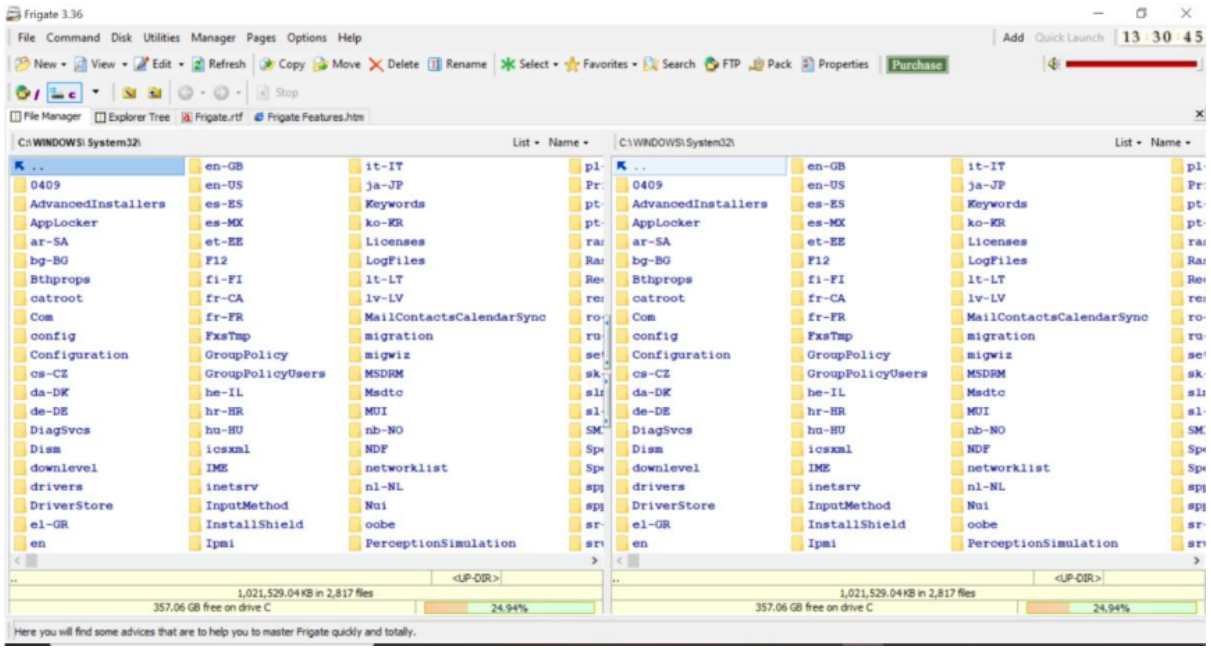
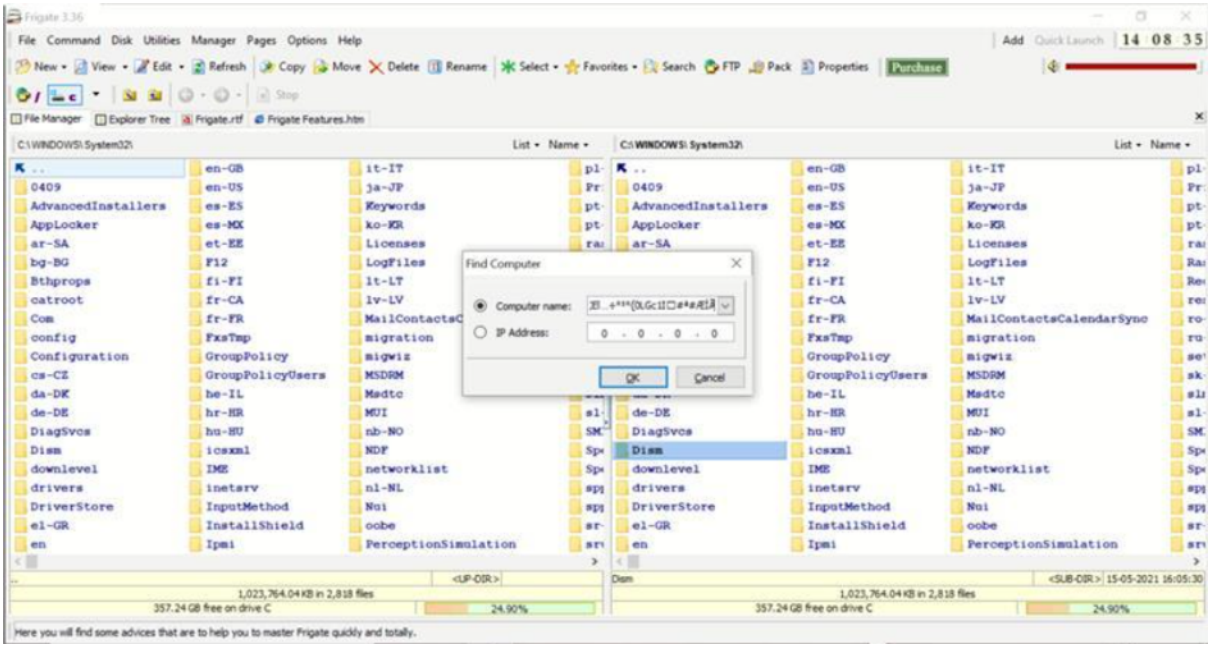
Secure Coding Lab - 10

Name: Charitha Bodapothula
Reg.No: 19BCN7005
Slot: L23+24

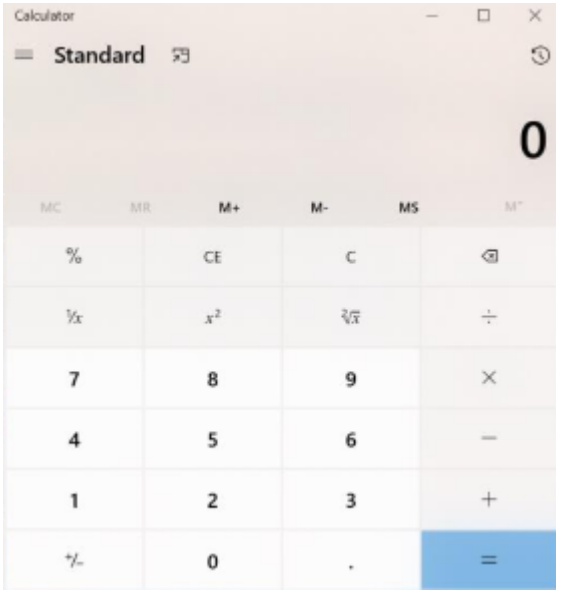
Install frigate



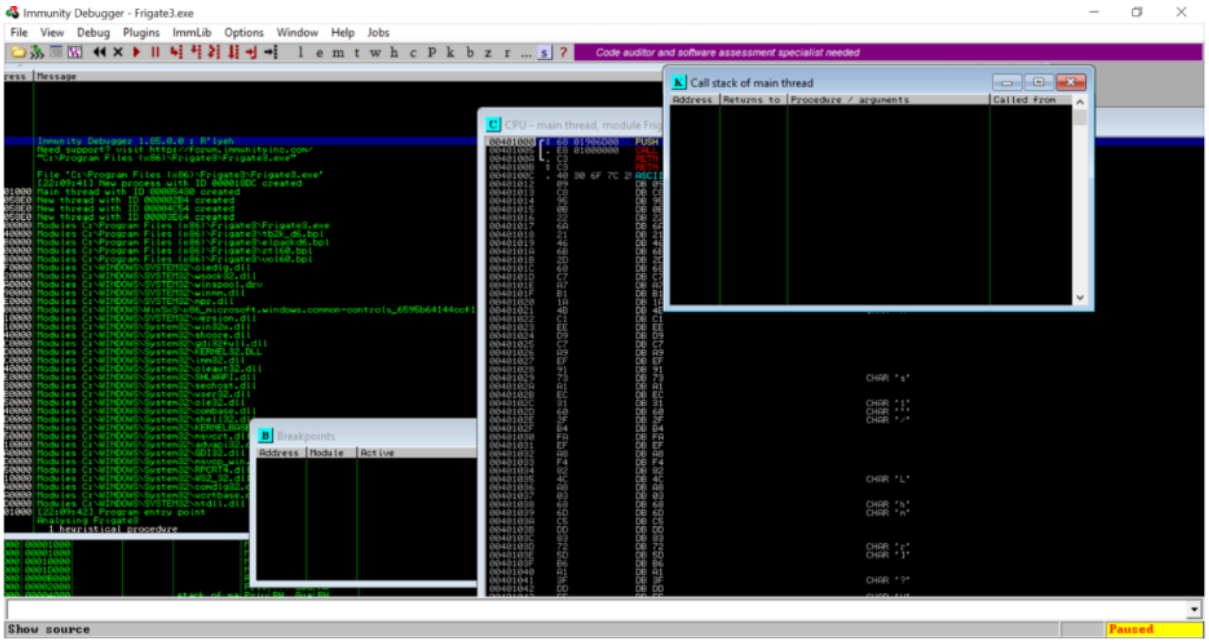
Generate the payload
Crash the payload using frigate3



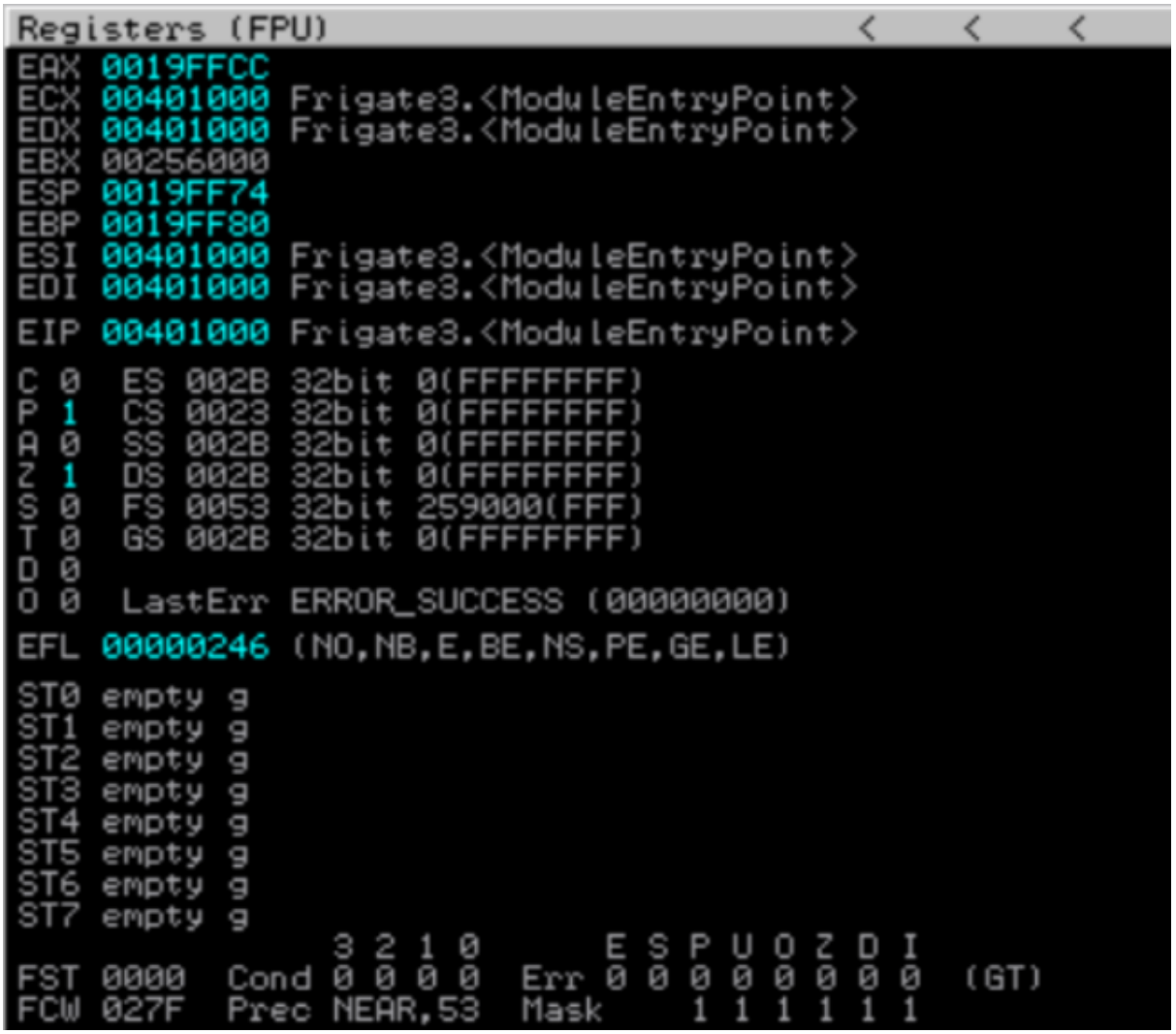
This triggers the calculator



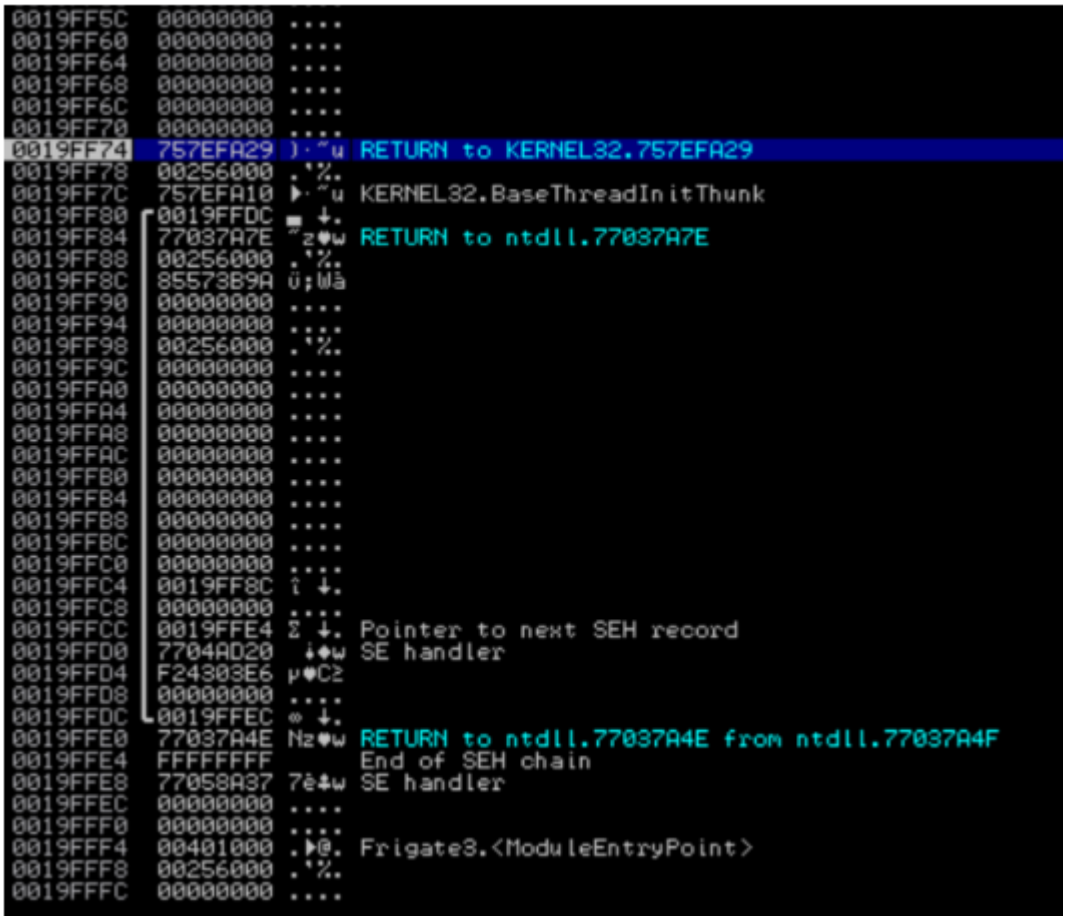
Immunity Debugger



Register Addresses



dll which are loaded are shown here


0019FF5C 00000000 ....
0019FF60 00000000 ....
0019FF64 00000000 ....
0019FF68 00000000 ....
0019FF6C 00000000 ....
0019FF70 00000000 ....
0019FF74 757EFA29)·~u RETURN to KERNEL32.757EFA29
0019FF78 00256000 .%.
0019FF7C 757EFA10 ▶·~u KERNEL32.BaseThreadInitThunk
0019FF80 0019FFDC ▀ ↓.
0019FF84 77037A7E ~z♥w RETURN to ntdll.77037A7E
0019FF88 00256000 .%.
0019FF8C 85573B9A ü;Wà
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 î ↓.
0019FFC8 00000000 ....
0019FFCC 0019FFE4 Σ ↓. Pointer to next SEH record
0019FFD0 7704AD20 ↓♦w SE handler
0019FFD4 F24303E6 µ♥C≥
0019FFD8 00000000 ....
0019FFDC 0019FFEC ∞ ↓.
0019FFE0 77037A4E Nz♥w RETURN to ntdll.77037A4E from ntdll.77037A4F
0019FFE4 FFFFFFFF End of SEH chain
0019FFE8 77058A37 7è♣w SE handler
0019FFEC 00000000 ....
0019FFF0 00000000 ....
0019FFF4 00401000 .▶@. Frigate3.<ModuleEntryPoint>
0019FFF8 00256000 .%.
0019FFFC 00000000 ....