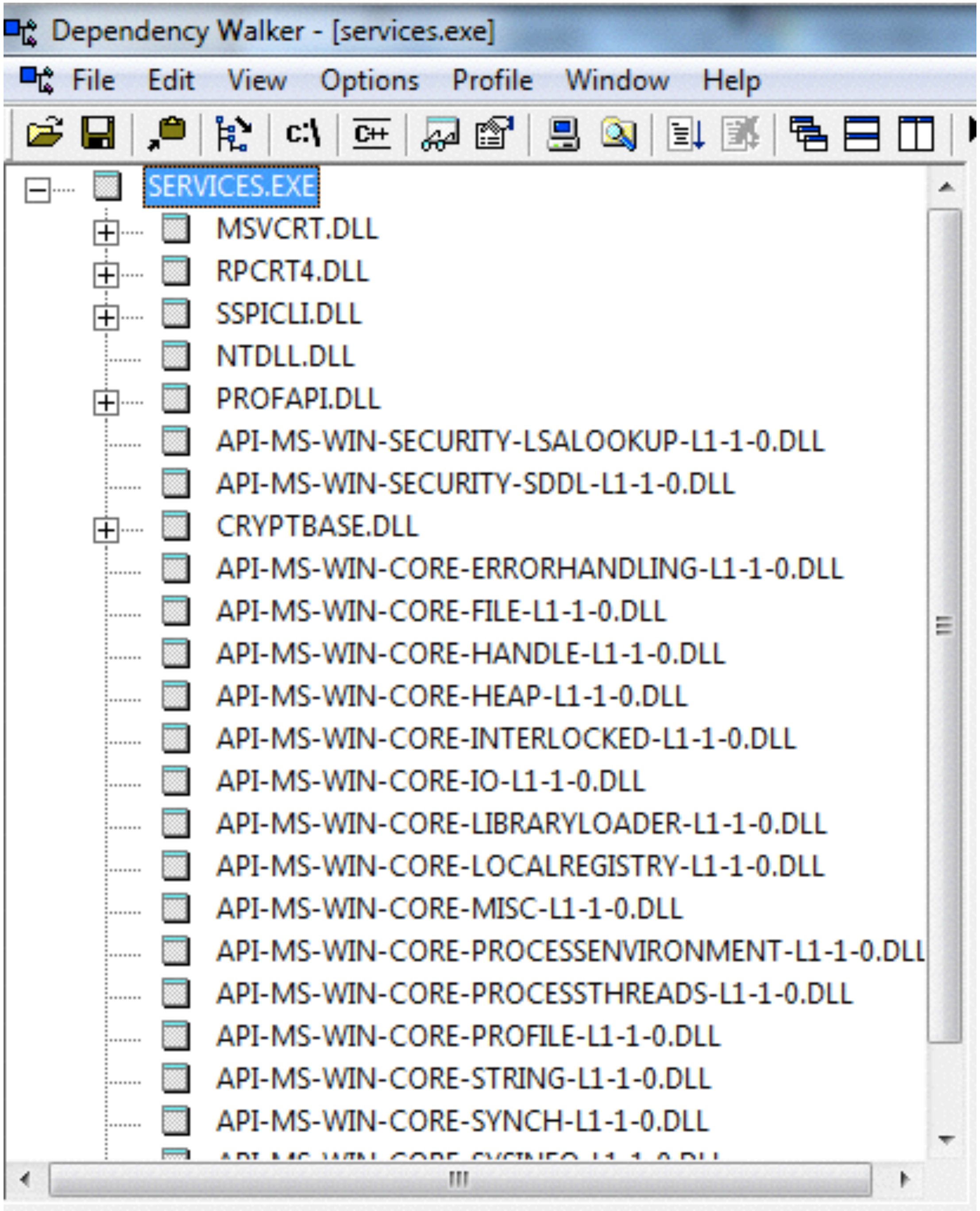
Dependency Walker

Shows Dynamically Linked Functions

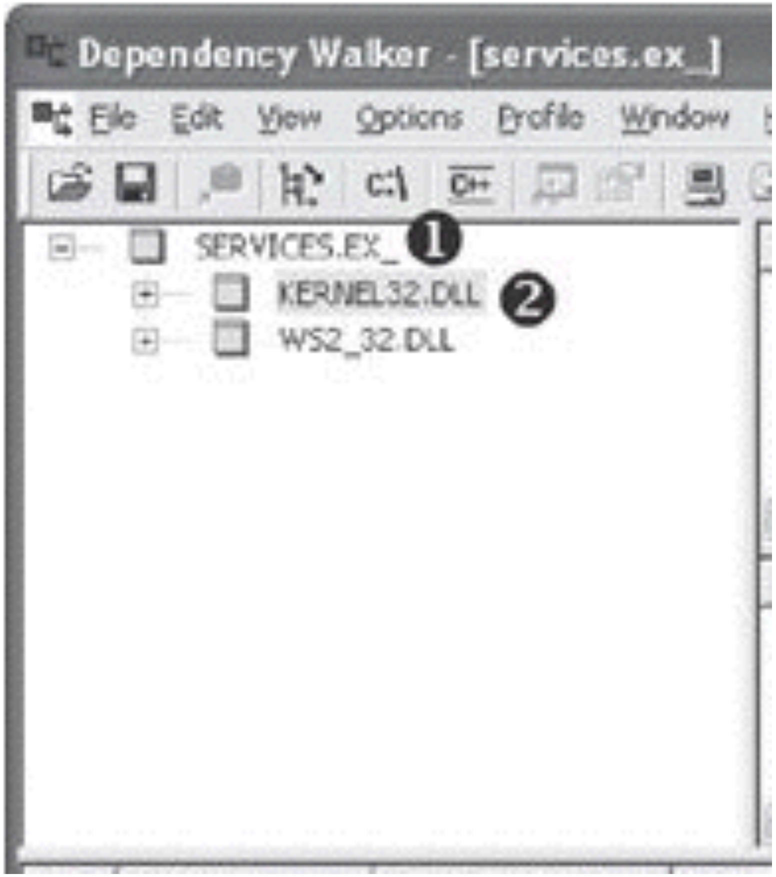
- Normal programs have a lot of DLLs
- Malware often has very few DLLs

