

# Operációs rendszerek Bsc

## 2.Gyak

2022. 02. 15.

**Készítette:**

Tucsa Eszter Boglárka  
Mérnökinformatikus Bsc  
G2QWPO

## 1. Feladat

### 1. 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/kokusz` 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.

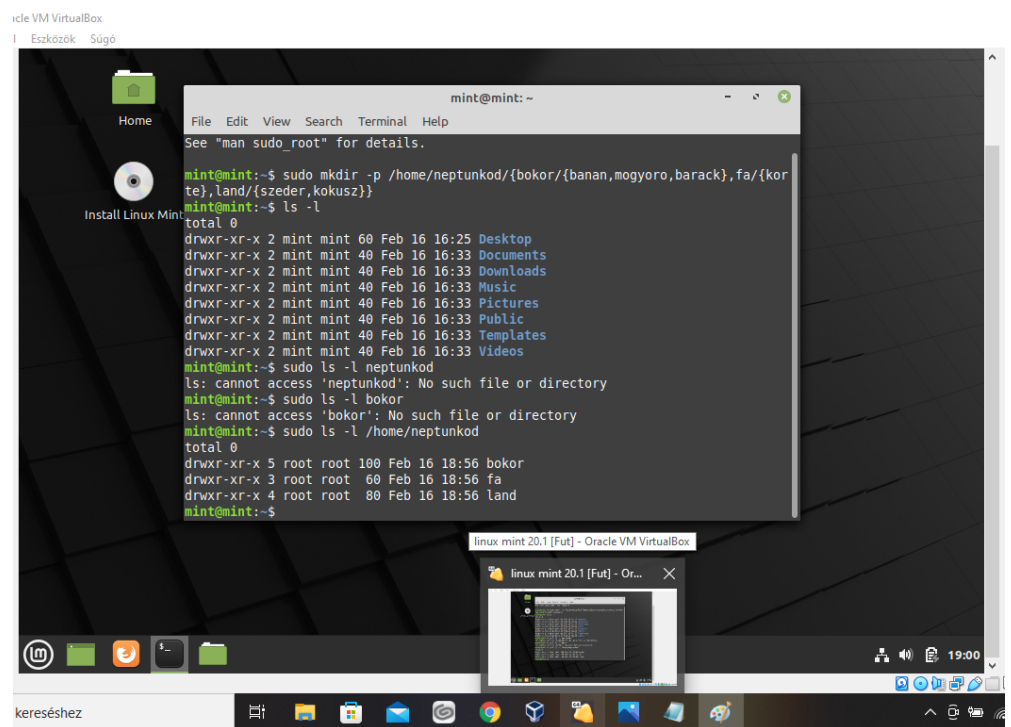
#### g.) Térjen vissza a gyökérmappába és keresse meg az összes olyan file-t, amelyek nevének második betűje e.

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

#### i.) Jelenítse meg, hogy mennyi helyet foglal a merevlemezzen a `neptunkod` mappa az al-mappáival együtt.

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

a)



**b)**



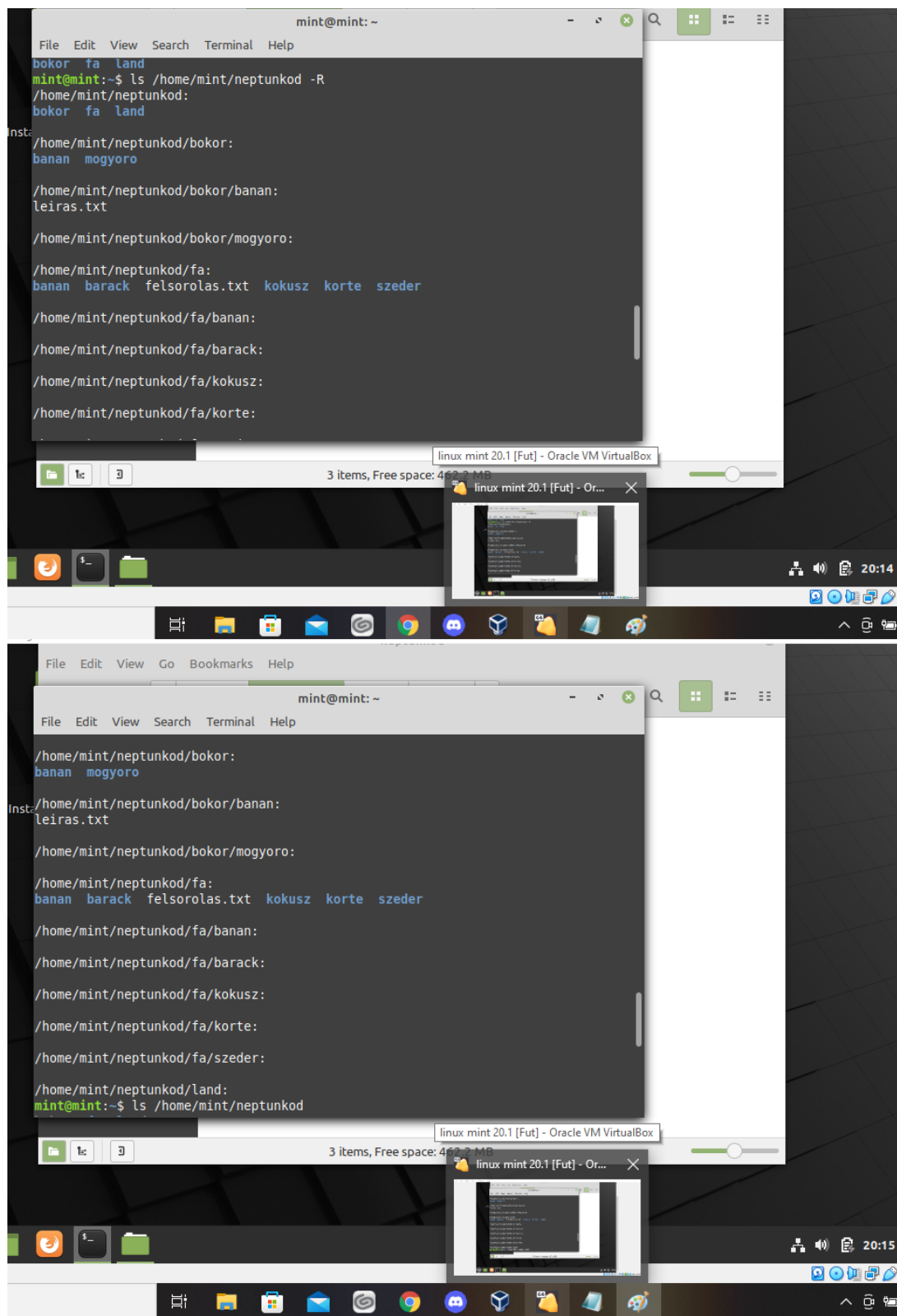
d) Törlés:

```
mint@mint:~$ sudo rm -rf /home/mint/neptunkod/land/szeder
mint@mint:~$ sudo ls -l /home/mint/neptunkod/land
total 0
mint@mint:~$

mint@mint:~$ sudo ls -l /home/mint/neptunkod/land
total 0
mint@mint:~$ sudo touch /home/mint/neptunkod/bokor/banan/leiras.txt /home/mint/n
eptunkod/fa/felsorolas.txt
mint@mint:~$ cat >> /home/mint/neptunkod/bokor/banan/leiras.txt
bash: /home/mint/neptunkod/bokor/banan/leiras.txt: Permission denied
mint@mint:~$ sudo cat >> /home/mint/neptunkod/bokor/banan/leiras.txt
bash: /home/mint/neptunkod/bokor/banan/leiras.txt: Permission denied
mint@mint:~$ sudo nano leiras.txt
mint@mint:~$ sudo ls -l leiras.txt
-rw-r--r-- 1 root root 94 Feb 19 19:51 leiras.txt
mint@mint:~$ sudo echo leiras.txt
leiras.txt
mint@mint:~$ cat leiras.txt
A barack finom.
A baracknak általában sargas-pirosas szine van.
A barack fan no, megse banan.
mint@mint:~$ sudo nano felsorolas.txt
mint@mint:~$ cat felsorolas.txt
Percsi Balazs
Darago Zsolt
Laszlo Andrea
Garamszegi Marton
Zsidai Virag
Ersek Norbert
//en egy evveel regebbi csapatbol vagyok
mint@mint:~$
```

.txt fájlok létrehozása és az e) feladat megoldása, ellenőrzése.

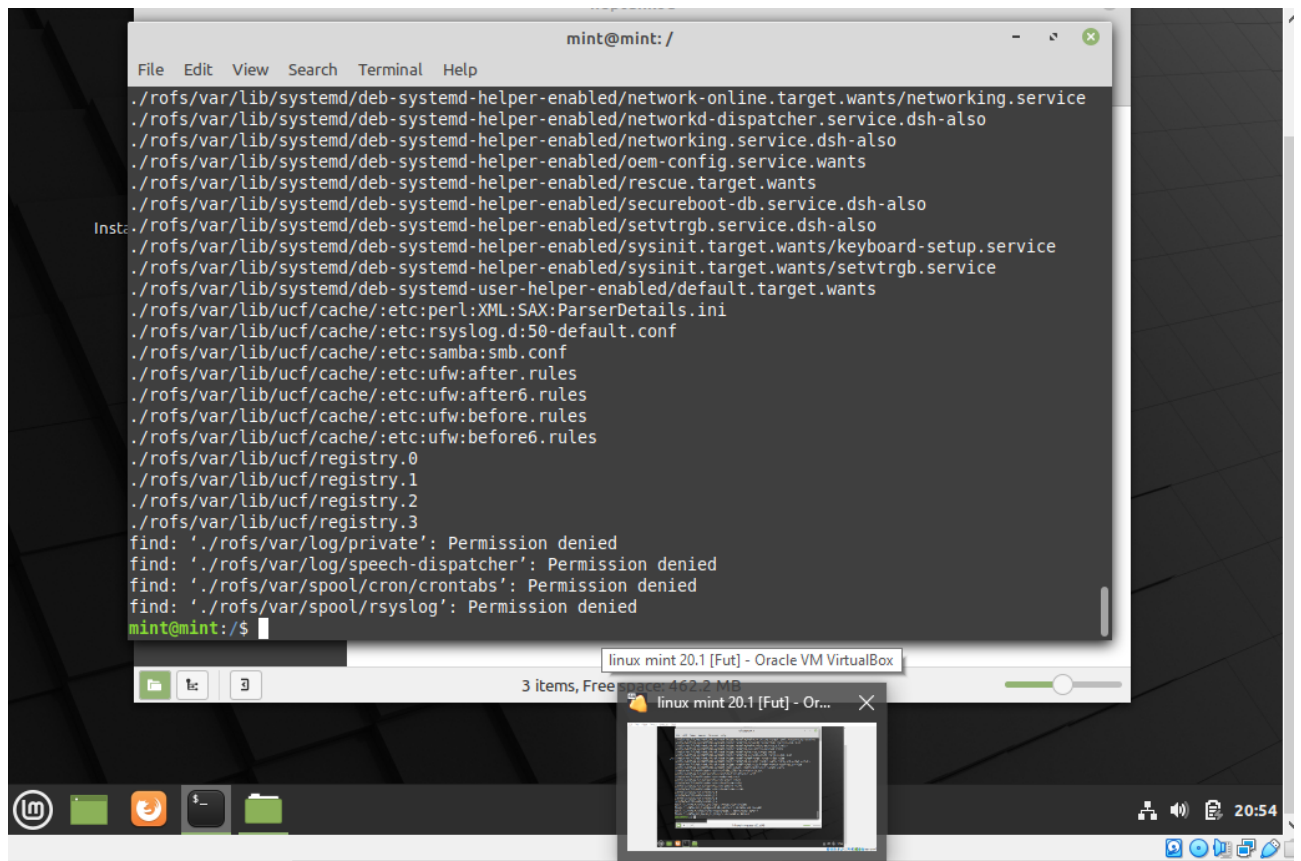
f)



Minden mappa és almappa kilistázva.

