CMPSC 443 Lab 10: Unpacking

# Lab Description

Note: you are supposed to use a Windows VM to finish all these labs

The ollydump plugin and PEid need to be installed to accomplish this lab.

Your goal for the labs in this chapter is simply to unpack the code for further analysis. For each lab, you should try to unpack the code so that other static analysis techniques can be used. While you may be able to find an automated unpacker that will work with some of these labs, automated unpackers won’t help you learn the skills you need when you encounter custom packers. Also, once you master unpacking, you may be able to manually unpack a file in less time than it takes to find, download, and use an automated unpacker.

## Task 1

Lab18-01.exe

## Task 2:

Lab18-02.exe

## Task 3:

Lab18-03.exe [in-class demo]: you need to repeat it in the lab, but do not have to include it in your report.

Lab18-04.exe: you should unpack this sample and write the steps in your report.

# Submission

|  |
| --- |
| * For each sample, please describe the unpacking process with a few sentences and screenshots in the lab report. * Please only submit the lab report. |