Services.exe



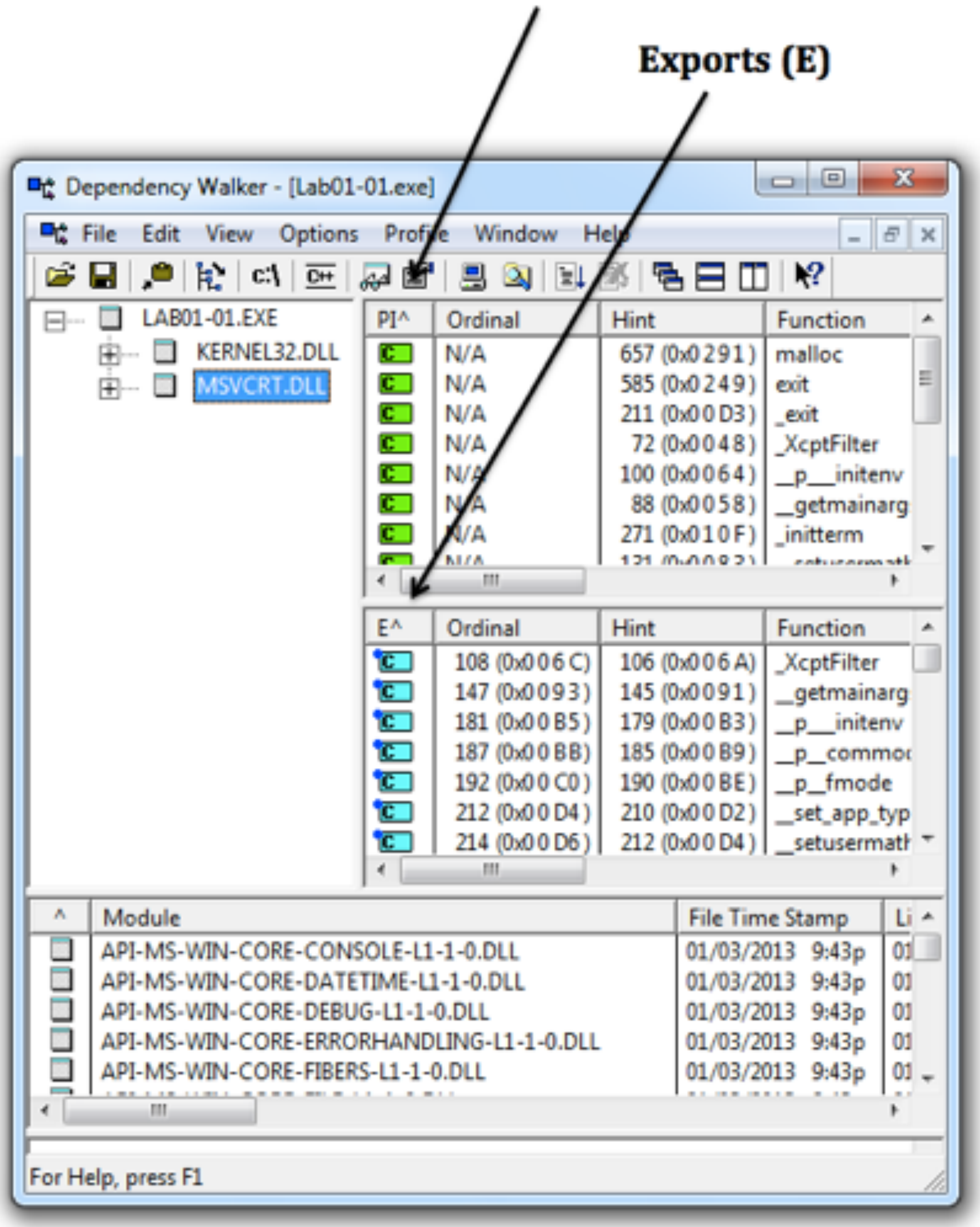
```
⊟ SERVICES.EXE
    ⊞ MSVCRT.DLL
    ⊞ RPCRT4.DLL
    ⊞ SSPICLI.DLL
      NTDLL.DLL
    ⊞ PROFAPI.DLL
      API-MS-WIN-SECURITY-LSALOOKUP-L1-1-0.DLL
      API-MS-WIN-SECURITY-SDDL-L1-1-0.DLL
    ⊞ CRYPTBASE.DLL
      API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL
      API-MS-WIN-CORE-FILE-L1-1-0.DLL
      API-MS-WIN-CORE-HANDLE-L1-1-0.DLL
      API-MS-WIN-CORE-HEAP-L1-1-0.DLL
      API-MS-WIN-CORE-INTERLOCKED-L1-1-0.DLL
      API-MS-WIN-CORE-IO-L1-1-0.DLL
      API-MS-WIN-CORE-LIBRARYLOADER-L1-1-0.DLL
      API-MS-WIN-CORE-LOCALREGISTRY-L1-1-0.DLL
      API-MS-WIN-CORE-MISC-L1-1-0.DLL
      API-MS-WIN-CORE-PROCESSENVIRONMENT-L1-1-0.DLL
      API-MS-WIN-CORE-PROCESSTHREADS-L1-1-0.DLL
      API-MS-WIN-CORE-PROFILE-L1-1-0.DLL
      API-MS-WIN-CORE-STRING-L1-1-0.DLL
      API-MS-WIN-CORE-SYNCH-L1-1-0.DLL
      API-MS-WIN-CORE-SYSINFO-L1-1-0.DLL
```

