PROJ 1 : BASIC STATIC TECHNIQUES 1

Prof. Alberto LaCava
CY -640
MALWARE ANALYSIS & DEFENSE

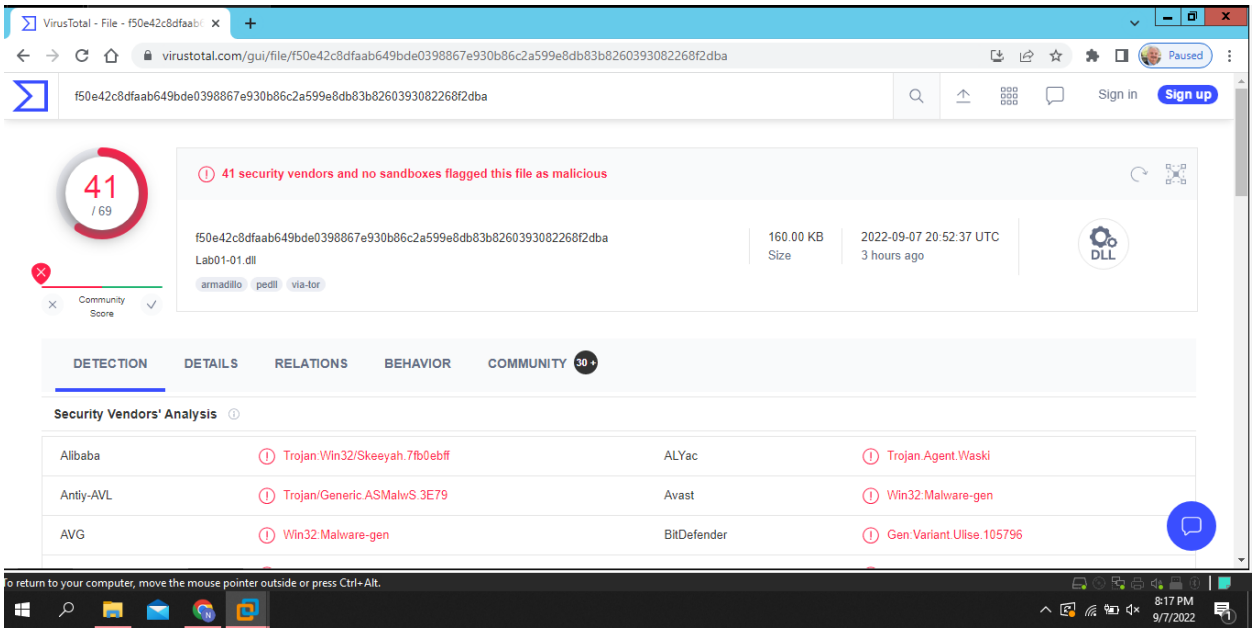
Nikhil Patel
09/13/2022

Overview : In this lab, I study static malware analysis methodologies. I utilized some of your tools. PEview, PEid, Dependency walker, strings, and so on are examples.

