Project #2: Using The Debugger

Santosh Ramesh ONID: #933674448

CS 271 Computer Architecture & Assembly Redfield & Vogel 1-27-21

Part #1: Initial Setup

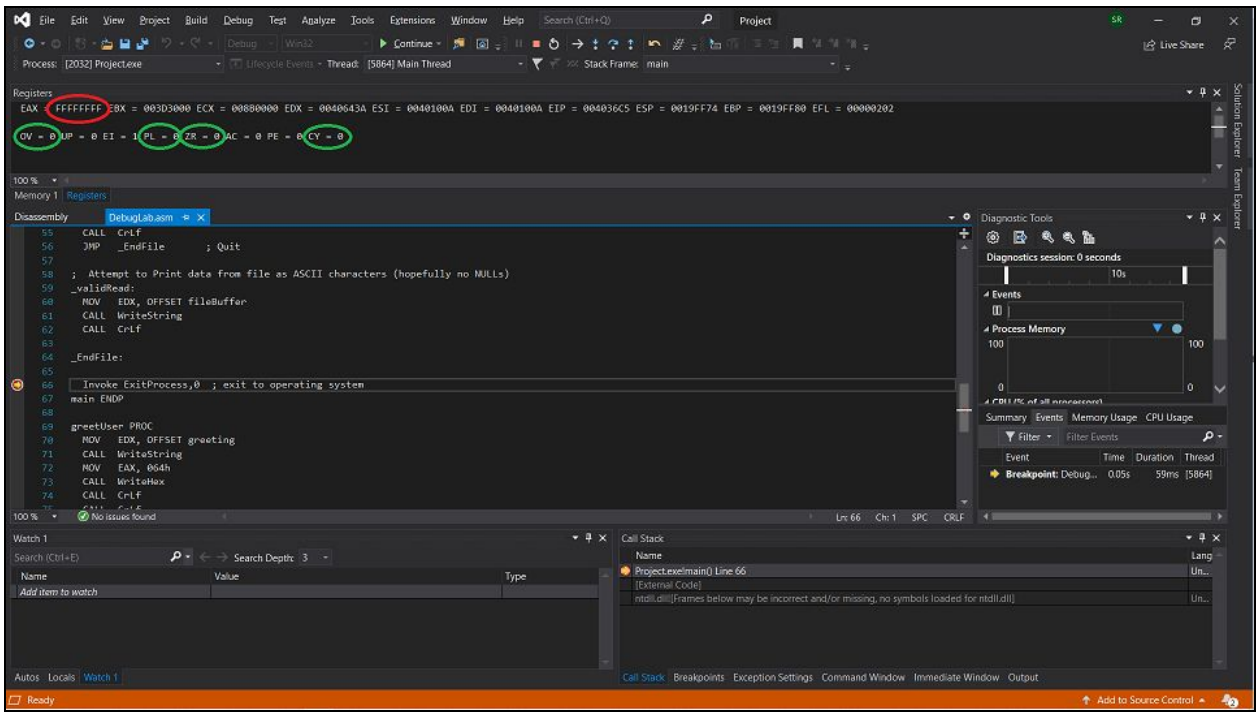

Figure 1.1

- 1. Current value of EAX: FFFFFFFF (value circled in red in *Figure 1.1*)
- 2. Current states of flags (values circled in green in *Figure 1.1*):
    - Carry: 0
    - Overflow: 0
    - Zero: 0
    - Sign: 0

Part #2: Navigating Code and Procedures

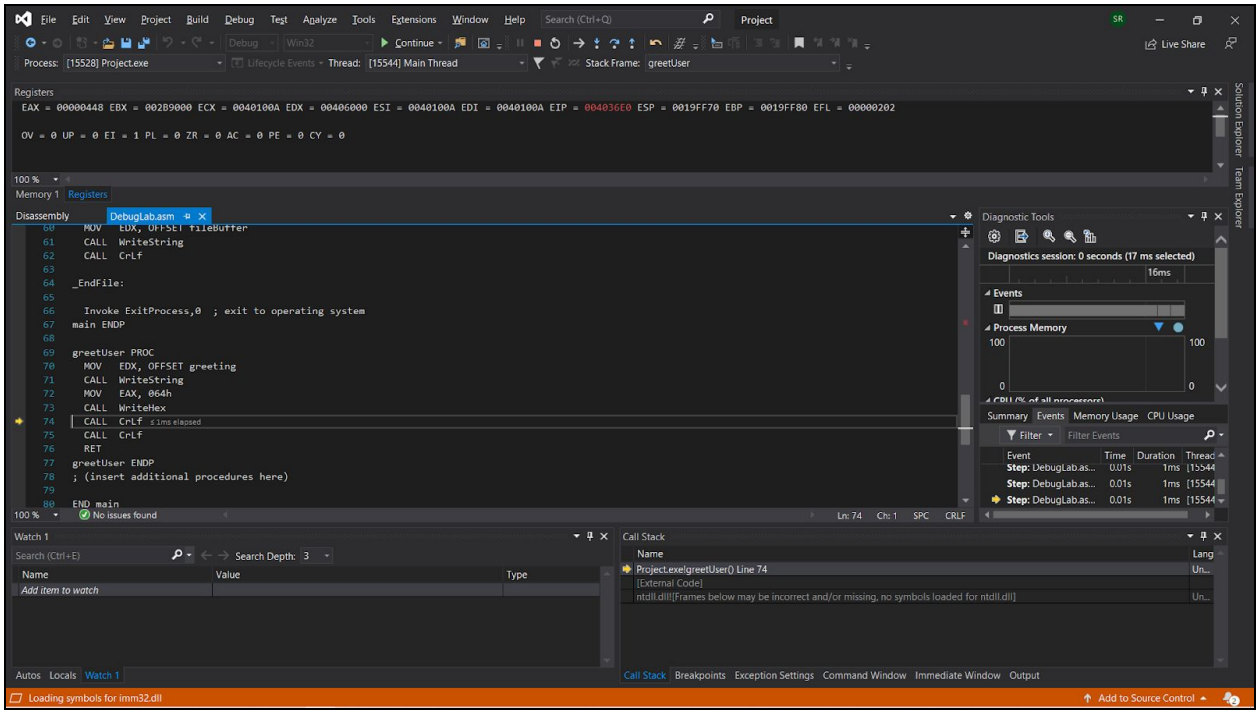

Figure 2.1

- 3. Attached below is my "user number" which I acquired from the last 3 digits of my ONID (#933-674-448) (*Figure 2.2*)