Services.ex_ (malware)



Dependency Walker - [services.ex_]
File Edit View Options Profile Window
SERVICES.EX_
1
KERNEL32.DLL
2
WS2_32.DLL

Imports & Exports in Dependency Walker



Dependency Walker - [Lab01-01.exe]
File Edit View Options Profile Window Help
LAB01-01.EXE
KERNEL32.DLL
MSVCRT.DLL
For Help, press F1

Imports (PI)

Exports (E)

PI^	Ordinal	Hint	Function
C	N/A	657 (0x0291)	malloc
C	N/A	585 (0x0249)	exit
C	N/A	211 (0x00D3)	_exit
C	N/A	72 (0x0048)	_XcptFilter
C	N/A	100 (0x0064)	__p__initenv
C	N/A	88 (0x0058)	__getmainarg
C	N/A	271 (0x010F)	_initterm
C	N/A	131 (0x0083)	__setusermatl

E^	Ordinal	Hint	Function
C	108 (0x006C)	106 (0x006A)	_XcptFilter
C	147 (0x0093)	145 (0x0091)	__getmainarg
C	181 (0x00B5)	179 (0x00B3)	__p__initenv
C	187 (0x00BB)	185 (0x00B9)	__p__commod
C	192 (0x00C0)	190 (0x00BE)	__p__fmode
C	212 (0x00D4)	210 (0x00D2)	__set_app_typ
C	214 (0x00D6)	212 (0x00D4)	__setusermatl

^	Module	File Time Stamp	Li
□	API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	01/03/2013 9:43p	01
□	API-MS-WIN-CORE-DATETIME-L1-1-0.DLL	01/03/2013 9:43p	01
□	API-MS-WIN-CORE-DEBUG-L1-1-0.DLL	01/03/2013 9:43p	01
□	API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL	01/03/2013 9:43p	01
□	API-MS-WIN-CORE-FIBERS-L1-1-0.DLL	01/03/2013 9:43p	01

