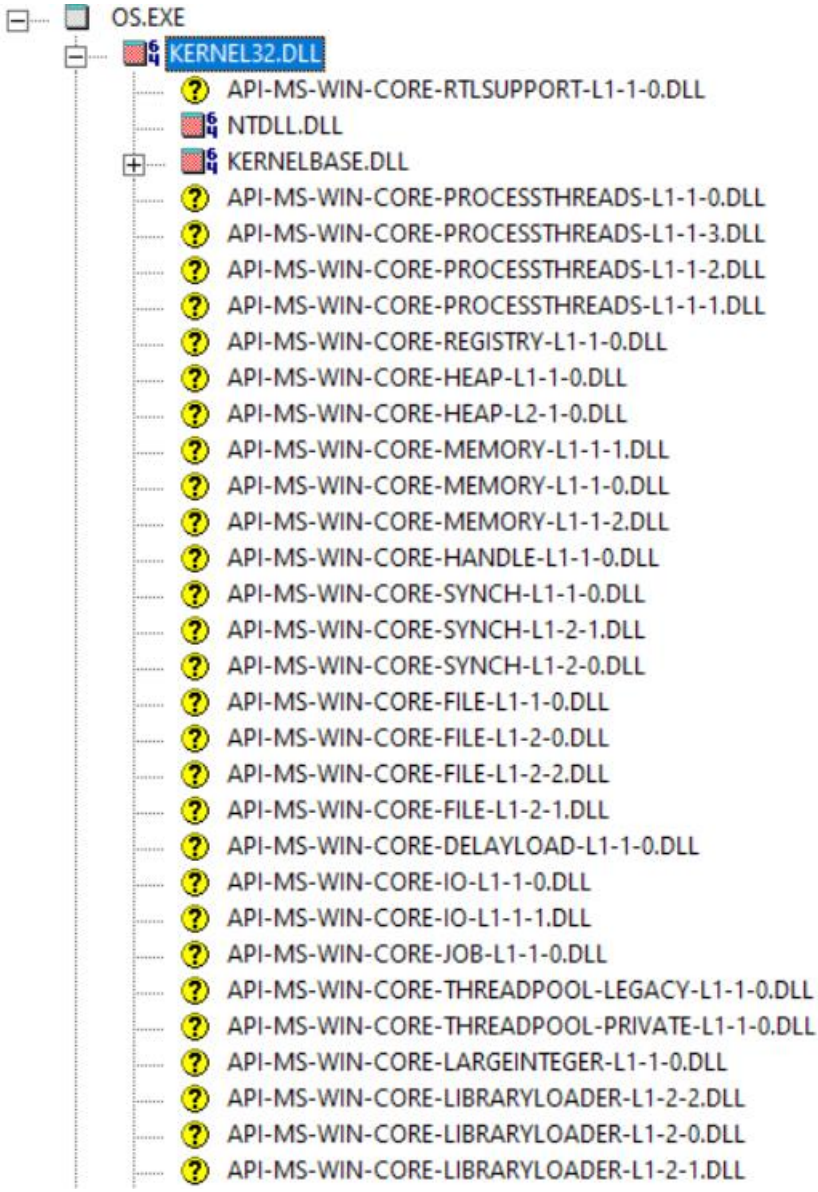
1. API hívások a kernel32.dll-ből

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

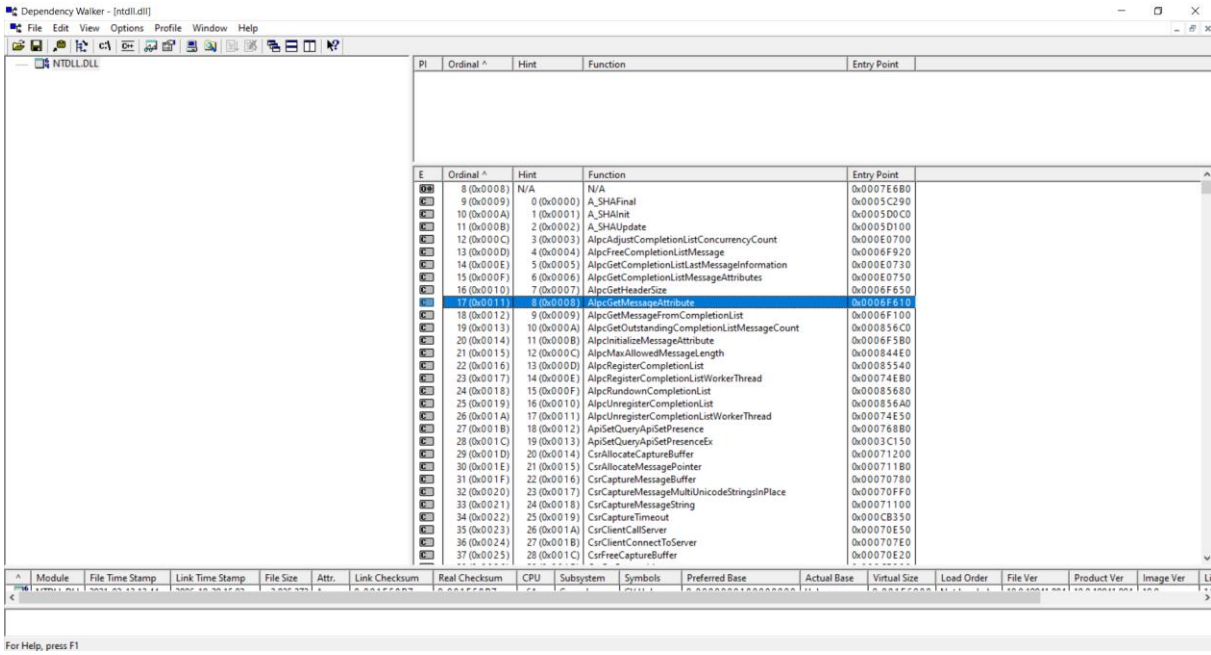
2. Kernel32.dll függőségei



3.

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

b. Függvényhívások



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