SECURE CODING LAB-10

CSE-2010

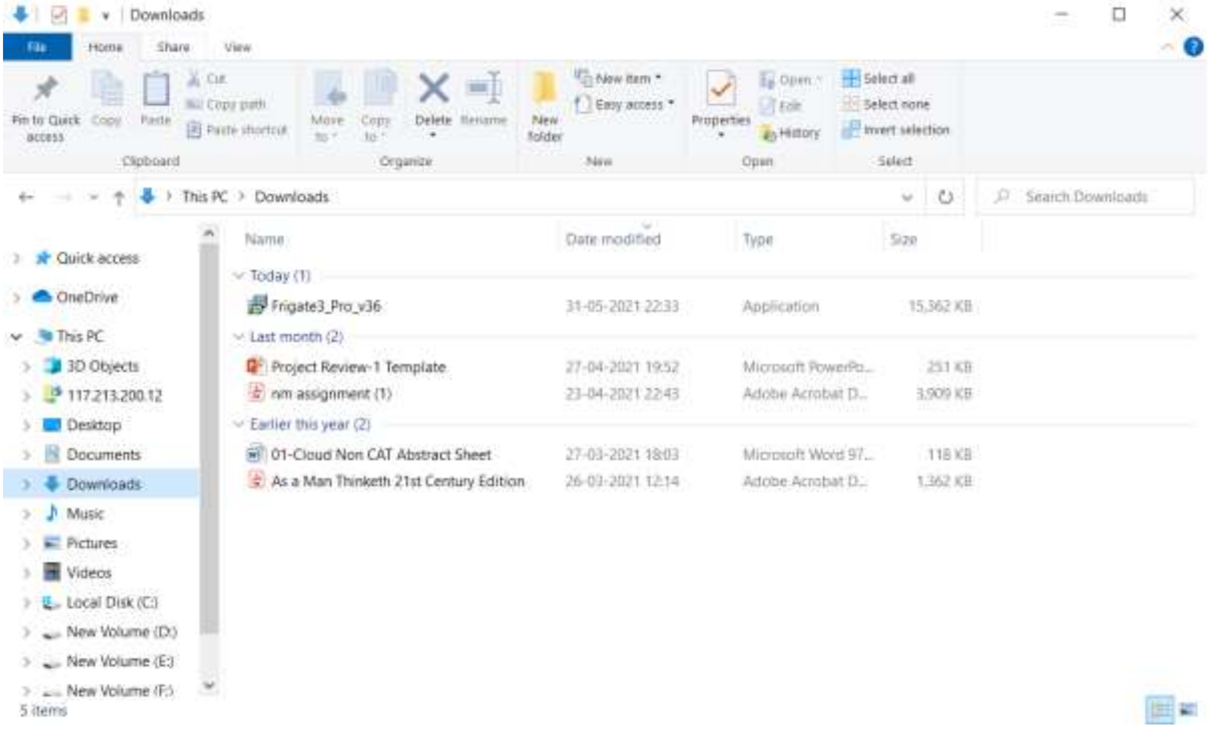
SLOT-L23&L24

DONE BY

HEMANTH KUMAR R

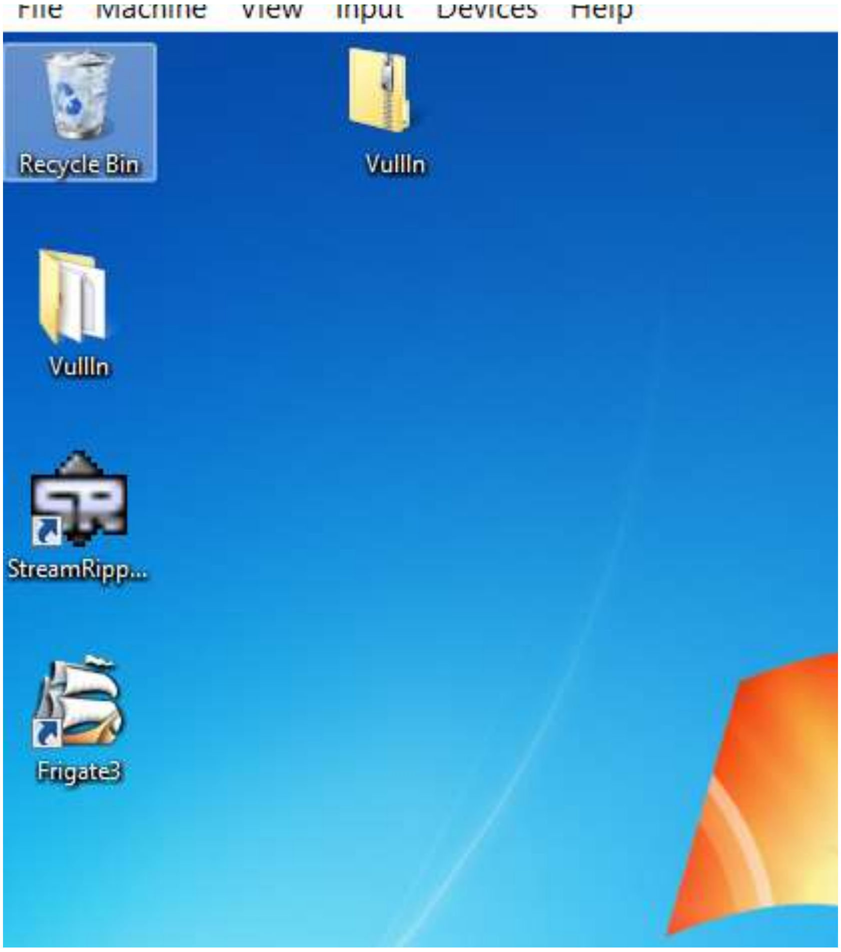
18BCN7028

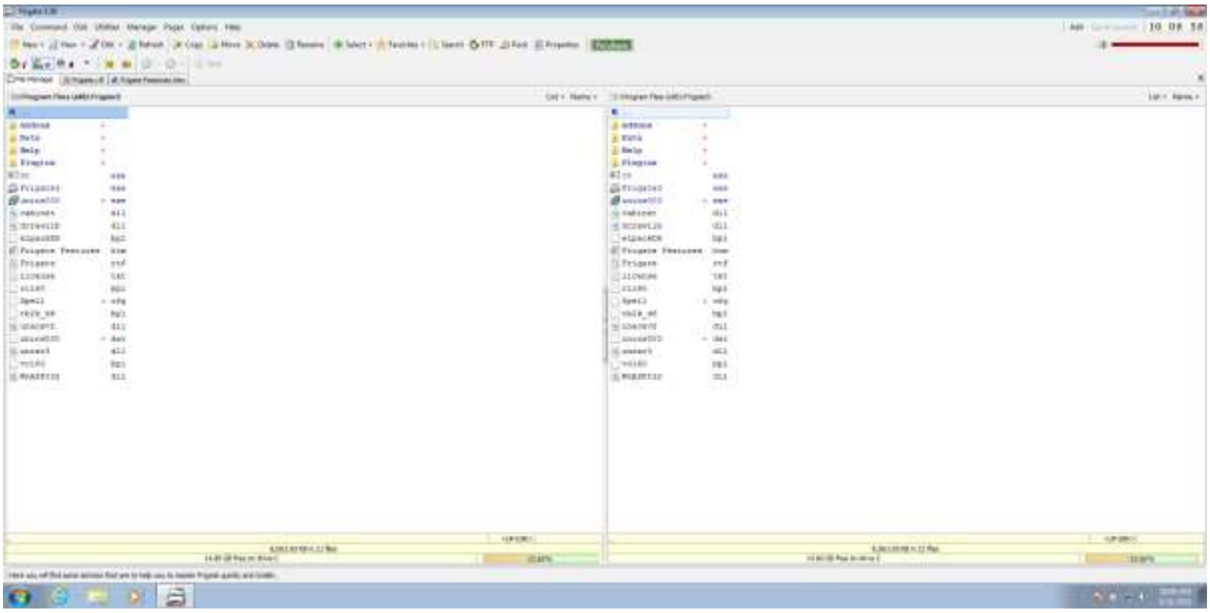
Download Frigate3_Pro_v36 from teams



