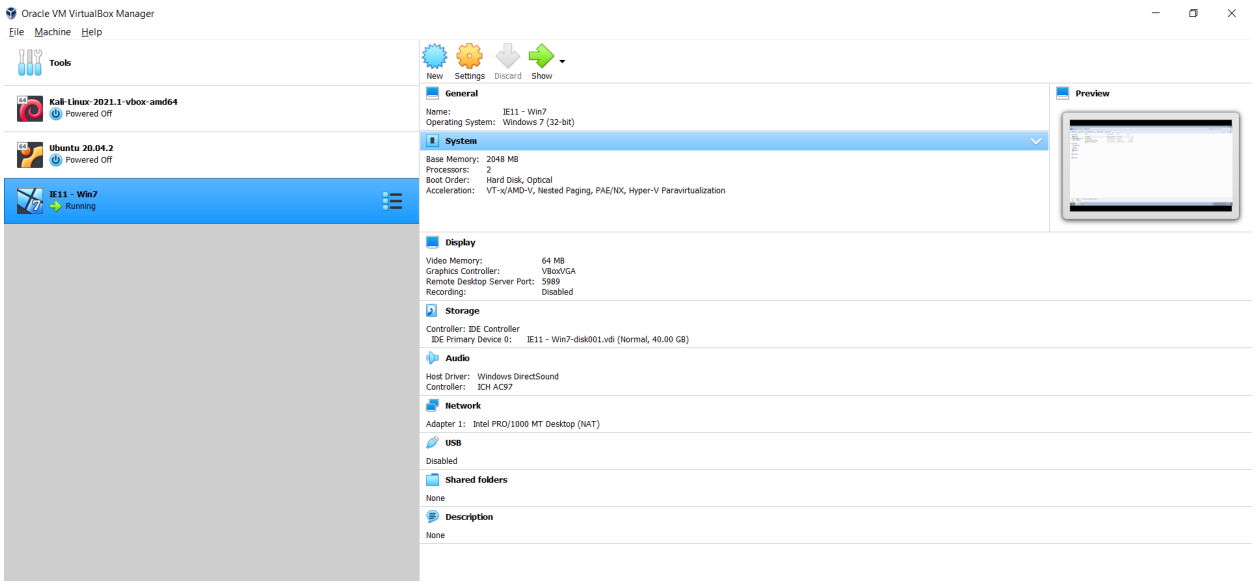
SECURE CODING LAB

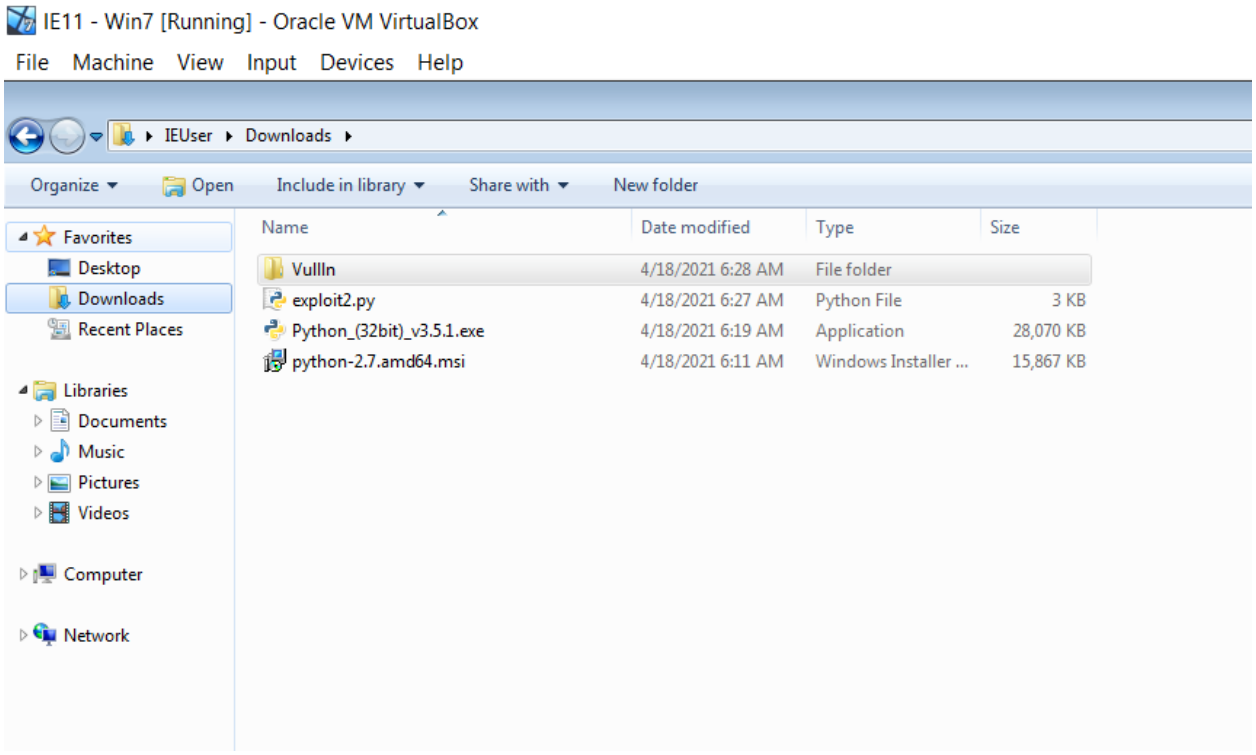
TOPIC : Working With Memory Vulnerabilities

