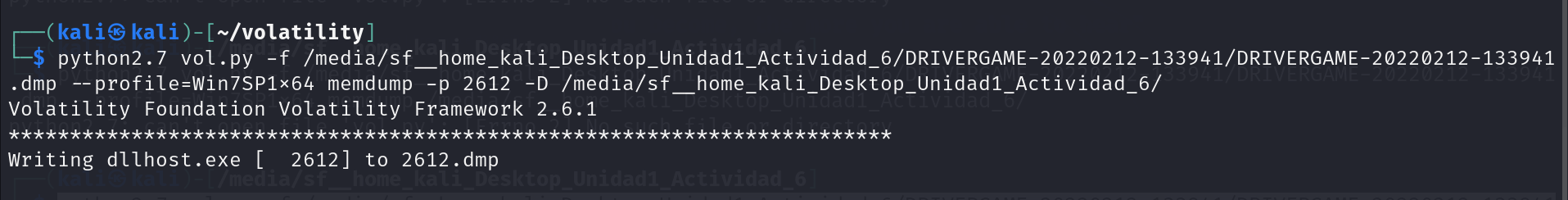




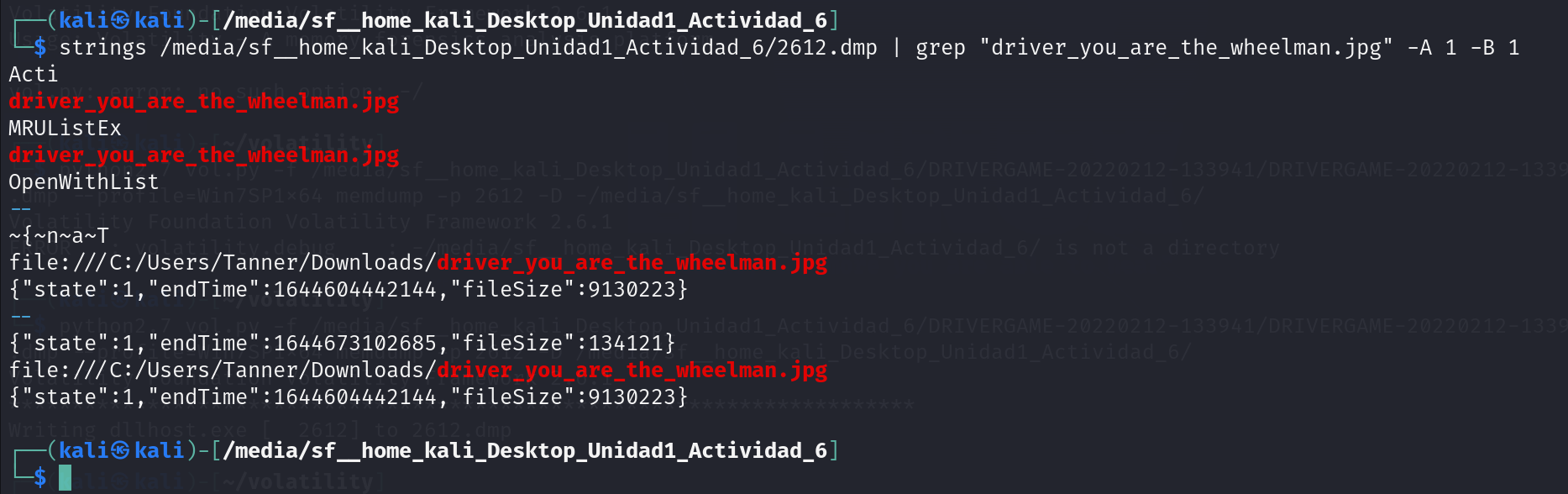
En nuestro caso, es el proceso con PID 2612. Podemos ver que dicho proceso tiene varios ficheros abiertos, y uno de ellos es \Device\HarddiskVolume2\Program Files\Windows Photo Viewer\es-ES\ PhotoViewer.dll.mui, pero desgraciadamente ninguno es la imagen que buscamos:



Volcamos el espacio de memoria:

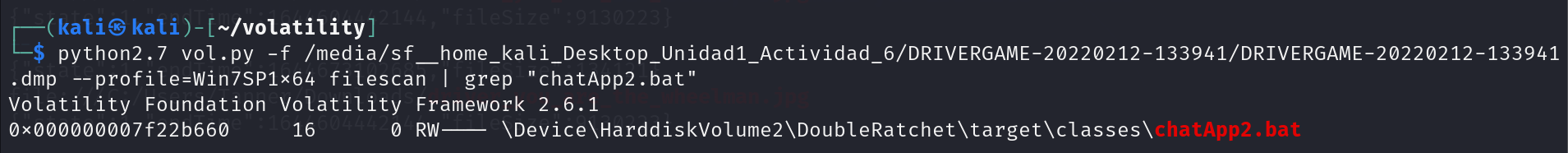


Para comprobar si ha sido ejecutado, usamos strings sobre ese proceso:

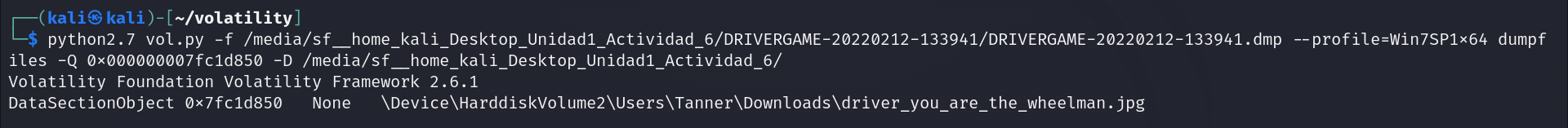


**Miscelanea**

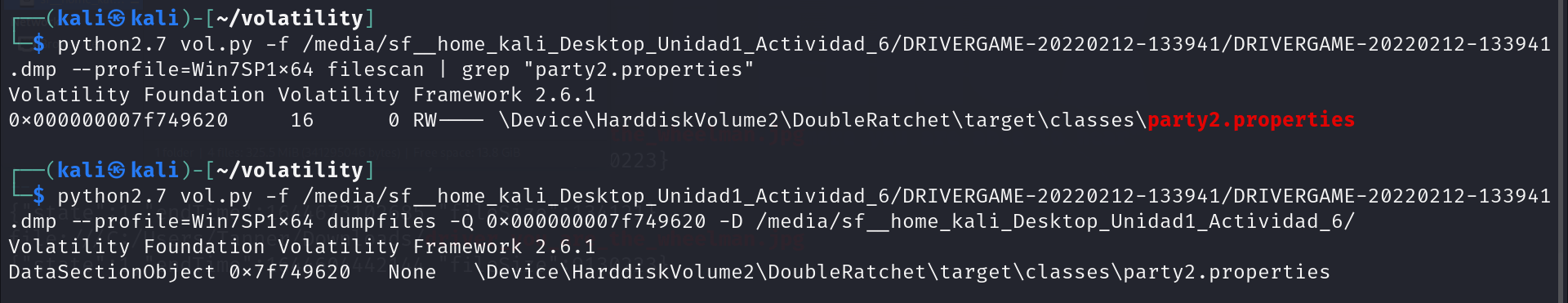
¿Es posible obtener el contenido del fichero chatApp2.bat que se menciona al emplear el plugin consoles?



Ahora podemos descargar con dumpfiles y ver su contenido:



Como se puede apreciar, la aplicación recibe como parámetro un fichero llamado party2.properties. Podemos repetir el proceso e intentar descargarlo:



Ahora vemos el contenido del archivo descargado:

