**Sample Lab01-01.exe**

1. Yes, the file matches 22/55 existing antivirus signatures.
2. The file was compiled on “2010:12:19 17:16:19+01:00”.
3. Yes, examining the file with PEiD v0.95 reports that the executable was packed with Microsoft visual C++ 6.0.
4. The executable imports KERNEL32.dll and MSVCRT.dll.
   1. Some of the main imports are all in KERNEL32.dll “FindFirstFileA”, “CopyFileA”, and “CreateFileA”. This leads me to believe that this executable deals with file manipulation.
5. …
6. …
7. …

**Task 1 – Sample Lab01-02.exe**

1. Yes, the file matches 28/54 existing antivirus definitions.
2. No, there are no indicators that the file is packed or obfuscated according to PEiD v0.95.
3. The executable imports ADVAPI32.dll, KERNEL32.DLL, MSVCRT.dll, and WININET.dll. The following imports hint at this programs’ functionality:
   1. CreateServiceA in ADVAPI32.dll is used likely to create a process.
   2. InternetOpenA in WININET.dll is used likely to communicate via an internet socket.

**Task 2 – Sample Lab01-03.exe**

1. …

**Task 3 – Sample Lab 01-04.exe**

1. …