

Operációs rendszerek BSc

2.Gyak.

2022. 02. 15.

Készítette:

Görög Krisztina Erzsébet BSc

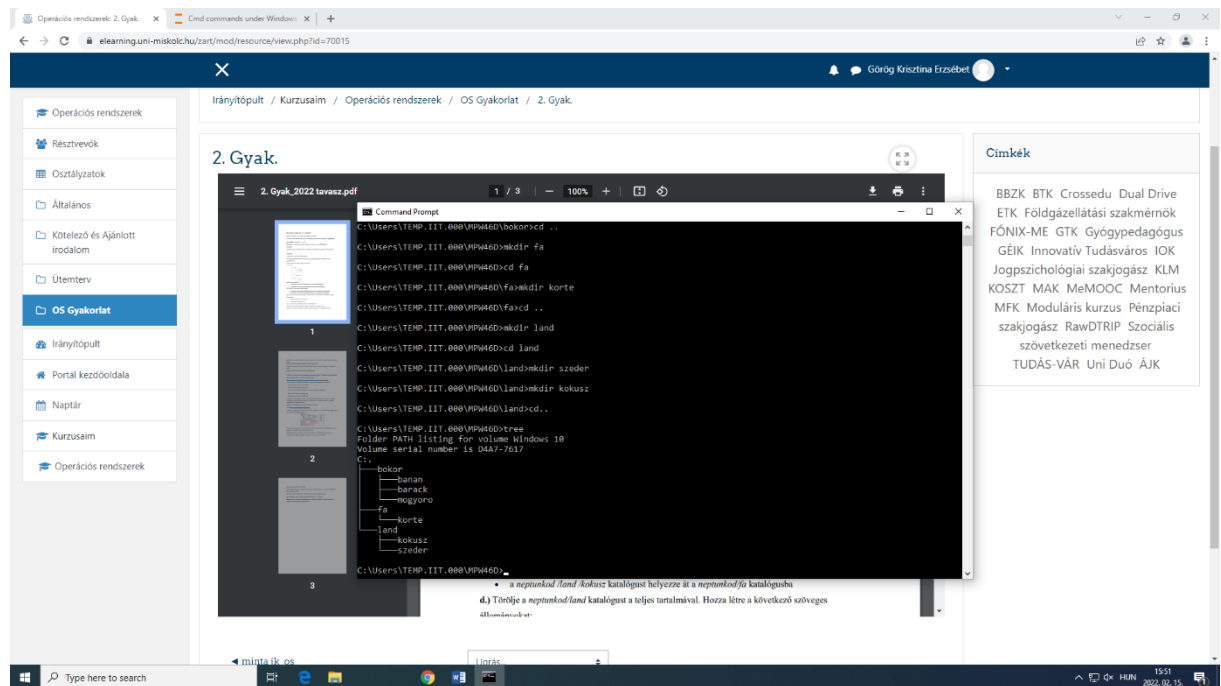
Programtervező informatikus

MPW46D

Miskolc, 2022

1. feladat

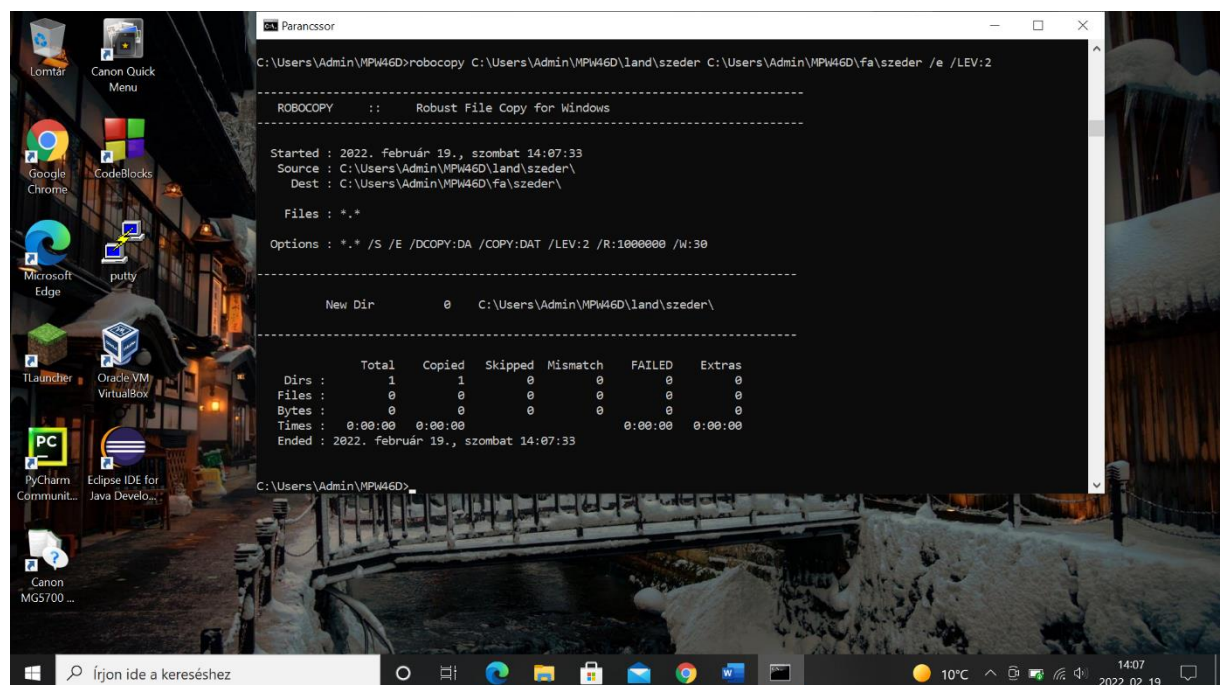
a.) Képernyőkép készítése a mappaszerkezeetről, amit a tree parancs segítségével jelenítettünk meg.



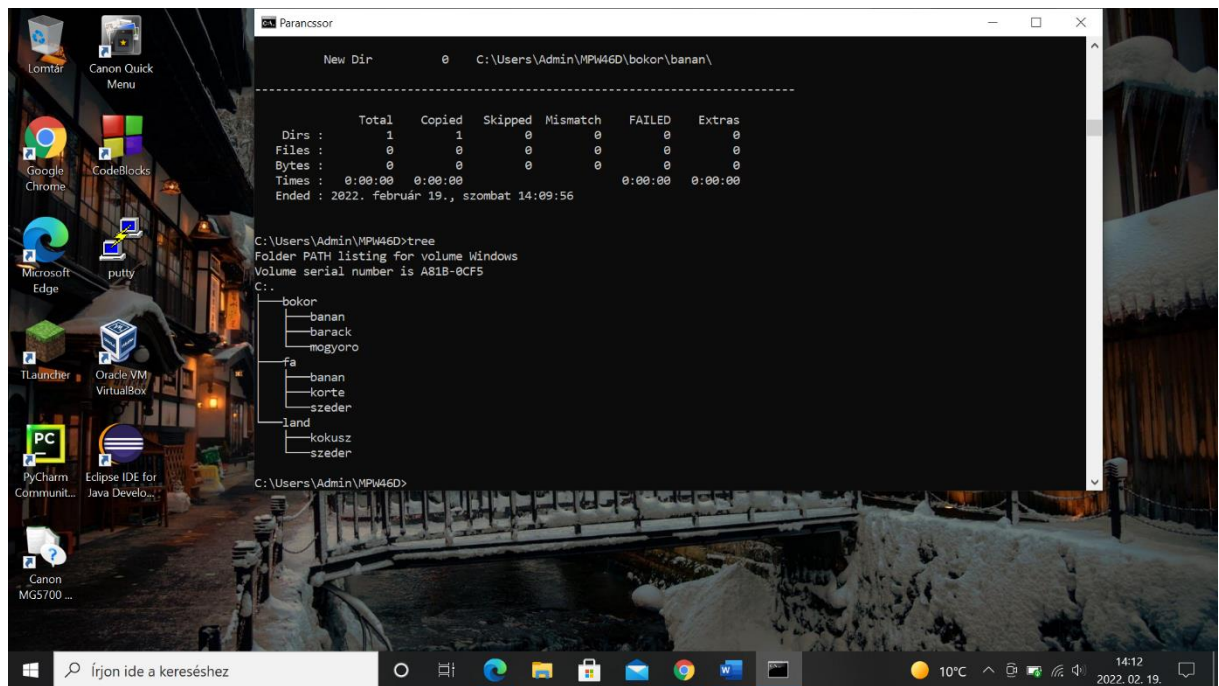
b.)

Másolatok készítése:

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



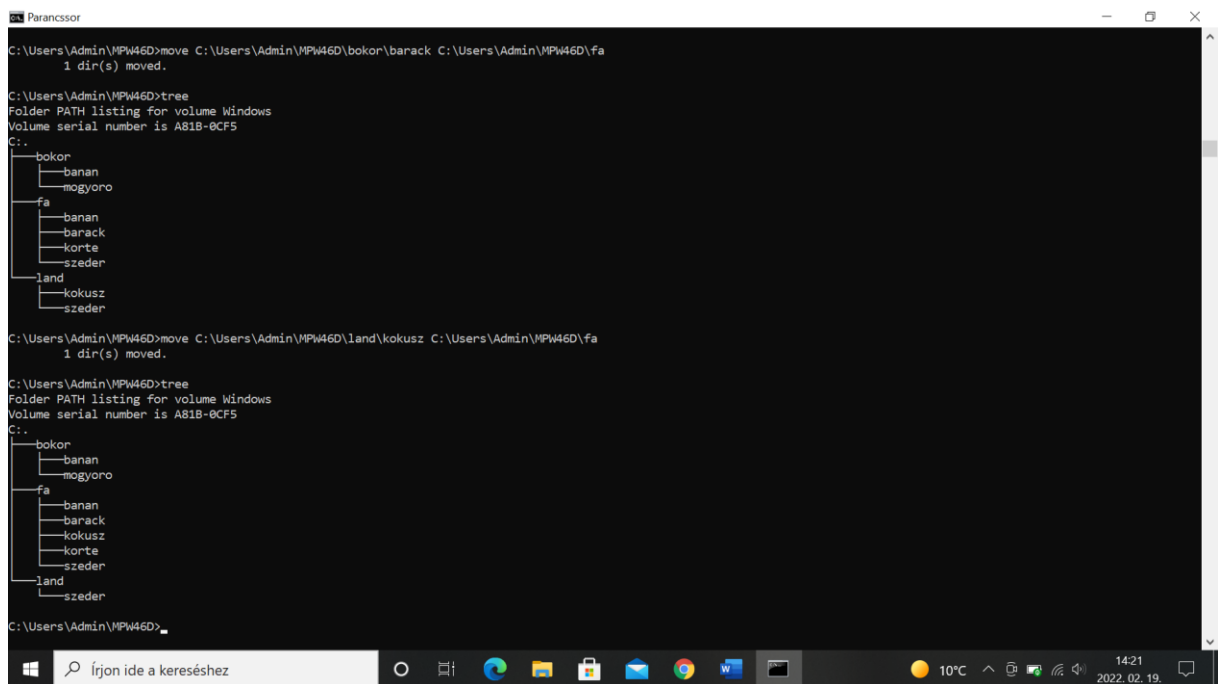
- a neptunkod /bokor/banan katalógusról a neptunkod /fa katalógusba



Mindkétszer a robocopy segítségével másolunk.

c.) A következő katalógusok áthelyezése:

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



A mappákat a move segítségével mozgatjuk.

d.) Töröljük a neptunkod/land katalógust a teljes tartalmával. Létre hozzuk a következőket:

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

```
Parancssor
Microsoft Windows [Version 10.0.19041.1415]
(c) Microsoft Corporation. Minden jog fenntartva.

C:\Users\Admin>cd MPW46D

C:\Users\Admin\MPW46D>rmdir land /S
land, Are you sure (Y/N)? y

C:\Users\Admin\MPW46D>tree
Folder PATH listing for volume Windows
Volume serial number is A81B-6CF5
C:.
|-- bokor
|   |-- banan
|   |-- mogyoro
|   |-- fa
|       |-- banan
|       |-- barack
|       |-- kokusz
|       |-- korte
|       |-- szeder
|
|-- ...

C:\Users\Admin\MPW46D>cd bokor

C:\Users\Admin\MPW46D\bokor>cd banan

C:\Users\Admin\MPW46D\bokor\banan>notepad leiras.txt

C:\Users\Admin\MPW46D\bokor\banan>cd ..

C:\Users\Admin\MPW46D\bokor>cd ..

C:\Users\Admin\MPW46D>cd fa

C:\Users\Admin\MPW46D\fa>notepad felsorolas.txt

C:\Users\Admin\MPW46D\fa>
```

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

```
Parancssor
C:\Users\Admin\MPW46D\fa>notepad felsorolas.txt

C:\Users\Admin\MPW46D\fa>cd ..

C:\Users\Admin\MPW46D>cd bokor

C:\Users\Admin\MPW46D\bokor>cd banan

C:\Users\Admin\MPW46D\bokor\banan>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Admin\MPW46D\bokor\banan>list
'list' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Admin\MPW46D\bokor\banan>notepad leiras.txt

C:\Users\Admin\MPW46D\bokor\banan>echo "A barack egy gyumolcs. Nagyon egeszseges, sok vitamint tartalmaz. Az egyhebb eghajlatu videkeken terem." > leiras.txt

C:\Users\Admin\MPW46D\bokor\banan>notepad leiras.txt

C:\Users\Admin\MPW46D\bokor\banan>cd ..

C:\Users\Admin\MPW46D\bokor>cd ..

C:\Users\Admin\MPW46D>cd fa

C:\Users\Admin\MPW46D\fa>echo "Hajdu Adrian, Karczub Roland, Kaskoto Gergo, Keresztes Julia, Kormos Balazs" > felsorolas.txt

C:\Users\Admin\MPW46D\fa>notepad felsorolas.txt

C:\Users\Admin\MPW46D\fa>
```

f.) A neptunkod almappa tartalmának listázása úgy, hogy megjelenjen az almappák tartalma is.

```
Parancssor
C:\Users\Admin\MPW46D\bokor\banan>list
'list' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Admin\MPW46D\bokor\banan>notepad leiras.txt

C:\Users\Admin\MPW46D\bokor\banan>echo "A barack egy gyumolcs. Nagyon eszsegzes, sok vitamint tartalmaz. Az egyhebb eghajlatu videkeken terem." > leiras.txt

C:\Users\Admin\MPW46D\bokor\banan>notepad leiras.txt

C:\Users\Admin\MPW46D\bokor\banan>cd ..

C:\Users\Admin\MPW46D\bokor>cd ..

C:\Users\Admin\MPW46D>cd fa

C:\Users\Admin\MPW46D\fa>echo "Hajdu Adrian, Karczub Roland, Kaskoto Gergo, Keresztes Julia, Kormos Balazs" > felsorolas.txt

C:\Users\Admin\MPW46D\fa>notepad felsorolas.txt

C:\Users\Admin\MPW46D\fa>cd ..

C:\Users\Admin\MPW46D>tree /F
Folder PATH listing for volume Windows
Volume serial number is A81B-0CF5
C:.
|-- bokor
|   |-- banan
|   |   |-- leiras.txt
|   |   |-- mogyoro
|   |-- fa
|       |-- felsorolas.txt
|       |-- banan
|       |-- barack
|       |-- kokusz
|       |-- korte
|       |-- szeder
--
```

g.) Olyan fájlok keresése, amiknek második betűje „e”.

```
Parancssor
C:\Users\Admin\MPW46D>dir ?e* /s
Volume in drive C is Windows
Volume Serial Number is A81B-0CF5

Directory of C:\Users\Admin\MPW46D\bokor\banan

2022. 02. 19.  18:34                108 leiras.txt
                1 File(s)                108 bytes

Directory of C:\Users\Admin\MPW46D\fa

2022. 02. 19.  18:40                 80 felsorolas.txt
                1 File(s)                 80 bytes

Total Files Listed:
                2 File(s)                188 bytes
                0 Dir(s) 186 731 360 256 bytes free

C:\Users\Admin\MPW46D>cd desktop
A rendszer nem találja a megadott elérési utat.

C:\Users\Admin\MPW46D>cd ..

C:\Users\Admin>dir ?e* /s
Volume in drive C is Windows
Volume Serial Number is A81B-0CF5

Directory of C:\Users\Admin

2022. 02. 13.  18:16        <DIR>        Desktop
2021. 05. 03.  14:16        <DIR>        Searches
                0 File(s)                 0 bytes

Directory of C:\Users\Admin\cache\tooling\gradle

2022. 02. 13.  18:18        159 504 versions.json
                1 File(s)        159 504 bytes

Directory of C:\Users\Admin\.eclipse\org.eclipse.omph.jreinfo
```

h.) felsorolas.txt olvashatóvá tétele.

```
Parancssor
C:\Users\Admin>cd MPW46D
C:\Users\Admin\MPW46D>cd fa
C:\Users\Admin\MPW46D\fa>attrib
A             C:\Users\Admin\MPW46D\fa\felsorolas.txt
C:\Users\Admin\MPW46D\fa>attrib +r felsorolas.txt
C:\Users\Admin\MPW46D\fa>attrib
A R          C:\Users\Admin\MPW46D\fa\felsorolas.txt
C:\Users\Admin\MPW46D\fa>
```

i.) Ennyi helyet foglal a neptunkod mappa a merevlemezén az almappjaival együtt. Ehhez a dir neptunkod /s parancsot használjuk. Tehát: dir MPW46D /s.

```
Parancssor
2022. 02. 19. 18:40      80 felsorolas.txt
2022. 02. 19. 12:50    <DIR>      kokusz
2022. 02. 19. 12:50    <DIR>      korte
2022. 02. 19. 12:50    <DIR>      szeder
                1 File(s)      80 bytes

Directory of C:\Users\Admin\MPW46D\fa\banan
2022. 02. 19. 12:49    <DIR>      .
2022. 02. 19. 12:49    <DIR>      ..
                0 File(s)      0 bytes

Directory of C:\Users\Admin\MPW46D\fa\barack
2022. 02. 19. 12:49    <DIR>      .
2022. 02. 19. 12:49    <DIR>      ..
                0 File(s)      0 bytes

Directory of C:\Users\Admin\MPW46D\fa\kokusz
2022. 02. 19. 12:50    <DIR>      .
2022. 02. 19. 12:50    <DIR>      ..
                0 File(s)      0 bytes

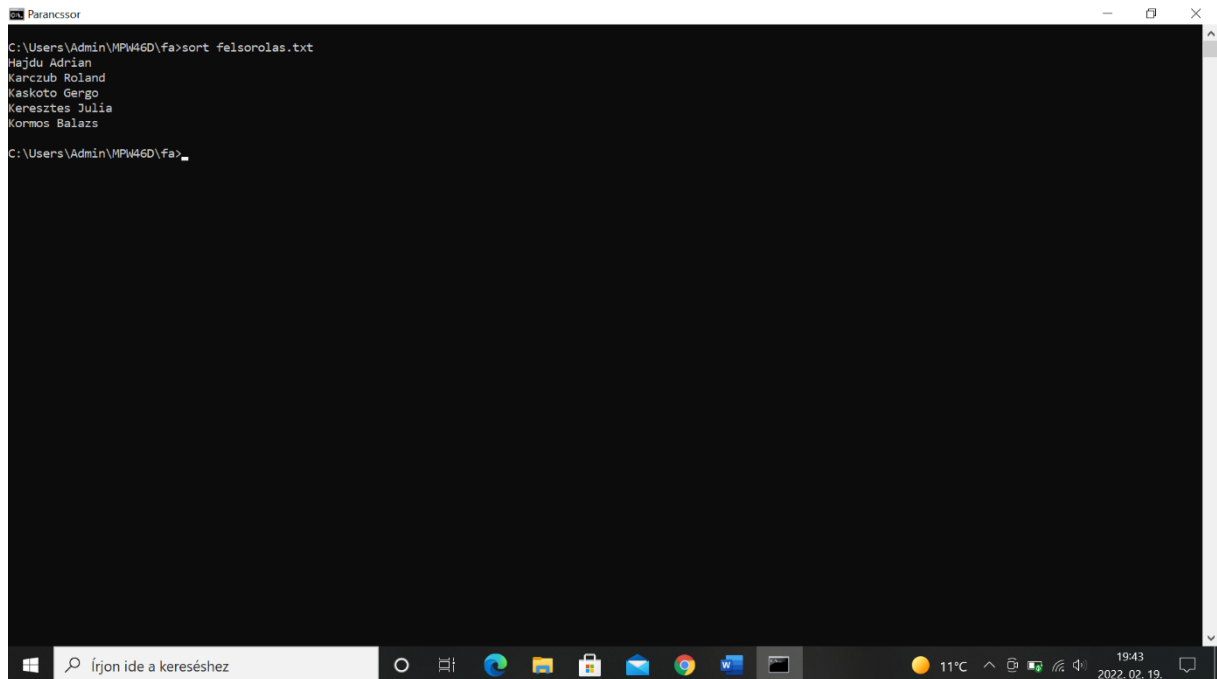
Directory of C:\Users\Admin\MPW46D\fa\korte
2022. 02. 19. 12:50    <DIR>      .
2022. 02. 19. 12:50    <DIR>      ..
                0 File(s)      0 bytes

Directory of C:\Users\Admin\MPW46D\fa\szeder
2022. 02. 19. 12:50    <DIR>      .
2022. 02. 19. 12:50    <DIR>      ..
                0 File(s)      0 bytes

Total Files Listed:
    2 File(s)      188 bytes
   29 Dir(s) 186 720 415 744 bytes free

C:\Users\Admin>
```

j.) ABC szerint sorrendbe tesszük a felsorolas.txt tartalmát.



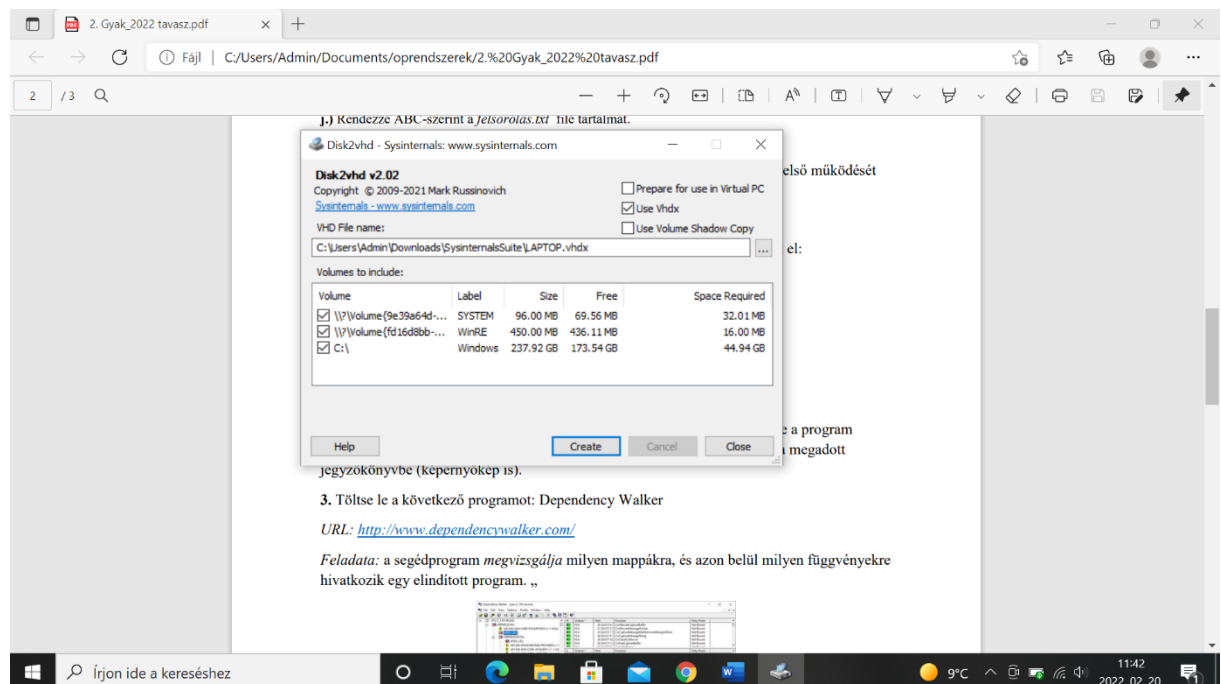
```
Parancssor
C:\Users\Admin\MPW46D\fa>sort felsorolas.txt
Hajdu Adrian
Karczub Roland
Kaskoto Gergo
Keresztes Julia
Komos Balazs
C:\Users\Admin\MPW46D\fa>
```

2. feladat

A Sysinternals Suite használata.

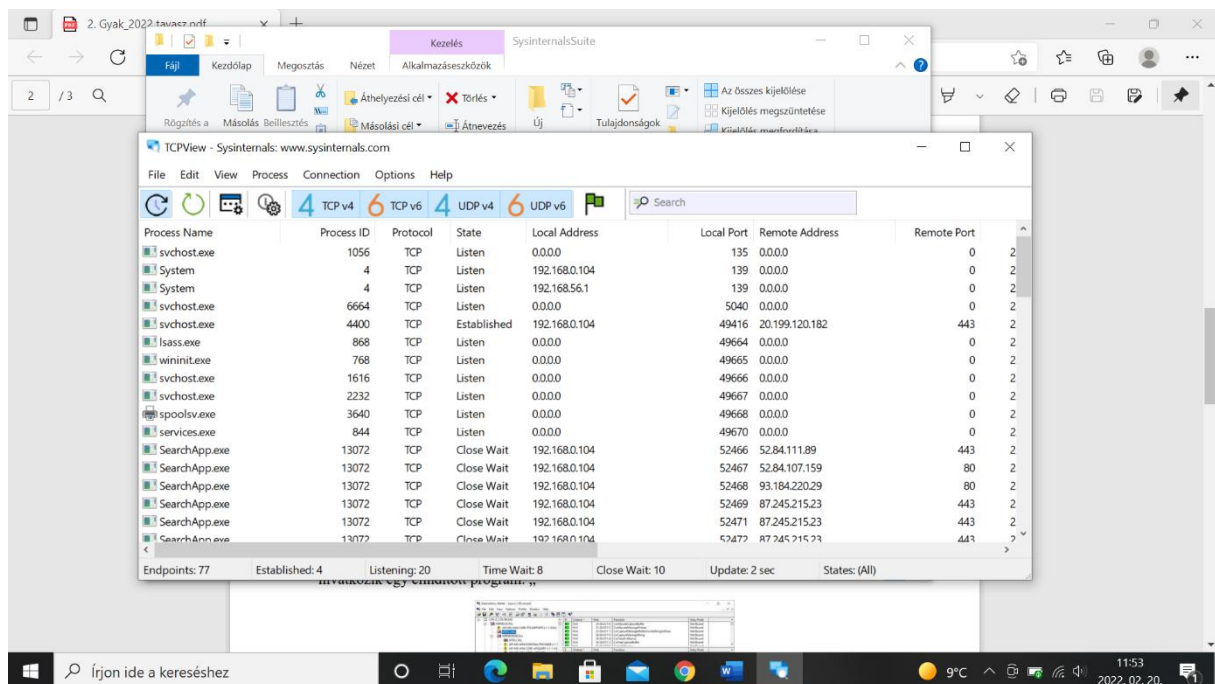
a) File and Disk Utilities (Disk2vhd)

Egy olyan segédprogram, melynek segítségével VHD-t (Virtual Hard Disk/Virtuális merevlemez) készíthetünk, a fizikai lemezeket virtuálissá konvertálhatjuk.



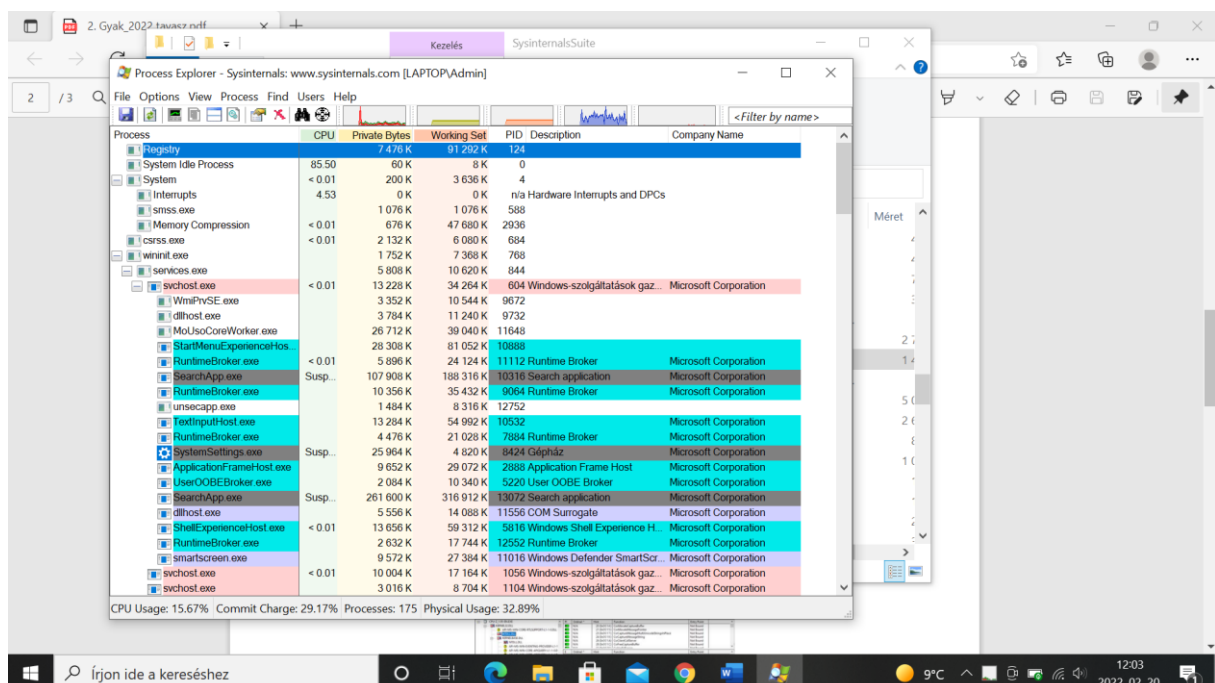
b) Networking Utilities (TCPView)

Egy listában bemutatja a rendszer összes TCP- és UDP-végpontját, beleértve a helyi és távoli címeket, valamint a TCP-kapcsolatok állapotát. Azok a végpontok, amelyek az egyik frissítésről a következőre váltják az állapotot, sárga színnel vannak kiemelve, törölt végpontok piros színnel jelennek meg, az új végpontok pedig zölddel. Másodpercenként frissül.

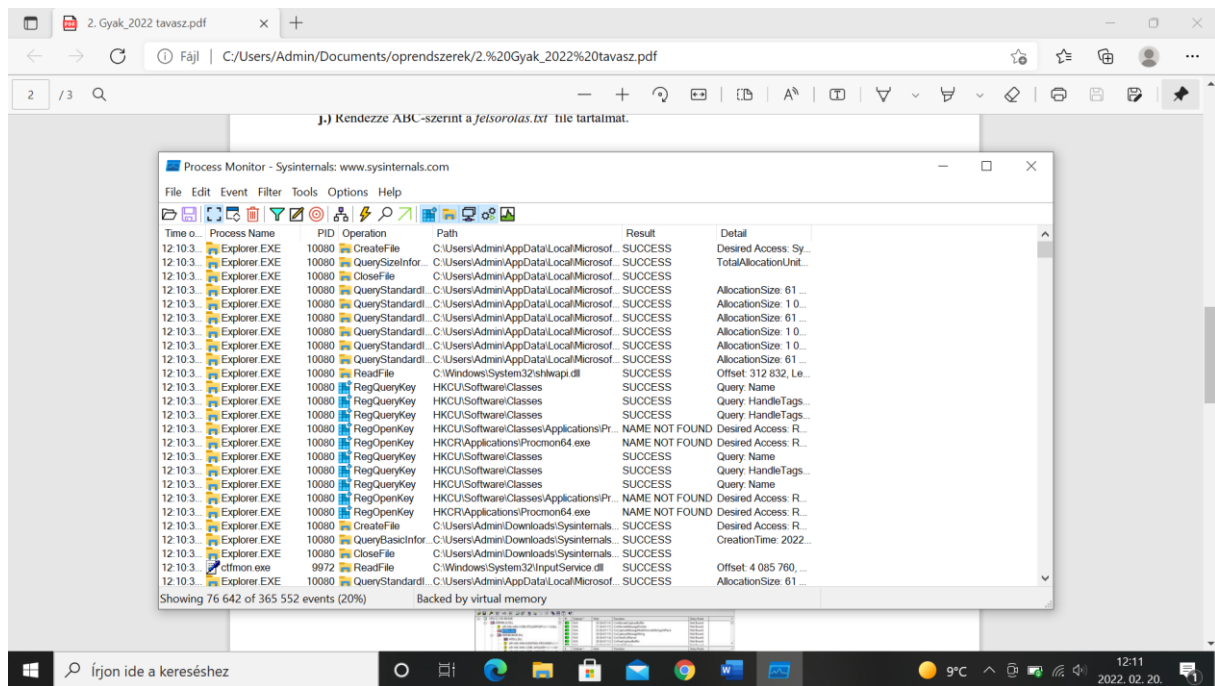


c) Process Utilities (Process Explorer, Process Monitor, AutoRuns)

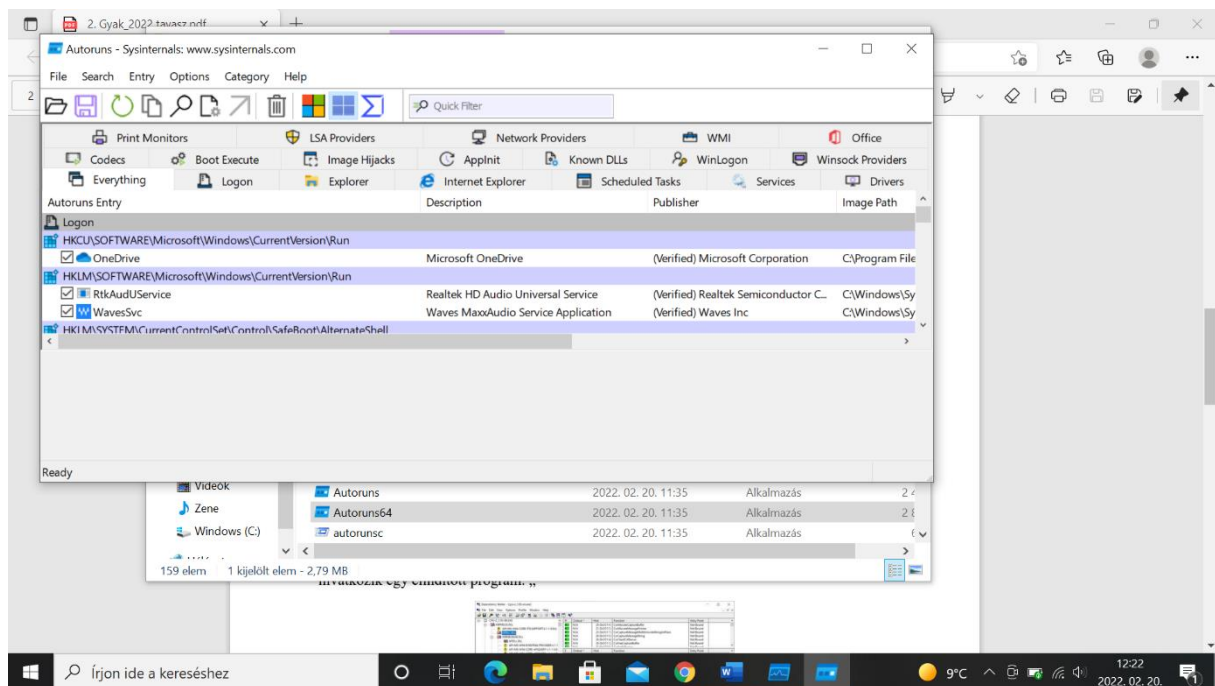
A Process Explorer a jelenleg futó processzeket listázza.



A Process Monitor egy fejlett monitorozási segédprogram, ami valós idejű fájlrendszer, bejegyzés, processz- és szálaktivitást mutat be. Lehetővé teszi a szűrést, átfogó eseménytulajdonságokat mutat, például munkamenet-azonosítókat és felhasználóneveket, megbízható folyamatinformációkat, teljes szálkészleteket az egyes műveletek integrált szimbólumtámogatásával.



Az AutoRuns megmutatja, milyen programok indulnak el a rendszer elindításakor és a különböző Windows alkalmazások elindításakor.



d) Security Utilities (LogonSession)

Felsorolja a jelenleg aktív bejelentkezési munkameneteket, a -p megadásával pedig az egyes munkamenetekben futó folyamatokat.

```
Administrator: Parancssor

C:\Users\Admin\Downloads\SysinternalsSuite>logonsessions

LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
  User name: WORKGROUP\LAPTOP$
  Auth package: NTLM
  Logon type: (none)
  Session: 0
  Sid: S-1-5-18
  Logon time: 2022. 02. 13. 12:54:14
  Logon server:
  DNS Domain:
  UPN:

[1] Logon session 00000000:0000f21d:
  User name:
  Auth package: NTLM
  Logon type: (none)
  Session: 0
  Sid: (none)
  Logon time: 2022. 02. 13. 12:54:14
  Logon server:
  DNS Domain:
  UPN:

[2] Logon session 00000000:0000fa47:
  User name: Font Driver Host\UMFD-0
  Auth package: Negotiate
  Logon type: Interactive
  Session: 0
  Sid: S-1-5-96-0-0
  Logon time: 2022. 02. 13. 12:54:14
  Logon server:
  DNS Domain:
  UPN:
```

e) Information Utilities (RAMMap)

Egy fizikai memória-elemző program. Megmutatja, hogyan menedzseli a Windows a memóriát, mennyi fájladat van gyorsítótárazva a RAM-ban, vagy mennyi RAM-ot használ a kernel és az eszközillesztők. A füleken mutatja be az információkat. A use counts: használati adatok összegzése típus és lapozási lista szerint, processes: a munkakészletek méretének feldolgozása, priority summary: rangsorolások készletlistaméretei, physical pages: oldalankénti használat az összes fizikai memóriához, physical ranges: fizikai memóriacímek, file summary: fájl adatok a RAM-ban fájl szerint, file details: egyes fizikai lapok fájl szerint.

The screenshot shows the Sysinternals Suite RAMMap application window. The 'Use Counts' tab is active, displaying a table of memory usage statistics. The table has columns for Usage, Total, Active, Standby, and Modified. The data is as follows:

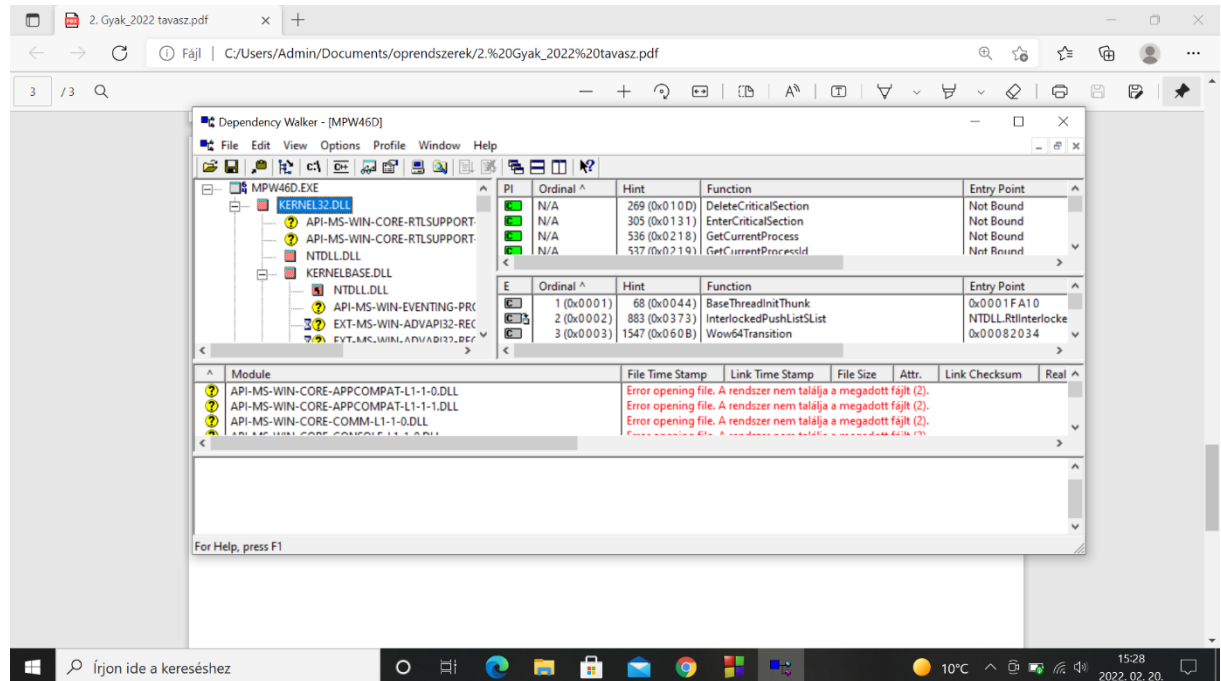
Usage	Total	Active	Standby	Modified
Process Private	3 249 832 K	3 107 168 K	88 668 K	5 000 K
Mapped File	3 039 708 K	984 248 K	2 055 276 K	0 K
Shareable	1 108 564 K	147 968 K	559 904 K	40 000 K
Page Table	101 972 K	101 856 K	116 K	0 K
Page Pool	257 476 K	253 832 K	3 280 K	0 K
Nonpaged Pool	931 708 K	931 708 K	0 K	0 K
System PTE	326 152 K	326 152 K	0 K	0 K
Session Private	28 068 K	27 928 K	140 K	0 K
Metafile	155 772 K	74 832 K	80 940 K	0 K
AWE	0 K	0 K	0 K	0 K
Driver Locked	42 960 K	42 960 K	0 K	0 K
Kernel Stack	37 392 K	33 944 K	2 440 K	0 K
Unused	7 303 780 K	6 064 K	12 K	0 K
Large Page	0 K	0 K	0 K	0 K
Total	16 583 384 K	6 038 660 K	2 790 776 K	45 000 K

The application also shows a file explorer on the left and a taskbar at the bottom with various icons and system information.

3. feladat

A Dependency Walker használata. Feladata: a segédprogram megvizsgálja milyen mappákra, és azon belül milyen függvényekre hivatkozik egy elindított program.

C program készítése, ami egy fájlt hoz létre az adataimról.

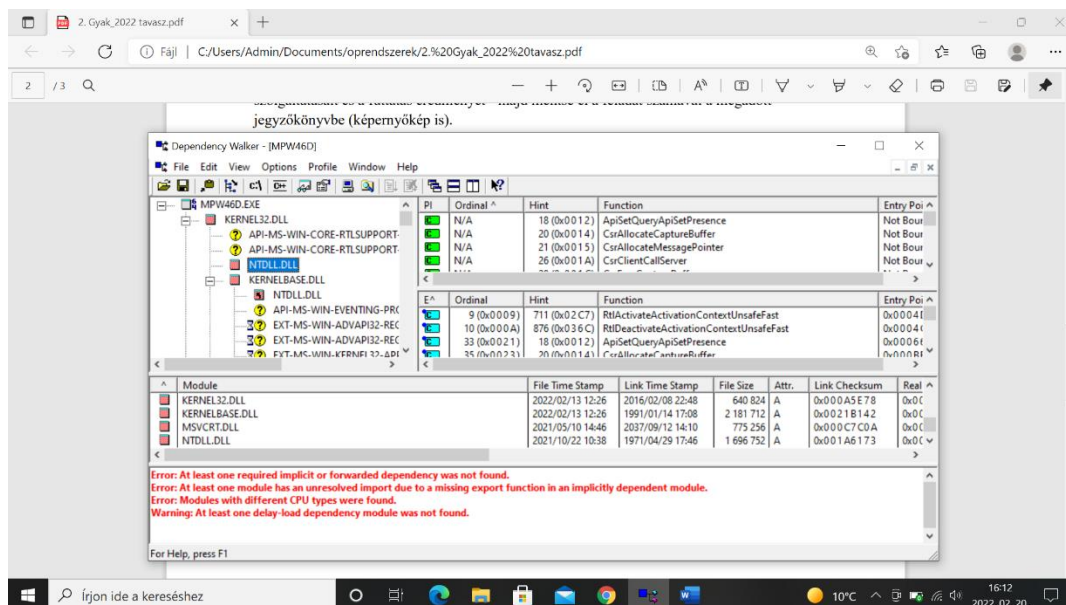


a.) Vizsgálja meg, hogy a neptunkod.exe milyen API hívásokat használ a kernel32.dll-ből (Win alrendszer DLL)!

API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL

API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL

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



Ez egy a Windows által létrehozott fájl, más néven NT Layer DLL, az NT kernel függvényeket tartalmazza. Exportálja a Windows Native API fájlt. Az exportált függvények C nyelven íródtak. A függvény első 2-3 betűje rövidítése annak, melyik függvénycsoportba tartozik az adott függvény. Pl. a Csr kezdetűek kliens-szerver függvények, amik a csrss.exe fájlal kommunikálnak, a Dbg kezdetűek debugging függvények. A Native API felelős a kényszer leállítás elvégzéséért, az elsőbbségek kezeléséért, a native applikáció futtatásáért, távoli szál létrehozásáért a különböző munkamenetekben futó folyamatokon belül.

Tehát a program megvizsgálja, hogy egy programnak milyen függőségei vannak; a bal felső ablakban fanézetben, alatta lista formában is láthatjuk. A szülő importált függvényeket a jobb felső sarokban, az exportált függvényeket ez alatt láthatjuk. A legalsó ablakban a figyelmeztetéseket, hibákat olvashatjuk.