

Operációs rendszerek BSc

3.gyak.

2021. 02. 24.

Készítette:

Tóth József BProf

Üzemtechnológus-

informatikus alapszak

WI2GDP

Miskolc, 2021

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 végrehajtható állományt.

```
1  #include "stdio.h"
2  #include "stdlib.h"
3
4  int main()
5  {
6      FILE *fp = fopen("toth.txt", "w");
7      fprintf(fp, "Toth Jozsef\nUzenmternoki informatikus (BProf)\nWI2GDP");
8      fclose(fp);
9      FILE *fpMasodik = fopen("toth.txt", "r");
10     char line[101];
11     while(!feof(fpMasodik))
12     {
13         fgets(line, 100, fpMasodik);
14         puts(line);
15     }
16     fclose(fpMasodik);
17     return 0;
18 }
19
```

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 interface. On the left, the 'Module' list includes various Windows system DLLs, with 'kernel32.dll' highlighted. On the right, the 'Function' list shows the API calls imported from 'kernel32.dll'. The functions are listed in two columns, each with a 'Function' name and an 'Entry Point'.

Function	Entry Point
DeleteCriticalSection	Not Bound
EnterCriticalSection	Not Bound
ExitProcess	Not Bound
FindClose	Not Bound
FindFirstFileA	Not Bound
FindNextFileA	Not Bound
FreeLibrary	Not Bound
GetCommandLineA	Not Bound

Below this, another table shows functions with their ordinal, hint, and entry point:

Ordinal	Hint	Function	Entry Point
1 (0x0001)	68 (0x0044)	BaseThreadInitThunk	0x0001FA10
2 (0x0002)	883 (0x0373)	InterlockedPushListSList	NTDLL.RtlInterlockedPushListSList
3 (0x0003)	1547 (0x060B)	Wow64Transition	0x00082034
4 (0x0004)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
5 (0x0005)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
6 (0x0006)	2 (0x0002)	ActivateActCtx	0x00020AC0
7 (0x0007)	3 (0x0003)	ActivateActCtxWorker	0x00020400

At the bottom, the 'Module' list shows several modules with error messages: 'Error opening file. The system cannot find the file specified (2)'. These errors are for modules like 'API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL', 'API-MS-WIN-CORE-COMM-L1-1-0.DLL', 'API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL', 'API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL', 'API-MS-WIN-CORE-CONSOLE-L1-2-1-0.DLL', and 'API-MS-WIN-CORE-CONSOLE-L1-2-2-0.DLL'.

A **kernel32.dll**-en belül rengeteg különböző API és DLL hivatkozás történik melyek között más-más függvény lapul. Ezek közül van amely felel a lokalizációért, a megszakítás kezeléséért, a fájlkezelésért, esetleges más könyvtárból való tallózásáért, stb.

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

- MS-WIN API-k
- ntdll.dll
- kernelbase.dll
- rpcrt4.dll

NTDLL.DLL	N/A	26 (0x001A)	CsrClientCallServer	Not Bound
KERNELBASE.DLL	N/A	28 (0x001C)	CsrFreeCaptureBuffer	Not Bound
NTDLL.DLL	N/A	32 (0x0020)	CsrVerifyRegion	Not Bound
API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL	N/A	34 (0x0022)	DbgPrint	Not Bound
EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL	N/A	35 (0x0023)	DbgPrintEx	Not Bound
EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL	N/A	45 (0x002D)	DbgUiGetThreadDebugObject	Not Bound
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-SIDEWAYSIDE-L1-1-0.DLL				

E	Ordinal ^	Hint	Function	Entry Point
8 (0x0008)	918 (0x0396)		RtlDispatchAPC	0x0002C0A0
9 (0x0009)	711 (0x02C7)		RtlActivateActivationContextUnsafeFast	0x0003FF90
10 (0x000A)	876 (0x036C)		RtlDeactivateActivationContextUnsafeFast	0x00044370
11 (0x000B)	1166 (0x048E)		RtlInterlockedPushListSList	0x000BE800
12 (0x000C)	1508 (0x05E4)		RtlUlongByteSwap	0x000BE8A0
13 (0x000D)	1509 (0x05E5)		RtlUlonglongByteSwap	0x000BE8B0
14 (0x000E)	1553 (0x0611)		RtlUshortByteSwap	0x000BE8D0
15 (0x000F)	0 (0x0000)		A_SHAFinal	0x00067740