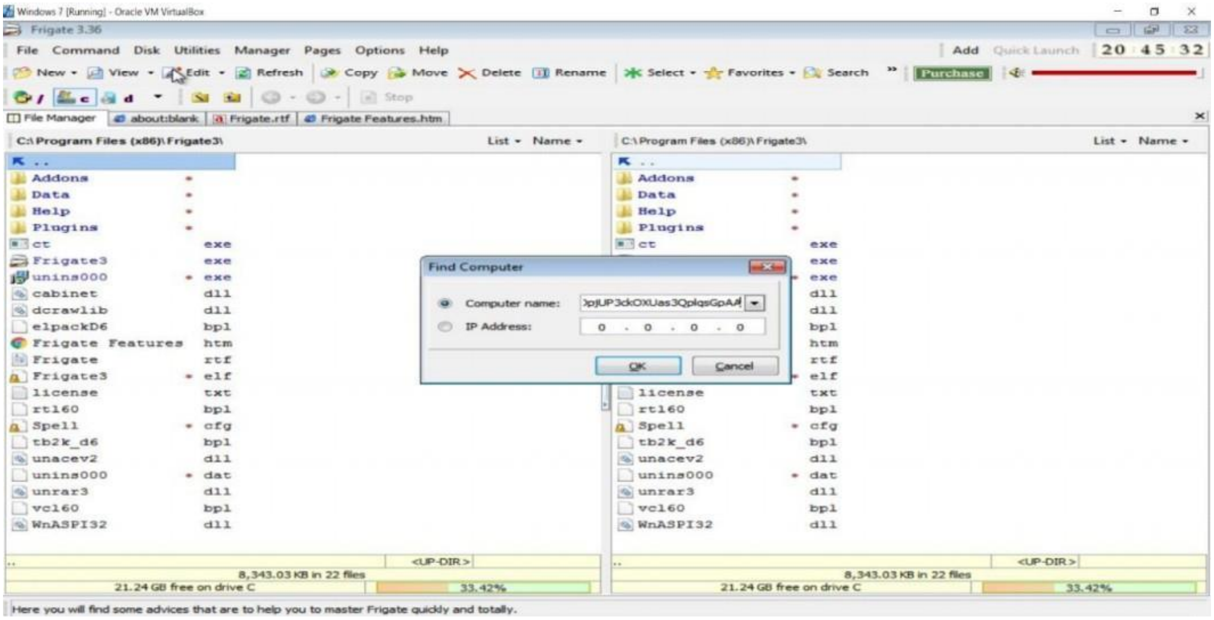
NAME: M SAI CHAITANYA

REG.NO: 18BCN7117

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

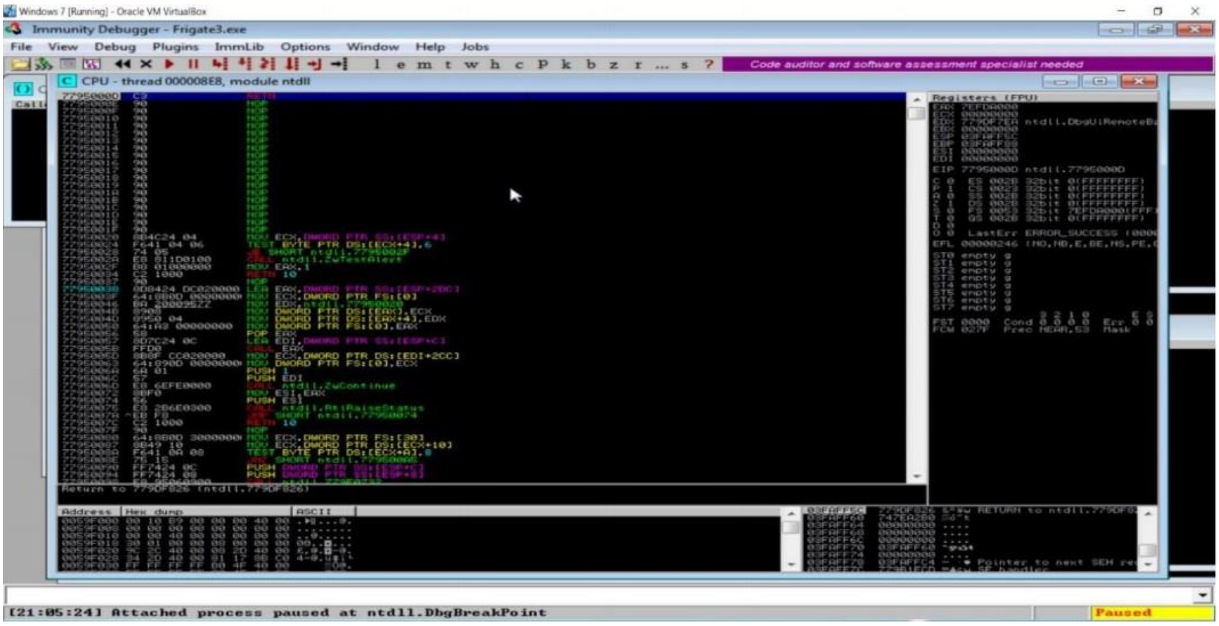


```
C:\Program Files (x86)\Frigate3\

..
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

<UP-DIR>
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.
```