RISHAB BANTHIA 18BCN7076

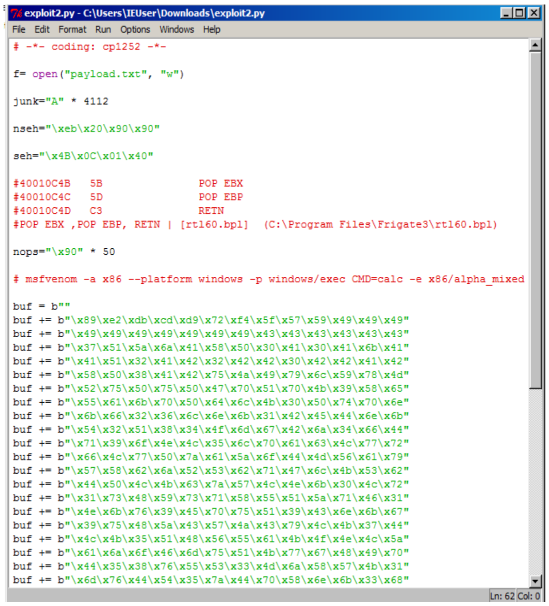
Opened the windows 7 on virtual machine and downloaded the vuln file and extracted it

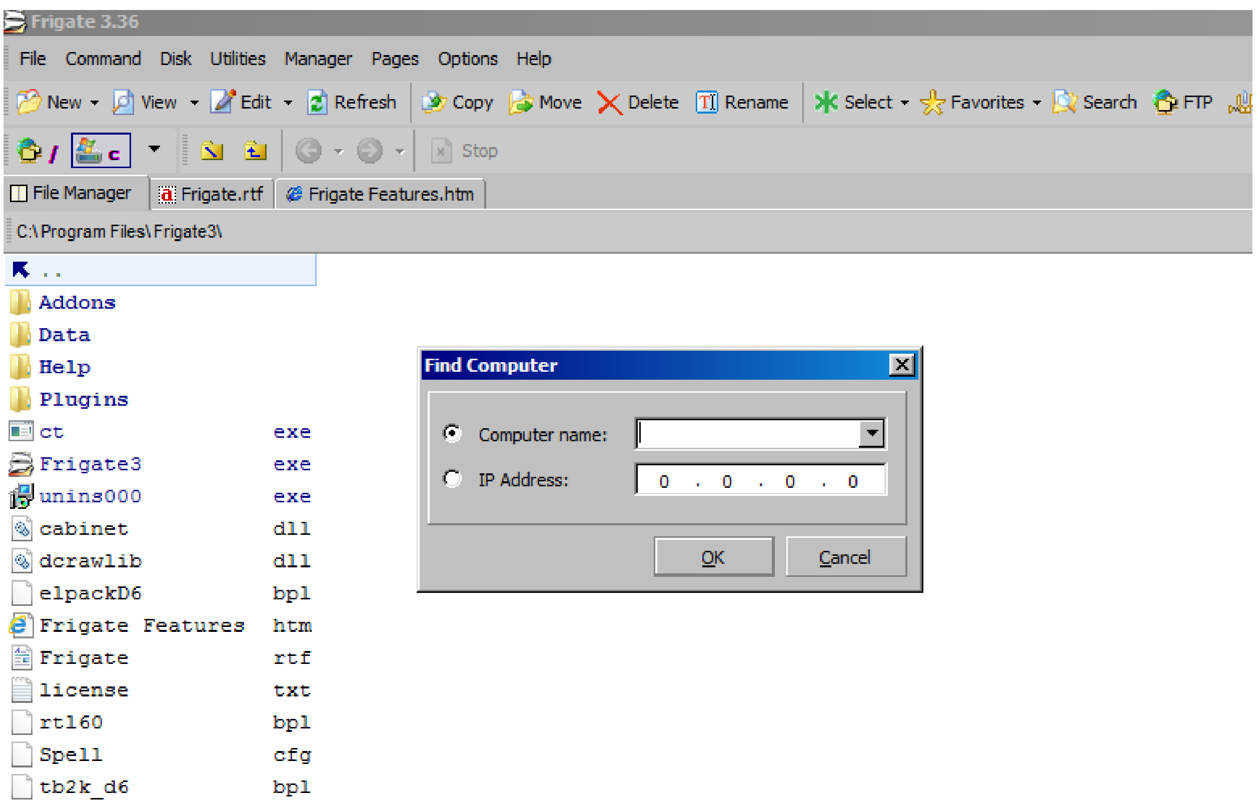


Downloaded python 2.7 and unzipped the Vulln file

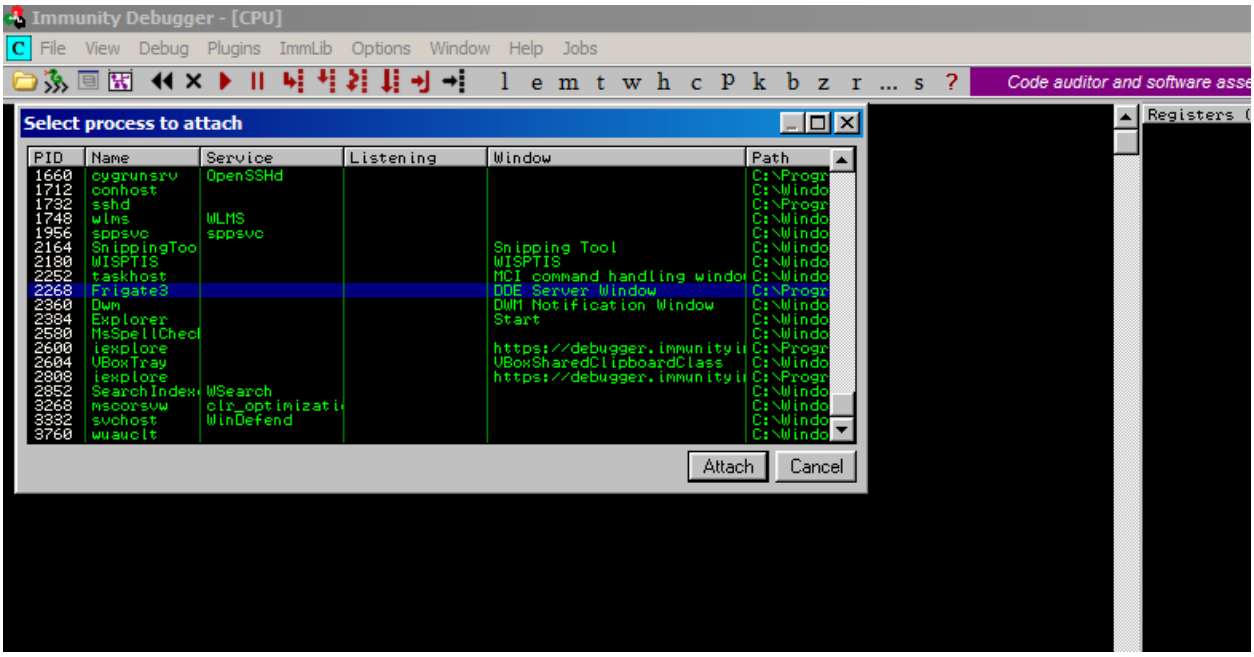


Running the exploit script 2 to generate the payload

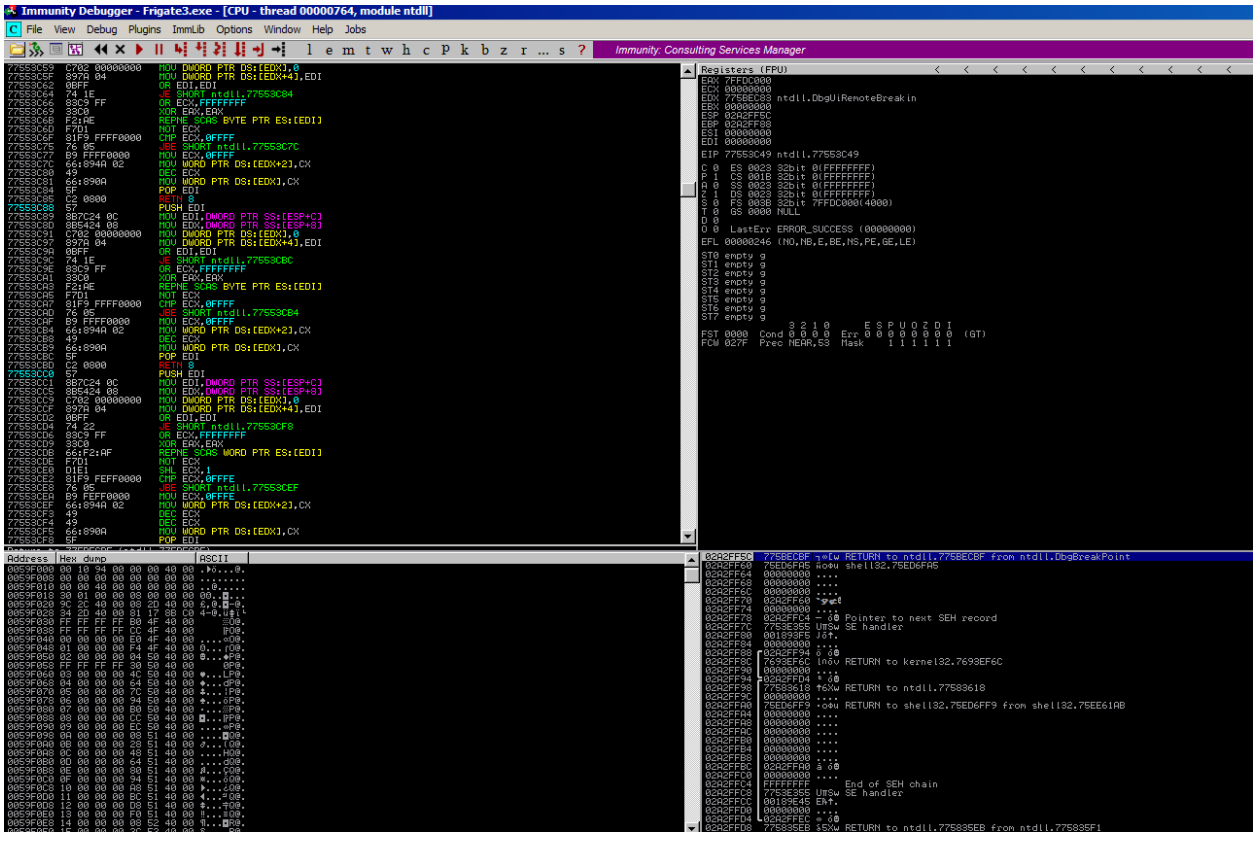




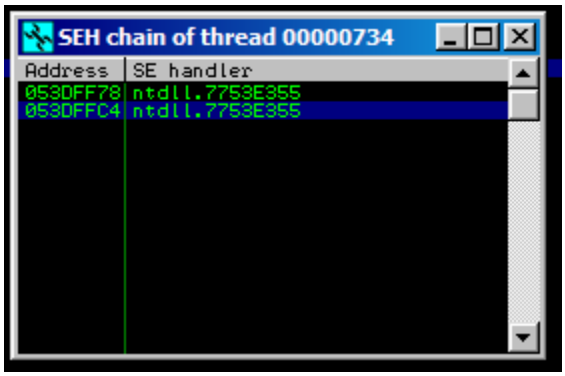
Attaching frigate to immunity debugger



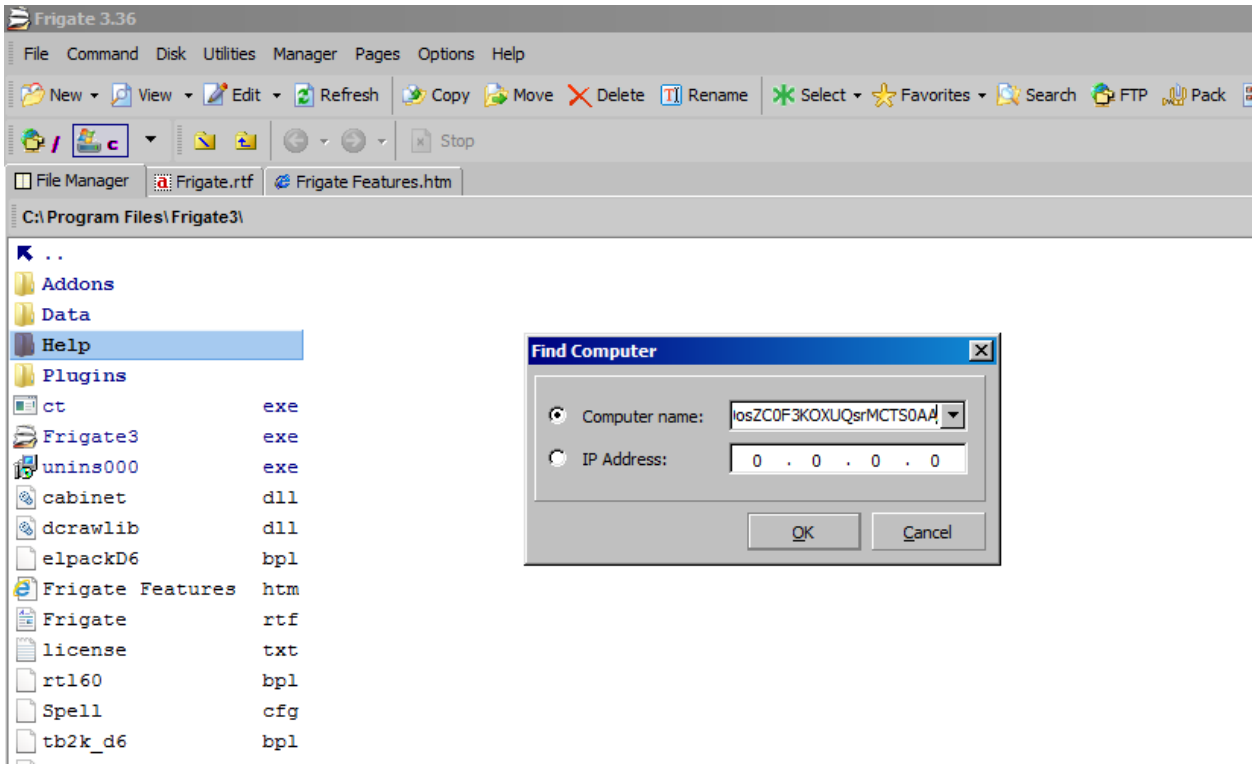
After attaching frigate to immunity debugger



