National University
of computer and emerging sciences

Lab 14

CYL2002 Digital Forensics - Lab

Name : Mirza Humayun Masood(i22-1749)

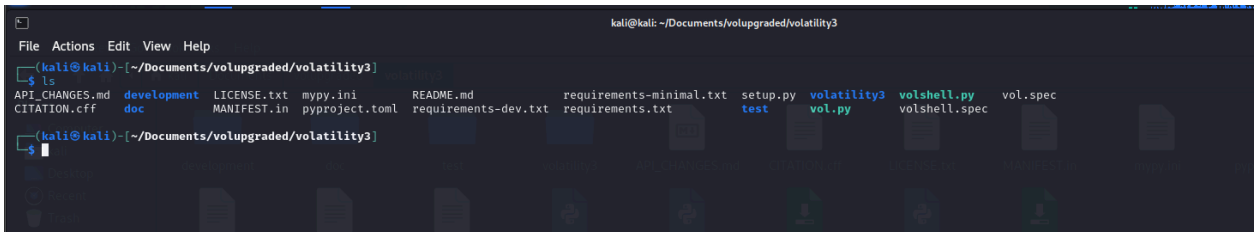
Section : CY-A

Submitted to: Sir Ubaid Ullah

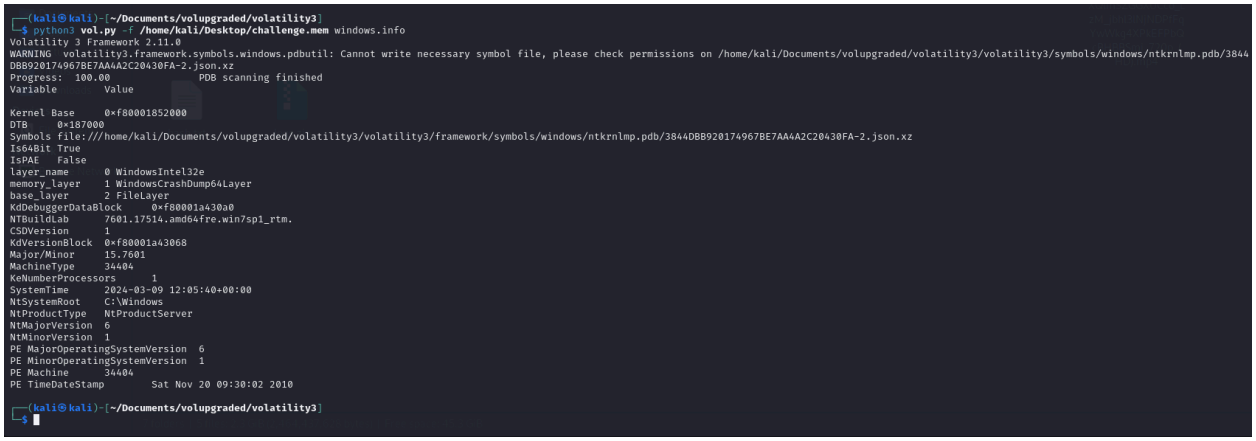
Department of Cyber Security BS(CY)

FAST-NUCES Islamabad

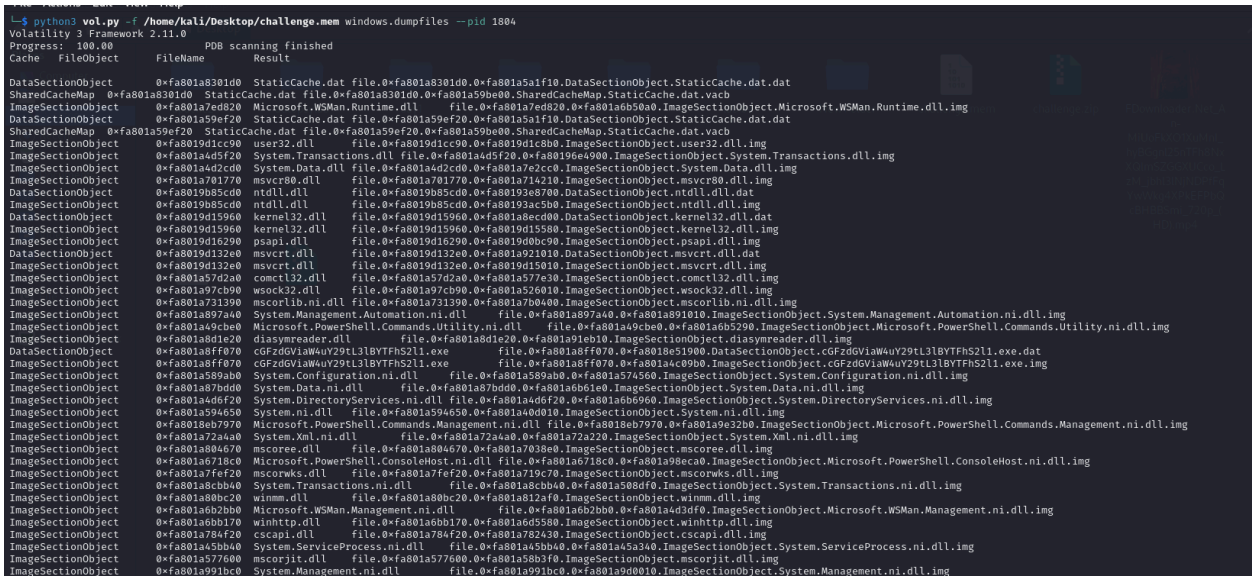
In this lab task , we were given a memory dump, so after installing volatility3, it showed.



