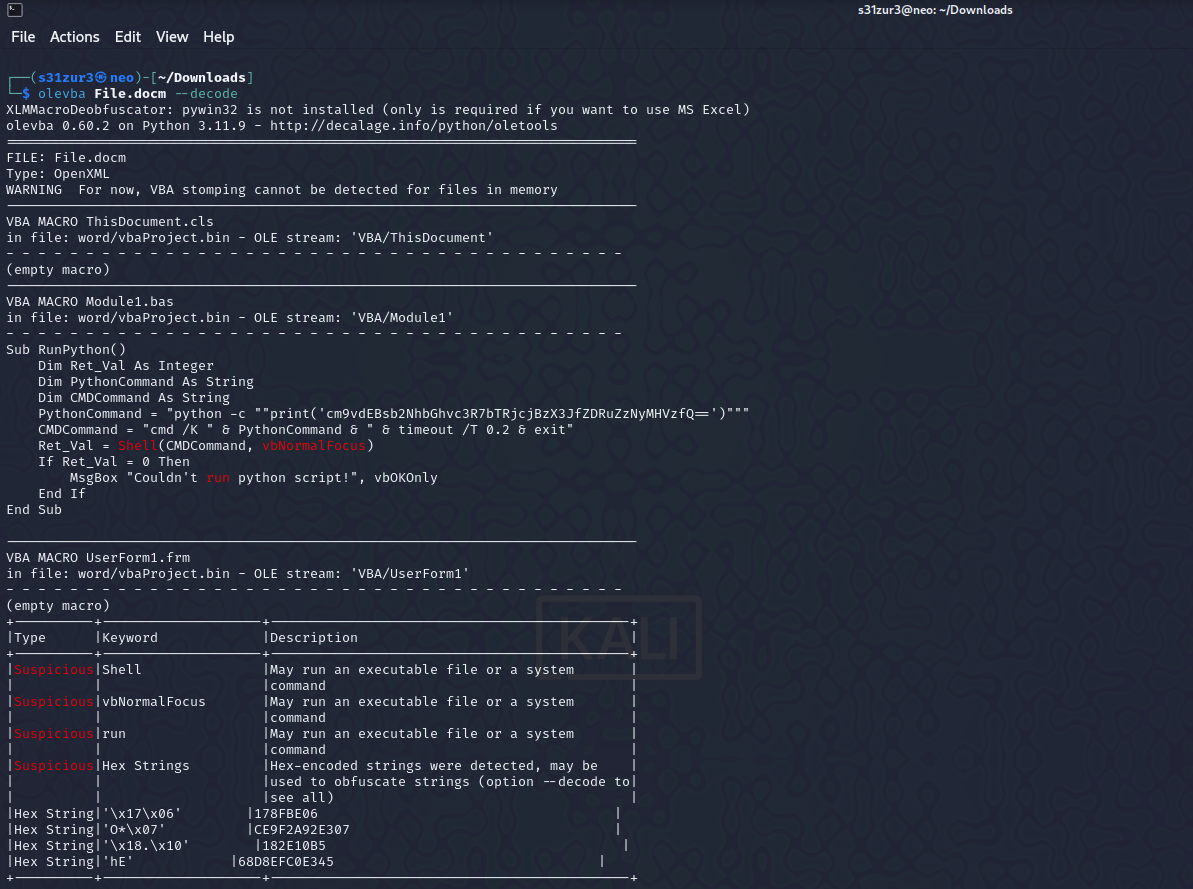
**Decrypting the Ransom: Malicious DOCM Analysis**

**Tools Used:**

Oletools

Base64 decoder

**Steps:**

1. Use “olevba File.docm” to check for any malicious macros. 
2. Decode the string using base 64

**Flag:** root@localhost{m4cr0s\_r\_d4ng3r0us}

**Avengers**

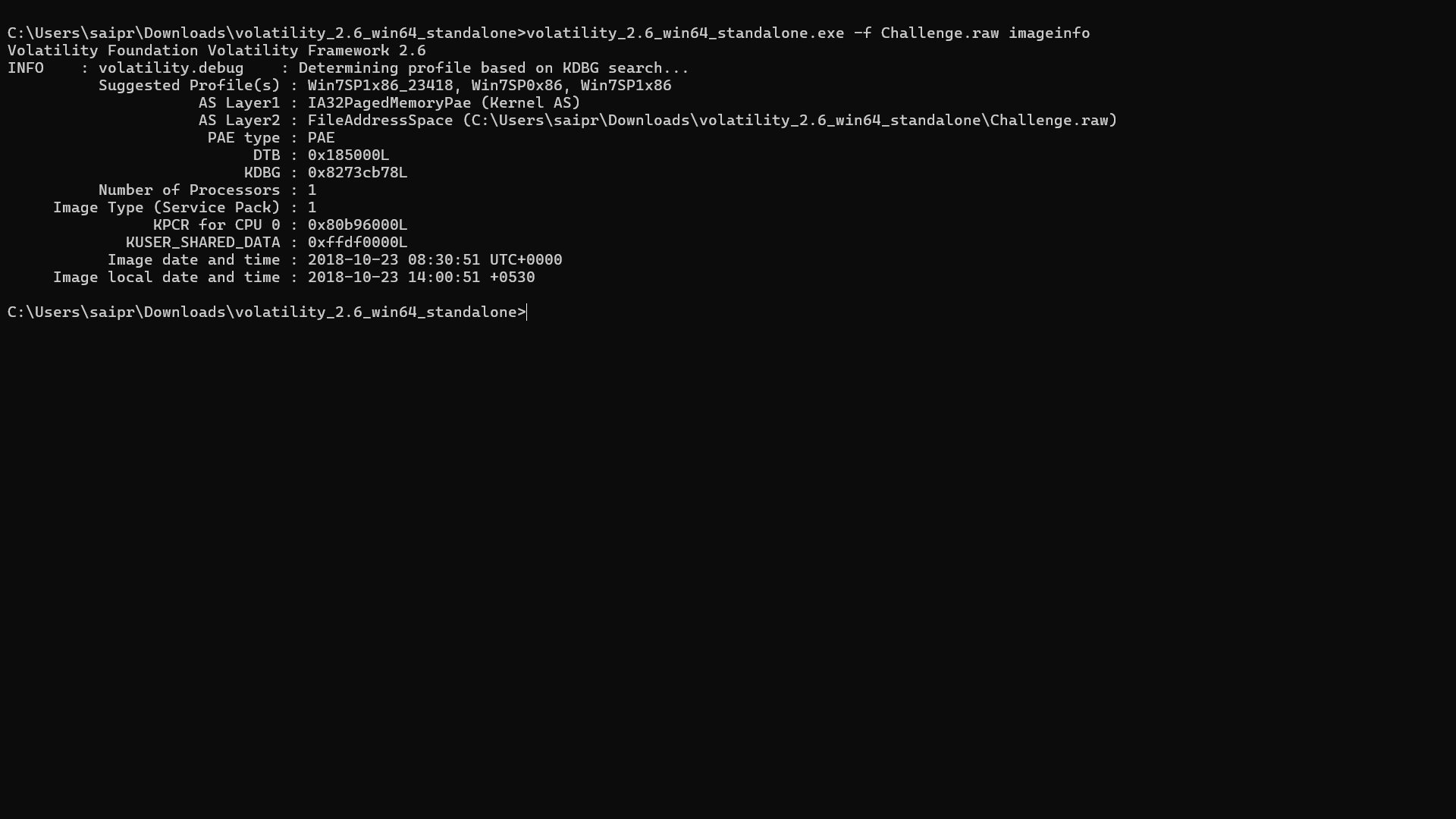
**Tools Used:**

Volatility

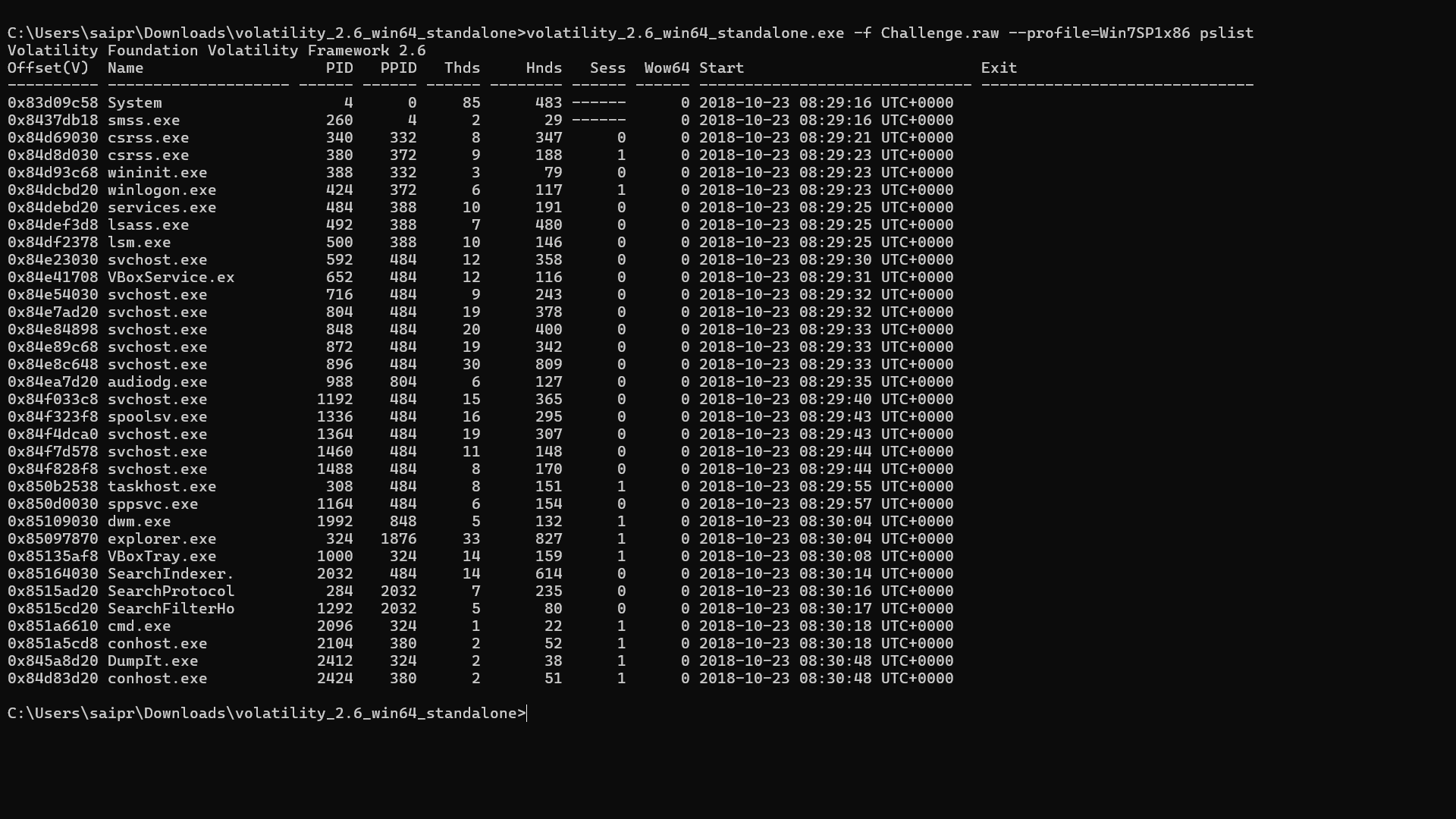
CyberChef

**Steps:**

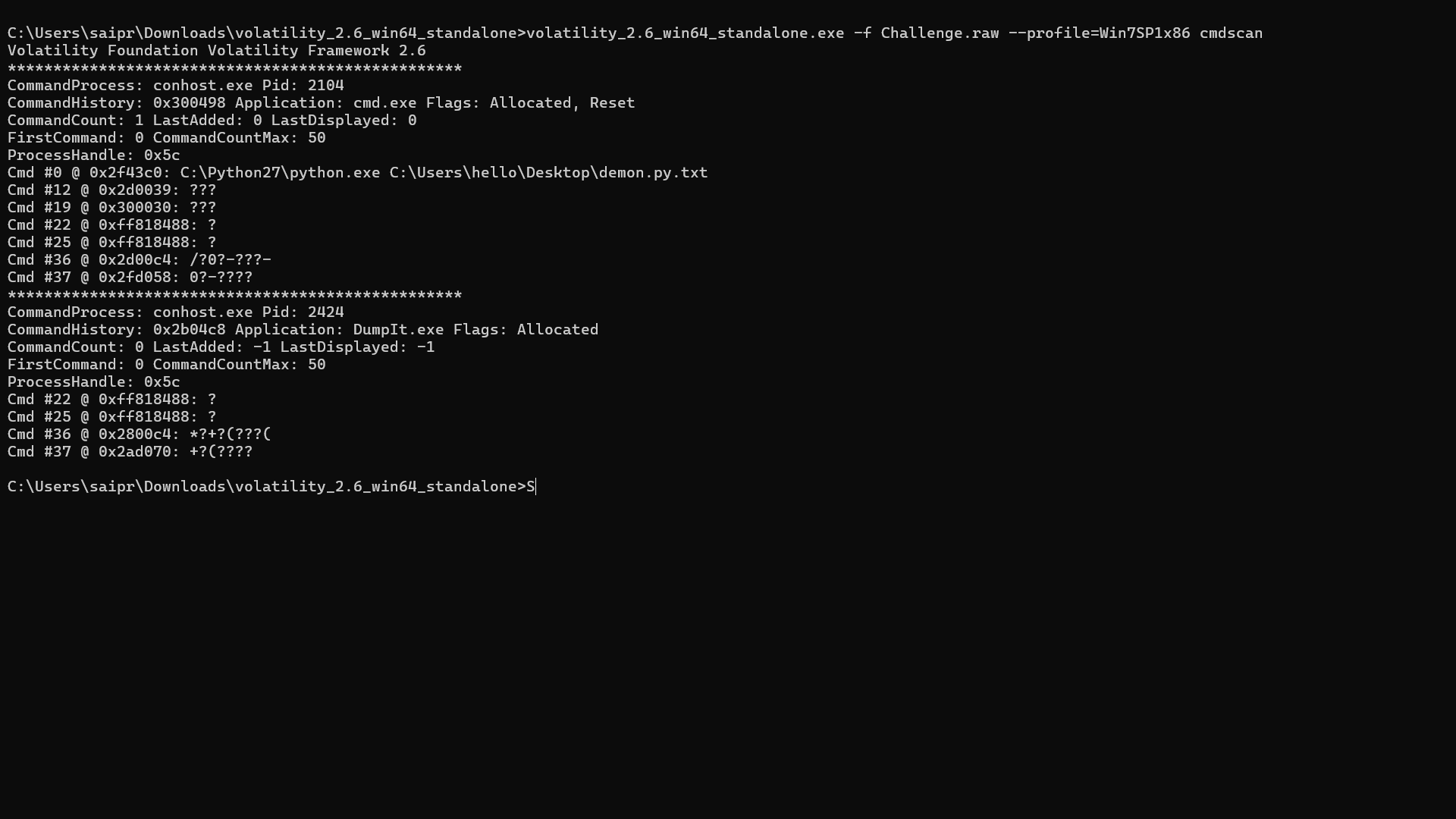
1. Type the cmd “volatility\_2.6\_win64\_standalone.exe -f Challenge.raw imageinfo” to get the profiles and info on the file.



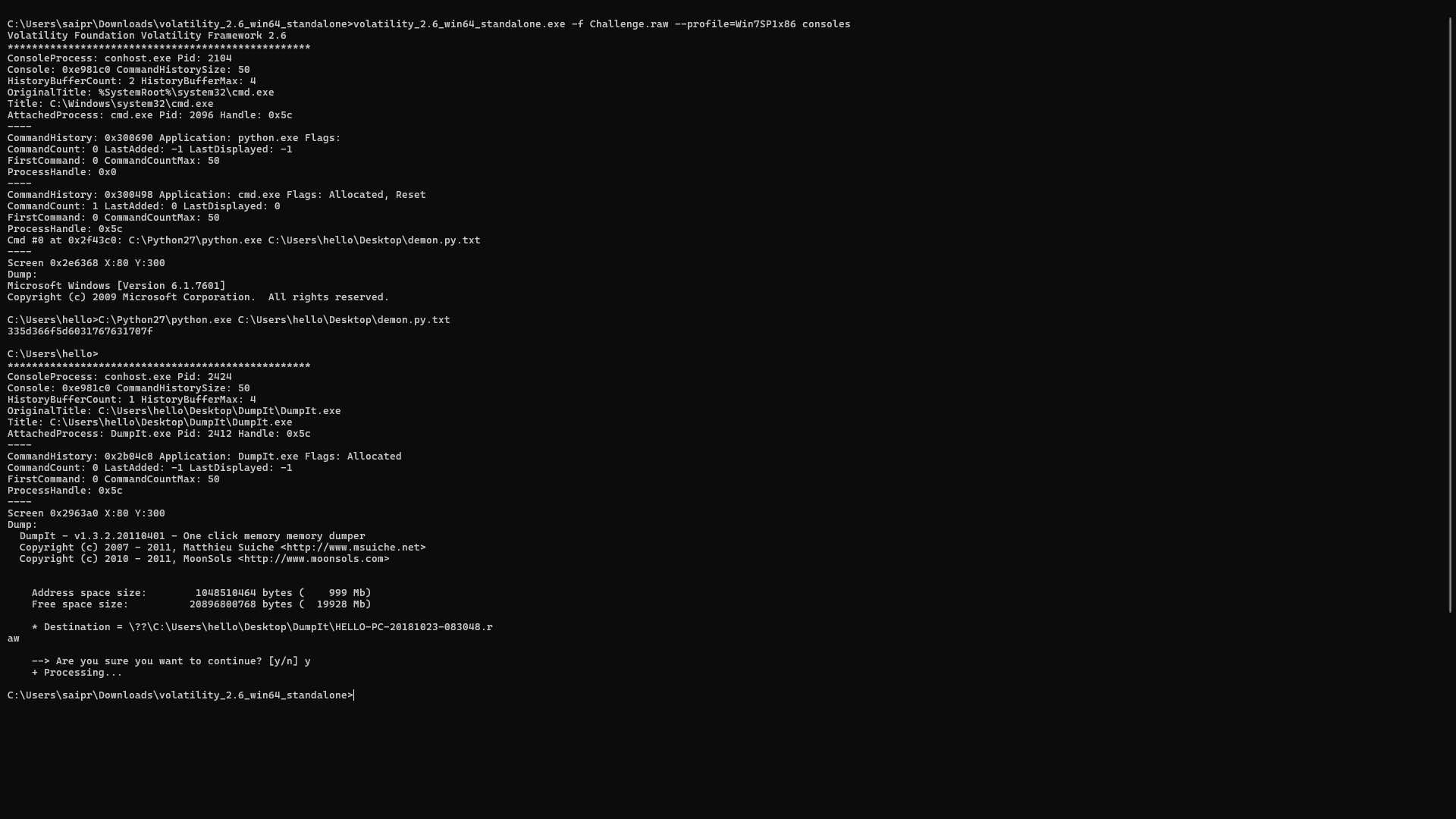
1. Use the cmd “volatility\_2.6\_win64\_standalone.exe -f Challenge.raw --profile=Win7SP1x86 pslist” to get list of process that was running.



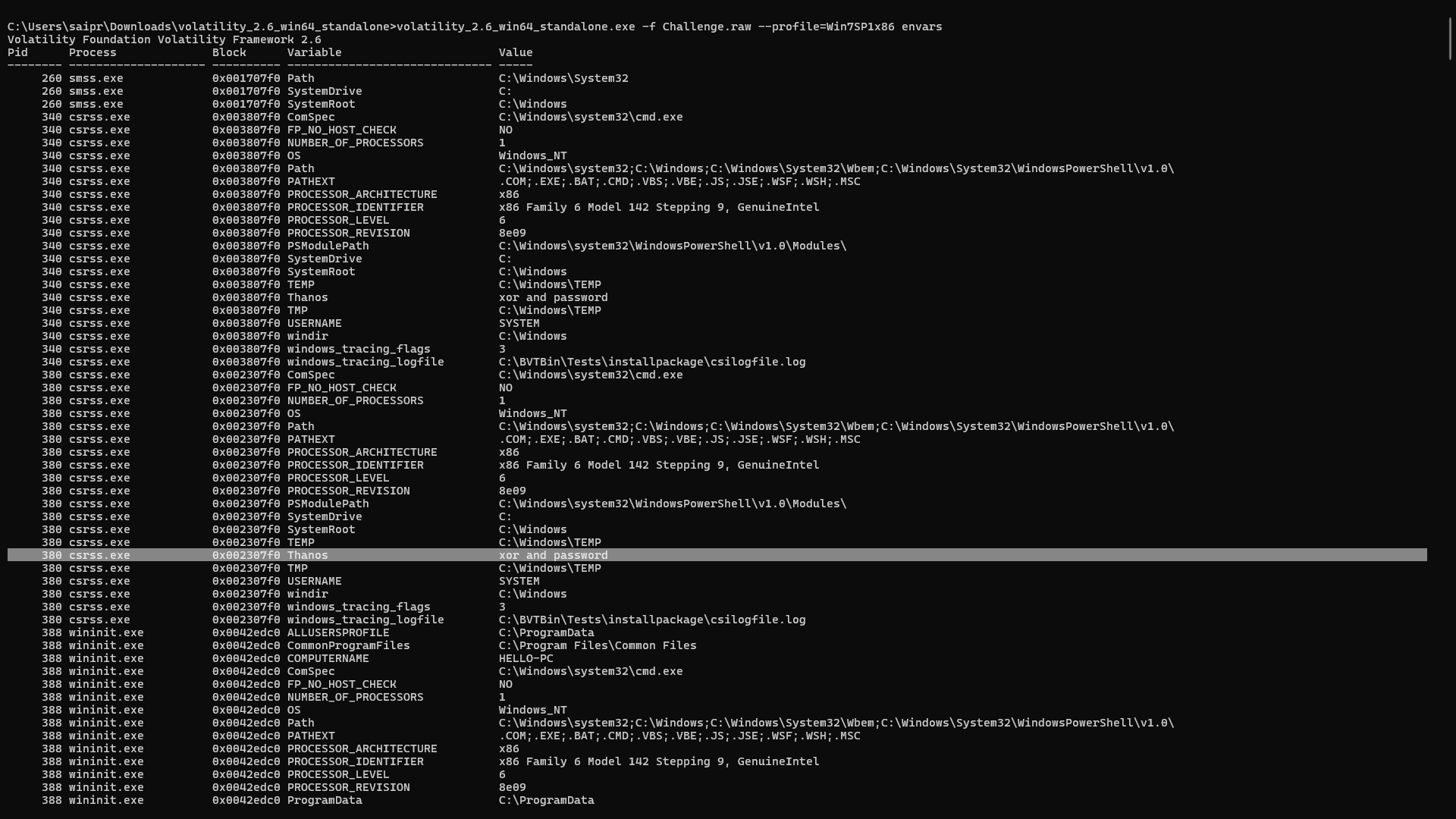
1. Use the cmd “volatility\_2.6\_win64\_standalone.exe -f Challenge.raw --profile=Win7SP1x86 cmdscan”. We see that 2 cmds were run on the machine ones is a python file and another is a memory dump software.



1. Now use the cmd “ volatility -f Challenge.raw --profile=Win7SP1x86 consoles” to get the contents of the commands run.



1. There is a encoded string in the python file. Now we decode it. We get a not meaningful message “3]6o]`1vv1p”. In the question they have given us three hints. He is an environment activist which can also mean environment variables, he hates thanos and used lot of variables. We now use “volatility\_2.6\_win64\_standalone.exe -f Challenge.raw --profile=Win7SP1x86 envars” to view environment variables.



1. The hint that he hates Thanos gives us a variable of the same name. We need to find the password. So we use hashcat.

**Flag:** flag{you\_are\_good\_but1\_4m\_b3tt3r}