CSE-2010

Secure Coding(L23 + L24)

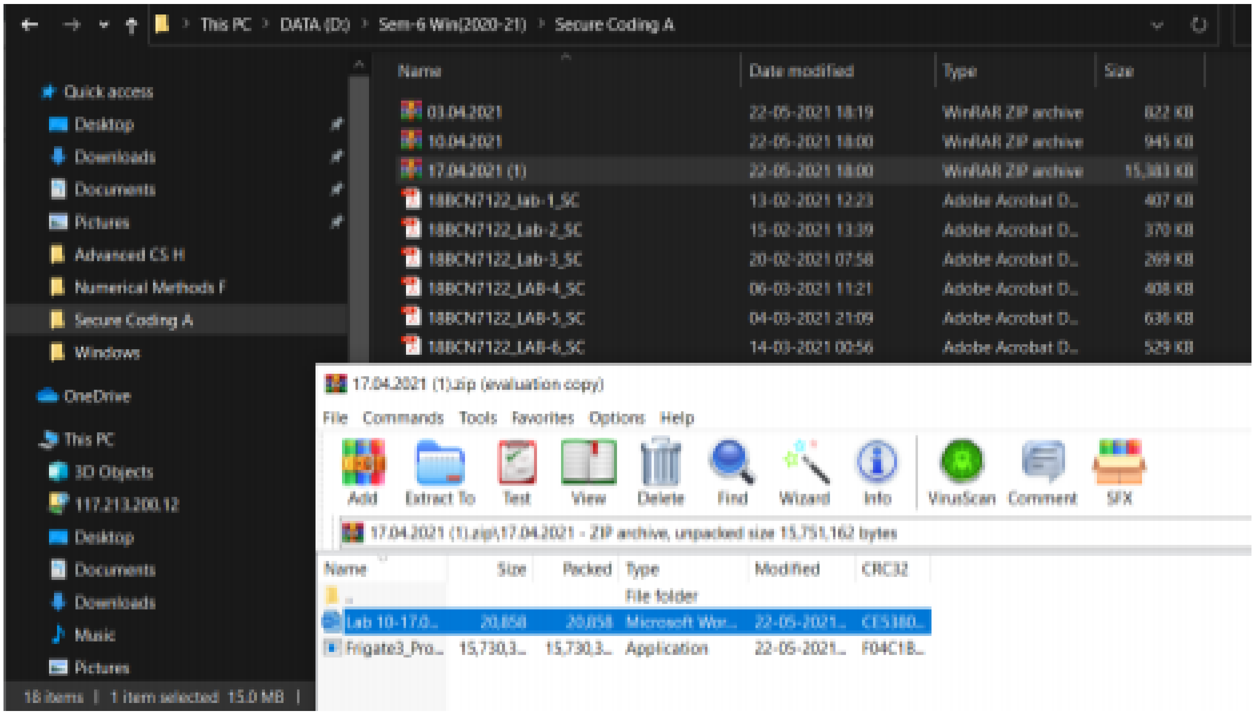
Lab - 10

Name :- Amritmoy Pain

Reg no :- 18BCE7344

Task

Download Frigate3_Pro_v36 from teams (check folder named 17.04.2021).



Name	Date modified	Type	Size
03.04.2021	22-05-2021 18:19	WinRAR ZIP archive	822 KB
10.04.2021	22-05-2021 18:00	WinRAR ZIP archive	945 KB
17.04.2021 (1)	22-05-2021 18:00	WinRAR ZIP archive	15,383 KB
18BCN7122_lab-1_SC	13-02-2021 12:23	Adobe Acrobat D...	407 KB
18BCN7122_Lab-2_SC	15-02-2021 13:39	Adobe Acrobat D...	370 KB
18BCN7122_Lab-3_SC	20-02-2021 07:58	Adobe Acrobat D...	269 KB
18BCN7122_LAB-4_SC	06-03-2021 11:21	Adobe Acrobat D...	408 KB
18BCN7122_LAB-5_SC	04-03-2021 21:09	Adobe Acrobat D...	636 KB
18BCN7122_LAB-6_SC	14-03-2021 00:56	Adobe Acrobat D...	529 KB

18 items | 1 item selected 15.0 MB |

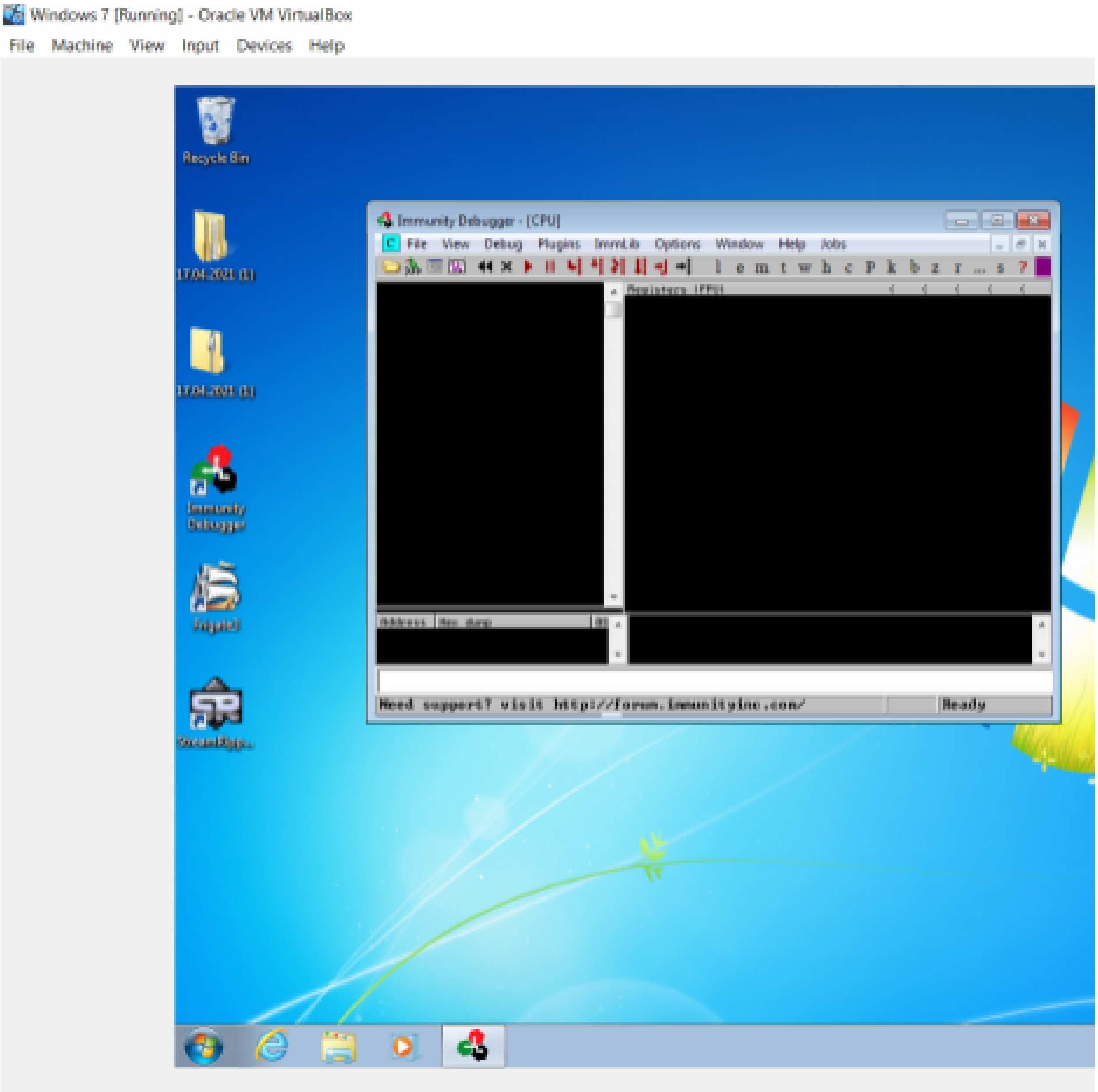
17.04.2021 (1).zip (evaluation copy)

17.04.2021 (1).zip\17.04.2021 - ZIP archive, unpacked size 15,751,162 bytes

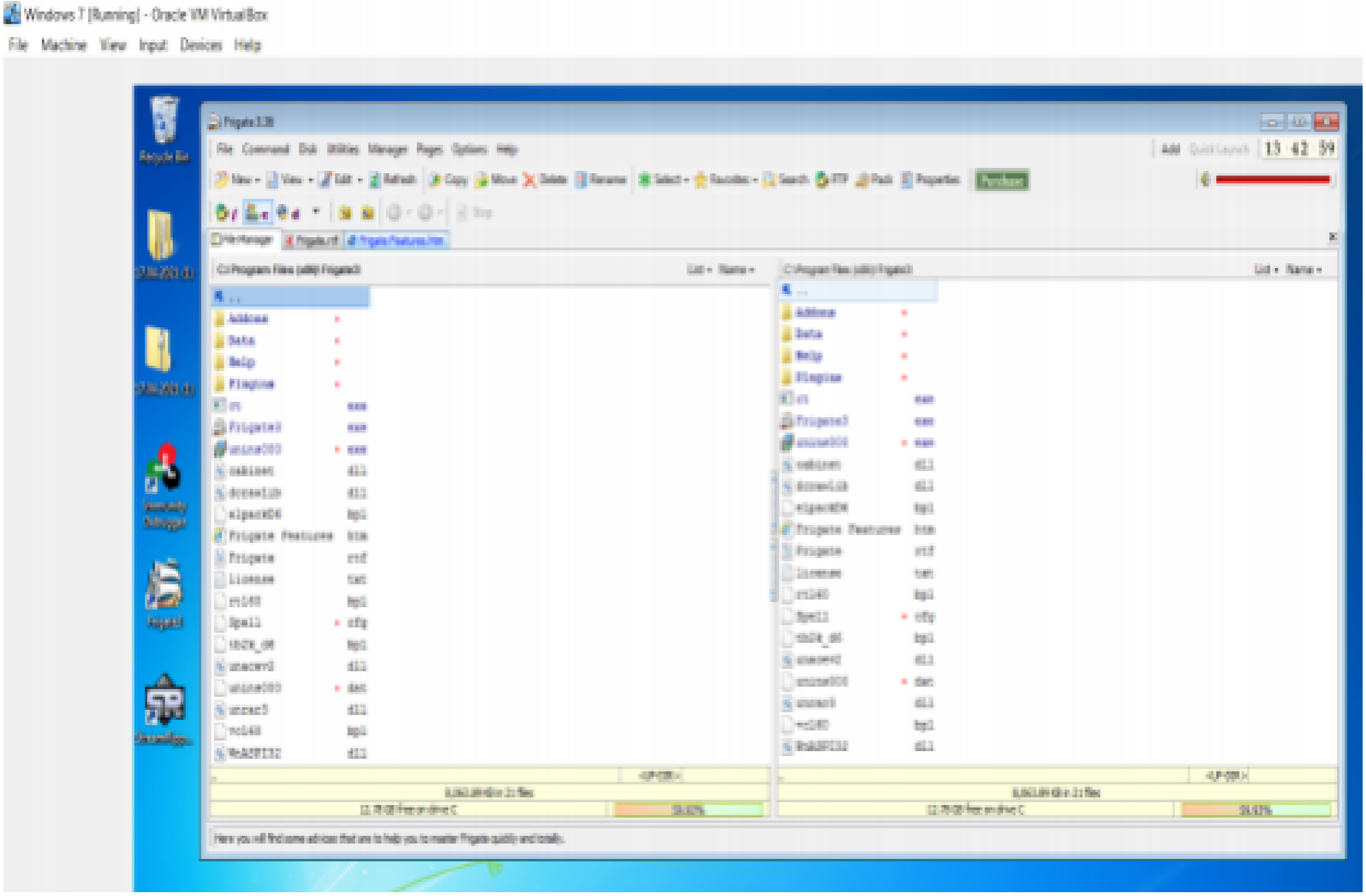
Name	Size	Packed	Type	Modified	CRC32
..			File folder		
Lab 10-17.0...	20,858	20,858	Microsoft Wor...	22-05-2021...	CE5380...
Frigate3_Pro...	15,730,3...	15,730,3...	Application	22-05-2021...	F04C1B...