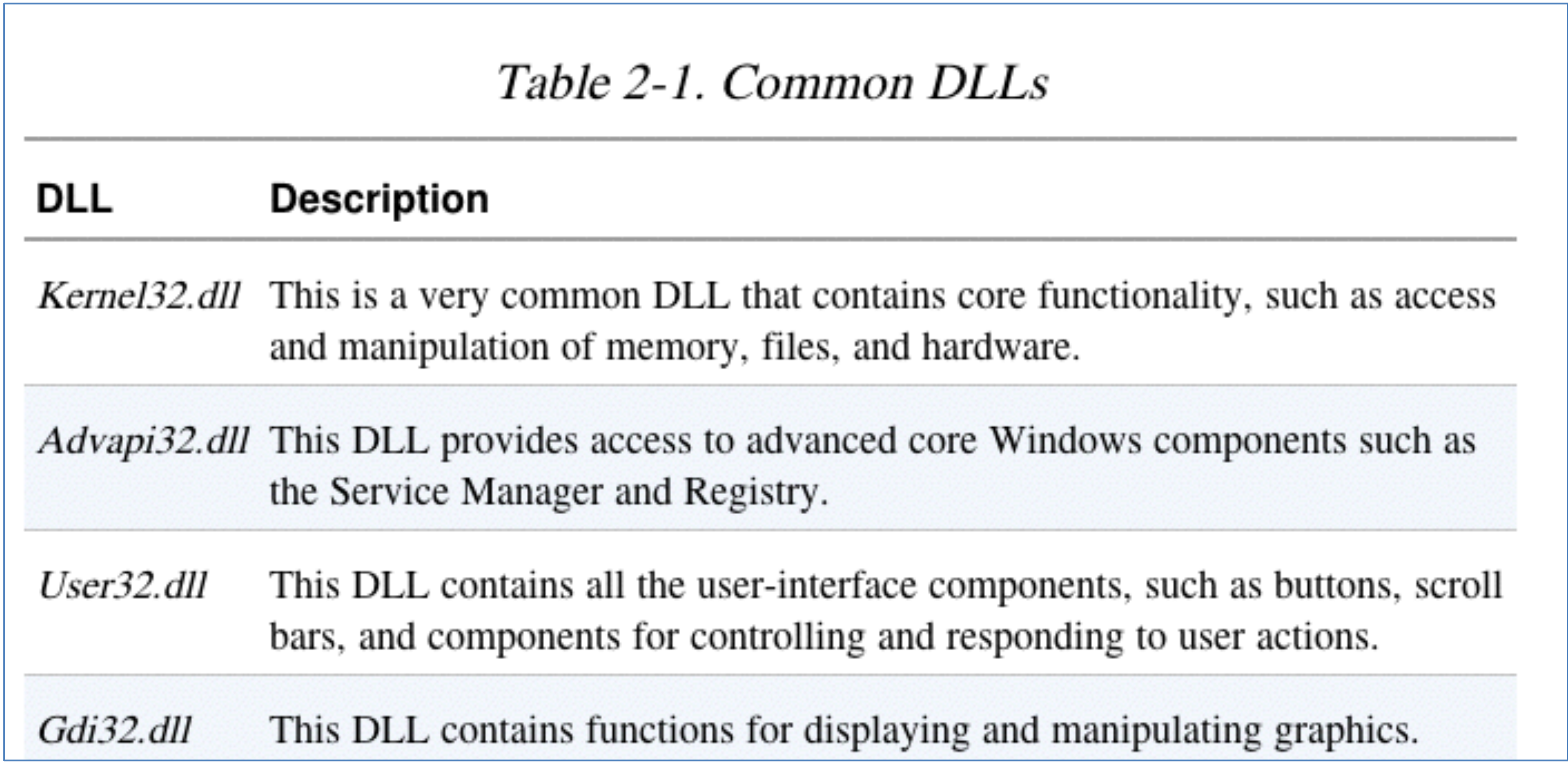
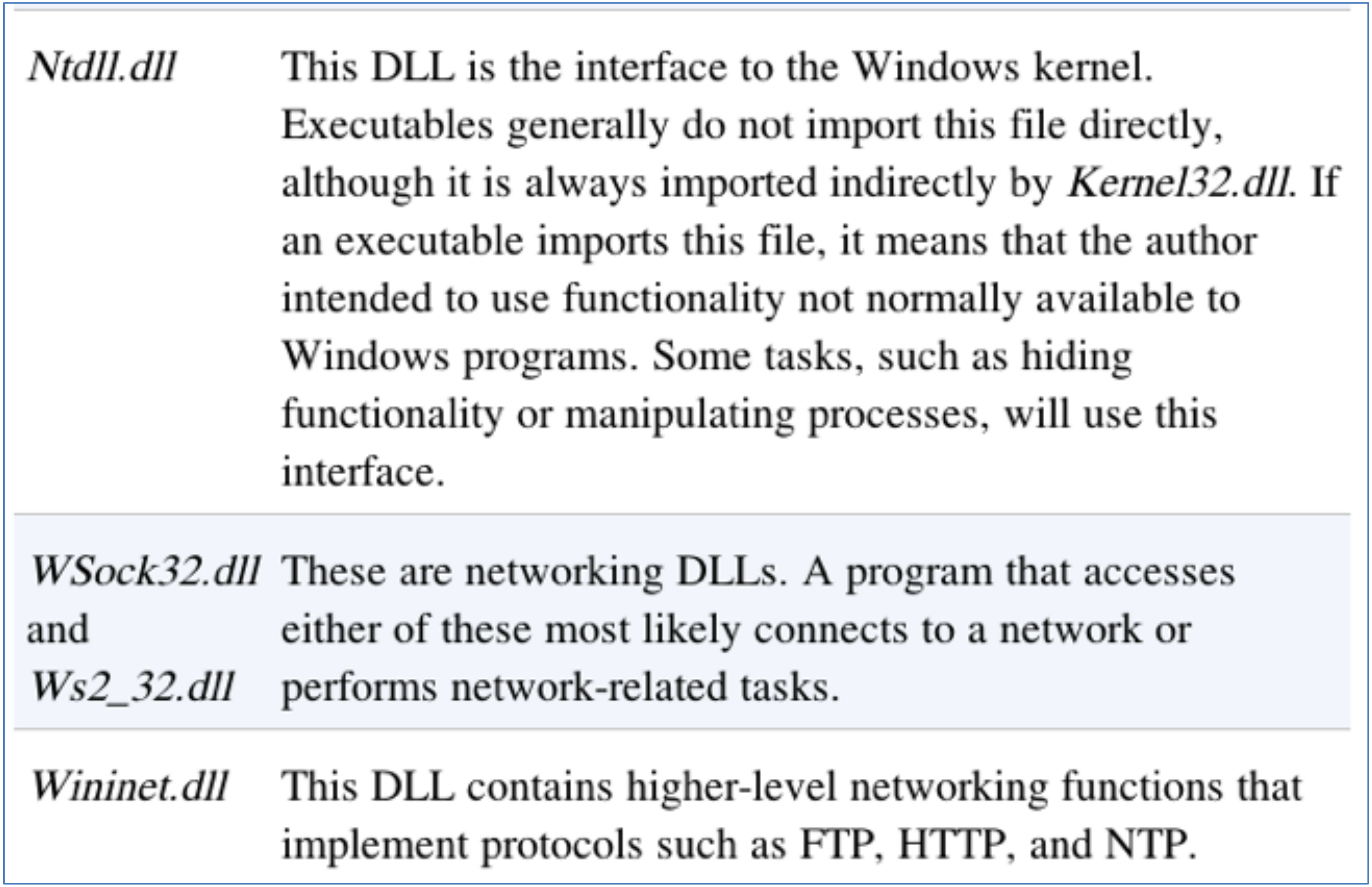


Table 2-1. Common DLLs

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

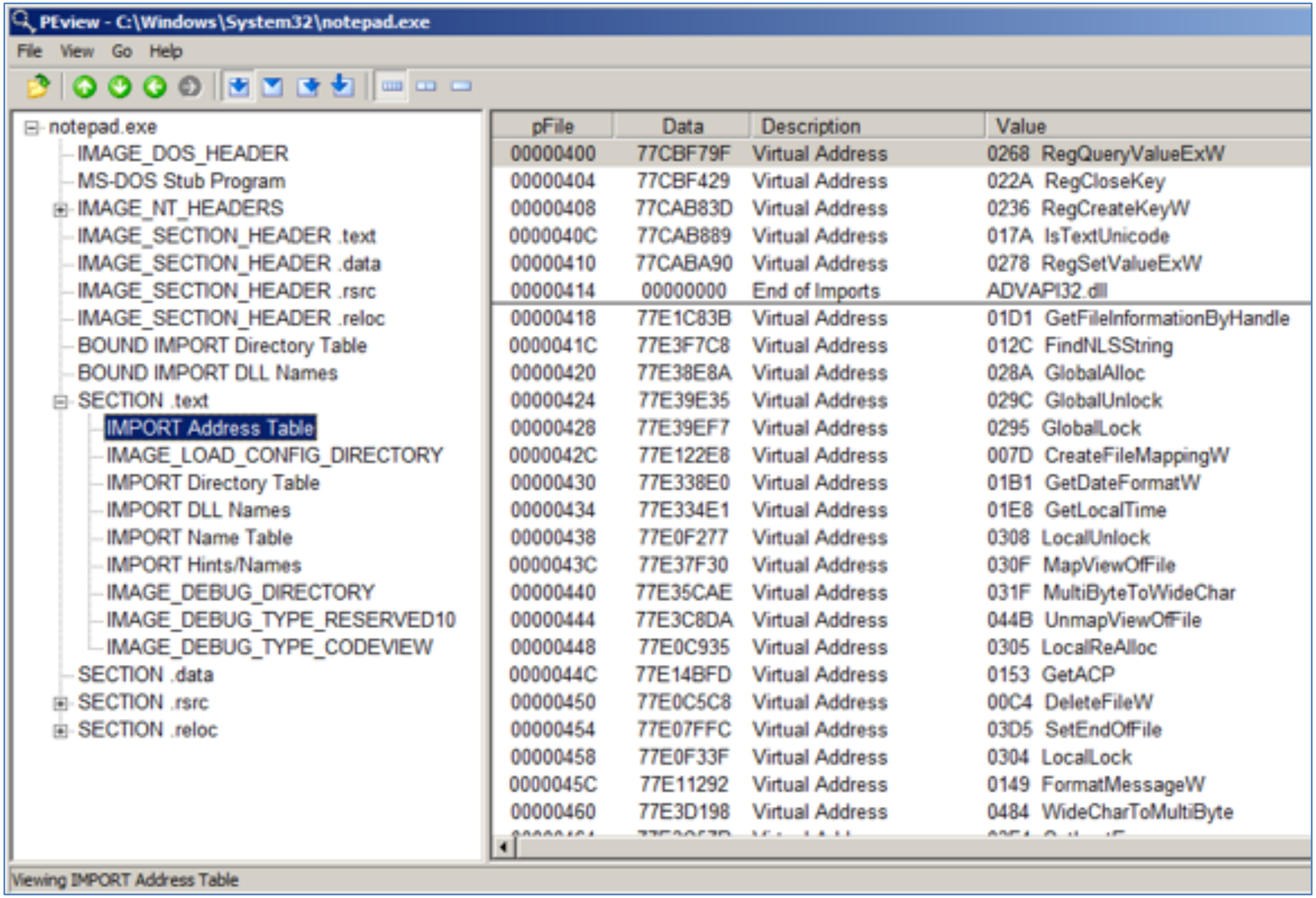
- DLLs **export** functions
- EXEs **import** functions
- Both exports and imports are listed in the PE header

FUNCTION NAMING CONVENTIONS

When evaluating unfamiliar Windows functions, a few naming conventions are worth noting because they come up often and might confuse you if you don't recognize them. For example, you will often encounter function names with an `Ex` suffix, such as `CreateWindowEx`. When Microsoft updates a function and the new function is incompatible with the old one, Microsoft continues to support the old function. The new function is given the same name as the old function, with an added `Ex` suffix. Functions that have been significantly updated twice have two `Ex` suffixes in their names.

Many functions that take strings as parameters include an `A` or a `W` at the end of their names, such as `CreateDirectoryW`. This letter does *not* appear in the documentation for the function; it simply indicates that the function accepts a string parameter and that there are two different versions of the function: one for ASCII strings and one for wide character strings. Remember to drop the trailing `A` or `W` when searching for the function in the Microsoft documentation.

