**Lab 1: Basic Static Techniques (Lab 1-1)**

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**

Get the lab files here:

<https://practicalmalwareanalysis.com/labs/>

Download the 7-Zip archive. Unzip it with the password **malware**

The file extracts to an 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.

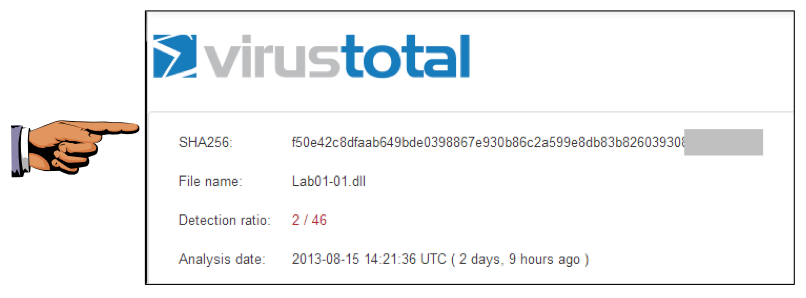
This project follows **Lab 1-1** in the textbook. There are more detailed solutions in the back of the book.

**VirusTotal**

Upload the **Lab01-01.exe** and **Lab01-01.dll** files to [www.virustotal.com](http://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**".

**PEview**

You can download PEview from here:

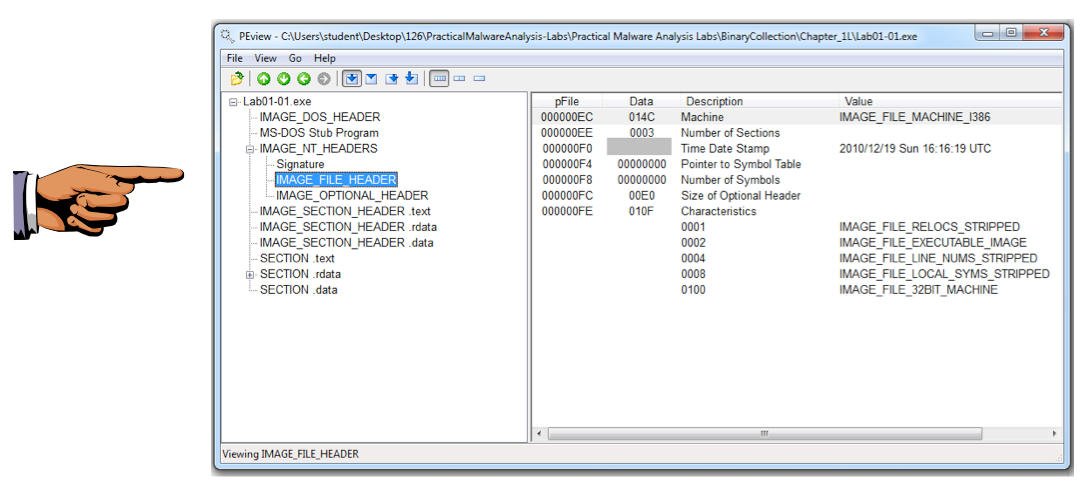
<http://wjradburn.com/software/>

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**".

**PEiD**

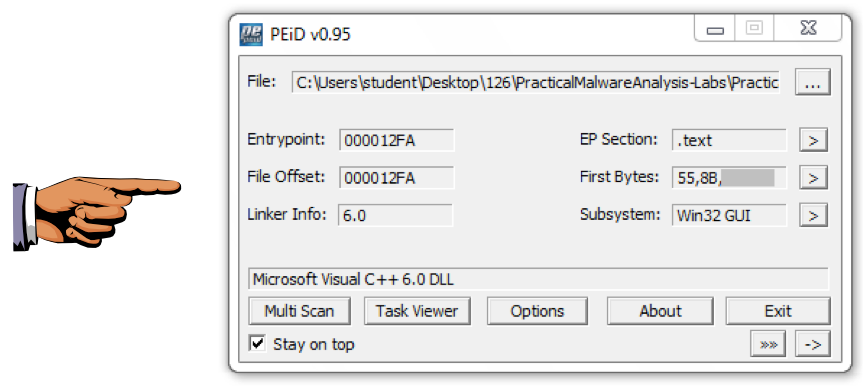
You can download PEiD here:

<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**".

**BinText**

BinText is a handy tool to view strings.

