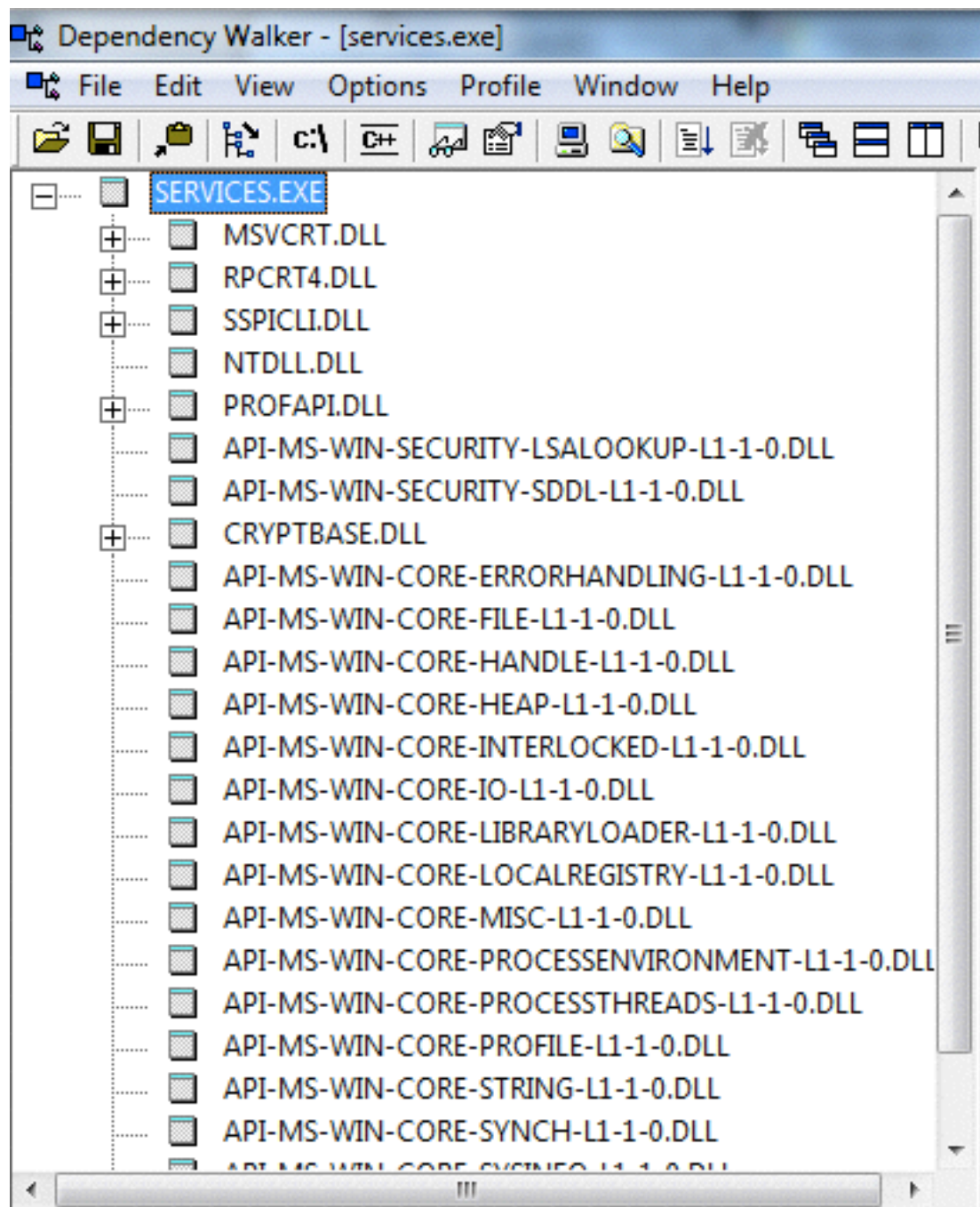


# Dependency Walker

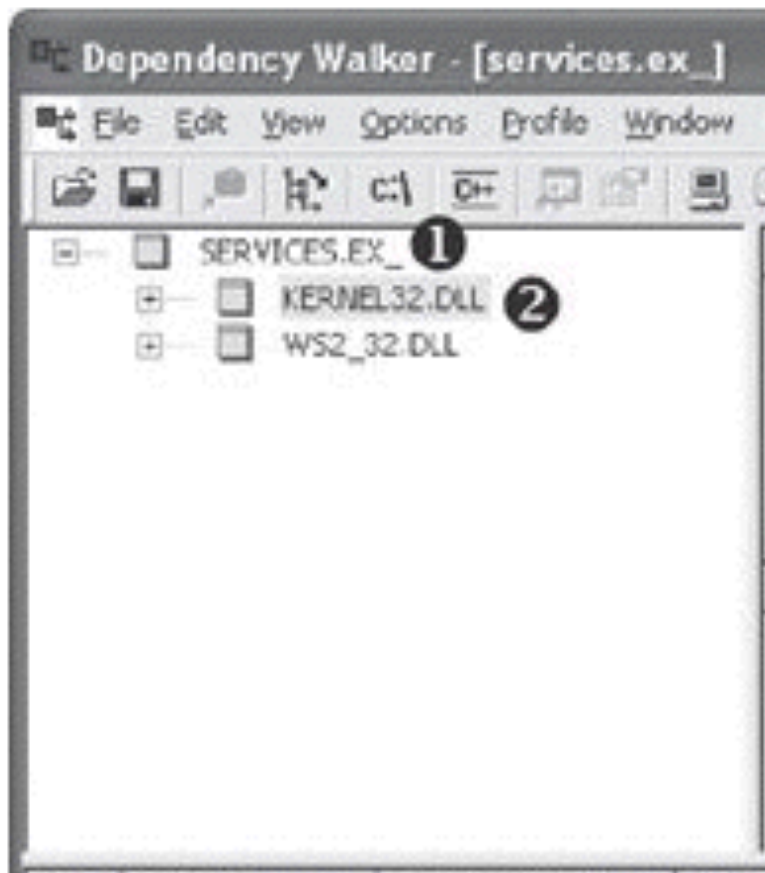
# Shows Dynamically Linked Functions

- Normal programs have a lot of DLLs
- Malware often has very few DLLs

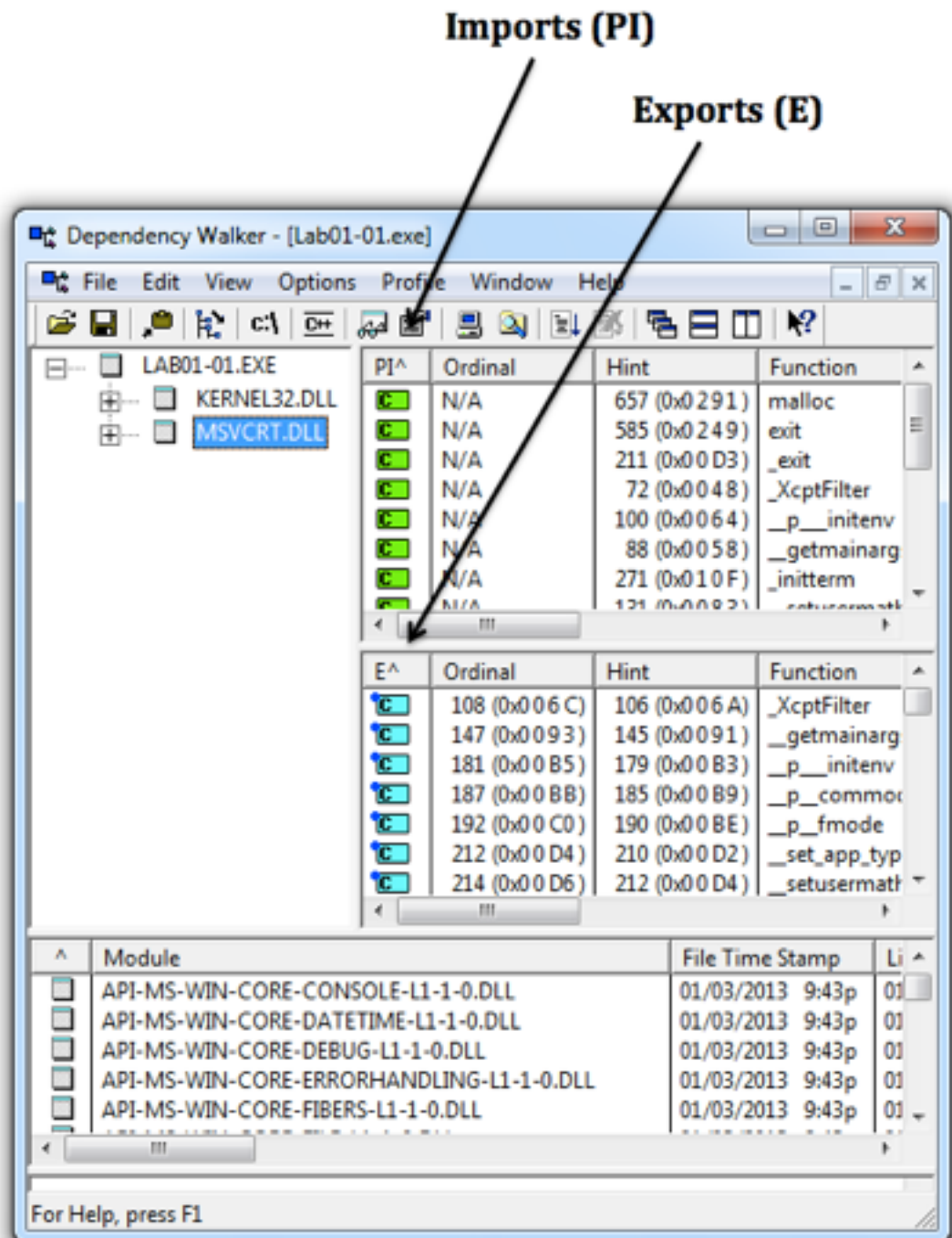
# Services.exe



# Services.ex\_ (malware)



# Imports & Exports in Dependency Walker



*Table 2-1. Common DLLs*

<b>DLL</b>	<b>Description</b>
<i>Kernel32.dll</i>	This is a very common DLL that contains core functionality, such as access and manipulation of memory, files, and hardware.
<i>Advapi32.dll</i>	This DLL provides access to advanced core Windows components such as the Service Manager and Registry.
<i>User32.dll</i>	This DLL contains all the user-interface components, such as buttons, scroll bars, and components for controlling and responding to user actions.
<i>Gdi32.dll</i>	This DLL contains functions for displaying and manipulating graphics.

*Ntdll.dll* This DLL is the interface to the Windows kernel. Executables generally do not import this file directly, although it is always imported indirectly by *Kernel32.dll*. If an executable imports this file, it means that the author intended to use functionality not normally available to Windows programs. Some tasks, such as hiding functionality or manipulating processes, will use this interface.

*WSock32.dll* and *Ws2\_32.dll* These are networking DLLs. A program that accesses either of these most likely connects to a network or performs network-related tasks.

*Wininet.dll* This DLL contains higher-level networking functions that implement protocols such as FTP, HTTP, and NTP.

# Exports

- DLLs **export** functions
- EXEs **import** functions
- Both exports and imports are listed in the PE header



# Notepad.exe

PEview - C:\Windows\System32\notepad.exe

File View Go Help

notepad.exe

- IMAGE\_DOS\_HEADER
- MS-DOS Stub Program
- IMAGE\_NT\_HEADERS
  - IMAGE\_SECTION\_HEADER .text
  - IMAGE\_SECTION\_HEADER .data
  - IMAGE\_SECTION\_HEADER .rsrc
  - IMAGE\_SECTION\_HEADER .reloc
  - BOUND\_IMPORT Directory Table
  - BOUND\_IMPORT DLL Names
- SECTION .text
  - IMPORT Address Table**
  - IMAGE\_LOAD\_CONFIG\_DIRECTORY
  - IMPORT Directory Table
  - IMPORT DLL Names
  - IMPORT Name Table
  - IMPORT Hints/Names
  - IMAGE\_DEBUG\_DIRECTORY
  - IMAGE\_DEBUG\_TYPE\_RESERVED10
  - IMAGE\_DEBUG\_TYPE\_CODEVIEW
- SECTION .data
- SECTION .rsrc
- SECTION .reloc

pFile	Data	Description	Value
00000400	77CBF79F	Virtual Address	0268 RegQueryValueExW
00000404	77CBF429	Virtual Address	022A RegCloseKey
00000408	77CAB83D	Virtual Address	0236 RegCreateKeyW
0000040C	77CAB889	Virtual Address	017A IsTextUnicode
00000410	77CABA90	Virtual Address	0278 RegSetValueExW
00000414	00000000	End of Imports	ADVAPI32.dll
00000418	77E1C83B	Virtual Address	01D1 GetFileInformationByHandle
0000041C	77E3F7C8	Virtual Address	012C FindNLSString
00000420	77E38E8A	Virtual Address	028A GlobalAlloc
00000424	77E39E35	Virtual Address	029C GlobalUnlock
00000428	77E39EF7	Virtual Address	0295 GlobalLock
0000042C	77E122E8	Virtual Address	007D CreateFileMappingW
00000430	77E338E0	Virtual Address	01B1 GetDateFormatW
00000434	77E334E1	Virtual Address	01E8 GetLocalTime
00000438	77E0F277	Virtual Address	0308 LocalUnlock
0000043C	77E37F30	Virtual Address	030F MapViewOfFile
00000440	77E35CAE	Virtual Address	031F MultiByteToWideChar
00000444	77E3C8DA	Virtual Address	044B UnmapViewOfFile
00000448	77E0C935	Virtual Address	0305 LocalReAlloc
0000044C	77E14BFD	Virtual Address	0153 GetACP
00000450	77E0C5C8	Virtual Address	00C4 DeleteFileW
00000454	77E07FFC	Virtual Address	03D5 SetEndOfFile
00000458	77E0F33F	Virtual Address	0304 LocalLock
0000045C	77E11292	Virtual Address	0149 FormatMessageW
00000460	77E3D198	Virtual Address	0484 WideCharToMultiByte
00000464	77E3D198	Virtual Address	0484 WideCharToMultiByte

Viewing IMPORT Address Table

# Advapi32.dll

PEview - C:\Windows\System32\advapi32.dll

File View Go Help

advapi32.dll

- IMAGE\_DOS\_HEADER
- MS-DOS Stub Program
- IMAGE\_NT\_HEADERS
  - IMAGE\_SECTION\_HEADER .text
  - IMAGE\_SECTION\_HEADER .data
  - IMAGE\_SECTION\_HEADER .rsrc
  - IMAGE\_SECTION\_HEADER .reloc
- BOUND\_IMPORT Directory Table
- BOUND\_IMPORT DLL Names
- SECTION .text
  - IMPORT Address Table
  - IMAGE\_LOAD\_CONFIG\_DIRECTORY
  - IMAGE\_EXPORT\_DIRECTORY
  - EXPORT Address Table**
  - EXPORT Name Pointer Table
  - EXPORT Ordinal Table
  - EXPORT Names
  - DELAY\_IMPORT Descriptors
  - DELAY\_IMPORT DLL Names
  - DELAY\_IMPORT Name Table
  - DELAY\_IMPORT Hints/Names
  - IMPORT Directory Table
  - IMPORT DLL Names
  - IMPORT Name Table
  - IMPORT Hints/Names

