Proj 1: Basic Static Techniques (Lab 1-1) (25 pts.)

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.

Install 7-Zip

On your Windows machine, in a Web browser, go to http://www.7-zip.org/

Download and install the correct version of 7-zip.

Downloading the Lab Files

In a Web browser, go here:

http://sourceforge.net/projects/labs-encryptzip/

Click the green **Download** button to download the encrypted 7-zip archive.

Right-click the **PracticalMalwareAnalysis-Labs.7z** fie, point to **7-Zip**, and click "**Extract Here**". Use the password **malware**

The file extracts to tn EXE file. Double-click it to perform a second extraction process. Click the **Accept** button. Click the **Extract** button.

A folder named "Practical Malware Analysis Labs" appears. The files you need are in that folder, in a subfolder named "BinaryCollection".

This project uses the files **Lab01-01.exe** and **Lab01-01.dll**, both in the "Chapter_1L" folder.

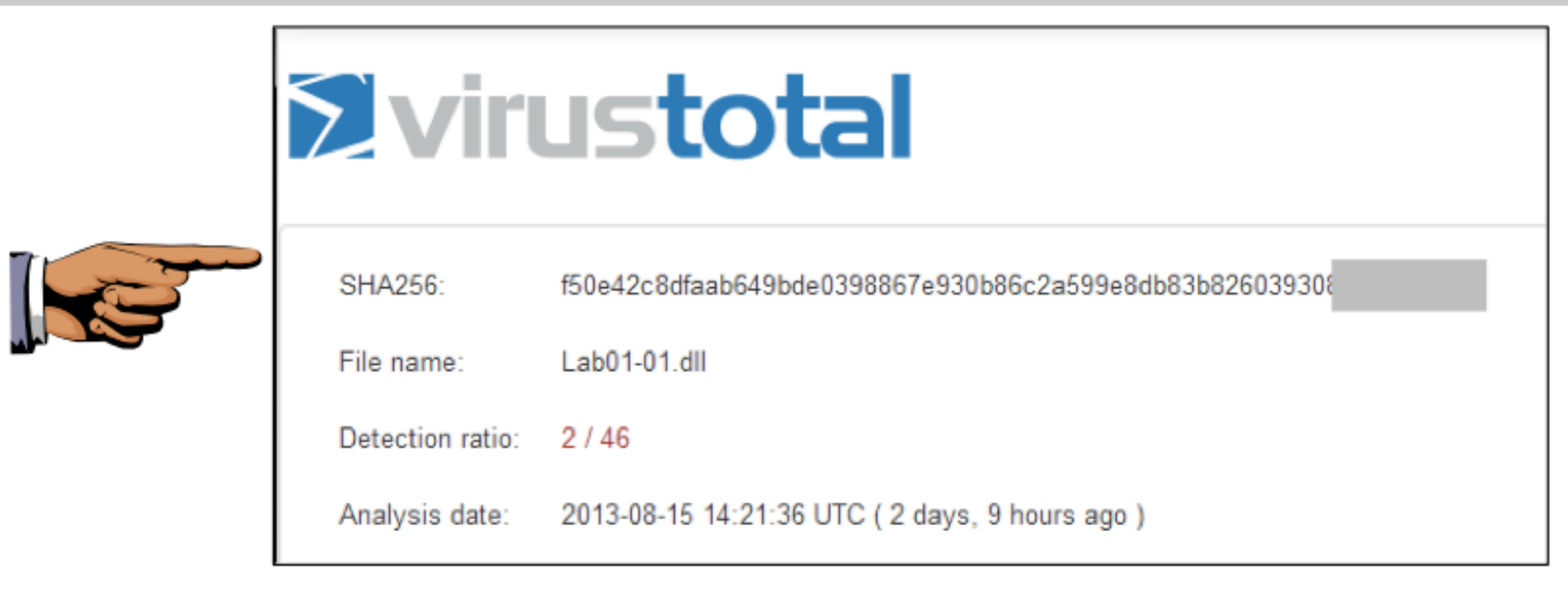
This project follows **Lab 1-1** in the textbook. There are more detailed solutions in the back of the book.

VirusTotal

Upload the **Lab01-01.exe** and **Lab01-01.dll** files to www.virustotal.com

Turn in the image showing your analysis of **Lab01-01.dll** 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 1a from YOUR NAME**".

