

Análisis forense

Unidad 1. Actividad 7



9 de ENERO de 2024

Carlos DÍAZ MONTES

ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

[Práctica Evaluable análisis de memoria 2](#_Toc156848248)

# Práctica Evaluable análisis de memoria

**1. Comprueba que la imagen de memoria pertenece al ordenador del alumno, llamado "DESKTOP-01S7HH9".**

Primero descargamos el archivo que esta junto al pdf, despues lo metemos en la carpeta compartida que tenemos y lo descomprimimos con unzip.

Ahora para comprobar que la imagen de memoria pertenece al mismo usuario, hacemos el hash y lo comparamos:

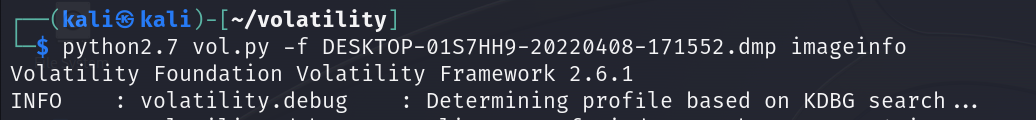


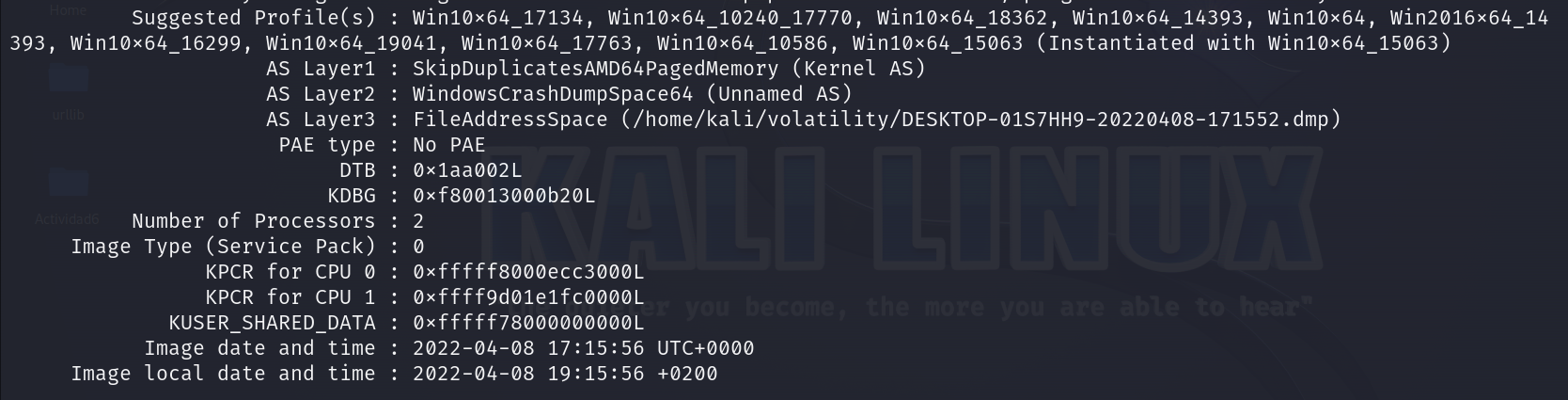


Como vemos son los mismos.

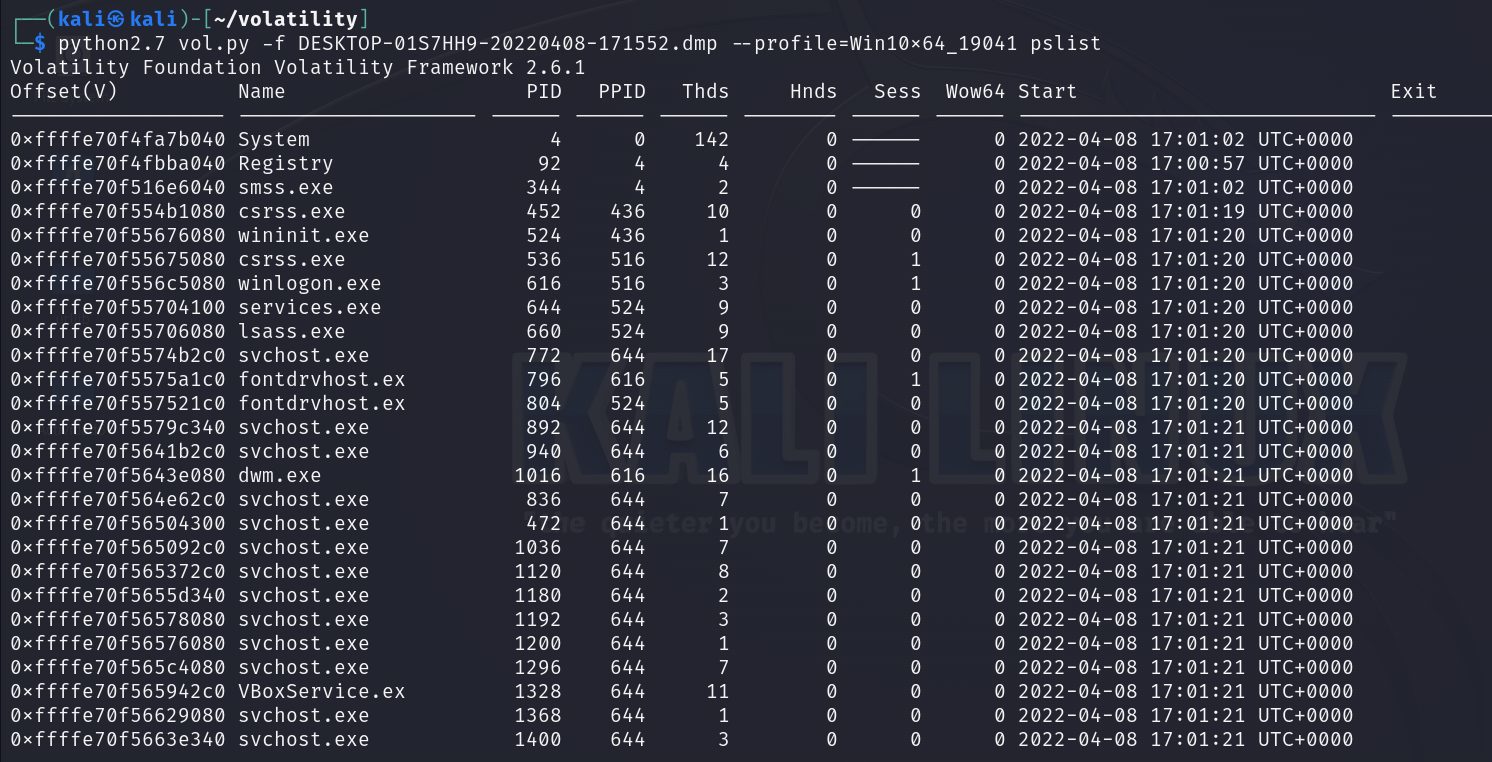
**2. Determina el o los PID del proceso correspondiente a una aplicación para realizar chats, especialmente entre jugadores .de videojuegos. ¿Cuál es su proceso padre?**

Ahora lo primero que vamos a usar es el comando imageinfo para saber que tipo de sistema operativo utilizaba:

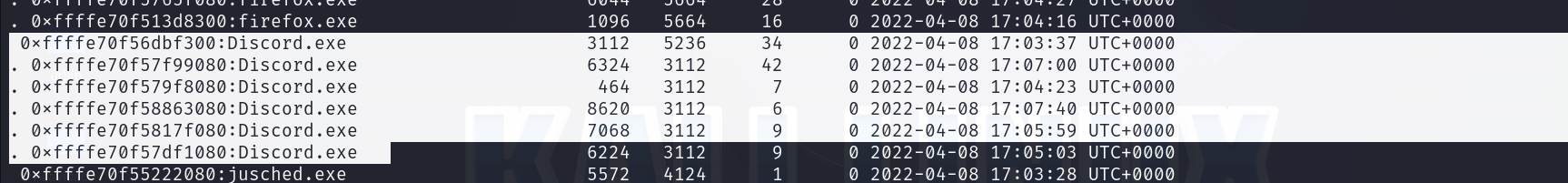




Ahora sabemos que el que necesitamos es el **19041,** podemos usar el comando pslist para ver los procesos:

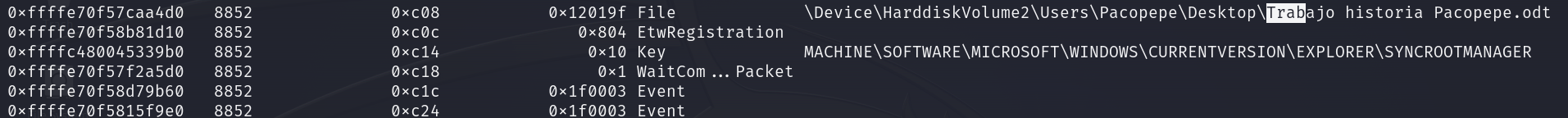


Ahora buscamos una aplicación de chat y videojuegos, como Discord.exe :



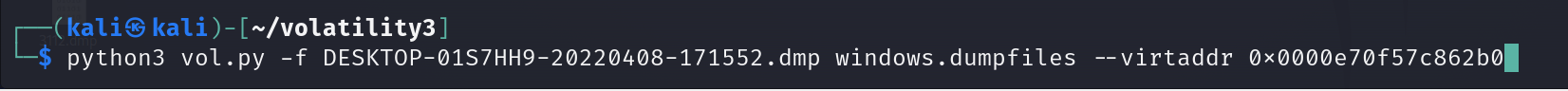
**3. Determina a través de los manejadores qué documento estaba editando el alumno durante la redada policial.**

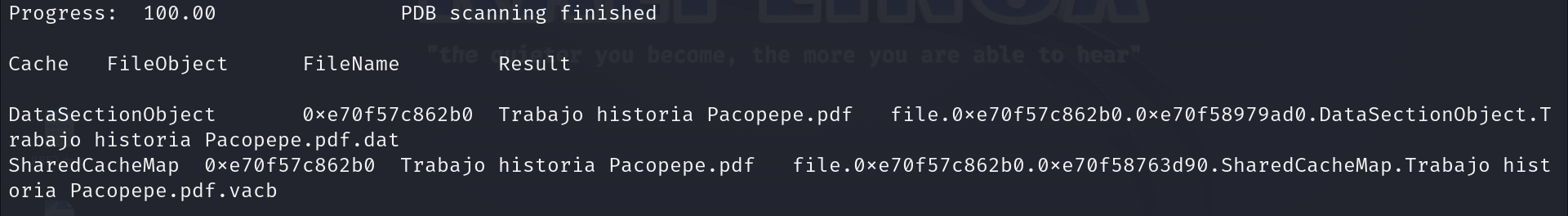
Con el comando handles podemos obtener información sobre los objetos de manejo de archivos y procesos. Buscando un poco encontré este documento:



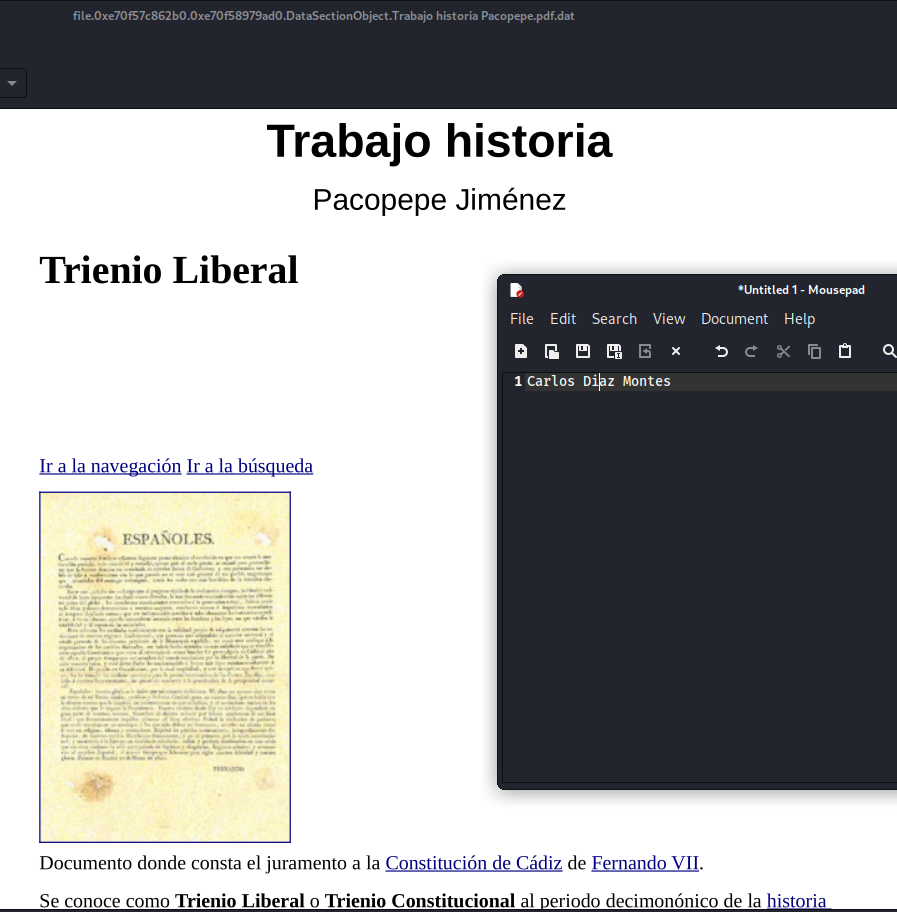
Ahora lo que queremos hacer es descargarnos el -odt, en mi caso he probado de muchas formas como con dumpfiles pero no me ha dejado.

Al final he optado por usar volatility3:





Ahora vamos a comprobar el archivo:



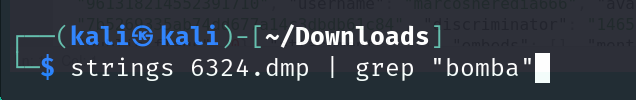
**4. Encuentra pruebas de que el usuario del equipo está tras la falsa amenaza de bomba**

Para esto vamos a comprobar los procesos antes vistos (los de discord).

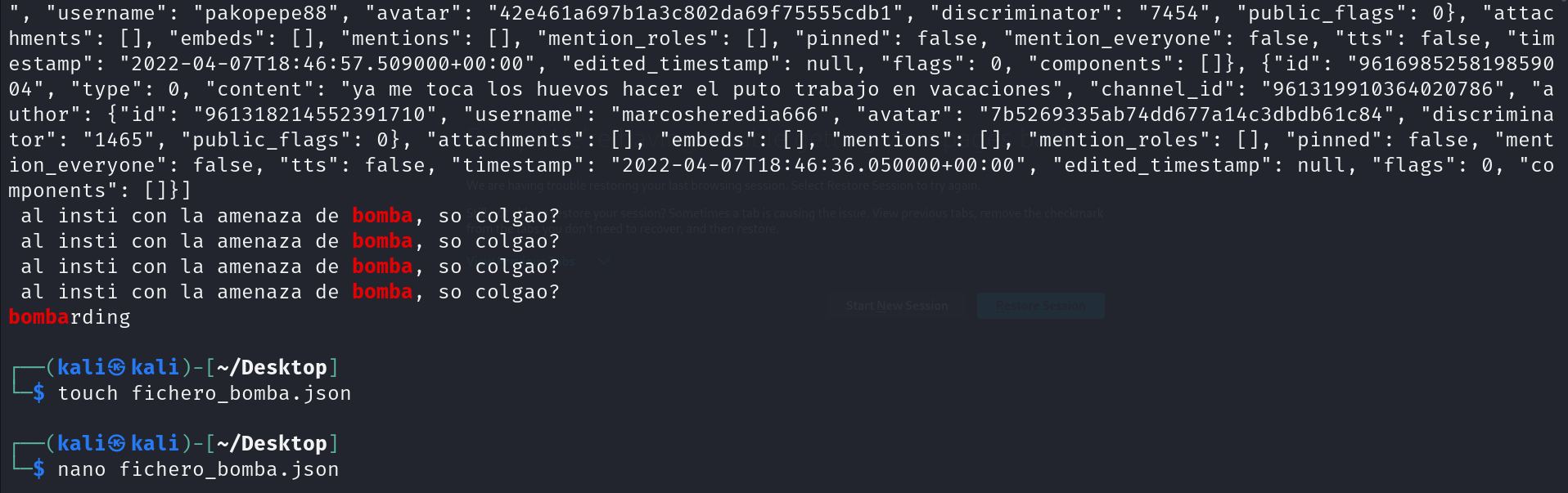
Para esto vamos a descarnarnos todos los procesos:



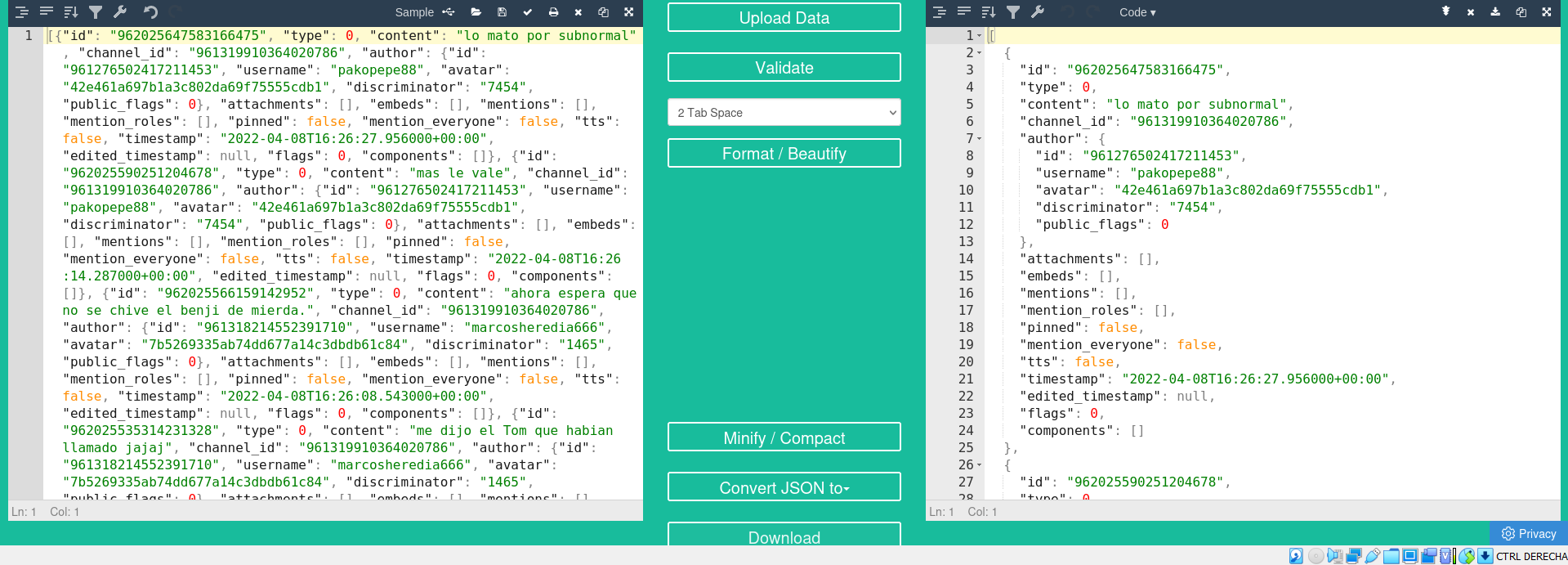
Ahora comprobamos los procesos (el proceso clavees el 6324).Primero vamos a usar el comando string para comprobar que sale alguna palabra clave como “bomba”:



Ahora vamos a copiar todo el contenido y vamos a pegarlos en un fichero .json:



Ahora vamos a poner el contenido legible desde internet:



Vamos a convertirlo para comprobar su contenido:

