

# **Operációs rendszerek BSc**

## **2. konzultáció gyakorlat**

**2021.02.26.**

**Készítette:**

Kocsis Katalin Bsc  
Mérnökinformatikus  
WGOWUG

**Miskolc, 2021**

## Operációs rendszerek – 3A. Gyakorlat

### 4. Feladat: Töltse le a következő programot: Dependency Walker

*Feladata:* a segédprogram *megvizsgálja* milyen könyvtárakra, és azon belül milyen függvényekre hivatkozik egy elindított program.

Készítsen egy *neptunkod.c* nevű forráskódot, amely egy *vezeteknev.txt* fájlt létrehoz, olvas, majd bezár. Tartalma: Név, Szak, Neptunkod etc.

Fordítsa le kódot a C fordító, amely létrehoz egy objektum kódot, ezután egy linker segítségével készítsen egy végrehajtott állományt: *neptunkod.exe*

A Dependency Walker segítségével végezze el a következő feladatokat.

Nyissa meg a *neptunkod.exe* fájlt!

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

The screenshot shows the Dependency Walker tool (Dependency Walker - [WGOWUG]) with the loaded modules and the list of functions used by the application.

**Loaded Modules:**

- 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-L1-1-1-0.DLL
- EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1-0.DLL
- EXT-MS-WIN-APPCOMPAT-L1-1-1-0.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-QUICKS-L1-1-0.DLL
- EXT-MS-WIN-KERNEL32-QUICKS-L1-1-0.DLL
- EXT-MS-WIN-KERNEL32-QUICKS-L1-1-0.DLL

**Functions:**

P/I	Ordinal	Hint	Function	Entry Point
N/A	0 (0x0000)	0 (0x0000)	RtlCaptureContext	Not Bound
N/A	1 (0x0001)	1 (0x0001)	RtlCaptureStackBackTrace	Not Bound
N/A	5 (0x0005)	5 (0x0005)	RtlUnwind	Not Bound

**Functions (continued):**

E	Ordinal	Hint	Function	Entry Point
1 (0x0001)	0 (0x0000)	0 (0x0000)	RtlAddFunctionTable	ntdll.RtlAddFunctionTable
2 (0x0002)	1 (0x0001)	1 (0x0001)	RtlCaptureContext	ntdll.RtlCaptureContext
3 (0x0003)	2 (0x0002)	2 (0x0002)	RtlCaptureStackBackTrace	ntdll.RtlCaptureStackBackTrace
4 (0x0004)	3 (0x0003)	3 (0x0003)	RtlCompareMemory	ntdll.RtlCompareMemory
5 (0x0005)	4 (0x0004)	4 (0x0004)	RtlDeleteFunctionTable	ntdll.RtlDeleteFunctionTable
6 (0x0006)	5 (0x0005)	5 (0x0005)	RtlInstallFunctionTableCallback	ntdll.RtlInstallFunctionTableCallback
7 (0x0007)	6 (0x0006)	6 (0x0006)	RtlLookupFunctionEntry	ntdll.RtlLookupFunctionEntry
8 (0x0008)	7 (0x0007)	7 (0x0007)	RtlPcToFileHeader	ntdll.RtlPcToFileHeader

**Errors:**

- 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.

## b.) Milyen függőségei vannak a kernel32.dll-nek!

Függőségek: mik azok a szolgáltatások, amiket meg kell várni, hogy elinduljanak, mielőtt a rendszer elindítja ezt a szolgáltatást, és mik azok, amik ettől a szolgáltatástól függenek. Ezeket az értékeket a szolgáltatás telepítésekor kell megadni.

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. A rendszer nem találja a megadott fájlt (2).										
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
API-MS-WIN-CORE-COMM-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (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.

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

**Szerepe:** Ntdll.dll, amely NT Layer DLL fájlként is ismert, Microsoft készítette Microsoft® Windows® Operating System fejlesztéséhez. DLL fájlok Win32 DLL (Dynamic link library) fájltypus kategóriába sorolandók.

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. A rendszer nem találja a megadott fájlt (2).										
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
API-MS-WIN-CORE-COMM-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (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.