

Operációs rendszerek BSc

3. gyak

2021.02.24.

Készítette:

Ferencsik Márk BSc

Programtervező informatika

UJTWLL

1. Dependency Walker működésének bemutatása:

a. ujtwwl.exe API hívásainak bemutatása:

Dependency Walker - [ujtwwl]

File Edit View Options Profile Window Help

UJTWWL.EXE

Module List:

- kernel32.dll
- user32.dll
- gdi32.dll
- kernelbase.dll
- api-ms-win-core-rtlsupport-l1-1-0.dll
- ntdll.dll
- api-ms-win-eventing-provider-l1-1-0.dll
- api-ms-win-core-apiquery-l1-1-0.dll
- api-ms-win-core-apiquery-l1-1-0.dll
- ext-ms-win-advapi32-registry-l1-1-0.dll
- ext-ms-win-advapi32-registry-l1-1-0.dll
- ext-ms-win-advapi32-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-date-time-l1-1-0.dll
- ext-ms-win-kernel32-quirks-l1-1-0.dll
- ext-ms-win-kernel32-quirks-l1-1-0.dll
- ext-ms-win-kernel32-side-by-side-l1-1-0.dll
- ext-ms-win-minicorerestmgr-l1-1-0.dll
- ext-ms-win-gapi-grouppolicy-l1-1-0.dll
- ext-ms-win-ntdsapi-activedirectoryclient-l1-1-0.dll
- ext-ms-win-ntdsapi-activedirectoryclient-l1-1-0.dll
- ext-ms-win-shell32-shellcom-l1-1-0.dll
- ext-ms-win-advapi32-ntmarta-l1-1-0.dll
- ext-ms-win-security-capauthz-l1-1-0.dll
- ext-ms-win-ecient-encrypted-l1-1-0.dll

Module	File Name	File Time Stamp	Link Time Stamp	File Size	Attributes	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size	Load Order	File Ver	Product Ver	Image Ver	Link Ver
kernel32.dll	kernel32.dll	2020/12/23 18:39	2020/12/23 15:57	764,976	A	0x0000C9C9	0x0000C9C9	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x00000000	Not Loaded	10.0.19041.662	10.0.19041.662	10.0	14.20
kernelbase.dll	kernelbase.dll	2020/12/23 18:40	2020/08/07 3:46	2,862,392	A	0x0012C7D7	0x0012C7D7	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x0012C9D0	Not Loaded	10.0.19041.662	10.0.19041.662	10.0	14.20
user32.dll	user32.dll	2020/12/07 02:25	2015/11/20 23:31	637,360	A	0x0000E8D0	0x0000E8D0	x64	GUI	CV,Unknown	0x0000000110100000	Unknown	0x0000E9D0	Not Loaded	7.0.19041.548	10.0.19041.548	10.0	14.20
gdi32.dll	gdi32.dll	2020/12/23 18:40	1991/02/18 11:01	2,025,272	A	0x001F0669	0x001F0669	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x001F06D0	Not Loaded	10.0.19041.662	10.0.19041.662	10.0	14.20
bcryptprimitives.dll	bcryptprimitives.dll	2020/12/23 18:40	2046/05/24 0:27	523,200	A	0x0007FF5D	0x0007FF5D	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x00080000	Not Loaded	10.0.19041.662	10.0.19041.662	10.0	14.20
cryptbase.dll	cryptbase.dll	2020/12/07 02:25	1991/10/01 16:54	34,152	A	0x00014A16	0x00014A16	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x0000C000	Not Loaded	10.0.19041.548	10.0.19041.548	10.0	14.20
dhcpcsvc.dll	dhcpcsvc.dll	2020/12/07 02:25	1984/12/12 9:19	101,376	A	0x00026A6A	0x00026A6A	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x00010000	Not Loaded	10.0.19041.548	10.0.19041.548	10.0	14.20
dhcpcsvc.dll	dhcpcsvc.dll	2020/12/07 02:25	2077/01/24 8:52	73,216	A	0x00014E4A	0x00014E4A	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x00017000	Not Loaded	10.0.19041.548	10.0.19041.548	10.0	14.20
dnsapi.dll	dnsapi.dll	2021/01/20 17:53	2004/01/14 14:22	828,448	A	0x000CDEE8	0x000CDEE8	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x000CB000	Not Loaded	10.0.19041.746	10.0.19041.746	10.0	14.20
ip4api.dll	ip4api.dll	2020/12/07 02:25	2080/05/15 7:41	220,384	A	0x00011EC0	0x00011EC0	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x00018000	Not Loaded	10.0.19041.548	10.0.19041.548	10.0	14.20
netbios.dll	netbios.dll	2020/12/07 02:25	2080/09/14 11:48	24,792	A	0x000117C3	0x000117C3	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x00008000	Not Loaded	10.0.19041.610	10.0.19041.610	10.0	14.20
rpcrt4.dll	rpcrt4.dll	2021/01/20 17:53	2100/06/18 16:07	1,222,056	A	0x00124684	0x00124684	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x00128000	Not Loaded	10.0.19041.746	10.0.19041.746	10.0	14.20

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.
Warning: At least one delay load dependency module was not found.

For Help, press F1

A képernyőképből kiolvasható, hogy a kernel32.dll-ből milyen API hívások keletkeztek (az API* formátumú dll fájlokat értjük ezek alatt).

b. Kernel32.dll függőségei:

c. NTDLL.dll szerepe, exportált függvények, információk az NT API-tól: