

Operációs rendszerek BSc

3.gyak.

2021. 02. 24.

Készítette:

Mészáros Ákos

Mérnök

Informatikus

BFNA2X

Sajólad, 2021

4. feladat – Dependency Walker

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

Dependency Walker - [BFNA2X]

File Edit View Options Profile Window Help

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual
EXT-MS-WIN32-SUBSYSTEM-QUERY-L1-1-0.DLL	2021/02/11 11:19	2084/05/06 3:04	764 976	A	0x000BF AE7	0x000BF AE7	x64	Console	CV,Unknown	0x0000000180000000	Unknown
KERNEL32.DLL	2021/02/11 11:19	1977/10/08 4:21	2 922 392	A	0x002 CC484	0x002 CC484	x64	Console	CV,Unknown	0x0000000180000000	Unknown
KERNELBASE.DLL	2021/02/11 11:19	1977/10/08 4:21	2 922 392	A	0x0009E85D	0x0009E85D	x64	GUI	CV,Unknown	0x0000000110100000	Unknown
MSVCRT.DLL	2021/02/11 11:19	2006/10/29 15:03	2 025 272	A	0x001 F58B7	0x001 F58B7	x64	Console	CV,Unknown	0x0000000180000000	Unknown
NTDLL.DLL	2021/02/11 11:19	2006/10/29 15:03	2 025 272	A	0x0007FF5D	0x0007FF5D	x64	Console	CV,Unknown	0x0000000180000000	Unknown
BCRYPTPRIMITIVES.DLL	2020/10/16 12:16	1991/10/01 16:54	34 152	A	0x00014A16	0x00014A16	x64	Console	CV,Unknown	0x0000000180000000	Unknown
CRYPTBASE.DLL	2020/10/16 12:16	1984/12/12 9:19	101 376	A	0x0002666A	0x0002666A	x64	Console	CV,Unknown	0x0000000180000000	Unknown
DHCPSCV6.DLL	2020/10/16 12:16	2077/01/24 8:52	73 216	A	0x00014E4A	0x00014E4A	x64	Console	CV,Unknown	0x0000000180000000	Unknown
DNSAPI.DLL	2021/01/15 12:24	2004/01/14 14:22	828 448	A	0x000 CDEEB	0x000 CDEEB	x64	Console	CV,Unknown	0x0000000180000000	Unknown

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.

For Help, press F1

A fájl főleg API-MS-WIN-CORE-... hívásokat használ, de van pár API-MS-WIN-SECURITY és egy API-MS-WIN-OOBE hívás is

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

Dependency Walker - [BFNA2X]

File Edit View Options Profile Window Help

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual
EXT-MS-WIN32-SUBSYSTEM-QUERY-L1-1-0.DLL	2021/02/11 11:19	2084/05/06 3:04	764 976	A	0x000BF AE7	0x000BF AE7	x64	Console	CV,Unknown	0x0000000180000000	Unknown
KERNEL32.DLL	2021/02/11 11:19	1977/10/08 4:21	2 922 392	A	0x002 CC484	0x002 CC484	x64	Console	CV,Unknown	0x0000000180000000	Unknown
KERNELBASE.DLL	2021/02/11 11:19	1977/10/08 4:21	2 922 392	A	0x0009E85D	0x0009E85D	x64	GUI	CV,Unknown	0x0000000110100000	Unknown
MSVCRT.DLL	2021/02/11 11:19	2006/10/29 15:03	2 025 272	A	0x001 F58B7	0x001 F58B7	x64	Console	CV,Unknown	0x0000000180000000	Unknown
NTDLL.DLL	2021/02/11 11:19	2006/10/29 15:03	2 025 272	A	0x0007FF5D	0x0007FF5D	x64	Console	CV,Unknown	0x0000000180000000	Unknown
BCRYPTPRIMITIVES.DLL	2020/10/16 12:16	1991/10/01 16:54	34 152	A	0x00014A16	0x00014A16	x64	Console	CV,Unknown	0x0000000180000000	Unknown
CRYPTBASE.DLL	2020/10/16 12:16	1984/12/12 9:19	101 376	A	0x0002666A	0x0002666A	x64	Console	CV,Unknown	0x0000000180000000	Unknown
DHCPSCV6.DLL	2020/10/16 12:16	2077/01/24 8:52	73 216	A	0x00014E4A	0x00014E4A	x64	Console	CV,Unknown	0x0000000180000000	Unknown
DNSAPI.DLL	2021/01/15 12:24	2004/01/14 14:22	828 448	A	0x000 CDEEB	0x000 CDEEB	x64	Console	CV,Unknown	0x0000000180000000	Unknown

