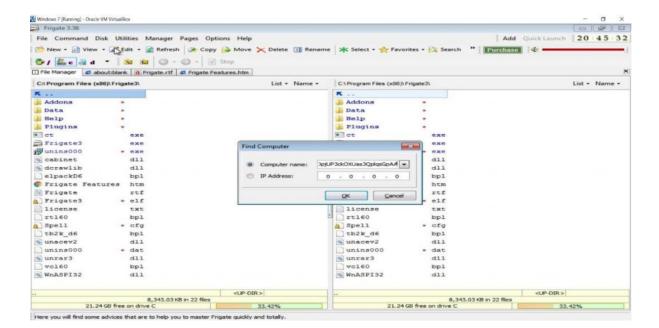
**NAME: Jayanth Chennupati** 

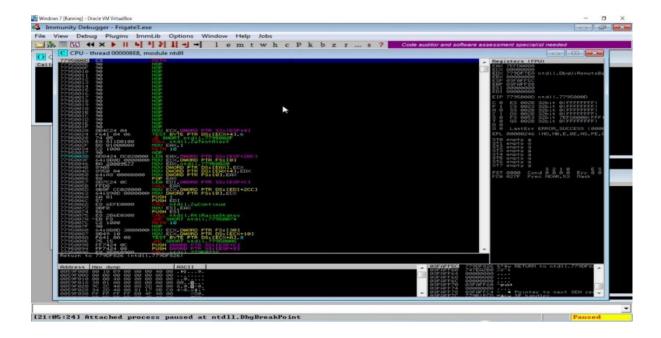
**REG.NO: 18BCN7084** 

**LAB-10** 

Crashing the Frigate3\_Pro\_v36 application and opening calc.exe (Calculator) by triggering it using the above generated payload:



Before Execution (Exploitation): Attaching the debugger (Immunity debugger) to the application Frigate3\_Pro\_v36 and analysing the address of various registers:



## Checking for EIP address:

```
(FPU)
Registers
     7EFDA000
00000000
     779DF7EA
00000000
                 ntdll.DbgUiRemoteB;
     Ø3FAFF
     Ø3FAFF88
     00000000
     00000000
     7795000D
                 ntdll.7795000D
                         0(FFFFFFFF
                 32bit
      čs
s
          0023
                 32bit
                         0(FFFFFFFF
  ø
          002B
                 32bit
                         0(FFFFFFFF)
                 325it
325it
325it
325it
                         Ø(FFFFFFFF)
ZEFDA000(FFF
  ã
          002B
0053
      DS
      FS
  Ø
          002B
                         0(FFFFFFFF)
О
  ø
      LastErr ERROR_SUCCESS (0000
0
  ø
     00000246 (NO,NB,E,BE,NS,PE,
     empty
             g
     empty
             g
             999
             g
             g
```

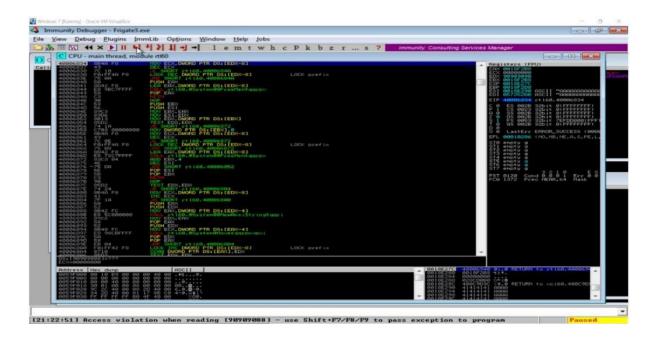
Verifying the SHE chain:

```
SEH chain of thread 000...

Address SE handler

08FAFF78 ntdll.779B1ECD

08FAFFC4 ntdll.779B1ECD
```



```
Registers (FPU)

EAX 0018F288

ECX 00000000

EDX 90909090

EBX 0018F288

ESP 0018E27C

EBP 0018E290 ASCII "AAAAAAAAAAAA

EDI 05725200 ASCII "AAAAAAAAAAAAA

EIP 40006834 rtl60.40006834

C 0 ES 0028 32bit 0(FFFFFFFF)

A 0 SS 0028 32bit 0(FFFFFFFF)

A 0 SS 0028 32bit 0(FFFFFFFF)

S 1 FS 0053 32bit 0(FFFFFFFF)

S 1 FS 0053 32bit 0(FFFFFFFF)

O 0 LastErr ERROR_SUCCESS (0006

EFL 00010286 (NO.NB.NE.A.S.PE.L.

ST0 empty 9

ST1 empty 9

ST1 empty 9

ST2 empty 9

ST3 empty 9

ST4 empty 9

ST5 empty 9

ST5 empty 9

ST6 empty 9

ST7 empty 9

ST7 empty 9

FST 0120 Cond 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:



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