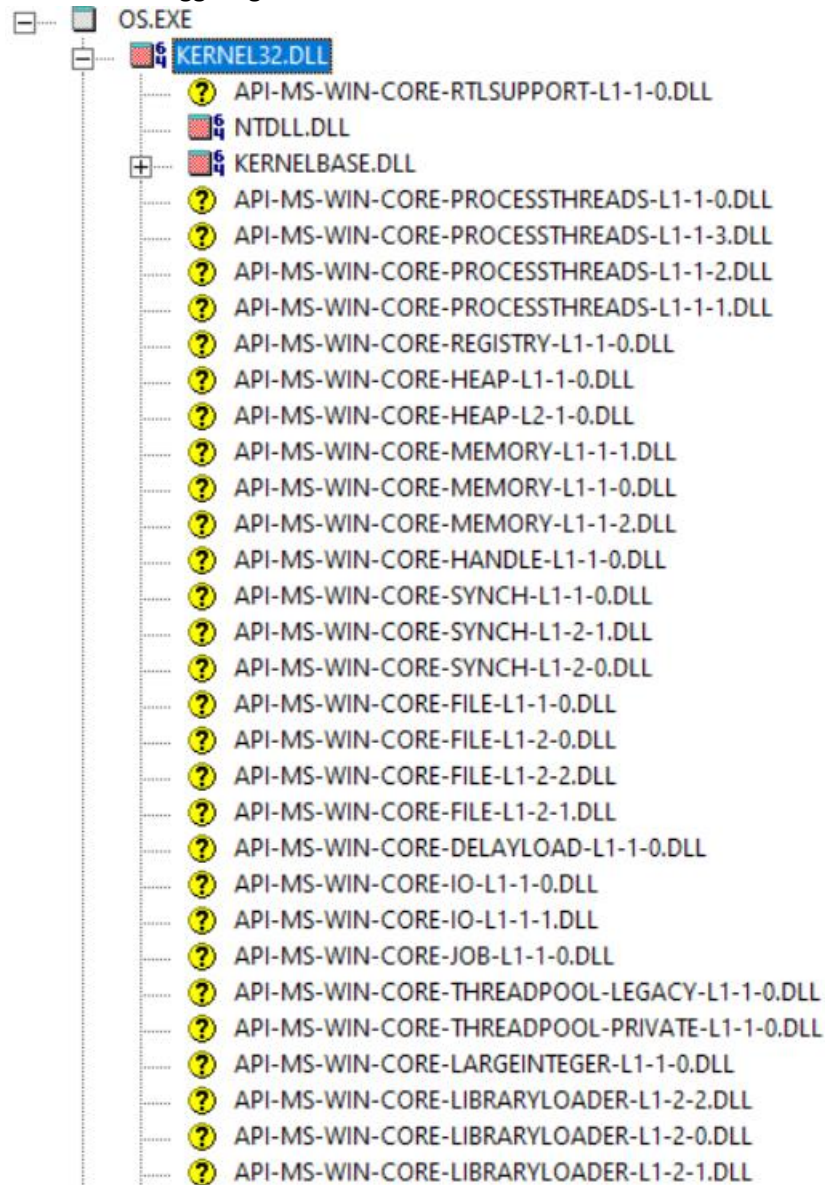


1. API hívások a kernel32.dll-ből

PI	Ordinal ^	Hint	Function	Entry Point
	N/A	0 (0x0000)	RtlAddFunctionTable	Not Bound
	N/A	2 (0x0002)	RtlCaptureContext	Not Bound
	N/A	4 (0x0004)	RtlCaptureStackBackTrace	Not Bound
	N/A	5 (0x0005)	RtlCompareMemory	Not Bound
	N/A	6 (0x0006)	RtlDeleteFunctionTable	Not Bound
	N/A	9 (0x0009)	RtlInstallFunctionTableCallback	Not Bound
	N/A	10 (0x000A)	RtlLookupFunctionEntry	Not Bound
	N/A	11 (0x000B)	RtlPcToFileHeader	Not Bound
	N/A	12 (0x000C)	RtlRaiseException	Not Bound
	N/A	13 (0x000D)	RtlRestoreContext	Not Bound
	N/A	14 (0x000E)	RtlUnwind	Not Bound
	N/A	15 (0x000F)	RtlUnwindEx	Not Bound
	N/A	16 (0x0010)	RtlVirtualUnwind	Not Bound

2. Kernel32.dll függőségei



3.

