Operációs rendszerek BSc

2. Gyak.

2022. 02. 16.

Készítette:

Palencsár Enikő Bsc

Mérnökinformatikus

YD11NL

Miskolc, 2022

1.Feladat

a) Hozza létre a következő mappa szerkezetet!

```
C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>cd fa

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\fa>md korte

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\fa>cd ..

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>cd land

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\land>md szeder

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\land>md kokusz

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\land>cd..

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>tree
Folder PATH listing for volume Windows-SSD
Volume serial number is F095-E92B
C:.
├───bokor
│   ├───banan
│   ├───barack
│   └───mogyoro
├───fa
│   └───korte
└───land
    ├───kokusz
    └───szeder

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>
```

b) Készítsen másolatot:

- a neptunkod/ land/szeder katalógusról a neptunkod/fa katalógusba
- a neptunkod /bokor/banan katalógusról a neptunkod /fa katalógusba

```
    ├───kokusz
    └───szeder

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>cd .\land\szeder

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\land\szeder>write >tmp.txt

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\land\szeder>cd..

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\land>cd..

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>xcopy .\land .\fa /T

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>tree
Folder PATH listing for volume Windows-SSD
Volume serial number is F095-E92B
C:.
├───bokor
│   ├───banan
│   ├───barack
│   └───mogyoro
├───fa
│   ├───banan
│   ├───korte
│   └───szeder
└───land
    ├───kokusz
    └───szeder

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>del ./land/szeder/tmp.txt
Invalid switch - "land".

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>del .\land\szeder\tmp.txt

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>del .\fa\szeder\tmp.txt
Could Not Find C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\fa\szeder\tmp.txt

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>del .\bokor\banan\tmp.txt
```

c) Végezze el a következő áthelyezéseket:

- a neptunkod /bokor/barack katalógust helyezze át a neptunkod /fa katalógusba
- a neptunkod /land /kokusz katalógust helyezze át a neptunkod/fa katalógusba

```
C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>move .\bokor\barack .\fa
        1 dir(s) moved.

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>move .\land\kokusz .\fa
        1 dir(s) moved.

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>tree
Folder PATH listing for volume Windows-SSD
Volume serial number is F095-E92B
C:.
├───bokor
│   ├───banan
│   └───mogyoro
├───fa
│   ├───banan
│   ├───barack
│   ├───kokusz
│   ├───korte
│   └───szeder
└───land
    └───szeder

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>
```

d) Törölje a neptunkod/land katalógust a teljes tartalmával. Hozza létre a következő szöveges állományokat:

- neptunkod/bokor/banan/ leiras.txt
- neptunkod/tree/felsorolas.txt

```
C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>rmdir /?
Removes (deletes) a directory.

RMDIR [/S] [/Q] [drive:]path
RD [/S] [/Q] [drive:]path

    /S      Removes all directories and files in the specified directory
            in addition to the directory itself.  Used to remove a directory
            tree.

    /Q      Quiet mode, do not ask if ok to remove a directory tree with /S

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>rmdir /S land
land, Are you sure (Y/N)? Y

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>tree
Folder PATH listing for volume Windows-SSD
Volume serial number is F095-E92B
C:.
├───bokor
│   ├───banan
│   └───mogyoro
└───fa
    ├───banan
    ├───barack
    ├───kokusz
    ├───korte
    └───szeder

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>
```

```
C:\Users\encip\OneDrive\Asztali gép\YD11NL\fa>type leiras.txt

C:\Users\encip\OneDrive\Asztali gép\YD11NL\fa>cd ..

C:\Users\encip\OneDrive\Asztali gép\YD11NL>cd bokor\banan

C:\Users\encip\OneDrive\Asztali gép\YD11NL\bokor\banan>write >leiras.txt

C:\Users\encip\OneDrive\Asztali gép\YD11NL\bokor\banan>type leiras.txt

C:\Users\encip\OneDrive\Asztali gép\YD11NL\bokor\banan>cd ..

C:\Users\encip\OneDrive\Asztali gép\YD11NL\bokor>cd ..

C:\Users\encip\OneDrive\Asztali gép\YD11NL>del leiras.txt
Could Not Find C:\Users\encip\OneDrive\Asztali gép\YD11NL\leiras.txt

C:\Users\encip\OneDrive\Asztali gép\YD11NL>cd fa

C:\Users\encip\OneDrive\Asztali gép\YD11NL\fa>del leiras.txt

C:\Users\encip\OneDrive\Asztali gép\YD11NL\fa>write >felsorolas.txt

C:\Users\encip\OneDrive\Asztali gép\YD11NL\fa>type felsorolas.txt

C:\Users\encip\OneDrive\Asztali gép\YD11NL\fa>dir
 Volume in drive C is Windows-SSD
 Volume Serial Number is F095-E92B

 Directory of C:\Users\encip\OneDrive\Asztali gép\YD11NL\fa

2022. 02. 16.  09:00    <DIR>          .
2022. 02. 16.  09:00    <DIR>          ..
2022. 02. 16.  08:45    <DIR>          banan
2022. 02. 16.  08:24    <DIR>          barack
2022. 02. 16.  09:00                 0 felsorolas.txt
2022. 02. 16.  08:25    <DIR>          kokusz
2022. 02. 16.  08:25    <DIR>          korte
2022. 02. 16.  08:44    <DIR>          szeder
               1 File(s)              0 bytes
               7 Dir(s)  106 206 851 072 bytes free
```

```
C:\Users\encip\OneDrive\Asztali gép\YD11NL\bokor>cd barack
A rendszer nem találja a megadott elérési utat.

C:\Users\encip\OneDrive\Asztali gép\YD11NL\bokor>cd banan

C:\Users\encip\OneDrive\Asztali gép\YD11NL\bokor\banan>dir
 Volume in drive C is Windows-SSD
 Volume Serial Number is F095-E92B

 Directory of C:\Users\encip\OneDrive\Asztali gép\YD11NL\bokor\banan

2022. 02. 16.  08:58    <DIR>          .
2022. 02. 16.  08:58    <DIR>          ..
2022. 02. 16.  08:58                 0 leiras.txt
               1 File(s)              0 bytes
               2 Dir(s)  106 206 130 176 bytes free
```

e) A leiras.txt szöveges állományba írjon 3 sort a barackról. A felsorolas szöveges állományba soroljon fel legalább 5 csoporttársa nevét.

```
C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\bokor\banan>echo A barack sarga szinu>leiras.txt

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\bokor\banan>echo A barack gyumolcs>>leiras.txt

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\bokor\banan>echo A barackot szeretik a gyerekek>>leiras.txt

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\bokor\banan>type leiras.txt
A barack sarga szinu
A barack gyumolcs
A barackot szeretik a gyerekek

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\bokor\banan>
```

```
C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\fa>echo Pazman Andras>felsorolas.txt

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\fa>echo Dobai Attila>>felsorolas.txt

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\fa>echo Gerocs Gergo>>felsorolas.txt

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\fa>echo Sikora David>>felsorolas.txt

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\fa>echo Nagy Bence>>felsorolas.txt

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\fa>type felsorolas.txt
Pazman Andras
Dobai Attila
Gerocs Gergo
Sikora David
Nagy Bence
```

f) Listázza a neptunkod mappa tartalmát úgy, hogy megjelenjen az almappák tartalma is.

```
C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>dir /S
 Volume in drive C is Windows-SSD
 Volume Serial Number is F095-E92B

 Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL

2022. 02. 16.  13:58    <DIR>          .
2022. 02. 16.  13:58    <DIR>          ..
2022. 02. 16.  13:56    <DIR>          bokor
2022. 02. 16.  14:02    <DIR>          fa
               0 File(s)              0 bytes

 Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\bokor

2022. 02. 16.  13:56    <DIR>          .
2022. 02. 16.  13:56    <DIR>          ..
2022. 02. 16.  14:01    <DIR>          banan
2022. 02. 16.  13:22    <DIR>          mogyoro
               0 File(s)              0 bytes

 Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\bokor\banan

2022. 02. 16.  14:01    <DIR>          .
2022. 02. 16.  14:01    <DIR>          ..
2022. 02. 16.  14:40                73 leiras.txt
               1 File(s)             73 bytes

 Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\bokor\mogyoro

2022. 02. 16.  13:22    <DIR>          .
2022. 02. 16.  13:22    <DIR>          ..
               0 File(s)              0 bytes

 Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\fa

2022. 02. 16.  14:02    <DIR>          .
2022. 02. 16.  14:02    <DIR>          ..
2022. 02. 16.  14:01    <DIR>          banan
2022. 02. 16.  13:42    <DIR>          barack
2022. 02. 16.  14:44                69 felsorolas.txt
2022. 02. 16.  13:25    <DIR>          kokusz
2022. 02. 16.  13:22    <DIR>          korte
2022. 02. 16.  13:46    <DIR>          szeder
```

```
2022. 02. 16.  14:01    <DIR>          .
2022. 02. 16.  14:01    <DIR>          ..
               0 File(s)              0 bytes

 Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\fa\barack

2022. 02. 16.  13:42    <DIR>          .
2022. 02. 16.  13:42    <DIR>          ..
               0 File(s)              0 bytes

 Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\fa\kokusz

2022. 02. 16.  13:25    <DIR>          .
2022. 02. 16.  13:25    <DIR>          ..
               0 File(s)              0 bytes

 Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\fa\korte

2022. 02. 16.  13:22    <DIR>          .
2022. 02. 16.  13:22    <DIR>          ..
               0 File(s)              0 bytes

 Directory of C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\fa\szeder

2022. 02. 16.  13:46    <DIR>          .
2022. 02. 16.  13:46    <DIR>          ..
               0 File(s)              0 bytes

     Total Files Listed:
               2 File(s)            142 bytes
              29 Dir(s)  105 929 854 976 bytes free

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL>
```

g.) Térjen vissza a gyökérmappába és keresse meg az összes olyan file-t, amelyek nevének második betűje e.

```
C:\Users\encip\OneDrive\Asztali gép\YD11NL>dir ?e* /s
 Volume in drive C is Windows-SSD
 Volume Serial Number is F095-E92B

 Directory of C:\Users\encip\OneDrive\Asztali gép\YD11NL\bokor\banan

2022. 02. 16.  09:05                58 leiras.txt
               1 File(s)             58 bytes

 Directory of C:\Users\encip\OneDrive\Asztali gép\YD11NL\fa

2022. 02. 16.  09:12                70 felsorolas.txt
               1 File(s)             70 bytes

    Total Files Listed:
               2 File(s)            128 bytes
               0 Dir(s)  106 209 079 296 bytes free
```

h.) Tegye mindenki számára olvashatóvá a felsorolas.txt file-t.

```
C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\fa>icacls felsorolas.txt
felsorolas.txt NT AUTHORITY\SYSTEM:(I)(F)
               BUILTIN\Rendszergazdák:(I)(F)
               LAPTOP-4BJLNKVT\encip:(I)(F)

Successfully processed 1 files; Failed processing 0 files

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\fa>icacls felsorolas.txt /grant mindenki:(R)
processed file: felsorolas.txt
Successfully processed 1 files; Failed processing 0 files

C:\Users\encip\OneDrive\Asztali gép\Mappam\YD11NL\fa>icacls felsorolas.txt
felsorolas.txt Mindenki:(R)
               NT AUTHORITY\SYSTEM:(I)(F)
               BUILTIN\Rendszergazdák:(I)(F)
               LAPTOP-4BJLNKVT\encip:(I)(F)

Successfully processed 1 files; Failed processing 0 files
```

i.) Jelenítse meg, hogy mennyi helyet foglal a merevlemezen a neptunkod mappa az almappáival együtt.

```
    Total Files Listed:
               2 File(s)            142 bytes
              29 Dir(s)  105 930 055 680 bytes free
```

j.) Rendezze ABC-szerint a felsorolas.txt file tartalmát

```
C:\Users\encip\OneDrive\Asztali gép\YD11NL>cd fa

C:\Users\encip\OneDrive\Asztali gép\YD11NL\fa>type felsorolas.txt
Dobai Attila
Sikora David
Gerocs Gergo
Nagy Bence
Pazman Andras

C:\Users\encip\OneDrive\Asztali gép\YD11NL\fa>sort felsorolas.txt
Dobai Attila
Gerocs Gergo
Nagy Bence
Pazman Andras
Sikora David
```

```
C:\Users\encip\OneDrive\Asztali gép\YD11NL\fa>sort felsorolas.txt /OUTPUT felsorolas2.txt

C:\Users\encip\OneDrive\Asztali gép\YD11NL\fa>type felsorolas2.txt
Dobai Attila
Gerocs Gergo
Nagy Bence
Pazman Andras
Sikora David
```

2.Feladat

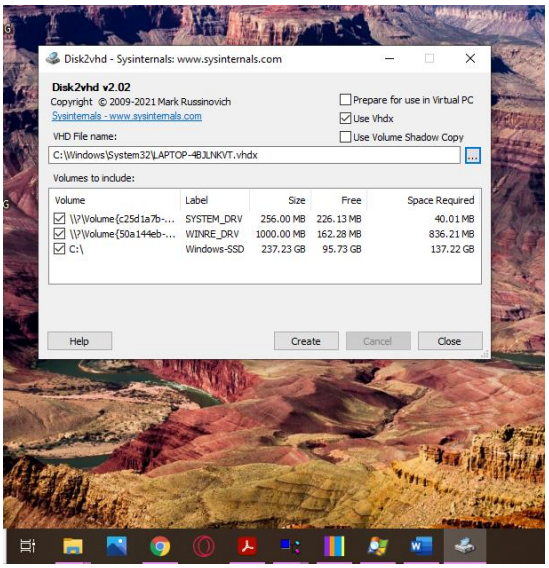
A felsorolt eszközök közül minden eszköz esetén töltse le, futtassa - és írja le a program szolgáltatásait és a futtatás eredményét - majd mentse el a feladat számával a megadott jegyzőkönyvbe (képernyőkép is).

a) File and Disk Utilities (Disk2vhd)

Szolgáltatások:

- virtuális másolat készítése fizikai lemezekről (virtuális géphez való használatra)
- egyszerű felület, 3 opcióval (Vhdx használata, felkészülés Virtuális PC-s használatra, árnyékmásolatok – azaz biztonsági mentések), valamint path választással

Eredmények: a képen látható, másolatot nem készítettem (nem is lett volna neki hely)

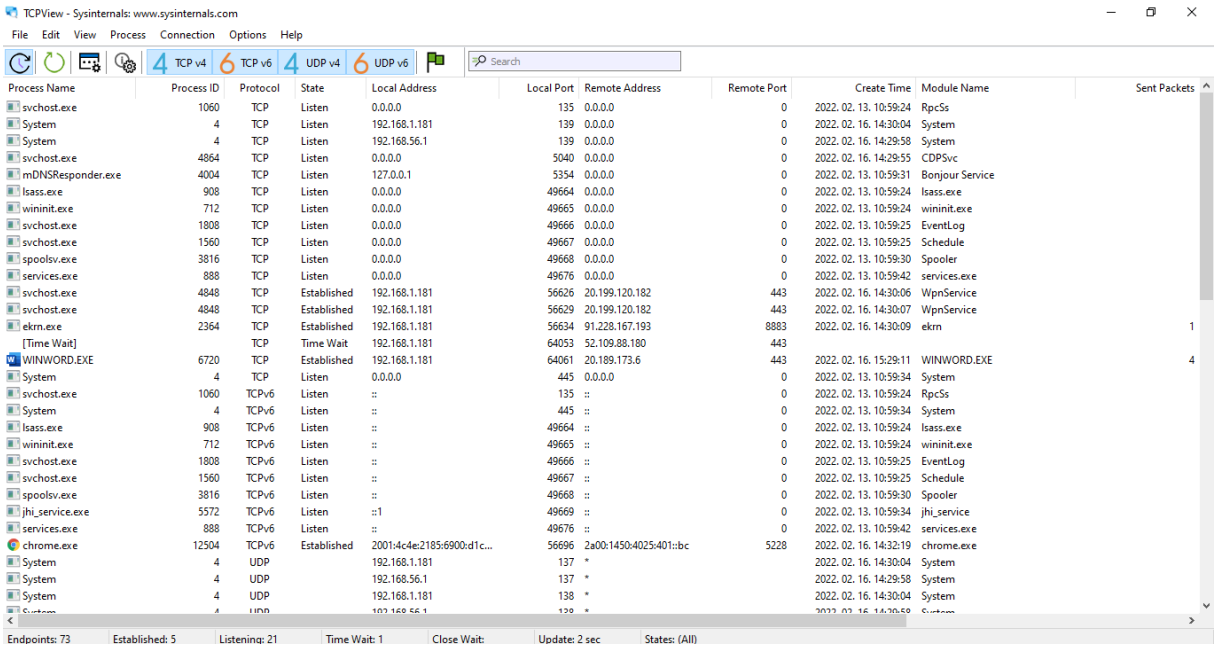


b) Networking Utilities (TCPView)

Szolgáltatások:

- megmutatja és részletezi a rendszer TCP és UDP végpontjait (IP címek)
- helyi és távoli címeket is mutat
- a TCP kapcsolatok állapotát jelzi (listen, established, wait)
- a hálózaton elküldött és fogadott csomagok, valamint bájtok számát tartja nyilván

Eredmények: (kép) Látható például, hogy a böngészésre használt chrome.exe folyamatosan kommunikál a szerverrel (30ezer feletti a küldött és a fogadott byte szám is), akárcsak a szövegszerkesztő winword.exe-je, de az Eset víruskereső is folyamatosan TCP kapcsolatban áll a távoli szerverrel.

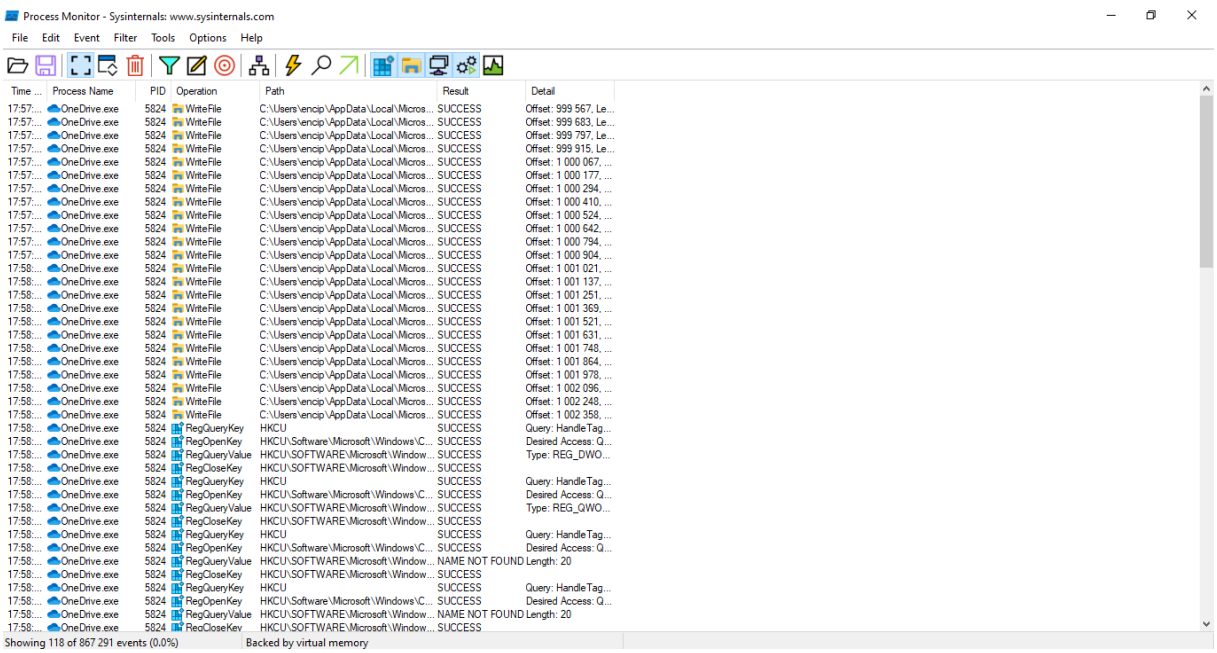


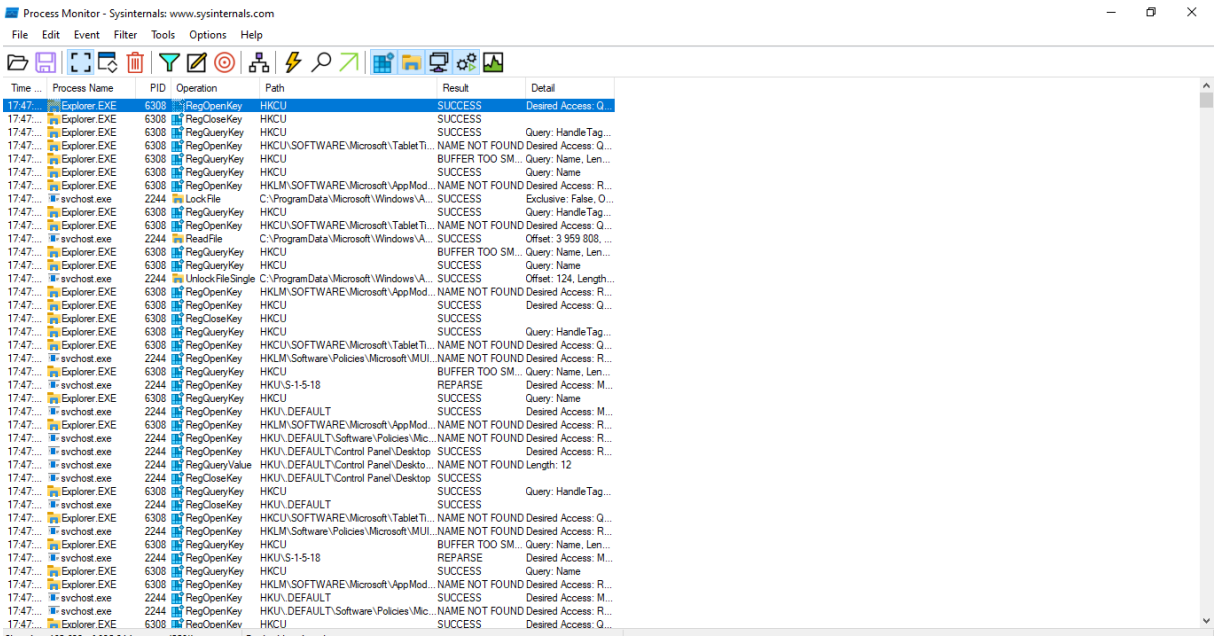
c) Process Utilities (Process Explorer, Process Monitor, AutoRuns)

Szolgáltatások – Process Monitor:

- valós időben mutatja a fájlrendszert és a processzeket, lehetővé teszi a szűrést is
- használhatjuk arra, hogy detektáljuk a sikertelen szerkesztését a Windows konfigurációs adatbázisának

Eredmények: Valóban valós időben fut és frissül a lista, a szűréseknek köszönhetően pedig rá lehet koncentrálni arra a területre, ahol problémát tapasztalunk. A program használható például arra, hogy kiderítsük, milyen függés mi tart nyitva egy fájlt, megakadályozva ezzel, hogy más programmal hozzáférhessünk annak tartalmához. Látható például, hogy amikor elmentem ezt a fájlt, a OneDrive.exe WriteFile műveletet végez.