Find Computer

● Computer name:)pjUP3ckOXUas3QplqsGpAA
○ IP Address: 0 . 0 . 0 . 0

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

```
7795000D  C3               RETN
7795000E  90               NOP
7795000F  90               NOP
77950010  90               NOP
77950011  90               NOP
77950012  90               NOP
77950013  90               NOP
77950014  90               NOP
77950015  90               NOP
77950016  90               NOP
77950017  90               NOP
77950018  90               NOP
77950019  90               NOP
7795001A  90               NOP
7795001B  90               NOP
7795001C  90               NOP
7795001D  90               NOP
7795001E  90               NOP
7795001F  90               NOP
77950020  8B4C24 04        MOV ECX,DWORD PTR SS:[ESP+4]
77950024  F641 04 06       TEST BYTE PTR DS:[ECX+4],6
77950028  74 05            JE SHORT ntdll.7795002F
7795002A  E8 811D0100      CALL ntdll.ZwTestAlert
7795002F  B8 01000000      MOV EAX,1
77950034  C2 1000          RETN 10
77950037  90               NOP
77950038  8D8424 DC020000  LEA EAX,DWORD PTR SS:[ESP+2DC]
7795003F  64:8B0D 00000000 MOV ECX,DWORD PTR FS:[0]
77950046  BA 20009577      MOV EDX,ntdll.77950020
7795004B  8908             MOV DWORD PTR DS:[EAX],ECX
7795004D  8950 04          MOV DWORD PTR DS:[EAX+4],EDX
77950050  64:A3 00000000   MOV DWORD PTR FS:[0],EAX
77950056  58               POP EAX
77950057  8D7C24 0C        LEA EDI,DWORD PTR SS:[ESP+C]
7795005B  FFD0             CALL EAX
7795005D  8B8F CC020000    MOV ECX,DWORD PTR DS:[EDI+2CC]
77950063  64:890D 00000000 MOV DWORD PTR FS:[0],ECX
7795006A  6A 01            PUSH 1
7795006C  57               PUSH EDI
7795006D  E8 6EFE0000      CALL ntdll.ZwContinue
77950072  8BF0             MOV ESI,EAX
77950074  56               PUSH ESI
77950075  E8 2B6E0300      CALL ntdll.RtlRaiseStatus
7795007A ^EB F8            JMP SHORT ntdll.77950074
7795007C  C2 1000          RETN 10
7795007F  90               NOP
77950080  64:8B0D 30000000 MOV ECX,DWORD PTR FS:[30]
77950087  8B49 10          MOV ECX,DWORD PTR DS:[ECX+10]
7795008A  F641 0A 08       TEST BYTE PTR DS:[ECX+A],8
7795008E  75 15            JNZ SHORT ntdll.779500A5
77950090  FF7424 0C        PUSH DWORD PTR SS:[ESP+C]
77950094  FF7424 08        PUSH DWORD PTR SS:[ESP+8]
Return to 779DF826 (ntdll.779DF826)
```

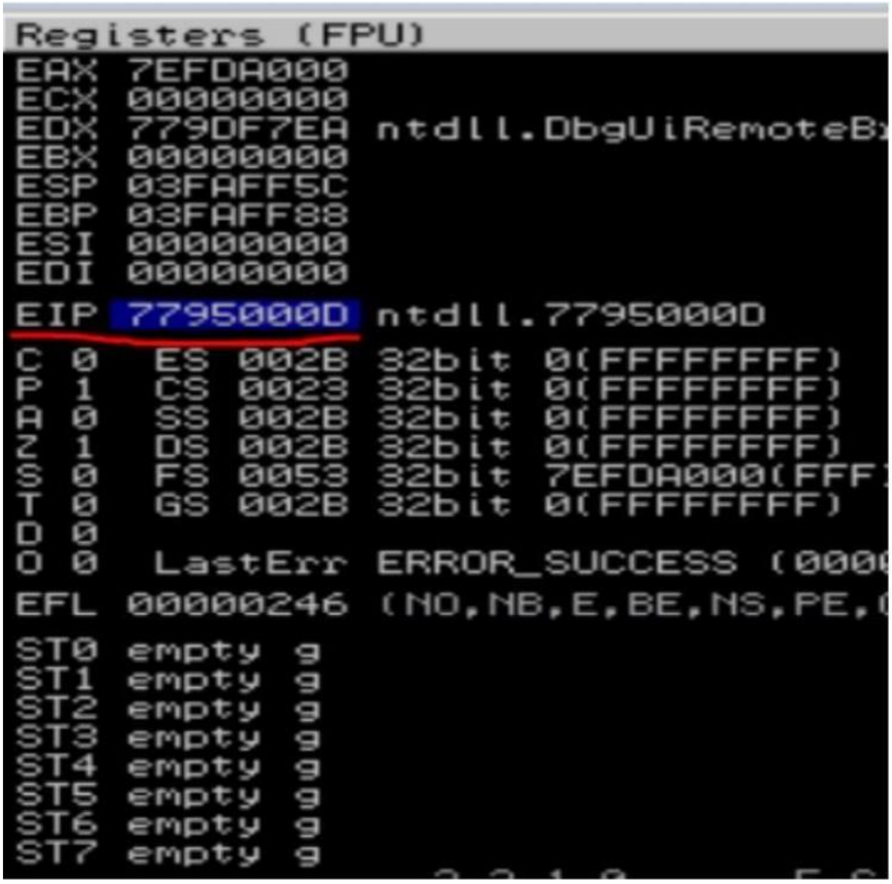
```
Address   Hex dump                  ASCII
0059F000  00 10 E9 00 00 00 40 00  .►é...@.
0059F008  00 00 00 00 00 00 00 00  ........
0059F010  00 00 40 00 00 00 00 00  ..@.....
0059F018  30 01 00 00 08 00 00 00  0☺......
0059F020  9C 2C 40 00 08 2D 40 00  £,@.◘-@.
0059F028  34 2D 40 00 01 17 8B C0  4-@.☺↨ï└
0059F030  FF FF FF FF 00 4F 40 00  ....O@.
```

```
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
               3 2 1 0      E S
FST 0000  Cond 0 0 0 0  Err 0 0
FCW 027F  Prec NEAR,53  Mask
```

```
03FAFF5C  779DF826  &°¥w  RETURN to ntdll.779DF8
03FAFF60  747EA2B0  ░ó~t
03FAFF64  00000000  ....
03FAFF68  00000000  ....
03FAFF6C  00000000  ....
03FAFF70  03FAFF60  `♠¶♥
03FAFF74  00000000  ....
03FAFF78  03FAFFC4  ─ ·♥  Pointer to next SEH re
03FAFF7C  779B1FCD  =▼¢w  SE handler
```

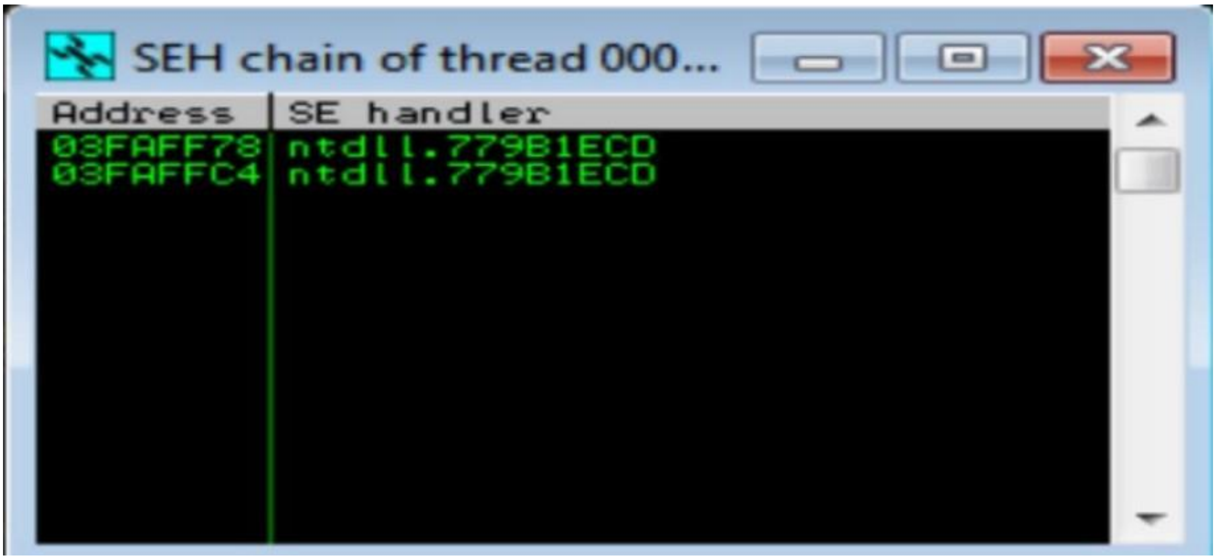
```
[21:05:24] Attached process paused at ntdll.DbgBreakPoint
```

Checking for EIP address:

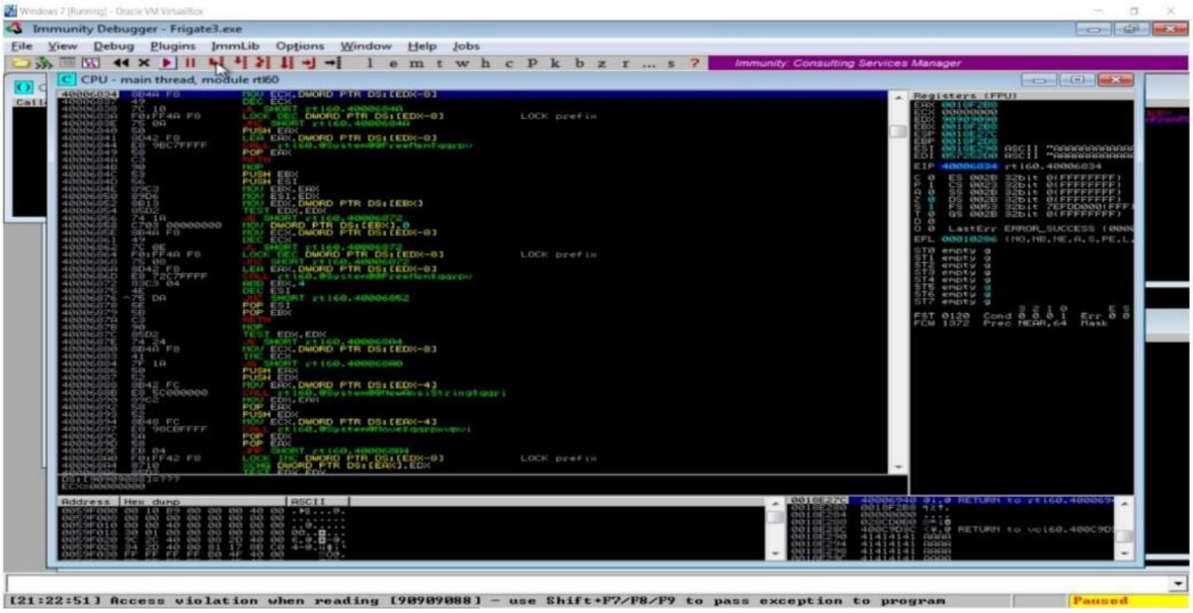


```
Registers (FPU)
EAX 7EFDA000
ECX 00000000
EDX 779DF7EA ntdll.DbgUiRemoteBr
EBX 00000000
ESP 03FAFF5C
EBP 03FAFF88
ESI 00000000
EDI 00000000

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:



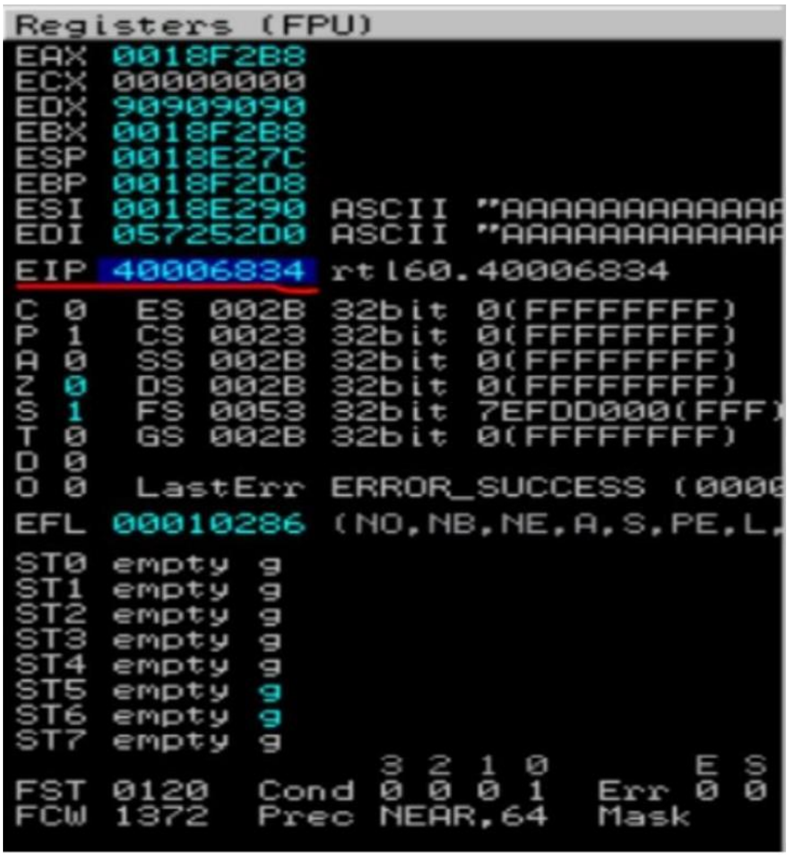
```
Address  SE handler
03FAFF78 ntdll.779B1ECD
03FAFFC4 ntdll.779B1ECD
```


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)
EAX 0018F2B8
ECX 00000000
EDX 90909090
EBX 0018F2B8
ESP 0018E27C
EBP 0018F2D0
ESI 0018E290 ASCII "AAAAAAAAAAAA
EDI 05725200 ASCII "AAAAAAAAAAAA
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
```

