

Operációs Rendszerek BSc

3. gyak.

2021. 02. 24.

Készítette:

Nyíri Beáta

Programtervező Informatikus

I40FDC

Miskolc, 2021

4. Dependency Walker

Az i40fdc.exe megnyitva a Dependency Walkerben:

Dependency Walker - [i40fdc]

File Edit View Options Profile Window Help

c:\users\bea\desktop\egyetem\ tárgyak\2020-21 második\os\gyak\c\3. gyak\i40fdc\bin\debug\i40FDC.EXE

c:\windows\system32\KERNEL32.DLL

- API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
- c:\windows\system32\NTDLL.DLL
- c:\windows\system32\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-L1-2-1.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

| PI | Ordinal | Hint | Function | Entry Point |
|----|---------|---------------|---------------------------|-------------|
| ✓ | N/A | 269 (0x010D) | DeleteCriticalSection | Not Bound |
| ✓ | N/A | 305 (0x0131) | EnterCriticalSection | Not Bound |
| ✓ | N/A | 536 (0x0218) | GetCurrentProcess | Not Bound |
| ✓ | N/A | 537 (0x0219) | GetCurrentProcessId | Not Bound |
| ✓ | N/A | 541 (0x021D) | GetCurrentThreadId | Not Bound |
| ✓ | N/A | 610 (0x0262) | GetLastError | Not Bound |
| ✓ | N/A | 722 (0x02D2) | GetStartupInfoA | Not Bound |
| ✓ | N/A | 747 (0x02EB) | GetSystemTimeAsFileTime | Not Bound |
| ✓ | N/A | 775 (0x0307) | GetTickCount | Not Bound |
| ✓ | N/A | 864 (0x0360) | InitializeCriticalSection | Not Bound |
| ✓ | N/A | 952 (0x03B8) | LeaveCriticalSection | Not Bound |
| ✓ | N/A | 1094 (0x0446) | OpenPerformanceCounter | Not Bound |

| E | Ordinal | Hint | Function | Entry Point |
|---|-------------|-------------|---------------------------------------|--|
| ✓ | 1 (0x0001) | 0 (0x0000) | AcquireSRWLockExclusive | NTDLL.RtlAcquireSRWLockExclusive |
| ✓ | 2 (0x0002) | 1 (0x0001) | AcquireSRWLockShared | NTDLL.RtlAcquireSRWLockShared |
| ✓ | 3 (0x0003) | 2 (0x0002) | ActivateActCtx | 0x0001E690 |
| ✓ | 4 (0x0004) | 3 (0x0003) | ActivateActCtxWorker | 0x0001A9A0 |
| ✓ | 5 (0x0005) | 4 (0x0004) | AddAtomA | 0x000216A0 |
| ✓ | 6 (0x0006) | 5 (0x0005) | AddAtomW | 0x00010890 |
| ✓ | 7 (0x0007) | 6 (0x0006) | AddConsoleAliasA | 0x00022BC0 |
| ✓ | 8 (0x0008) | 7 (0x0007) | AddConsoleAliasW | 0x00022BD0 |
| ✓ | 9 (0x0009) | 8 (0x0008) | AddDllDirectory | api-ms-win-core-libraryloader-l1-1-0.AddDllDir |
| ✓ | 10 (0x000A) | 9 (0x0009) | AddIntegrityLabelToBoundaryDescriptor | 0x00036C50 |
| ✓ | 11 (0x000B) | 10 (0x000A) | AddLocalAlternateComputerNameA | 0x00052BE0 |
| ✓ | 12 (0x000C) | 11 (0x000B) | AddLocalAlternateComputerNameW | 0x00052C40 |

| Module | File Time Stamp | Link Time Stamp | File Size | Attr. | Link Checksum | Real Checksum | CPU | Subsystem | Symbols | Pref |
|--------------------------------------|-----------------|-----------------|-----------|-------|---------------|---------------|-----|-----------|---------|------|
| API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL | | | | | | | | | | |
| API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL | | | | | | | | | | |
| API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL | | | | | | | | | | |
| API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL | | | | | | | | | | |
| API-MS-WIN-CORE-COMM-L1-1-0.DLL | | | | | | | | | | |
| API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL | | | | | | | | | | |
| API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL | | | | | | | | | | |
| API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL | | | | | | | | | | |
| API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL | | | | | | | | | | |
| API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL | | | | | | | | | | |

Error: At least one required implicit or forwarded dependency was not found.
Warning: At least one delay-load dependency module was not found.

