

## Week 3

1. Answer the following questions:

- A. Which is the syntax of an instruction?
- B. What is a label?
- C. Explain how the following instructions work (what they do, how many parameters, which restrictions):
  - a. MOV, LEA
  - b. INC, DEC
  - c. ADD, SUB, CMP, MUL, DIV
  - d. NOT, AND, OR, XOR, TEST
  - e. PUSH, POP
- D. How do we declare data? Which are the accepted data types?
- E. How do we declare constants?
- F. How do we declare segments?
- G. How do we declare procedures?
- H. What does ASSUME directive mean?
- I. What does END directive mean?

2. Open s3model.asm with Notepad. The file contains a program model in .EXE format.

Please read with care the comments.

3. Open s3ex1.asm with Notepad. Please follow:

- a. Data declarations
- b. Constant declarations
- c. Program structure
- d. Identify the directives, labels and instruction format

4. Compile s3ex1.asm with MASM Minimal and execute with Olly Debugger (Ollydbg):

- a. Each student will create his own folder and will copy here the archive found at <http://users.utcluj.ro/~madalin/teaching-SM.html> -> ASM tools. Unzip the archive.
- b. Open Notepad++ from "NPP/notepad++.exe". Open s3ex1.asm within.
- c. Compile s3ex1.asm using the menu "Plugins -> MASM Plugin -> Build MASM. For debugging, use "Plugins -> MASM Plugin -> Debug program (ollydbg)".

- OlllyDbg - s2ex1.exe - [CPU - main thread, module s2ex1.exe]
File View Debug Trace Options Windows Help

File View Debug Trace Options Windows Help

Open Hardware breakpoints window (Alt+H)

| Address               | Hex dump         | ASCII                        | Comment                                      |
|-----------------------|------------------|------------------------------|--|
| 001F1000              | BB 00000000      | MOV EAX,0                    |  |
| 001F1005              | A0 00301F00      | MOV AL,BYTE PTR DS:[1F3000]  |  |
| 001F100A              | B4 00            | MOV AH,0E                    |  |
| 001F100C              | BB 00000000      | MOV EAX,0                    |  |
| 001F1011              | 66:8B1D 04301F00 | MOV ECX,WORD PTR DS:[1F3004] |  |
| 001F1013              | 3B00 0C301F00    | MOV ECX,WORD PTR DS:[1F300C] |  |
| 001F101E              | BA 0A000000      | MOV EDI,0A                   |  |
| 001F1023              | 03CA             | ADD ECX,EDX                  |  |
| 001F1025              | 8A15 18301F00    | MOV DL,BYTE PTR DS:[1F3018]  |  |
| 001F1028              | 5A55 1D301F00    | MOV DH,BYTE PTR DS:[1F301D]  |  |
| 001F1031              | 6A 00            | PUSH 0                       |  |
| 001F1033              | ES 00000000      | CALL 001F1038                |  |
| 001F1038              | FF25 00001F00    | JMP 00000000 PTR DS:[1F2000] |  |
| 001F103E              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F1040              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F1042              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F1044              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F1046              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F1048              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F104A              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F104C              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F104E              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F1050              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F1052              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F1054              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F1056              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F1058              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F105A              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F105C              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F105E              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F1060              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F1062              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F1064              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F1066              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| 001F1068              | 0000             | ADD BYTE PTR DS:[EAX],AL     |  |
| Imm=0<br>EAX=30CA8794 |                  |                              |  |
| Address               | Hex dump         | ASCII                        | Comment                                      |
| 00A4FF84              | 77787C04         | RETURN to KERNEL32.77787C04  |  |
| 00A4FF88              | 7EFD0000         | ...                          |  |
| 00A4FF90              | 77787B00         | ...                          |  |
| 00A4FF94              | 30CA8794         | ...                          |  |
| 00A4FF98              | 00A4FFDC         | ...                          |  |
| 00A4FF9C              | 77DCAB5F         | ...                          | RETURN to ntddi.77DCAB5F                     |
| 00A4FFA0              | 7EFD0000         | ...                          |  |
| 00A4FFA4              | 30A0DFFA         | ...                          |  |
| 00A4FFA8              | 00000000         | ...                          |  |
| 00A4FFAC              | 00000000         | ...                          |  |
| 00A4FFB0              | 7EFD0000         | ...                          |  |
| 00A4FFB4              | FFFFF803         | ...                          |  |
| 00A4FFB8              | 19583000         | ...                          |  |
| 00A4FFBC              | 00007FDD         | ...                          |  |
| 00A4FFC0              | A5EC8A2B         | ...                          |  |
| 00A4FFC4              | 30A0DFFA         | ...                          |  |
| 00A4FFC8              | 00000000         | ...                          |  |
| 00A4FFD0              | 00A4FFE4         | ...                          | Pointer to next SEH record                   |
| 00A4FFD4              | 77E07300         | ...                          | SE handler                                   |
| 00A4FFD8              | 00000000         | ...                          |  |
| 00A4FFDC              | 00A4FFEC         | ...                          |  |
| 00A4FFE0              | 77DCAB5A         | ...                          | RETURN from ntddi.77DCAB50 to ntddi.77DCAB5A |
| 00A4FFE4              | FFFFFFFF         | ...                          | End of SEH chain                             |
| 00A4FFE8              | 77DAFFD2         | ...                          | SE handler                                   |
| 00A4FFEC              | 00000000         | ...                          |  |

Entry point of main module
Paused

- ## Hex Dump

[illegible]

- g. Execute each instruction and follow the changes in the registers, flags and stack.
5. Compile and execute s3ex2.asm. The program computes the sum of 6 values declared in the data segment.
  6. Write a program that computes the average value of 6 values declared in the data segment.