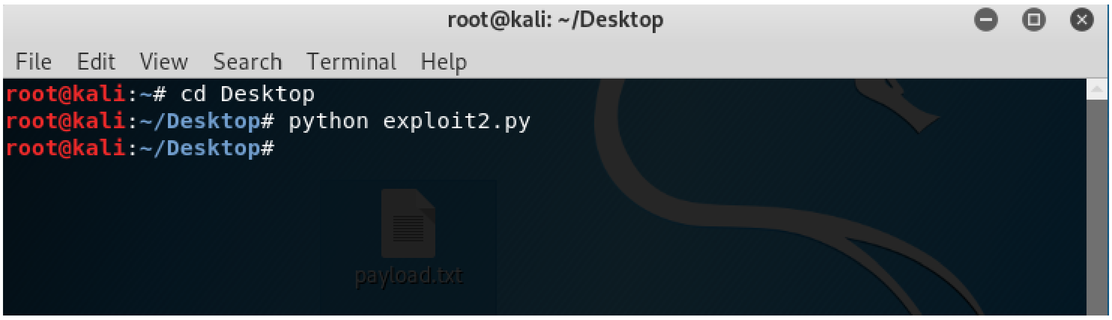
SECURE CODING LAB

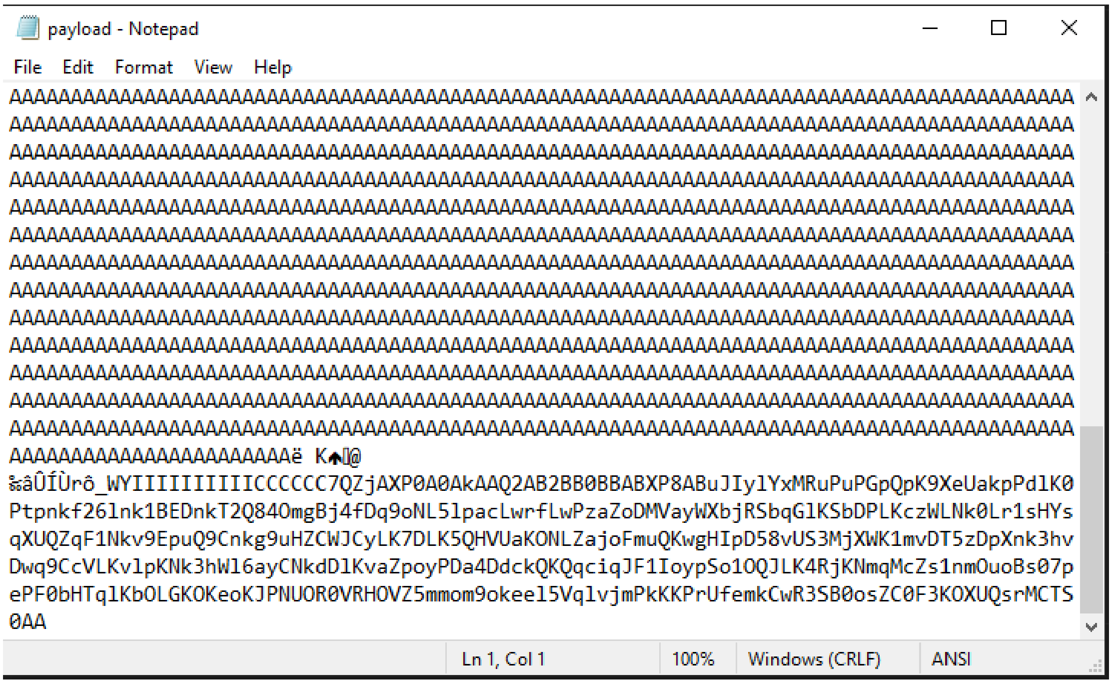
ASSIGNMENT 10

Varun Parikh
19BCE7202

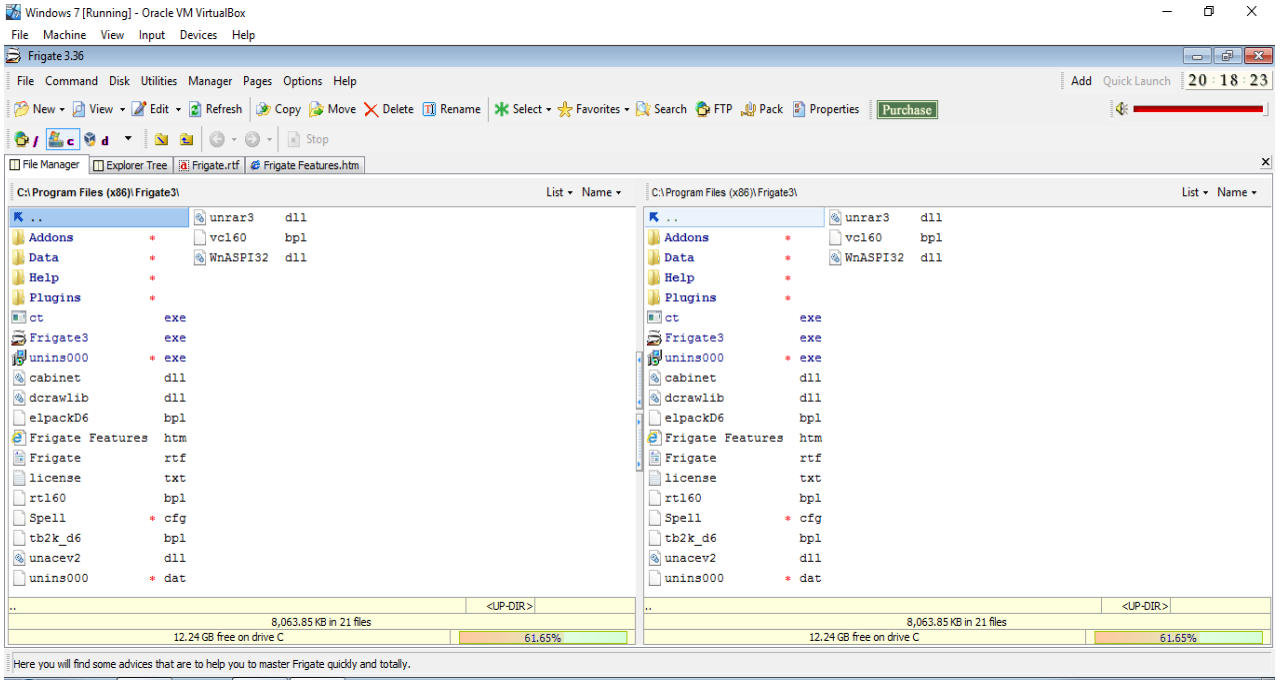
Running the exploit script to generate payload



Exploit payload

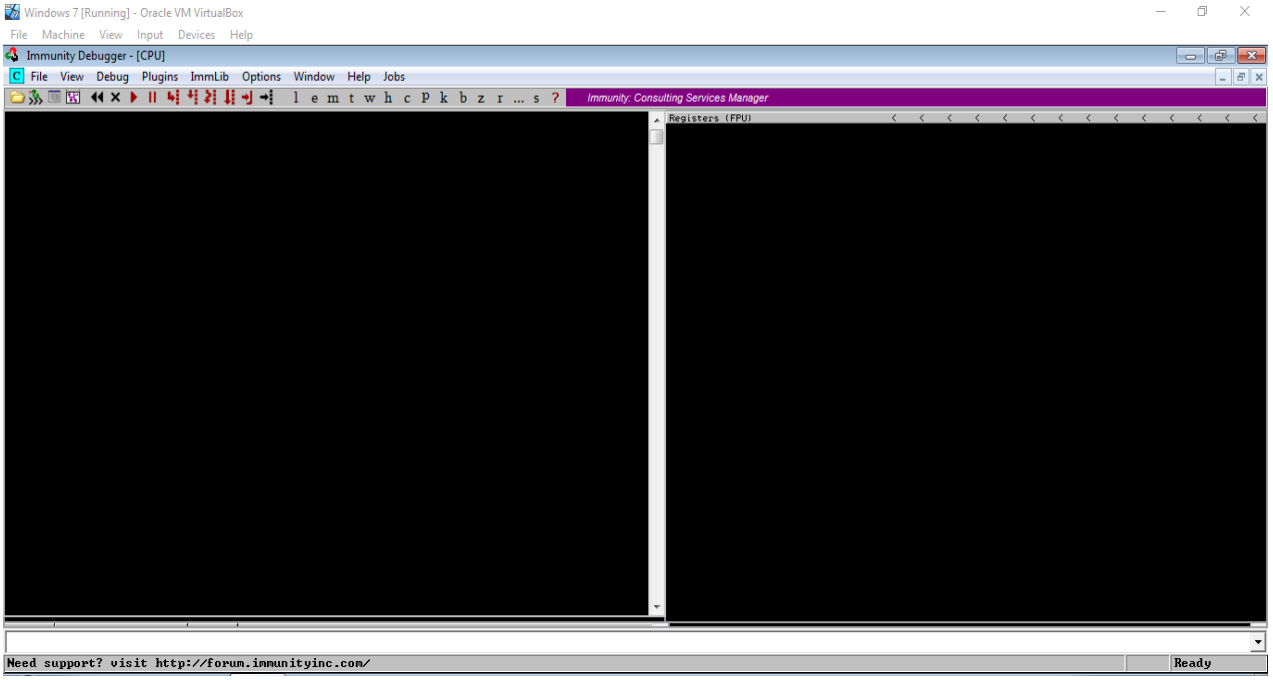


Installing Frigate3:

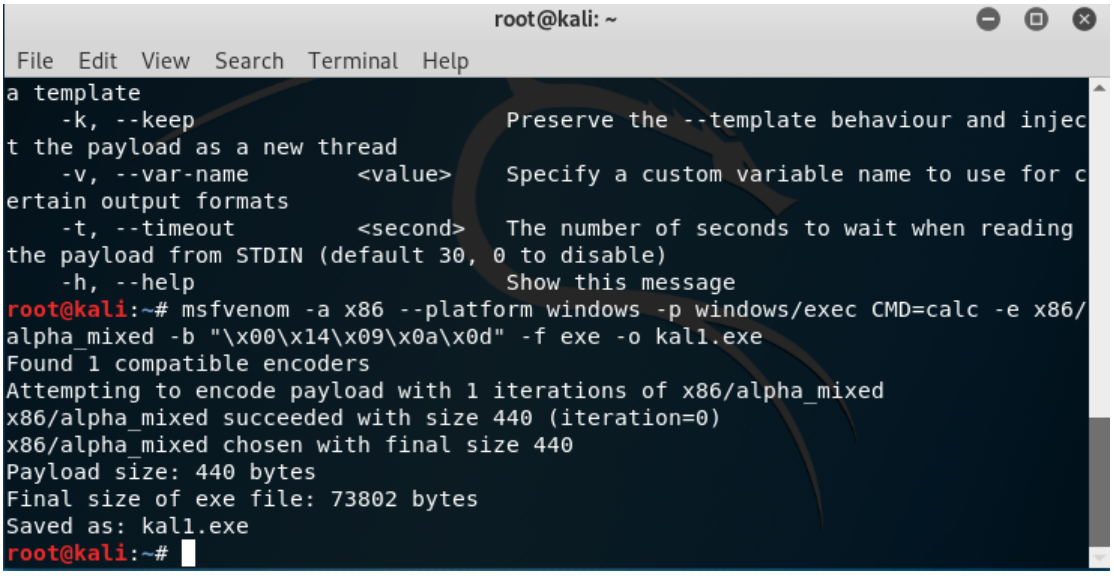


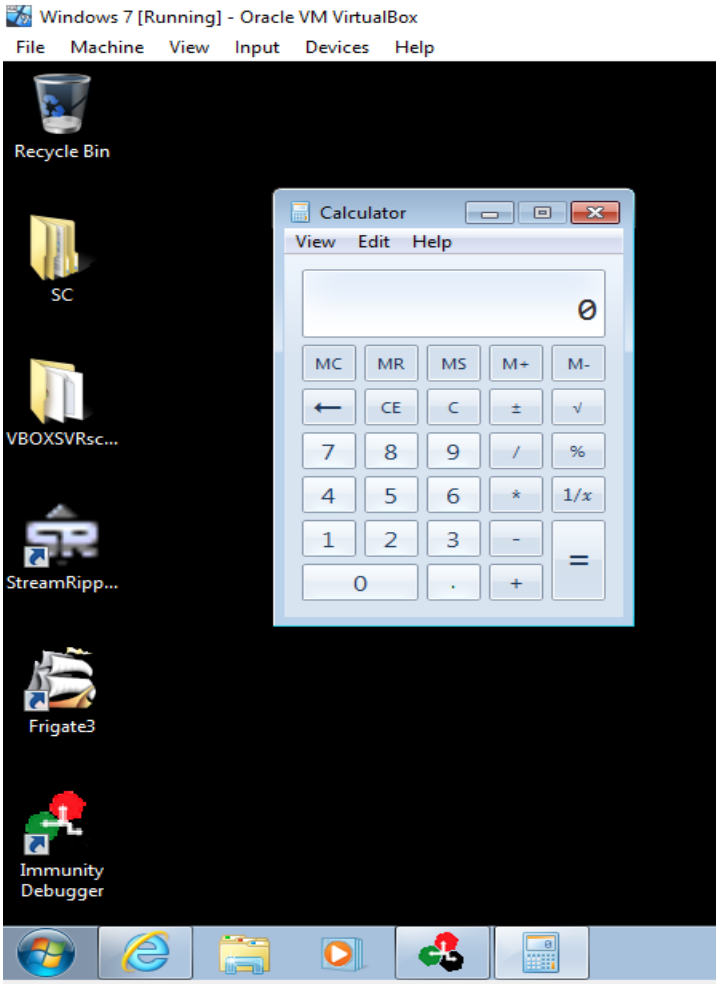
After running the exploit2.py ,the application unexpectedly stopped working.

Installing Immunity debugger:

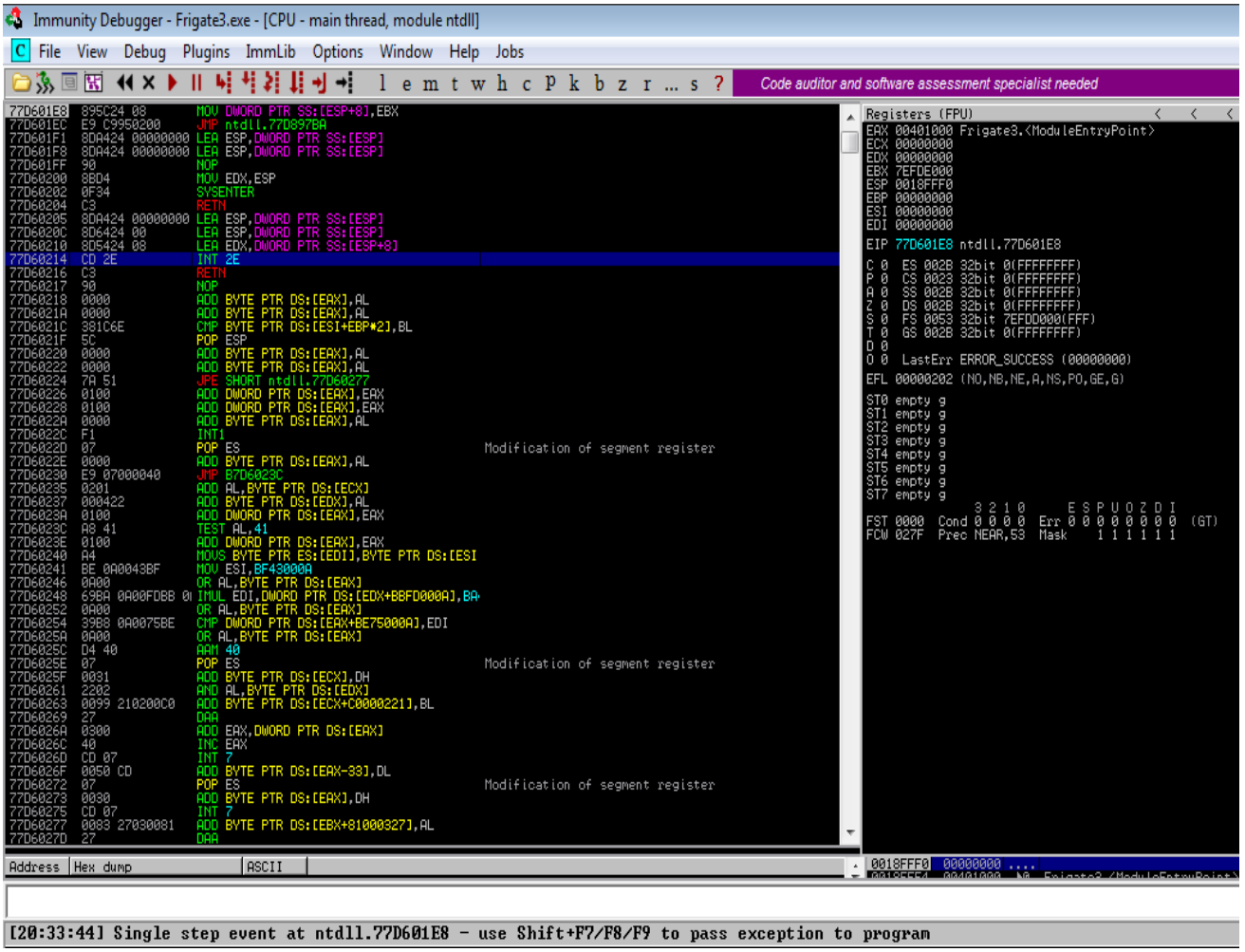


Creating the default trigger from cmd.exe to calc.exe using msfvenom in Kali linux .





Attaching the Frigate3 to immunity debugger and analyse the address of various registers listed below :



Check for EIP address :

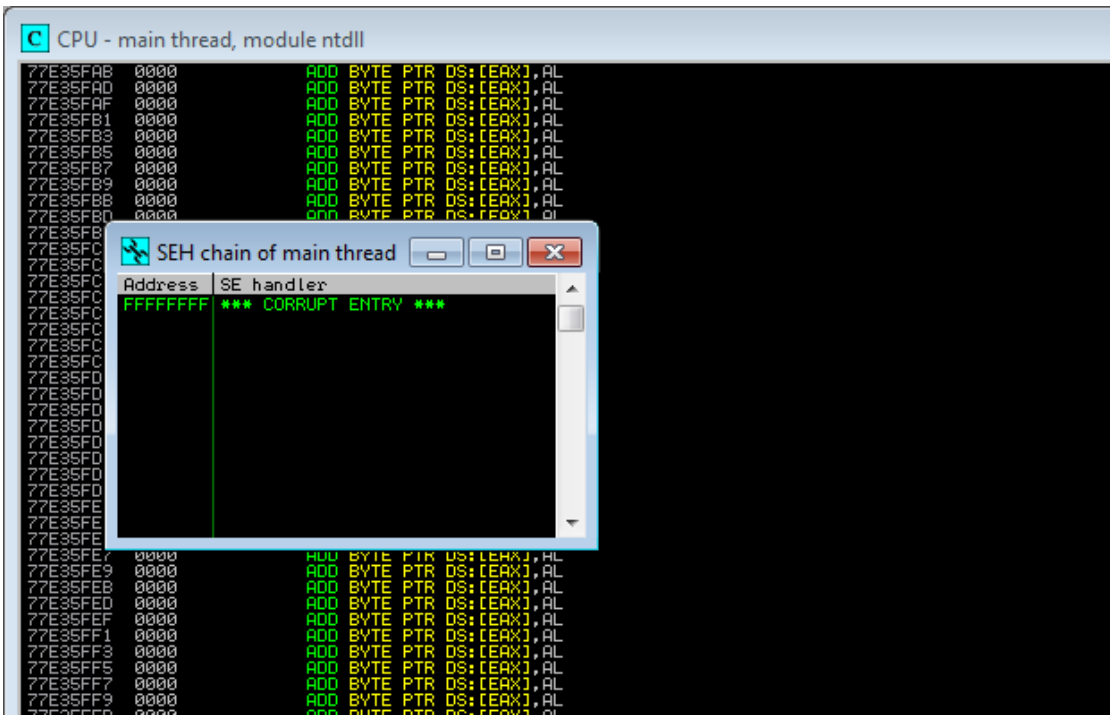
EIP Address:77D601E8

Verify the starting and ending addresses of stack frame :

Starting Address: 77D60000

Ending Address : 77045FFE

Verify the SEH chain and report the dll loaded along with the addresses. For viewing SEH chain, goto view à SEH :



(Having some error*)