

Dependency Walker - [XUE9MH.exe]

File Edit View Options Profile Window Help

XUE9MH.EXE
 -> KERNEL32.DLL
 -> API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
 -> NTDLL.DLL
 -> API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL
 -> NTDLL.DLL
 -> KERNELBASE.DLL
 -> NTDLL.DLL
 -> API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
 -> EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL
 -> EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL
 -> EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL
 -> EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL
 -> EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL
 -> EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL
 -> EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL
 -> EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-1.DLL

PI	Ordinal ^	Hint	Function	Entry Point
0	N/A	N/A	RtlCaptureContext	Not Bound
1	N/A	N/A	RtlUnwind	Not Bound
2	N/A	N/A	RtlCaptureStackBackTrace	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
8	8 (0x0008)	918 (0x0396)	RtlDispatchAPC	0x0002C0A0
9	9 (0x0009)	711 (0x02C7)	RtlActivateActivationContextUnsafeFast	0x0003FF90
10	10 (0x000A)	876 (0x036C)	RtlDeactivateActivationContextUnsafeFast	0x00043170
11	11 (0x000B)	1166 (0x048E)	RtlInterlockedPushListSList	0x000BE880
12	12 (0x000C)	1508 (0x05E4)	RtlUlongByteSwap	0x000BE920
13	13 (0x000D)	1509 (0x05E5)	RtlUlonglongByteSwap	0x000BE930
14	14 (0x000E)	1553 (0x0611)	RtlUshortByteSwap	0x000BE950
15	15 (0x000F)	0 (0x0000)	A_SHAFinal	0x00067680

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual
API-MS-WIN-APIQUERY-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).										
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).										
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL	Error opening file. The system cannot find the file specified (2).										
API-MS-WIN-CORE-COMM-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).										
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL	Error opening file. The system cannot find the file specified (2).										
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL	Error opening file. The system cannot find the file specified (2).										
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL	Error opening file. The system cannot find the file specified (2).										
API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL	Error opening file. The system cannot find the file specified (2).										
API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL	Error opening file. The system cannot find the file specified (2).										
API-MS-WIN-CORE-CRT-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).										

Error: At least one required implicit or forwarded dependency was not found.
 Error: At least one module has an unresolved import due to a missing export function in an implicitly dependent module.
 Error: Modules with different CPU types were found.
 Error: A circular dependency was detected.
 Warning: At least one delay-load dependency module was not found.
 Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

For Help, press F1

4. a) Ha jól értelmezem akkor a NTDLL.DLL api-t hívást használja.

Dependency Walker - [XUE9MH.exe]

File Edit View Options Profile Window Help

XUE9MH.EXE

- KERNEL32.DLL
 - API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
 - NTDLL.DLL
 - API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL
 - NTDLL.DLL
 - KERNELBASE.DLL
 - API-MS-WIN-CORE-PROCESSTHREADS-L1-1-0.DLL
 - API-MS-WIN-CORE-PROCESSTHREADS-L1-1-3.DLL
 - API-MS-WIN-CORE-PROCESSTHREADS-L1-1-2.DLL
 - API-MS-WIN-CORE-PROCESSTHREADS-L1-1-1.DLL
 - API-MS-WIN-CORE-REGISTRY-L1-1-0.DLL
 - API-MS-WIN-CORE-HEAP-L1-1-0.DLL
 - API-MS-WIN-CORE-HEAP-L2-1-0.DLL
 - API-MS-WIN-CORE-MEMORY-L1-1-1.DLL
 - API-MS-WIN-CORE-MEMORY-L1-1-0.DLL
 - API-MS-WIN-CORE-MEMORY-L1-1-2.DLL
 - API-MS-WIN-CORE-MEMORY-L1-1-0.DLL
 - API-MS-WIN-CORE-HANDLE-L1-1-0.DLL
 - API-MS-WIN-CORE-SYNCH-L1-1-0.DLL
 - API-MS-WIN-CORE-SYNCH-L1-2-1.DLL
 - API-MS-WIN-CORE-SYNCH-L1-2-0.DLL
 - API-MS-WIN-CORE-FILE-L1-1-0.DLL
 - API-MS-WIN-CORE-FILE-L1-2-0.DLL
 - API-MS-WIN-CORE-FILE-L1-2-2.DLL
 - API-MS-WIN-CORE-FILE-L1-2-1.DLL
 - API-MS-WIN-CORE-DELAYLOAD-L1-1-0.DLL
 - API-MS-WIN-CORE-IO-L1-1-0.DLL
 - API-MS-WIN-CORE-IO-L1-1-1.DLL
 - API-MS-WIN-CORE-JOB-L1-1-0.DLL
 - API-MS-WIN-CORE-THREADPOOL-LEGACY-L1-1-0.DLL
 - API-MS-WIN-CORE-THREADPOOL-PRIVATE-L1-1-0.DLL
 - API-MS-WIN-CORE-LIBRARYLOADER-L1-2-2.DLL