YOU MUST SUBMIT WHOLE-DESKTOP IMAGES TO GET FULL CREDIT!

PEview

You can download PEview from here:

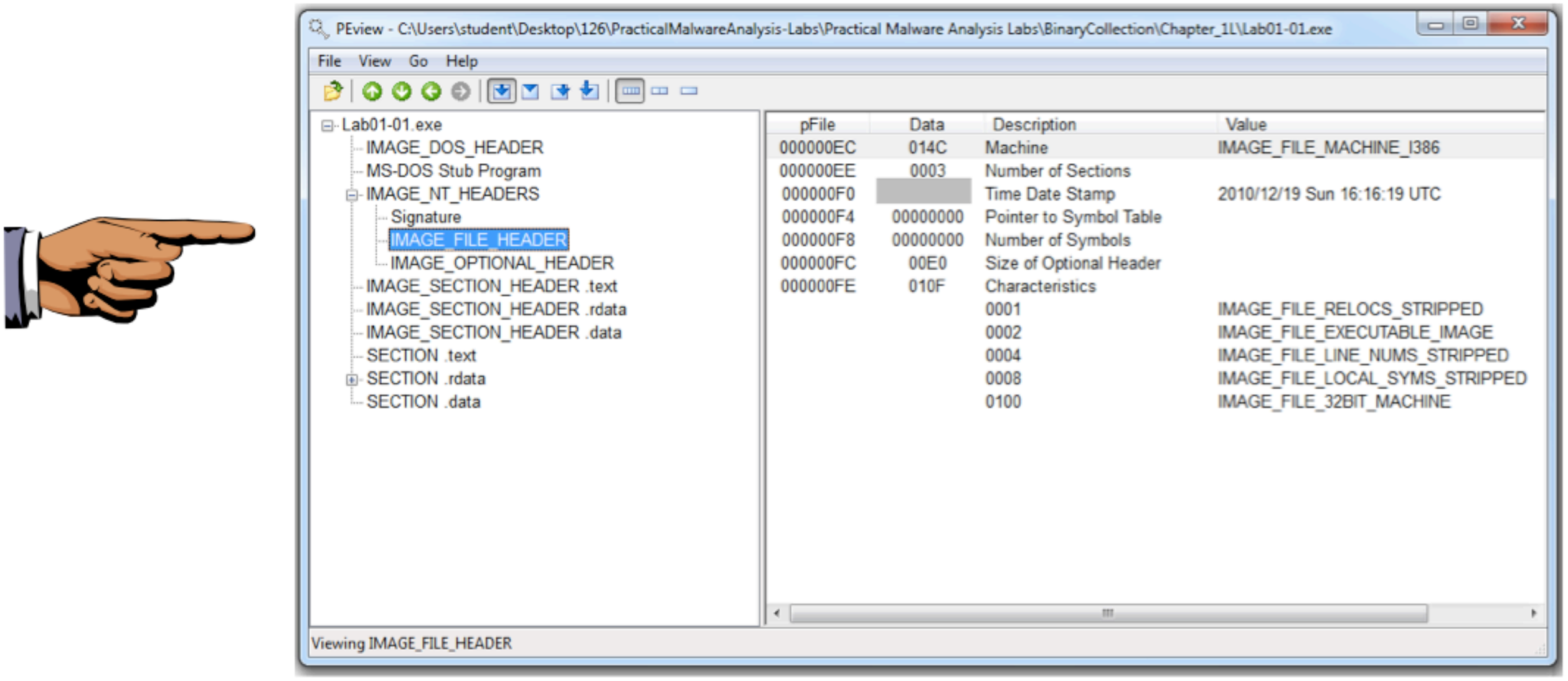
http://wjradburn.com/software/

Open the files in PEview. For each file, find the "Time Date Stamp" as shown below.

The files were both compiled on the same date within a minute of each other, indicating that they are part of the same package.

Turn in the image showing your analysis of **Lab01-01.exe** as shown below.

We will grade it based on the "Data" column of the "Time Date Stamp" field.



Save this image with the filename "**Proj 1b from YOUR NAME**".

YOU MUST SUBMIT WHOLE-DESKTOP IMAGES TO GET FULL CREDIT!

PEiD

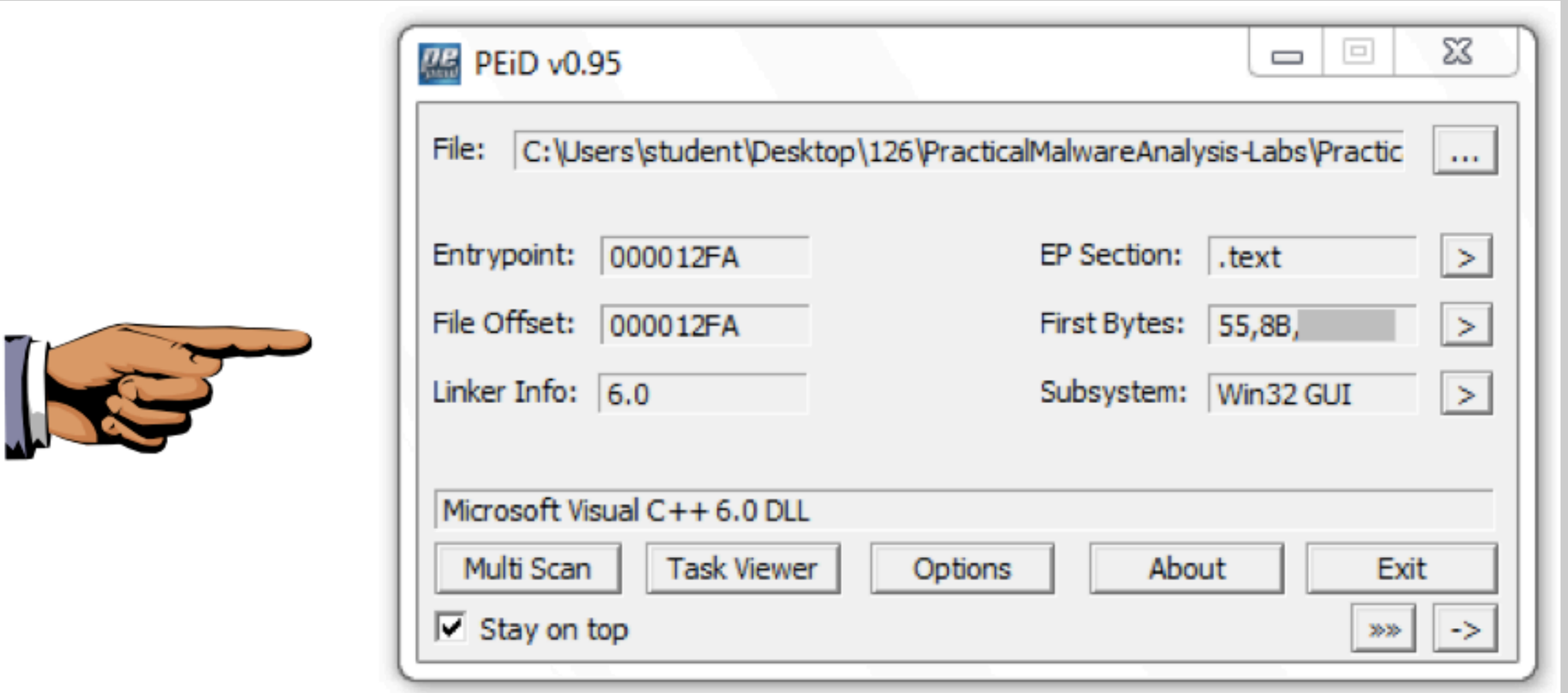
You can download PEiD here:

http://www.softpedia.com/progDownload/PEiD-updated-Download-4102.html

Open the files in PEiD. They are identified as "Microsoft Visual C++" files, which shows that they are unpacked.

Turn in the image showing your analysis of **Lab01-01.dll** as shown below.

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



Save this image with the filename "**Proj 1c from YOUR NAME**".

YOU MUST SUBMIT WHOLE-DESKTOP IMAGES TO GET FULL CREDIT!

Strings

You can download Strings for Windows go here:

http://technet.microsoft.com/en-us/sysinternals/bb897439

Click the "**Download Strings**" link.

Save the **Strings.zip** file on your desktop. Unzip it, and copy **strings.exe** to the **C:\Windows\System32** folder.

Open a Command Prompt and use the CD command to move to the directory containing your lab files.

Then collect the strings from the **Lab01-01.exe** file.

