reverse Engineering

**02 - PE File Analysis**

# Analyzing a PE File

**Lab Description:** The goal of this lab is to provide a practical application to study the PE file format. In completing this lab you will demonstrate a working knowledge of the data contained within the PE file format and demonstrate the use of tools used for parsing this information.

**Lab Environment:** The following PE parsing utilities are recommended, these all require a Windows OS to run.

* PE Studio: https://www.winitor.com/
* Dependency Walker: http://www.dependencywalker.com/

**Lab Files that are Needed:** example.bin

### **Lab Exercise 1:**

In this lab, you will download and use PE studio/Dependency Walker to dive into the example PE file. PE Studio will point out any suspicious items, and generally give you a simple interface to view the contents of an executable or dynamically-linked library (DLL). Explore the application and use it to answer the following questions:

1. What is the image base? Does this deviate from the standard image base value used by most compilers?
2. What is the value for the **Size of code**?
3. Where is the base of code? What section is this in?
4. What are the names of the sections in this file? Do any of them deviate from standard names?
5. Based on the imported functionality, what do you suspect this program does? What other information can you use to determine program functionality?

## What to submit

Submissions should be neatly organized. Each question should include at least one screenshot and a brief explanation if possible.