

Análisis forense

Unidad 1. Actividad 3



13 de Noviembre de 2023

Carlos DÍAZ MONTES

ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

[1. ¿Cuál es el hash SHA-1 del archivo memory-triage.mem? 2](#_Toc150791256)

[2. ¿Cuál es el perfil más apropiado para la máquina? 2](#_Toc150791257)

[3. ¿Cuál es el PID del proceso notepad.exe? 2](#_Toc150791258)

[4. Nombre del proceso hijo de wscript.exe. 2](#_Toc150791259)

[5. ¿Cuál era la dirección IP de la máquina en el momento en el que se hizo la imagen de memoria? 2](#_Toc150791260)

[6. Basándose en la respuesta relacionada con el PID infectado ¿Cuál es la IP del atacante? 3](#_Toc150791261)

[7. ¿Cuál es el nombre del proceso relacionado con la librería VCRUNTIME140.dll? 3](#_Toc150791262)

[8. ¿Cuál es el valor del hash MD5 del potencial malware en el sistema? 4](#_Toc150791263)

[9. ¿Cuál es el hash LM de la cuenta de Bob? 4](#_Toc150791264)

[10. ¿Qué protecciones tiene el nodo VAD en la dirección 0xfffffa800577ba10? 4](#_Toc150791265)

[11. ¿Qué protecciones tenía el nodo VAD que empieza en la dirección 0x00000000033c0000 y 4](#_Toc150791266)

[termina en la dirección 0x00000000033dffff? 4](#_Toc150791267)

[12. Hubo un script VBS corriendo en la máquina. ¿Cuál es el nombre del script (sin extensión)? 5](#_Toc150791268)

[13. Se ejecutó una aplicación el 2019-03-07 23:06:58 UTC. ¿Cuál es el nombre del programa? 5](#_Toc150791269)

[14. ¿Qué estaba escrito en el notepad.exe en el momento de la captura de memoria? 5](#_Toc150791270)

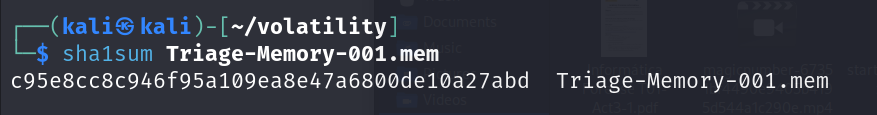
[15. ¿Cuál es el nombre corto del archivo en el registro 59045? 6](#_Toc150791271)

[16. Este equipo ha sido comprometido y tiene una sesión de meterpreter. ¿Qué PID ha sido 6](#_Toc150791272)

[infectado? 6](#_Toc150791273)

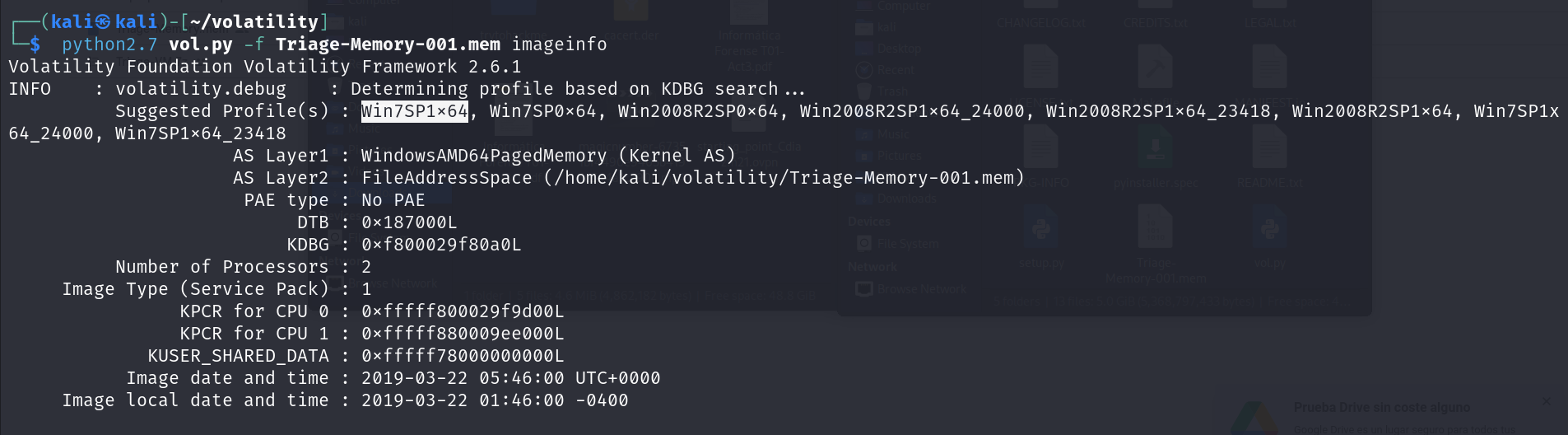
# 1. ¿Cuál es el hash SHA-1 del archivo memory-triage.mem?

Usamos el comando sha1sum (nombre del archivo):



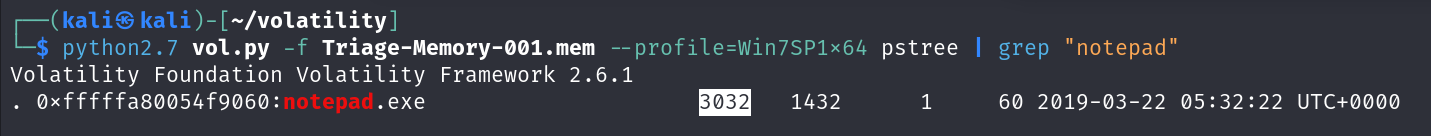
# 2. ¿Cuál es el perfil más apropiado para la máquina?

Usamos el comando python2.7 vol.py -f (nombre del archivo) imageinfo y como vemos es Win7SP1X64Bits:



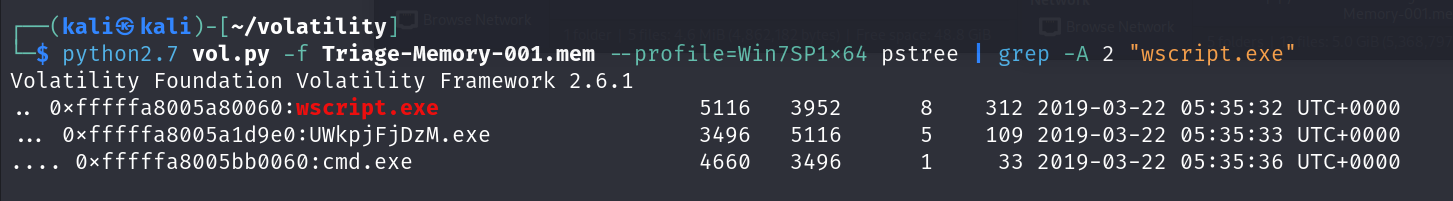
# 3. ¿Cuál es el PID del proceso notepad.exe?

Usamos el comando python2.7 vol.py -f (nombre del archivo) –profile=Win7SP1X64 pstree | grep “notepad”, como vemos la respuesta es el 3032:



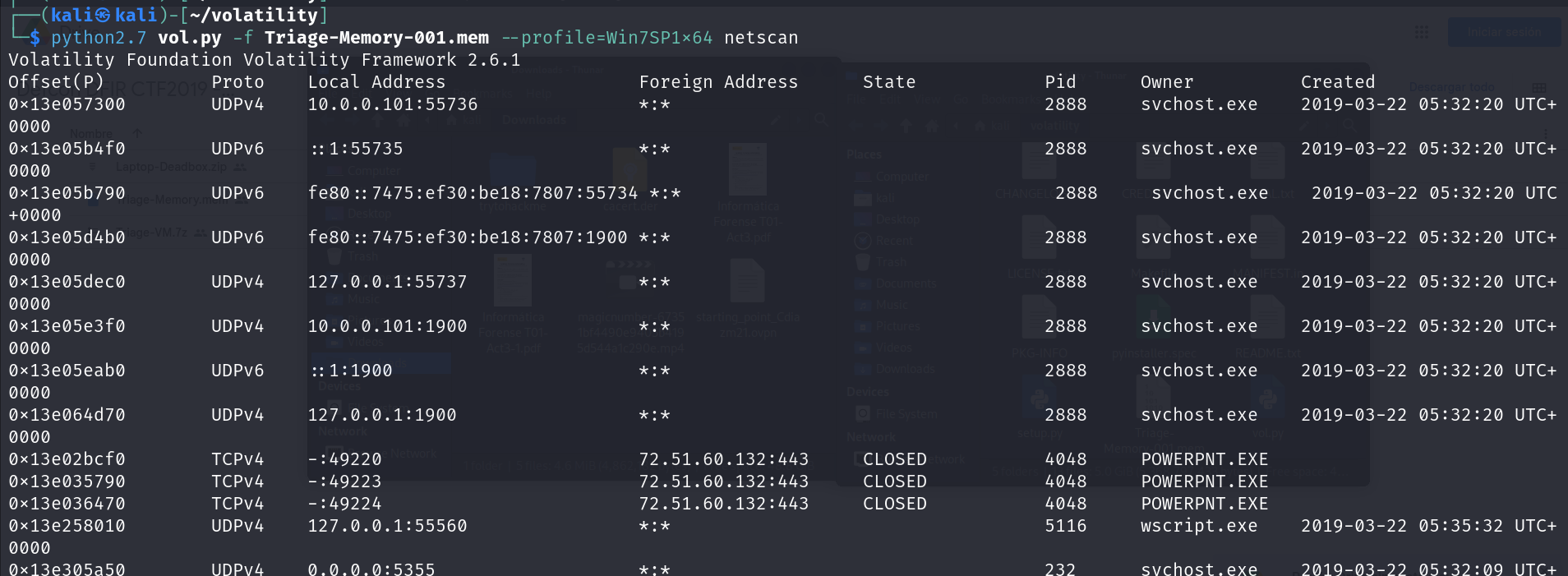
# 4. Nombre del proceso hijo de wscript.exe.

Usamos el comando python2.7 vol.py -f (nombre del archivo) -–profile=Win7SP1x64 pstree | grep -A 2 “wscript.exe”, como vemos se llama:



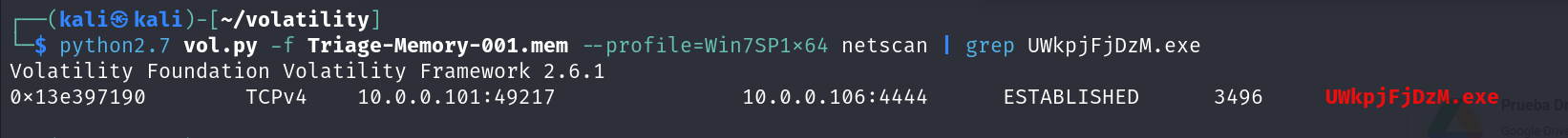
# 5. ¿Cuál era la dirección IP de la máquina en el momento en el que se hizo la imagen de memoria?

Para ver la ip que tenia en el momento de la imagen es 10.0.0.101:



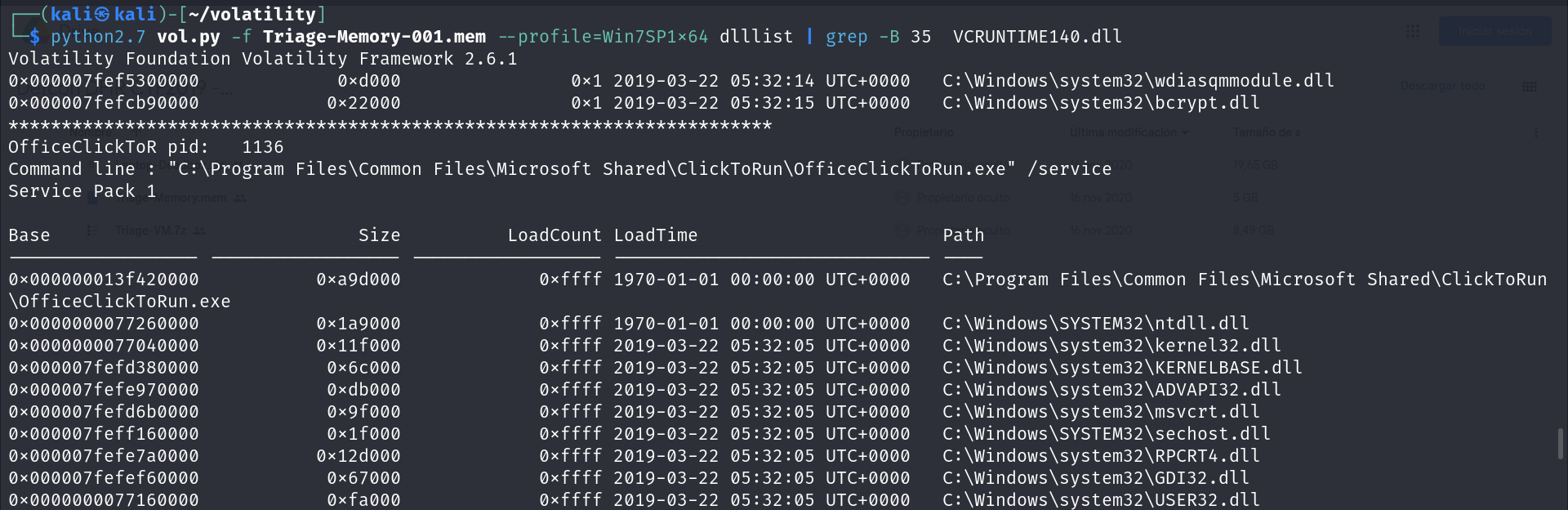
# 6. Basándose en la respuesta relacionada con el PID infectado ¿Cuál es la IP del atacante?

La ip del atacante es 10.0.0.106:



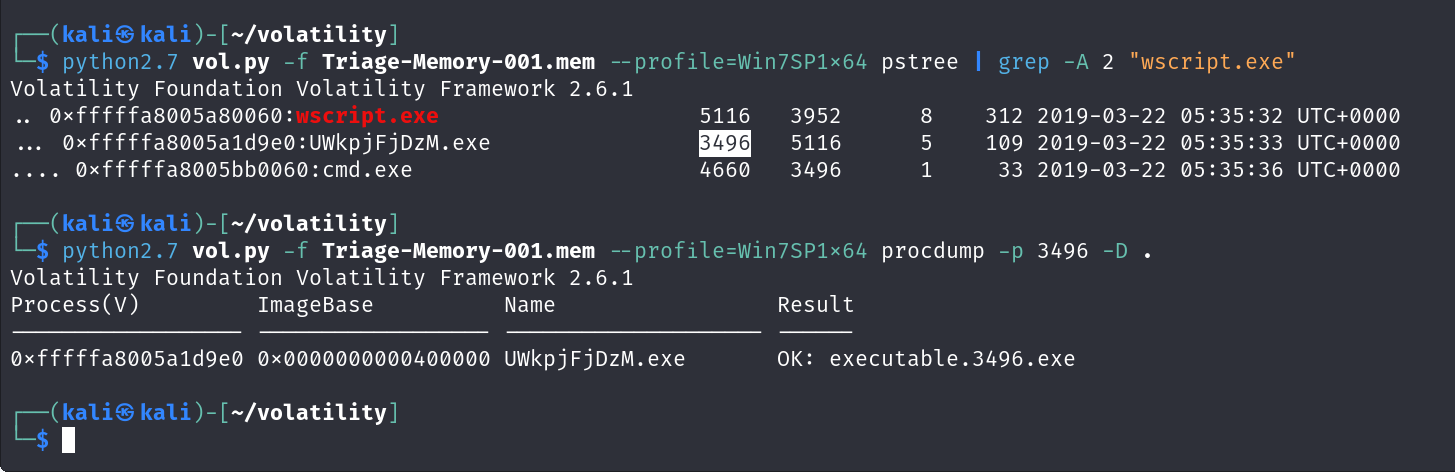
# 7. ¿Cuál es el nombre del proceso relacionado con la librería VCRUNTIME140.dll?

El nombre del proceso relacionado es officeclicktorun



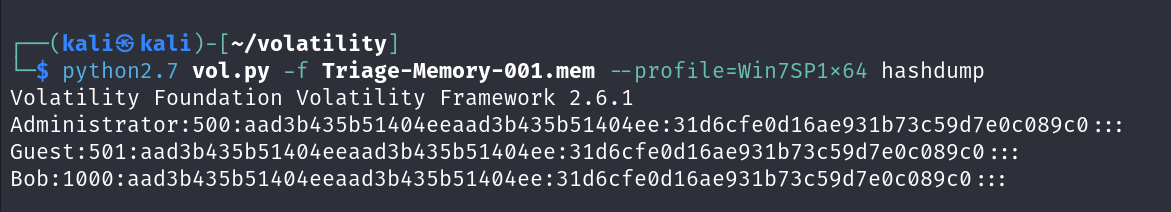
# 8. ¿Cuál es el valor del hash MD5 del potencial malware en el sistema?

Es el 3496:

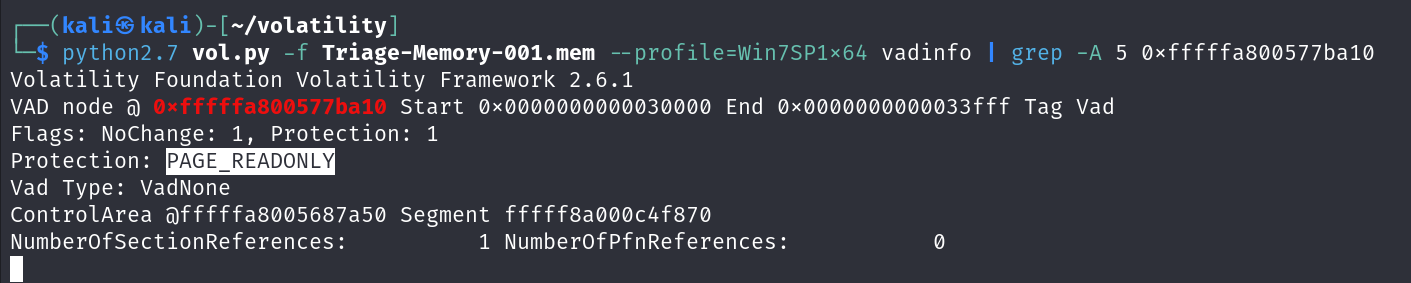




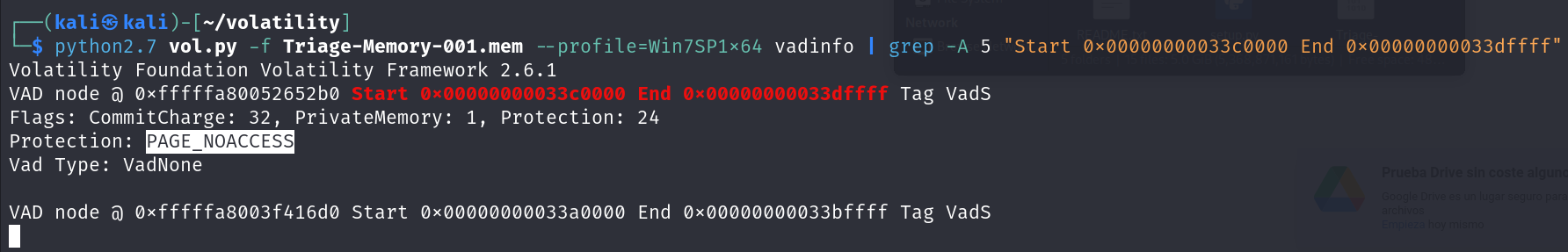
# 9. ¿Cuál es el hash LM de la cuenta de Bob?



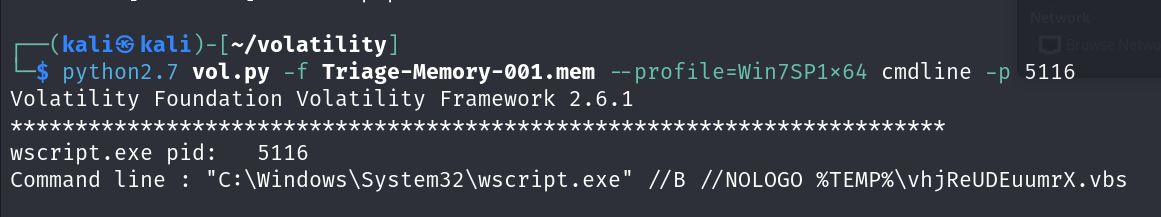
# 10. ¿Qué protecciones tiene el nodo VAD en la dirección 0xfffffa800577ba10?



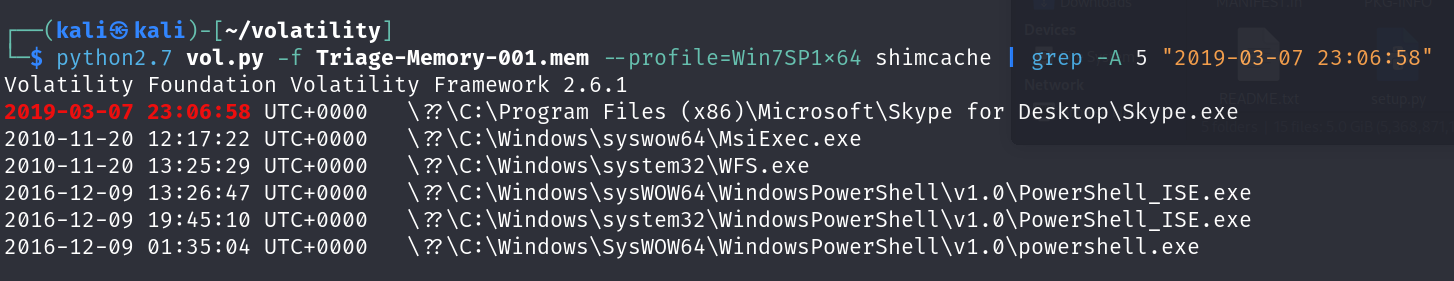
# 11. ¿Qué protecciones tenía el nodo VAD que empieza en la dirección 0x00000000033c0000 y termina en la dirección 0x00000000033dffff?



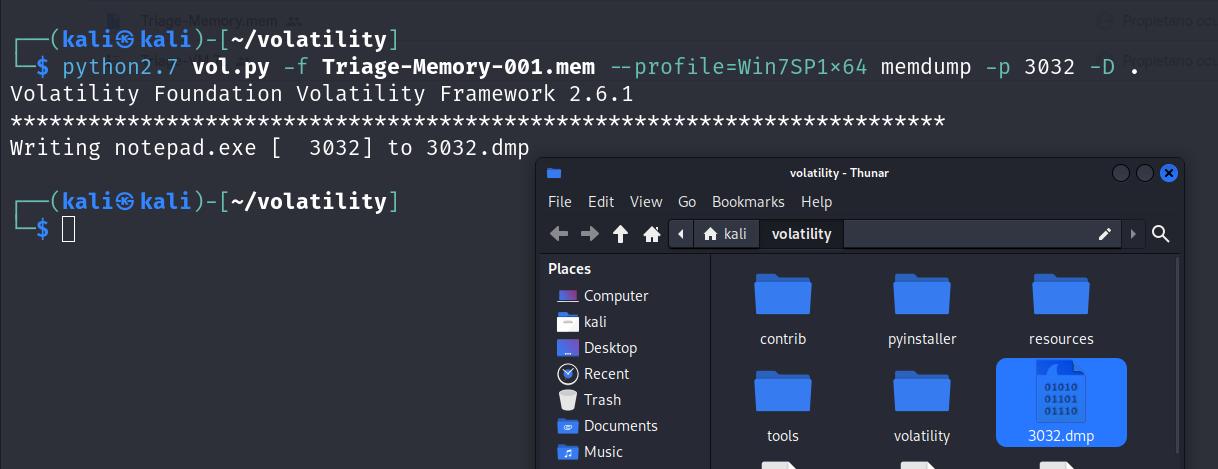
# 12. Hubo un script VBS corriendo en la máquina. ¿Cuál es el nombre del script (sin extensión)?



# 13. Se ejecutó una aplicación el 2019-03-07 23:06:58 UTC. ¿Cuál es el nombre del programa?

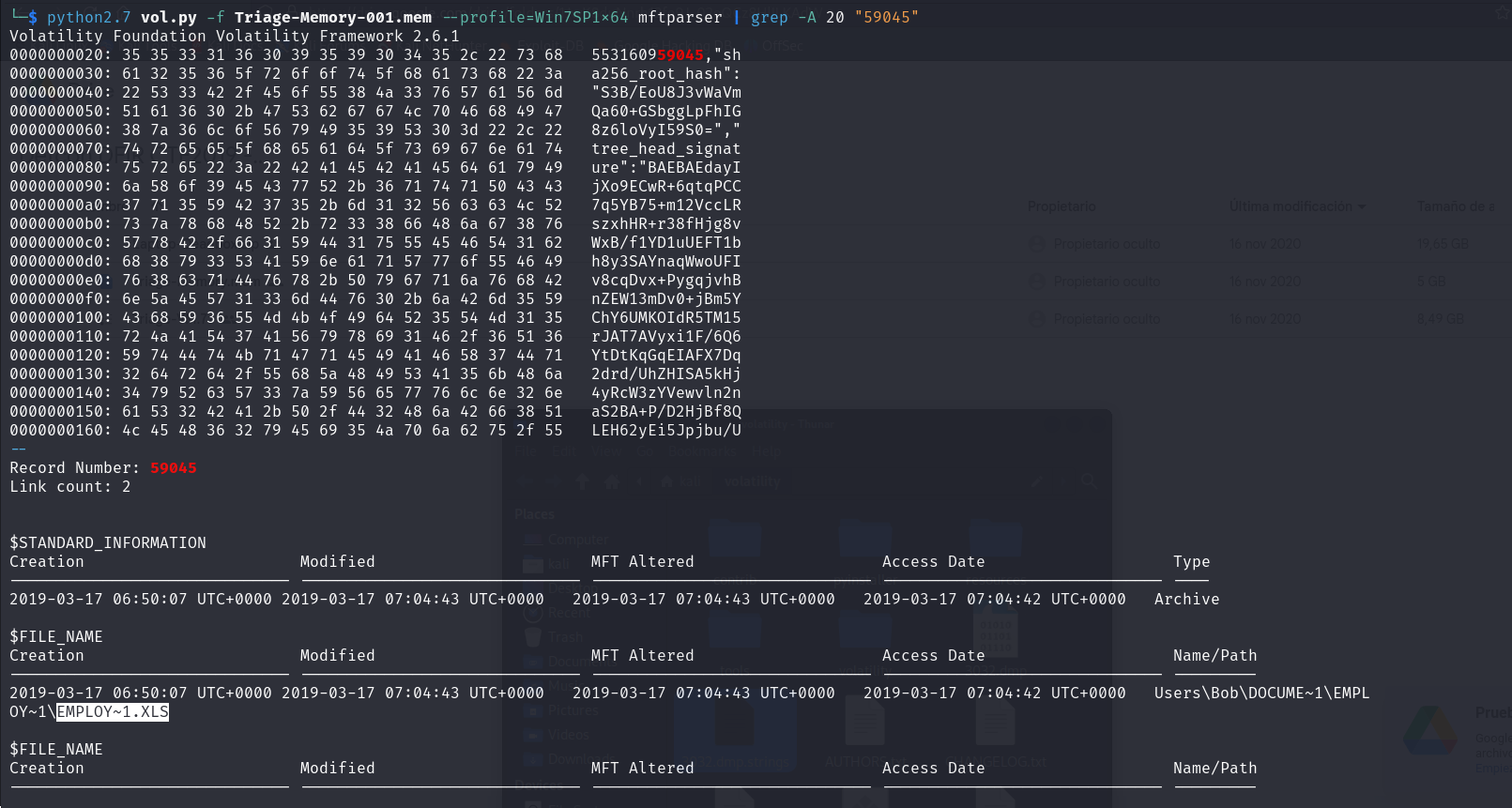


# 14. ¿Qué estaba escrito en el notepad.exe en el momento de la captura de memoria?



# 

# 15. ¿Cuál es el nombre corto del archivo en el registro 59045?



# 16. Este equipo ha sido comprometido y tiene una sesión de meterpreter. ¿Qué PID ha sido infectado?