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

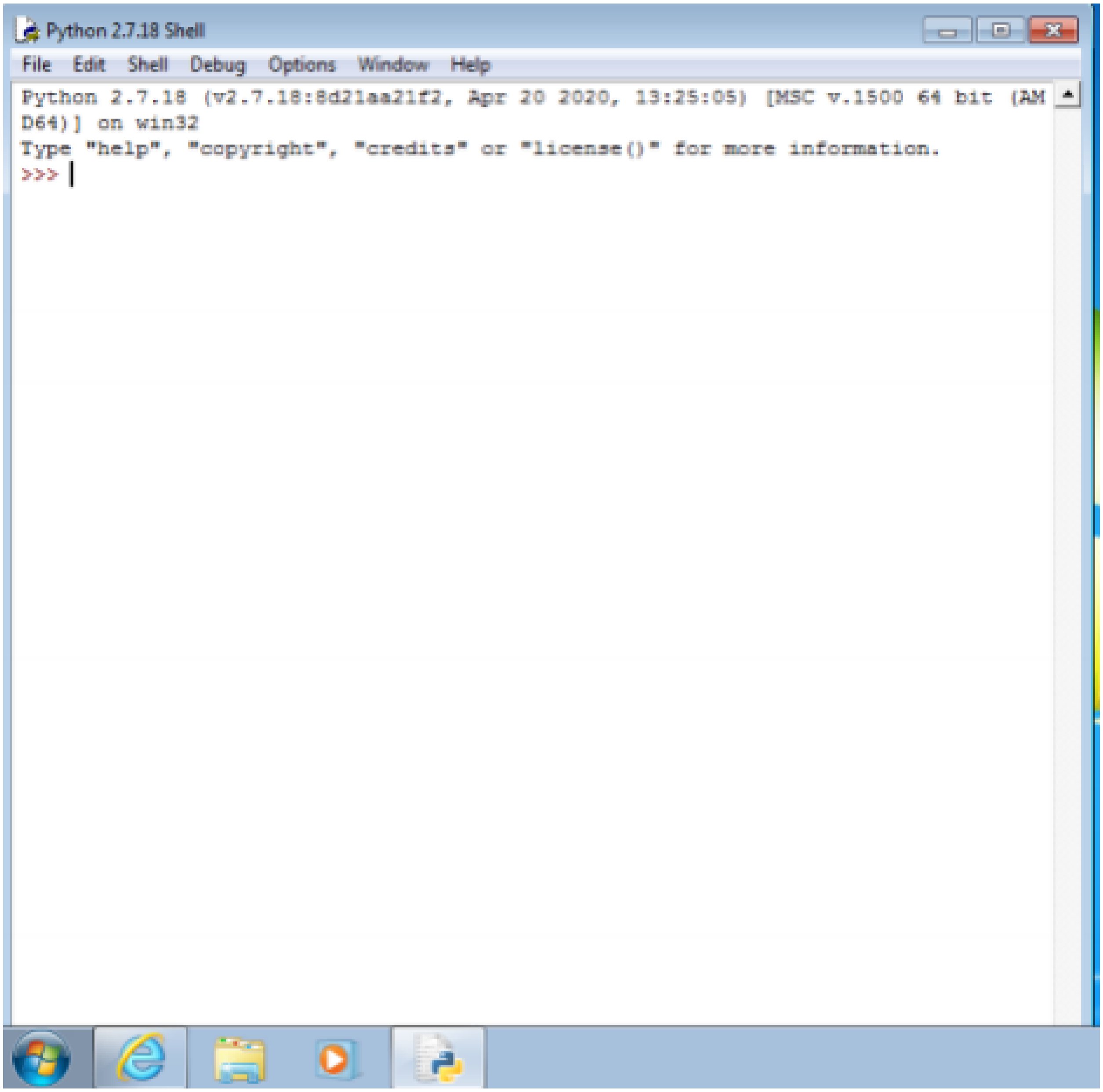
Install Immunity debugger or ollydbg in windows7


Windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
17.04.2021 (1)
17.04.2021 (1)
Immunity Debugger
Frigate3
StreamRipp...
Immunity Debugger - [CPU]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Registers (FPU)
Address Hex dump
Need support? visit http://forum.immunityinc.com/
Ready

Install Frigate3_Pro_v36 and Run the same


Windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Frigate3
C:\Program Files (x86)\Frigate3
Addons
Data
Help
Plugins
Frigate3
Frigate Features
license

Download and install python 2.7.* or 3.5.*



```
Python 2.7.18 (v2.7.18:8d21aa21f2, Apr 20 2020, 13:25:05) [MSC v.1500 64 bit (AM
D64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>> 
```

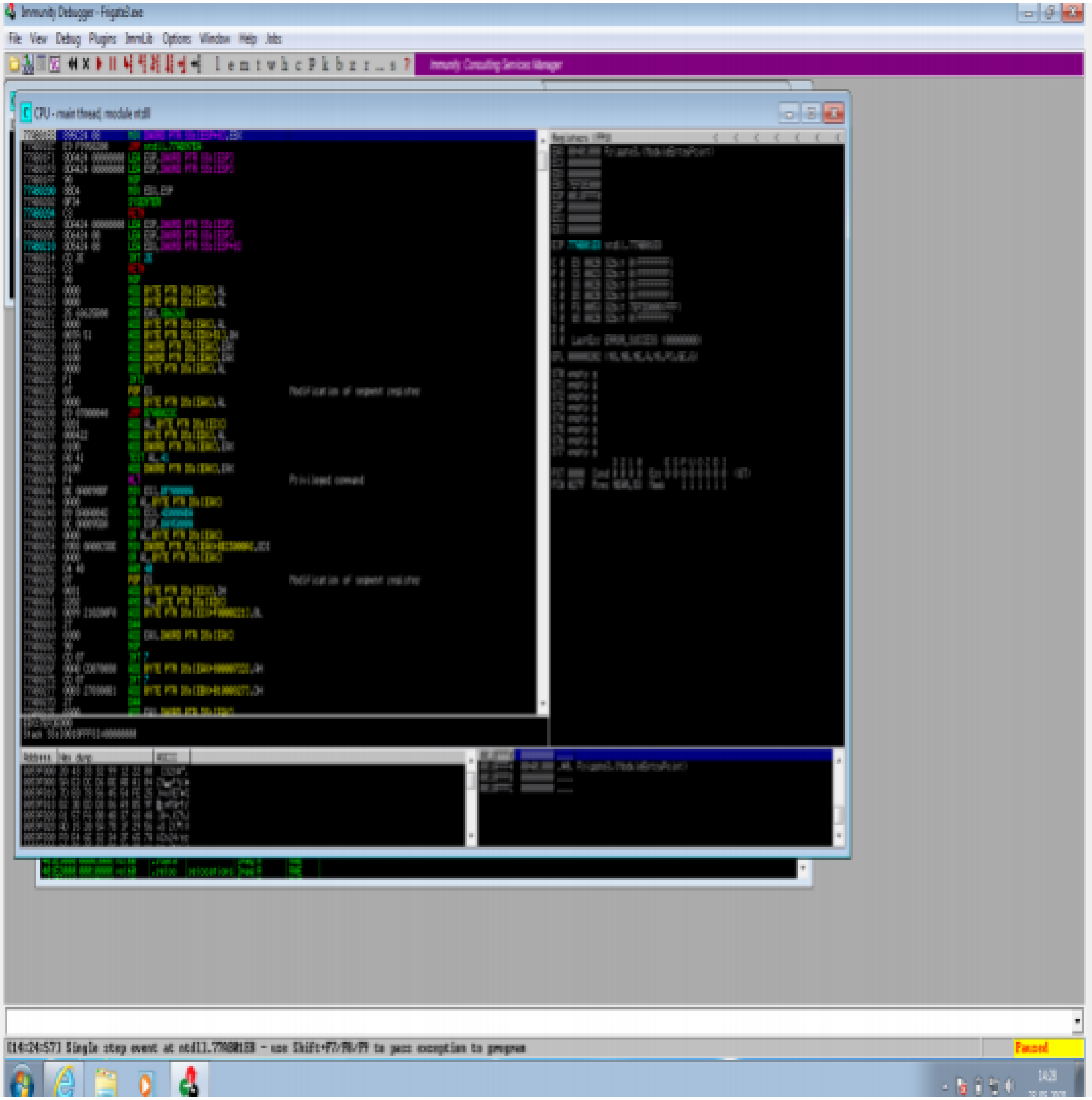
1. Analysis :-

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).

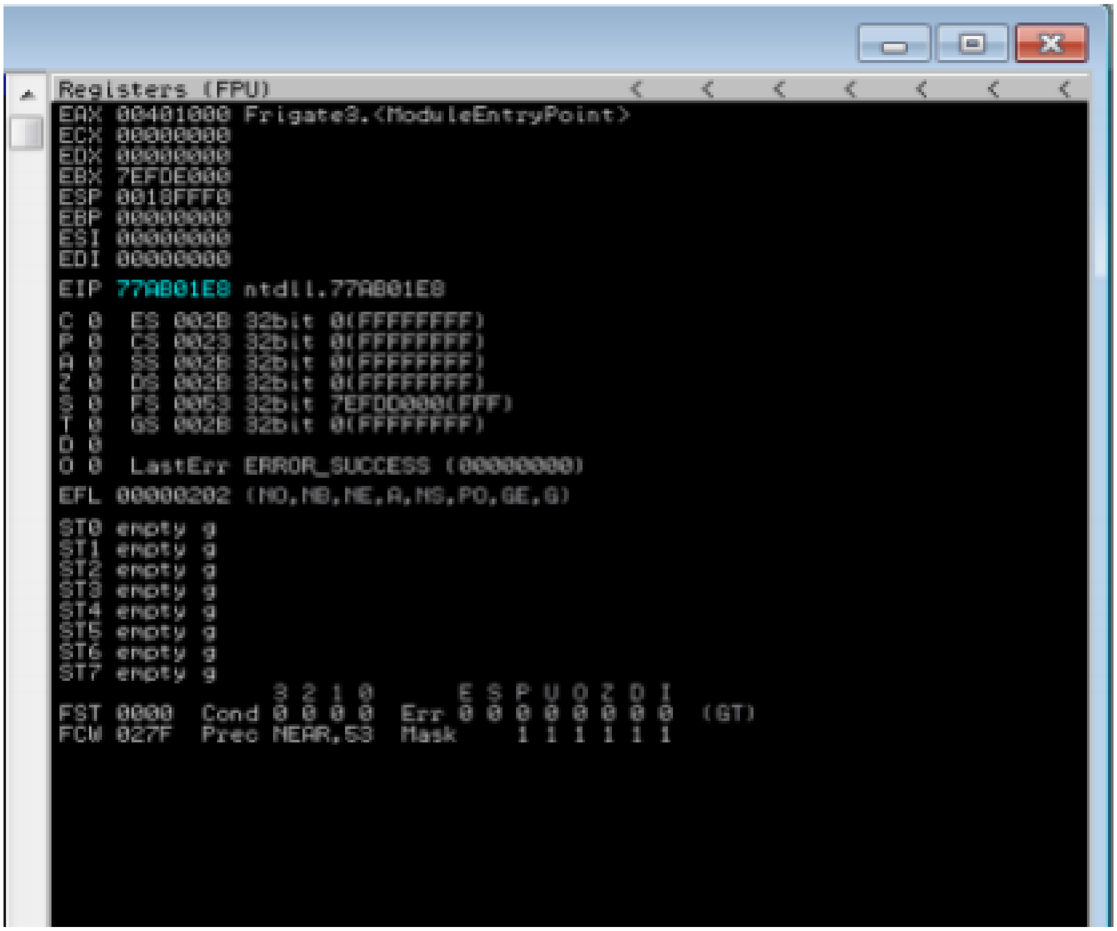
```
msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
```

