CSIT-444 Reverse Engineering
PE Parser
Project Part 1: 25 points

Use the following resources to parse a PE formatted Windows executable. You will print out **all** the info in the DOS_HEADER. You will then follow the e_lfanew pointer to the IMAGE_NT_HEADER.

You need to print the following information.

Entry point for the code (calculated)
Timestamp exe was created
Enumerate each section listed in the Section Table. Print the following(indented please).

Section Name
Section Size
Virtual Address (calculated)
Virtual Size
Raw Data offset

What to turn in

A screen shot showing output. Run your program on…your own program for this (if in C).
Your executable
Your source

References

1. http://msdn.microsoft.com/en-us/magazine/ms809762.aspx
2. http://msdn.microsoft.com/en-us/magazine/bb985992.aspx
3. Image_File_Header
   http://msdn.microsoft.com/en-us/library/windows/desktop/ms680313(v=vs.85).aspx
4. Image_Optional_Header
   http://msdn.microsoft.com/en-us/library/windows/desktop/ms680339(v=vs.85).aspx
5. Image_Data_Directory
   http://msdn.microsoft.com/en-us/library/windows/desktop/ms680305(v=vs.85).aspx
6. _IMAGE_NT_HEADERS
   http://msdn.microsoft.com/en-us/library/windows/desktop/ms680336(v=vs.85).aspx
7. DOS_HEADER

http://en.wikibooks.org/wiki/X86_Disassembly/Windows_Executable_Files#MS-DOS_header

8. Image_Section_Header
   http://msdn.microsoft.com/en-us/library/windows/desktop/ms680341(v=vs.85).aspx