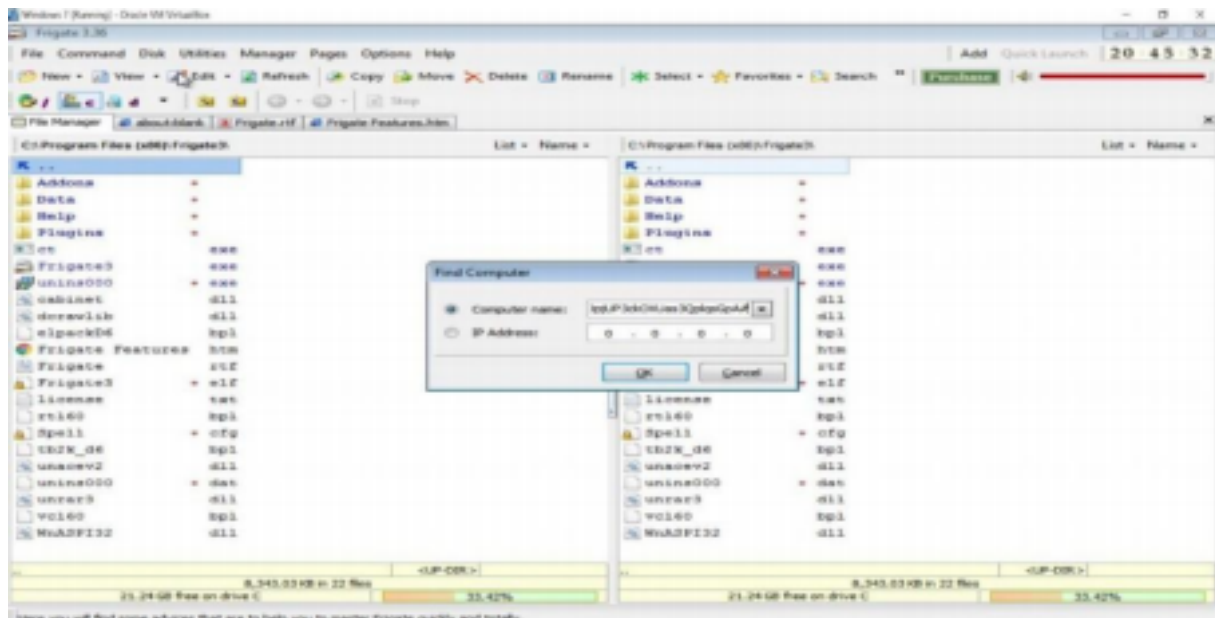


Lab-10

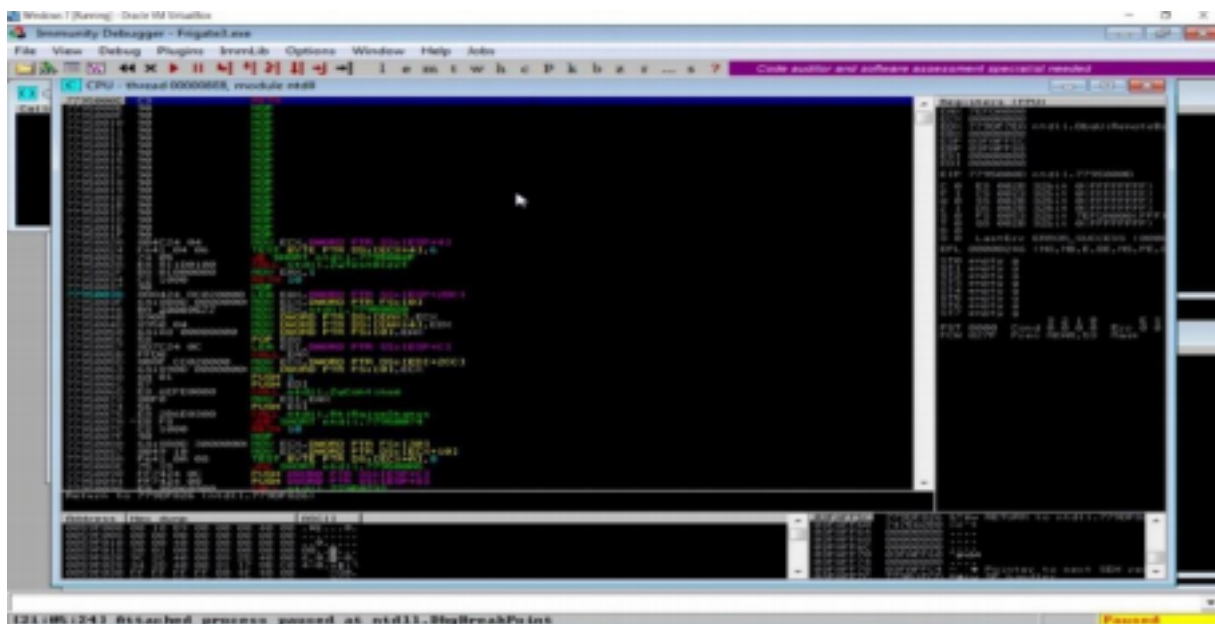
B.KRANTHI

18BCE7103

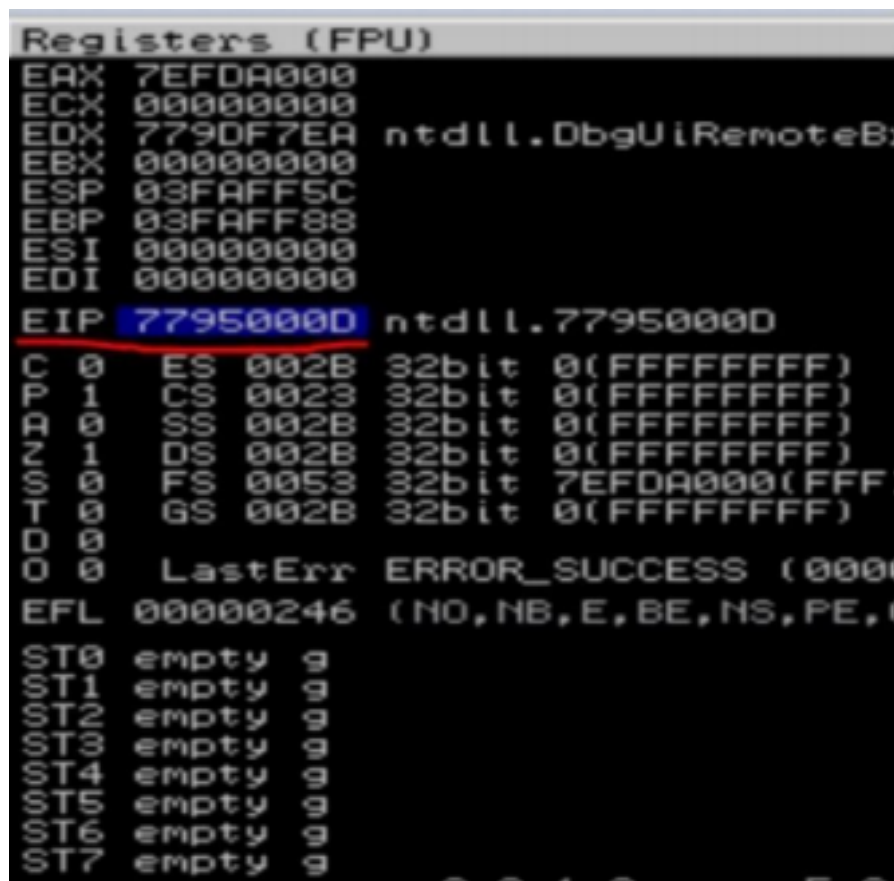
Crashing the Frigate3_Pro_v36 application and opening calc.exe (Calculator) by triggering it using the above generated payload:



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:

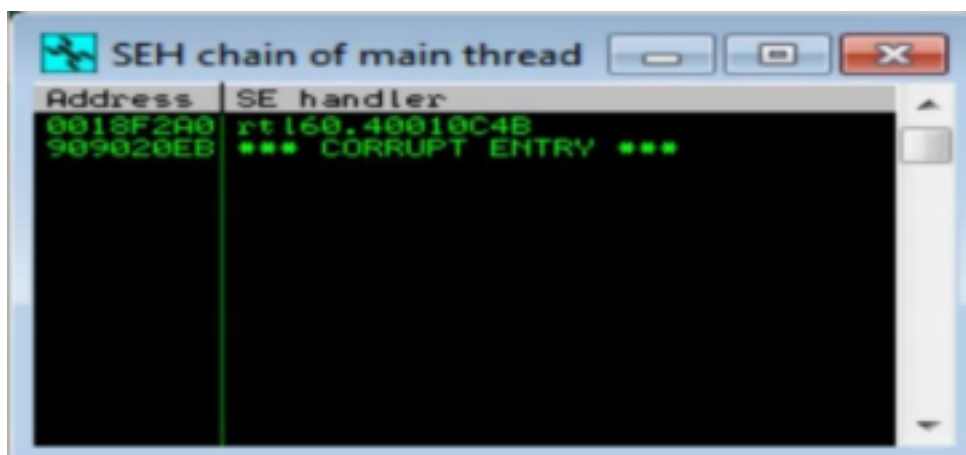


Verifying the SHE chain:

Checking for EIP address:

```
Registers (FPU)
EAX 0018F2B8
ECX 00000000
EDX 90909090
EBX 0018F2B8
ESP 0018E27C
EBP 0018F2D8
ESI 0018E290 ASCII "AAAAAAAAAAAAAA"
EDI 057252D0 ASCII "AAAAAAAAAAAAAA"
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 (0000)
EFL 00010286 (NO,NB,NE,A,S,PE,L)
ST0 empty 9
ST1 empty 9
ST2 empty 9
ST3 empty 9
ST4 empty 9
ST5 empty 9
ST6 empty 9
ST7 empty 9
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:



Hence from the above analysis we found that the dll 'rtl60.40010C4B' is corrupted and is located at the address '0018F2A0'.