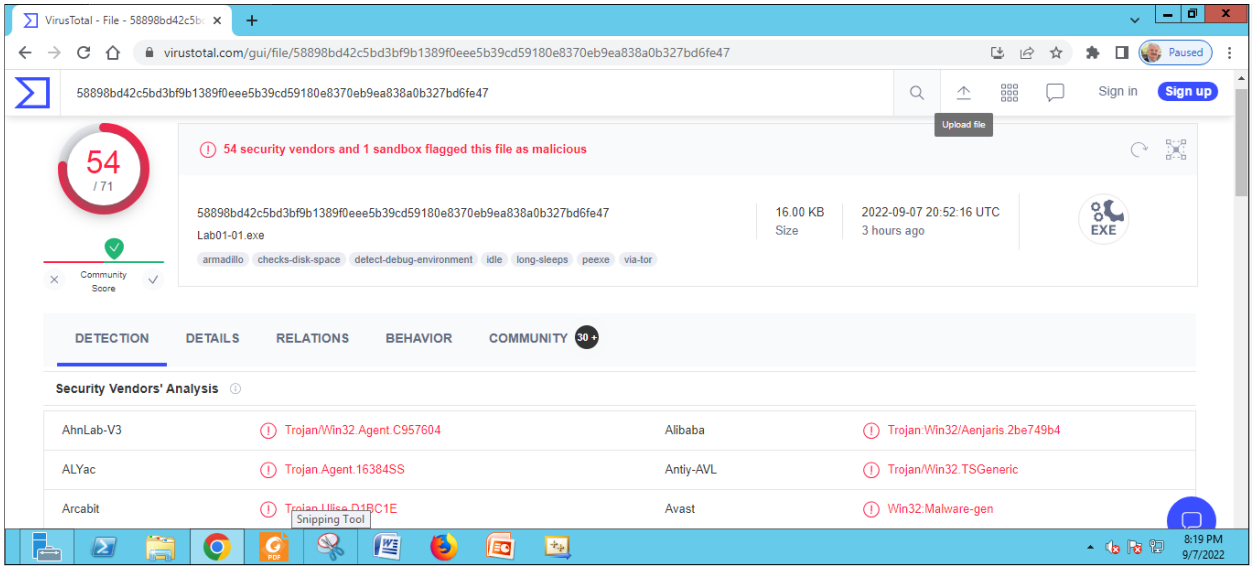
Procedure :

Step 1: Virus Total

- Go to Browser type virustotal.com
- Click on Upload a file
- Add those two files given in the folder of week 1 (Lab01-01.exe and Lab01-01.dll)
- You see the summary of those files you uploaded to virus total.