Miskolc, 2022

g)



```
mint@mint: /
File Edit View Search Terminal Help
./rofs/var/lib/systemd/deb-systemd-helper-enabled/network-online.target.wants/networking.service
./rofs/var/lib/systemd/deb-systemd-helper-enabled/networkd-dispatcher.service.dsh-also
./rofs/var/lib/systemd/deb-systemd-helper-enabled/networking.service.dsh-also
./rofs/var/lib/systemd/deb-systemd-helper-enabled/oem-config.service.wants
./rofs/var/lib/systemd/deb-systemd-helper-enabled/rescue.target.wants
./rofs/var/lib/systemd/deb-systemd-helper-enabled/secureboot-db.service.dsh-also
./rofs/var/lib/systemd/deb-systemd-helper-enabled/setvtrgb.service.dsh-also
./rofs/var/lib/systemd/deb-systemd-helper-enabled/sysinit.target.wants/keyboard-setup.service
./rofs/var/lib/systemd/deb-systemd-helper-enabled/sysinit.target.wants/setvtrgb.service
./rofs/var/lib/systemd/deb-systemd-user-helper-enabled/default.target.wants
./rofs/var/lib/ucf/cache/etc:perl:XML:SAX:ParserDetails.ini
./rofs/var/lib/ucf/cache/etc:rsyslog.d:50-default.conf
./rofs/var/lib/ucf/cache/etc:samba:smb.conf
./rofs/var/lib/ucf/cache/etc:ufw:after.rules
./rofs/var/lib/ucf/cache/etc:ufw:after6.rules
./rofs/var/lib/ucf/cache/etc:ufw:before.rules
./rofs/var/lib/ucf/cache/etc:ufw:before6.rules
./rofs/var/lib/ucf/registry.0
./rofs/var/lib/ucf/registry.1
./rofs/var/lib/ucf/registry.2
./rofs/var/lib/ucf/registry.3
find: './rofs/var/log/private': Permission denied
find: './rofs/var/log/speech-dispatcher': Permission denied
find: './rofs/var/spool/cron/crontabs': Permission denied
find: './rofs/var/spool/rsyslog': Permission denied
mint@mint:/$
```

Ez a gyönyörűség ~1 percre futott, minden találatot megmutatni legalább 2 oldal lenne ha nem 3, így csak a végéről csináltam képernyőképet. A használt kód: (mint mindenhez, hogy permission probléma annyira ne legyen) `sudo find ./ -name „^?e*.*”`, ezelőtt pedig `cd /`, `pwd` kóddal ellenőriztem, hogy tényleg a gyökérben vagyok.

h)

```

find: './rofs/var/spool/cron/crontabs': Permission denied
find: './rofs/var/spool/rsyslog': Permission denied
mint@mint:/$ sudo chmod ugo+r felsorolas.txt
chmod: cannot access 'felsorolas.txt': No such file or directory
mint@mint:/$ sudo chmod ugo+r /home/mint/neptunkod/fa/felsorolas.txt
mint@mint:/$ du -sh /home/mint/neptunkod
0      /home/mint/neptunkod
mint@mint:/$ du -a /home/mint/neptunkod
0      /home/mint/neptunkod/land
0      /home/mint/neptunkod/bokor/mogyoro
0      /home/mint/neptunkod/bokor/banan/leiras.txt
0      /home/mint/neptunkod/bokor/banan
0      /home/mint/neptunkod/bokor
0      /home/mint/neptunkod/fa/felsorolas.txt

```

felsorolas.txt fájlra mindenki olvasási jogot kapott.