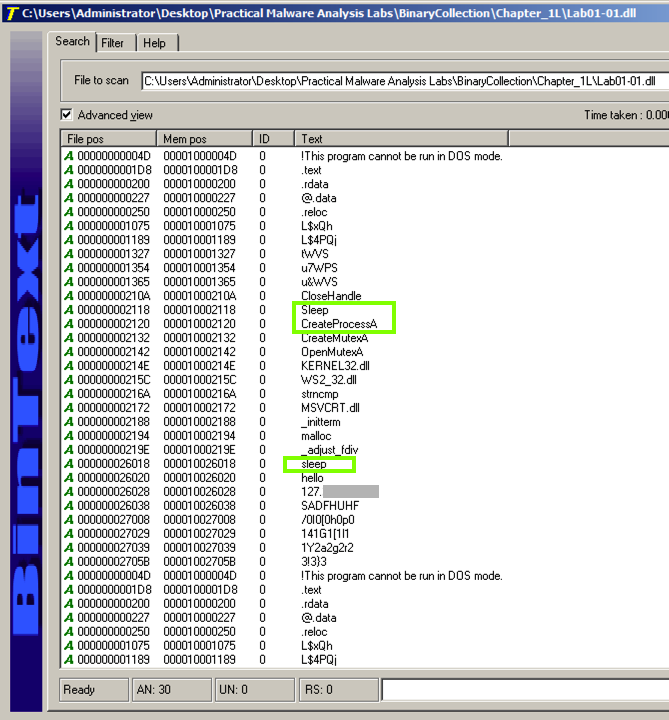
Get it here:

[https://www.mcafee.com/us/downloads/free-tools/bintext.aspx#](https://www.mcafee.com/us/downloads/free-tools/bintext.aspx)

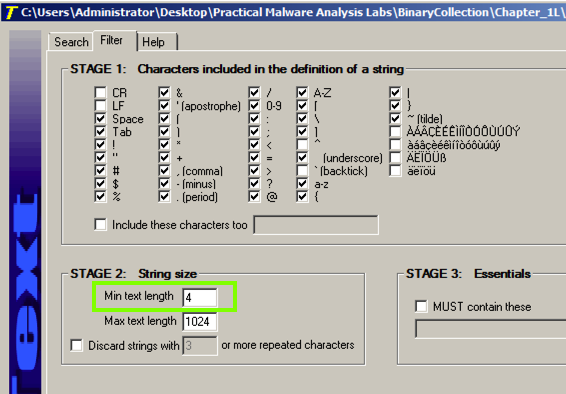
Look at the strings for **Lab01-01.dll**.

Notice these items, as shown below:

* **CreateProcessA** -- Windows API function used to launch a program
* **Sleep** -- Windows API function used to sleep
* **sleep** -- Commands that can be sent over the network to tell the malware to sleep

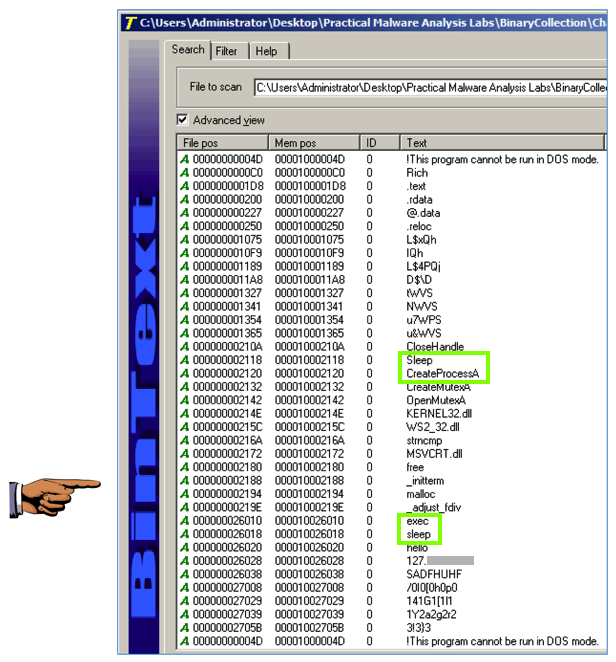


The command to launch a program is missing. To see it, click the **Filter** tab and adjust the "Min. text length" to **4** as shown below.



Click the **Search** tab. At the top right, click **Go**.

Now you can see that the command to launch a program is **exec**, as shown below.



