**Lab 2: Basic Static Techniques**

What you need:

* A Windows computer (real or virtual) with an Internet connection
* Recommended: the textbook: "Practical Malware Analysis"

**Purpose**

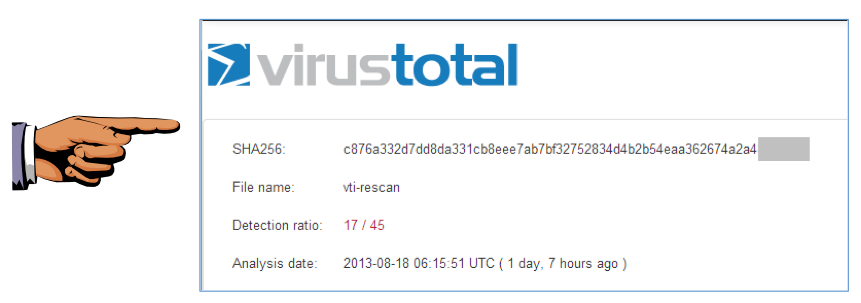
You will practice the techniques in chapter 1.

This project follows **Lab 1-2** in the textbook. There are more detailed solutions in the back of the book.

**VirusTotal**

Turn in an image showing your analysis of **Lab01-02.exe** as shown below.

We will grade it by checking the last digits of the SHA256 value.



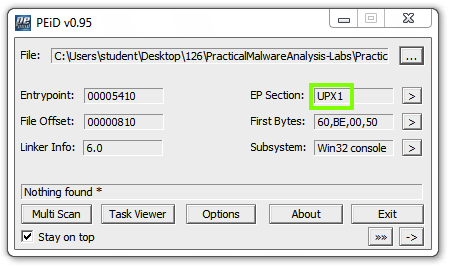
Press the **PrntScrn** key to capture an imag of the whole desktop.

Open Paint and paste the image in with **Ctrl+V**.

Save this image with the filename "**Proj 2a from YOUR NAME**".

**Unpacking the File**

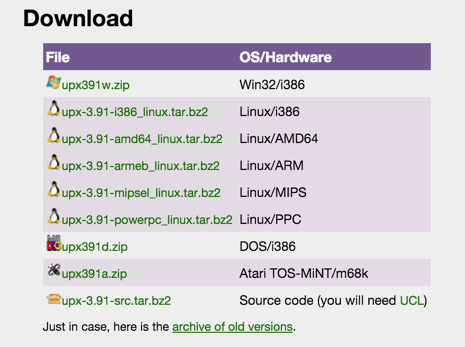
Run PEiD on the file. It shows that the file is packed with UPX, as shown in the "EP Section" below.



Download the UPX Zip file from here:

<http://upx.sourceforge.net/>

Download the **upx391w.zip** file, as shown below.

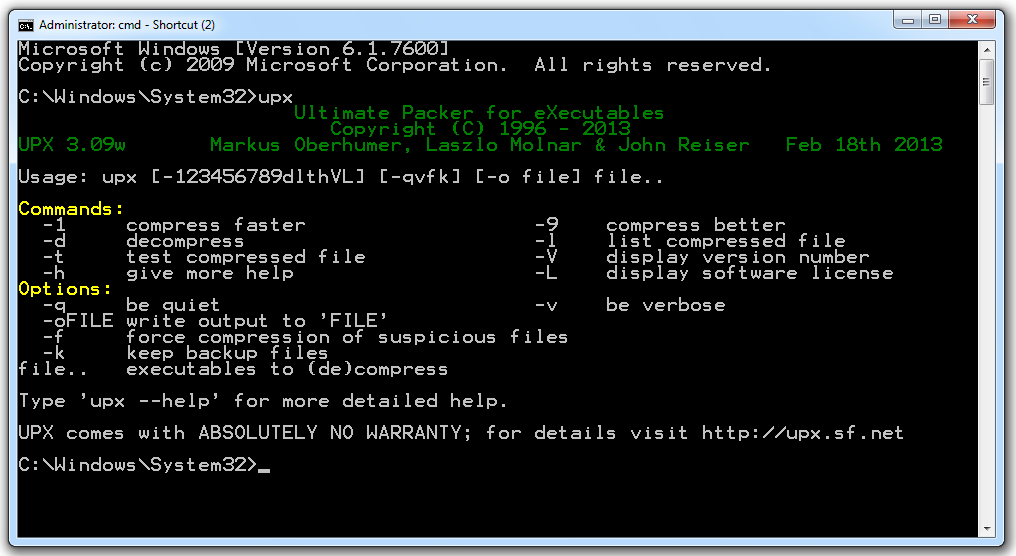


Unzip it and put upx.exe in your C:\Windows\System32 folder.

Open a Command Prompt window and execute this command:

**UPX**

You see a UPX help message, as shown below:



Use the CD command to move to the directory containing your malware samples.

