Malware Analysis
Fall 2015
Lab 04 - Debugging Concepts and Tools

**Lab_04-1.malware**
This sample uses an anti-analysis technique that we will discuss later on in the course. The anti-analysis technique makes static analysis harder. Using dynamic analysis is highly recommended!

1. (5%) Set a breakpoint at 0x00401092, what is this this sample calling?

2. (5%) What is being called at 0x004010A6? What is the callee doing?

3. (5%) What is sub_401360 doing? What about sub_401372 and sub_401388?

4. (15%) What Windows API functions did the sample import?

5. (10%) How did you find the Imported functions?

6. (10%) What does this sample do?

**Lab_04-2.malware**
1. (5%) What is the address of the win/lose function?

2. (15%) What does this sample do with the user input?

3. (10%) What is the address of the encrypted flag?

4. (20%) Flag? :-)