Derek Greene
934603866
4/23/2024

Part 1 - Initial Setup

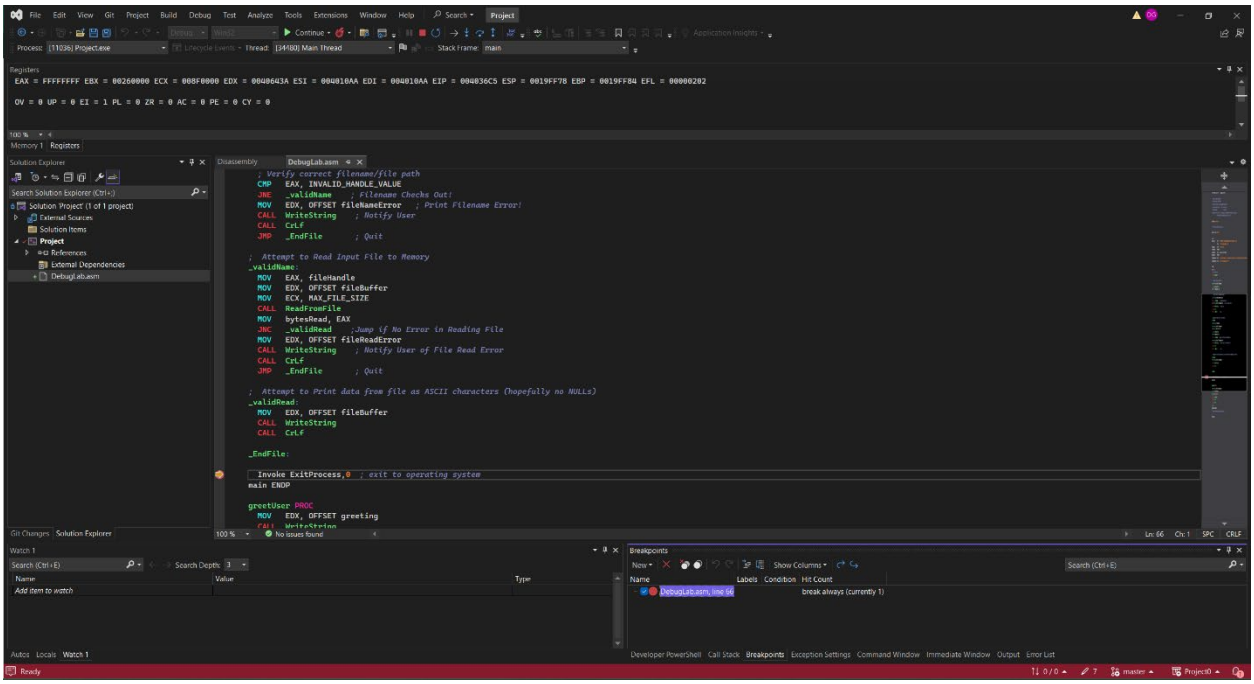

Figure 1: Part 1 - Initial Setup

Part 1 Questions

1. FFFFFFFF

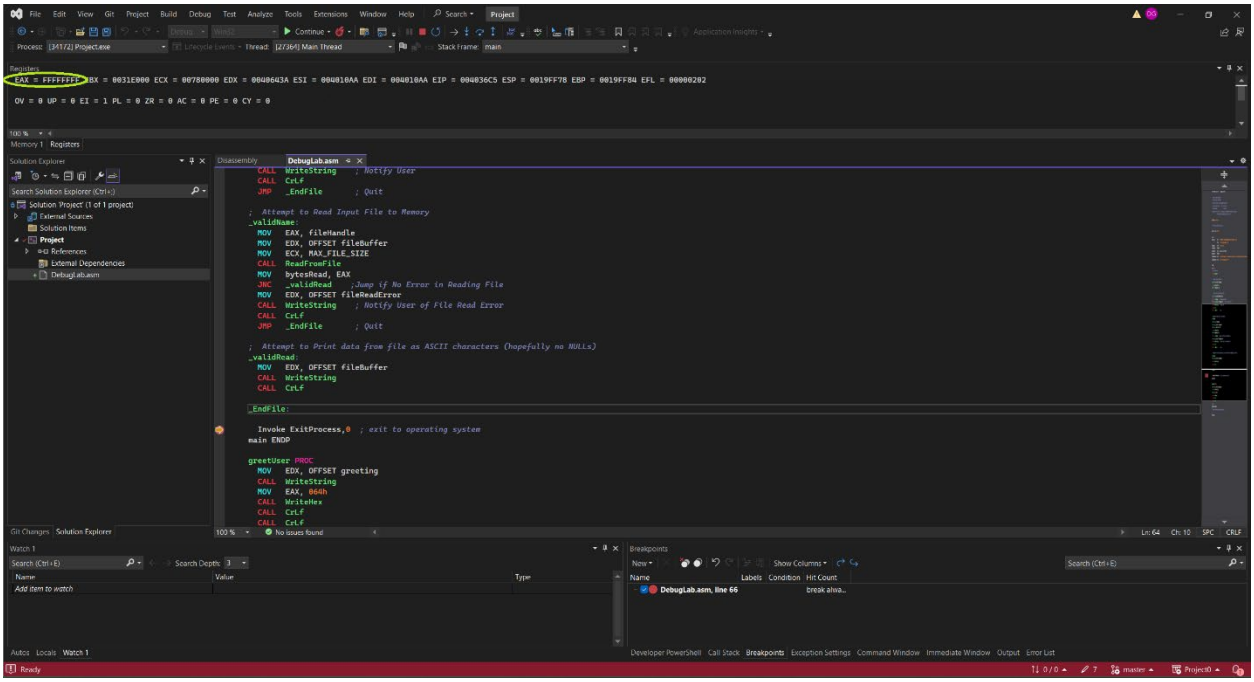

Figure 2: Part 1 - Question # 1

Derek Greene
934603866
4/23/2024
2. CY = 0 (clear) OV = 0 (clear) ZR = 0 (clear) PL = 0 (clear)

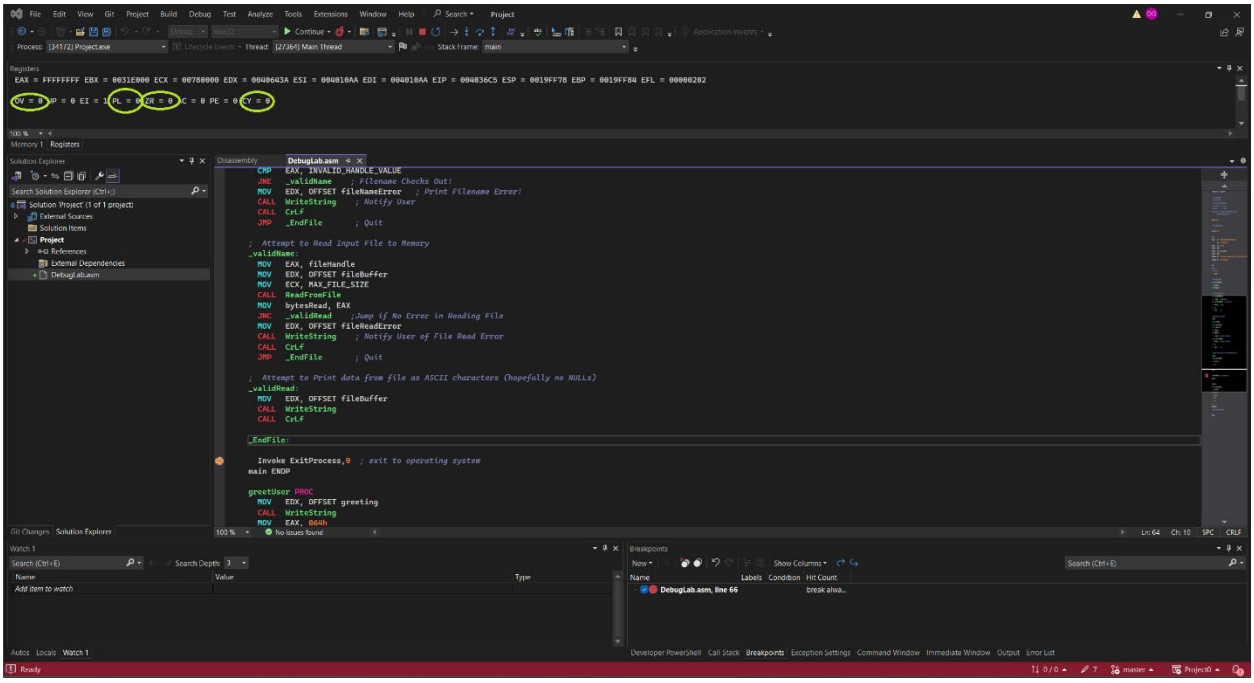

Figure 3: Part 1 - Question # 2

Part 2 – Navigating Code and Procedures

Part 2 Questions

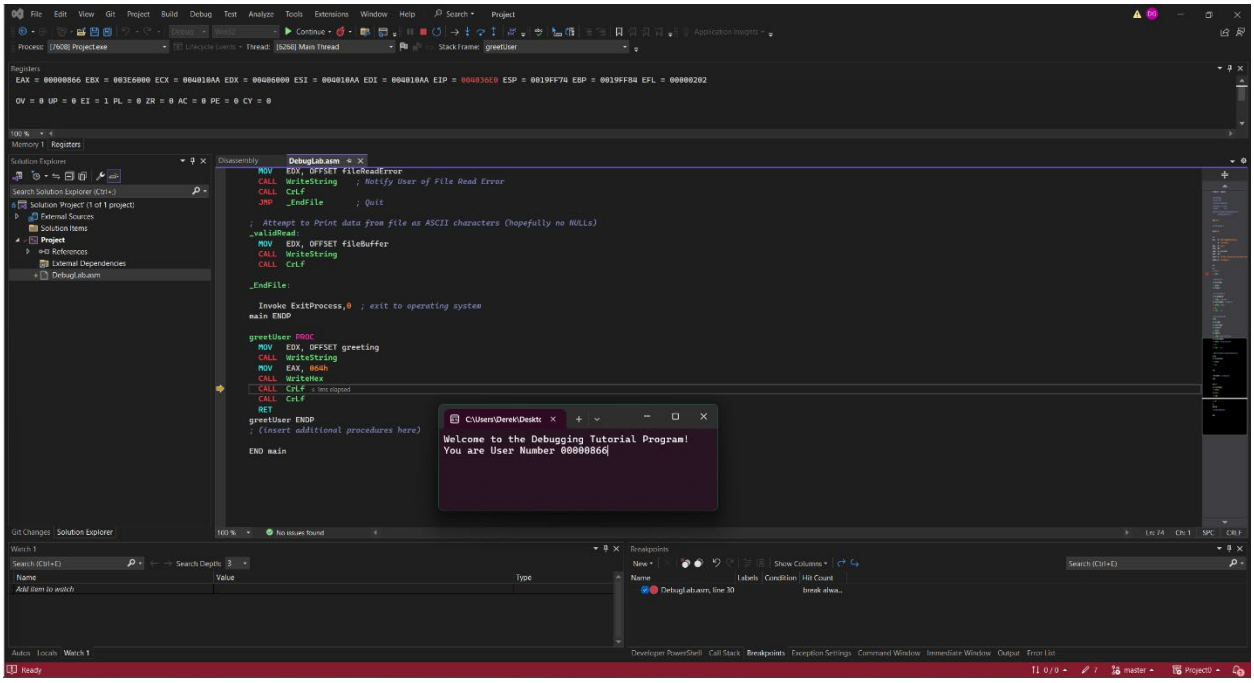

Figure 4: Part 2 - Question # 1

Derek Greene
934603866
4/23/2024

Part 3 – Disassembly View

Part 3 – Questions