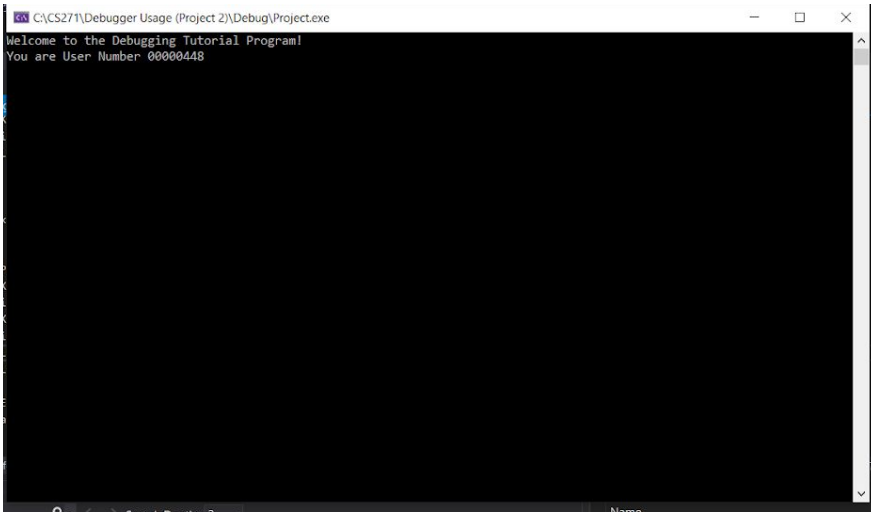

Figure 2.2

Part #3: Disassembly View

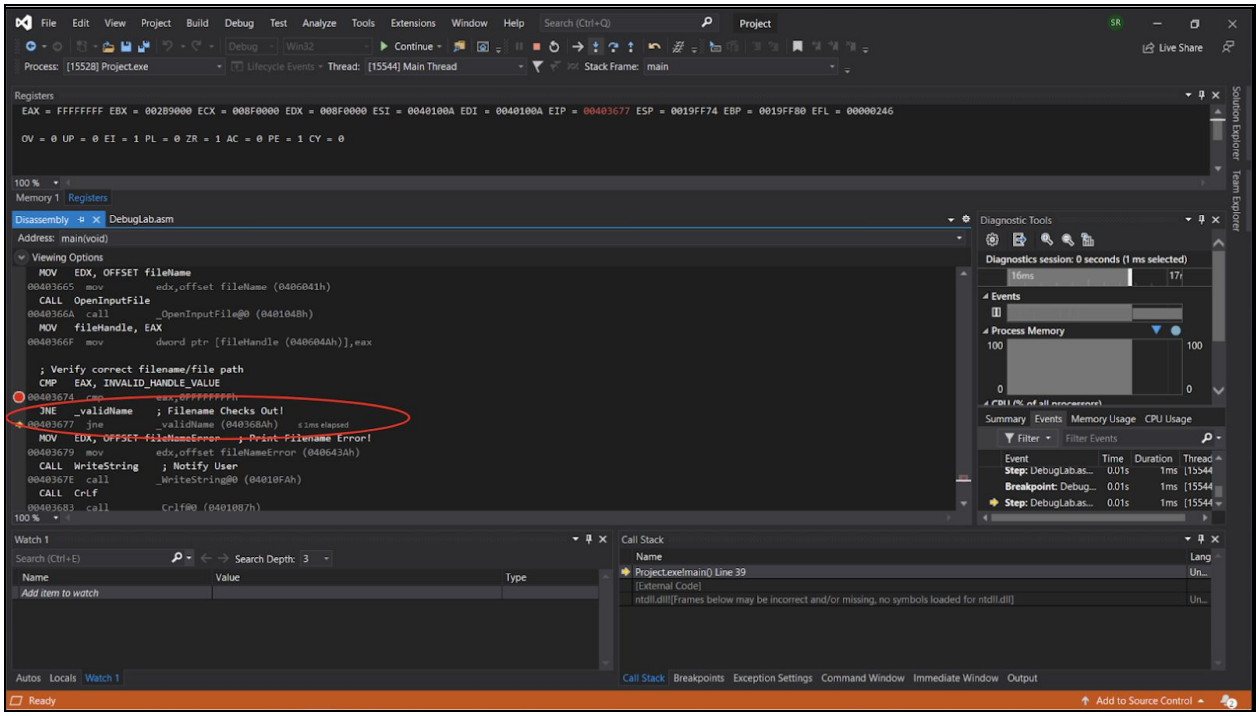

Figure 3.1

- 4. memory address of "_validName": 040368Ah
- 5. The "JNE" instruction is stored at this code segment. Technically speaking, the code label itself represents an operand that is being used for the JNE Jcond (refer to *Figure 3.1*):
    - instruction: `JNE _validName ; Filename Checks Out!`
- 6. The EIP is always going to the be exact same as the leftmost value on any given line, as it is the instruction pointer (pointing to the current-most instruction).

Part #4: Spelunking through Memory

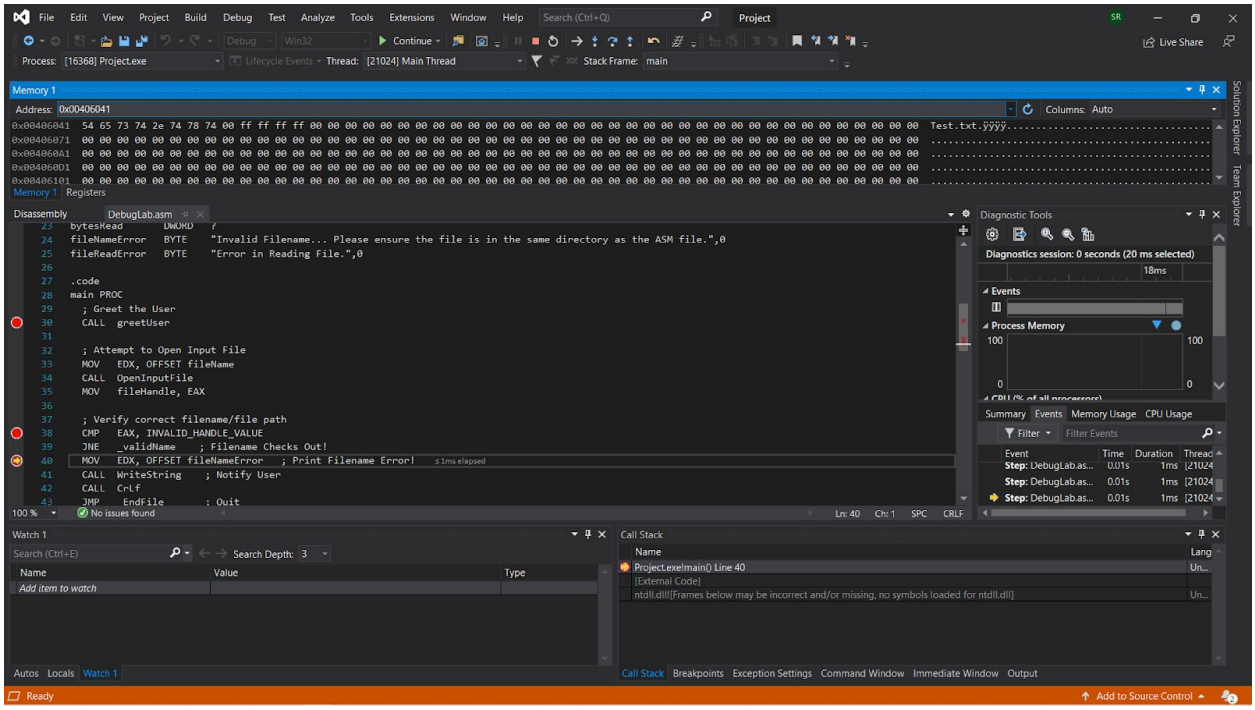

Figure 4.1: Searching up the Address of the "fileName"