pFile	Data	Description	Value
00037F20	0008606A	Function RVA	0001 I_ScGetCurrentGroupStateW
00037F24	0003EC70	Forwarded Name RVA	0002 A_SHAFinal -> NTDLL.A_SHAFinal
00037F28	0003EC81	Forwarded Name RVA	0003 A_SHAInit -> NTDLL.A_SHAInit
00037F2C	0003EC91	Forwarded Name RVA	0004 A_SHAUpdate -> NTDLL.A_SHAUpdate
00037F30	00081746	Function RVA	0005 AbortSystemShutdownA
00037F34	000816F2	Function RVA	0006 AbortSystemShutdownW
00037F38	000341F0	Function RVA	0007 AccessCheck
00037F3C	000630A1	Function RVA	0008 AccessCheckAndAuditAlarmA
00037F40	00011BA7	Function RVA	0009 AccessCheckAndAuditAlarmW
00037F44	0002B4F9	Function RVA	000A AccessCheckByType
00037F48	0006318B	Function RVA	000B AccessCheckByTypeAndAuditAlarmA
00037F4C	00062E8F	Function RVA	000C AccessCheckByTypeAndAuditAlarmW
00037F50	00062E21	Function RVA	000D AccessCheckByTypeResultList
00037F54	00063284	Function RVA	000E AccessCheckByTypeResultListAndAuditAlarmA
00037F58	0006337D	Function RVA	000F AccessCheckByTypeResultListAndAuditAlarmByHandleA
00037F5C	00062FEC	Function RVA	0010 AccessCheckByTypeResultListAndAuditAlarmByHandleW
00037F60	00062F3A	Function RVA	0011 AccessCheckByTypeResultListAndAuditAlarmW
00037F64	0002D7E0	Function RVA	0012 AddAccessAllowedAce
00037F68	0001BBB9	Function RVA	0013 AddAccessAllowedAceEx
00037F6C	00063635	Function RVA	0014 AddAccessAllowedObjectAce
00037F70	00009988	Function RVA	0015 AddAccessDeniedAce
00037F74	0006359F	Function RVA	0016 AddAccessDeniedAceEx
00037F78	00063683	Function RVA	0017 AddAccessDeniedObjectAce
00037F7C	00013C00	Function RVA	0018 AddAce
00037F80	00001B89	Function RVA	0019 AddAuditAccessAce

Viewing EXPORT Address Table

# iTunesSetup.exe

PEview - C:\Users\Administrator\Downloads\iTunesSetup.exe

File View Go Help

iTunesSetup.exe

- IMAGE\_DOS\_HEADER
- MS-DOS Stub Program
- IMAGE\_NT\_HEADERS
  - IMAGE\_SECTION\_HEADER .text
  - IMAGE\_SECTION\_HEADER .rdata
  - IMAGE\_SECTION\_HEADER .data
  - IMAGE\_SECTION\_HEADER .rsrc
  - IMAGE\_SECTION\_HEADER .reloc
  - SECTION .text
  - SECTION .rdata
    - IMPORT Address Table
    - IMAGE\_DEBUG\_DIRECTORY
    - IMAGE\_LOAD\_CONFIG\_DIRECTORY
    - IMAGE\_DEBUG\_TYPE\_CODEVIEW
    - IMPORT Directory Table
    - IMPORT Name Table
    - IMPORT Hints/Names & DLL Names
  - SECTION .data
  - SECTION .rsrc
  - SECTION .reloc
  - CERTIFICATE Table