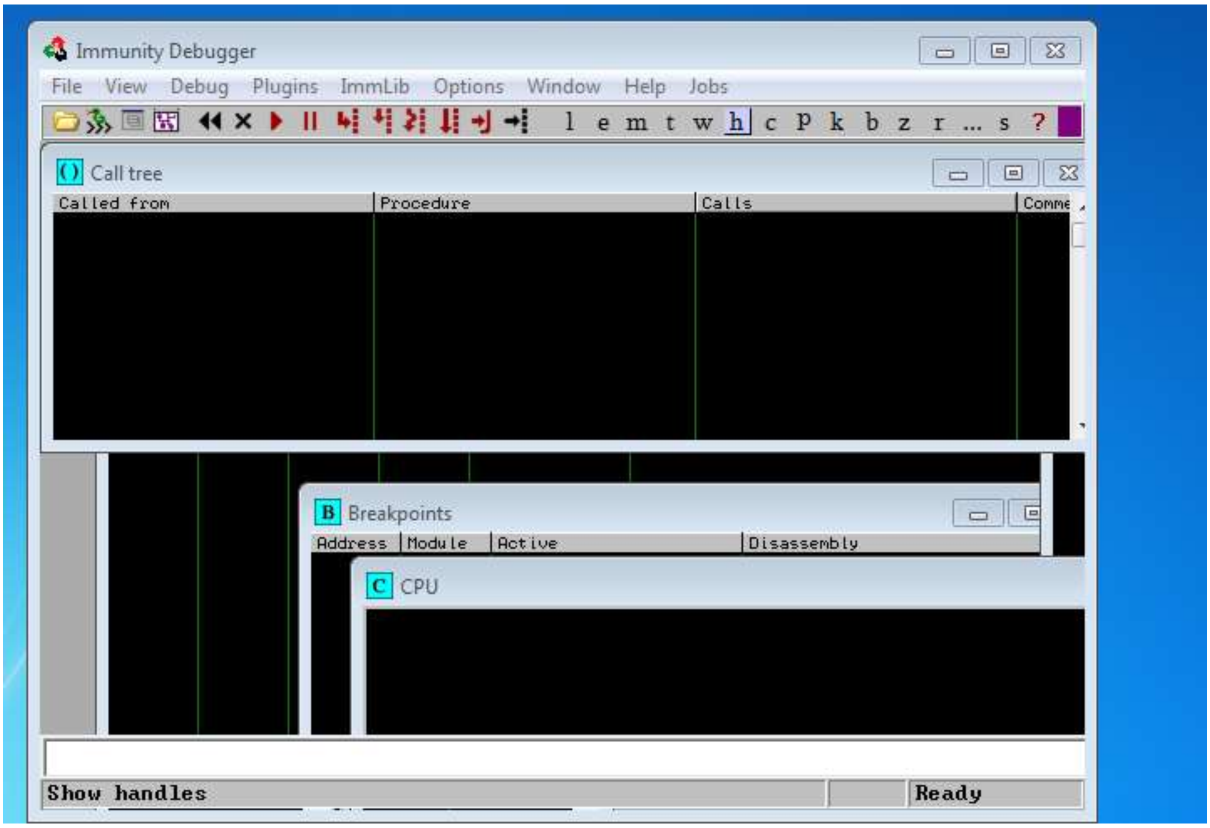
Name	Date modified	Type	Size
Today (1)			
Frigate3_Pro_v36	31-05-2021 22:33	Application	15,362 KB
Last month (2)			
Project Review-1 Template	27-04-2021 19:52	Microsoft PowerPo...	251 KB
nm assignment (1)	23-04-2021 22:43	Adobe Acrobat D...	3,909 KB
Earlier this year (2)			
01-Cloud Non CAT Abstract Sheet	27-03-2021 18:03	Microsoft Word 97...	118 KB
As a Man Thinketh 21st Century Edition	26-03-2021 12:14	Adobe Acrobat D...	1,362 KB

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

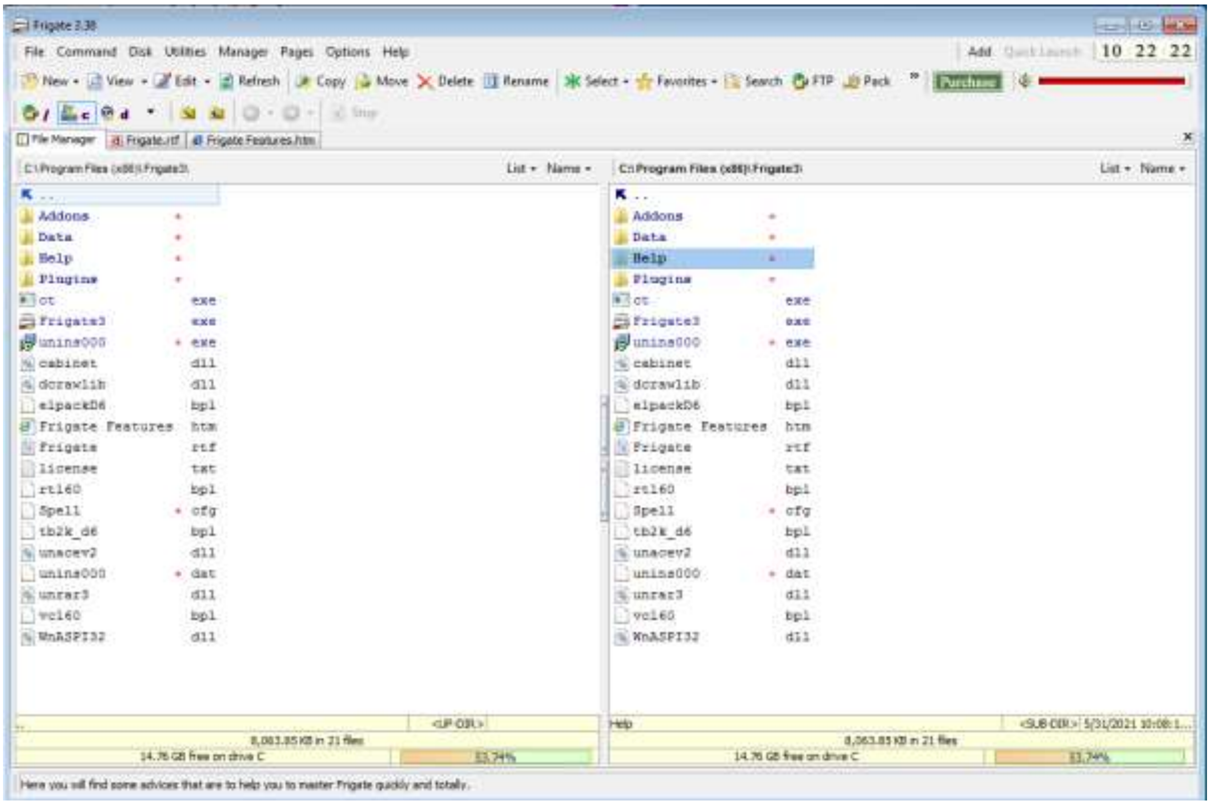




Install Immunity debugger or ollydbg in windows7



Install Frigate3_Pro_v36 and Run the same


Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
Add Quick launch 10 22 22
New View Edit Refresh Copy Move Delete Rename Select Favorites Search FTP Pack
Purchase
File Manager
Frigate.rtf
Frigate Features.htm
C:\Program Files (x86)\Frigate3\
List Name
C:\Program Files (x86)\Frigate3\
List Name

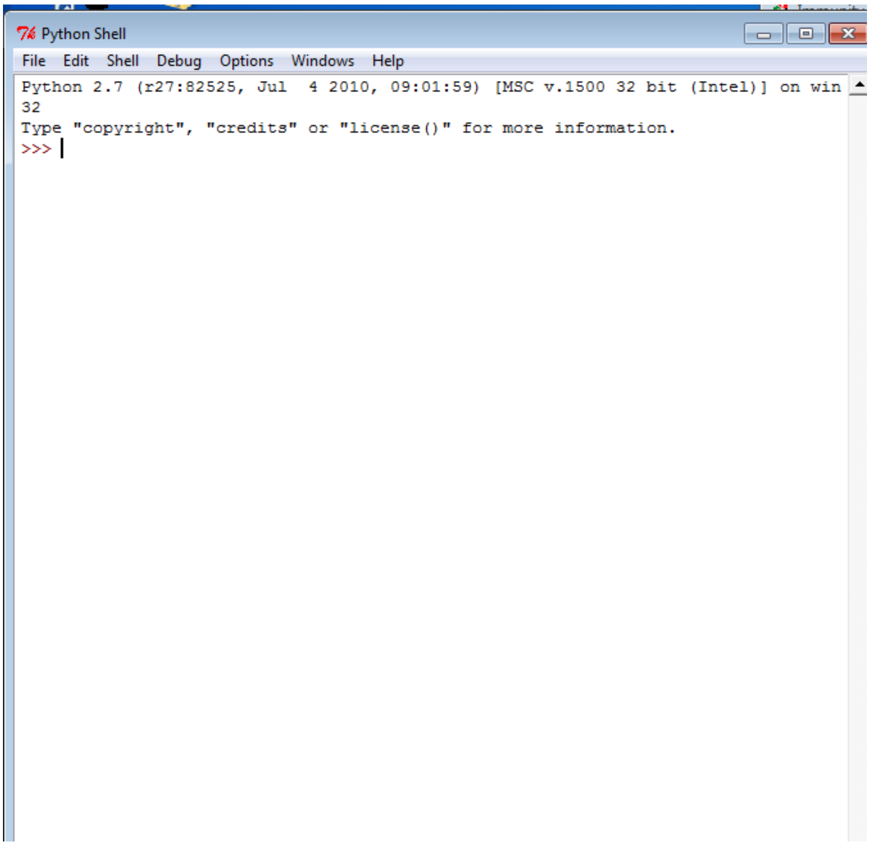
..	
Addons	
Data	
Help	
Plugins	
ct	exe
Frigate3	exe
unins000	exe
cabinet	dll
dcrawlib	dll
elpackD6	bpl
Frigate Features	htm
Frigate	rtf
license	txt
rtl60	bpl
Spell	cfg
tb2k_d6	bpl
unacev2	dll
unins000	dat
unrar3	dll
vcl60	bpl
WnASPI32	dll