For Help, press F1

a.) Az i40fdc.exe milyen hívásokat használ a kernel32.dll-ből:

| | |
|--|--|
| c:\users\bea\desktop\egyetem\targyak\2020-21 masodik\os\gyak\c\3. gyak\i40fdc\bin\debug\i40FDC.EXE | |
| c:\windows\system32\kernel32.dll | |
| API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL | API-MS-WIN-CORE-DEBUG-L1-1-1.DLL |
| c:\windows\system32\NTDLL.dll | API-MS-WIN-CORE-DEBUG-L1-1-0.DLL |
| c:\windows\system32\kernelbase.dll | API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL |
| API-MS-WIN-CORE-PROCESSTHREADS-L1-1-0.DLL | API-MS-WIN-CORE-ERRORHANDLING-L1-1-3.DLL |
| API-MS-WIN-CORE-PROCESSTHREADS-L1-1-3.DLL | API-MS-WIN-CORE-FIBERS-L1-1-0.DLL |
| API-MS-WIN-CORE-PROCESSTHREADS-L1-1-2.DLL | API-MS-WIN-CORE-UTIL-L1-1-0.DLL |
| API-MS-WIN-CORE-PROCESSTHREADS-L1-1-1.DLL | API-MS-WIN-CORE-PROFILE-L1-1-0.DLL |
| API-MS-WIN-CORE-REGISTRY-L1-1-0.DLL | API-MS-WIN-SECURITY-BASE-L1-1-0.DLL |
| API-MS-WIN-CORE-HEAP-L1-1-0.DLL | API-MS-WIN-SECURITY-BASE-L1-2-0.DLL |
| API-MS-WIN-CORE-HEAP-L2-1-0.DLL | API-MS-WIN-SECURITY-APPCONTAINER-L1-1-0.DLL |
| API-MS-WIN-CORE-MEMORY-L1-1-1.DLL | API-MS-WIN-CORE-COMM-L1-1-0.DLL |
| API-MS-WIN-CORE-MEMORY-L1-1-0.DLL | API-MS-WIN-CORE-REALTIME-L1-1-0.DLL |
| API-MS-WIN-CORE-MEMORY-L1-1-2.DLL | API-MS-WIN-CORE-WOW64-L1-1-1.DLL |
| API-MS-WIN-CORE-HANDLE-L1-1-0.DLL | API-MS-WIN-CORE-WOW64-L1-1-0.DLL |
| API-MS-WIN-CORE-SYNCH-L1-1-0.DLL | API-MS-WIN-CORE-SYSTEMTOPOLOGY-L1-1-1.DLL |
| API-MS-WIN-CORE-SYNCH-L1-2-1.DLL | API-MS-WIN-CORE-SYSTEMTOPOLOGY-L1-1-0.DLL |
| API-MS-WIN-CORE-SYNCH-L1-2-0.DLL | API-MS-WIN-CORE-PROCESSTOPOLOGY-L1-1-0.DLL |
| API-MS-WIN-CORE-FILE-L1-1-0.DLL | API-MS-WIN-CORE-NAMESPACE-L1-1-0.DLL |
| API-MS-WIN-CORE-FILE-L1-2-0.DLL | API-MS-WIN-CORE-FILE-L2-1-2.DLL |
| API-MS-WIN-CORE-FILE-L1-2-1.DLL | API-MS-WIN-CORE-FILE-L2-1-0.DLL |
| API-MS-WIN-CORE-FILE-L1-2-2.DLL | API-MS-WIN-CORE-FILE-L2-1-3.DLL |
| API-MS-WIN-CORE-DELAYLOAD-L1-1-0.DLL | API-MS-WIN-CORE-FILE-L2-1-1.DLL |
| API-MS-WIN-CORE-IO-L1-1-1.DLL | API-MS-WIN-CORE-XSTATE-L2-1-0.DLL |