pFile	Raw Data	Value
00000000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ.....
00000010	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00	.....@.....
00000020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000030	00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00	.....E8.....
00000040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	.....!..L.!Th
00000050	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno
00000060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
00000070	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00	mode...\$. ....
00000080	3C E2 60 D1 78 83 0E 82 78 83 0E 82 78 83 0E 82	<..`x...x...x...
00000090	66 D1 8A 82 59 83 0E 82 66 D1 9B 82 6B 83 0E 82	f...Y...f...k...
000000A0	5F 45 63 82 6D 83 0E 82 5F 45 75 82 71 83 0E 82	_Ec.m..._Eu.q...
000000B0	78 83 0F 82 01 83 0E 82 66 D1 8D 82 17 83 0E 82	x...f...
000000C0	66 D1 9A 82 79 83 0E 82 66 D1 9F 82 79 83 0E 82	f...y...f...y...
000000D0	52 69 63 68 78 83 0E 82 00 00 00 00 00 00 00	Richx.....
000000E0	00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00	.....PE..L...
000000F0	16 44 F7 55 00 00 00 00 00 00 00 00 E0 00 02 01	.D.U.....
00000100	0B 01 09 00 00 1E 01 00 00 BE 7A 06 00 00 00 00	.....z.....
00000110	63 BA 00 00 00 10 00 00 00 30 01 00 00 00 40 00	c.....0...@...
00000120	00 10 00 00 00 02 00 00 05 00 00 00 00 00 00	.....
00000130	05 00 00 00 00 00 00 00 00 00 7C 06 00 04 00	..... .....
00000140	58 97 7C 06 02 00 40 81 00 00 10 00 00 10 00	X. ...@.....
00000150	00 00 10 00 00 00 00 00 00 00 00 00 10 00 00	.....
00000160	00 00 00 00 00 00 00 00 74 4D 01 00 64 00 00	.....tM..d...
00000170	00 C0 01 00 48 CE 79 06 00 00 00 00 00 00 00	...H.y.....
00000180	00 9E 7B 06 18 19 00 00 00 90 7B 06 F8 0B 00	..{.....{.....
00000190	F0 31 01 00 1C 00 00 00 00 00 00 00 00 00 00	1

Viewing iTunesSetup.exerectory Table

# Example: Keylogger

- Imports User32.dll and uses the function **SetWindowsHookEx** which is a popular way keyloggers receive keyboard inputs
- It exports **LowLevelKeyboardProc** and **LowLevelMouseProc** to send the data elsewhere
- It uses **RegisterHotKey** to define a special keystroke like Ctrl+Shift+P to harvest the collected data

# Ex: A Packed Program

- Very few functions
- All you see is the unpacker

*Table 2-3. DLLs and Functions Imported from PackedProgram.exe*

Kernel32.dll	User32.dll
GetModuleHandleA	MessageBoxA
LoadLibraryA	
GetProcAddress	
ExitProcess	
VirtualAlloc	
VirtualFree	