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.

For Help, press F1

Dependency Walker - [BFNA2X]

File Edit View Options Profile Window Help

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	300 (0x012C)	FindClose	Not Bound
?	N/A	304 (0x0130)	FindFirstFileA	Not Bound
?	N/A	321 (0x0141)	FindNextFileA	Not Bound
?	N/A	352 (0x0160)	FreeLibrary	Not Bound
?	N/A	388 (0x0184)	GetCommandLineA	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	744 (0x02E8)	InterlockedExchange	Not Bound
?	N/A	763 (0x02FB)	IsDBCSLeadByteEx	Not Bound
?	N/A	814 (0x032E)	LeaveCriticalSection	Not Bound
?	N/A	817 (0x0331)	LoadLibraryA	Not Bound
?	N/A	860 (0x035C)	MultiByteToWideChar	Not Bound
?	N/A	1140 (0x0474)	SetUnhandledExceptionFilter	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
1	1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
2	2 (0x0002)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
3	3 (0x0003)	2 (0x0002)	ActivateActCtx	0x00020800
4	4 (0x0004)	3 (0x0003)	ActivateActCtxWorker	0x00018700
5	5 (0x0005)	4 (0x0004)	AddAtomA	0x00059170
6	6 (0x0006)	5 (0x0005)	AddAtomW	0x000128F0
7	7 (0x0007)	6 (0x0006)	AddConsoleAliasA	0x00025640
8	8 (0x0008)	7 (0x0007)	AddConsoleAliasW	0x00025650

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual
EXT-MS-WIN32-SUBSYSTEM-QUERY-L1-1-0.DLL	2021/02/11 11:19	2084/05/06 3:04	764 976	A	0x0008FAE7	0x0008FAE7	x64	Console	CV,Unknown	0x0000000180000000	Unknown
KERNEL32.DLL	2021/02/11 11:19	1977/10/08 4:21	2 922 392	A	0x0002CC484	0x0002CC484	x64	Console	CV,Unknown	0x0000000180000000	Unknown
KERNELBASE.DLL	2020/10/16 12:16	2015/11/20 23:31	637 360	A	0x0009E85D	0x0009E85D	x64	GUI	CV,Unknown	0x0000000110100000	Unknown
MSVCRT.DLL	2021/02/11 11:19	2006/10/29 15:03	2 025 272	A	0x0001F58B7	0x0001F58B7	x64	Console	CV,Unknown	0x0000000180000000	Unknown
NTDLL.DLL	2020/12/11 15:04	2046/05/24 0:27	523 200	A	0x0007FF5D	0x0007FF5D	x64	Console	CV,Unknown	0x0000000180000000	Unknown
BCRYPTPRIMITIVES.DLL	2020/10/16 12:16	1991/10/01 16:54	34 152	A	0x00014A16	0x00014A16	x64	Console	CV,Unknown	0x0000000180000000	Unknown
CRYPTBASE.DLL	2020/10/16 12:16	1984/12/12 9:19	101 376	A	0x0002666A	0x0002666A	x64	Console	CV,Unknown	0x0000000180000000	Unknown
DHCPSPV6.DLL	2020/10/16 12:16	2077/01/24 8:52	73 216	A	0x00014E4A	0x00014E4A	x64	Console	CV,Unknown	0x0000000180000000	Unknown
DNSAPI.DLL	2021/01/15 12:24	2004/01/14 14:22	828 448	A	0x000CDEEB	0x000CDEEB	x64	Console	CV,Unknown	0x0000000180000000	Unknown

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.

For Help, press F1

Az NTDLL.DLL, KERNELBASE.DLL és KPCR14.DLL a függőségei.

c) Keresse meg NTDLL.DLL-t! Mi ennek a szerepe?

Dependency Walker - [BFNA2X]

File Edit View Options Profile Window Help

PI	Ordinal ^	Hint	Function	Entry Point
?	N/A	N/A	RtlLeaveCriticalSection	Not Bound
?	N/A	N/A	RtlInitializeCriticalSection	Not Bound
?	N/A	N/A	RtlEnterCriticalSection	Not Bound
?	N/A	N/A	RtlDeleteCriticalSection	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
8	8 (0x0008)	N/A	N/A	0x0007E6B0
9	9 (0x0009)	0 (0x0000)	A_SHAFinal	0x0005C290
10	10 (0x000A)	1 (0x0001)	A_SHAInit	0x0005D0C0
11	11 (0x000B)	2 (0x0002)	A_SHAUpdate	0x0005D100
12	12 (0x000C)	3 (0x0003)	AlpcAdjustCompletionListConcurrencyCount	0x000E0700
13	13 (0x000D)	4 (0x0004)	AlpcFreeCompletionListMessage	0x0006F920
14	14 (0x000E)	5 (0x0005)	AlpcGetCompletionListLastMessageInformation	0x000E0730
15	15 (0x000F)	6 (0x0006)	AlpcGetCompletionListMessageAttributes	0x000E0750
16	16 (0x0010)	7 (0x0007)	AlpcGetHeaderSize	0x0006F650

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual
EXT-MS-WIN32-SUBSYSTEM-QUERY-L1-1-0.DLL	2021/02/11 11:19	2084/05/06 3:04	764 976	A	0x0008FAE7	0x0008FAE7	x64	Console	CV,Unknown	0x0000000180000000	Unknown
KERNEL32.DLL	2021/02/11 11:19	1977/10/08 4:21	2 922 392	A	0x0002CC484	0x0002CC484	x64	Console	CV,Unknown	0x0000000180000000	Unknown
KERNELBASE.DLL	2020/10/16 12:16	2015/11/20 23:31	637 360	A	0x0009E85D	0x0009E85D	x64	GUI	CV,Unknown	0x0000000110100000	Unknown
MSVCRT.DLL	2021/02/11 11:19	2006/10/29 15:03	2 025 272	A	0x0001F58B7	0x0001F58B7	x64	Console	CV,Unknown	0x0000000180000000	Unknown
NTDLL.DLL	2020/12/11 15:04	2046/05/24 0:27	523 200	A	0x0007FF5D	0x0007FF5D	x64	Console	CV,Unknown	0x0000000180000000	Unknown
BCRYPTPRIMITIVES.DLL	2020/10/16 12:16	1991/10/01 16:54	34 152	A	0x00014A16	0x00014A16	x64	Console	CV,Unknown	0x0000000180000000	Unknown
CRYPTBASE.DLL	2020/10/16 12:16	1984/12/12 9:19	101 376	A	0x0002666A	0x0002666A	x64	Console	CV,Unknown	0x0000000180000000	Unknown
DHCPSPV6.DLL	2020/10/16 12:16	2077/01/24 8:52	73 216	A	0x00014E4A	0x00014E4A	x64	Console	CV,Unknown	0x0000000180000000	Unknown
DNSAPI.DLL	2021/01/15 12:24	2004/01/14 14:22	828 448	A	0x000CDEEB	0x000CDEEB	x64	Console	CV,Unknown	0x0000000180000000	Unknown

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.

For Help, press F1

az NTDLL.dll foglalkozik az user-mode és kermnel-mode közötti váltással