Lab 03 - Variables, Types & Functions

In this lab, we will be trying the reverse engineer a C program and label the local variables and functions.

**Required Materials**

You will need to be able to copy the binary onto a machine that has a working copy of IDA on it. The file is named **Lab03.exe**. You will also be using the file named Lab03.c. The binary was compilied using Visual Studio 2017.

**Learning Objectives**

This lab will get you familiar with adding comments, locating variables are renaming variables and functions.

Perform the following tasks:

1. Locate *main.* Once you have located *main,* rename it.

PNGs attatched

1. Rename all of the local variables used in this program - this not only includes main, but any functions called from main. Use the *exact* same name for variables that were used in the original C program.

PNGs attatched

1. Rename all of the functions called from main. Use the *exact* same name for variables that were used in the original C program.

PNGs attatched

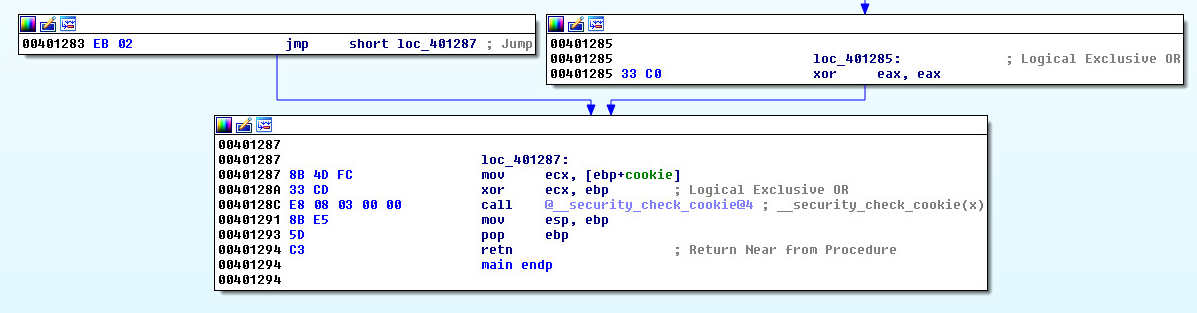
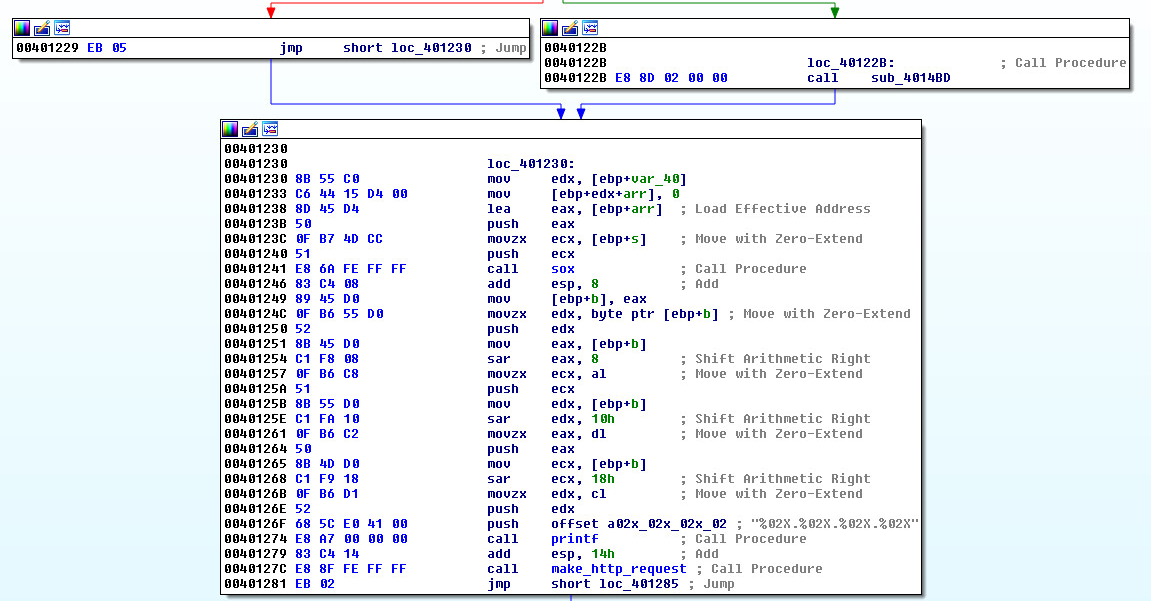
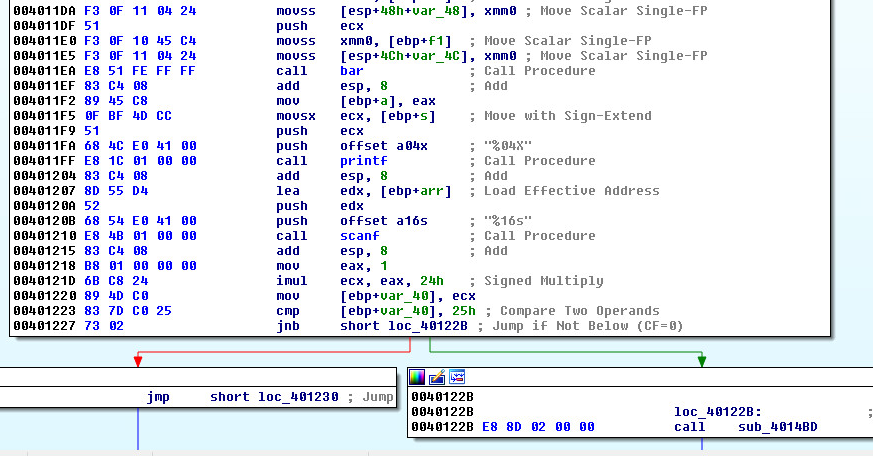
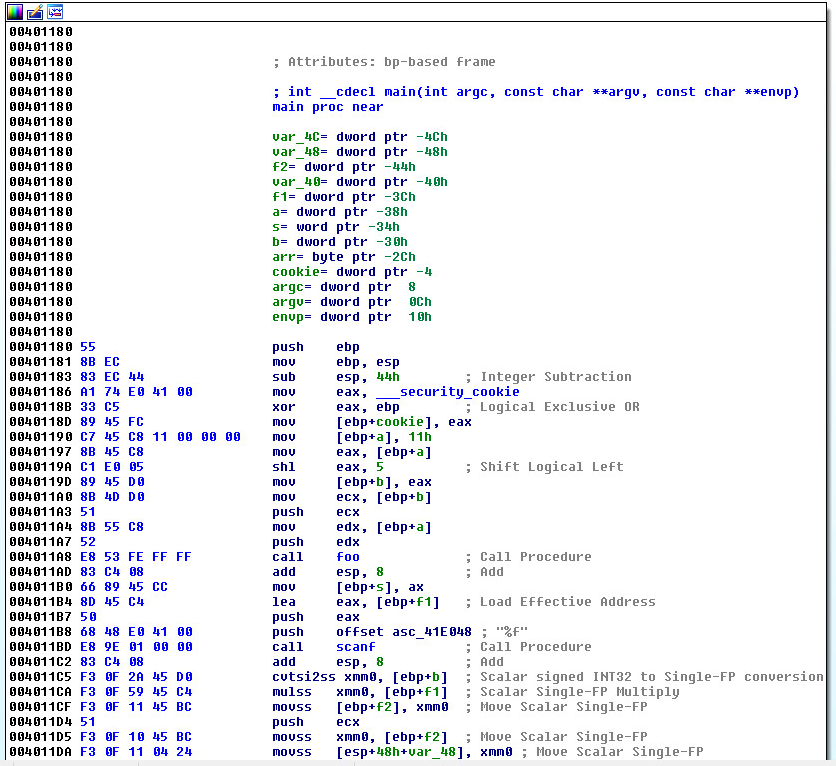
1. Had I not given you the source code but told you that this program makes HTTP request, how could you have identified where this code was used? That is, what function is responsible for making HTTP requests? Not all programs will be this simple so inspecting the functions called from main won’t always yield results - think of other ways you could have identified this functionality.