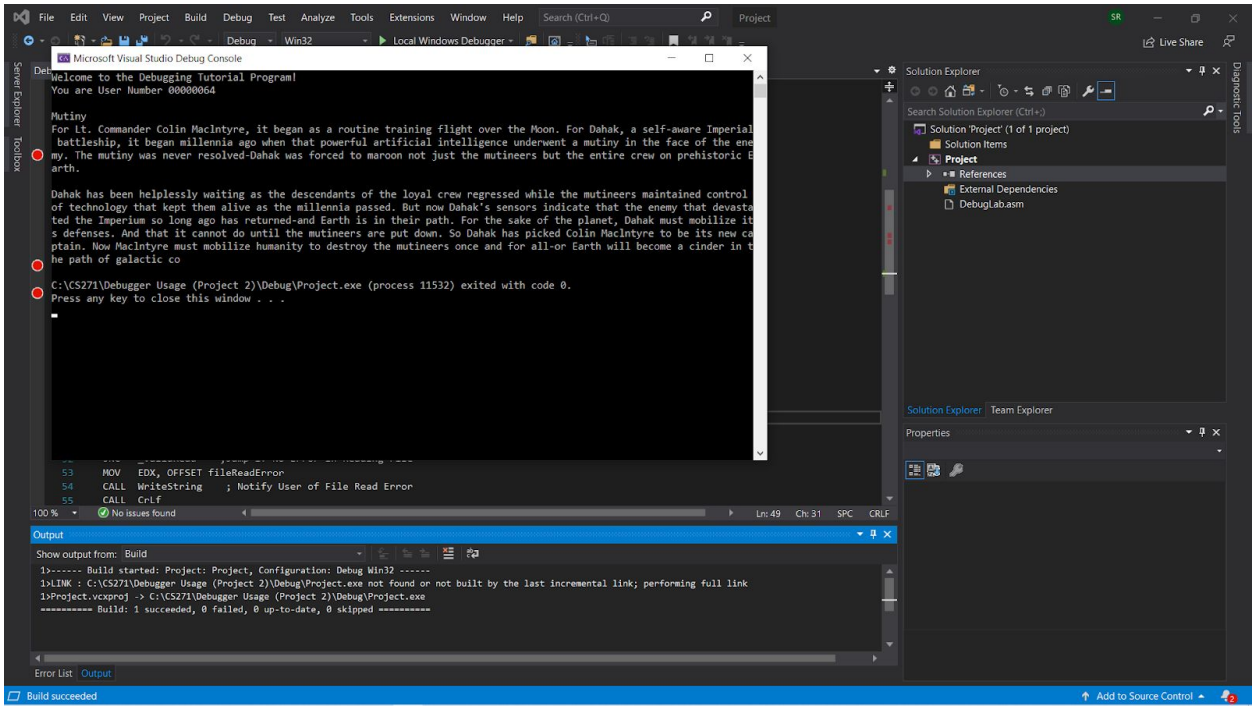

Figure 4.2: The text printing out to the console, with no bugs

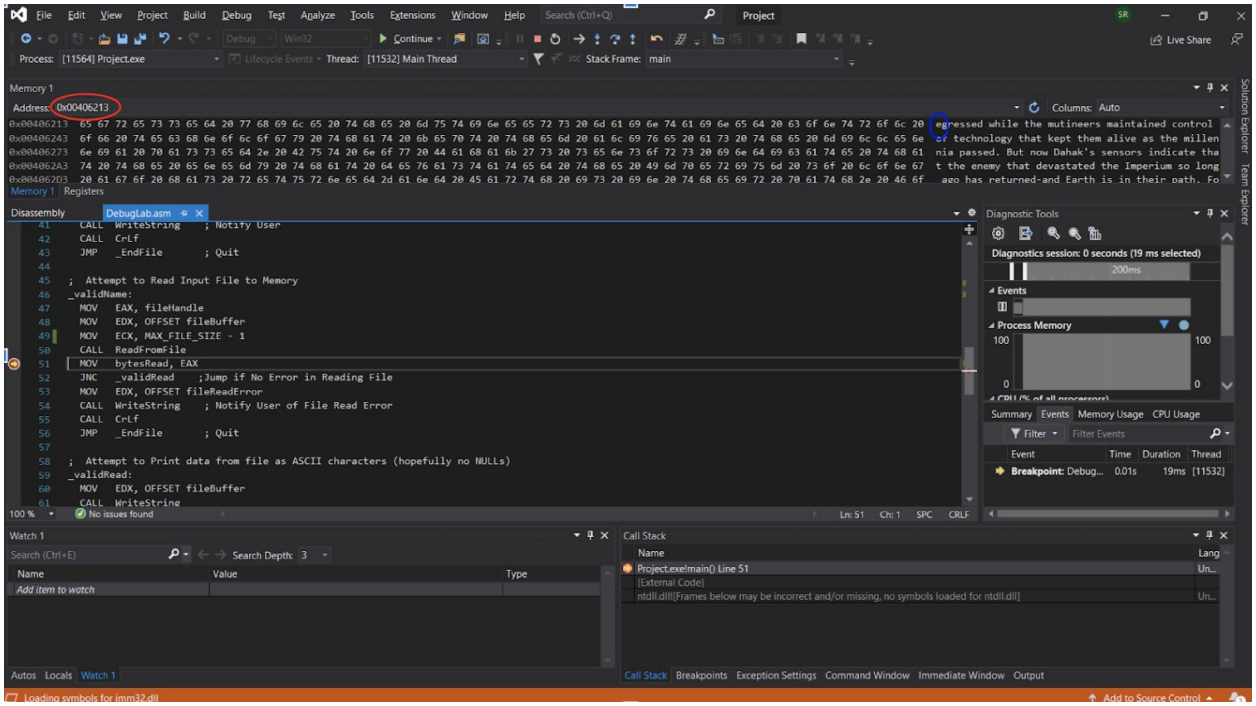

Figure 4.3

- 7. Given n = 448, the "n+1" byte of TestText.txt is the ASCII character "e" (*Figure 4.3*)
- 8. The screenshot of the Memory window for the previous question is in "Figure 4.3"