<UP-DIR>
8,083.85 KB in 21 files
14.76 GB free on drive C
53.74%

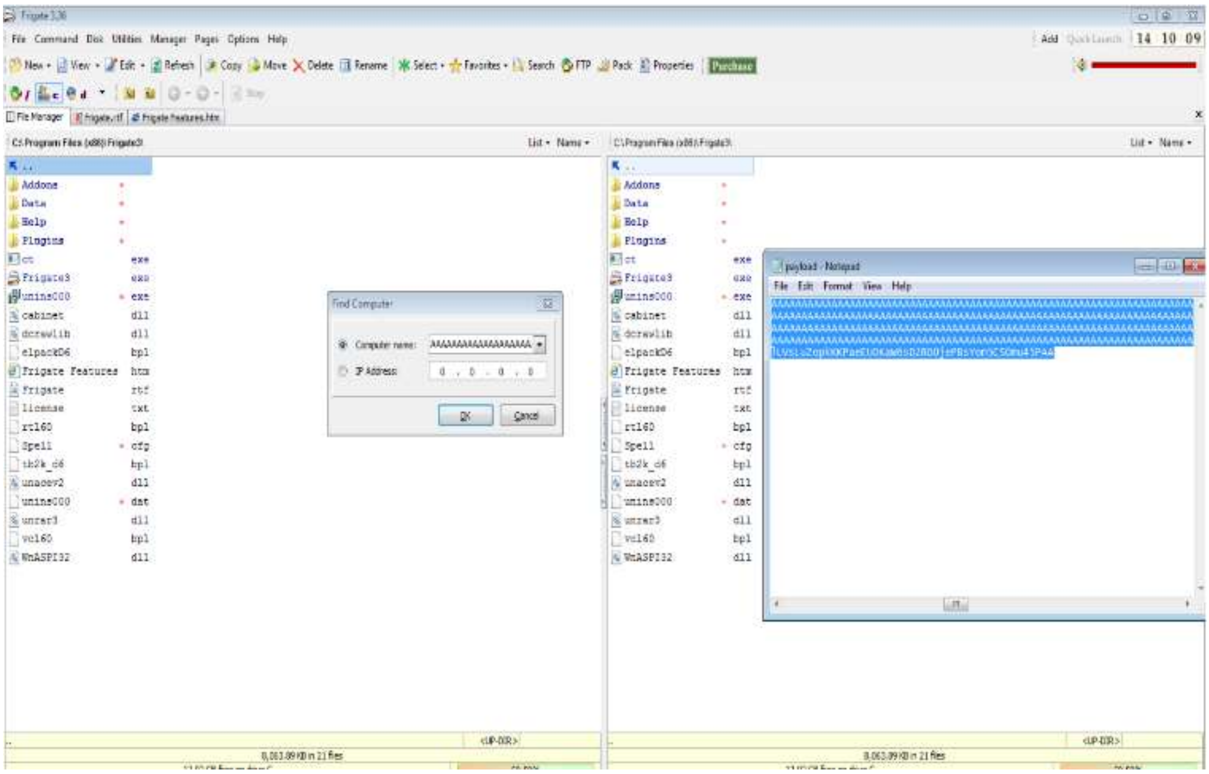
Help
<SUB-DIR> 5/31/2021 10:08:1...
8,083.85 KB in 21 files
14.76 GB free on drive C
53.74%

Here you will find some advices that are to help you to master Frigate quickly and totally.

