

Operációs rendszerek BSc

3.gyak.

2021. 02. 24.

Készítette:
Kovács Krisztián
Programtervező informatikus
WIQPM2

Miskolc, 2021

1. A Dependency Walker segédprogram segítségével vizsgálja meg milyen könyvtárakra, és azon belül milyen függvényekre hivatkozik egy elindított program.

Forráskód:

```
#include <stdio.h>
#include <stdlib.h>

int main()
{
    FILE *f;
    f = fopen("Kovacs.txt", "w+t");
    fprintf(f, "Kovacs Krisztian\nBP\nWIQPM2");
    rewind(f);
    char vnev[50], knev[50], szak[50], neptun[7];
    fscanf(f, "%s", vnev);
    fscanf(f, "%s", knev);
    fscanf(f, "%s", szak);
    fscanf(f, "%s", neptun);
    printf("Nev: %s %s\n", vnev, knev);
    printf("Szak: %s\n", szak);
    printf("Neptun: %s\n", neptun);
    fclose(f);
    return 0;
}
```

a) Vizsgálja meg, hogy a *neptunkod.exe* milyen API hívásokat használ a kernel32.dll-ből (Win alrendszer DLL)!

Dependency Walker - [wiqpm2.exe]

File Edit View Options Profile Window Help

Module List:

- KERNEL32.DLL
- API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
- NTDLL.DLL
- KERNELBASE.DLL
- API-MS-WIN-CORE-PROCESSTHREADS-L1-1-0.DLL
- API-MS-WIN-CORE-PROCESSTHREADS-L1-1-3.DLL
- API-MS-WIN-CORE-PROCESSTHREADS-L1-1-2.DLL
- API-MS-WIN-CORE-PROCESSTHREADS-L1-1-1.DLL
- API-MS-WIN-CORE-REGISTRY-L1-1-0.DLL
- API-MS-WIN-CORE-HEAP-L1-1-0.DLL

Function List:

| 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 | 510 (0x01FE) | GetLastError | Not Bound |

Module List (Bottom):

| Module | File Time Stamp | Link Time Stamp | File Size | Attr. | Link Checksum | Real Checksum |
|--------------------------------------|--|-----------------|-----------|-------|---------------|---------------|
| API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL | Error opening file. A rendszer nem találja a megadott fájlt (2). | | | | | |
| API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL | Error opening file. A rendszer nem találja a megadott fájlt (2). | | | | | |
| 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). | | | | | |

Error Messages:

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

For Help, press F1

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

Dependency Walker - [KERNEL32.DLL]

File Edit View Options Profile Window Help

Kernel32.DLL dependencies:

- API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
- NTDLL.DLL
- KERNELBASE.DLL
- API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
- API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL
- API-MS-WIN-CORE-APIQUERY-L1-1-1.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

Functions:

| E | Ordinal | Hint | Function | Entry Point |
|---|---------|------------|-------------------------|----------------------------------|
| 1 | 0x0001 | 0 (0x0000) | AcquireSRWLockExclusive | NTDLL.RtlAcquireSRWLockExclusive |
| 2 | 0x0002 | 1 (0x0001) | AcquireSRWLockShared | NTDLL.RtlAcquireSRWLockShared |
| 3 | 0x0003 | 2 (0x0002) | ActivateActCtx | 0x00020080 |
| 4 | 0x0004 | 3 (0x0003) | ActivateActCtxWorker | 0x0001B700 |

Modules:

| Module | File Time Stamp | Link Time Stamp | File Size | Attr. | Link Checksum | Real Checksum |
|--------------------------------------|--|-----------------|-----------|-------|---------------|---------------|
| API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL | Error opening file. A rendszer nem találja a megadott fájlt (2). | | | | | |
| API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL | Error opening file. A rendszer nem találja a megadott fájlt (2). | | | | | |
| 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). | | | | | |

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

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

Dependency Walker - [wiqpm2.exe]

File Edit View Options Profile Window Help

WIQPM2.EXE dependencies:

- KERNEL32.DLL
- API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
- NTDLL.DLL
- KERNELBASE.DLL
- API-MS-WIN-CORE-PROCESSTHREADS-L1-1-0.DLL
- API-MS-WIN-CORE-PROCESSTHREADS-L1-1-3.DLL
- API-MS-WIN-CORE-PROCESSTHREADS-L1-1-2.DLL
- API-MS-WIN-CORE-PROCESSTHREADS-L1-1-1.DLL
- API-MS-WIN-CORE-REGISTRY-L1-1-0.DLL
- API-MS-WIN-CORE-HEAP-L1-1-0.DLL

Functions:

| E | Ordinal | Hint | Function | Entry Point |
|----|---------|------------|-------------|-------------|
| 8 | 0x0008 | N/A | N/A | 0x0007 |
| 9 | 0x0009 | 0 (0x0000) | A_SHAFinal | 0x0005 |
| 10 | 0x000A | 1 (0x0001) | A_SHAInit | 0x0005 |
| 11 | 0x000B | 2 (0x0002) | A_SHAUpdate | 0x0005 |

Modules:

| Module | File Time Stamp | Link Time Stamp | File Size | Attr. | Link Checksum | Real Checksum |
|----------------------|------------------|------------------|-----------|-------|---------------|---------------|
| KERNELBASE.DLL | 2021/02/13 13:27 | 1977/10/08 4:21 | 2 922 392 | A | 0x002CC484 | 0x002CC484 |
| MSVCRT.DLL | 2020/11/21 6:42 | 2015/11/20 23:31 | 637 360 | A | 0x0009E85D | 0x0009E85D |
| NTDLL.DLL | 2021/02/13 13:27 | 2006/10/29 15:03 | 2 025 272 | A | 0x001F58B7 | 0x001F58B7 |
| BCRYPTPRIMITIVES.DLL | 2020/12/11 14:39 | 2046/05/24 0:27 | 523 200 | A | 0x0007FF5D | 0x0007FF5D |

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

For Help, press F1

NTDLL.DLL fő szerepe: Összeköti a User és Kernel módot. Az Executive függvényeknek megfelelő függvénycsomók vannak benne.