

Operációs rendszerek BSc

2. Gyak.

2022. 02. 14.

Készítette:

Nagy Balázs Bsc
Programtervező
informatikus
EIO1RQ

Miskolc, 2022

1. feladat – Készítse el a következő feladatokat!

Az elvégzett feladatokról készítsen (a.)-j.)-ig.) képernyőképet, majd illessze be a jegyzőkönyvbe.

a) Hozza létre a következő mappa szerkezetet!

neptunkod

|

|- bokor

|

|- banan

|

|- mogyoro

|

|- barack

|

|- fa

|

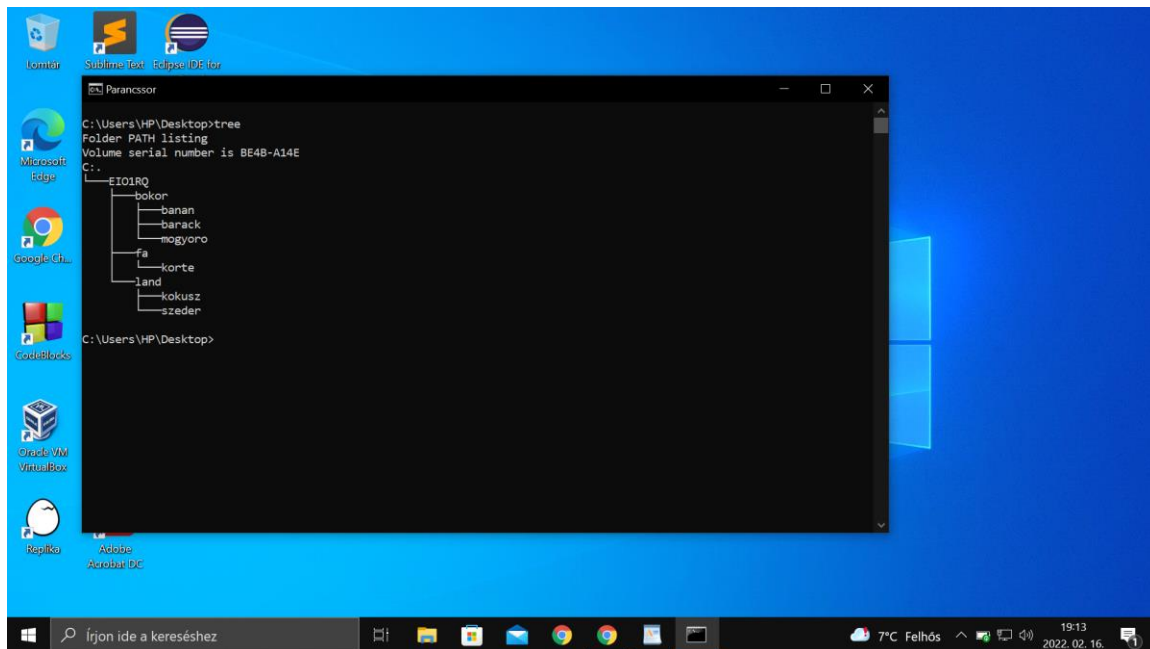
|- korte

|

|-land

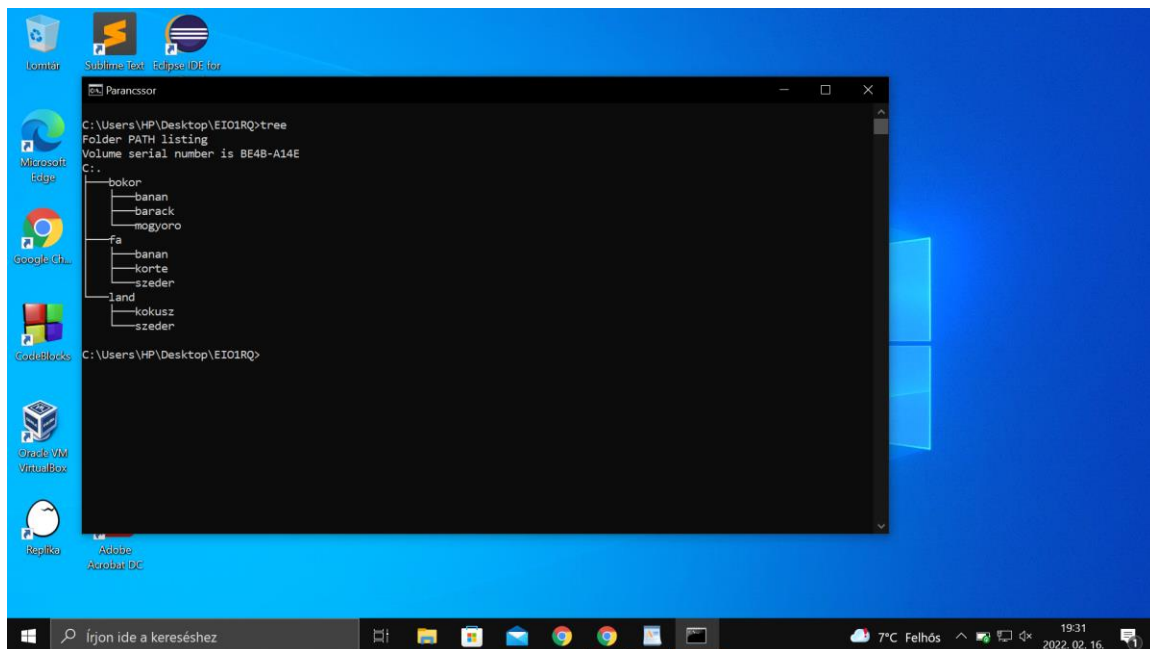
|- szeder

|- kokusz



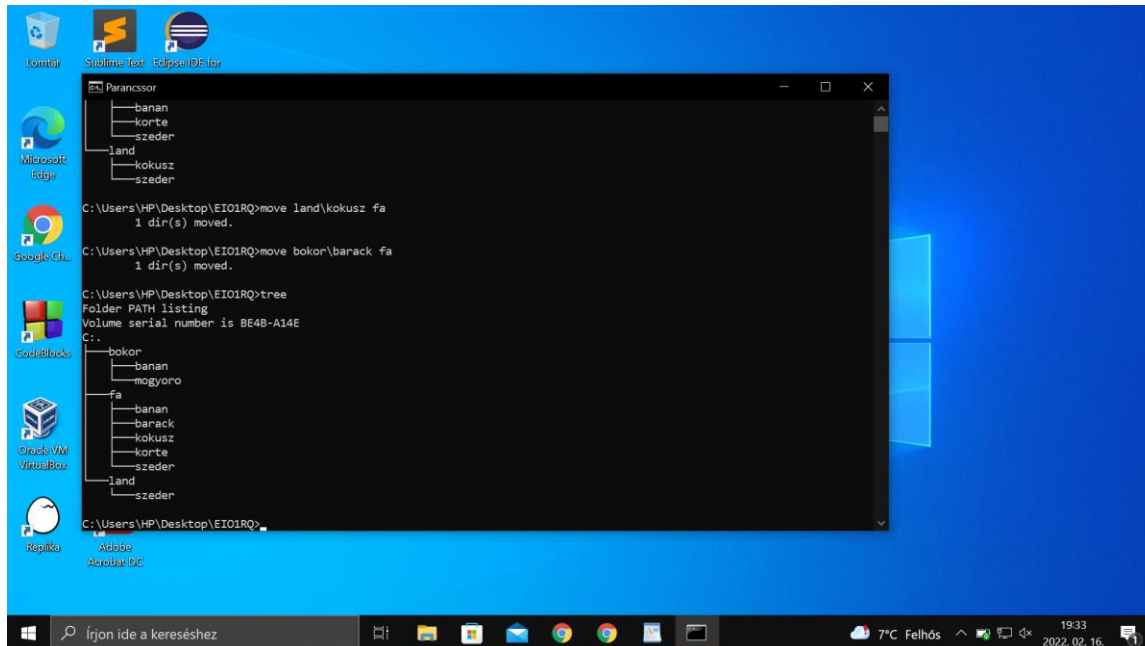
b) Készítsen másolatot:

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

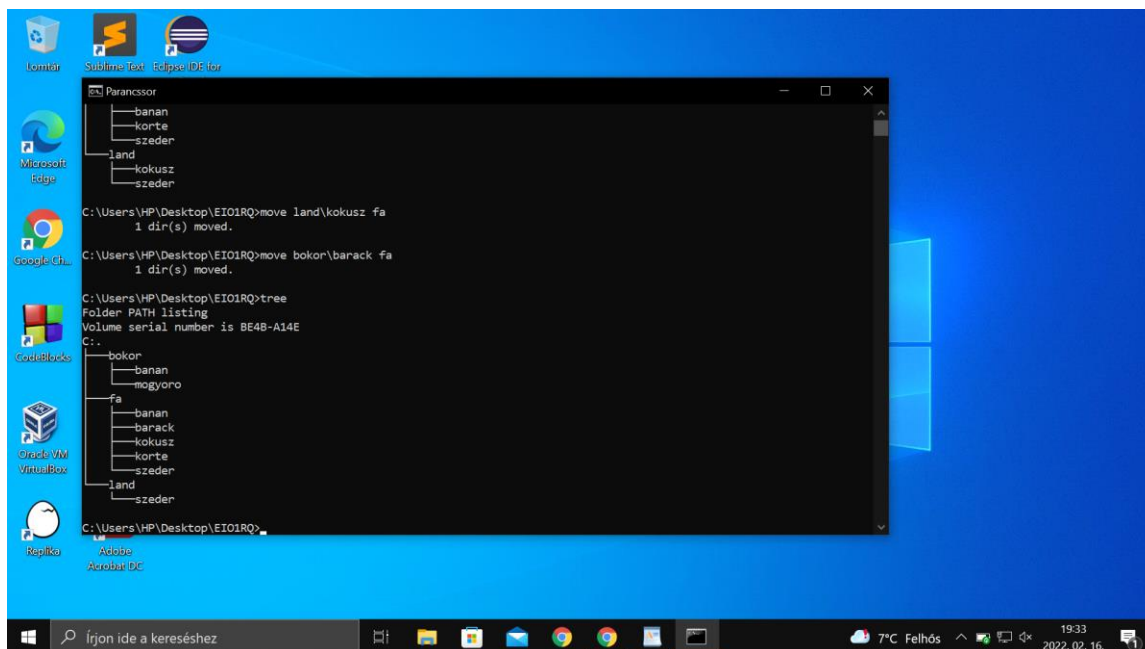


c) Végezze el a következő áthelyezéseket:

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

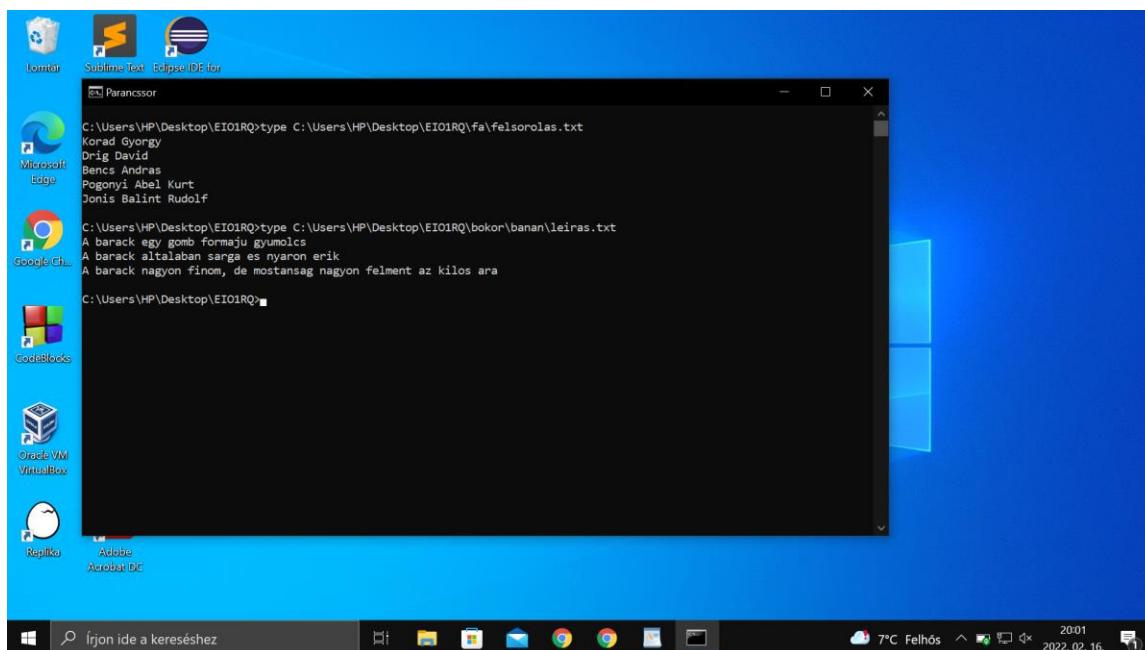


- d)** Törölje a *neptunkod/land* katalógust a teljes tartalmával. Hozza létre a következő szöveges állományokat:
- *neptunkod/bokor/banan/leiras.txt*
 - *neptunkod/tree/felsorolas.txt*

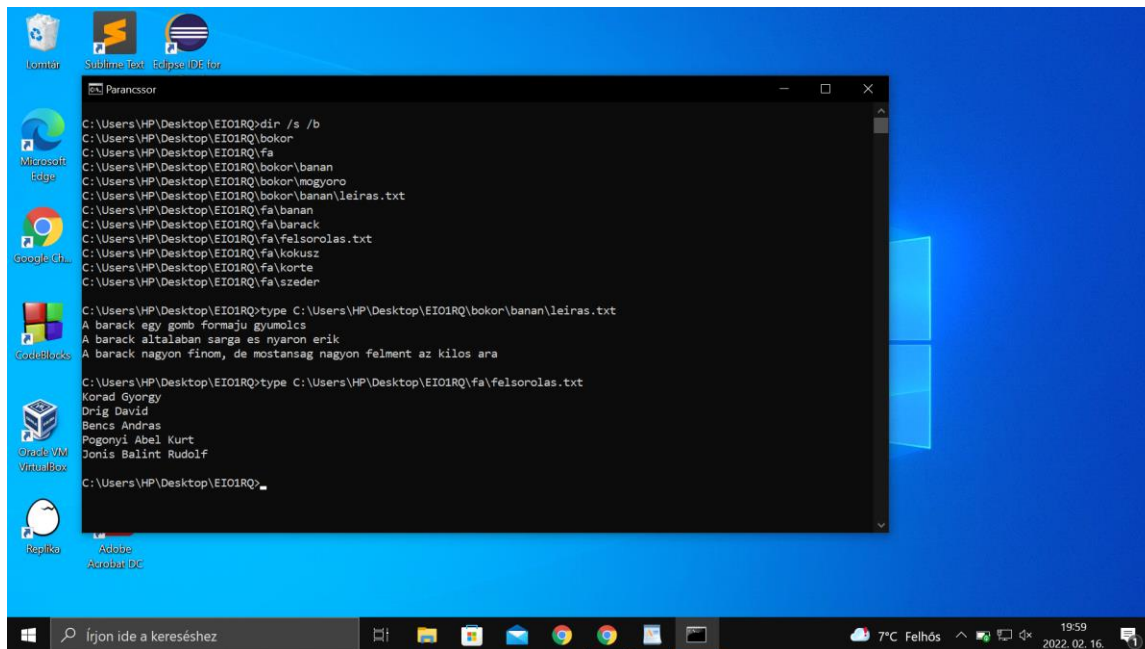


e) A *leiras.txt* szöveges állományba írjon 3 sort a barackról.

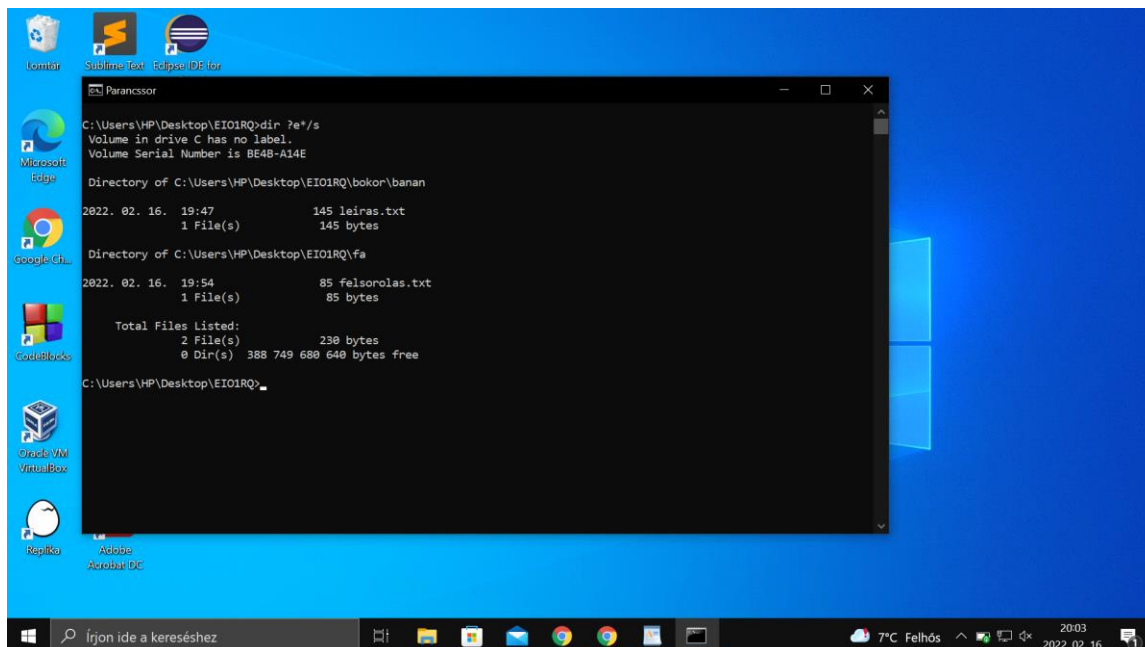
A felsorolas szöveges állományba soroljon fel legalább 5 csoporttársa nevét.



