Operációs rendszerek BSc

3.gyak.

2021. 02. 24.

Készítette:

Tóth József BProf
Üzemmérnök-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 végrehajtó állományt.

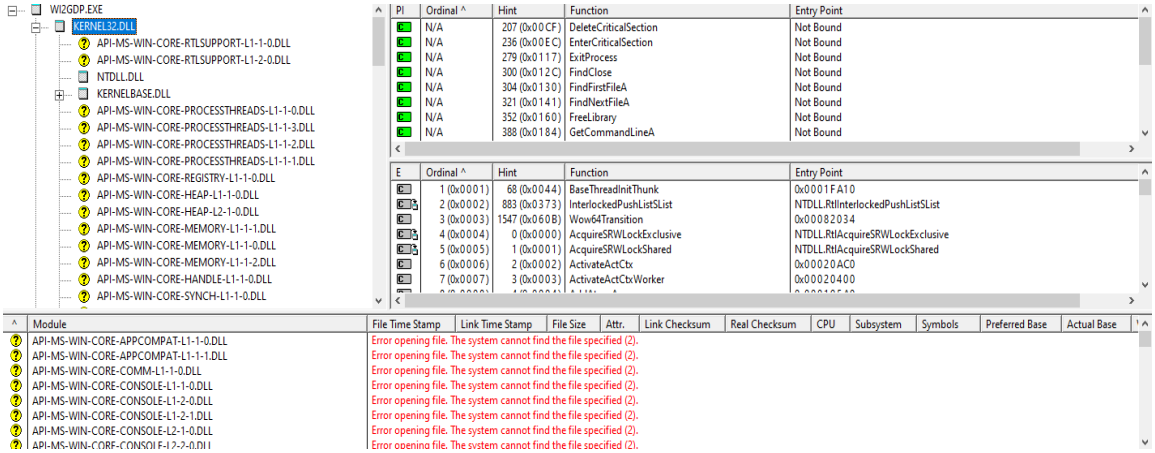
```c
#include "stdio.h"
#include "stdlib.h"

int main()
{
    FILE *fp = fopen("toth.txt","w");
    fprintf(fp,"Toth Jozsef\nUzemmernoki informatikus (BProf)\nWI2GDP");
    fclose(fp);
    FILE *fpMasodik = fopen("toth.txt","r");
    char line[101];
    while(!feof(fpMasodik))
    {
        fgets(line, 100, fpMasodik);
        puts(line);
    }
    fclose(fpMasodik);
    return 0;
}
```

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)!*

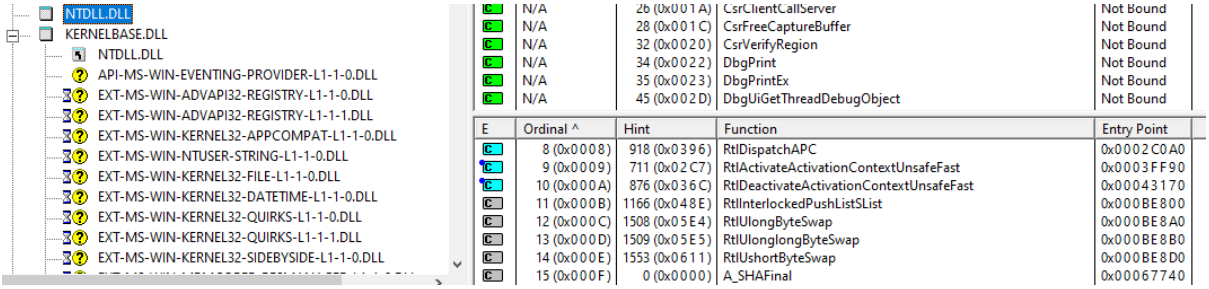


A **kernel32.dll**-en belül rengeteg különböző API és DLL hivatkozás történik melyek között más-más függvény lapul. Ezek közül van amely felel a lokalizációért, a megszakítás kezeléséért, a fájlkezelésért, esetleges más könyvtárból való tallózásáért, stb.

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

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

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



Az **ntdll.dll** egy a Microsoft által készített dinamikus csatolású könyvtár, mely többek között az NT kerneles függvényeket tartalmazza. Az exportált függvények közül az **NtAccessCheck** függvényt vizsgáltam meg, ami tulajdonképpen, eldönti hogy a hozzáférési engedéllyel rendelkező felhasználó beléphet-e az adott rendszerbe. A kiszolgálóalkalmazások általában ezt a funkciót használják egy privát objektumhoz való hozzáférés ellenőrzésére.