

Dependency Walker

Lab 1:

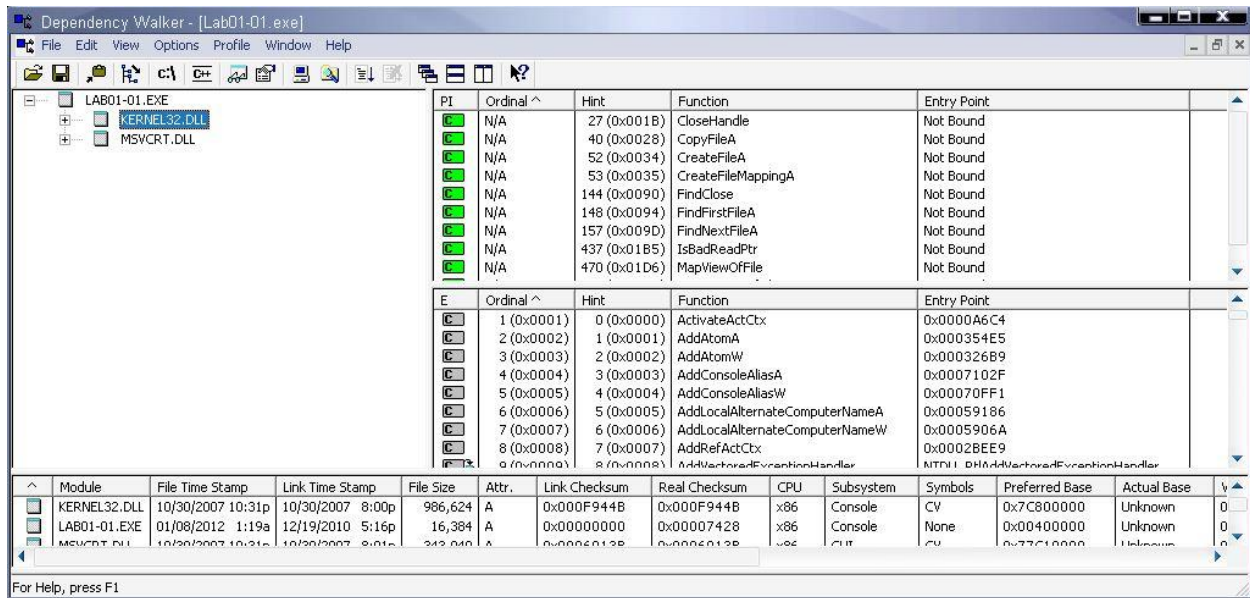


Figure 1 Lab1-01

Lab 2:

The screenshot shows the Dependency Walker application for Lab01-02.exe. The left pane displays the module tree with KERNEL32.DLL selected. The right pane shows the function list for the selected module. The bottom pane shows a list of loaded modules with a warning message.

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base
MSJAVA.DLL	Error opening file. The system cannot find the file specified (2).										
MPR.DLL	10/30/2007 10:31p	10/30/2007 7:59p	59,904	A	0x00018FCC	0x00018FCC	x86	Console	CV	0x71B20000	Unknown
ADVAPI32.DLL	10/30/2007 10:31p	10/30/2007 7:57p	617,472	A	0x000996BA	0x000996BA	x86	Console	CV	0x77DD0000	Unknown
CRYPT32.DLL	10/30/2007 10:31p	10/30/2007 7:58p	599,552	A	0x00094B92	0x00094B92	x86	GUI	CV	0x77A80000	Unknown

Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

For Help, press F1

Figure 2 Lab1-02

Lab 3:

Dependency Walker - [Lab01-03.exe]

File Edit View Options Profile Window Help

LAB01-03.EXE
 + KERNEL32.DLL

P/I	Ordinal ^	Hint	Function	Entry Point
	N/A	0 (0x0000)	LoadLibraryA	Not Bound
	N/A	0 (0x0000)	GetProcAddress	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
	1 (0x0001)	0 (0x0000)	ActivateActCtx	0x0000A6C4
	2 (0x0002)	1 (0x0001)	AddAtomA	0x000354E5
	3 (0x0003)	2 (0x0002)	AddAtomW	0x000326B9
	4 (0x0004)	3 (0x0003)	AddConsoleAliasA	0x0007102F
	5 (0x0005)	4 (0x0004)	AddConsoleAliasW	0x00070FF1