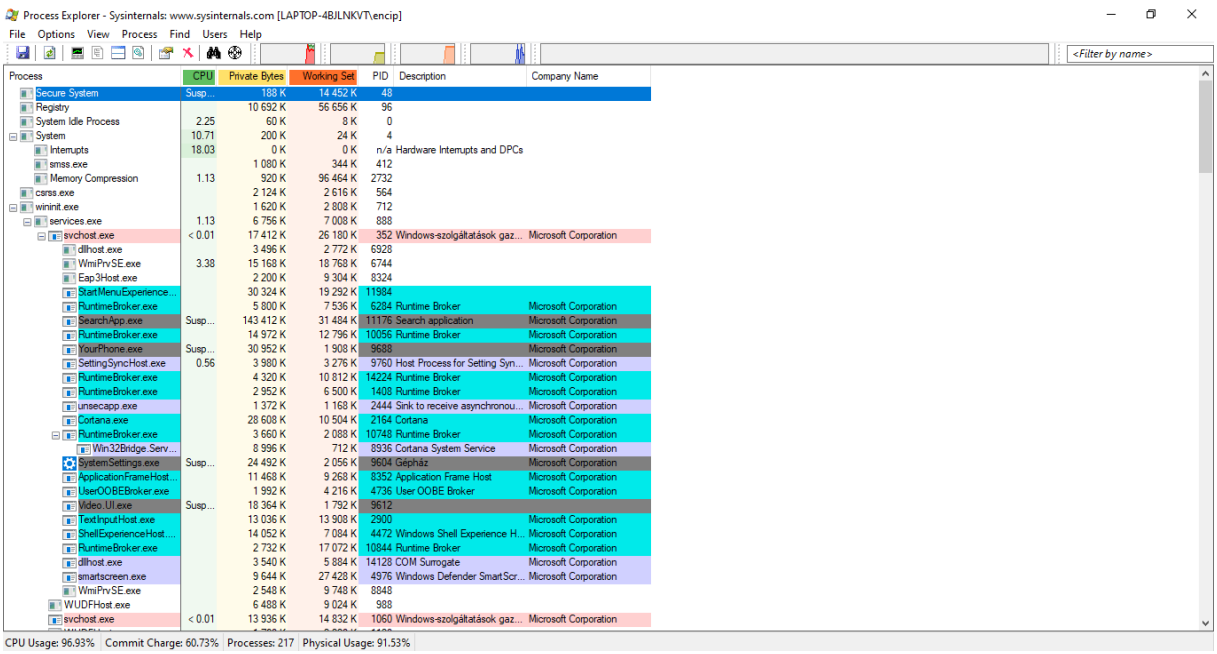




Szolgáltatások – Process Explorer:

- információt ad a CPU használatról, a futó processzek számáról, a memóriahasználatról, a GPU és I/O használatról (a System Information ablakban grafikonok jeleníthetők meg)
- listázza az éppen aktív processzeket, azonosítóval, és a fenti információkkal együtt
- processzeket tudunk leállítani, felfüggeszteni, újraindítani

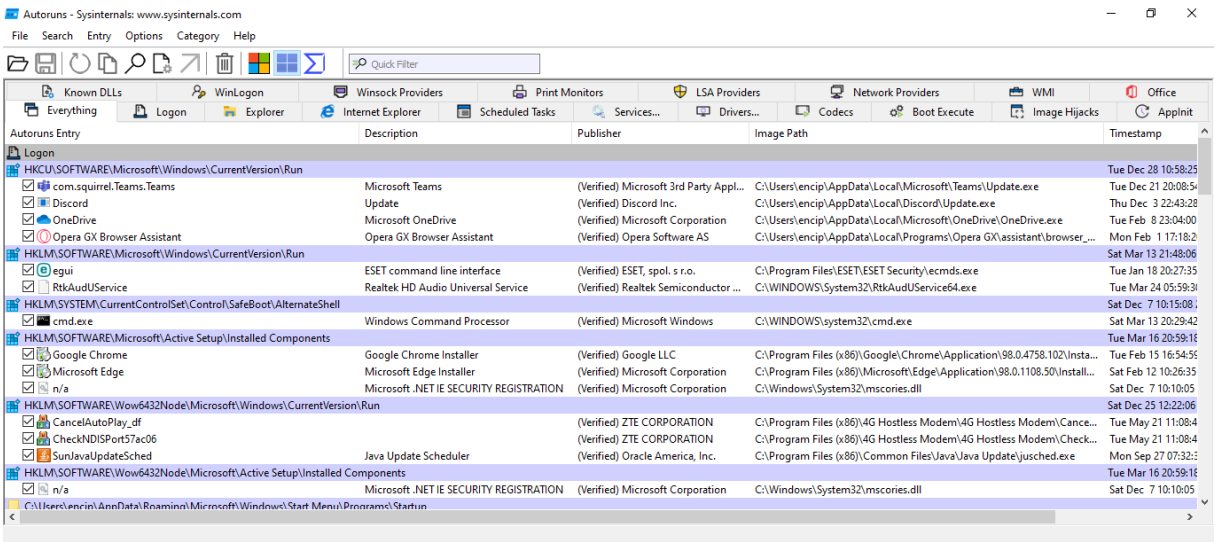
Eredmények: körülbelül 200 aktív processz, 60%-os processzorhasználat (kép). A Dependency Walker CPU használata olyan magas volt, hogy azonnal be is zártam, ne fusson a háttérben feleslegesen. Teszt: a Process Explorer felett a Wordbe írok, mire valóban megnő a CPU használata a winword.exének.



Szolgáltatások – Autoruns:

- azt lehet megnézni, mely programok indulnak el automatikusan a Windows-zal, bejelentkezéskor
- kategóriákra bontva is megtekinthetjük
- információkat kapunk a programok kibocsátójáról, az elérési útvonalukról
- különböző színek jelzik például, ha az Autoruns nem találja meg a program kibocsátóját, vagy az nem ellenőrzött gyártó
- segítségével kiszűrhetjük a vírusokat, melyek futása automatikusan, a Windows-zal együtt indul, ezeket le is tudjuk törölni a listáról, ezáltal megelőzhetjük, hogy a legközelebbi indításkor futni kezdjenek
- lehetővé teszi azt is, hogy ha egy listát elmentünk, egy későbbi időpontban megnézhetjük (compare), melyek az újonnan megjelent programok a listában

A futtatás eredménye: (kép) A listában szerepel a OneDrive, a Teams és a Discord, az Eset víruskereső parancssori interfésze, vagy a Java frissítés ütemezője. A listában szerepelnek driverek (pl: Bluetooth driver) és ütemezett feladatok is (pl: Microsoft Office updaterek, melyek lehetővé teszik az Installernek, hogy frissítéseket keressen).

