30 pts

Name: _____

Class Day / Time: _____

Due Date: _____

Lab #13 – WinDbg Introduction

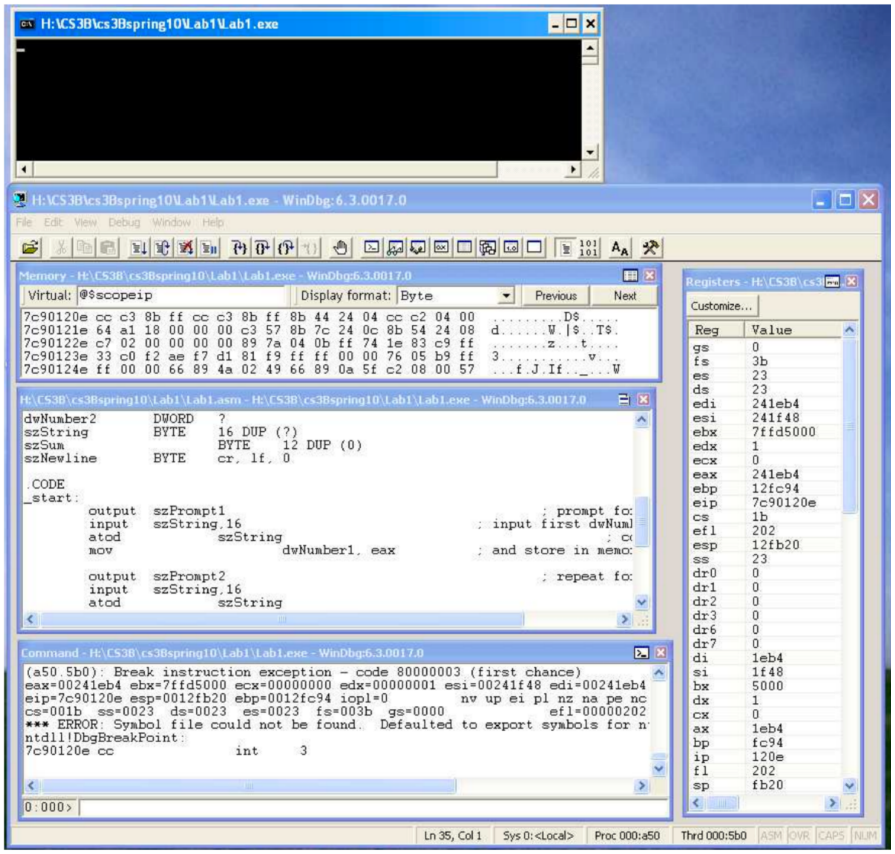
This lab is a tutorial for learning how to use the WinDbg to help us to debug our assembly programs. You will use the assembly program created for Lab #4 – Add Two Numbers. The program was called **LAB1**.

In the TextPad, check Configure > Preferences > Tools > Debug 32-bit Assembly and confirm that the **Parameters** for the WinDbg are:
-i $WspDir -y $WspDir -srcpath $WspDir $WspDir\$WspBaseName.exe
If not correct it and select OK.

Open the workspace for **LAB1** in TextPad and choose Debug 32-bit Assembly from the Tools > External Tools menu.

Resize the Output window and move it above the WinDbg window.
In WinDbg:

1) From the Window Menu, unselect the Auto-arrange option (if selected)
2) If Disassembly window is open, you should close it
3) From the File menu, choose Open Source File, Assembly Source Files and Lab1.asm
4) From the View menu open a Memory window and the Registers window.
5) Arrange the WinDbg window approximately as shown below, or in another equivalent format you may prefer



In the Command window entry bar (at the bottom of the Command window), type **bp start**. Press ENTER after each Command window command. Again, in the entry bar, type **g** to run the program to the breakpoint at the label start. "Output szPrompt1" is highlighted in the Source window.
What address is in the Instruction Pointer (the EIP register)? _____

The Command window should display "Breakpoint 0 hit", the current contents of the registers, and the next instruction to be executed. The Command window gives information about this instruction. The address of this instruction is the address in EIP.
What is this instruction? _____
What is the machine code of this instruction? _____

To execute "output szPrompt1" press the **F10** key (or press the Step-Over button, or type **p** in the Command window entry bar).
What is on the Output screen? _____

Press **F10**. The message "Debugger is running . . ." appears in the Command window entry bar and the Registers window is grayed out. The program will wait for you to enter a number. Click in the Output window and enter **125**.

