

# **Operációs rendszerek BSc**

## **3.gyak**

2021. 02. 24.

**Készítette:**

Rontó Eszter Bsc

Programtervező inf

QTFL19

**Miskolc, 2021**

a.) Vizsgálja meg, hogy a neptunkod.exe milyen API hívásokat használ a kernel32.dll-ből.

## API-MS-WIN-CORE-RTLSSUPPORT-L1-1-0.DLL

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

Module	File Time Stamp	Link Time Stamp	File Size	Attr	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size
Kernel32.dll	2021/02/10 16:37	2084/05/06 3:04	764 976	A	0x0008FAE7	0x0008FAE7	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x0008B000
KernelBase.dll	2021/02/10 16:37	1977/10/08 4:21	2 922 392	A	0x0022C484	0x0022C484	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x002C9000
MSVCRT.dll	2020/10/14 13:24	2015/11/20 23:31	637 360	A	0x0009E85D	0x0009E85D	x64	GUI	CV,Unknown	0x0000000110100000	Unknown	0x00099E00
NTDLL.dll	2021/02/10 16:37	2006/10/29 15:03	2 025 272	A	0x001F58B7	0x001F58B7	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x001F6000
QTFL19.EXE	2021/02/27 15:42	2021/02/27 15:42	55 739	A	0x000113FF	0x000113FF	x64	Console	None	0x0000000040000000	Unknown	0x00013000
BCRYPTPRIMITIVES.DLL	2020/12/14 8:32	2046/05/24 0:27	523 200	A	0x0007FF5D	0x0007FF5D	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x00080000
CRYPTBASE.dll	2020/10/14 13:24	1991/10/01 16:54	34 152	A	0x00014A16	0x00014A16	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x0000C000
DHCPVC.DLL	2020/10/14 13:24	1984/12/12 9:19	101 376	A	0x0002666A	0x0002666A	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x0001D000
DHCPVC6.DLL	2020/10/14 13:24	2077/01/24 8:52	73 216	A	0x00014E4A	0x00014E4A	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x00017000
DNSAPI.dll	2021/01/14 13:44	2004/01/14 14:22	828 448	A	0x000CDEEB	0x000CDEEB	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x000CB000
IPHLPAPI.dll	2020/10/14 13:24	2080/05/15 7:41	230 392	A	0x0003ECBD	0x0003ECBD	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x00038000
NSI.dll	2020/11/16 10:34	2060/09/14 11:48	24 792	A	0x000117C5	0x000117C5	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x00008000
RPCRT4.dll	2021/01/14 13:44	2100/06/18 16:37	1 222 056	A	0x00134684	0x00134684	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x0012B000
SSPICLI.dll	2020/12/14 8:32	2075/09/10 18:29	230 904	A	0x0003C952	0x0003C952	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x0003C000
WINNSI.dll	2020/10/14 13:24	2037/05/08 12:38	35 640	A	0x0000C473	0x0000C473	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x0000B000
WS2_32.dll	2020/10/14 13:24	2063/07/18 3:18	427 200	A	0x0006CF4B	0x0006CF4B	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x0006B000

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

### NTDLL.DLL szerepe:

Információkat és útmutatásokat tartalmaznak a végrehajtható (EXE) fájlhoz.

### NT API információkat:

- NtAccessCheck
- NtAccessCheckAndAuditAlarm
- NtAccessCheckByType
- NtAccessCheckByTypeResultList
- NtAddAtom