Download and install python 2.7.* or 3.5.*



```
Python 2.7 (r27:82525, Jul  4 2010, 09:01:59) [MSC v.1500 32 bit (Intel)] on win
32
Type "copyright", "credits" or "license()" for more information.
>>> 
```


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
Add Quick Launch
14 10 09
File Manager
Frigate.rtf
Frigate Features.htm
List Name
<UP-DIR>

```
C:\Program Files (x86)\Frigate3\
..
Addons
Data
Help
Plugins
ct                  exe
Frigate3            exe
unins000            exe
cabinet             dll
dcrawlib            dll
elpack06            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
8,063.89 KB in 21 files
```

Find Computer

● Computer name: AAAAAAAAAAAAAAAAA

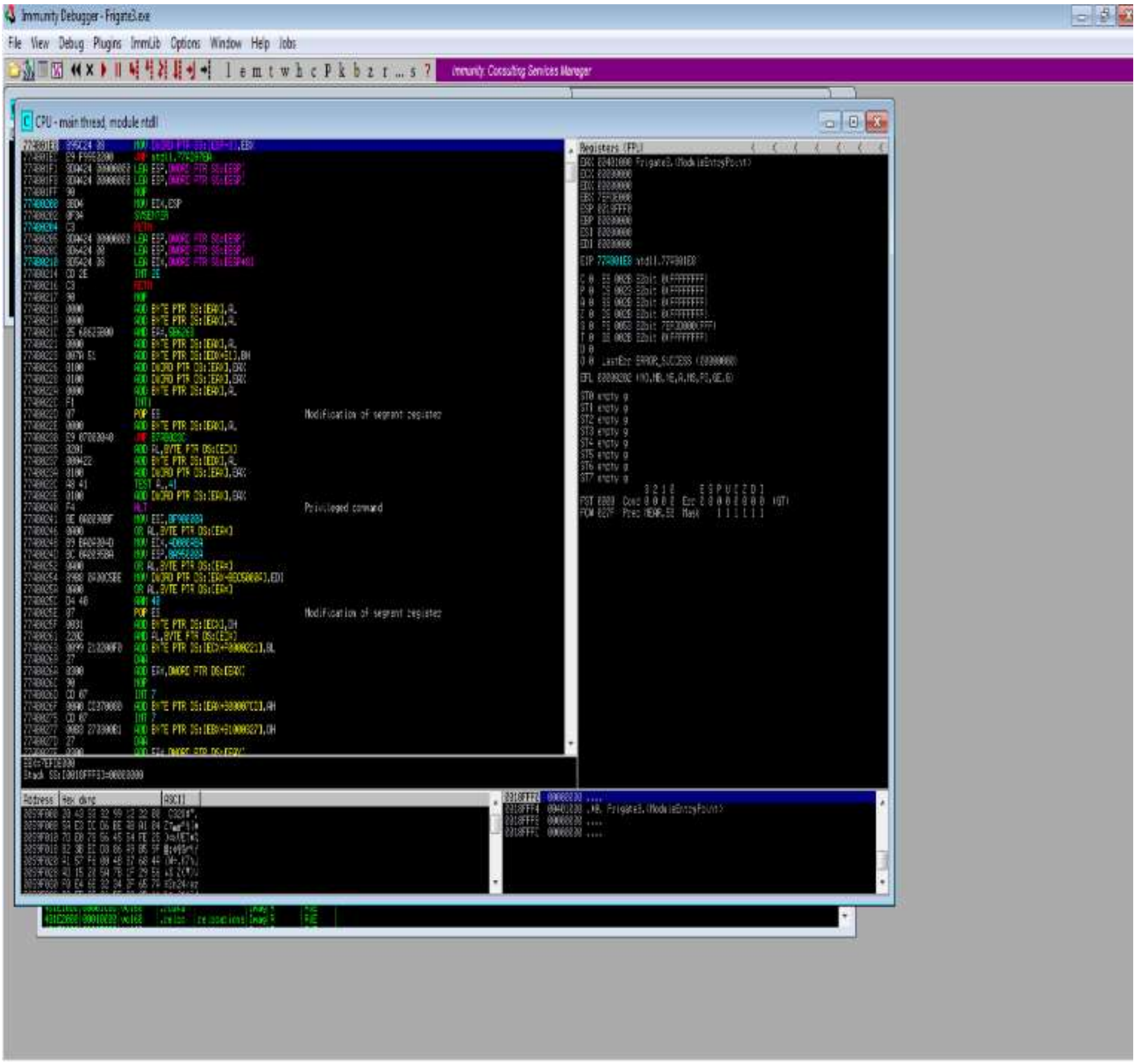
○ IP Address: 0 . 0 . 0 . 0

OK Cancel

payload - Notepad

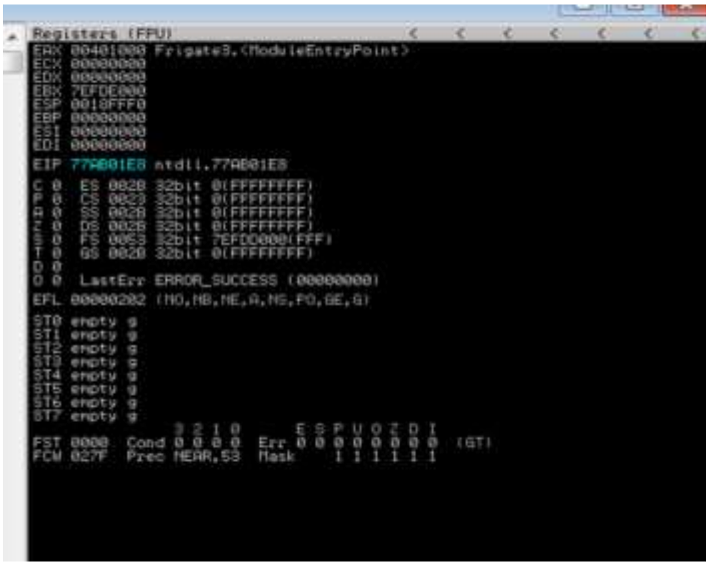
```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
[illegible]
```

Run the exploit script II


Immunity Debugger - Frigate3.exe
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Immunity: Consulting Services Manager
CPU - main thread, module ntdll
Registers (FPU)

