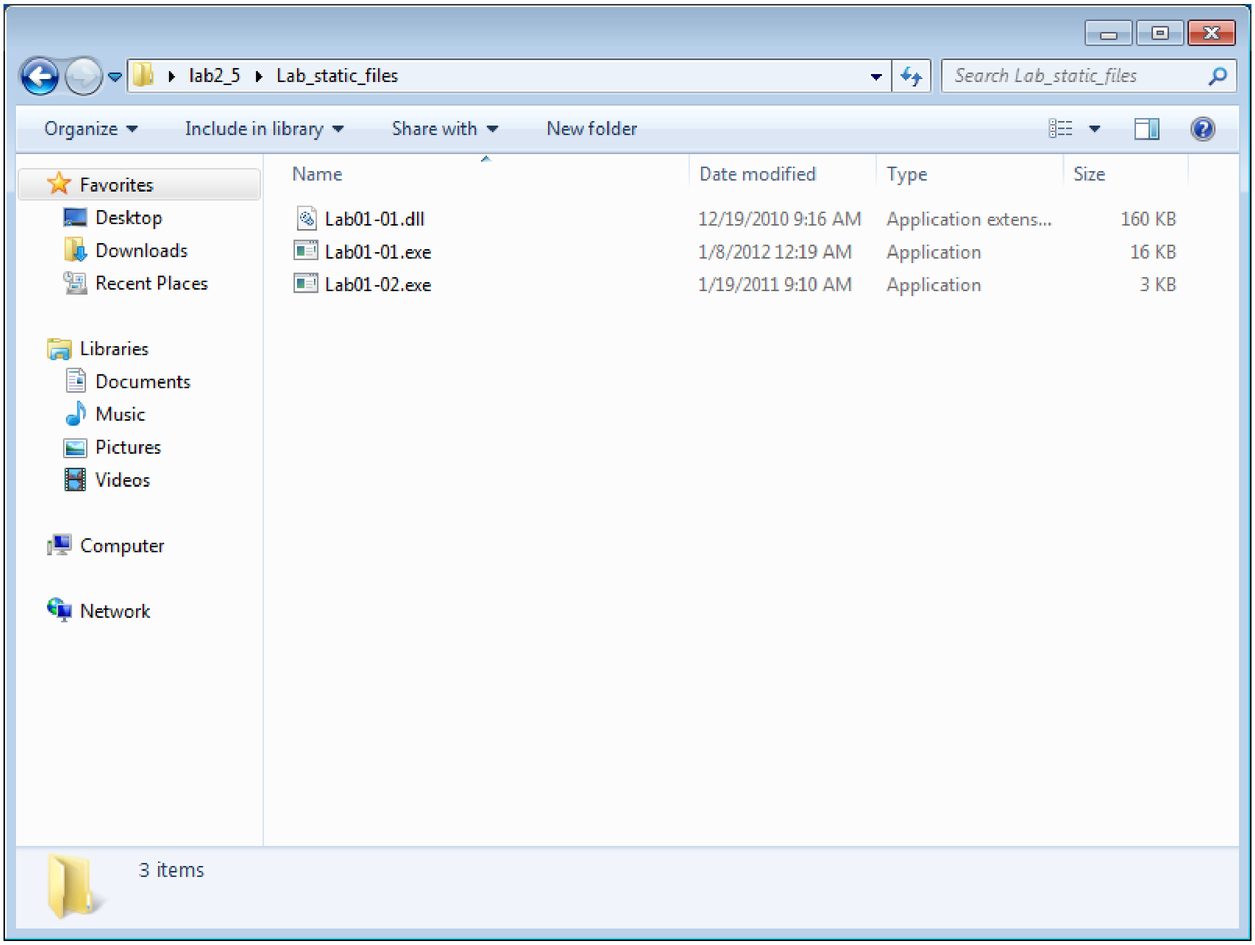
Overview

We are going to install several tools(PEView, PEiD, Dependency Walker) which are useful for analyze malware execution files in Win7 VM.

Part 1 - Download and install the tools

1. Download the 'Lab_static_files.7z' from Canvas. Please remember to make it a habit not to run any binary in your local environment even when practicing static analysis. Instead, move the files to your safe VM environment. The password is "infected".



Name	Date modified	Type	Size
Lab01-01.dll	12/19/2010 9:16 AM	Application extens...	160 KB
Lab01-01.exe	1/8/2012 12:19 AM	Application	16 KB
Lab01-02.exe	1/19/2011 9:10 AM	Application	3 KB

2. Download a PE viewer tool. You can choose whichever one you want and trust. The book uses PEview, which we find safe although VirusTotal may report it as suspicious (false positive?). Make sure you can run your selected PE Viewer on your Windows VM. The instructions in this lab will follow the book which uses PEview. Based on the slides and/or other resources, what does this tool do?

PEView, as the name suggests, provides a quick and easy way to view the structure and contents of Portable Executable (PE) and Component Object File Format (COFF) files. PE (Portable Executable) file refers to the executable file format used in Windows OS and is based on COFF (Common Object File Format) of UNIX. Among the extensions we often encounter in Windows, PE files are EXE, SCR, DLL, OCX, SYS, and OBJ. In summary, it is a program that looks into the structure of a file running on Windows.

3. Download PEiD (look for Download PEiD-0.95-20081103.zip. Make sure you can run it on your Windows VM.
Based on the slides and/or other resources, what does this tool do?

PEiD detects the most common packers, ciphers, and compilers for PE files. Before using this program, we need to know what a packed program is. Malware authors try to hide malicious malware programs. So they packed or obfuscated the program in order not to show the contents of the program. In short, the PEiD is used to determine which compiler or packer is being used.

4. Download Dependency Walker, and make sure you can run it in your Windows VM.
Based on the slides and/or other resources, what does this tool do?

Basically, it is a program that shows hierarchically all modules used in the relevant executable file. And you can see which functions are used in each module. For each module found, it lists all functions exported by that module and functions actually called by other modules. It can also detects many common application issues such as missing modules, invalid modules, import/export mismatches and etc.