Notepad.exe

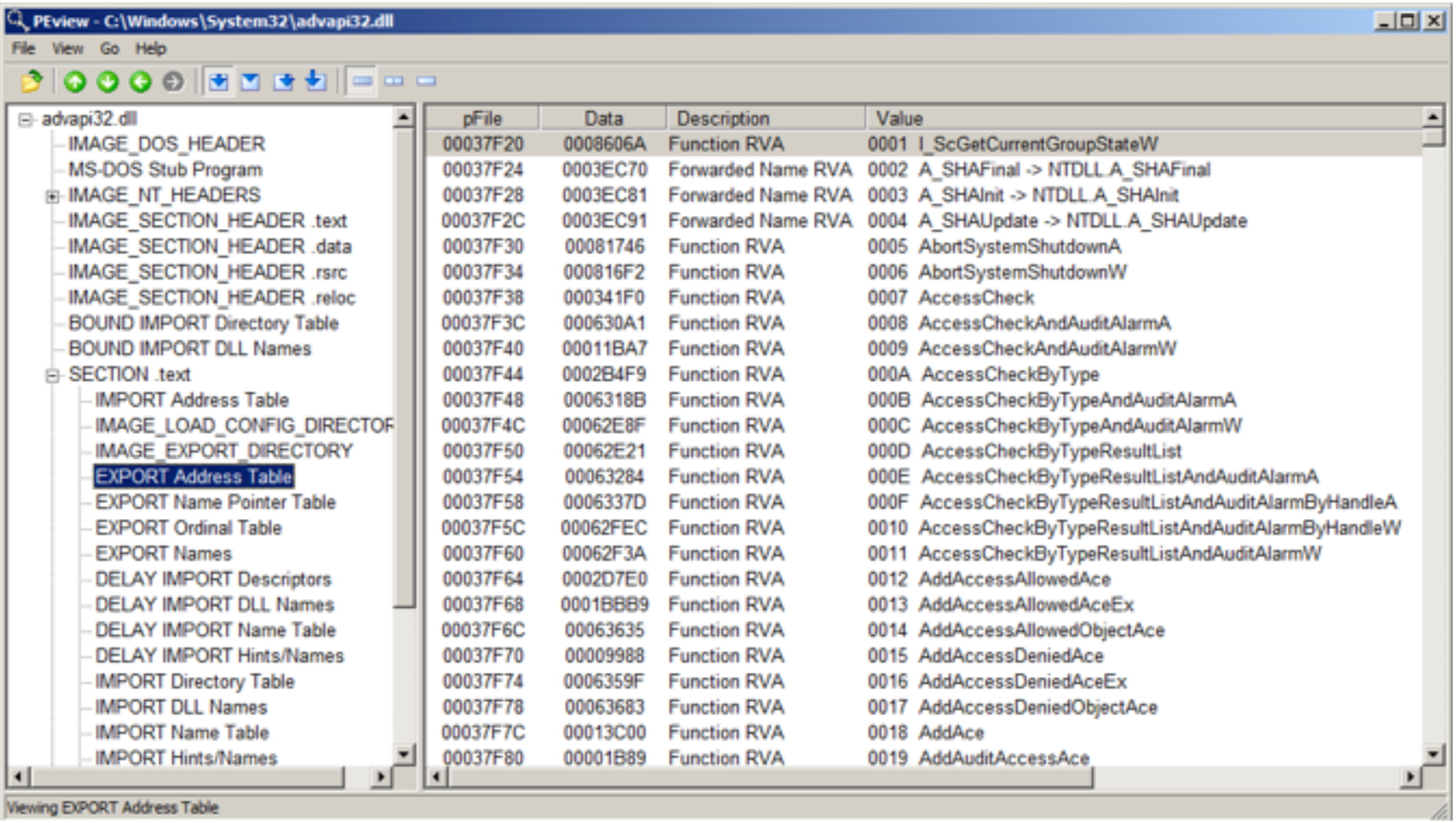


```
⊟ notepad.exe
   IMAGE_DOS_HEADER
   MS-DOS Stub Program
 ⊞ IMAGE_NT_HEADERS
   IMAGE_SECTION_HEADER .text
   IMAGE_SECTION_HEADER .data
   IMAGE_SECTION_HEADER .rsrc
   IMAGE_SECTION_HEADER .reloc
   BOUND IMPORT Directory Table
   BOUND IMPORT DLL Names
 ⊟ SECTION .text
     IMPORT Address Table
     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

Viewing IMPORT Address Table

Advapi32.dll



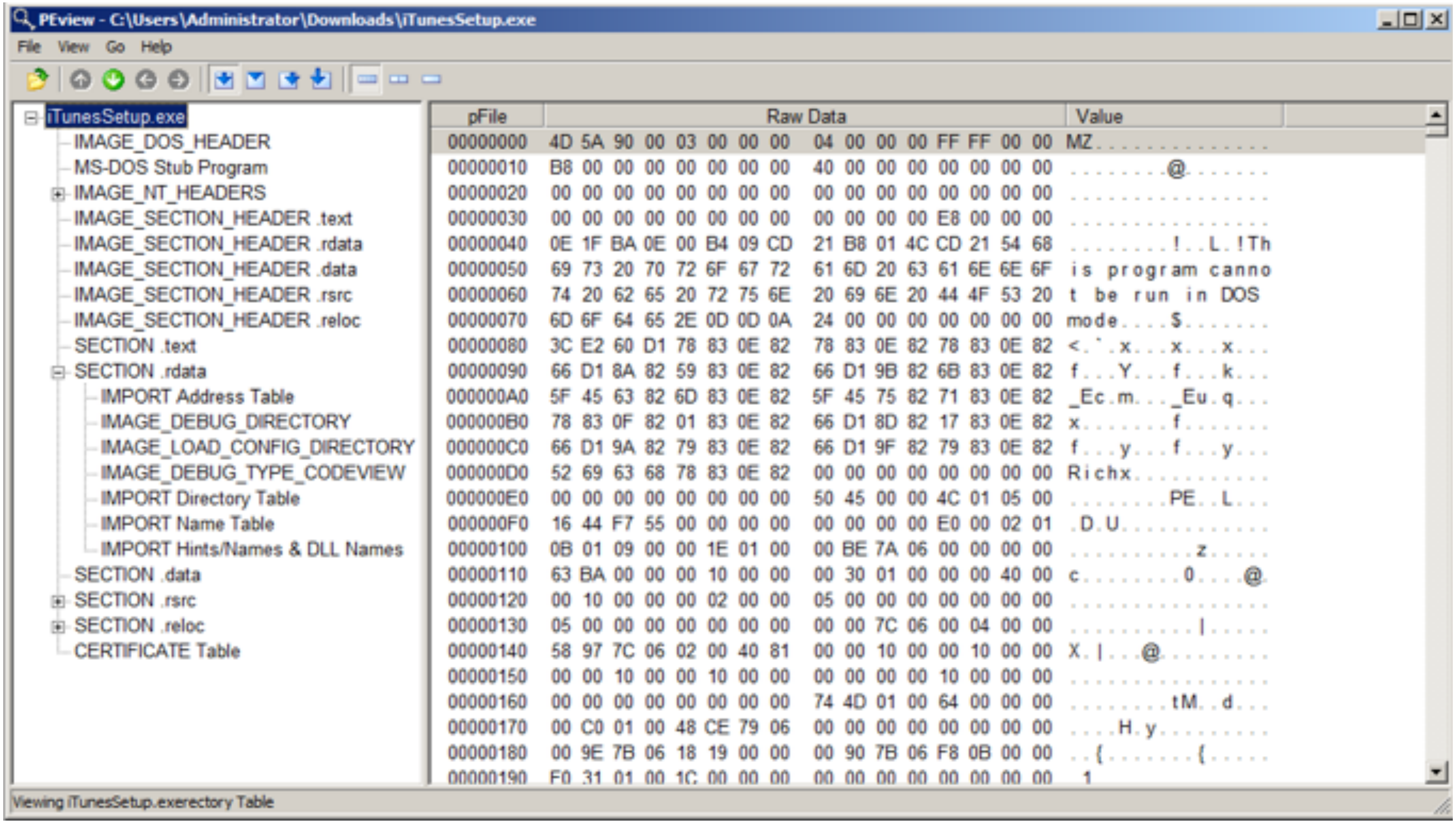
PEview - C:\Windows\System32\advapi32.dll

- 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_DIRECTOR
    - 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