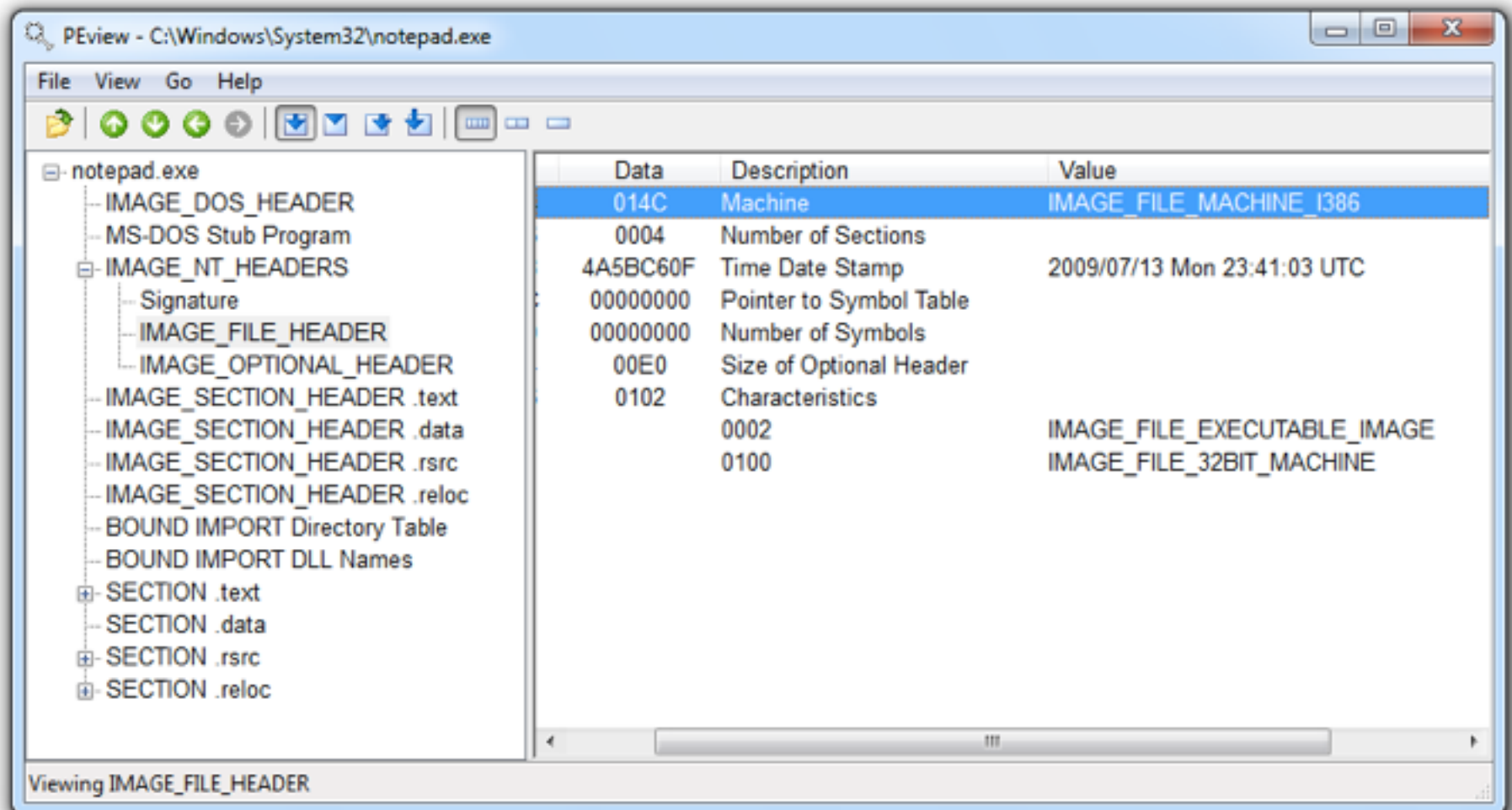
# The PE File Headers and Sections

# Important PE Sections

- **.text** -- instructions for the CPU to execute
- **.rdata** -- imports & exports
- **.data** - global data
- **.rsrc** - strings, icons, images, menus