On my machine, I used these commands:

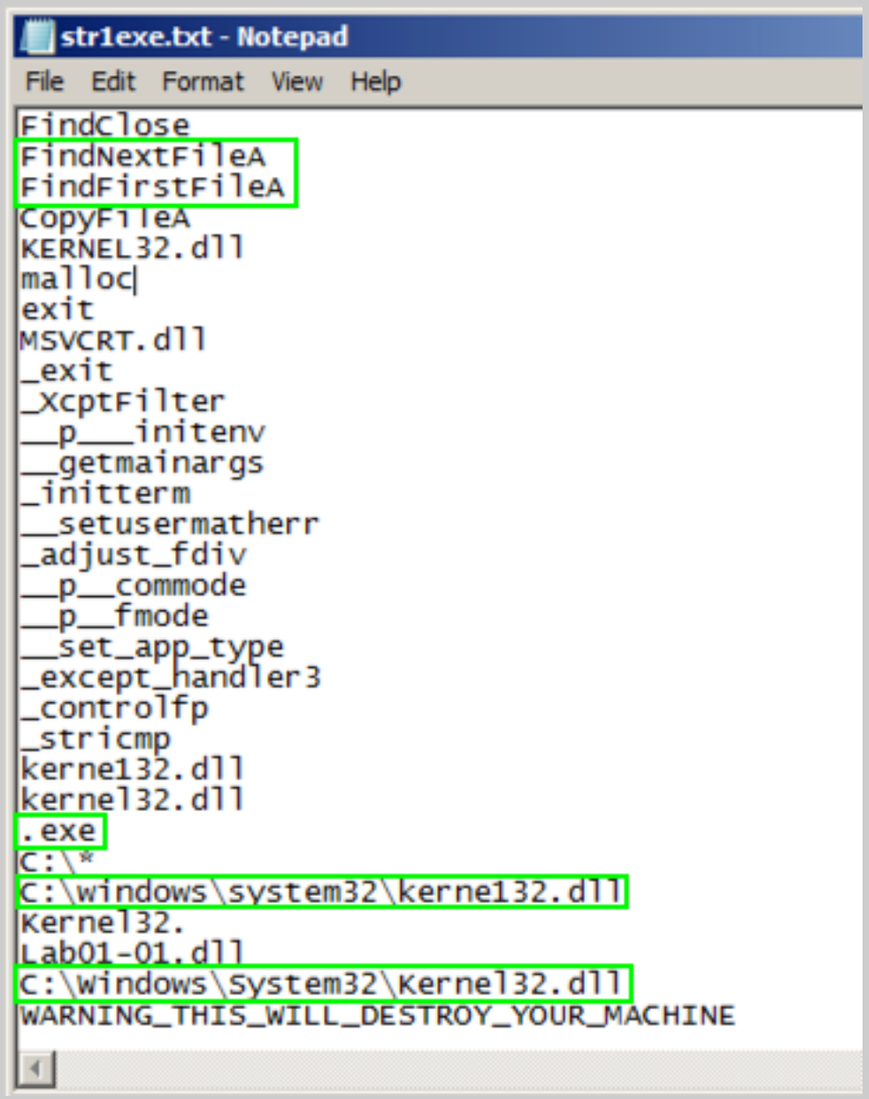
```
cd "\Users\Administrator\Desktop\126\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L"

strings Lab01-01.exe > str1exe.txt

notepad str1exe.txt
```

Notice these items, as shown below:

- "**FindNextFileA**" and "**FindFirstFileA**" -- Windows functions to find files
- "**.exe**" -- suggesting that it will search for EXE files
- "**C:\windows\system32\kerne132.dll**" -- fake DLL with "kerne132" instead of "kernel32"
- "**C:\Windows\System32\Kernel32.dll**" -- the real Windows kernel



Look at the strings for **Lab01-01.dll**.

Notice these items, as shown below:

- "exec" and "sleep" -- commands that can be sent over the network to control this backdoor malware
- ".CreateProcessA" -- used to launch a program in response to the "exec" command
- "Sleep" -- used to put the backdoor to sleep in response to the "sleep" command

Turn in the image showing your analysis of **Lab01-01.dll** as shown below.

Below "sleep" and "hello" there is an IP address, starting with 127.

We will grade it by checking the last digits of the IP address.