i)

```

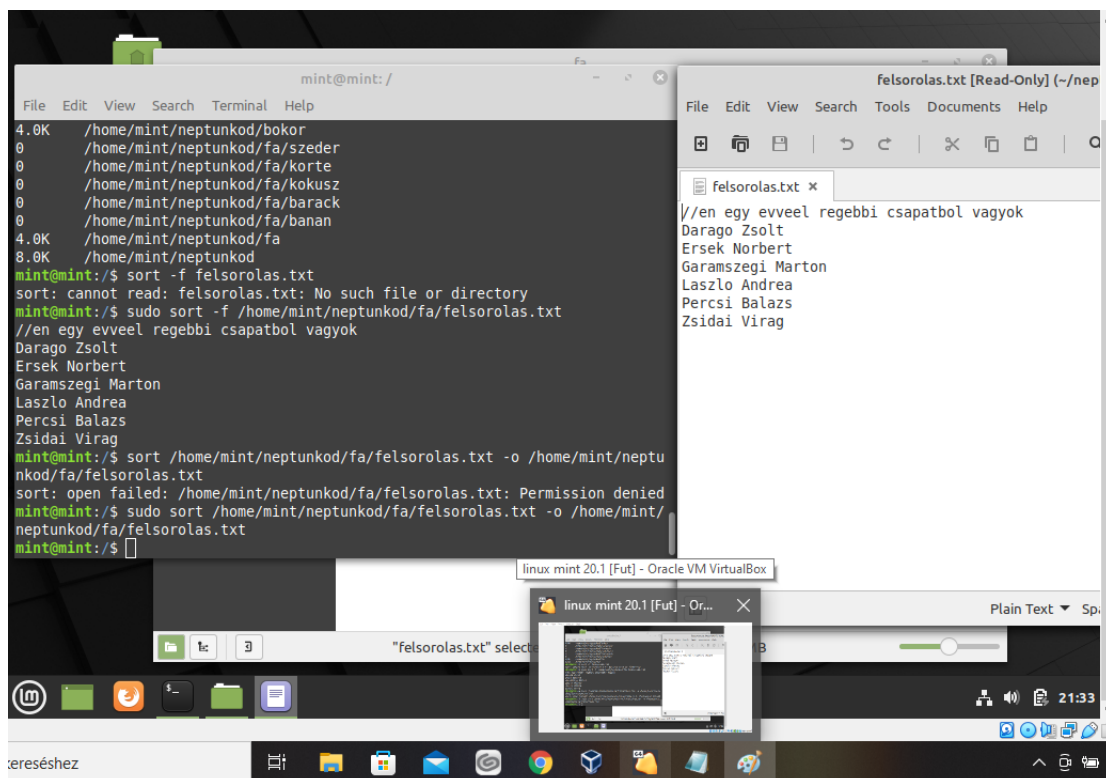
File Edit View Search Terminal Help
0      /home/mint/neptunkod/fa/banan
0      /home/mint/neptunkod/fa
0      /home/mint/neptunkod
mint@mint:/$ sudo du -s /home/mint/neptunkod
0      /home/mint/neptunkod
mint@mint:/$ du -h /home/mint/neptunkod -d 1
Inst:0  /home/mint/neptunkod/land
0      /home/mint/neptunkod/bokor
0      /home/mint/neptunkod/fa
0      /home/mint/neptunkod
mint@mint:/$ sudo du -shc /neptunkod/*
du: cannot access '/neptunkod/*': No such file or directory
0      total
mint@mint:/$ sudo du -h --max-depth=2 /home/mint/neptunkod
0      /home/mint/neptunkod/land
0      /home/mint/neptunkod/bokor/mogyoro
4.0K   /home/mint/neptunkod/bokor/banan
4.0K   /home/mint/neptunkod/bokor
0      /home/mint/neptunkod/fa/szeder
0      /home/mint/neptunkod/fa/korte
0      /home/mint/neptunkod/fa/kokus
0      /home/mint/neptunkod/fa/barack
0      /home/mint/neptunkod/fa/banan
4.0K   /home/mint/neptunkod/fa
8.0K   /home/mint/neptunkod
mint@mint:/$

```

A mappa helyfoglalása összességében és részenként.



j)



The screenshot shows a Linux Mint desktop environment. A terminal window is open, displaying the following commands and output:

```
mint@mint:/$ ls -l /home/mint/neptunkod/
total 40K
drwxr-xr-x 2 mint mint 4.0K 2022.01.12 10:00 bokor
drwxr-xr-x 2 mint mint 0    2022.01.12 10:00 szeder
drwxr-xr-x 2 mint mint 0    2022.01.12 10:00 korte
drwxr-xr-x 2 mint mint 0    2022.01.12 10:00 kokusz
drwxr-xr-x 2 mint mint 0    2022.01.12 10:00 barack
drwxr-xr-x 2 mint mint 0    2022.01.12 10:00 banan
drwxr-xr-x 2 mint mint 4.0K 2022.01.12 10:00 fa
drwxr-xr-x 2 mint mint 8.0K 2022.01.12 10:00 neptunkod
mint@mint:/$ sort -f felsorolas.txt
sort: cannot read: felsorolas.txt: No such file or directory
mint@mint:/$ sudo sort -f /home/mint/neptunkod/fa/felsorolas.txt
//en egy eveel regebbi csapatbol vagyok
Darago Zsolt
Ersek Norbert
Garamszegi Marton
Laszlo Andrea
Percsi Balazs
Zsidai Virag
mint@mint:/$ sort /home/mint/neptunkod/fa/felsorolas.txt -o /home/mint/neptunkod/fa/felsorolas.txt
sort: open failed: /home/mint/neptunkod/fa/felsorolas.txt: Permission denied
mint@mint:/$ sudo sort /home/mint/neptunkod/fa/felsorolas.txt -o /home/mint/neptunkod/fa/felsorolas.txt
mint@mint:/$
```