PI	Ordinal ^	Hint	Function	Entry Point
✓	N/A	207 (0x00CF)	DeleteCriticalSection	Not Bound
✓	N/A	236 (0x00EC)	EnterCriticalSection	Not Bound
✓	N/A	279 (0x0117)	ExitProcess	Not Bound
✓	N/A	510 (0x01FE)	GetLastError	Not Bound
✓	N/A	529 (0x0211)	GetModuleHandleA	Not Bound
✓	N/A	577 (0x0241)	GetProcAddress	Not Bound
✓	N/A	734 (0x02DE)	InitializeCriticalSection	Not Bound
✓	N/A	814 (0x032E)	LeaveCriticalSection	Not Bound
✓	N/A	1140 (0x0474)	SetUnhandledExceptionFilter	Not Bound
✓	N/A	1173 (0x0495)	TlsGetValue	Not Bound
✓	N/A	1213 (0x04BD)	VirtualProtect	Not Bound
✓	N/A	1215 (0x04BF)	VirtualQuery	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
✓	1 (0x0001)	68 (0x0044)	BaseThreadInitThunk	0x0001FA10
✓	2 (0x0002)	883 (0x0373)	InterlockedPushListSList	NTDLL.RtlInterlockedPushListSList
✓	3 (0x0003)	1547 (0x060B)	Wow64Transition	0x00082034
✓	4 (0x0004)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
✓	5 (0x0005)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
✓	6 (0x0006)	2 (0x0002)	ActivateActCtx	0x00020AC0
✓	7 (0x0007)	3 (0x0003)	ActivateActCtxWorker	0x00020400
✓	8 (0x0008)	4 (0x0004)	AddAtomA	0x000195A0
✓	9 (0x0009)	5 (0x0005)	AddAtomW	0x0001B8D0
✓	10 (0x000A)	6 (0x0006)	AddConsoleAliasA	0x00023C10
✓	11 (0x000B)	7 (0x0007)	AddConsoleAliasW	0x00023C20
✓	12 (0x000C)	8 (0x0008)	AddDllDirectory	api-ms-win-core-libraryloader-l1-1-0.AddDllDirectory
✓	13 (0x000D)	9 (0x0009)	AddIntegrityLabelToBoundaryDescriptor	0x000352A0
✓	14 (0x000E)	10 (0x000A)	AddLocalAlternateComputerNameA	0x000520E0
✓	15 (0x000F)	11 (0x000B)	AddLocalAlternateComputerNameW	0x00052140

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).										
API-MS-WIN-CORE-APPCOMBAT-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).										

Error: At least one required implicit or forwarded dependency was not found.
For Help, press F1

4.b) Itt a KERNEL32.DLL alatt található összes '.dll' fájl függősége annak.

Dependency Walker - [XUE9MH.exe]

File Edit View Options Profile Window Help

XUE9MH.EXE

- KERNEL32.DLL
 - API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
 - NTDLL.DLL
 - API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL
 - NTDLL.DLL
 - KERNELBASE.DLL
 - API-MS-WIN-CORE-PROCESSTHREADS-L1-1-0.DLL
 - API-MS-WIN-CORE-PROCESSTHREADS-L1-1-3.DLL
 - API-MS-WIN-CORE-PROCESSTHREADS-L1-1-2.DLL
 - API-MS-WIN-CORE-PROCESSTHREADS-L1-1-1.DLL
 - API-MS-WIN-CORE-REGISTRY-L1-1-0.DLL
 - API-MS-WIN-CORE-HEAP-L1-1-0.DLL
 - API-MS-WIN-CORE-HEAP-L2-1-0.DLL
 - API-MS-WIN-CORE-MEMORY-L1-1-1.DLL
 - API-MS-WIN-CORE-MEMORY-L1-1-0.DLL
 - API-MS-WIN-CORE-MEMORY-L1-1-2.DLL
 - API-MS-WIN-CORE-HANDLE-L1-1-0.DLL
 - API-MS-WIN-CORE-SYNCH-L1-1-0.DLL
 - API-MS-WIN-CORE-SYNCH-L1-2-1.DLL
 - API-MS-WIN-CORE-SYNCH-L1-2-0.DLL
 - API-MS-WIN-CORE-FILE-L1-1-0.DLL
 - API-MS-WIN-CORE-FILE-L1-2-0.DLL
 - API-MS-WIN-CORE-FILE-L1-2-2.DLL
 - API-MS-WIN-CORE-FILE-L1-2-1.DLL
 - API-MS-WIN-CORE-DELAYLOAD-L1-1-0.DLL
 - API-MS-WIN-CORE-IO-L1-1-0.DLL
 - API-MS-WIN-CORE-IO-L1-1-1.DLL
 - API-MS-WIN-CORE-JOB-L1-1-0.DLL
 - API-MS-WIN-CORE-THREADPOOL-LEGACY-L1-1-0.DLL
 - API-MS-WIN-CORE-THREADPOOL-PRIVATE-L1-1-0.DLL
 - API-MS-WIN-CORE-LIBRARYLOADER-L1-2-2.DLL

PI	Ordinal ^	Hint	Function	Entry Point
✓	N/A	18 (0x0012)	ApiSetQueryApiSetPresence	Not Bound
✓	N/A	20 (0x0014)	CsrAllocateCaptureBuffer	Not Bound
✓	N/A	21 (0x0015)	CsrAllocateMessagePointer	Not Bound
✓	N/A	26 (0x001A)	CsrClientCallServer	Not Bound
✓	N/A	28 (0x001C)	CsrFreeCaptureBuffer	Not Bound
✓	N/A	32 (0x0020)	CsrVerifyRegion	Not Bound
✓	N/A	34 (0x0022)	DbgPrint	Not Bound
✓	N/A	35 (0x0023)	DbgPrintEx	Not Bound
✓	N/A	45 (0x002D)	DbgUiGetThreadDebugObject	Not Bound
✓	N/A	46 (0x002E)	DbgUiIssueRemoteBreakin	Not Bound
✓	N/A	57 (0x0039)	EtwEventEnabled	Not Bound
✓	N/A	59 (0x003B)	EtwEventRegister	Not Bound
✓	N/A	61 (0x003D)	EtwEventUnregister	Not Bound
✓	N/A	62 (0x003E)	EtwEventWrite	Not Bound
✓	N/A	66 (0x0042)	EtwEventWriteNoRegistration	Not Bound
✓	N/A	102 (0x0066)	LdrAddRefDll	Not Bound
✓	N/A	108 (0x006C)	LdrDisableThreadCalloutsForDll	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
✓	8 (0x0008)	918 (0x0396)	RtlDispatchAPC	0x0002C0A0
✓	9 (0x0009)	711 (0x02C7)	RtlActivateActivationContextUnsafeFast	0x0003FF90
✓	10 (0x000A)	876 (0x036C)	RtlDeactivateActivationContextUnsafeFast	0x00043170
✓	11 (0x000B)	1166 (0x048E)	RtlInterlockedPushListSList	0x000BE880
✓	12 (0x000C)	1508 (0x05E4)	RtlUlongByteSwap	0x000BE920
✓	13 (0x000D)	1509 (0x05E5)	RtlUlonglongByteSwap	0x000BE930
✓	14 (0x000E)	1553 (0x0611)	RtlUshortByteSwap	0x000BE950
✓	15 (0x000F)	0 (0x0000)	A_SHAFinal	0x00067680
✓	16 (0x0010)	1 (0x0001)	A_SHALnit	0x00087480
✓	17 (0x0011)	2 (0x0002)	A_SHAUpdate	0x00067760
✓	18 (0x0012)	3 (0x0003)	AlpcAdjustCompletionListConcurrencyCount	0x000BE960
✓	19 (0x0013)	4 (0x0004)	AlpcFreeCompletionListMessage	0x000BE990
✓	20 (0x0014)	5 (0x0005)	AlpcGetCompletionListLastMessageInformation	0x000BEA80
✓	21 (0x0015)	6 (0x0006)	AlpcGetCompletionListMessageAttributes	0x000BEAB0
✓	22 (0x0016)	7 (0x0007)	AlpcGetHeaderSize	0x000690B0
✓	23 (0x0017)	8 (0x0008)	AlpcGetMessageAttribute	0x00069070

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).										
API-MS-WIN-CORE-APPCOMM-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).										

Error: At least one required implicit or forwarded dependency was not found.
For Help, press F1

4.c) Az NTDLL.DLL -t háromszor találtam meg a függőségek közt és mindháromszor eltérő függvényeket exportált. Leírása szerint ez a dll egy „NT Layer DLL”. Ez egy fájl ami NT kernel függvényeket tartalmaz.