

# **Operációs rendszerek BSc**

## **3.gyak.**

2021. 02. 24.  
Készítette:  
Bolgár Dominik Bsc  
Mérnökinformatikus  
AAH5X1

## 1. feladat –

Töltse le a következő programot: Dependency Walker

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 végrehajtó 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 a C code editor with the following code:

```
1 #include <stdio.h>
2 #include <stdlib.h>
3
4 int main()
5 {
6     FILE* fp;
7     fp = fopen("vezeteknev.txt", "w");
8     fprintf(fp, "Bolgár Dominik, Műnőkinformatikus, AAH5X1");
9     fclose(fp);
10
11     return 0;
12 }
```

The Dependency Walker tool shows the list of modules loaded by the program, including various Windows system DLLs like API-MS-WIN-CORE-FIBERS-L2-1-0.DLL, API-MS-WIN-CORE-SIDE-BY-SIDE-L1-1-0.DLL, API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL, API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL, API-MS-WIN-CORE-WINDOWS-ERROR-REPORTING-L1-1-0.DLL, API-MS-WIN-CORE-WINDOWS-ERROR-REPORTING-L1-1-2.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, API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL, API-MS-WIN-CORE-PSAPI-L1-1-0.DLL, API-MS-WIN-CORE-PSAPI-ANSI-L1-1-0.DLL, API-MS-WIN-SECURITY-APPCONTAINER-L1-1-0.DLL, and API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL. The tool also shows the list of functions used by the program, including RtlLeaveCriticalSection, RtlInitializeCriticalSection, RtlEnterCriticalSection, RtlDeleteCriticalSection, RtlDispatchAPC, RtlActivateActivationContextUnsafeFast, RtlDeactivateActivationContextUnsafeFast, RtlInterlockedPushListSList, RtlUlongByteSwap, RtlUshortByteSwap, A\_SHAFinal, A\_SHALimit, and A\_SHAUpdate. The tool also shows the list of modules loaded by the program, including various Windows system DLLs like API-MS-WIN-CORE-FIBERS-L2-1-0.DLL, API-MS-WIN-CORE-SIDE-BY-SIDE-L1-1-0.DLL, API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL, API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL, API-MS-WIN-CORE-WINDOWS-ERROR-REPORTING-L1-1-0.DLL, API-MS-WIN-CORE-WINDOWS-ERROR-REPORTING-L1-1-2.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, API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL, API-MS-WIN-CORE-PSAPI-L1-1-0.DLL, API-MS-WIN-CORE-PSAPI-ANSI-L1-1-0.DLL, API-MS-WIN-SECURITY-APPCONTAINER-L1-1-0.DLL, and API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL. The tool also shows the list of functions used by the program, including RtlLeaveCriticalSection, RtlInitializeCriticalSection, RtlEnterCriticalSection, RtlDeleteCriticalSection, RtlDispatchAPC, RtlActivateActivationContextUnsafeFast, RtlDeactivateActivationContextUnsafeFast, RtlInterlockedPushListSList, RtlUlongByteSwap, RtlUshortByteSwap, A\_SHAFinal, A\_SHALimit, and A\_SHAUpdate.

Module	File Time Stamp	Link Time Stamp	File Size	Attr	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size	Load
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).												
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).												
API-MS-WIN-CORE-COMM-L1-1-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).												
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).												
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).												
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).												
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).												
API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).												
API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).												

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

Ezen a képen a NTDLL.DLL látható. Ha jól értelmezem ezzel nyitja és zárja le az egyes folyamatokat. Minden egyes folyamat előtt megtalálható és minden folyamat végén.

2. feladat - Milyen függőségei vannak a kernel32.dll-nek!  
Keresse meg NTDLL.DLL-t! Mi ennek a szerepe? Vizsgálja meg az exportált függvényeket, milyen információkat kap az NT API-ról!

Dependency Walker - [AAHSX1]

File Edit View Options Profile Window Help

AAHSX1.EXE

- KERNEL32.DLL
  - API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.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-L1-1-0.DLL
  - EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL
  - EXT-MS-WIN-KERNEL32-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-DATETIME-L1-1-0.DLL
  - EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL
  - EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-1.DLL
  - EXT-MS-WIN-KERNEL32-SIDEBYSIDE-L1-1-0.DLL
  - EXT-MS-WIN-MRMCMCORE-RESMANAGER-L1-1-0.DLL
  - EXT-MS-WIN-GPAPI-GROUPPOLICY-L1-1-0.DLL
  - EXT-MS-WIN-NTKADIRECTORYCLIENT-L1-1-0.DLL

PI	Ordinal	Hint	Function	Entry Point
N/A	208 (0x00D0)		DeleteCriticalSection	Not Bound
N/A	237 (0x00ED)		EnterCriticalSection	Not Bound
N/A	280 (0x0118)		ExitProcess	Not Bound
N/A	301 (0x012D)		FindClose	Not Bound
N/A	305 (0x0131)		FindFirstFileA	Not Bound
N/A	322 (0x0142)		FindNextFileA	Not Bound
N/A	353 (0x0161)		FreeLibrary	Not Bound
N/A	389 (0x0185)		GetCommandLineA	Not Bound
N/A	511 (0x01FF)		GetLastError	Not Bound
N/A	530 (0x0212)		GetModuleHandleA	Not Bound
1	1 (0x0001)	68 (0x0044)	BaseThreadInitThunk	0x00016340
2	2 (0x0002)	880 (0x0370)	InterlockedPushListSList	NTDLL.RtlInterlockedPushListSList
3	3 (0x0003)	1543 (0x0607)	Wow64Transition	0x00081F94
4	4 (0x0004)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
5	5 (0x0005)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
6	6 (0x0006)	2 (0x0002)	ActivateActCtx	0x00022090
7	7 (0x0007)	3 (0x0003)	ActivateActCtxWorker	0x00017D60
8	8 (0x0008)	4 (0x0004)	AddAtomA	0x0001F270
9	9 (0x0009)	5 (0x0005)	AddAtomW	0x00013890
10	10 (0x000A)	6 (0x0006)	AddConsoleAliasA	0x00024A20

Module	File Time Stamp	Link Time Stamp	File Size	Attr	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size	Load
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-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).												
API-MS-WIN-CORE-CONSOLE-L1-2-0.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-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.  
Warning: At least one delay-load dependency module was not found.

For Help, press F1

Írjon ide a kereséshez

11:02 2021.02.28

Ezen a képen látható milyen API hívásokat használ a KERNEL32.DLL(WIN SUPPORT). A KERNEL32.DLL a saját belső API .dll fájljaira hivatkozik.