reverse engineering

**03 – structures and calling conventions**

# structures and calling conventiopns

**Lab Description:** The ability of a reverse engineer to identify the use of structures and calling conventions will greatly enhance their ability to analyze a program from disassembly. This lab will require the student to identify the use of structures, create custom structures in IDA Pro and identify calling conventions.

**Lab Environment:** IDA Pro Educational

**Lab Files that are Needed:** labFile.exe

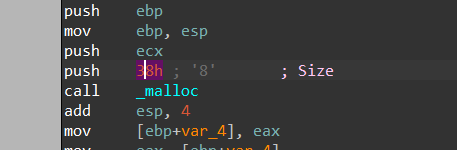
**Lab – Complete the following tasks**

1. Identify the use of the structure, what is the size of the structure?
2. Create a structure in IDA that represents the identified structure. Ensure that each member of your structure aligns with how it is used in the program.
3. Rename the members to something appropriate based off of your analysis.
4. In IDA View-A, add the structure offsets for each variable used.
5. There is a single regular function called in main, what calling convention does it use? What does it expect as an argument?

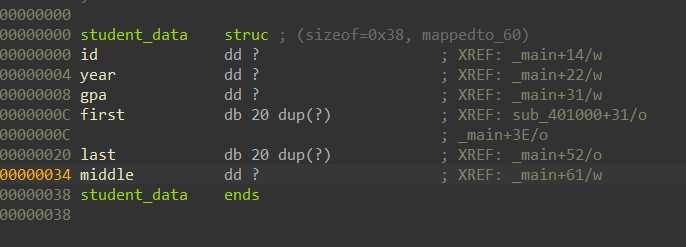
## What to submit

Submit a Microsoft Word document or PDF that includes answers to the questions posed.

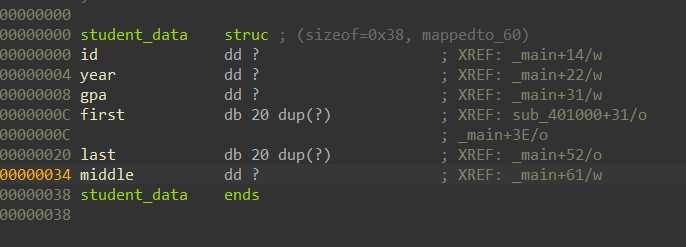
**1.** The size is 0x38.

****

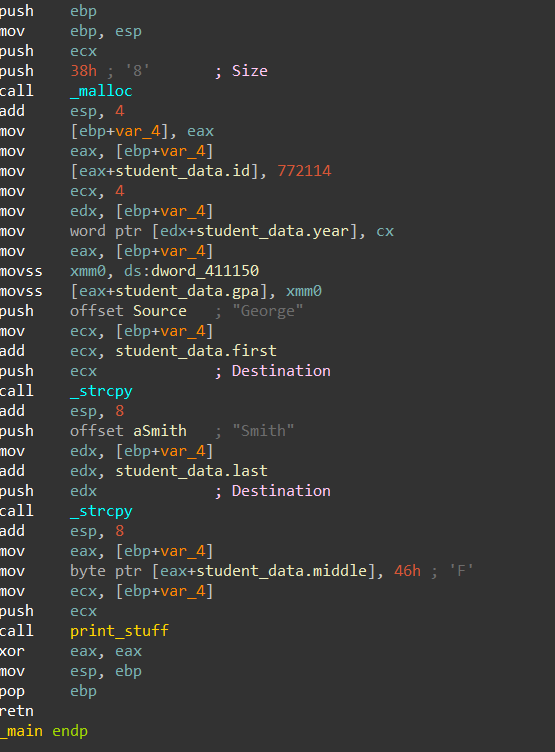
**2.**

****

**3.**

****

**4.**

****

**5.** The calling convention used is stdcall. It expects a pointer to the structure as an argument.