Save this image with the filename "**Proj 1d from YOUR NAME**".

Dependency Walker

You can download Dependency Walker here:

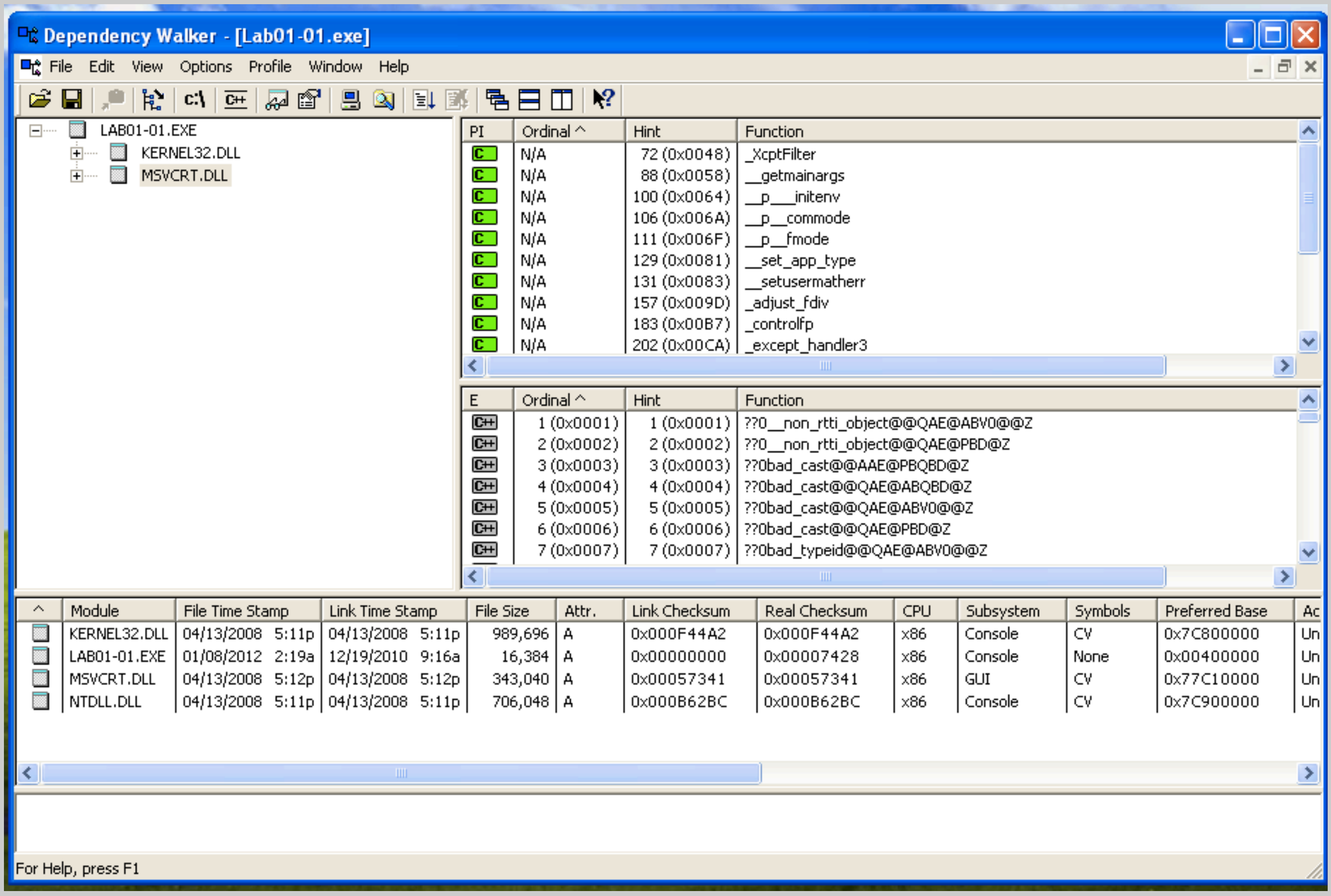
http://www.dependencywalker.com/

> ## Troubleshooting
>
> If that link fails, use this alternate download link:
>
> https://samsclass.info/126/proj/depends22_x86.zip

Open **Lab01-01.exe** in Dependency Walker.

In the left pane, click **MSVCRT.DLL** as shown below.