```
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 00  ........@.......
00000020  00 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 00  ................
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 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 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 00  ................
00000130  05 00 00 00 00 00 00 00  00 00 7C 06 00 04 00 00  ..........|.....
00000140  58 97 7C 06 02 00 40 81  00 00 10 00 00 10 00 00  X.|...@.........
00000150  00 00 10 00 00 10 00 00  00 00 00 00 10 00 00 00  ................
00000160  00 00 00 00 00 00 00 00  74 4D 01 00 64 00 00 00  ........tM..d...
00000170  00 C0 01 00 48 CE 79 06  00 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 00  ..{.......{.....
00000190  F0 31 01 00 1C 00 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

Kernel32.dll

CreateDirectoryW

CreateFileW

CreateThread

DeleteFileW

ExitProcess

FindClose

FindFirstFileW

FindNextFileW

GetCommandLineW

GetCurrentProcess

GetCurrentThread

GetFileSize

GetModuleHandleW

GetProcessHeap

GetShortPathNameW

HeapAlloc

HeapFree

IsDebuggerPresent

MapViewOfFile

OpenProcess

ReadFile

SetFilePointer

WriteFile

User32.dll

BeginDeferWindowPos

CallNextHookEx

CreateDialogParamW

CreateWindowExW

DefWindowProcW

DialogBoxParamW

EndDialog

GetMessageW

GetSystemMetrics

GetWindowLongW

GetWindowRect

GetWindowTextW

InvalidateRect

IsDlgButtonChecked

IsWindowEnabled

LoadCursorW

LoadIconW

LoadMenuW

MapVirtualKeyW

MapWindowPoints

MessageBoxW

RegisterClassExW

RegisterHotKey

SendMessageA

SetClipboardData

SetDlgItemTextW

SetWindowTextW

SetWindowsHookExW

User32.dll (continued)

ShowWindow

ToUnicodeEx

TrackPopupMenu

TrackPopupMenuEx

TranslateMessage

UnhookWindowsHookEx

UnregisterClassW

UnregisterHotKey

GDI32.dll

GetStockObject

SetBkMode

SetTextColor

Shell32.dll

CommandLineToArgvW

SHChangeNotify

SHGetFolderPathW

ShellExecuteExW

ShellExecuteW

Advapi32.dll

RegCloseKey

RegDeleteValueW

RegOpenCurrentUser

RegOpenKeyExW

RegQueryValueExW

RegSetValueExW

Ex: A Packed Program

- Very few functions
- All you see is the unpacker

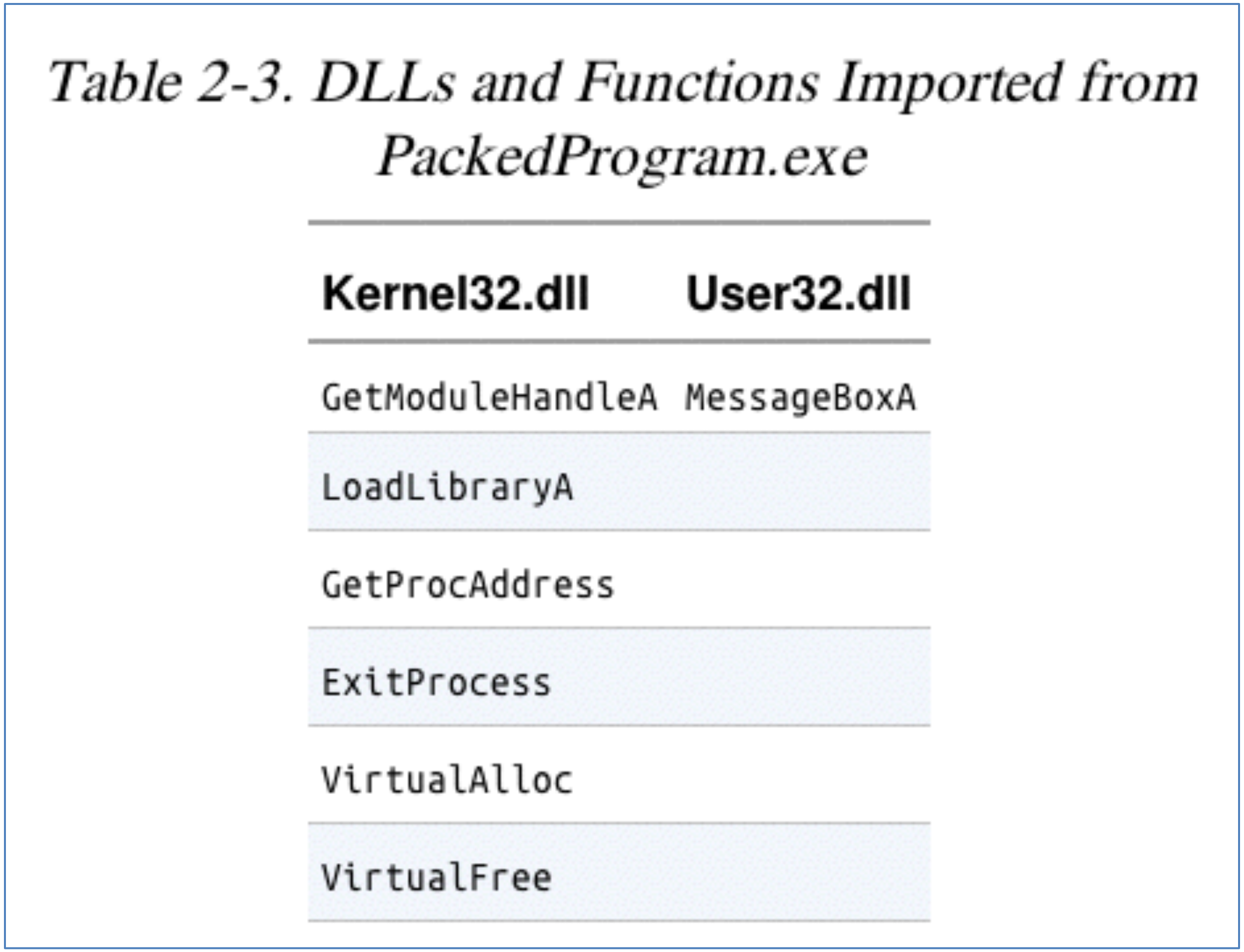


Table 2-3. DLLs and Functions Imported from PackedProgram.exe

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

The PE File Headers and Sections

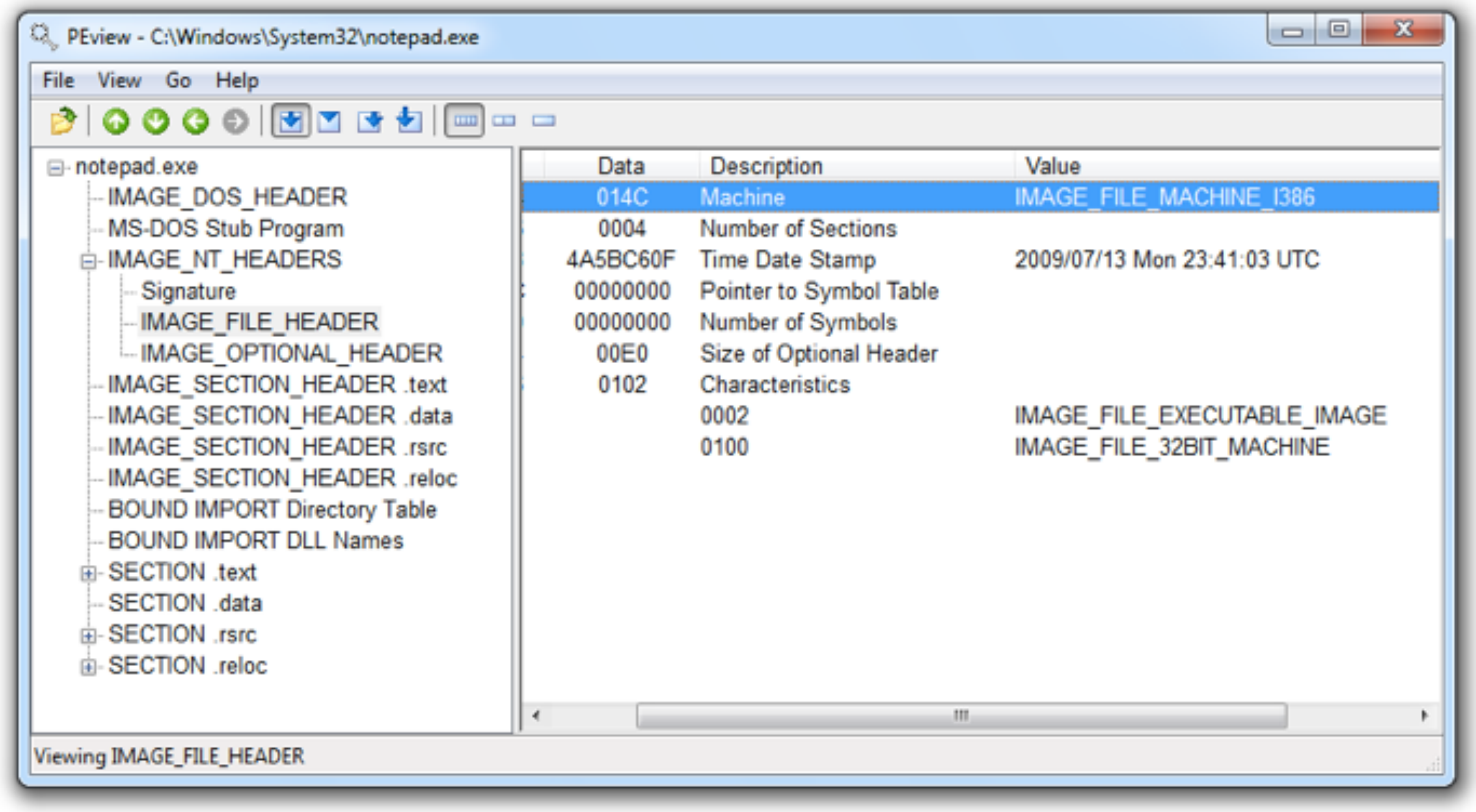
Important PE Sections

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

Table 1-4: Sections of a PE File for a Windows Executable

Executable	Description
`.text`	Contains the executable code
`.rdata`	Holds read-only data that is globally accessible within the program
`.data`	Stores global data accessed throughout the program
`.idata`	Sometimes present and stores the import function information; if this section is not present, the import function information is stored in the `.rdata` section
`.edata`	Sometimes present and stores the export function information; if this section is not present, the export function information is stored in the `.rdata` section
`.pdata`	Present only in 64-bit executables and stores exception-handling information
`.rsrc`	Stores resources needed by the executable
`.reloc`	Contains information for relocation of library files

PEView (Link Ch 2e)



```
notepad.exe
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
    Signature
    IMAGE_FILE_HEADER
    IMAGE_OPTIONAL_HEADER
  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
  SECTION .data
  SECTION .rsrc
  SECTION .reloc
```

Data	Description	Value
014C	Machine	IMAGE_FILE_MACHINE_I386
0004	Number of Sections	
4A5BC60F	Time Date Stamp	2009/07/13 Mon 23:41:03 UTC
00000000	Pointer to Symbol Table	
00000000	Number of Symbols	
00E0	Size of Optional Header	
0102	Characteristics	
	0002	IMAGE_FILE_EXECUTABLE_IMAGE
	0100	IMAGE_FILE_32BIT_MACHINE

Viewing IMAGE_FILE_HEADER

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