

Análisis forense

Unidad 1. Actividad 4



20 de NOVIEMbre de 2023

Carlos DÍAZ MONTES

ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

[Ejercicio 1. 2](#_Toc148985456)

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

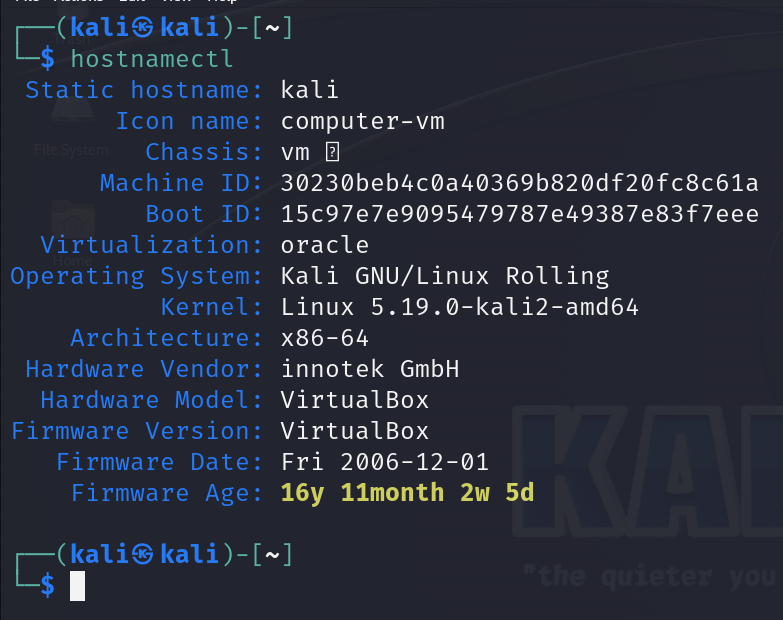
[Ejercicio 3. **¡Error! Marcador no definido.**](#_Toc148985458)

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

# Ejercicios

# Caso 1

**1. ¿Cuál es el nombre del equipo?**



**2. El usuario tenía establecida una conexión FTP con un organismo público. ¿Cuál es?**

**3. Hay por lo menos un proceso que contiene malware. ¿Cuál es su nombre y su PID? Deberás justificar que está infectado.**

**4. Hay un proceso infectado que tiene establecida una conexión HTTPS. ¿Cuál es la dirección**

**IP a la que está conectado? Deberás justificar que es un proceso infectado.**

**5. Hay una contraseña de un fichero comprimido escrita en el bloc de notas. ¿Cuál es?**

**6. Existe un fichero ZIP accesible en la memoria RAM. ¿Qué animal se encuentra dentro?**

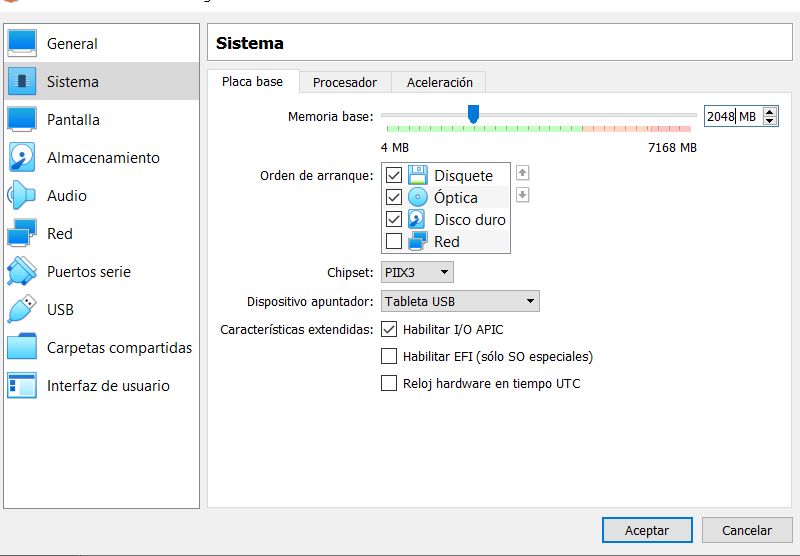
# Caso 2.

Crea una máquina virtual Windows 7. Durante el proceso de instalación de Windows es

recomendable que le des bastantes recursos para que vaya más rápido.