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

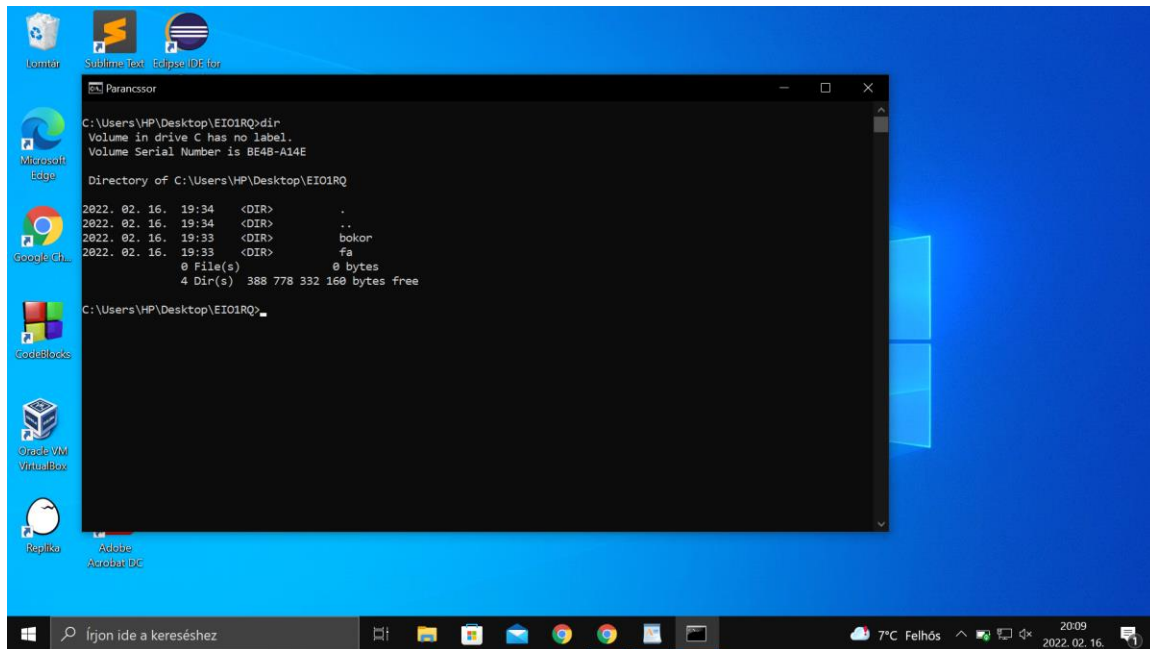


g) Térjen vissza a gyökérmappába és keresse meg az összes olyan file-t, amelyek nevének második betűje *e*.



i) Jelenítse meg, hogy mennyi helyet foglal a merevlemezen a neptunkod mappa az al-mappáival

együtt.



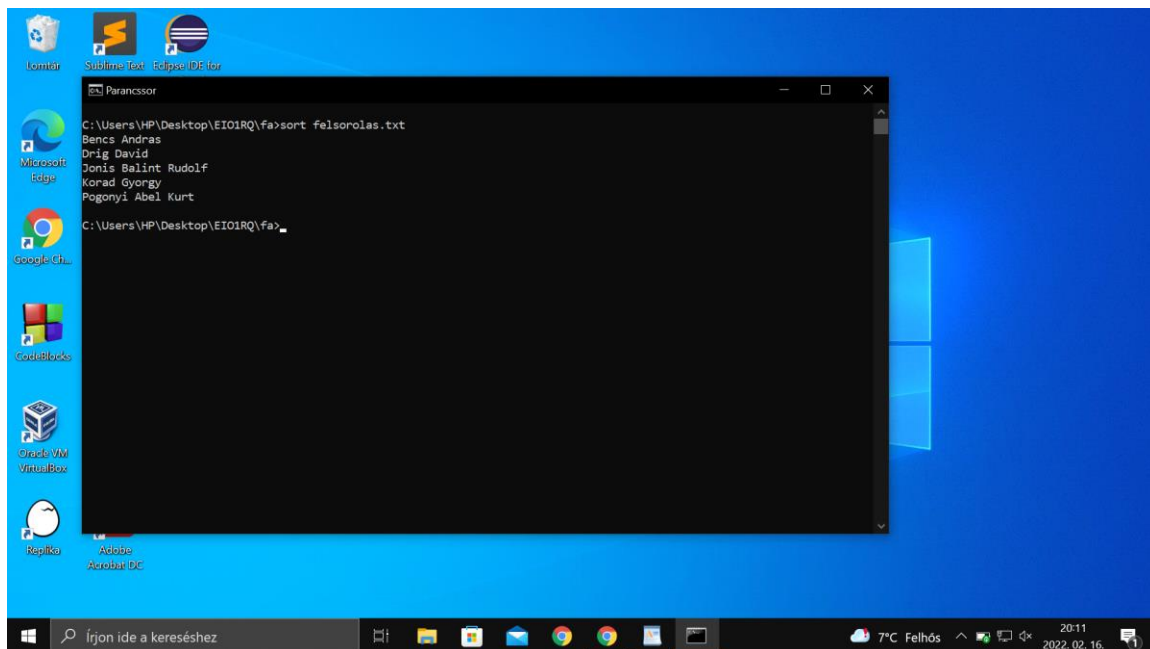
```
C:\Users\HP\Desktop\EIO1RQ>dir
Volume in drive C has no label.
Volume Serial Number is BE48-A14E

Directory of C:\Users\HP\Desktop\EIO1RQ

2022. 02. 16. 19:34 <DIR>      .
2022. 02. 16. 19:34 <DIR>      ..
2022. 02. 16. 19:33 <DIR>      bokor
2022. 02. 16. 19:33 <DIR>      fa
0 File(s)          0 bytes
4 Dir(s)  388 778 332 160 bytes free

C:\Users\HP\Desktop\EIO1RQ>
```

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



```
C:\Users\HP\Desktop\EIO1RQ\fa>sort felsorolas.txt
Bencs Andras
Drig David
Jonis Balint Rudolf
Korad Gyongy
Pogonyi Abel Kurt

C:\Users\HP\Desktop\EIO1RQ\fa>
```

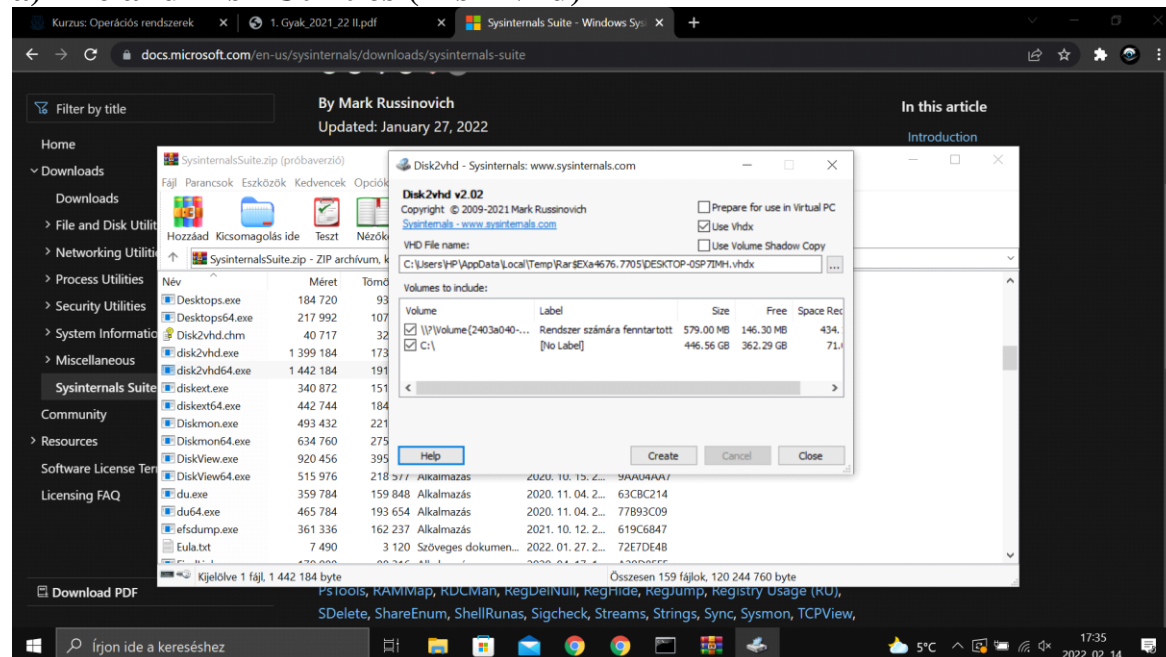
- **2. feladat** – Tölts le a Sysinternals Suite csomagot, majd csomagolja ki. A Windows belső működését lehet tanulmányozni, vagy a hibakeresésben segít.
<https://docs.microsoft.com/hu-hu/sysinternals/downloads/sysinternals-suite>

A Sysinternals weboldalán kategóriákba sorolva hasznos programok érhetők el:

- a) File and Disk Utilities (Disk2vhd)
- b) Networking Utilities (TCPView)
- c) Process Utilities (Process Explorer, Process Monitor, AutoRuns)
- d) Security Utilities (LogonSession)
- e) Information Utilities (RAMMap)

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

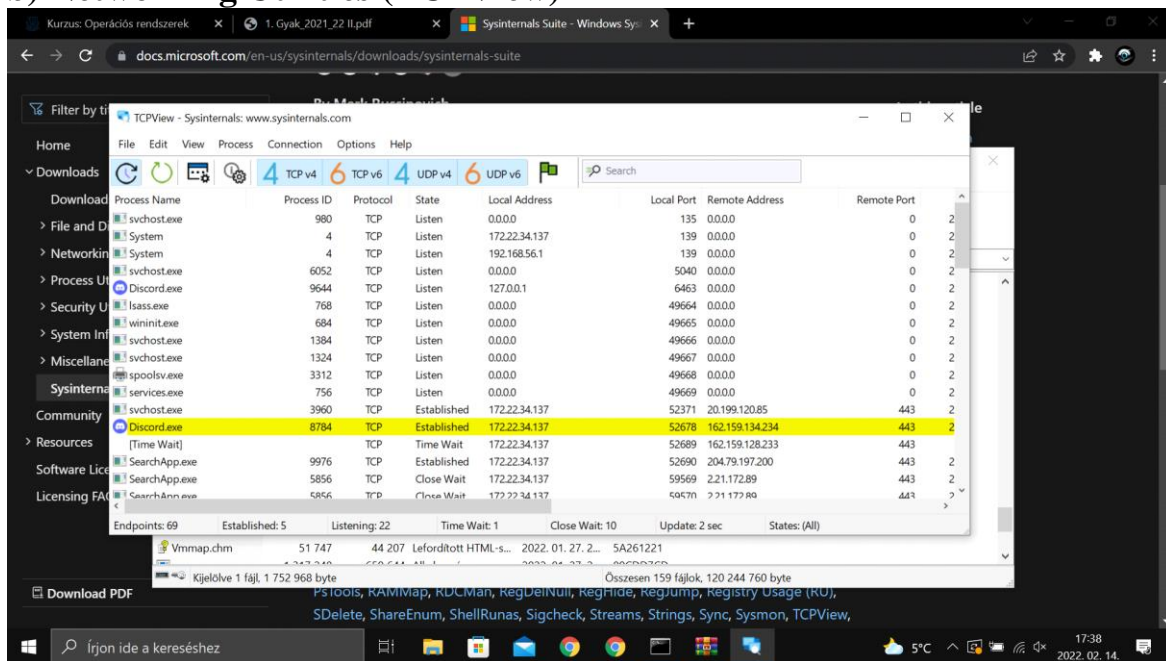
a) File and Disk Utilities (Disk2vhd)



A program segítségével fizikális lemezekről készíthetünk virtuális másolatokat (VHD - Virtual Hard Disk) a Microsoft Virtual PC vagy a Microsoft VM virtuális gépek számára.

A user interface különböző információkat szolgáltat a fizikális meghajtókról a felhasználónak. A "Create" gomb lenyomásával készíthetünk VHD másolatokat a kijelölt lemezekről.

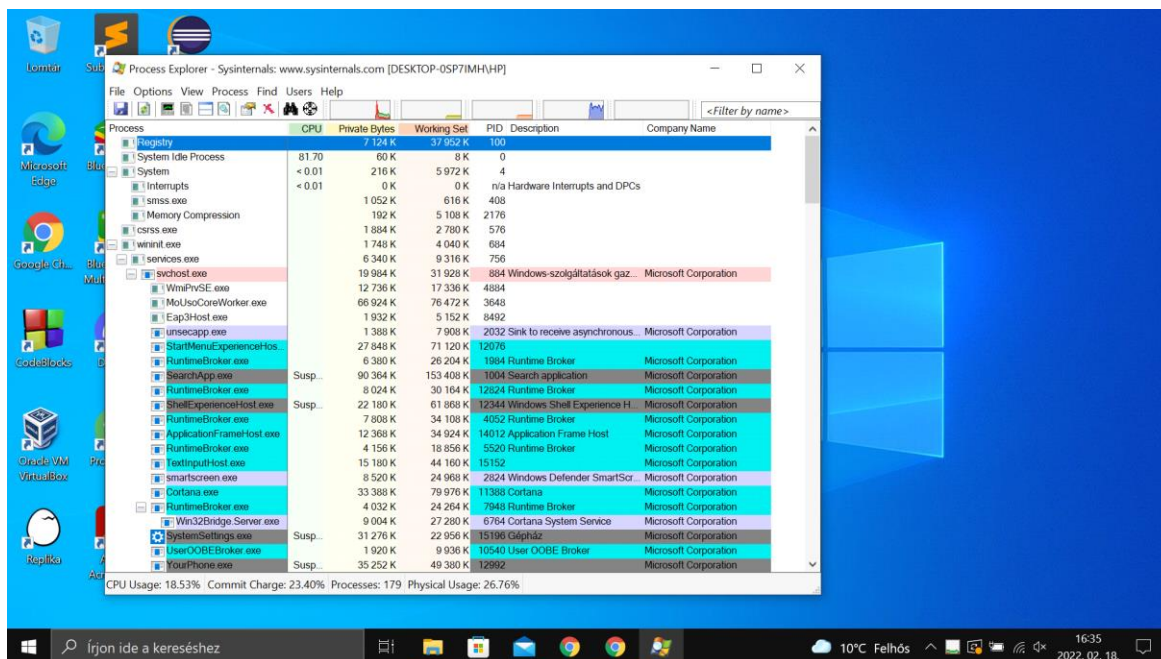
b) Networking Utilities (TCPView)



A TCPView segítségével láthatjuk az összes TCP, valamint UDP végpontokat a rendszeren, beleértve a lokális és távoli IP címeket is. Ezen felül a TCP kapcsolat állapota is meg van jelenítve a felhasználó számára.

Azok a végpontok, amelyek frissítik a jelenlegi állapotukat sárgával láthatjuk; az új végpontokat zölddel, a töröltek pedig piros színnel jelennek meg. A felhasználó, ha kívánja, manuálisan is megszakíthatja a fennálló TCP/IP kapcsolatokat a File - Close Connections kiválasztásával vagy a kívánt kapcsolat kijelölése után jobb klikk - Close Connections.

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

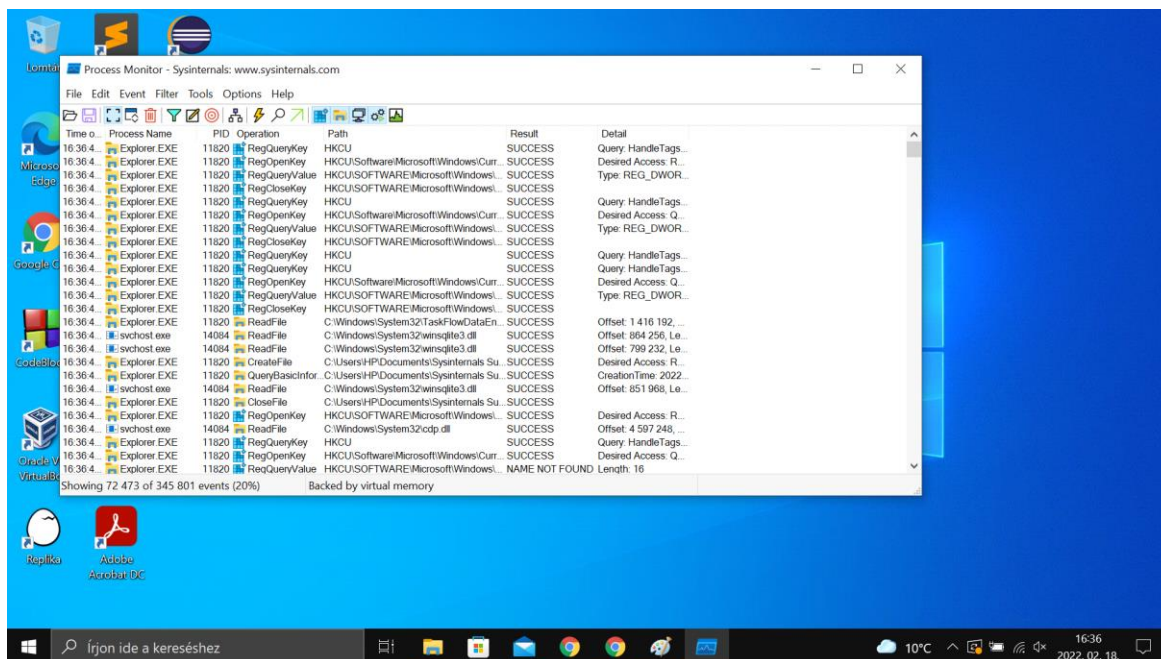


A Process Explorer információt tartalmaz arról, hogy a jelenleg futó processzek milyen handle-eket, illetve DLL-eket (Dynamic Link Library) nyitottak meg, használnak.