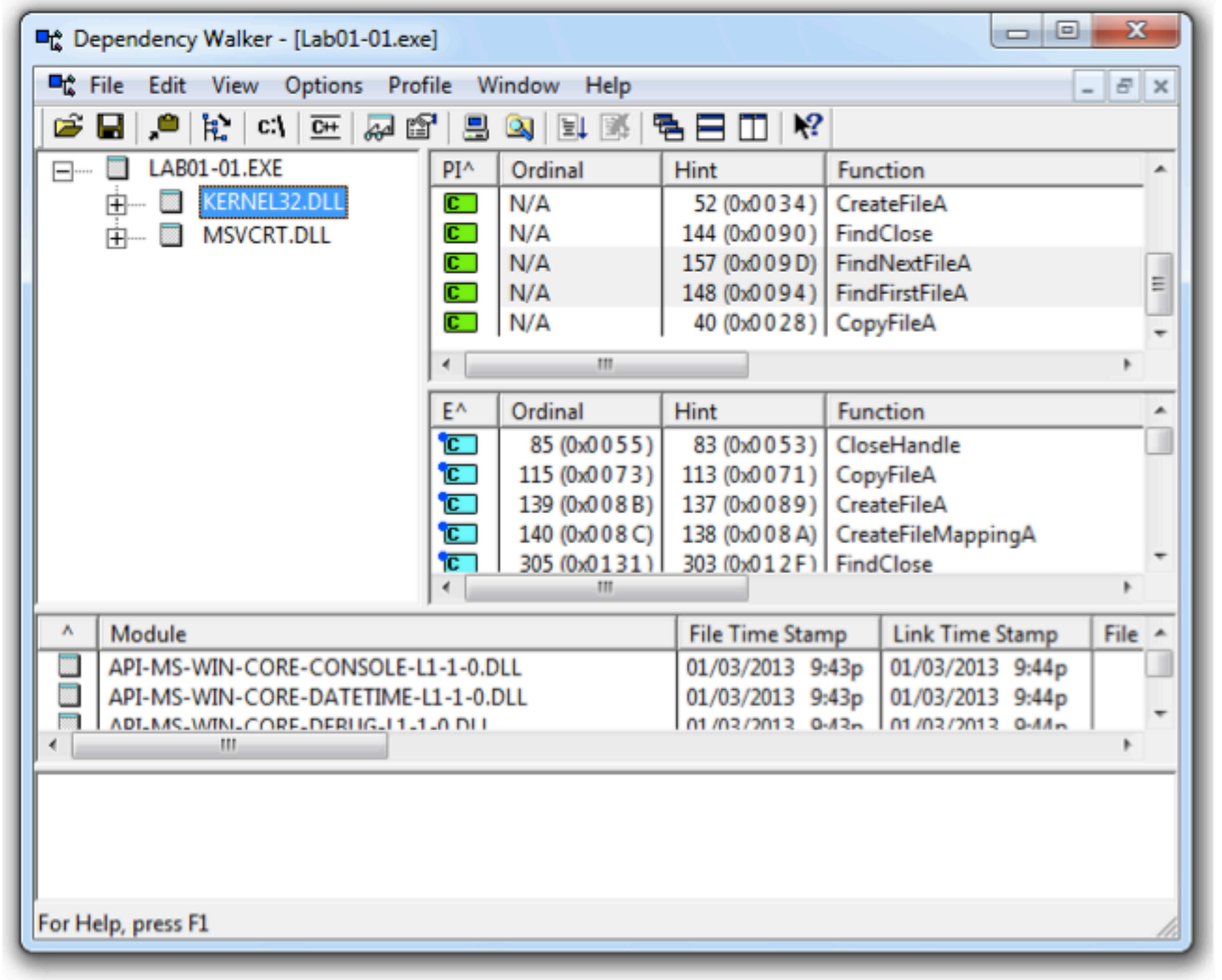
There are several imports in the upper right pane, and exports in the middle right pane. Scan through them--these are normal for any EXE.



In the left pane, click **KERNEL32.DLL**.