A text editor window titled "felsorolas.txt [Read-Only] (~/.neptunkod/fa/felsorolas.txt)" is also open, showing the following content:

```
//en egy eveel regebbi csapatbol vagyok
Darago Zsolt
Ersek Norbert
Garamszegi Marton
Laszlo Andrea
Percsi Balazs
Zsidai Virag
```

A felsorolás mappa tartalma rendezett kiírása, és ABC rendezett átírása.



## 2.feladat

2. 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)

DESKTOP-DK3MC3M	2022. 02. 20. 18:02	VHD fájl	3 373 897 KB
-----------------	---------------------	----------	--------------

Lemásolja a fizikai merevlemez tartalmát, és ebből a másolatból virtuális gépet konvertál. Ami változtatás történik a fizikai lemezen a virtuális gép létrehozása után, az már nem lesz jelen a virtual hard disk-ben.

//A gép Word Padhoz társította.

b)

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6 Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
svchost.exe	792	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2022. 02. 16. 17:09:27	RpcSs	
System	4	TCP	Listen	192.168.1.137	139	0.0.0.0	0	2022. 02. 20. 17:05:43	System	
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	2022. 02. 20. 17:05:41	System	
svchost.exe	2240	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2022. 02. 20. 17:05:38	CDPSvc	
TeamViewer_Service.exe	9188	TCP	Listen	127.0.0.1	5939	0.0.0.0	0	2022. 02. 20. 17:12:47	TeamViewer	
Discord.exe	4324	TCP	Listen	127.0.0.1	6463	0.0.0.0	0	2022. 02. 20. 17:06:32	Discord.exe	
lsass.exe	880	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2022. 02. 16. 17:09:27	lsass.exe	
wininit.exe	780	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2022. 02. 16. 17:09:27	wininit.exe	
svchost.exe	1500	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2022. 02. 16. 17:09:28	EventLog	
svchost.exe	1544	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2022. 02. 16. 17:09:28	Schedule	
spoolsv.exe	4160	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	2022. 02. 16. 17:09:32	Spooler	
services.exe	852	TCP	Listen	0.0.0.0	49679	0.0.0.0	0	2022. 02. 16. 17:09:43	services.exe	
svchost.exe	4560	TCP	Established	192.168.1.137	53905	20.199.120.182	443	2022. 02. 20. 17:05:46	WpnService	
Discord.exe	5596	TCP	Established	192.168.1.137	56542	162.159.130.234	443	2022. 02. 20. 17:06:11	Discord.exe	2
WinStore.App.exe	7316	TCP	Close Wait	192.168.1.137	60434	13.71.194.194	443	2022. 02. 20. 18:25:18	WinStore.App.exe	
[Time Wait]		TCP	Time Wait	192.168.1.137	60870	40.76.174.66	443			
SearchApp.exe	7272	TCP	Established	192.168.1.137	60897	204.79.197.222	443	2022. 02. 20. 18:35:40	SearchApp.exe	
[Time Wait]		TCP	Time Wait	192.168.1.137	60912	40.76.174.66	443			
RadsonSoftware.exe	11952	TCP	Syn Sent	127.0.0.1	60929	127.0.0.1	4843	2022. 02. 20. 18:36:47	RadsonSoftware.exe	
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	2022. 02. 16. 17:09:33	System	
System	4	TCP	Listen	0.0.0.0	5357	0.0.0.0	0	2022. 02. 16. 17:09:40	System	
svchost.exe	8944	TCP	Listen	0.0.0.0	7680	0.0.0.0	0	2022. 02. 19. 17:36:25	DoSvc	
Wacom_Tablet.exe	5416	TCP	Listen	0.0.0.0	23130	0.0.0.0	0	2022. 02. 20. 17:05:47	Wacom_Tablet.exe	
Wacom_Tablet.exe	5416	TCP	Listen	0.0.0.0	23131	0.0.0.0	0	2022. 02. 20. 17:05:48	Wacom_Tablet.exe	
svchost.exe	792	TCPv6	Listen	::	135	::	0	2022. 02. 16. 17:09:27	RpcSs	
System	4	TCPv6	Listen	::	445	::	0	2022. 02. 16. 17:09:33	System	
System	4	TCPv6	Listen	::	5357	::	0	2022. 02. 16. 17:09:40	System	
svchost.exe	8944	TCPv6	Listen	::	7680	::	0	2022. 02. 19. 17:36:25	DoSvc	
Wacom_Tablet.exe	5416	TCPv6	Listen	::	23130	::	0	2022. 02. 20. 17:05:47	Wacom_Tablet.exe	
Wacom_Tablet.exe	5416	TCPv6	Listen	::	23131	::	0	2022. 02. 20. 17:05:48	Wacom_Tablet.exe	
svchost.exe	892	TCPv6	Listen	::	49664	::	0	2022. 02. 16. 17:09:27	lsass.exe	