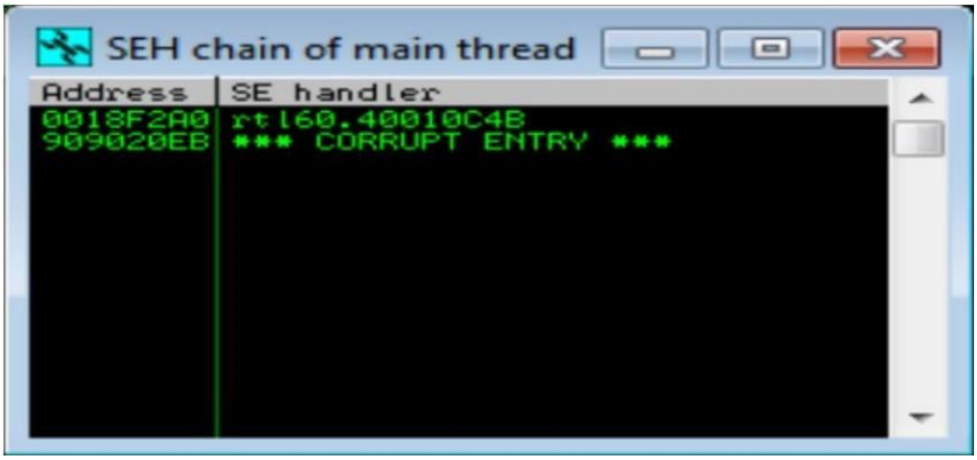
```
[21:22:51] Access violation when reading [90909088] - use Shift+F7/F8/F9 to pass exception to program
```

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 (0000
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:



```
SEH chain of main thread
Address   SE handler
0018F2A0  rtl60.40010C4B
909020EB  *** CORRUPT ENTRY ***
```

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