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Address
KERNEL32.DLL	10/30/2007 10:31p	10/30/2007 8:00p	986,624	A	0x000F944B	0x000F944B	x86	Console	CV	0x7C800000	Unknown	0x00400000
LAB01-03.EXE	03/26/2011 6:54a	01/01/1970 1:00a	4,752	A	0x00000000	0x0000CED2	x86	Console	None	0x00400000	Unknown	0x00400000
NTDLL.DLL	10/30/2007 10:30p	10/30/2007 8:00p	706,048	A	0x000AF170	0x000AF170	x86	Console	CV	0x7C900000	Unknown	0x00400000

For Help, press F1

Figure 3 Lab1-03

Lab 4:

Dependency Walker - [Lab01-04.exe]

File Edit View Options Profile Window Help

LAB01-04.EXE

- NTDLL.DLL
- ADVAPI32.DLL
- KERNEL32.DLL
- NTDLL.DLL
- RPCRT4.DLL
- WINTRUST.DLL
- SECUR32.DLL
- MSVCRT.DLL
- KERNEL32.DLL
- NTDLL.DLL

PI	Ordinal ^	Hint	Function	Entry Point
6	N/A	27 (0x001B)	CloseHandle	Not Bound
6	N/A	52 (0x0034)	CreateFileA	Not Bound
6	N/A	70 (0x0046)	CreateRemoteThread	Not Bound
6	N/A	163 (0x00A3)	FindResourceA	Not Bound
6	N/A	247 (0x00F7)	GetCurrentProcess	Not Bound
6	N/A	294 (0x0126)	GetModuleHandleA	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
1	1 (0x0001)	0 (0x0000)	ActivateActCtx	0x0000A6C4
2	2 (0x0002)	1 (0x0001)	AddAtomA	0x000354E5
3	3 (0x0003)	2 (0x0002)	AddAtomW	0x000326B9
4	4 (0x0004)	3 (0x0003)	AddConsoleAliasA	0x0007102F
5	5 (0x0005)	4 (0x0004)	AddConsoleAliasW	0x00070FF1

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base
MSJAVA.DLL	10/30/2007 10:31p	10/30/2007 7:59p	59,904	A	0x00018FCC	0x00018FCC	x86	Console	CV	0x71B20000	Unknown
MPR.DLL	10/30/2007 10:31p	10/30/2007 7:57p	617,472	A	0x000996BA	0x000996BA	x86	Console	CV	0x77DD0000	Unknown
ADVAPI32.DLL	10/30/2007 10:31p	10/30/2007 8:00p	986,624	A	0x000F9448	0x000F9448	x86	Console	CV	0x7C800000	Unknown
KERNEL32.DLL	10/30/2007 10:31p	10/30/2019 11:26p	36,864	A	0x00000000	0x0000D3EE	x86	GUI	None	0x00400000	Unknown
LAB01-04.EXE	07/05/2011 6:16p	08/30/2019 11:26p	343,040	A	0x0006013B	0x0006013B	x86	GUI	CV	0x77C10000	Unknown
MSVCRT.DLL	10/30/2007 10:31p	10/30/2007 8:01p	706,048	A	0x000AF170	0x000AF170	x86	Console	CV	0x7C900000	Unknown
NTDLL.DLL	10/30/2007 10:30p	10/30/2007 8:00p									

Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

For Help, press F1

Figure 4 Lab1-04

PEview

Image File Header

Lab 01:

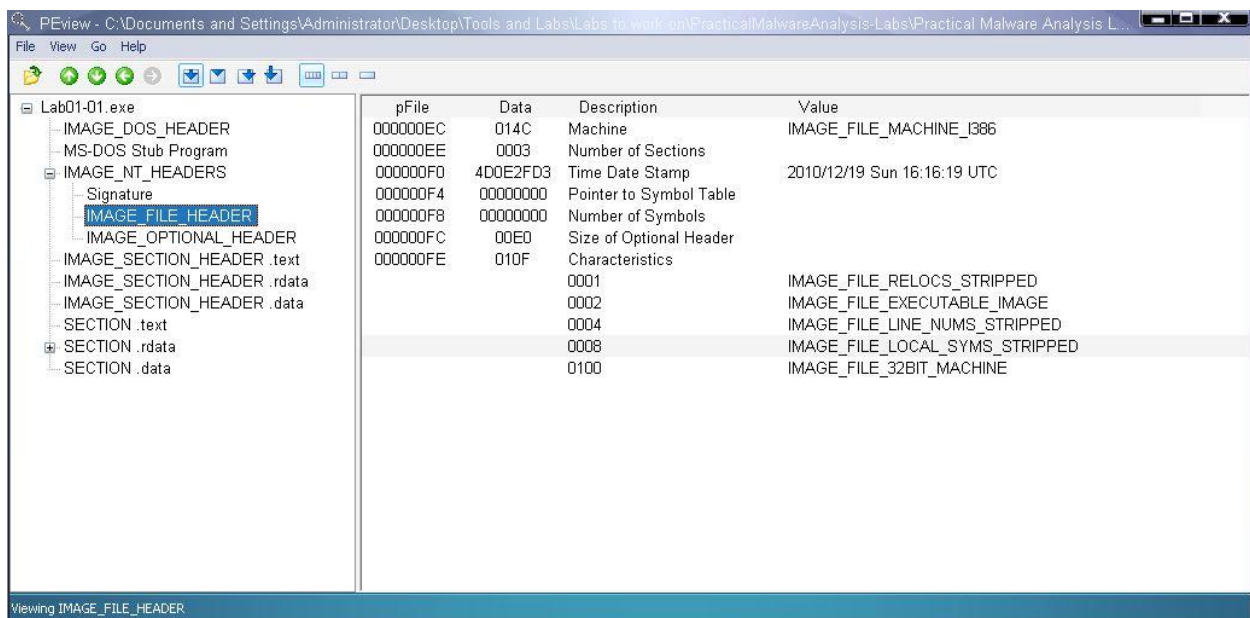


Figure 5 Lab1-01

Lab 02:

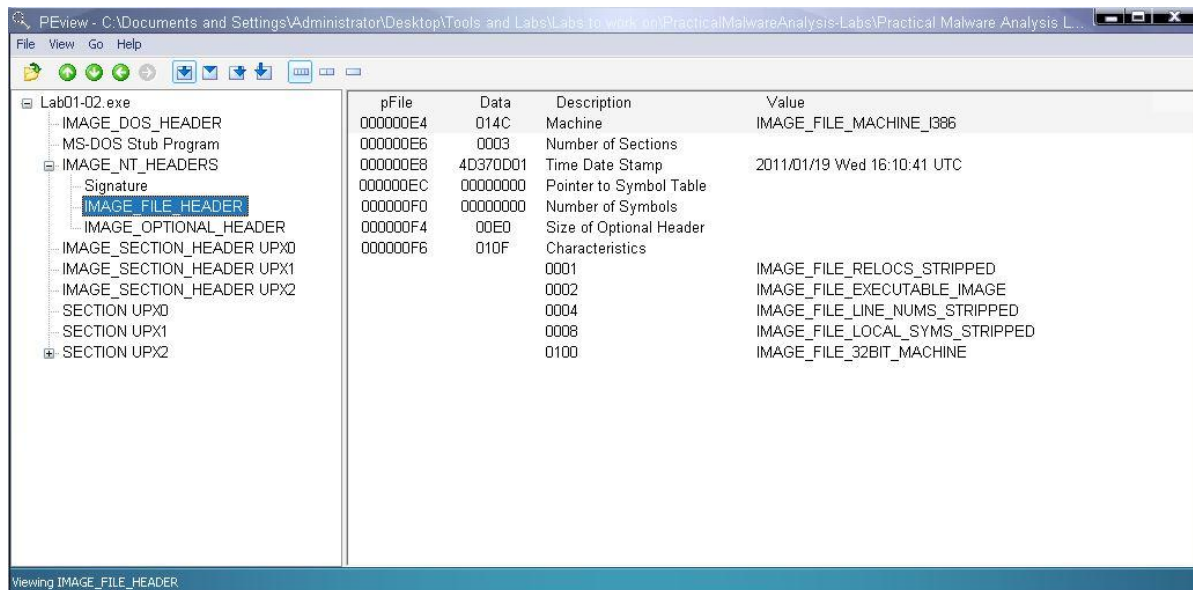


Figure 6 Lab01-2

Lab 03:

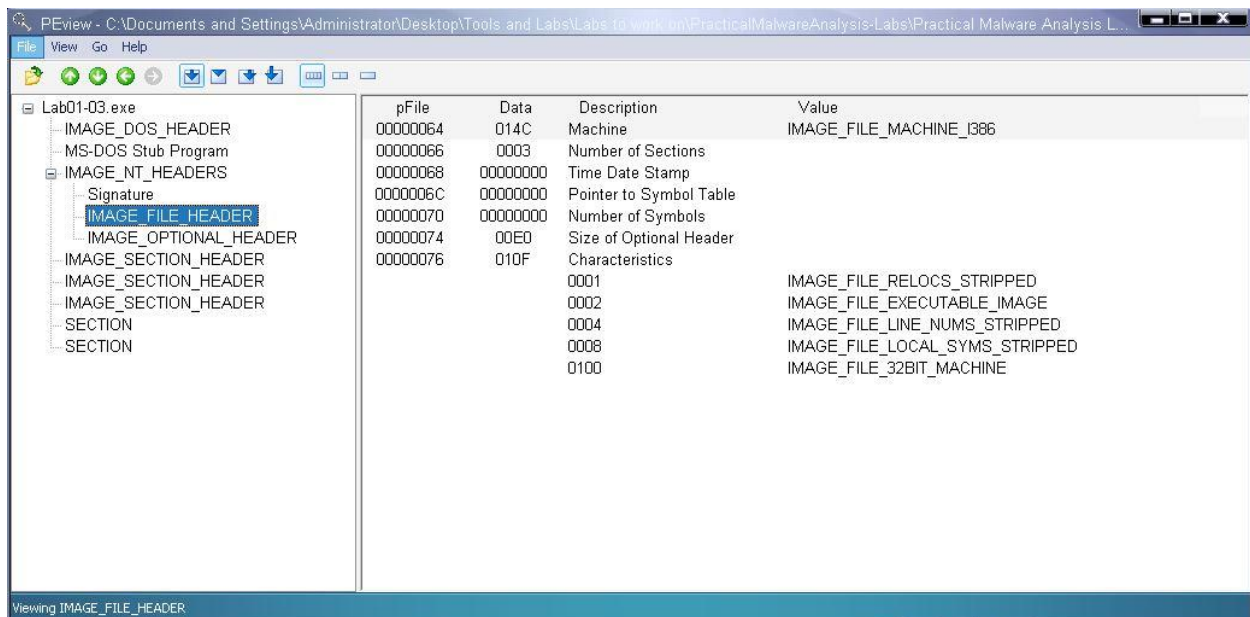


Figure 7 Lab01-3

Lab 04:

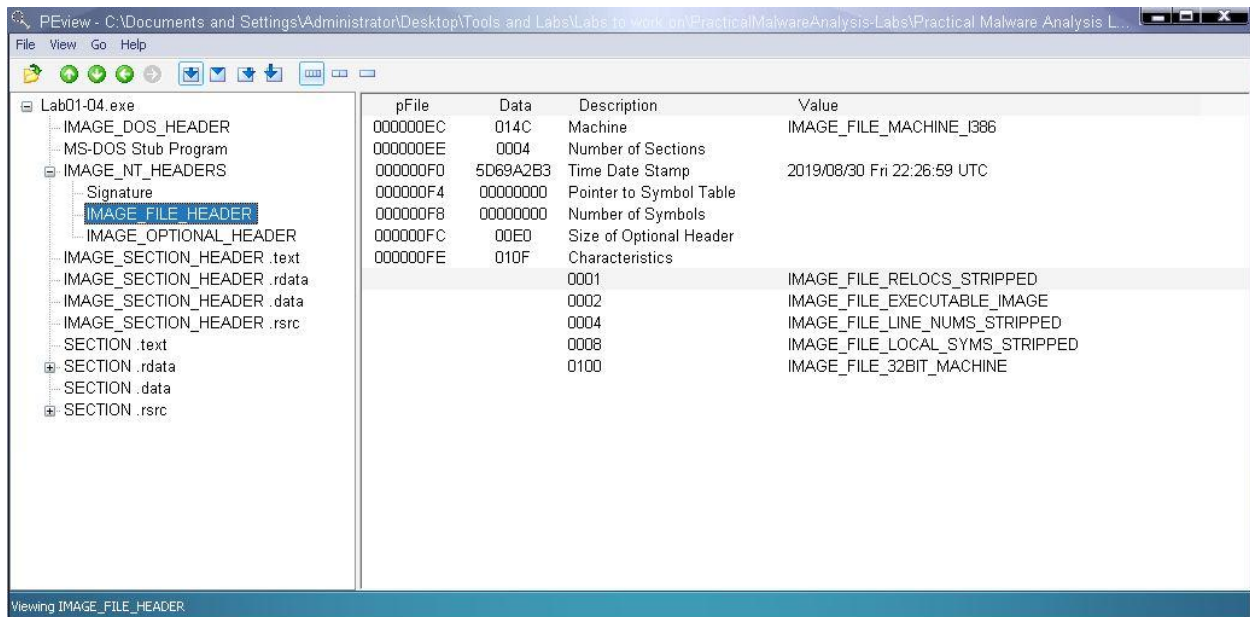


Figure 8 Lab01-4

Image Section Header

Lab 01:

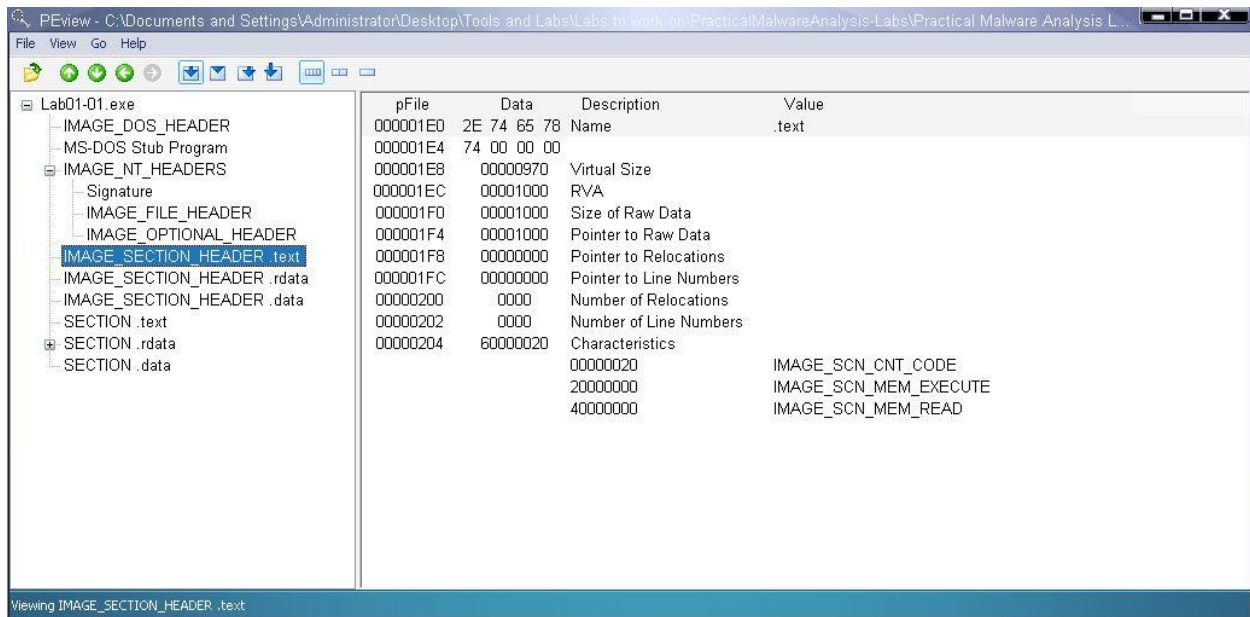


Figure 9 Lab01-1

Lab 02:

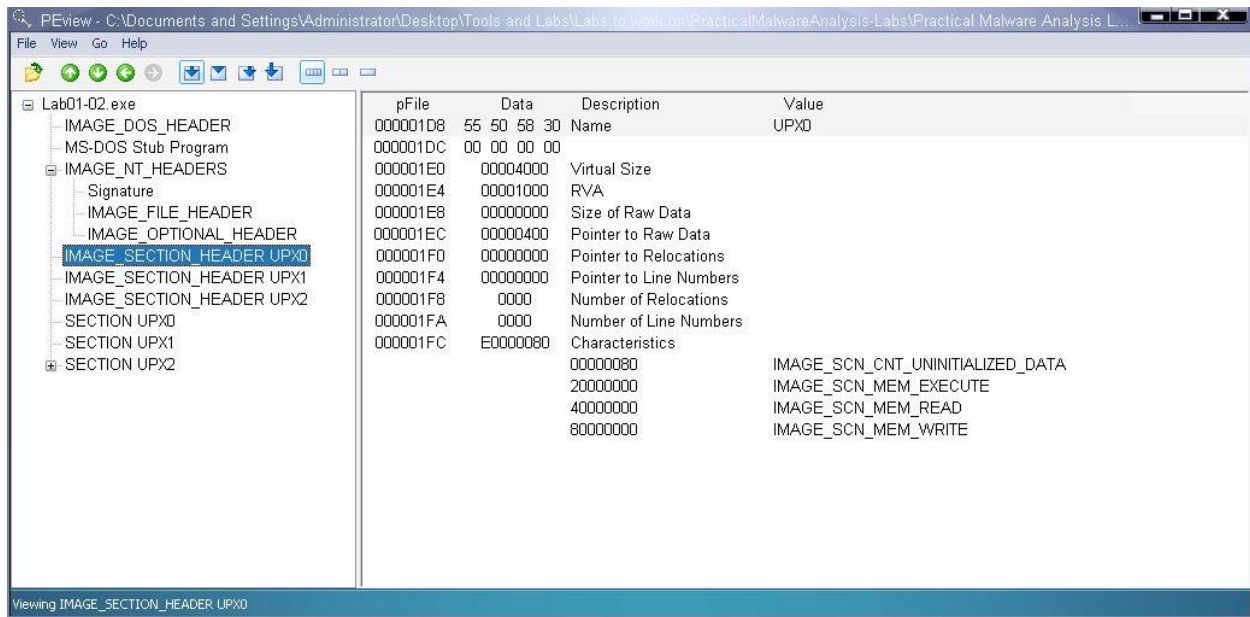


Figure 10 Lab01-2

Lab 03:

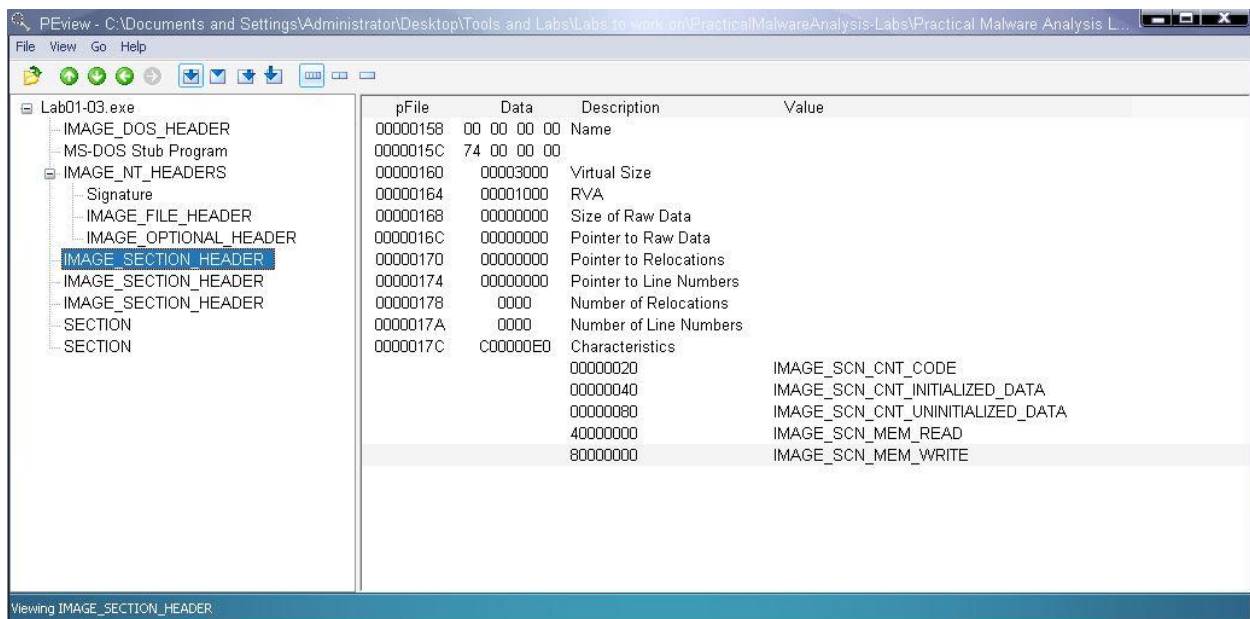


Figure 11 Lab01-3

Lab 04:

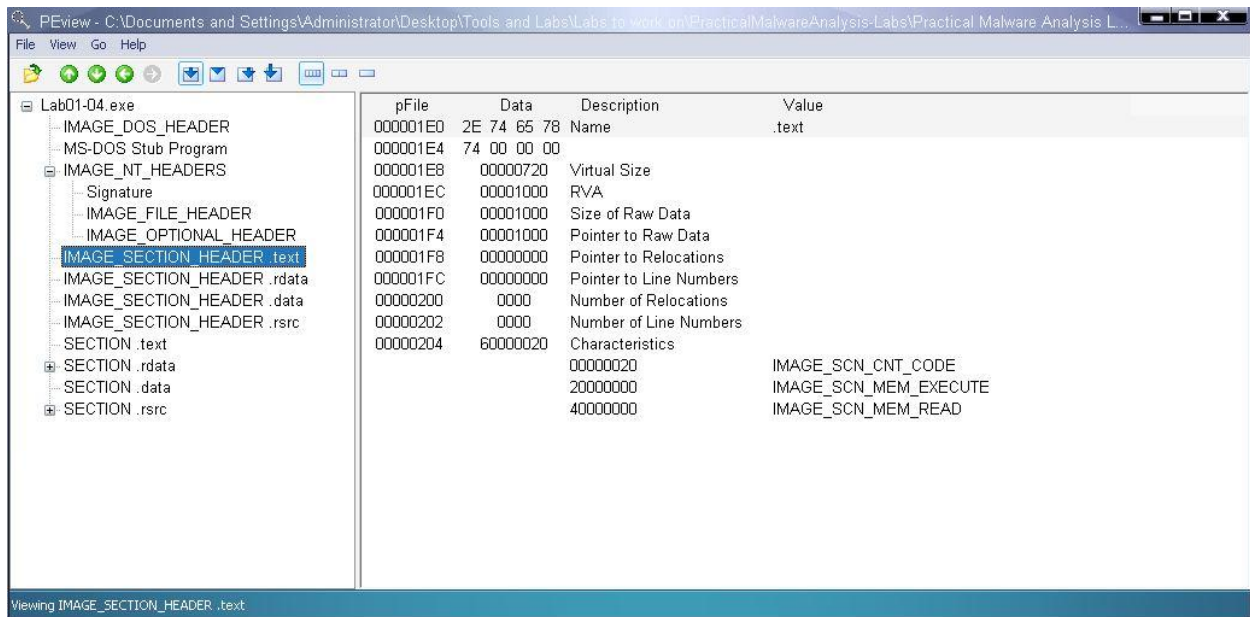


Figure 12 Lab01-4