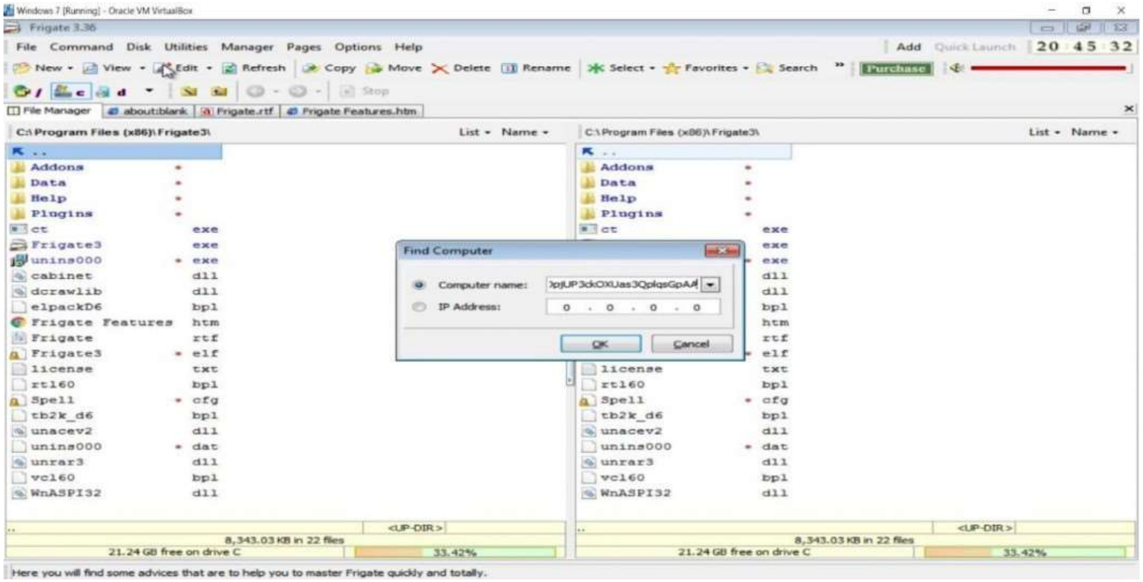
NAME:k.jayanth

REG.NO: 19bci7021

Crashing the Frigate3_Pro_v36 application and opening calc.exe (Calculator) by triggering it using the above generated payload:



C:\Program Files (x86)\Frigate3\

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

Find Computer

● Computer name:)pjUP3ckOXUas3QplqsGpA#

○ IP Address: 0 . 0 . 0 . 0

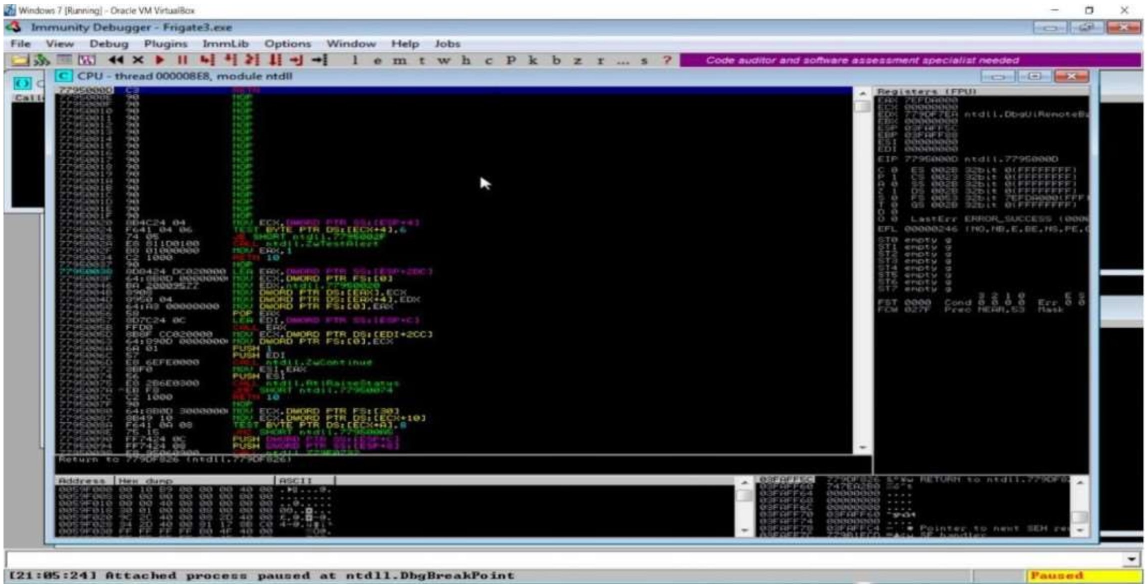
OK Cancel

8,343.03 KB in 22 files

21.24 GB free on drive C 33.42%

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

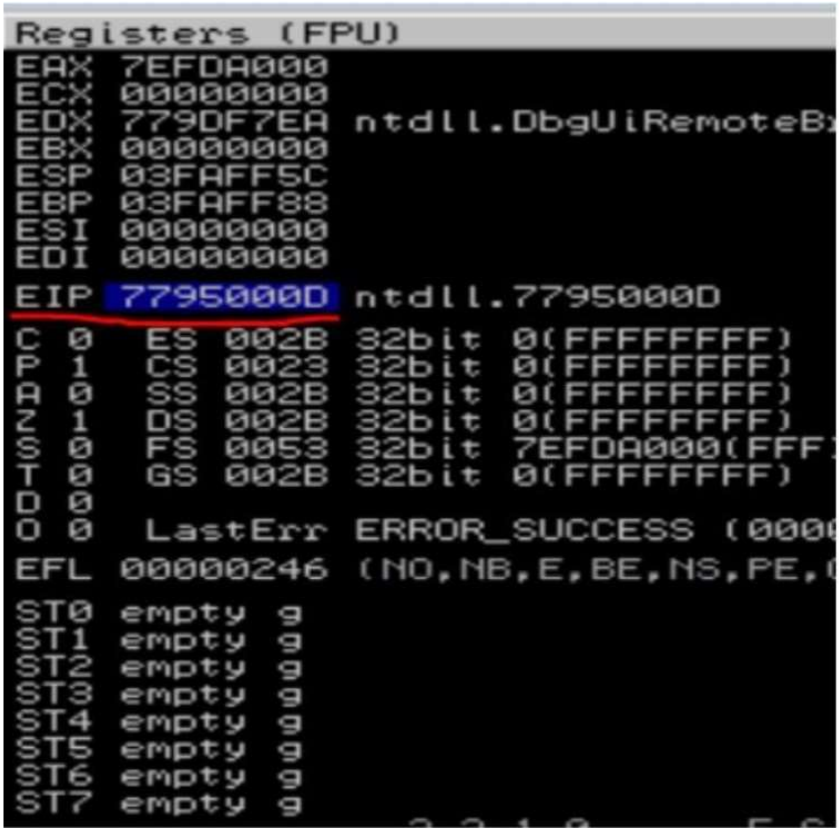
Before Execution (Exploitation): Attaching the debugger (Immunity debugger) to the application Frigate3_Pro_v36 and analysing the address of various registers:


Windows 7 [Running] - Oracle VM VirtualBox
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 ?
Code auditor and software assessment specialist needed
CPU - thread 000008E8, module ntdll
Registers (FPU)
Address Hex dump ASCII
Paused

```
Return to 779DF826 (ntdll.779DF826)
```

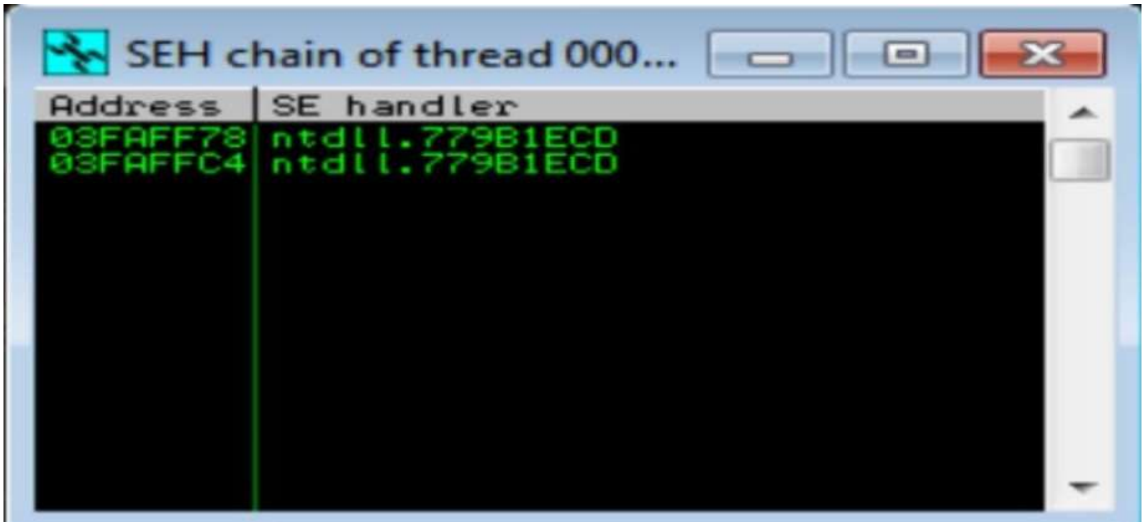
```
[21:05:24] Attached process paused at ntdll.DbgBreakPoint
```

Checking for EIP address:

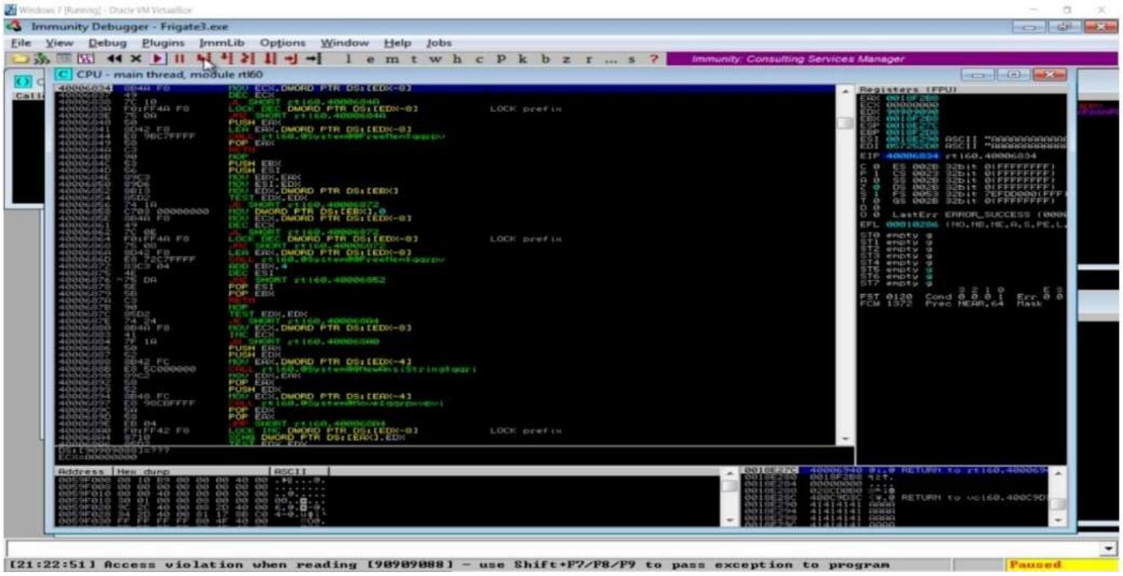


```
Registers (FPU)
EAX 7EFDA000
ECX 00000000
EDX 779DF7EA ntdll.DbgUiRemoteBr
EBX 00000000
ESP 03FAFF5C
EBP 03FAFF88
ESI 00000000
EDI 00000000
EIP 7795000D ntdll.7795000D
C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 7EFDA000(FFF
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (000
EFL 00000246 (NO,NB,E,BE,NS,PE,
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
```

Verifying the SHE chain:

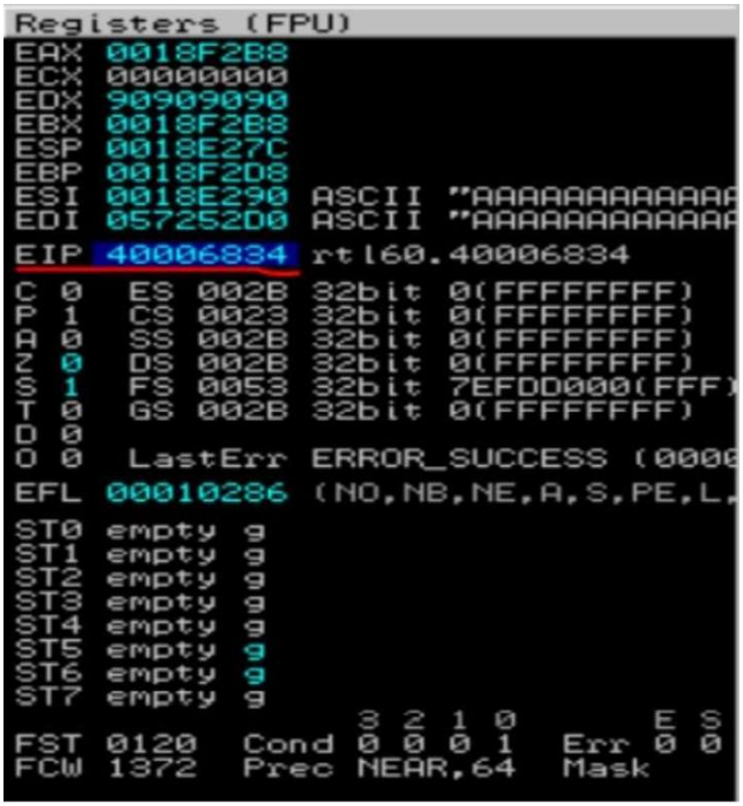


```
Address   SE handler
03FAFF78  ntdll.779B1ECD
03FAFFC4  ntdll.779B1ECD
```


Windows 7 [Running] - Oracle VM VirtualBox
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 rtl60
Registers (FPU)
Address Hex dump ASCII
Paused

```
[21:22:51] Access violation when reading [90909088] - use Shift+F7/F8/F9 to pass exception to program
```

Checkingfor EIP address:



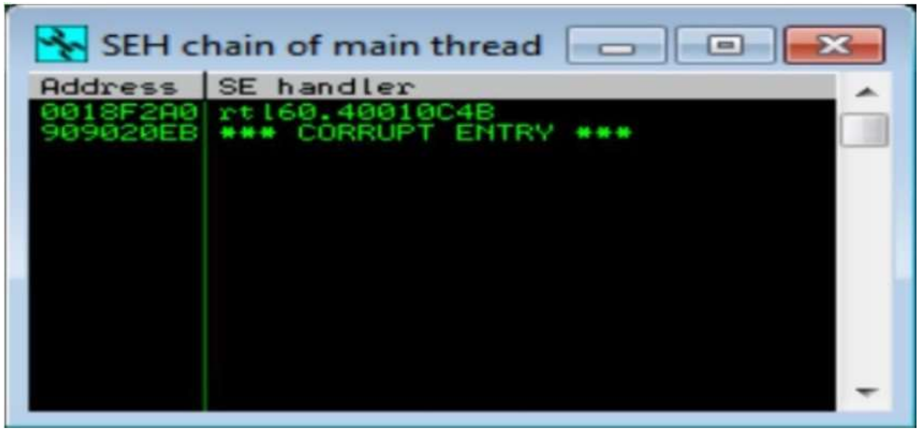
```
Registers (FPU)
EAX 0018F2B8
ECX 00000000
EDX 90909090
EBX 0018F2B8
ESP 0018E27C
EBP 0018F2D8
ESI 0018E290 ASCII "AAAAAAAAAAAAA
EDI 057252D0 ASCII "AAAAAAAAAAAAA

EIP 40006834 rtl60.40006834

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 1  FS 0053 32bit 7EFDD000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (000
EFL 00010286 (NO,NB,NE,A,S,PE,L,

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
FST 0120  Cond 0 0 0 1  Err 0 0
FCW 1372  Prec NEAR,64  Mask
```

Verifying the SHE chain and reporting the dll loaded along with the addresses:



```
Address   SE handler
0018F2A0  rtl60.40010C4B
909020EB  *** CORRUPT ENTRY ***
```

Hence from the above analysis we found that the dll ‘rtl60.40010C4B’iscorruptedandislocatedatthe address ‘0018F2A0’.