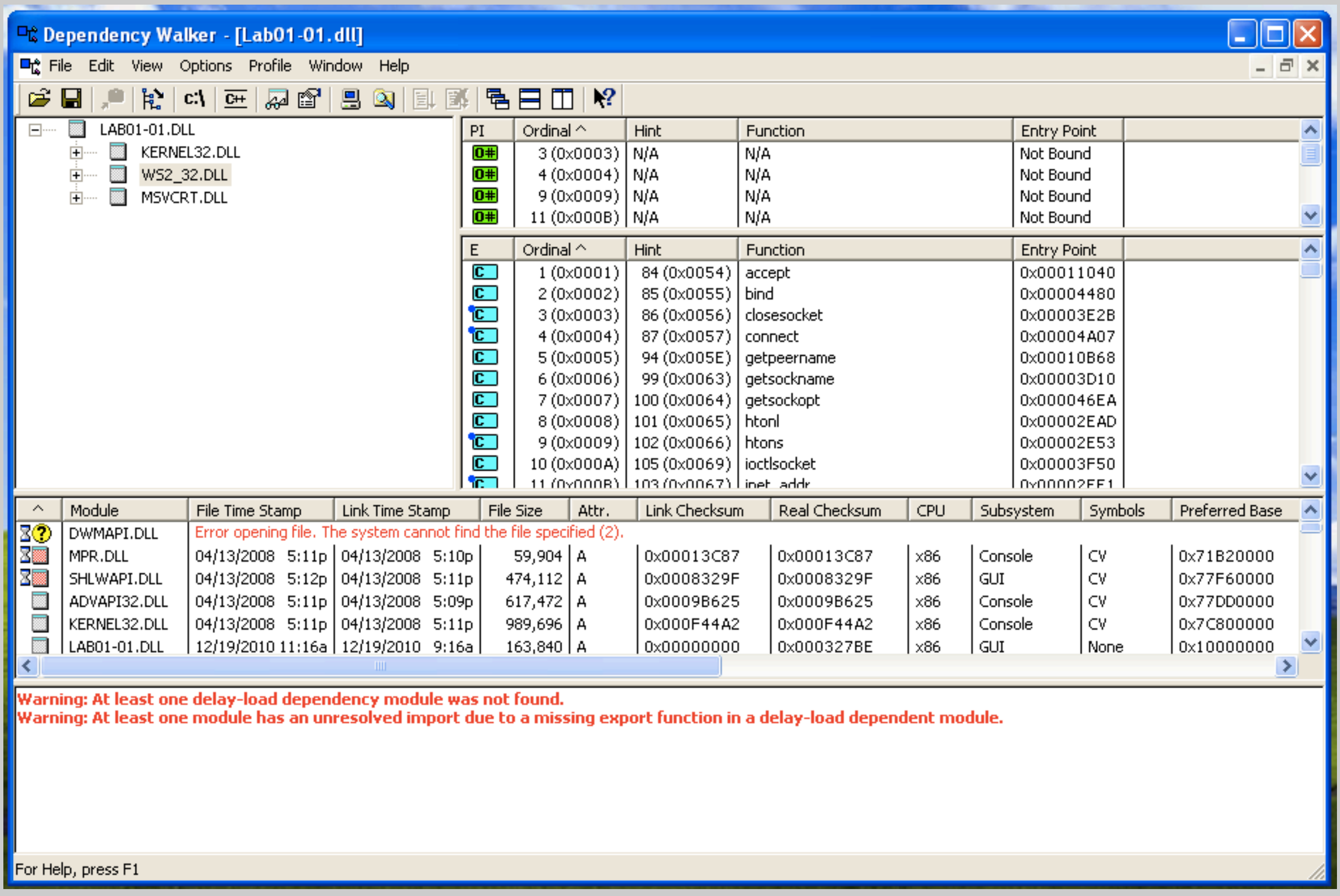
Turn in the image showing your analysis of **Lab01-01.exe** as shown below.

In the "PI^" section (Parent Import), you should see **FindNextFileA** and **FindFirstFileA** as shown below.



Save this image with the filename "**Proj 1e from YOUR NAME**". Open **Lab01-01.dll** in Dependency Walker. Notice that it imports functions from "WS2_32.DLL".

WS2_32.DLL has networking functions. The right center pane shows function names that perform networking tasks, such as "bind", "closesocket", and "connect", as shown below.



Turning in your Project

Email the images showing the secret messages to cnit.126sam@gmail.com with the subject line: **Proj 1 from YOUR NAME**

Last modified 7-20-14 12:05 pm