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

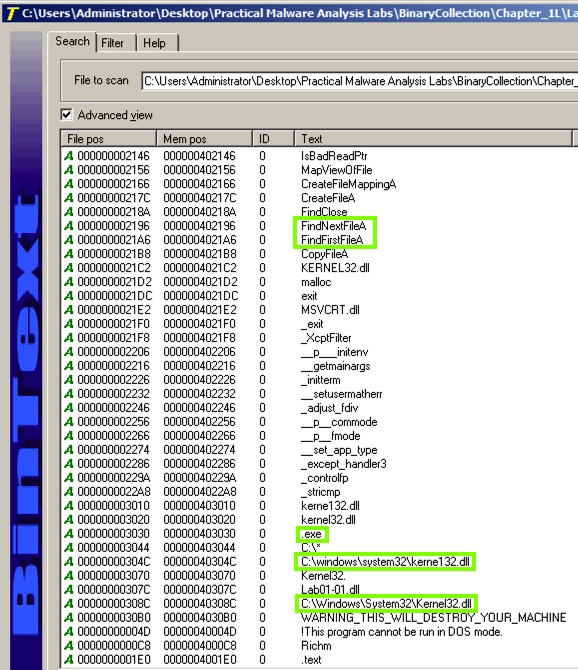
Below "sleep" and "hello" there is an IP address, starting with 127.

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

Save this image with the filename "**Proj 1d from YOUR NAME**". Then collect the strings from the **Lab01-01.exe** file.

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



**Dependency Walker**

You can download Dependency Walker here:

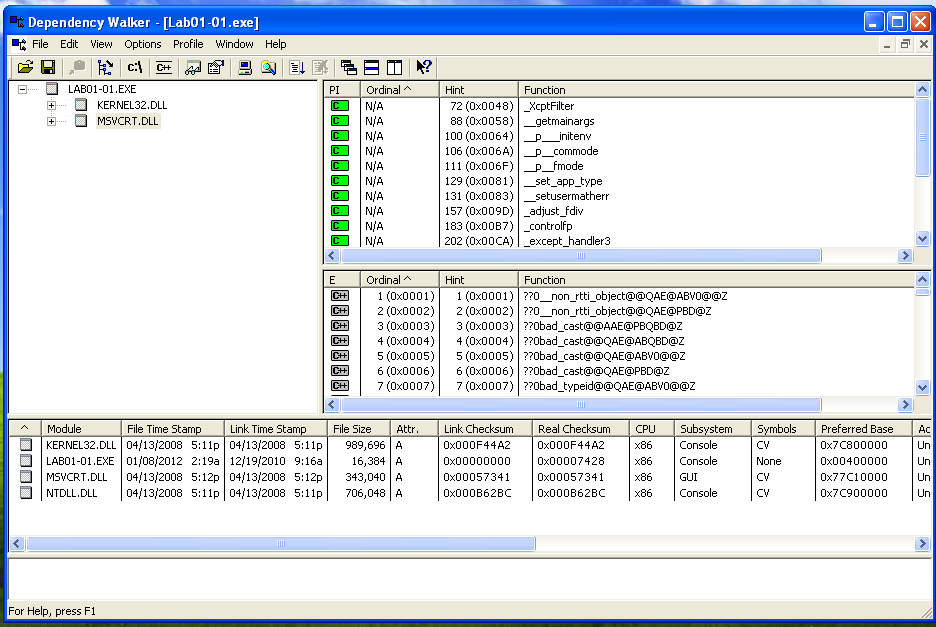
<http://www.dependencywalker.com/>

|  |
| --- |
| **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.

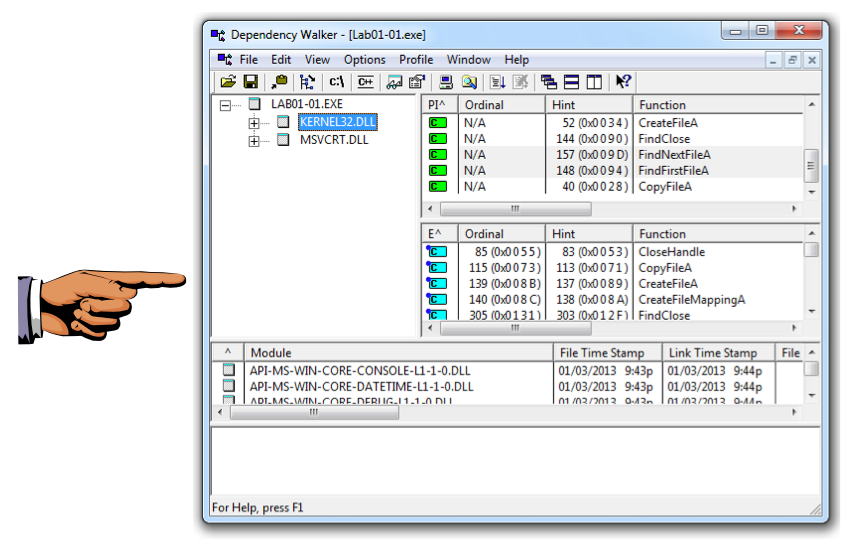
There are several imports in the upper right pane, and exports in the middle right pane. Scan through them--these are normal for any EXE.



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.