Above Image shows the Summary of Lab01-01.dll

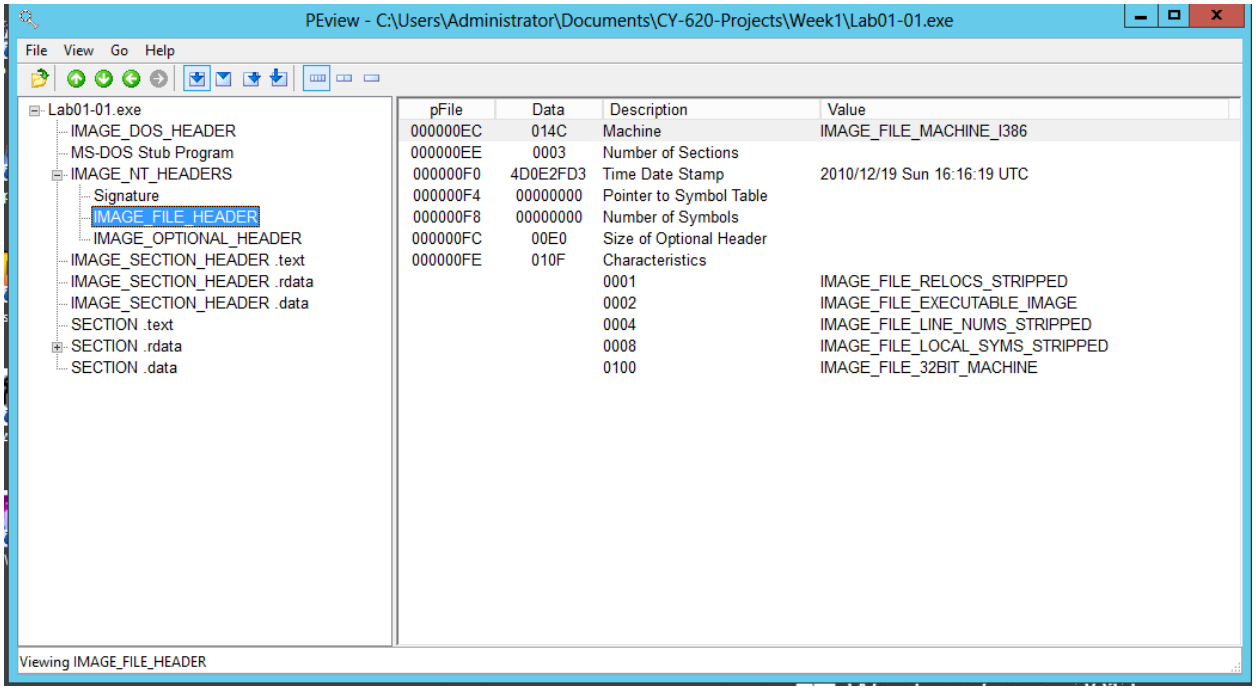


Above Image shows the Summary of Lab01-01.exe

<u>Step 2</u> : PEview

It gives fast simple way to the construction and content of 32-cycle versatile and part object record design documents.

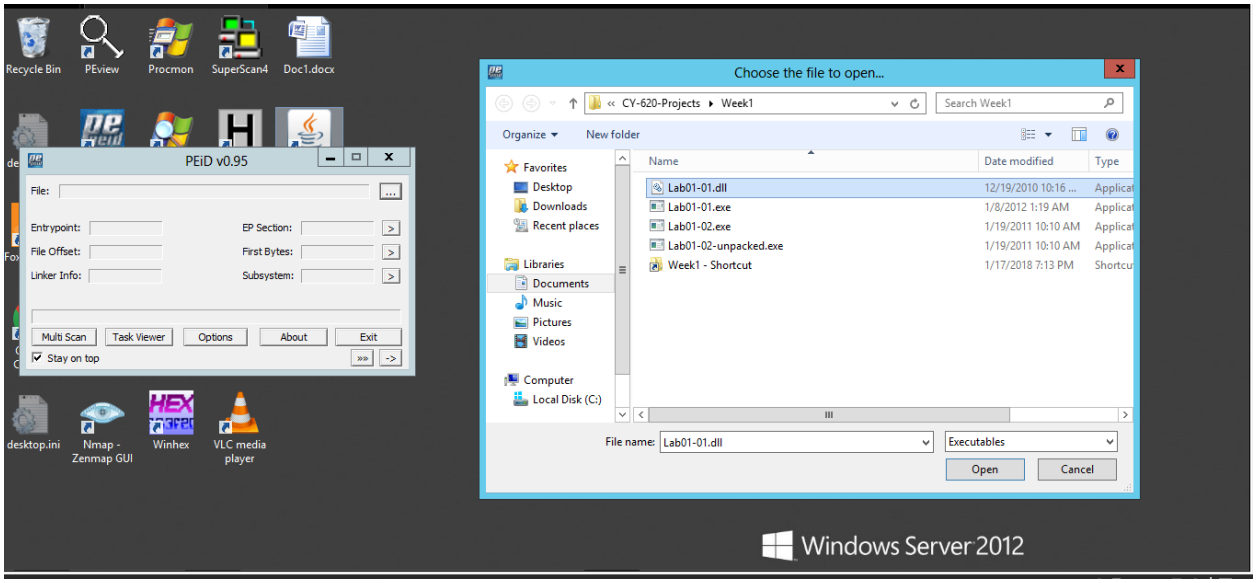
- Go to Start menu and type PEview or download it from the browser.
- Open Lab01-01.exe in PEview
- Then expand the image_nt_headers from left panel of the PEview.
- Click on Image_file_header and on right side of panel you can see data.

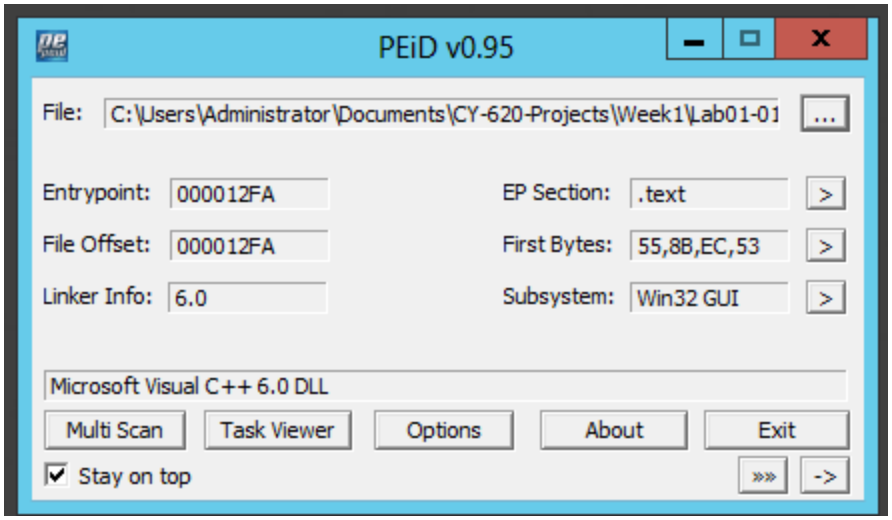


<u>Step 3</u> : PEiD

Cybercriminals generally pack their malware so deciding it is extremely challenging. This is a device that can distinguish 470 distinct structure marks in the PE document.

- Go to the Start menu and type PEiD or download it from the browser.
- Open Lab01-01.dll and it shows you the first bytes.

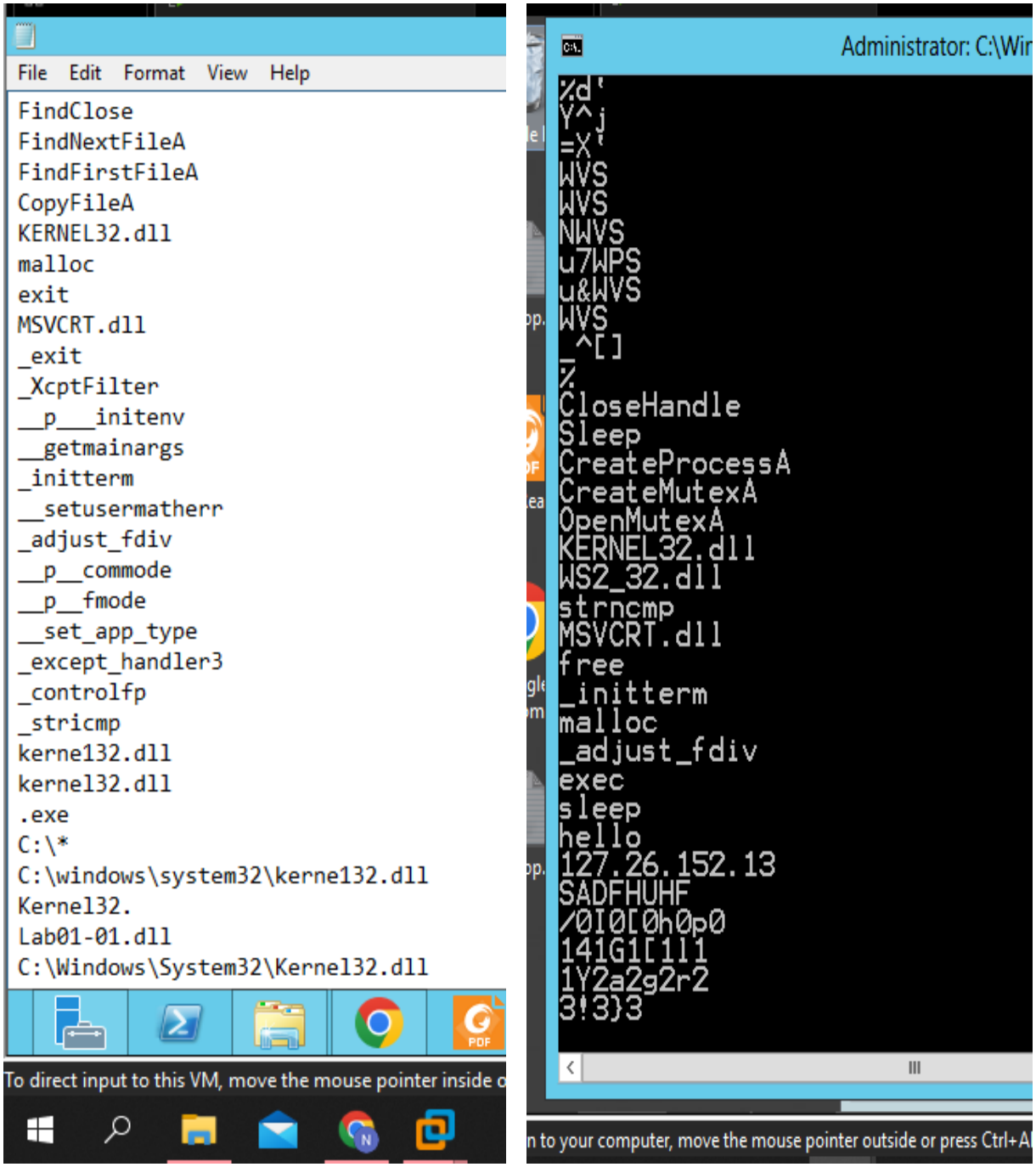




<u>Step 3</u> : Strings

The strings order searches for printable strings in a document. A string is any grouping of at least 4 printable characters that end with a new-line or an invalid person. The string order is helpful for recognizing arbitrary article documents.

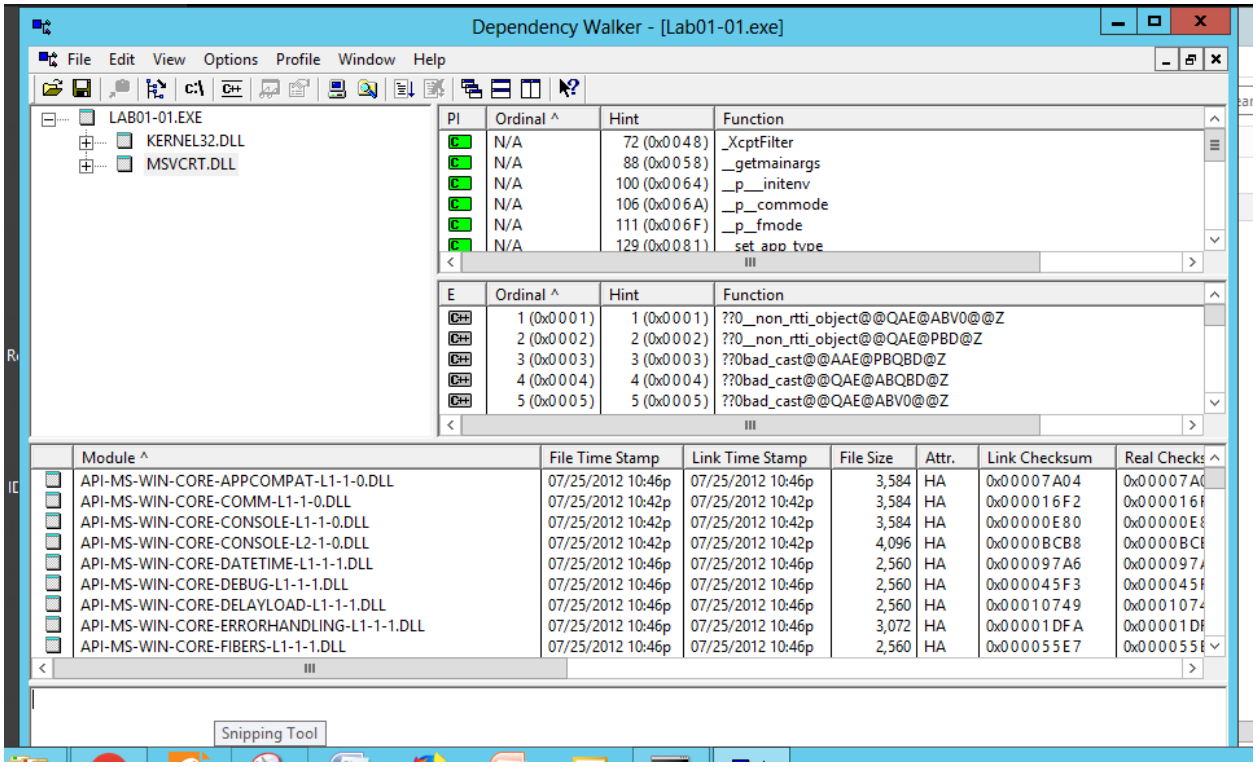
- Go to start and open Cmd in the C:\Windows\System32 folder.
- Cd "\Users\Administrator\Desktop\126\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L"
- Stings Lab01-01.exe > Str1exe.txt
- Notepad str1exe.txt