Change "@$scopeip", at the top of the Memory window, to **szString** (we are asking for the address of the memory location allocated to the variable szString)
What is the address of szString? _____

What is stored in the first three bytes of szString? _____
What do these numbers represent? _____

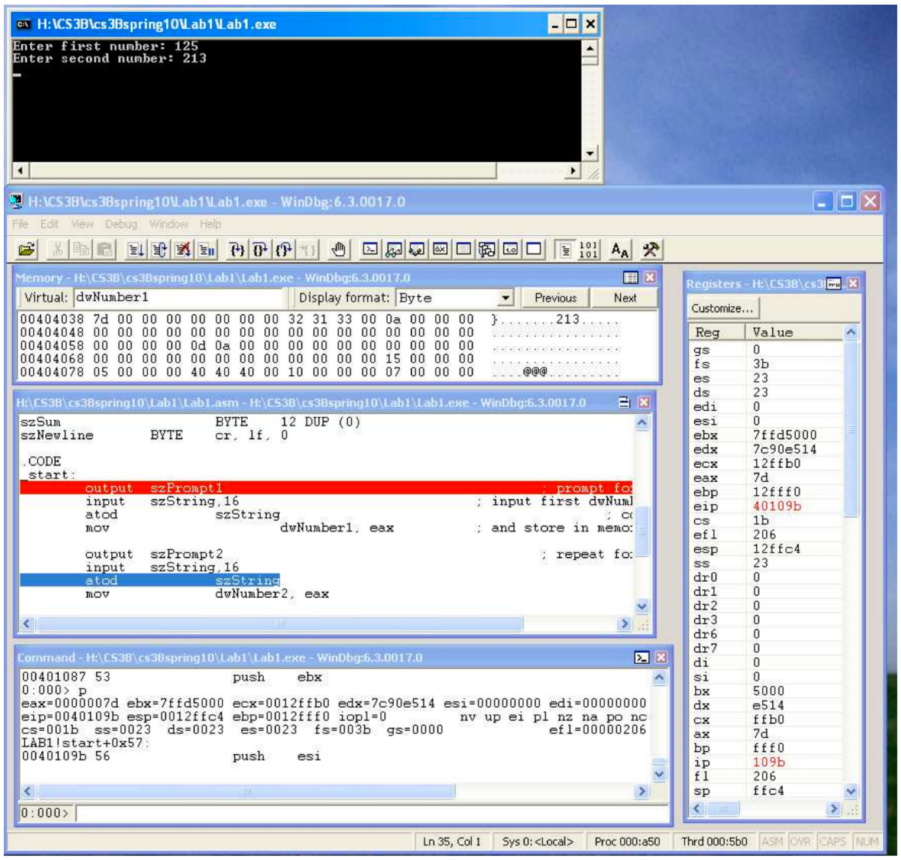
Press **F10** to execute "atod szString".

What is in the EAX register? _____

What instruction is highlighted in blue in the Source window? _____

Press **F10** to execute it. Look at the memory location for **dwNumber1** (type in the Memory window), which is defined as a dword.
How many bytes will it use? _____
What is stored in those bytes? _____
What is this number? _____

Press **F10** twice to output the second prompt and input the second number. Enter the number **213**. Your screen should now look something like the following.



Click back in the WinDbg window. Press **F10**.
What is in EAX? _____

What is the current value of EIP? _____

This is the address of the instruction "mov dwNumber2, eax". The Command window gives information about this instruction.
What is the machine code for "mov dwNumber2, eax"? _____

The first two hex digits of the machine code represent "move from the EAX register". The last eight digits are the address in memory for dwNumber2. Does this address match the address in parentheses after "mov [LAB1!dwNumber2" on the same line?
Why are they different?
_____

_____

Press **F10**. You should see the number from EAX in the Memory window immediately after the memory location for dwNumber1.
Why does dwNumber2 immediately follow dwNumber1 in memory? _____
_____

What is in EIP? _____

The value in EIP has been incremented by 5.
Why?
_____

Press **F10** twice.
What is in EAX? _____

Press **F10** to execute "dtoa szSum,eax".
What is stored in the 11-byte memory location for **szSum**?
_____

What is the address of szSum? _____

Press **F10** three times to output the heading, the result and a newline.
What is the relationship between the result of 338 and the number stored in EAX?
_____

What is the relationship between the bytes containing 33, 33, and 38 and the result 338?
_____

Press **F10** to complete execution of the program.

From the Debug menu, choose Restart.
In the Command window entry bar, type **bp start;** and **g** as before to start execution of the program again. Step through the program and enter –5 for the first number. Press **F10** twice.
What is stored in the memory location for dwNumber1?
_____

Why is dwNumber1 stored this way? _____

Turn in (STAPLED IN THIS ORDER)

1. The **ALL PAGES** of this assignment completed.