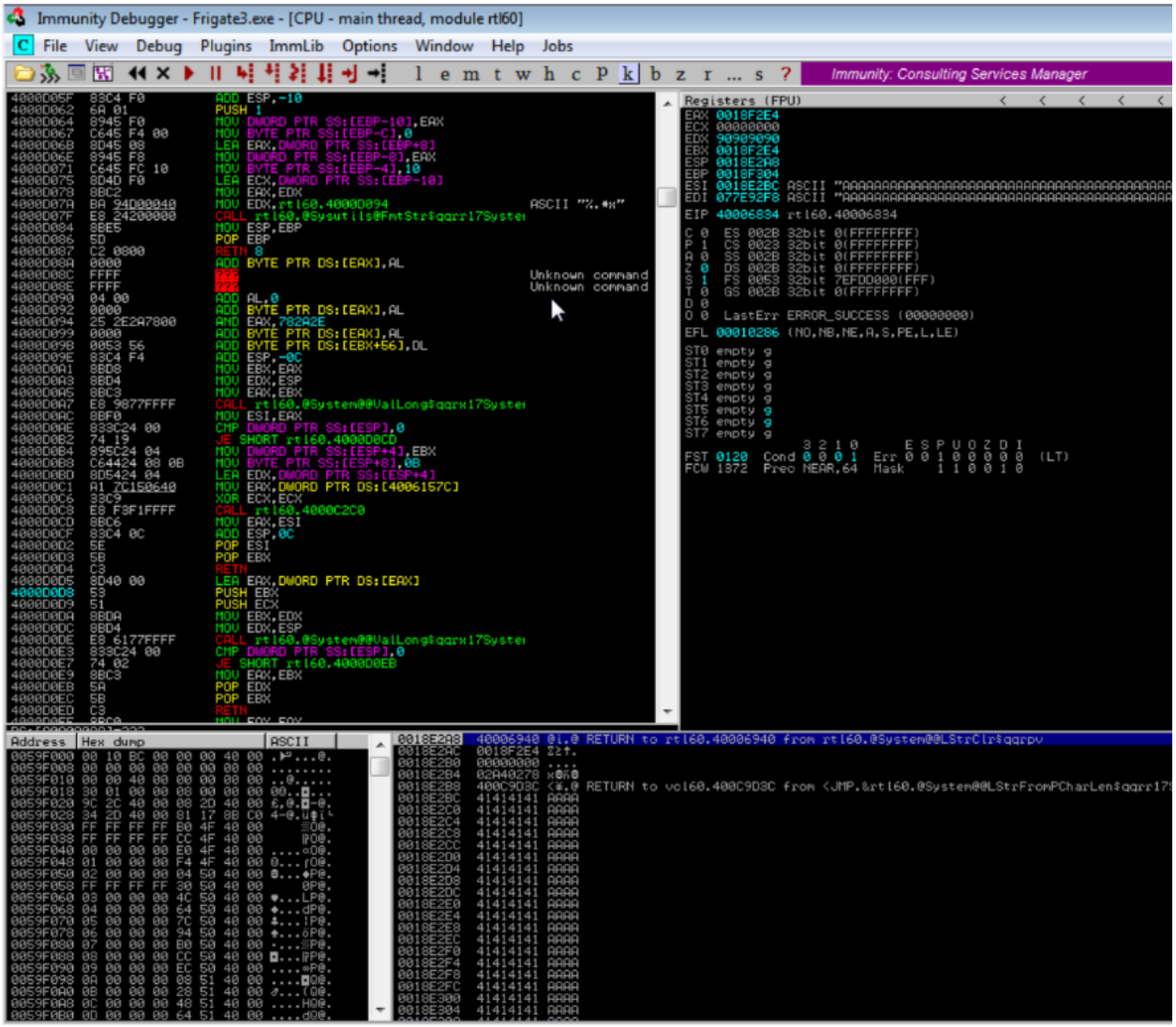
You can see that EIP is loading default exception handler



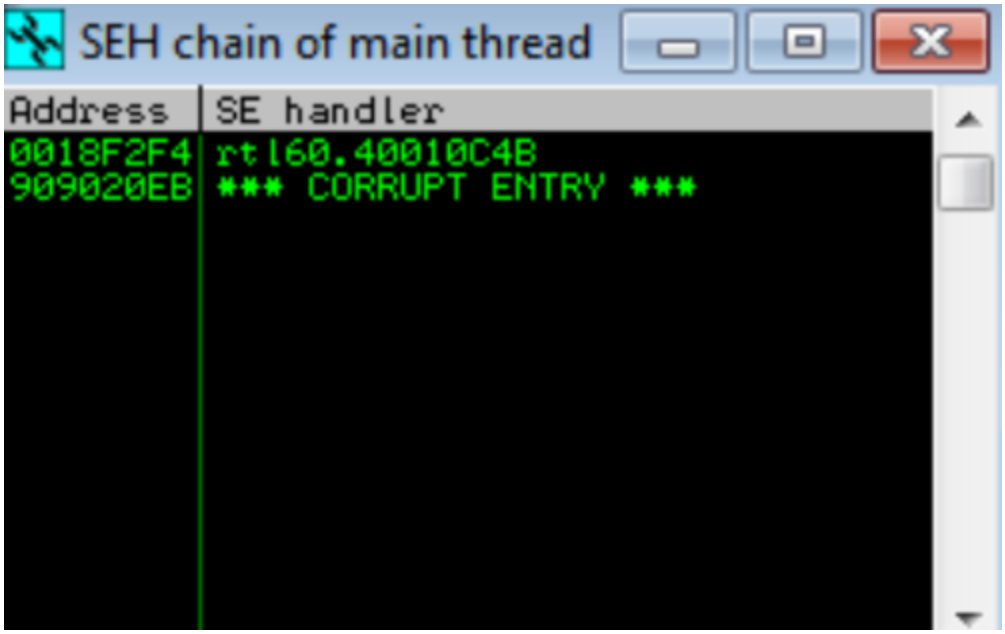
Now paste the payload in frigate



Checking Immunity Debugger



Now you can see that the EIP has changed and the loaded dll is rtl60


SEH chain of main thread
Address
SE handler
0018F2F4
rtl60.40010C4B
909020EB
*** CORRUPT ENTRY ***