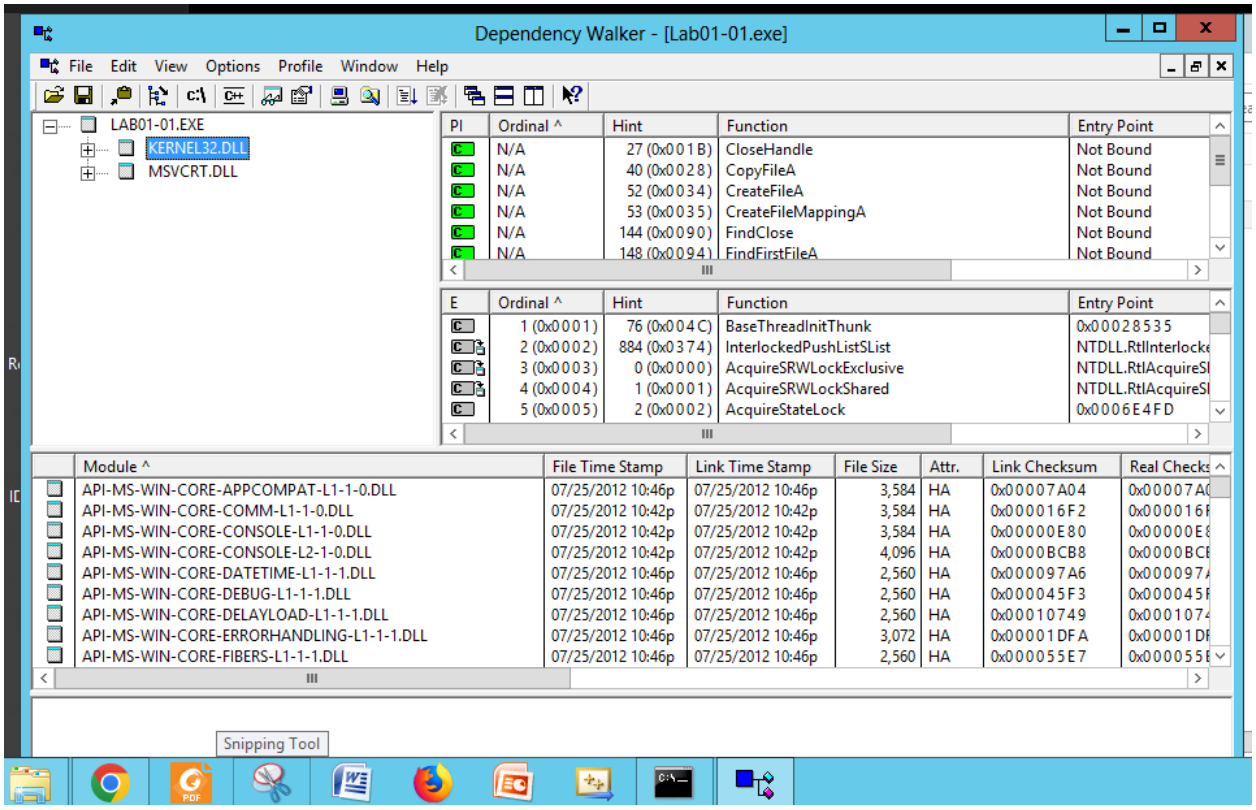
<u>Step 4</u>: Dependency Walker

It is utility outputs instrument which filters 32/64 pieces module(exe, dll, ocx, sys, and so on). It constructs a progressive tree chart of every single ward module. It is exceptionally valuable for investigating framework blunders related stacking and run modules.

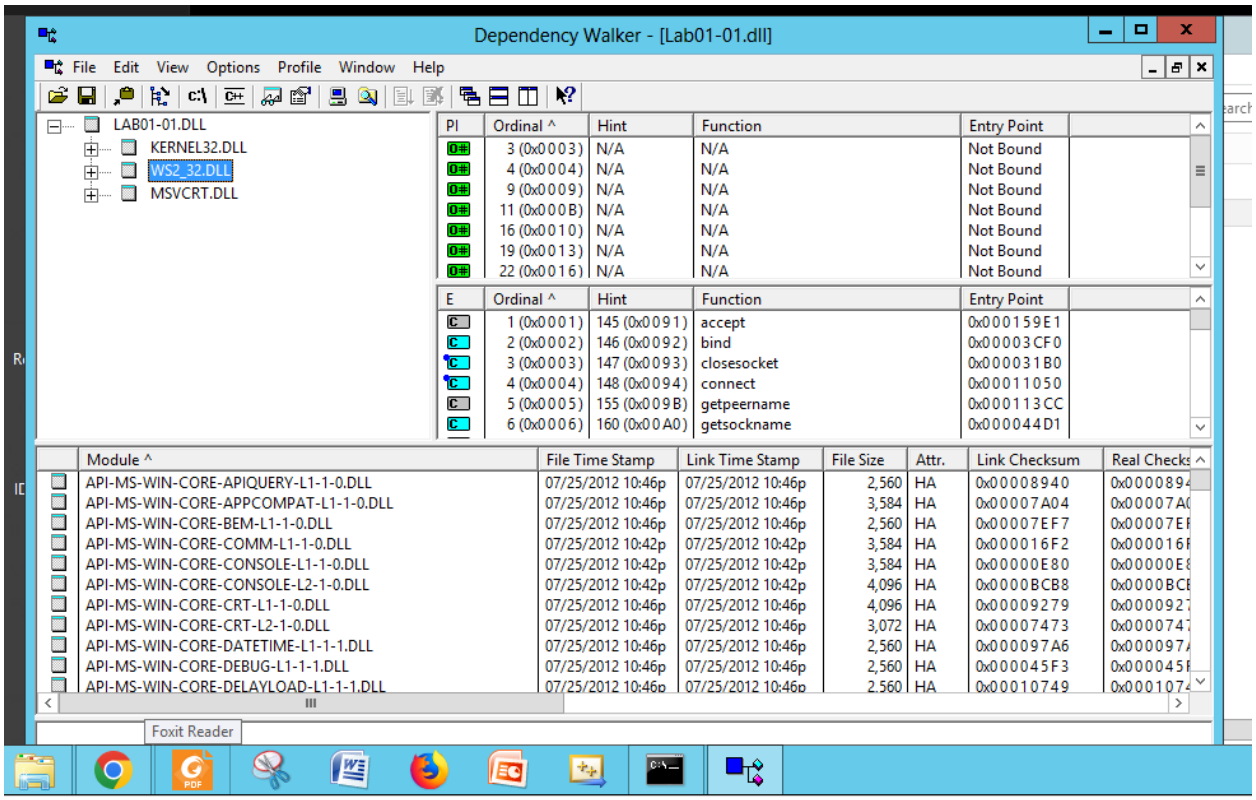
- Open Lab01-01.exe in Dependency Walker.
- In the left panel, click MSVCRT.DLL as shown below.



- In the left panel, click KERNEL32.DLL as shown below.



- Open Lab01-01.dll in Dependency Walker, you will notice WS2_32.DLL in the left panel.



Conclusion : To conclude with the lab, we have learned how to use Basic Static Techniques using VirusTotal, PEview, PEiD, Strings and at the end by using Dependency Walker tools.