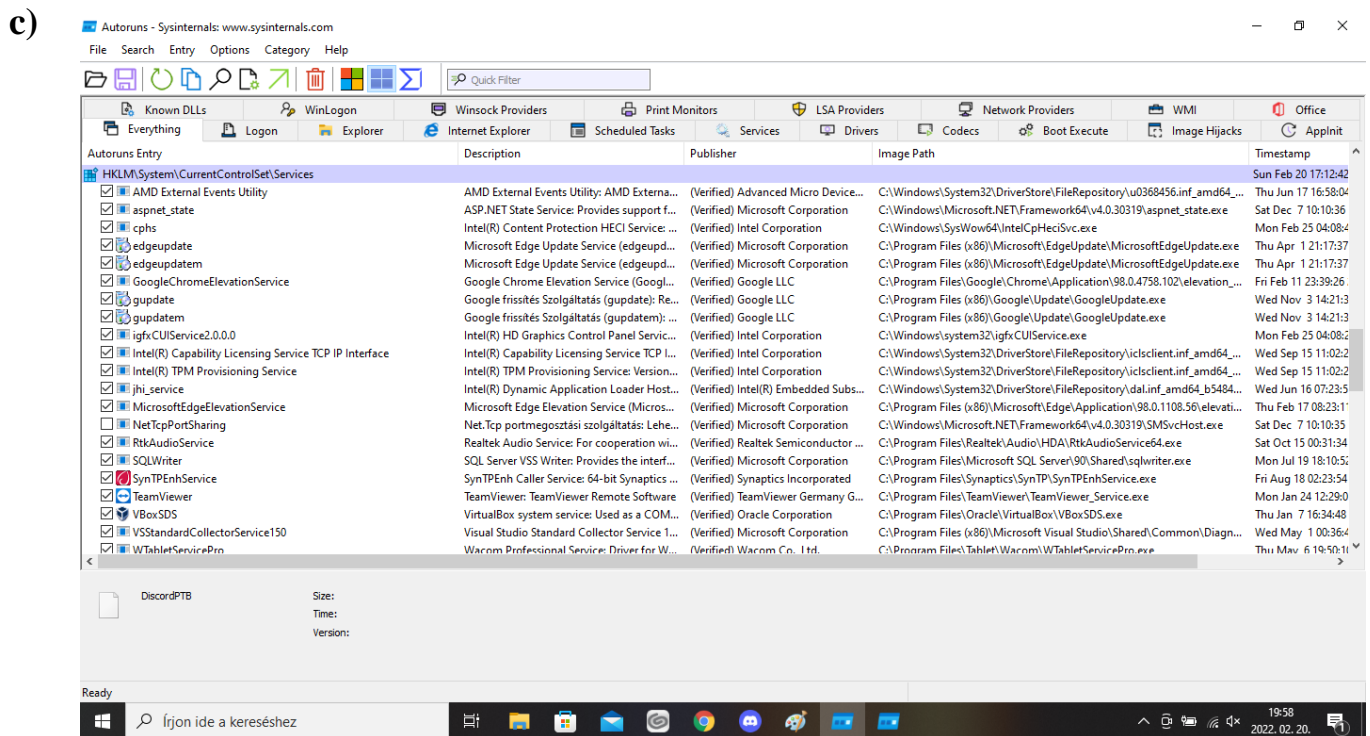
Endpoints: 90 Established: 6 Listening: 30 Time Wait: 2 Close Wait: 3 Update: 2 sec States: (All)

Írjon ide a kereséshez

18:36 2022. 02. 20.