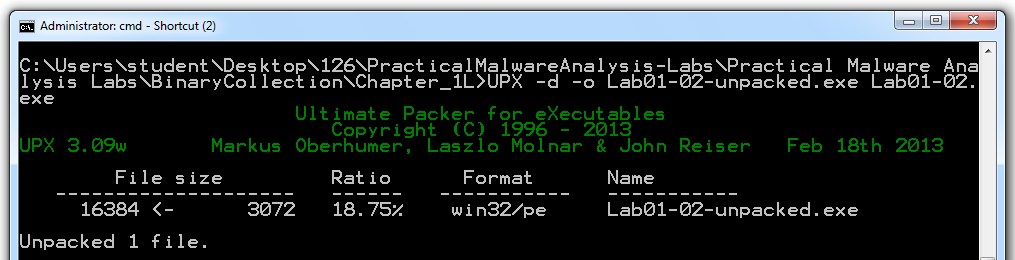
On my machine, I used this command:

**cd "\Users\Administrator\Desktop\126\Practical Malware Analysis Labs\BinaryCollection\Chapter\_1L"**

Execute this command to unpack the file:

**UPX -d -o Lab01-02-unpacked.exe Lab01-02.exe**

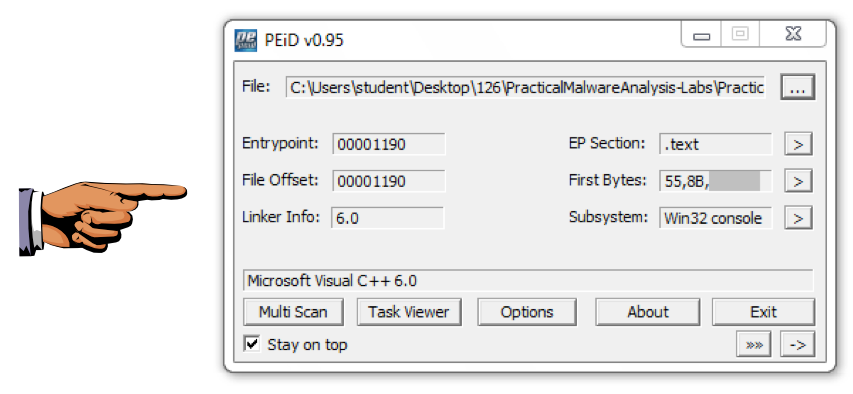
The file unpacks, as shown below:



Analyze the unpacked file with PEiD. It now is regognized as a "Microsoft Visual C++ 6.0" file, as shown below.

Turn in the image showing your analysis of **Lab01-02-unpacked.exe** as shown below.

We will grade it based on the "First Bytes".

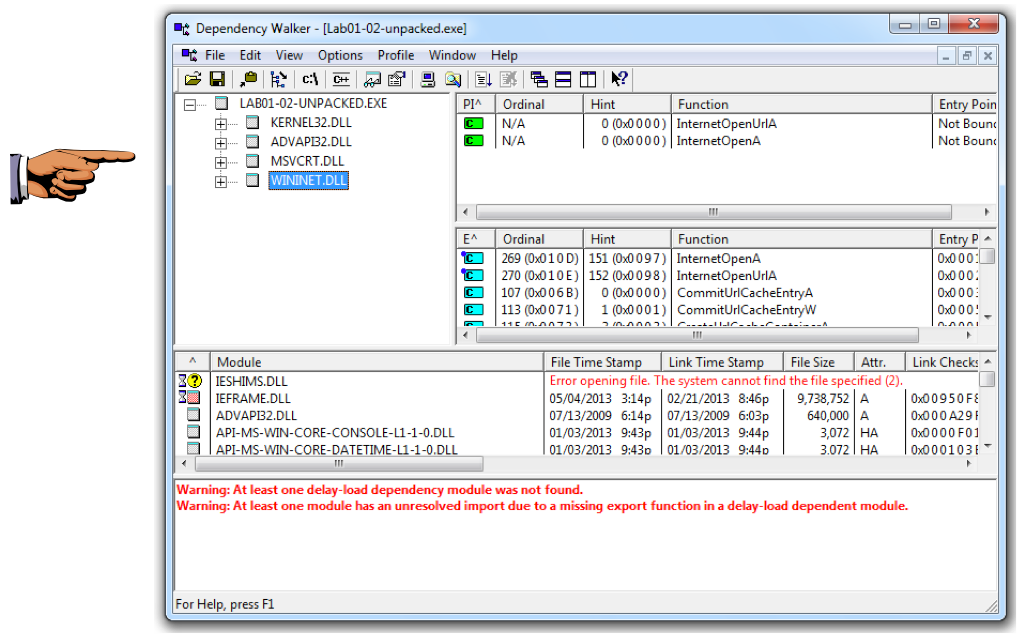


Save this image with the filename "**Proj 2b from YOUR NAME**".

**Imports**

Find the unpacked file's imports with Dependency Walker.

Turn in the image showing the two functions **InternetOpenUrlA** and **InternetOpenA** as shown in the upper right pane of the image below.



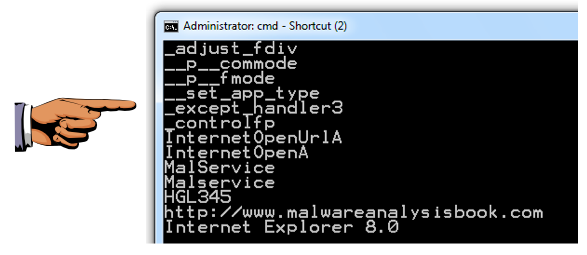
Save this image with the filename "**Proj 2c from YOUR NAME**".

**Strings**

Find the strings in the unpacked file.

You should see **MalService** and **http://www.malwareanalysisbook.com** as shown below.

These suggest that infected machines will connect to **http://www.malwareanalysisbook.com** and will show a running service named **MalService**.



Save this image with the filename "**Proj 2d from YOUR NAME**".