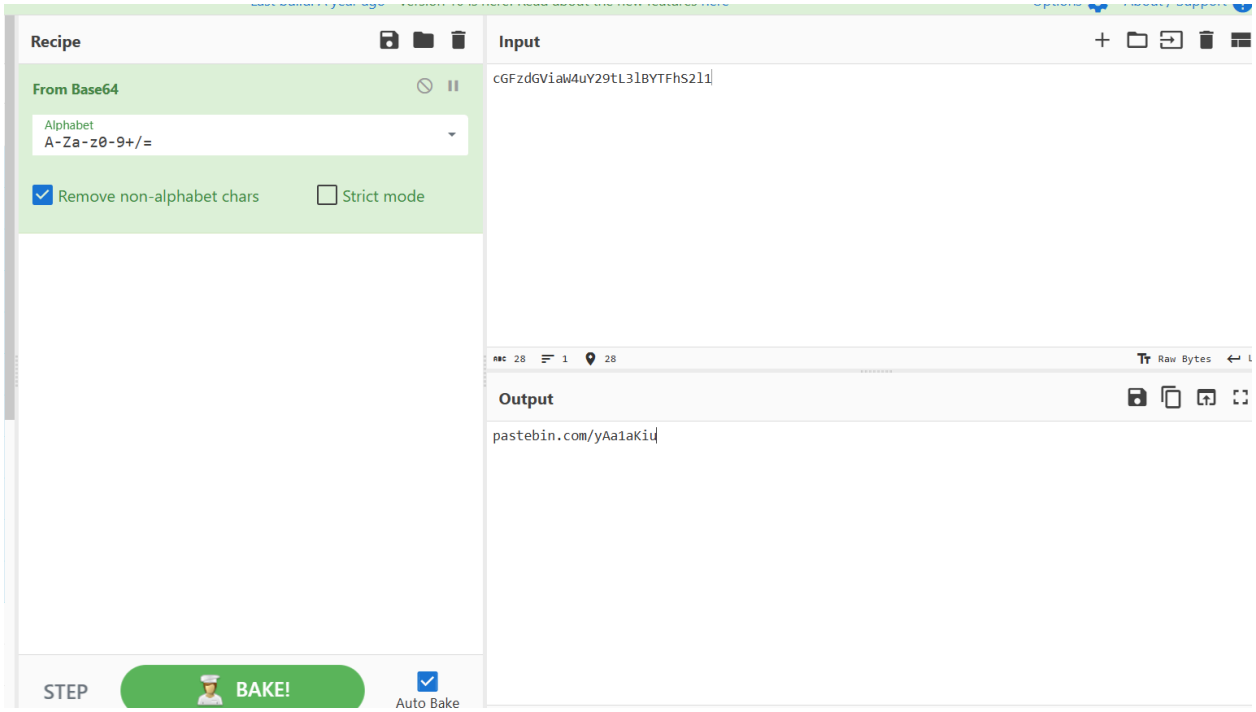
Then I tried the command to identify the windows version.

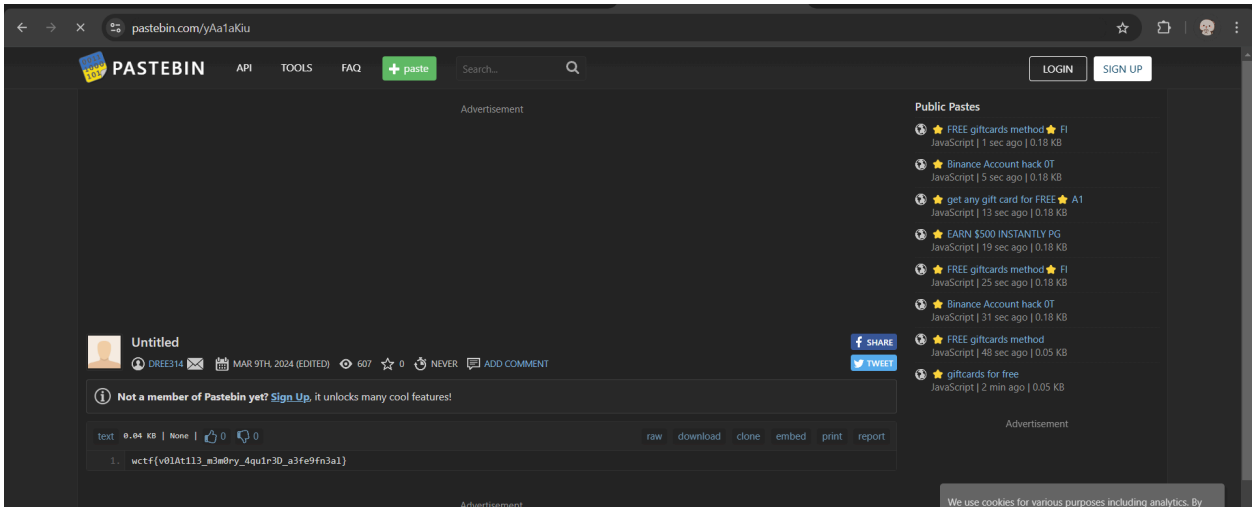


Then i ran psutil to see all the processes, and found a suspicious process, with pid 1804., then i tried to see its dump



It was found that a random .exe file was running , and i opened cyberchef to see its name, so there was a link, as soon as i opened the link the flag was there.





wctf{v0lAt1l3_m3m0ry_4qu1r3D_a3fe9fn3al}