Ez az ablak mindig a a jelenleg futó processzekről mutat információt. Egy külön, kisebb ablak is megnyitható, amely kettéosztja az interface-t. Ebben az alsó ablakban a Process Explorer jelenlegi módjától (Handle vagy DLL) függően látható információ. A Handle módban a processzek által megnyitott handle-ek vannak listázva, míg DLL módban a processzek által betöltött DLL-ek vannak feltüntetve.

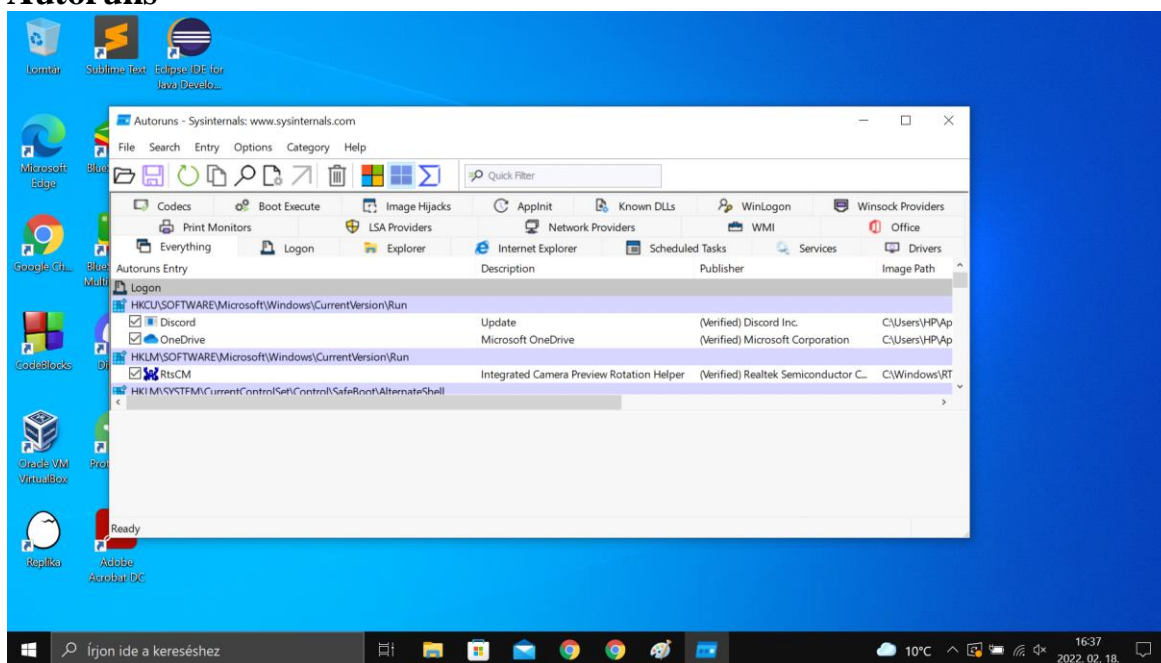
A Process Explorer rendkívül hasznos DLL verzió problémák vagy handle leak-ek felkutatására.

Process Monitor



A Process Monitor valós idejű információt mutat a fájlrendszer, registry, processzek és fonalak tevékenységeiről.

Autoruns



Autoruns megmutatja, hogy mely programok indulnak el rendszer bootup vagy bejelentkezés során, valamint különböző beépített Windows alkalmazások indításakor (Pl. mediaplayerek).

d) Security Utilities (LogonSession)

```
Administrator: Parancssor

UPN:

[22] Logon session 00000000:0f45d7a4:
User name: Window Manager\DM-9
Auth package: Negotiate
Logon type: Interactive
Session: 9
Sid: S-1-5-90-0-9
Logon time: 2022. 02. 16. 13:00:45
Logon server:
DNS Domain:
UPN:

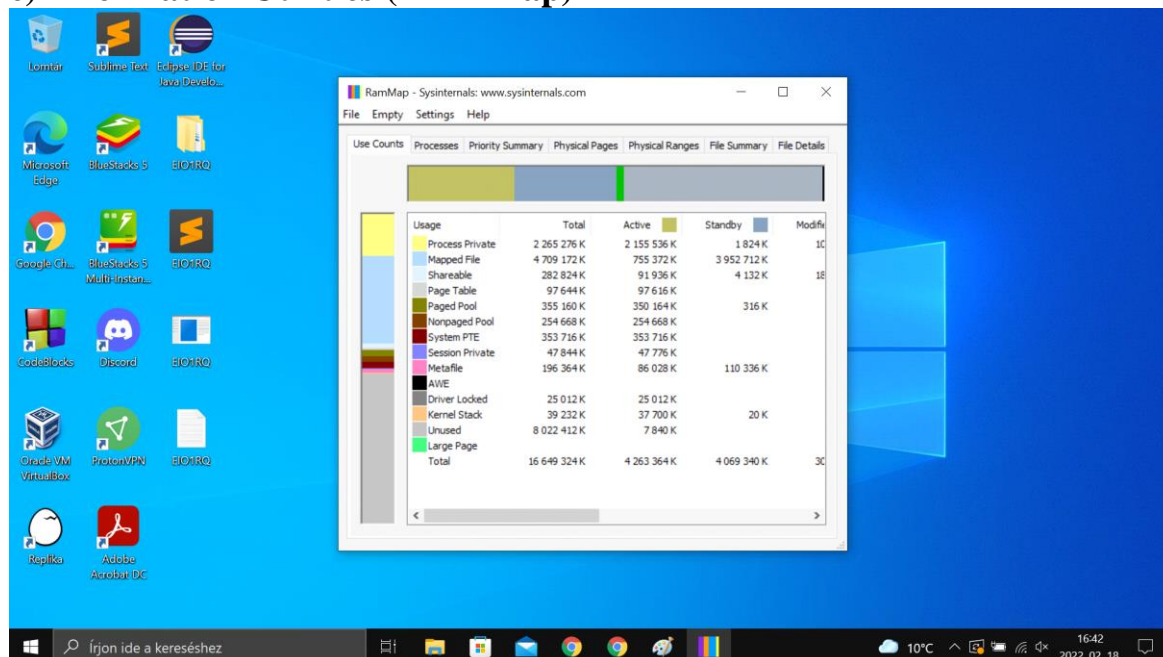
[23] Logon session 00000000:0f45d7c5:
User name: Window Manager\DM-9
Auth package: Negotiate
Logon type: Interactive
Session: 9
Sid: S-1-5-90-0-9
Logon time: 2022. 02. 16. 13:00:45
Logon server:
DNS Domain:
UPN:

[24] Logon session 00000000:0f49c600:
User name: DESKTOP-OK08NMS\Acer
Auth package: NTLM
Logon type: Interactive
Session: 9
Sid: S-1-5-21-1800262312-3136869809-3468689867-1001
Logon time: 2022. 02. 16. 13:30:41
Logon server: DESKTOP-OK08NMS
DNS Domain:
UPN:

[25] Logon session 00000000:0f49c61f:
User name: DESKTOP-OK08NMS\Acer
Auth package: NTLM
Logon type: Interactive
Session: 9
Sid: S-1-5-21-1800262312-3136869809-3468689867-1001
Logon time: 2022. 02. 16. 13:30:41
Logon server: DESKTOP-OK08NMS
DNS Domain:
UPN:
```