    - Memory address value circled in red
    - ASCII character value circled in blue

Part #5: Keeping Careful Watch

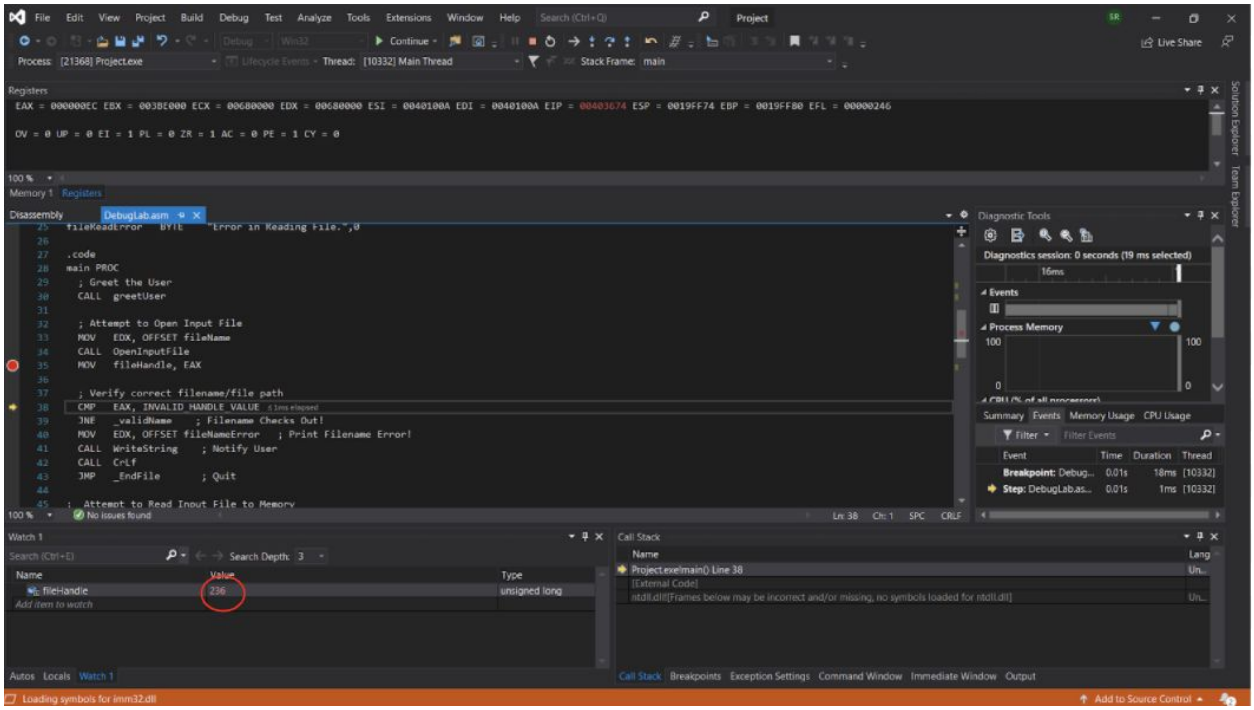

Figure 5.1

- 9. The value of "fileHandle" after opening the TestText.txt file is "236"
    - (circled in red in *Figure 5.1*)