|  |  |  |
| --- | --- | --- |
| C:\Users\thg\Desktop\ICT Logo\ICT_4C.jpg | | |
| Week | Malware Analysis Tools and Techniques | Duration |
| 1 | Basic Static Analysis - Practical | 120 mins |

**Lesson Objectives**

Perform Basic Static Analysis on unknown Portable Executable with the following tools:

* PEView
* Dependency Walker
* PEiD
* Strings

Submit your answers on MeL.

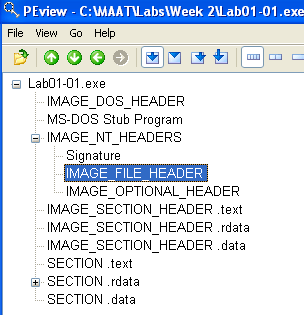
# Lab 01 [40 mins]

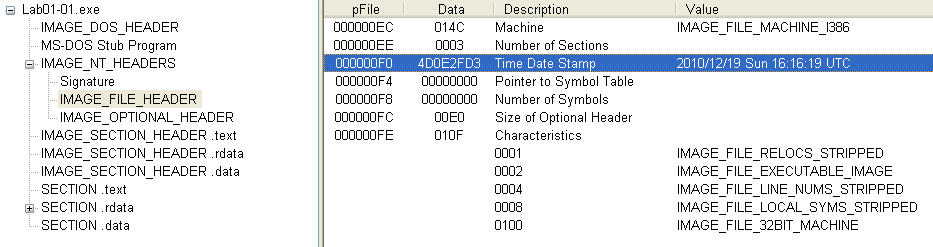
Refer to the files: lab01-01.exe and lab01-01.dll.