# PEView (Link Ch 2e)





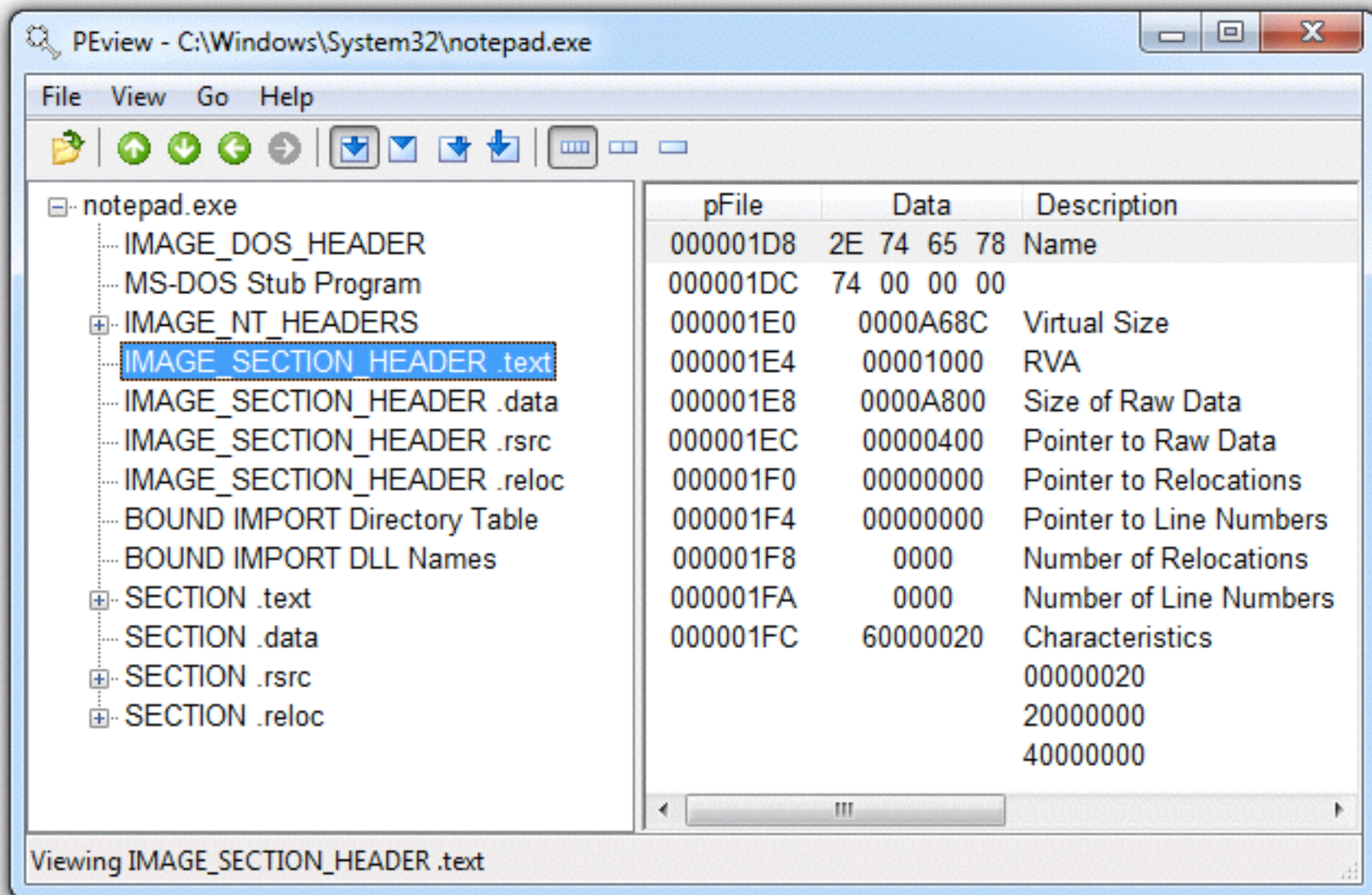
# Time Date Stamp

- Shows when this executable was compiled
- Older programs are more likely to be known to antivirus software
- But sometimes the date is wrong
  - All Delphi programs show June 19, 1992
  - Date can also be faked

# IMAGE\_SECTION\_HEADER

- Virtual Size - RAM
- Size of Raw Data - DISK
- For **.text** section, normally equal, or nearly equal
- Packed executables show Virtual Size much larger than Size of Raw Data for **.text** section

# Not Packed



*Table 2-6. Section Information for  
PackedProgram.exe*

<b>Name</b>	<b>Virtual size</b>	<b>Size of raw data</b>
.text	A000	0000
.data	3000	0000
.rdata	4000	0000
.rsrc	19000	3400
Dijfpds	20000	0000
.sdfuok	34000	3313F
Kijijl	1000	0200

# Resource Hacker

- Lets you browse the .rsrc section
- Strings, icons, and menus
- Link Ch 2f

# Resource Hacker