I forget the name of the tool off the top of my head, but one of those we went through in class that lists imported libraries/functions and highlights potentially suspicious bits might bring it up… otherwise, I noticed that a lot of the variables defined in the windows libraries were filled in by ida (i.e. hInternet and internetOpenA) -> just clicking through the first few handles on the function pane would quickly reveal which function is making those http requests.

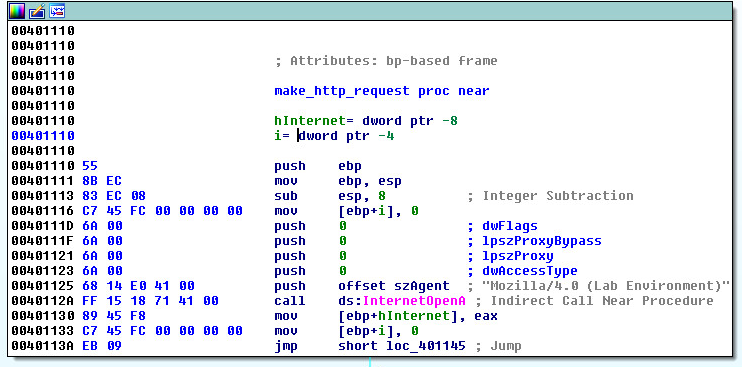
Deliverables

* Turn in a Word document or PDF that includes screenshots of your IDA database and all renaming, along with your answer to the final question.

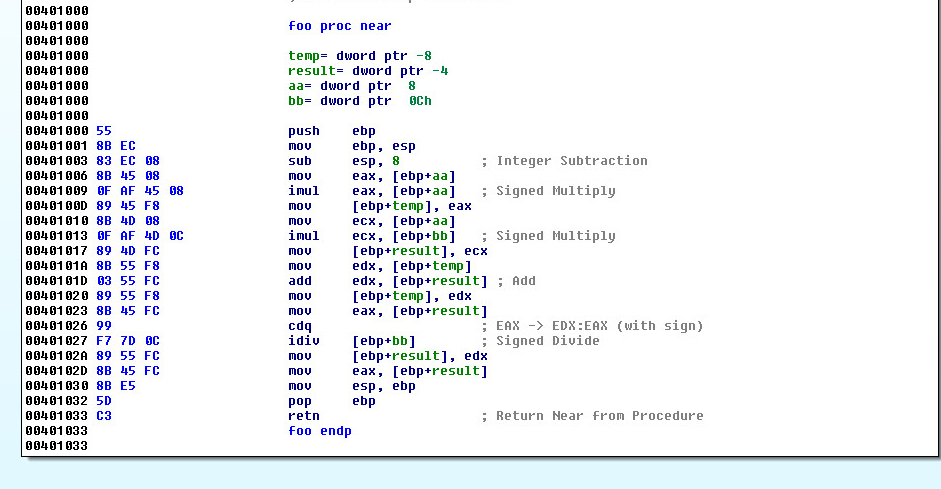
**Main:**



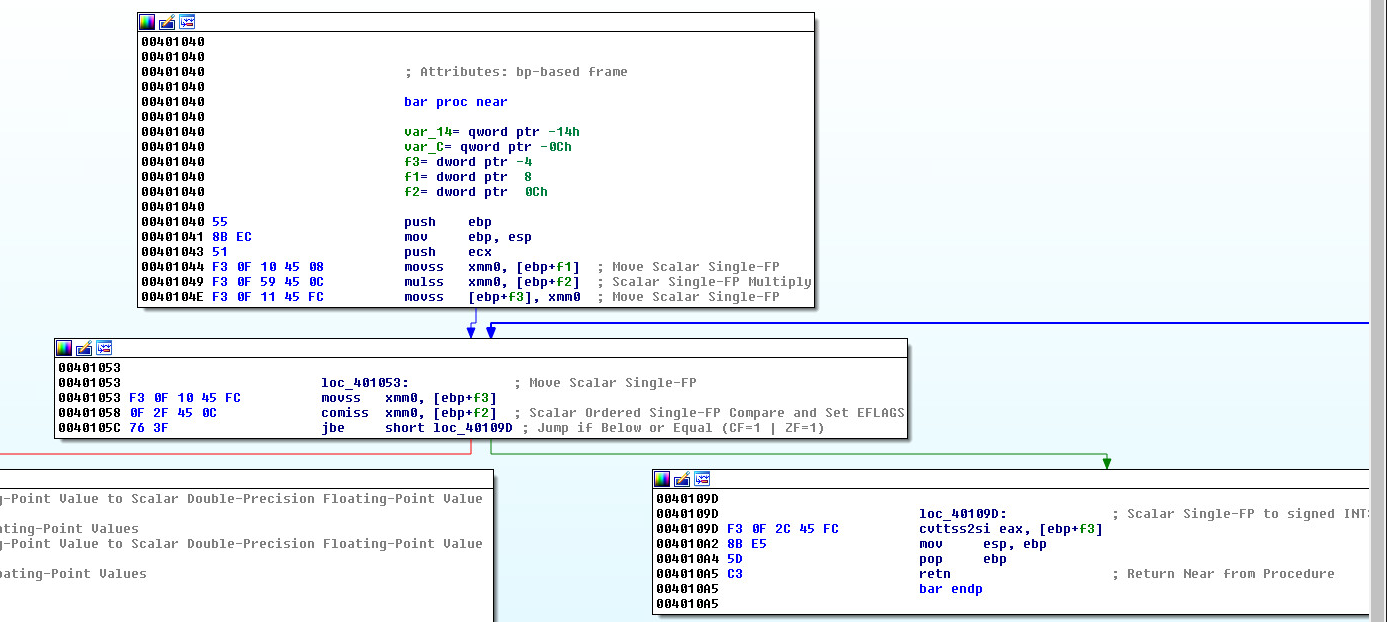
**Make\_http\_request:**



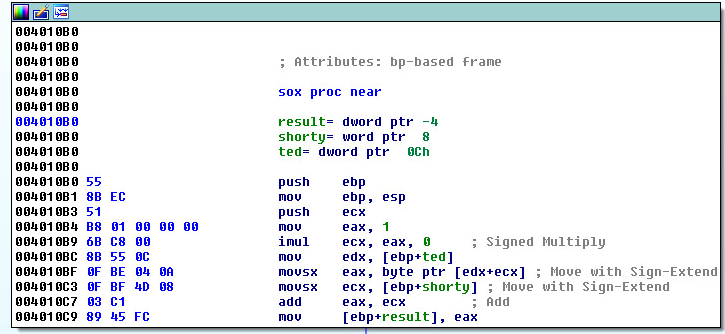
**Foo:**

****

**Bar:**

****

**Sox:**

****