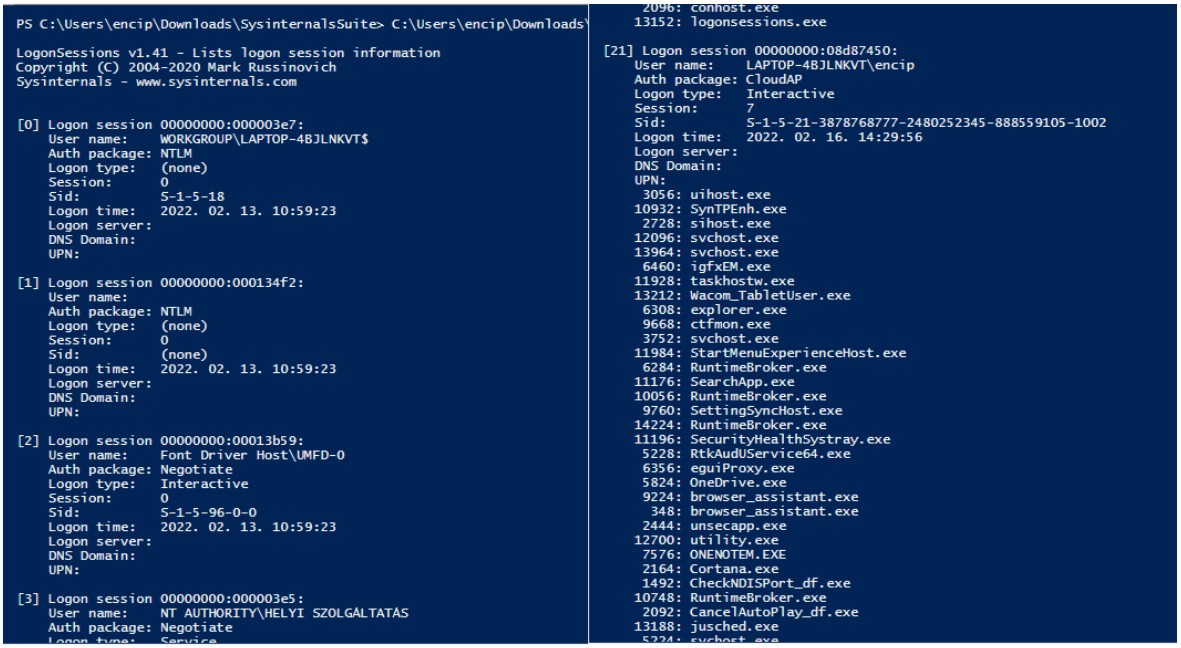


d) Security Utilities (LogonSession)

Szolgáltatások – Autoruns:

- kilistázza az aktív belépéseket, a létesített üléseket, azok azonosítóit, a belépő nevét és a belépés típusát, továbbá a belépés pontos idejét
- információt ad a DNS domainről és a belépéshez használt szerverről is

A futtatás eredménye: (kép) A program csak Powershellben, adminisztrátorként megnyitva futott. Kilistázta az aktív belépéseimet, az üléseket megszámozva, így képet kaptam arról, pontosan mikor használtam a számítógépet. Láthattam például azt is, hogy 13-án a Font Driver Host általi belépés történt a Windowsra, ami azóta is aktív. A -p kapcsolóval a belépéskor futó programokat is kilistáztam.

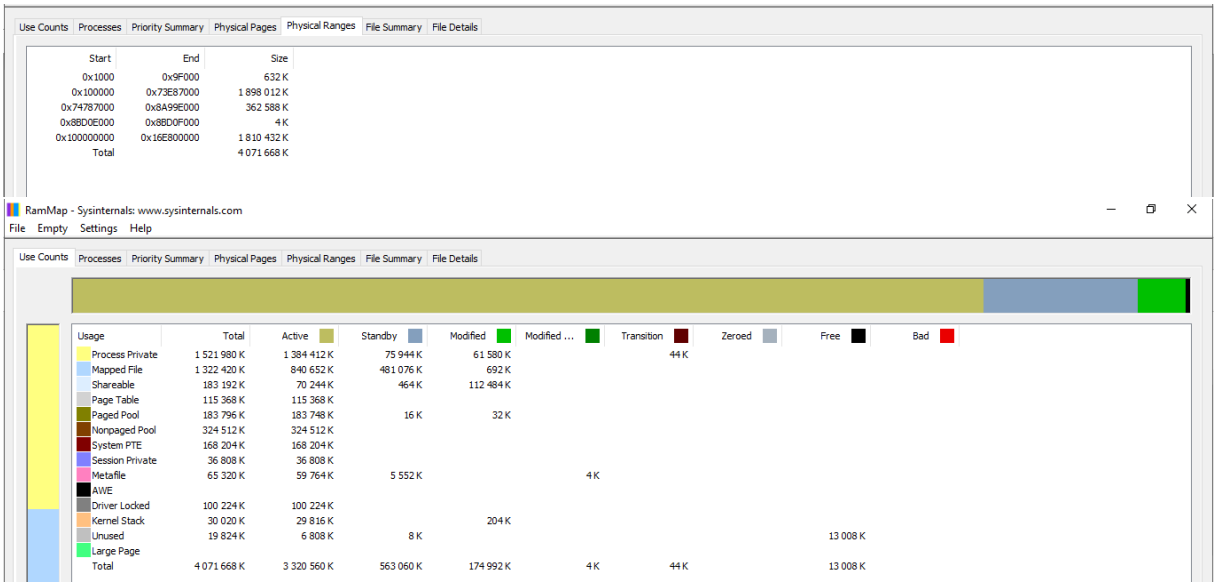


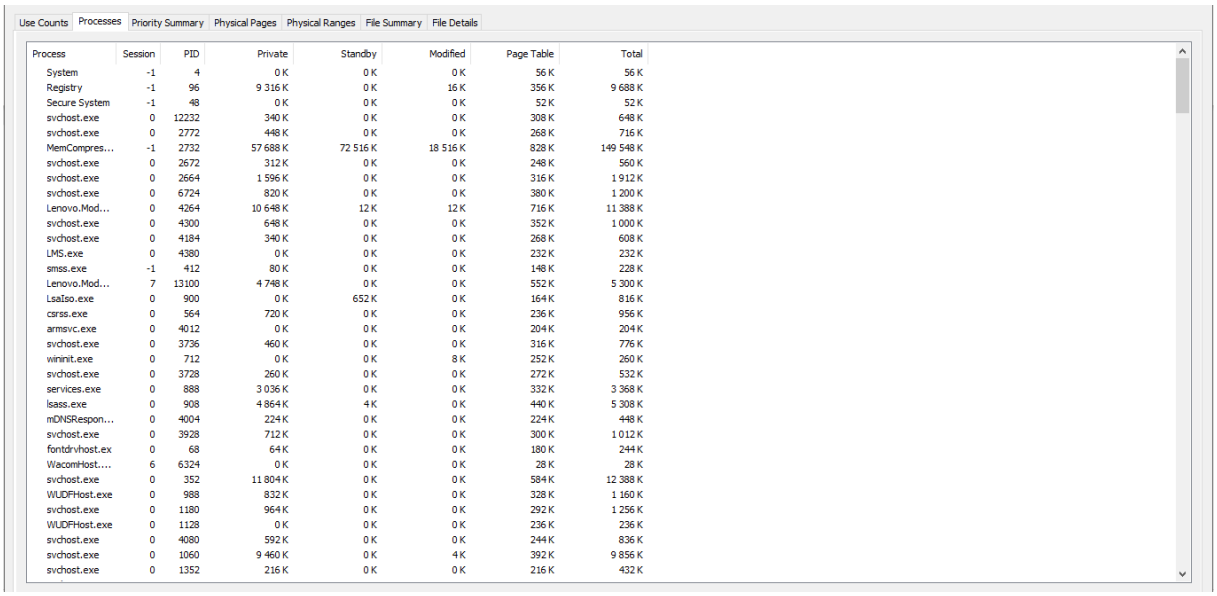
e) Information Utilities (RAMMap)

