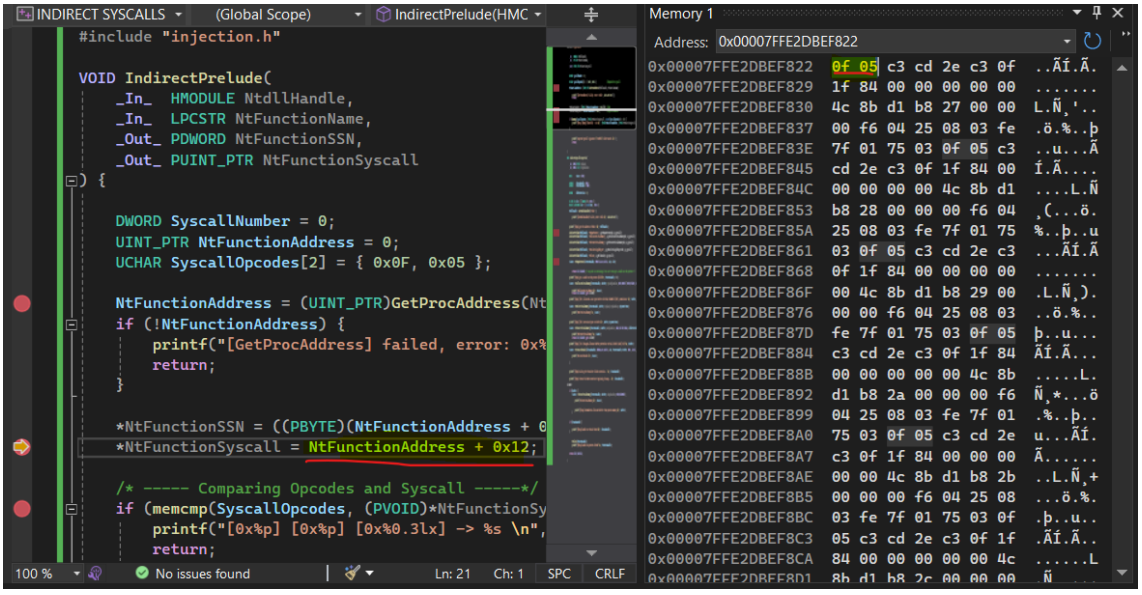
Indirect Syscall

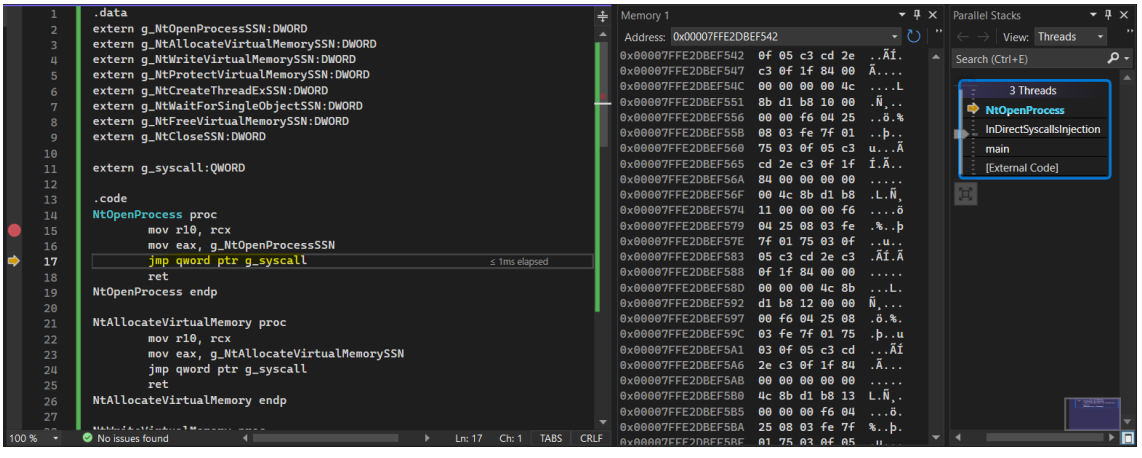
Debugging Code for Indirect Syscall



Opcode for Syscall

1. Flow

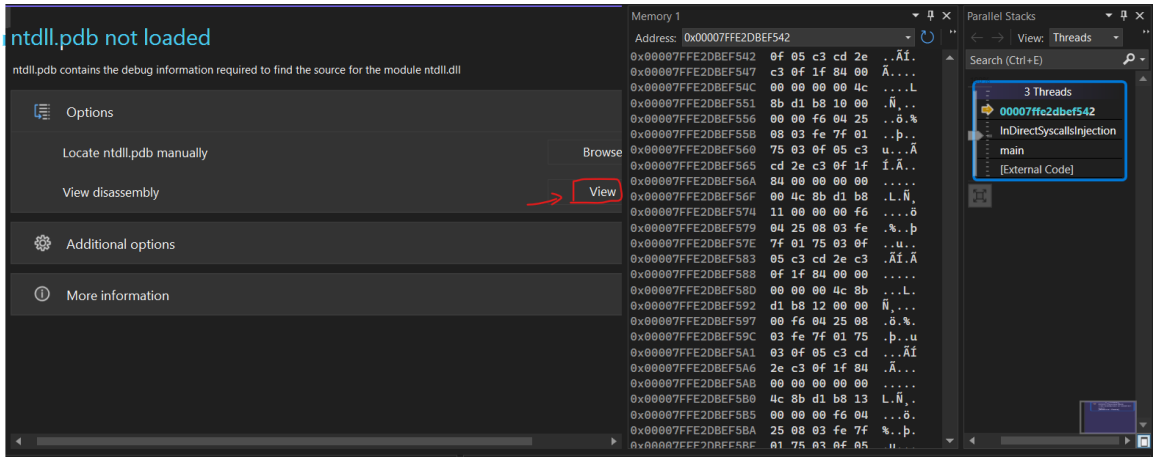
➡️ Making a Unconditional Jump to address assigned to g_syscall (Global variable storing op codes for syscall)



jmp qword ptr g_syscall

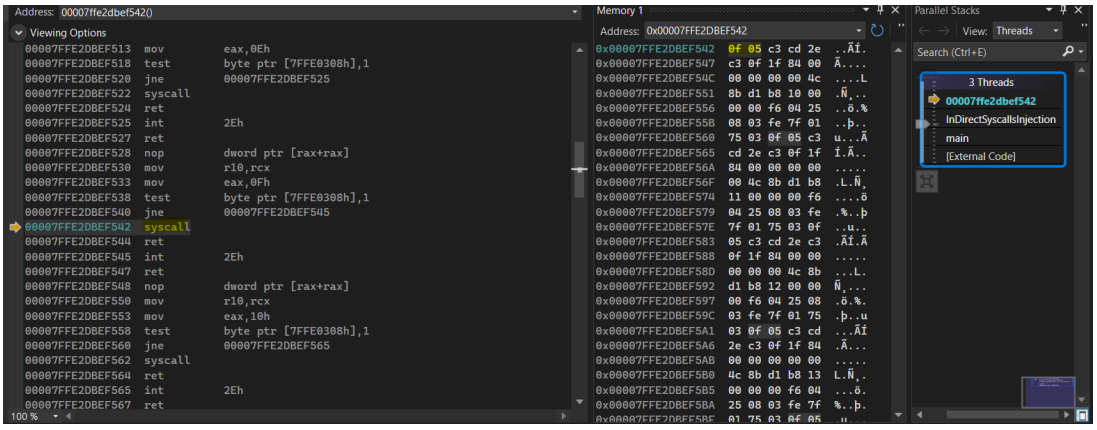
➡️ No Syscall Issued…

Jumping to something we don't have source code of it.



On Source Code

➡️ Jumping to Syscall (i.e Opcode syscall we have defined…) indirectly



View Disassembly

2. Output :

➡️Popping Calc.exe