# Windows Portable Executable (PE) File

## Objectives

In today's hands-on labs, you will perform the following:
Part #1 – Analyze Windows PE File using CFF Explorer or PE-bear

## Overview

This is our first lab of our series of the Offensive Security & Reverse Engineering course. We will start by analyzing a Windows Portable Executable (PE) file using very common and well known tools. Then you will be required to finish the last lab that guides you how to write your own PE analyzer using your Python skills.

**Requirements:**

1. For this lab, please use the Windows 10 VM.
2. All tools can be found under C:\users\user1\Documents\Tools (VHD drive). All you need to do is **mount** the drive.
3. Use the same putty.exe that we used for lab 0.
4. CFF Explorer could be downloaded from here and PE-bear from here. **Note:** you do not need to download them, but just in case you want them for offline usage.

## Part #1 – Analyze Windows PE File using CFF Explorer or PE-bear

In this part of the lab, we will go through some of the main and important features we learned during the PE File session.

Let’s get to work by starting **PE-bear** or **CFF Explorer** and then select the putty.exe file. Now you are required to walk through the file and answer the questions required below:

Deliverable #1: What is the signature (magic no.) of the DOS header?

Deliverable #2: What is the signature (magic no.) of the PE header?

Deliverable #3: For what architecture was this file built for and which entry gave you the answer?

Deliverable #4: When was it compiled? (tricky question ☺ )

Deliverable #5: What is the base address of the code section?

Deliverable #6: How many sections does this file have?

Deliverable #7: What is each section used for?

Deliverable #8: Can you change a section’s flag? How?

Deliverable #9: How many libraries is this file importing?

Deliverable #10: Do you know what functions are being imported?

Deliverable #11: Did you find any export table? Why do you think, no table was found?

Deliverable #12: Finally, what is the address of the entry point, and to what section it points?

Deliverable #13: Please reflect on your learning from this lab and what was not clear to you so we can discuss it together.