- a. NTDLL.dll NT kernel funkciókat tartalmaz. C:\windows\system32 -ben vagy C:\i386 -ban található.
- b. Függvényhívások

Dependency Walker - [ntdll.dll]

File Edit View Options Profile Window Help

NTDLL.DLL

PI	Ordinal ^	Hint	Function	Entry Point
E	Ordinal ^	Hint	Function	Entry Point
8 (0x0008)	N/A	N/A		0x0007E6B0
9 (0x0009)	0 (0x0000)	A_SHAFinal		0x0005C290
10 (0x000A)	1 (0x0001)	A_SHAInit		0x0005D0C0
11 (0x000B)	2 (0x0002)	A_SHAUpdate		0x0005D100
12 (0x000C)	3 (0x0003)	AlpcAdjustCompletionListConcurrencyCount		0x000E0700
13 (0x000D)	4 (0x0004)	AlpcFreeCompletionListMessage		0x0006F920
14 (0x000E)	5 (0x0005)	AlpcGetCompletionListLastMessageInformation		0x000E0730
15 (0x000F)	6 (0x0006)	AlpcGetCompletionListMessageAttributes		0x000E0750
16 (0x0010)	7 (0x0007)	AlpcGetHeaderSize		0x0006F650
17 (0x0011)	8 (0x0008)	AlpcGetMessageStatus		0x000E0770
18 (0x0012)	9 (0x0009)	AlpcGetMessageFromCompletionList		0x0006F100
19 (0x0013)	10 (0x000A)	AlpcGetOutstandingCompletionListMessageCount		0x000856C0
20 (0x0014)	11 (0x000B)	AlpcInitializeMessageAttribute		0x0006F5B0
21 (0x0015)	12 (0x000C)	AlpcMaxAllowedMessageLength		0x000844E0
22 (0x0016)	13 (0x000D)	AlpcRegisterCompletionList		0x00085540
23 (0x0017)	14 (0x000E)	AlpcRegisterCompletionListWorkerThread		0x00074EB0
24 (0x0018)	15 (0x000F)	AlpcRundownCompletionList		0x00085680
25 (0x0019)	16 (0x0010)	AlpcUnregisterCompletionList		0x000856A0
26 (0x001A)	17 (0x0011)	AlpcUnregisterCompletionListWorkerThread		0x00074E50
27 (0x001B)	18 (0x0012)	ApiSetQueryApiSetPresence		0x000768B0
28 (0x001C)	19 (0x0013)	ApiSetQueryApiSetPresenceEx		0x0003C150
29 (0x001D)	20 (0x0014)	CsrAllocateCaptureBuffer		0x00071200
30 (0x001E)	21 (0x0015)	CsrAllocateMessagePointer		0x00071180
31 (0x001F)	22 (0x0016)	CsrCaptureMessageBuffer		0x00070780
32 (0x0020)	23 (0x0017)	CsrCaptureMessageMultiUnicodeStringsInPlace		0x00070FF0
33 (0x0021)	24 (0x0018)	CsrCaptureMessageString		0x00071100
34 (0x0022)	25 (0x0019)	CsrCaptureTimeout		0x000CB350
35 (0x0023)	26 (0x001A)	CsrClientCallServer		0x00070E50
36 (0x0024)	27 (0x001B)	CsrClientConnectToServer		0x000707E0
37 (0x0025)	28 (0x001C)	CsrFreeCaptureBuffer		0x00070E20

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size	Load Order	File Ver	Product Ver	Image Ver
NTDLL.DLL	2000-05-20 12:00:00	2000-05-20 12:00:00	0x00000000	0x00000000	0x00000000	0x00000000	32	0	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000

For Help, press F1

- c. Az NT API vezérli a windows fájlrendszerét, rendszerhívásokat, futásidejű könyvtárakat és még rengeteg minden mást.