Szolgáltatások:

- megmutatja, hogyan menedzseli a Windows a memóriát az eszközön
- láthatjuk a processzek memóriahasználatát, a fizikai címekhez társított virtuális címeket
- megmutatja a fájlok méretét, pontos helyét az eszközön

A futtatás eredménye: (képek) Megtekinthetők például a VirtualBox, az Eset, a CodeBlocks és számos dll fájl prioritási szintje, fizikai címei, az általuk foglalt memória mérete, a fizikai címtartományok és a memórialapok, valamint egy összesítés az aktív és a standby RAMról.





Process	Session	PID	Private	Standby	Modified	Page Table	Total
System	-1	4	0 K	0 K	0 K	56 K	56 K
Registry	-1	96	9 316 K	0 K	16 K	356 K	9 688 K
Secure System	-1	48	0 K	0 K	0 K	52 K	52 K
svchost.exe	0	12232	340 K	0 K	0 K	308 K	648 K
svchost.exe	0	2772	448 K	0 K	0 K	268 K	716 K
MemCompres...	-1	2732	57 688 K	72 516 K	18 516 K	828 K	149 548 K
svchost.exe	0	2672	312 K	0 K	0 K	248 K	560 K
svchost.exe	0	2664	1 596 K	0 K	0 K	316 K	1 912 K
svchost.exe	0	6724	820 K	0 K	0 K	380 K	1 200 K
Lenovo.Mod...	0	4264	10 648 K	12 K	12 K	716 K	11 388 K
svchost.exe	0	4300	648 K	0 K	0 K	352 K	1 000 K
svchost.exe	0	4184	340 K	0 K	0 K	268 K	608 K
LMS.exe	0	4380	0 K	0 K	0 K	232 K	232 K
smss.exe	-1	412	80 K	0 K	0 K	148 K	228 K
Lenovo.Mod...	7	13100	4 748 K	0 K	0 K	552 K	5 300 K
LsaIso.exe	0	900	0 K	652 K	0 K	164 K	816 K
csrss.exe	0	564	720 K	0 K	0 K	236 K	956 K
armsvc.exe	0	4012	0 K	0 K	0 K	204 K	204 K
svchost.exe	0	3736	460 K	0 K	0 K	316 K	776 K
wininit.exe	0	712	0 K	0 K	8 K	252 K	260 K
svchost.exe	0	3728	260 K	0 K	0 K	272 K	532 K
services.exe	0	888	3 036 K	0 K	0 K	332 K	3 368 K
lsass.exe	0	908	4 864 K	4 K	0 K	440 K	5 308 K
mDNSRespon...	0	4004	224 K	0 K	0 K	224 K	448 K
svchost.exe	0	3928	712 K	0 K	0 K	300 K	1 012 K
fontdrvhost.ex	0	68	64 K	0 K	0 K	180 K	244 K
WacomHost....	6	6324	0 K	0 K	0 K	28 K	28 K
svchost.exe	0	352	11 804 K	0 K	0 K	584 K	12 388 K
WUDFHost.exe	0	988	832 K	0 K	0 K	328 K	1 160 K
svchost.exe	0	1180	964 K	0 K	0 K	292 K	1 256 K
WUDFHost.exe	0	1128	0 K	0 K	0 K	236 K	236 K
svchost.exe	0	4080	592 K	0 K	0 K	244 K	836 K
svchost.exe	0	1060	9 460 K	0 K	4 K	392 K	9 856 K
svchost.exe	0	1352	216 K	0 K	0 K	216 K	432 K

3.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, majd tegye futtathatóvá az állományt: *neptunkod.exe*

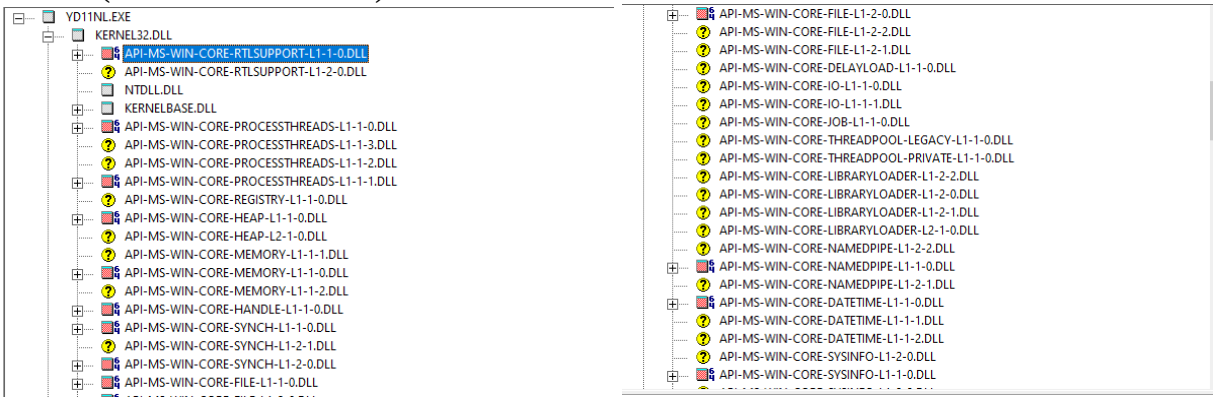
```
C:\Users\encip\OneDrive\Asztali gép\Mappam>gcc YD11NL.c -o YD11NL

C:\Users\encip\OneDrive\Asztali gép\Mappam>YD11NL.exe

C:\Users\encip\OneDrive\Asztali gép\Mappam>type palencsar.txt
Nev: Palencsar Eniko
Neptun: YD11NL
Szak: Mernokinformatikus
Kepzes: nappali
Szint: Bsc
C:\Users\encip\OneDrive\Asztali gép\Mappam>
```

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)!