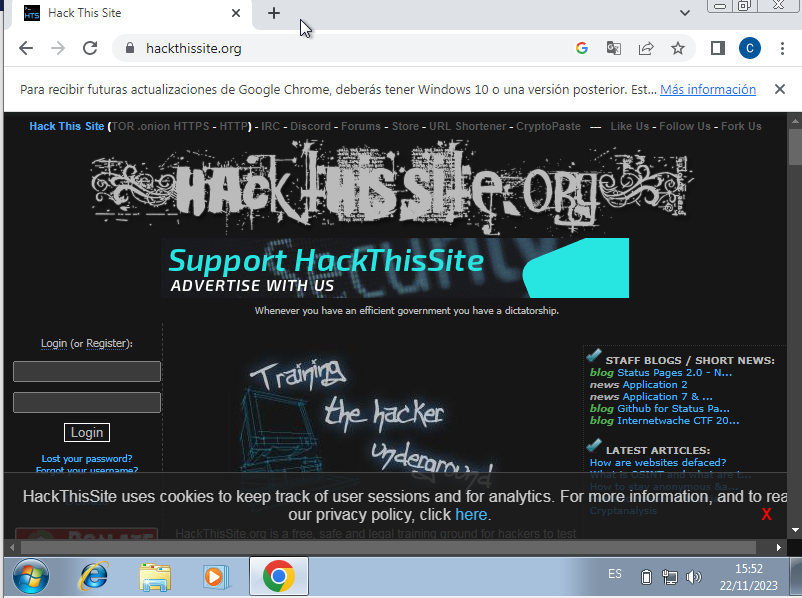
**2. Para la máquina. Asígnale una cantidad no muy grande de RAM (<= 2GB). Vuelve a arrancarla.**

Le ponemos 2048:



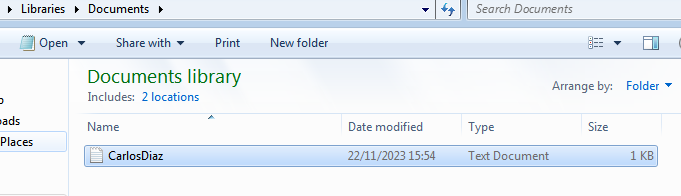
**3. Abre un navegador web y conecta con una página relacionada con hacking.**

Nos conectamos a la pagina web hack this site:

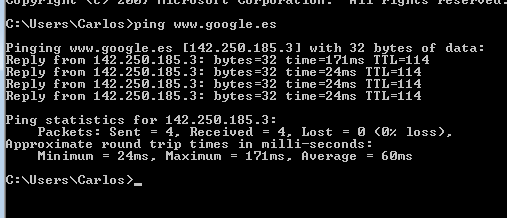


**4. Abre un bloc de notas y escribe un mensaje. Guarda el fichero en la carpeta de documentos.**

Me creo un documento con mi nombre:

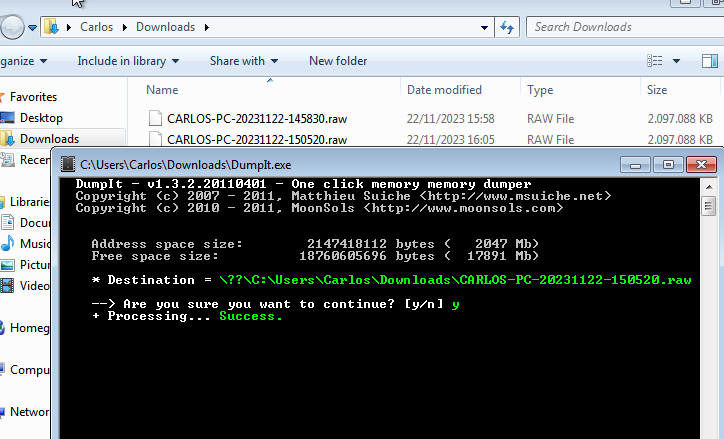


**5. Abre una consola y haz ping a** [**www.google.es**](http://www.google.es)**.**



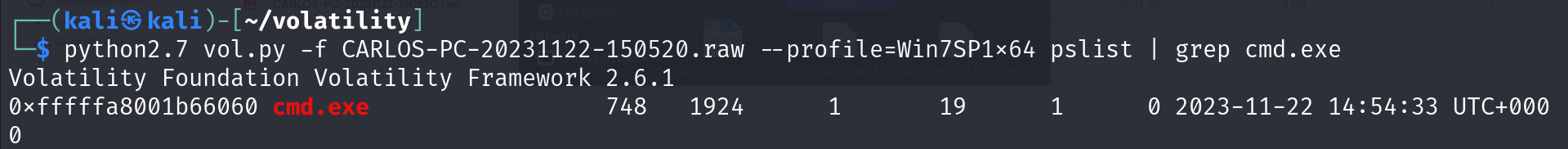
**6. Sin cerrar el navegador ni el bloc ni la consola, realiza una adquisición de memoria de la máquina mediante una herramienta como DumpIt o similar.**

Nos descargamos Dumplt y una vez lo ejecutamos podemos encontrar un raw:

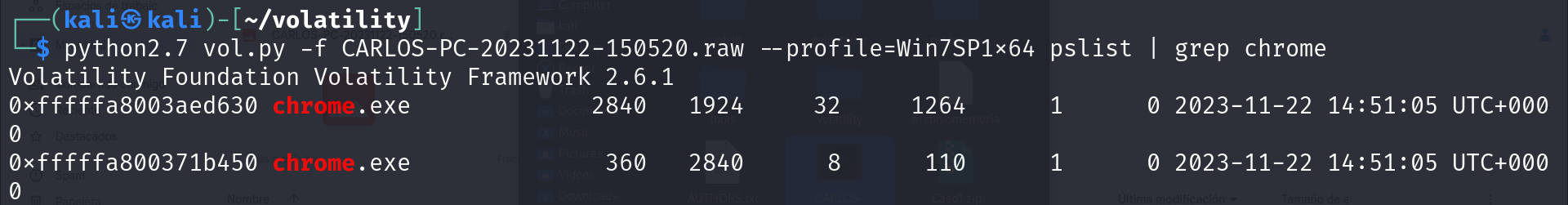


**7. Con Volatility, comprueba que encuentras los procesos del Bloc de Notas, el navegador Web y la consola.**

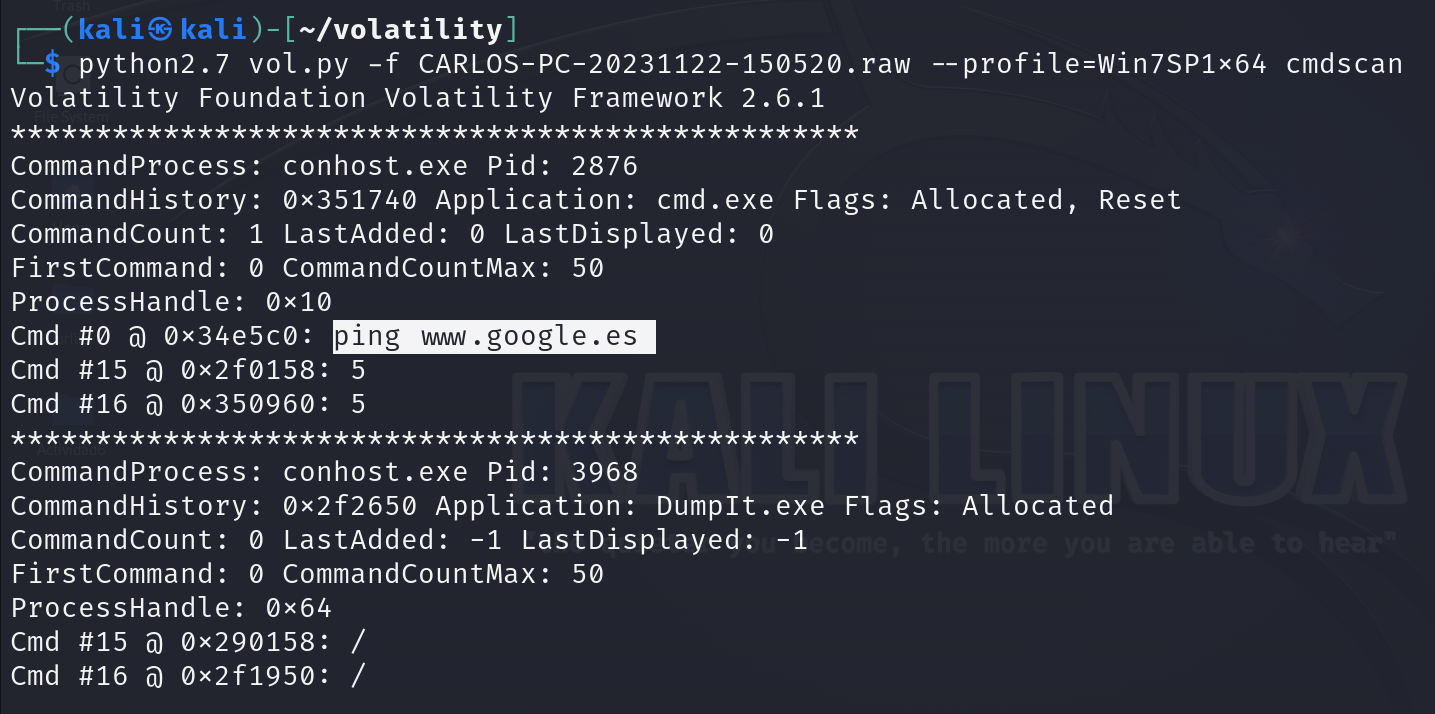
El de la consola:



Los del navegador:

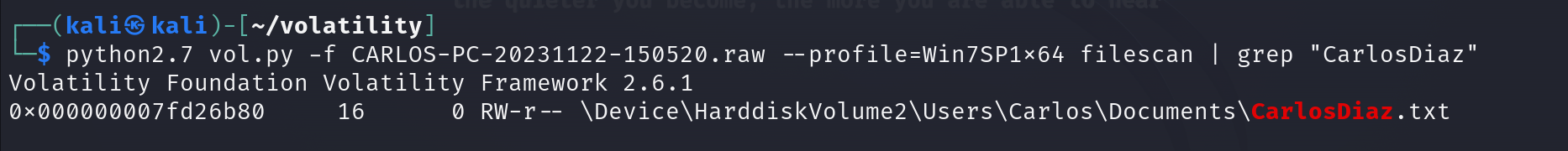


**8. Comprueba si puedes averiguar el comando que se estaba ejecutando en la consola.**



**9. Comprueba si puedes averiguar el texto que estaba en el bloc de notas.**

Primero confirmamos que existe el documento:



Ahora miramos el contenido del documento:

**10. Comprueba que encuentras la conexión de red a la página de hacking y la conexión del ping.**