

Operációs Rendszerek Gyakorlat 4.A 0. Feladat, Dependency Walker

1. Vizsgálja meg, hogy a *neptunkod.exe* milyen API hívásokat használ a kernel32.dll-ből (Win alrendszer DLL)!

Dependency Walker - [C:\WINDOWS\...]									
File Edit View Options Profile Windows Help									
CONSOLE									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									
C:\WINDOWS\...									

3. Keresse meg NTDLL.DLL-t! Mi ennek a szerepe? Vizsgálja meg az exportált függvényeket, milyen információkat kap az NT API-ról!

Az egyes objektumok közötti kapcsolattartás az LPC mechanizmuson keresztül történik, így minden felhasználói objektum az NTDLL.DLL-en keresztül éri el a környezetét.

Ha egy hívás érkezik, ellenőrzi a hívás paramétereit, és megvalósítja a user–kernel módváltást

COOKSI.EXE					P1	Ordinal ^	Hint	Function	Entry Point
KERNEL32.DLL					18	(0x0012)		CsrAllocateCaptureBuffer	Not Bound
API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL					19	(0x0013)		CsrAllocateMessagePointer	Not Bound
NTDLL.DLL					24	(0x0018)		CsrClientCallServer	Not Bound
KERNELBASE.DLL					26	(0x001A)		CsrFreeCaptureBuffer	Not Bound
NTDLL.DLL					27	(0x001B)		CsrGetProcessId	Not Bound
API-MS-WIN-CORE-PROCESS-THREADS-L1-1-0.DLL					30	(0x001E)		CsrVerifyRegion	Not Bound
API-MS-WIN-CORE-HEAP-L1-1-0.DLL					32	(0x0020)		DbgPrint	Not Bound
API-MS-WIN-CORE-MEMORY-L1-1-0.DLL					33	(0x0021)		DbgPrintEx	Not Bound
API-MS-WIN-CORE-HANDLE-L1-1-0.DLL					38	(0x0026)		DbgUiConnectToDbg	Not Bound
API-MS-WIN-CORE-SYNCH-L1-1-0.DLL					39	(0x0027)		DbgUiContinue	Not Bound
API-MS-WIN-CORE-FILE-L1-1-0.DLL					40	(0x0028)		DbgUiConvertStateChangeStructure	Not Bound
API-MS-WIN-CORE-IO-L1-1-0.DLL					41	(0x0029)		DbgUiDebugActiveProcess	Not Bound
API-MS-WIN-CORE-THREADPOOL-L1-1-0.DLL					42	(0x002A)		DbgUiGetThreadDebugObject	Not Bound
API-MS-WIN-CORE-LIBRARYLOADER-L1-1-0.DLL					43	(0x002B)		DbgUiIssueRemoteBreakin	Not Bound
API-MS-WIN-CORE-NAMEDPIPE-L1-1-0.DLL					46	(0x002E)		DbgUiStopDebugging	Not Bound
API-MS-WIN-CORE-MISC-L1-1-0.DLL					47	(0x002F)		DbgUiWaitStateChange	Not Bound
API-MS-WIN-CORE-SYSINFO-L1-1-0.DLL					53	(0x0035)		EtwEventEnabled	Not Bound
API-MS-WIN-CORE-LOCALIZATION-L1-1-0.DLL									
API-MS-WIN-CORE-PROCESS-ENVIRONMENT-L1-1-0.DLL					E	Ordinal ^	Hint	Function	Entry Point
API-MS-WIN-CORE-STRING-L1-1-0.DLL					1	(0x0001)	N/A	N/A	0x000ABFEC
API-MS-WIN-CORE-DEBUG-L1-1-0.DLL					2	(0x0002)	N/A	N/A	0x000AC088
API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL					3	(0x0003)	N/A	N/A	0x000ABBB1
API-MS-WIN-CORE-FIBERS-L1-1-0.DLL					4	(0x0004)	N/A	N/A	0x000ABD45
API-MS-WIN-CORE-UTIL-L1-1-0.DLL					5	(0x0005)	N/A	N/A	0x000AB68D
API-MS-WIN-CORE-PROFILE-L1-1-0.DLL					6	(0x0006)	N/A	N/A	0x000AB981
API-MS-WIN-CORE-SECURITY-BASE-L1-1-0.DLL					7	(0x0007)	N/A	N/A	0x000ABF8D
MSVCRT.DLL					8	(0x0008)	N/A	N/A	0x000740D4
					9	(0x0009)	606 (0x025E)	RtlActivateActivationContextUnsafeFast	0x00022201
					10	(0x000A)	741 (0x02E5)	RtlDeactivateActivationContextUnsafeFast	0x00022169
					11	(0x000B)	981 (0x03D5)	RtlInterlockedPushListSList	0x000327F0
					12	(0x000C)	1237 (0x04D5)	RtlUlongByteSwap	0x0007CD60
					13	(0x000D)	1238 (0x04D6)	RtlUlongByteSwap	0x0007CD70
					14	(0x000E)	1275 (0x04FB)	RtlUshortByteSwap	0x0007CD50
					15	(0x000F)	89 (0x0059)	ExpInterlockedPopEntrySListEnd	0x000327B3
					16	(0x0010)	90 (0x005A)	ExpInterlockedPopEntrySListFault	0x000327B1