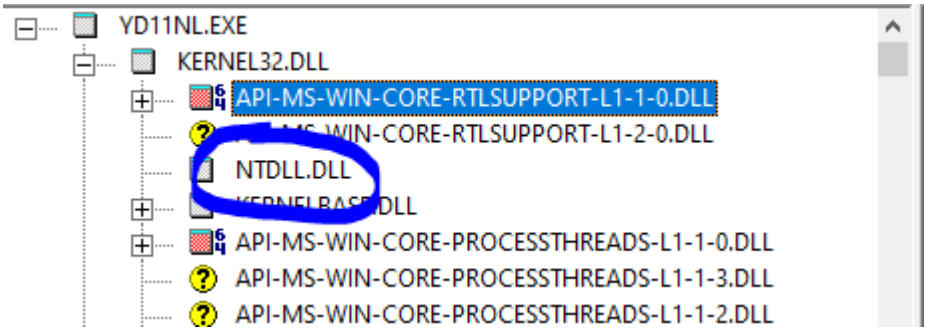


…

Ebben a viszonylag kicsi programban is rengeteg API hívás történik, melyek a teljesség igénye nélkül kapcsolatosak: processz szálakkal, a kupac kezelésével, a memóriával, a szinkronizációval, a fájlkezeléssel, az inputtal/outputtal, a konzollal, a debuggolással és a hibajelzéssel. Van köztük rendszerinformációkkal és könyvtárbetöltéssel kapcsolatos API is.

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

Az NTDLL.DLL fájl kernel függvényeket tartalmaz, a Windows Native API-t exportálja, mely az OS user-módbeli komponensei (melyeknek a Win32 és egyéb API alrendszerek nélkül kell futniuk) által használt interfész. Éppen ezért nagyon fontos rendszerfájl, a user mód és a kernel mód határán.



Az exportált függvények között szerepel például az RtlCreateHeap, ami kupac memóriaterületet hoz létre, vannak továbbá virtuális memória allokáló, hozzáférést ellenőrző függvények is.

E	Ordinal ^	Hint	Function	Entry Point
C	852 (0x0354)	838 (0x0346)	RtlCreateActivationContext	0x000632E0
C	853 (0x0355)	839 (0x0347)	RtlCreateAndSetSD	0x000B5D90
C	854 (0x0356)	840 (0x0348)	RtlCreateAtomTable	0x00060050
C	855 (0x0357)	841 (0x0349)	RtlCreateBootStatusDataFile	0x000D0B10
C	856 (0x0358)	842 (0x034A)	RtlCreateBoundaryDescriptor	0x0002A210
C	857 (0x0359)	843 (0x034B)	RtlCreateEnvironment	0x0005AD10
C	858 (0x035A)	844 (0x034C)	RtlCreateEnvironmentEx	0x0005AD40
C	859 (0x035B)	845 (0x034D)	RtlCreateHashTable	0x000DAFB0
C	860 (0x035C)	846 (0x034E)	RtlCreateHashTableEx	0x000DAFE0
C	861 (0x035D)	847 (0x034F)	RtlCreateHeap	0x00040FA0
C	862 (0x035E)	848 (0x0350)	RtlCreateMemoryBlockLookaside	0x0002A990
C	863 (0x035F)	849 (0x0351)	RtlCreateMemoryZone	0x0002AAF0
C	864 (0x0360)	850 (0x0352)	RtlCreateProcessParameters	0x000B5A90
C	865 (0x0361)	851 (0x0353)	RtlCreateProcessParametersEx	0x000B5AD0
C	866 (0x0362)	852 (0x0354)	RtlCreateProcessParametersWithTemplate	0x000282C0

E	Ordinal ^	Hint	Function	Entry Point
C	205 (0x00CD)	190 (0x00BE)	NlsMbCodePageTag	0x00126930
C	206 (0x00CE)	191 (0x00BF)	NlsMbOemCodePageTag	0x00126918
C	207 (0x00CF)	192 (0x00C0)	NtAcceptConnectPort	0x000729D0
C	208 (0x00D0)	193 (0x00C1)	NtAccessCheck	0x000729B0
C	209 (0x00D1)	194 (0x00C2)	NtAccessCheckAndAuditAlarm	0x00072C60
C	210 (0x00D2)	195 (0x00C3)	NtAccessCheckByType	0x00073000
C	211 (0x00D3)	196 (0x00C4)	NtAccessCheckByTypeAndAuditAlarm	0x00072F60
C	212 (0x00D4)	197 (0x00C5)	NtAccessCheckByTypeResultList	0x00073010
C	213 (0x00D5)	198 (0x00C6)	NtAccessCheckByTypeResultListAndAuditAlarm	0x00073020
C	214 (0x00D6)	199 (0x00C7)	NtAccessCheckByTypeResultListAndAuditAlarmByHandle	0x00073030
C	215 (0x00D7)	200 (0x00C8)	NtAcquireCrossVmMutant	0x00073040
C	216 (0x00D8)	201 (0x00C9)	NtAcquireProcessActivityReference	0x00073050
C	217 (0x00D9)	202 (0x00CA)	NtAddAtom	0x00072E40
C	218 (0x00DA)	203 (0x00CB)	NtAddAtomEx	0x00073060
C	219 (0x00DB)	204 (0x00CC)	NtAddBootEntry	0x00073070

Mentés: Írja le a program szolgáltatásait és a futtatás eredményét a feladat számával a megadott jegyzőkönyvbe (képernyőkép is).

Szolgáltatások:

- egy alkalmazás függőségeinek vizsgálata, az általa használt API-k megismerése
- importált és exportált függvények listázása
- mindazon elemek faszerkezetbe rendezése, melyek egy adott program futásához szükségesek, ez könnyebbé teszi a problémák forrásának megtalálását
- általános rendszerinformációk lekérdezése