| API-MS-WIN-CORE-IO-L1-1-0.DLL | API-MS-WIN-CORE-XSTATE-L2-1-1.DLL |
| API-MS-WIN-CORE-JOB-L1-1-0.DLL | API-MS-WIN-CORE-LOCALIZATION-L2-1-0.DLL |
| API-MS-WIN-CORE-THREADPOOL-LEGACY-L1-1-0.DLL | API-MS-WIN-CORE-NORMALIZATION-L1-1-0.DLL |
| API-MS-WIN-CORE-THREADPOOL-PRIVATE-L1-1-0.DLL | API-MS-WIN-CORE-FIBERS-L2-1-0.DLL |
| API-MS-WIN-CORE-LARGEINTEGER-L1-1-0.DLL | API-MS-WIN-CORE-FIBERS-L2-1-1.DLL |
| API-MS-WIN-CORE-LIBRARYLOADER-L1-2-2.DLL | API-MS-WIN-CORE-LOCALIZATION-PRIVATE-L1-1-0.DLL |
| API-MS-WIN-CORE-LIBRARYLOADER-L1-2-0.DLL | API-MS-WIN-CORE-SIDEWAYSIDE-L1-1-0.DLL |
| API-MS-WIN-CORE-LIBRARYLOADER-L1-2-1.DLL | API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL |
| API-MS-WIN-CORE-LIBRARYLOADER-L2-1-0.DLL | API-MS-WIN-CORE-WINDOWSERRORREPORTING-L1-1-0.DLL |
| API-MS-WIN-CORE-NAMEDPIPE-L1-2-2.DLL | API-MS-WIN-CORE-WINDOWSERRORREPORTING-L1-1-1.DLL |
| API-MS-WIN-CORE-NAMEDPIPE-L1-1-0.DLL | API-MS-WIN-CORE-WINDOWSERRORREPORTING-L1-1-2.DLL |
| API-MS-WIN-CORE-NAMEDPIPE-L1-2-1.DLL | API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL |
| API-MS-WIN-CORE-DATETIME-L1-1-0.DLL | API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL |
| API-MS-WIN-CORE-DATETIME-L1-1-1.DLL | API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL |
| API-MS-WIN-CORE-DATETIME-L1-1-2.DLL | API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL |
| API-MS-WIN-CORE-SYSINFO-L1-2-0.DLL | API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL |
| API-MS-WIN-CORE-SYSINFO-L1-1-0.DLL | API-MS-WIN-CORE-PSAPI-L1-1-0.DLL |
| API-MS-WIN-CORE-SYSINFO-L1-2-3.DLL | API-MS-WIN-CORE-PSAPI-ANSI-L1-1-0.DLL |
| API-MS-WIN-CORE-SYSINFO-L1-2-1.DLL | API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL |
| API-MS-WIN-CORE-TIMEZONE-L1-1-0.DLL | API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL |
| API-MS-WIN-CORE-LOCALIZATION-L1-2-0.DLL | |
| API-MS-WIN-CORE-PROCESSSNAPSHOT-L1-1-0.DLL | |
| API-MS-WIN-CORE-PROCESSENVIRONMENT-L1-1-0.DLL | |
| API-MS-WIN-CORE-PROCESSENVIRONMENT-L1-2-0.DLL | |
| API-MS-WIN-CORE-STRING-L1-1-0.DLL | |

b.) Milyen függőségei vannak a kernel32.dll-nek?

