|  |  |  |
| --- | --- | --- |
| 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

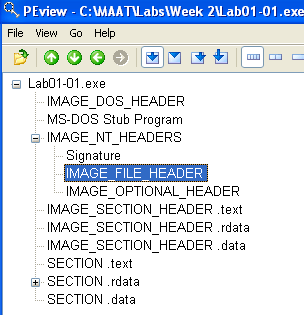
# Lab 01 [40 mins]

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

**Question 1**

When were these files compiled?

(*hint: use PEview)*



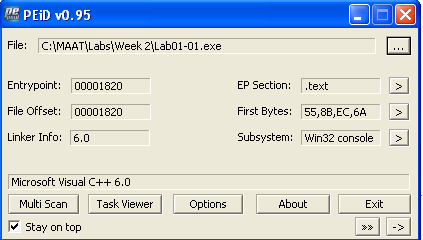
**Ans: 2010/12/19 Sun 16:16:19 UTC for .exe**

**Ans: 2010/12/19 Sun 16:16:39 UTC for .dll**

**Question 2**

Were these files packed?

(*hint: use PEiD)*

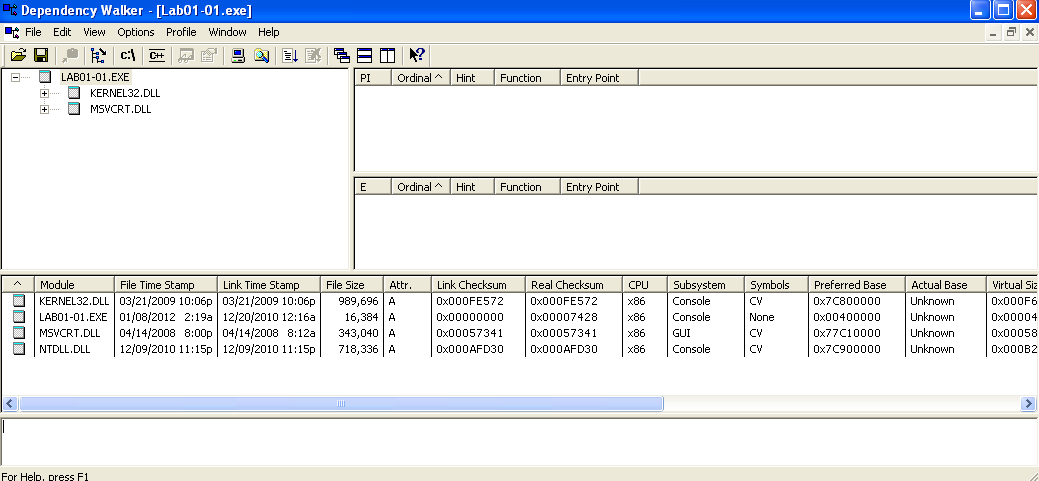


**Ans: It is not packed because PEiD does not display a packer. Rather it displays Microsoft Visual C++ 6.0 and Microsoft Visual C++ 6.0 DLL as the compiler respectively.**

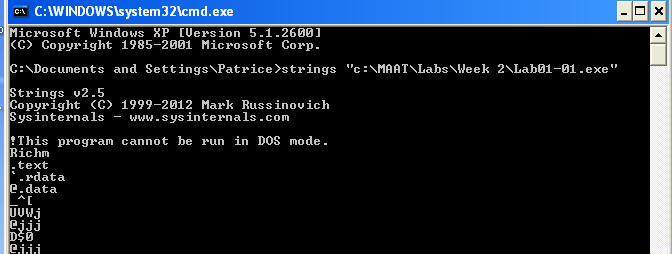
**Question 3**

What could be the functionalities of this malware, the exe and the dll, based on the imports?

(*hint: use Dependency Walker and Strings)*



It copies a file based on the functino that is imports (CopyFileA).



**host affects the system, network = internet, url, port number, protocols**

**Question 4**

What are some host-based indicators of this malware?

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

DLL – CreateMutex

**Question 5**

What could be the purpose of this 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?

Lab01-02 is packed. As the EP Section starts is UPX1

Lab01-03 is packed as the EP section is blank showing that there have been encryption or modifications made to it. The compiler is also the software name of the packer

Unpack using PeID plugins, unpacker for UPX.

Unable to unpack Lab01-03. No unpacked found to unpack the malware.

Analysis is inconclusive.

**Question 2**

What are the imports of the malware?

LoadLibraryA

GetPrcoAddress

**Question 3**

What important functions are imported in the DLL?

CsrCaptrueMessageString

**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?