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


Immunity Debugger - FrigateS.exe
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity Consulting Services Manager
CPU - main thread, module ntdll
Registers (FPU)
Paused

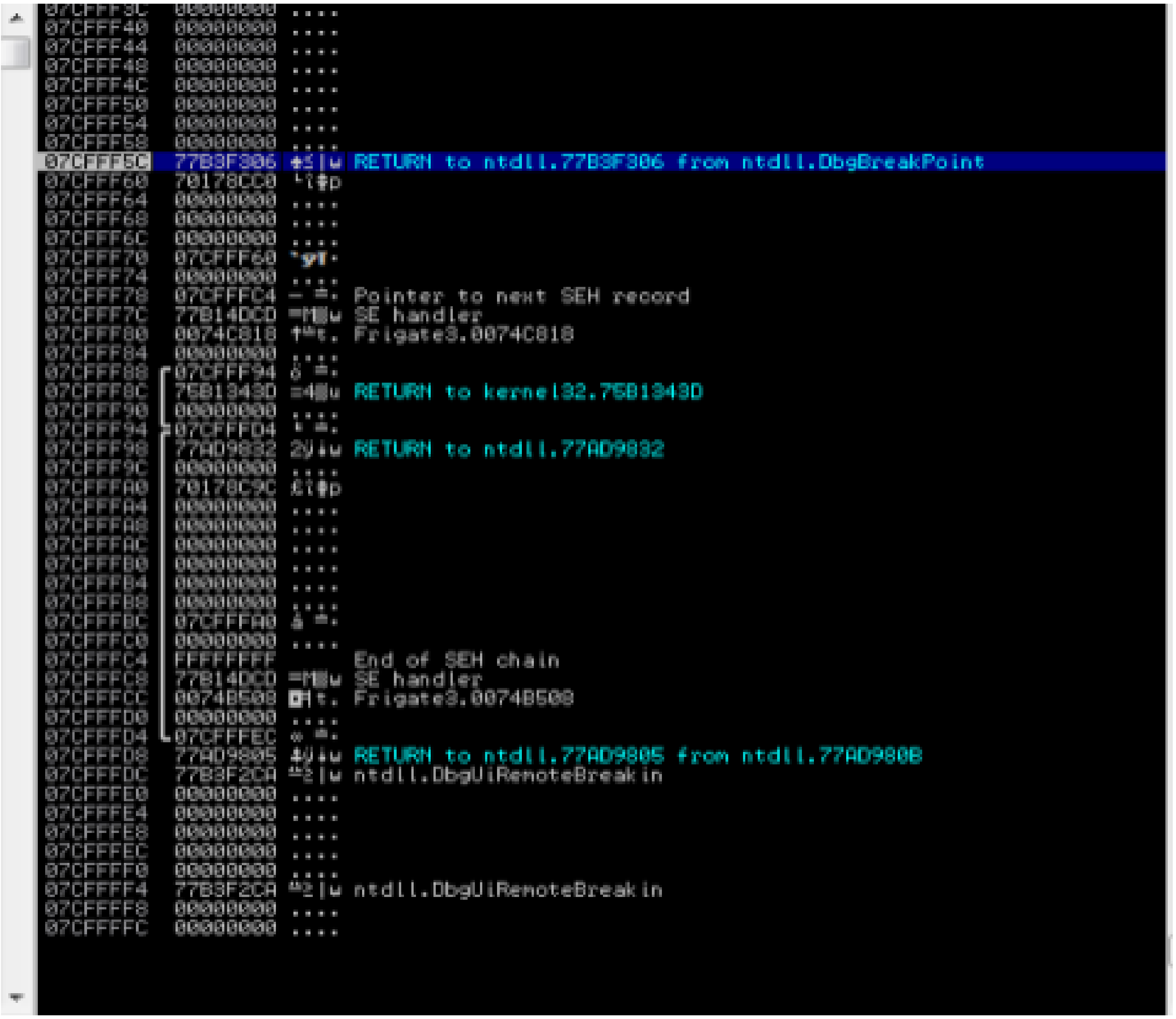
```
[14:24:57] Single step event at ntdll.7768H1EB - use Shift+F7/F8/F9 to pass exception to program
```

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 7EFDD000(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 g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
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



```
07CFFF3C  00000000  ....
07CFFF40  00000000  ....
07CFFF44  00000000  ....
07CFFF48  00000000  ....
07CFFF4C  00000000  ....
07CFFF50  00000000  ....
07CFFF54  00000000  ....
07CFFF58  00000000  ....
07CFFF5C  77B3F306  ♦S|w RETURN to ntdll.77B3F306 from ntdll.DbgBreakPoint
07CFFF60  70178CC0  └î▓p
07CFFF64  00000000  ....
07CFFF68  00000000  ....
07CFFF6C  00000000  ....
07CFFF70  07CFFF60  `yÏ•
07CFFF74  00000000  ....
07CFFF78  07CFFFC4  ─ ═•  Pointer to next SEH record
07CFFF7C  77B14DCD  ═M▓w  SE handler
07CFFF80  0074C818  ↑╚t.  Frigate3.0074C818
07CFFF84  00000000  ....
07CFFF88 ┌07CFFF94  ö ═•
07CFFF8C │75B1343D  =4▓u  RETURN to kernel32.75B1343D
07CFFF90 │00000000  ....
07CFFF94 ├07CFFFD4  ╘ ═•
07CFFF98 │77AD9832  2ÿ↓w  RETURN to ntdll.77AD9832
07CFFF9C │00000000  ....
07CFFFA0 │70178C9C  £î▓p
07CFFFA4 │00000000  ....
07CFFFA8 │00000000  ....
07CFFFAC │00000000  ....
07CFFFB0 │00000000  ....
07CFFFB4 │00000000  ....
07CFFFB8 │00000000  ....
07CFFFBC │07CFFFA0  á ═•
07CFFFC0 │00000000  ....
07CFFFC4 │FFFFFFFF       End of SEH chain
07CFFFC8 │77B14DCD  ═M▓w  SE handler
07CFFFCC │0074B508  ◘╡t.  Frigate3.0074B508
07CFFFD0 │00000000  ....
07CFFFD4 └07CFFFEC  ∞ ═•
07CFFFD8  77AD9805  ♣ÿ↓w  RETURN to ntdll.77AD9805 from ntdll.77AD980B
07CFFFDC  77B3F2CA  ╩≥|w  ntdll.DbgUiRemoteBreakin
07CFFFE0  00000000  ....
07CFFFE4  00000000  ....
07CFFFE8  00000000  ....
07CFFFEC  00000000  ....
07CFFFF0  00000000  ....
07CFFFF4  77B3F2CA  ╩≥|w  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