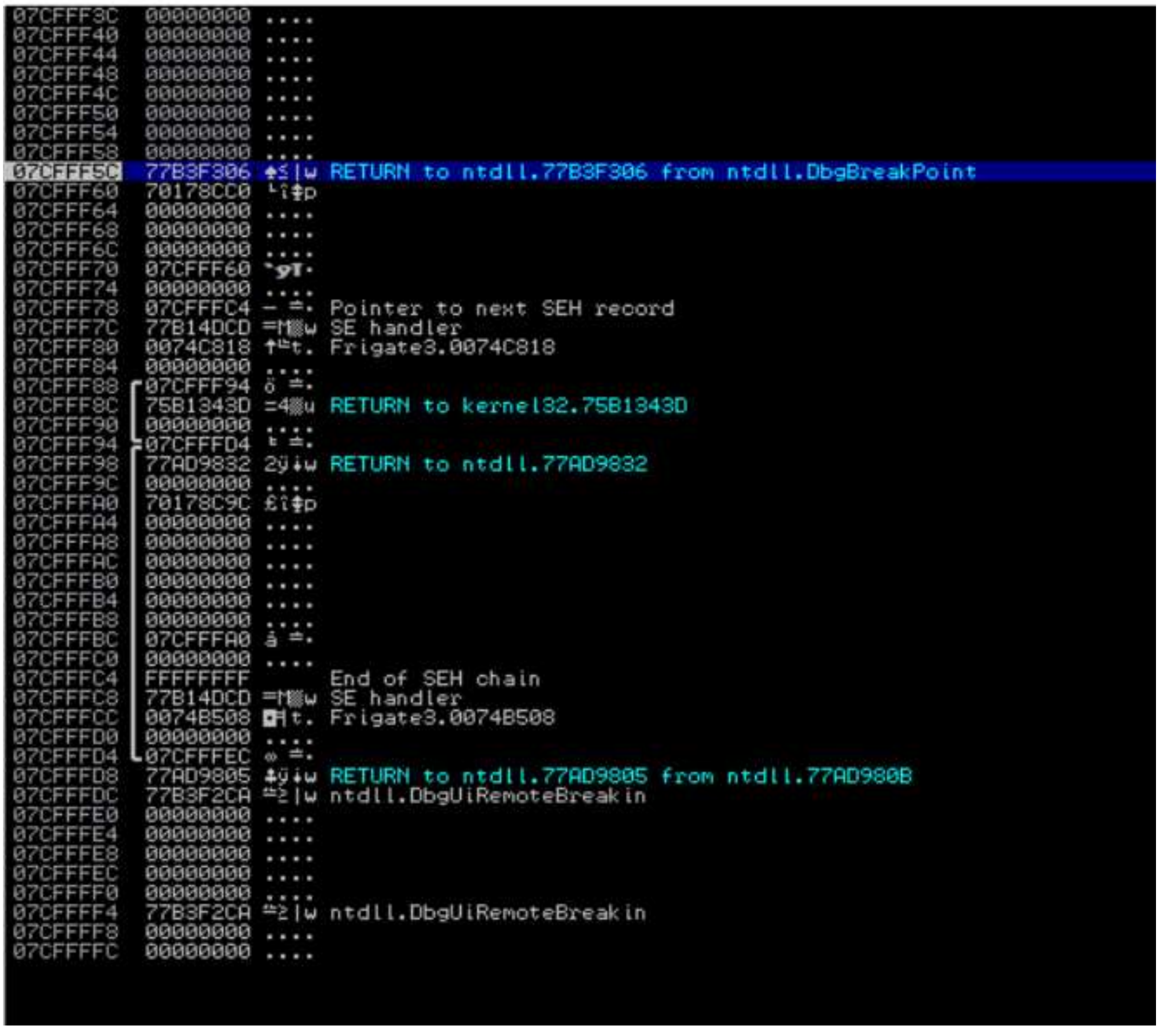
```
Modification of segment register
Privileged command
Modification of segment register
```

Check for EIP address



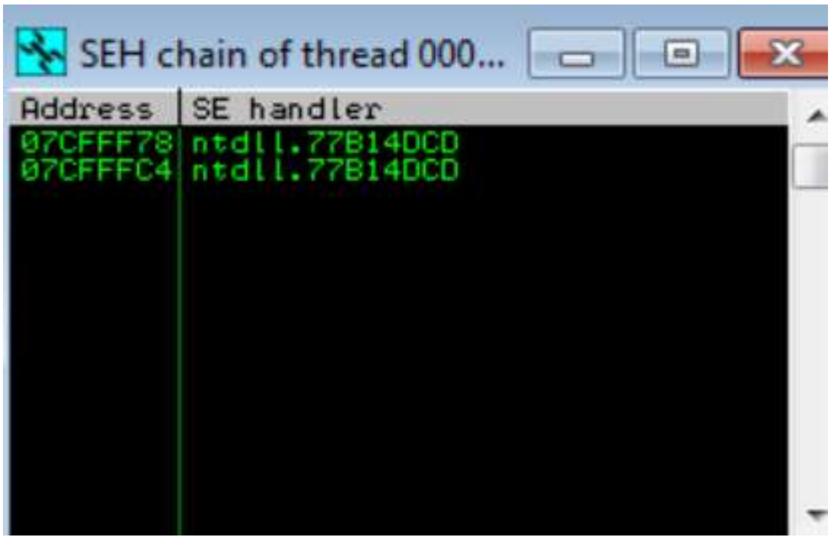
```
Registers (FPU)
EAX 00401000 Frigate3.<ModuleEntryPoint>
ECX 00000000
EDX 00000000
EBX 7EFDE000
ESP 0018FFF0
EBP 00000000
ESI 00000000
EDI 00000000

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 ♠≤|w RETURN to ntdll.77B3F306 from ntdll.DbgBreakPoint
07CFFF60  70178CC0 └î‡p
07CFFF64  00000000 ....
07CFFF68  00000000 ....
07CFFF6C  00000000 ....
07CFFF70  07CFFF60 `ϑ╤•
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 SSH chain and report the dll loaded along with address. For viewing SHE chain, go to view SEH



```
Address  | SE handler
07CFFF78 | ntdll.77B14DCD
07CFFFC4 | ntdll.77B14DCD
```