Az NTDLL.DLL függősége a kernel32.dll-nek:





























c:\windows\system32\NTDLL.DLL

Forwarded module. This module is a dependency because the parent module has forwarded one of its functions to this module.

c.) Mi az NTDLL.DLL szerepe?

Importálja a Windows Native API-t.

Exportált függvényei:

| E | Ordinal ^ | Hint | Function | Entry Point | |
|---|-------------|-------------|--|-------------|--|
|  | 8 (0x0008) | N/A | N/A | 0x0007D5E0 | |
|  | 9 (0x0009) | 0 (0x0000) | A_SHAFinal | 0x0000C4D0 | |
|  | 10 (0x000A) | 1 (0x0001) | A_SHAInit | 0x0000C600 | |
|  | 11 (0x000B) | 2 (0x0002) | A_SHAUpdate | 0x0000C640 | |
|  | 12 (0x000C) | 3 (0x0003) | AlpcAdjustCompletionListConcurrencyCount | 0x000DFA10 | |
|  | 13 (0x000D) | 4 (0x0004) | AlpcFreeCompletionListMessage | 0x0006C7A0 | |
|  | 14 (0x000E) | 5 (0x0005) | AlpcGetCompletionListLastMessageInformation | 0x000DFA40 | |
|  | 15 (0x000F) | 6 (0x0006) | AlpcGetCompletionListMessageAttributes | 0x000DFA60 | |
|  | 16 (0x0010) | 7 (0x0007) | AlpcGetHeaderSize | 0x0006F020 | |
|  | 17 (0x0011) | 8 (0x0008) | AlpcGetMessageAttribute | 0x0006EFE0 | |
|  | 18 (0x0012) | 9 (0x0009) | AlpcGetMessageFromCompletionList | 0x00031DF0 | |
|  | 19 (0x0013) | 10 (0x000A) | AlpcGetOutstandingCompletionListMessageCount | 0x00085740 | |
|  | 20 (0x0014) | 11 (0x000B) | AlpcInitializeMessageAttribute | 0x0006EF80 | |
|  | 21 (0x0015) | 12 (0x000C) | AlpcMaxAllowedMessageLength | 0x00084260 | |
|  | 22 (0x0016) | 13 (0x000D) | AlpcRegisterCompletionList | 0x000855B0 | |
|  | 23 (0x0017) | 14 (0x000E) | AlpcRegisterCompletionListWorkerThread | 0x0006FEB0 | |
|  | 24 (0x0018) | 15 (0x000F) | AlpcRundownCompletionList | 0x00085700 | |
|  | 25 (0x0019) | 16 (0x0010) | AlpcUnregisterCompletionList | 0x00085720 | |
|  | 26 (0x001A) | 17 (0x0011) | AlpcUnregisterCompletionListWorkerThread | 0x0006FE50 | |
|  | 27 (0x001B) | 18 (0x0012) | ApiSetQueryApiSetPresence | 0x000754B0 | |
|  | 28 (0x001C) | 19 (0x0013) | ApiSetQueryApiSetPresenceEx | 0x000D5710 | |
|  | 29 (0x001D) | 20 (0x0014) | CsrAllocateCaptureBuffer | 0x0004C260 | |
|  | 30 (0x001E) | 21 (0x0015) | CsrAllocateMessagePointer | 0x0004C220 | |
|  | 31 (0x001F) | 22 (0x0016) | CsrCaptureMessageBuffer | 0x0004C330 | |
|  | 32 (0x0020) | 23 (0x0017) | CsrCaptureMessageMultiUnicodeStringsInPlace | 0x0004C060 | |
|  | 33 (0x0021) | 24 (0x0018) | CsrCaptureMessageString | 0x0004C170 | |
|  | 34 (0x0022) | 25 (0x0019) | CsrCaptureTimeout | 0x000CBED0 | |
|  | 35 (0x0023) | 26 (0x001A) | CsrClientCallServer | 0x0004BFF0 | |