1. MOV EAX, fileHandle

2. 0040368Ah

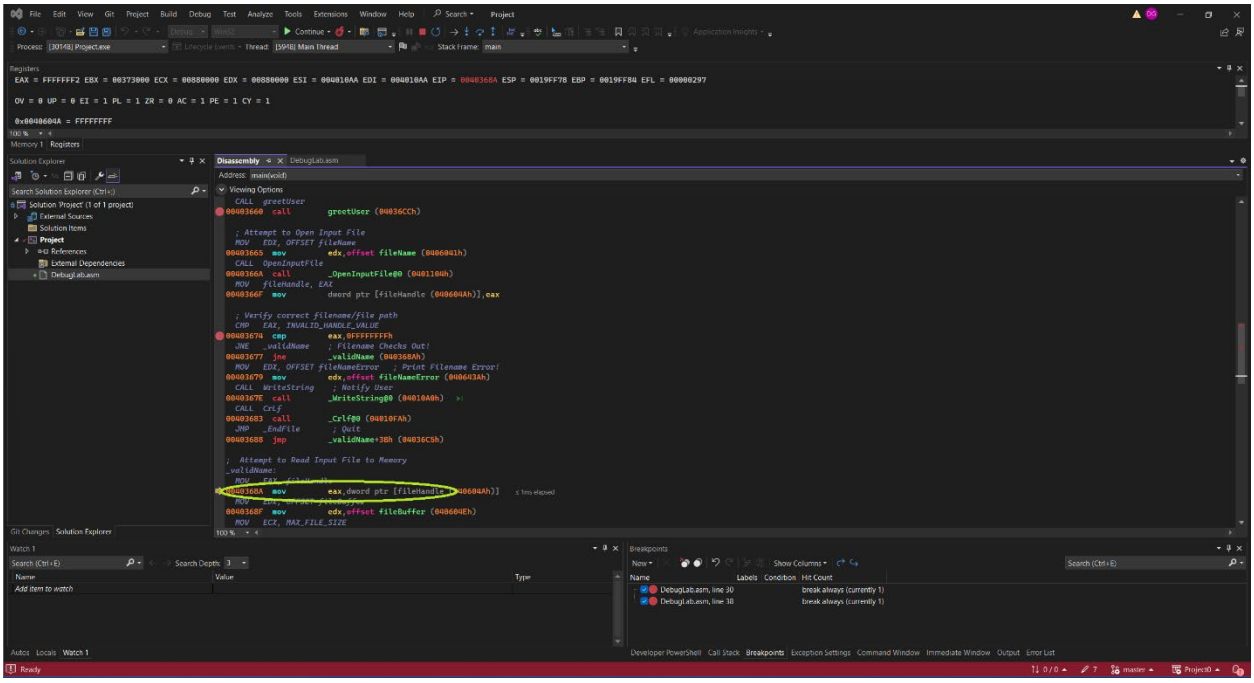

Figure 5: Part 3 - Question # 2

3. The value in the EIP register corresponds to the memory address of the current instruction and will match the leftmost value of any given line as you step through the code in the debugger.