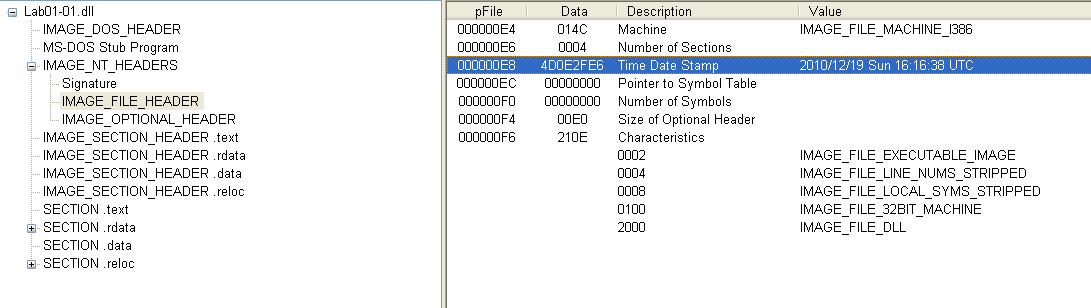
**Question 1**

When were these files compiled? 2010/12/19

(*hint: use PEview)*



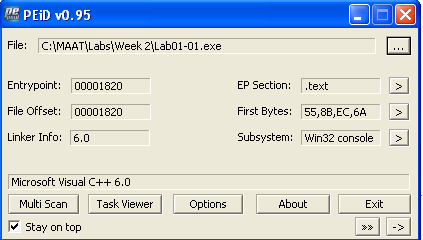


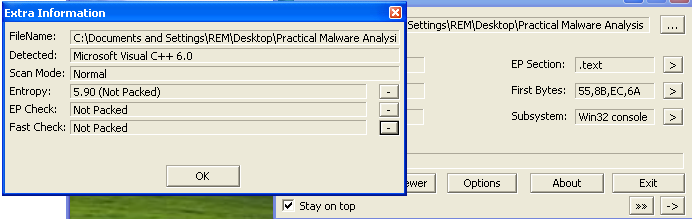


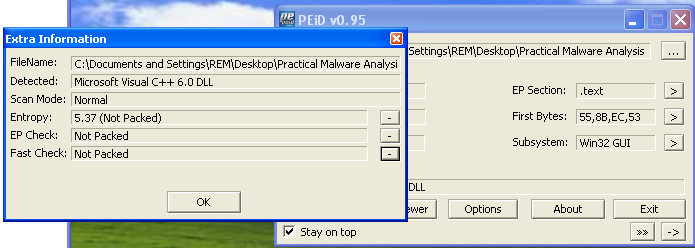
**Question 2**

Were these files packed? **The file is not packed**

(*hint: use PEiD)*



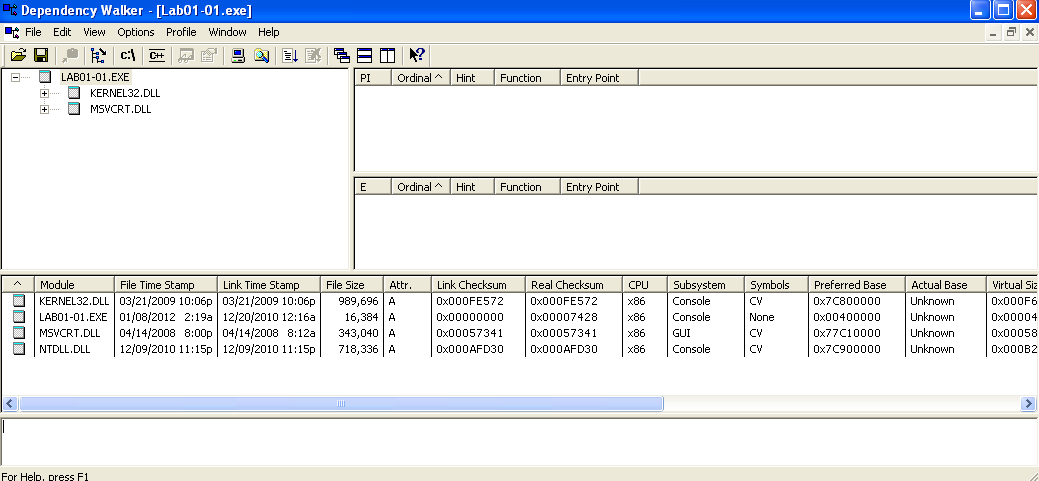




**Question 3**

What could be the functionalities of this malware, the exe and the dll, based on the imports? From exe file, we see FindFirstFileA, FindNextFileA, CopyFileA and CreateFileA being imported. It look like it is looking for a file and coping/moving the file somewhere else and create another file. From dlll file, we see CreateProcess and sleep imported, it look like it is creating a process.

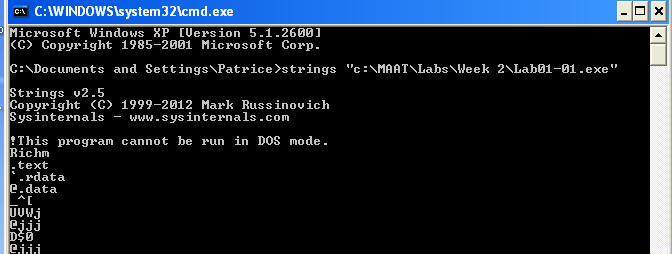
(*hint: use Dependency Walker and Strings)*



**Question 4**

What are some host-based indicators of this malware? 127.26.152.13

(*hint: is there any file being installed?)*



**Question 5**

What could be the purpose of this malware? The exe file is a malware installer that install the dll file which most likely is a backdoor malware.

# Lab 02 [80 mins]

Refer to the files: Lab01-02.exe and Lab01-03.exe

**Question 1**

Are the files packed? If so, what are the indicators and how could you unpack it?

**Question 2**

What are the imports of the malware?

**Question 3**

What important functions are imported in the DLL?

**Question 4**

What could be the functionality of the malware based on the import of the malware?

**Question 5**

What could be some host-based indicators?

**Question 6**

What could be some of the network-based indicators?