A felhasználók bejelentkezéseit és egyéb fontos információkat listáz a program.

e) Information Utilities (RAMMap)



RAMMap különböző lemez használati információkat mutat a felhasználó számára.

A program segítségével megvizsgálhatjuk az egyes alkalmazások memória használatát, RAM allokációt, RAM-ban tárolt cache méretét, kernel által jelenleg használt RAM-ot, valamint sok más memória menedzseléssel kapcsolatos dolgot.

- **3. feladat** – Töltse le a következő programot: Dependency Walker

URL: <http://www.dependencywalker.com/>

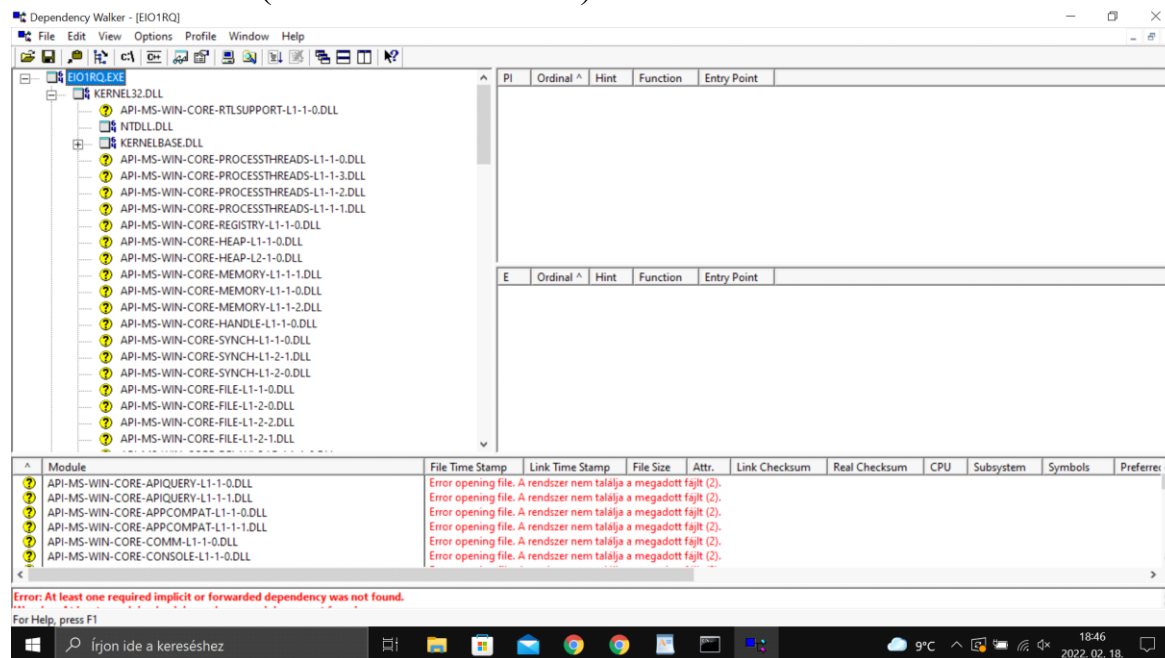
Feladata: a segédprogram megvizsgálja milyen mappákra, és azon belül milyen függvényekre hivatkozik egy elindított program.

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, majd tegye futtathatóvá az állományt: neptunkod.exe

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)!



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

The screenshot shows the Dependency Walker application for EIO1RQ.EXE. The left pane lists the loaded DLLs, with NTDLL.DLL highlighted. The right pane shows the exported functions for the selected DLL. The bottom pane displays error messages for several API-MS-WIN-CORE-*.DLL files, indicating that the required implicit or forwarded dependencies were not found.

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferer
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL										
API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL										
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL										
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL										
API-MS-WIN-CORE-COMM-L1-1-0.DLL										
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL										

Error: At least one required implicit or forwarded dependency was not found.

For Help, press F1

Az NTDLL.DLL egy rejtett rendszerfájl, amely NT kernel függvényeket tartalmaz. Ez a fájl felelős a Windows Natív API exportálásáért, melyet a kernel API-k, valamint a base API-k is implementálnak.

A programok, amelyek közvetlenül ehhez a könyvtárhoz kapcsolódnak, felelősek a rendszer indításakor felmerülő folyamatok elvégzéséért mielőtt a Win32 subsystem elérhetővé válik.