Part 4 – Spelunking through Memory

Part 4 Questions

1. The 867th Byte (index 866) is interpreted as ASCII character: w

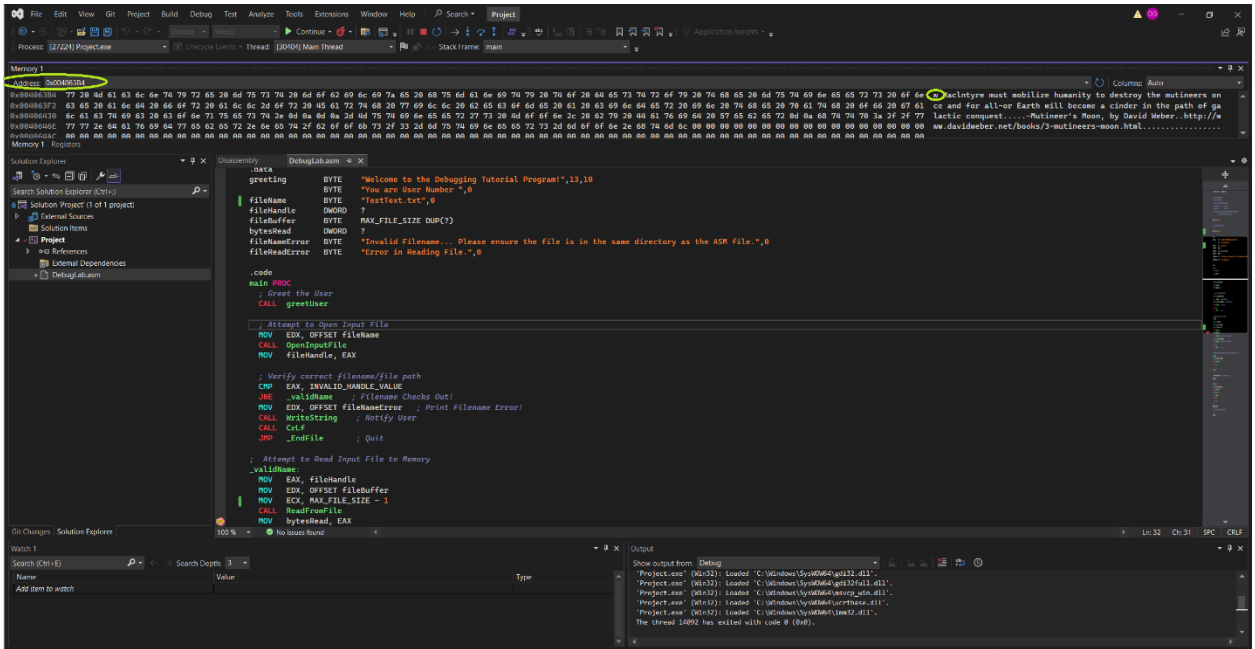

Figure 6: Part 4 - Question # 2

Derek Greene
934603866
4/23/2024

Part 5 – Keeping Careful Watch

1. 0x0000011C

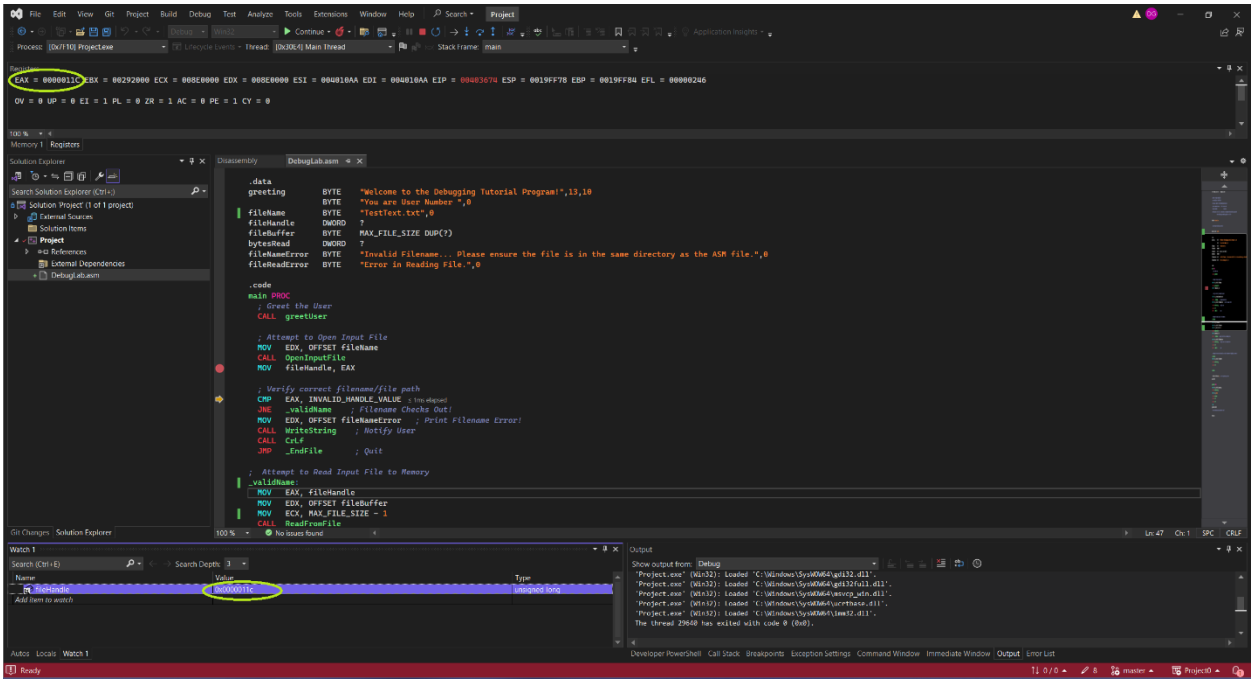

Figure 7: Part 5 - Question # 1