Miskolc, 2022

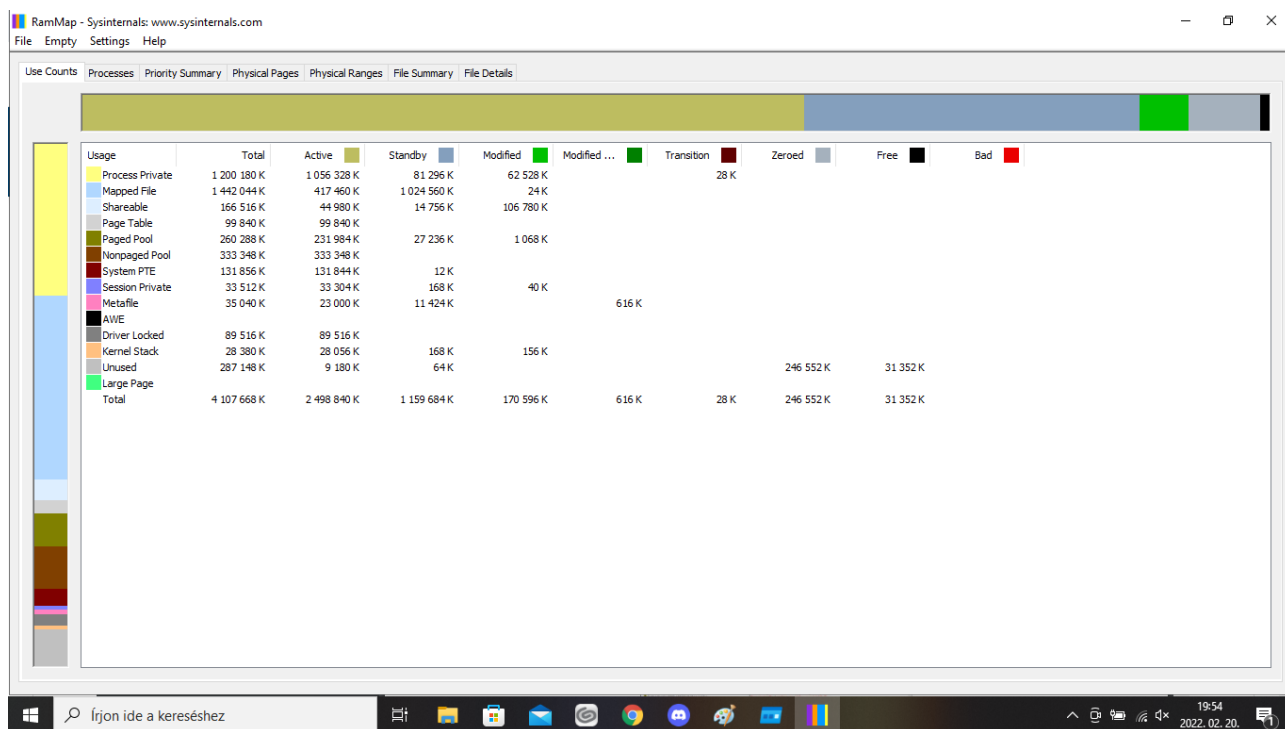
Megmutatja a rendszer minden TCP-, UDP-végpontjának részletes listáját, helyi és távoli címeket és a TCP kapcsolatok állapotát is. A Netstat program informatívabb és kényelmesebb ekvivalense.



A Windows-zal automatikusan elinduló programokat és programrészleteket lehet vele megtekinteni és kezelni. Jól használható malware keresésre és megszüntetésre.

**d) LogonSessions:** Felsorolja az LSA által létrehozott és menedzselte login session-okat (bejelentkezéseket). Ezt futtattam, 2 másodpercre feljött egy ablak, majd meg is szűnt. Így erről nem tudok képernyőképet készíteni.

e)



A memóriahasználatot analizálja. Különböző szempontok alapján lehet megtekinteni, User Counts alatt, hogy mik, milyen típusú, és mennyi memóriát használ. Process alatt a futó folyamatok memóriahasználatát. De a készenléti állapotban lévő programok méretét, a fizikai memóriák címét stb is meg lehet nézni.

### 3. feladat

3. 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*

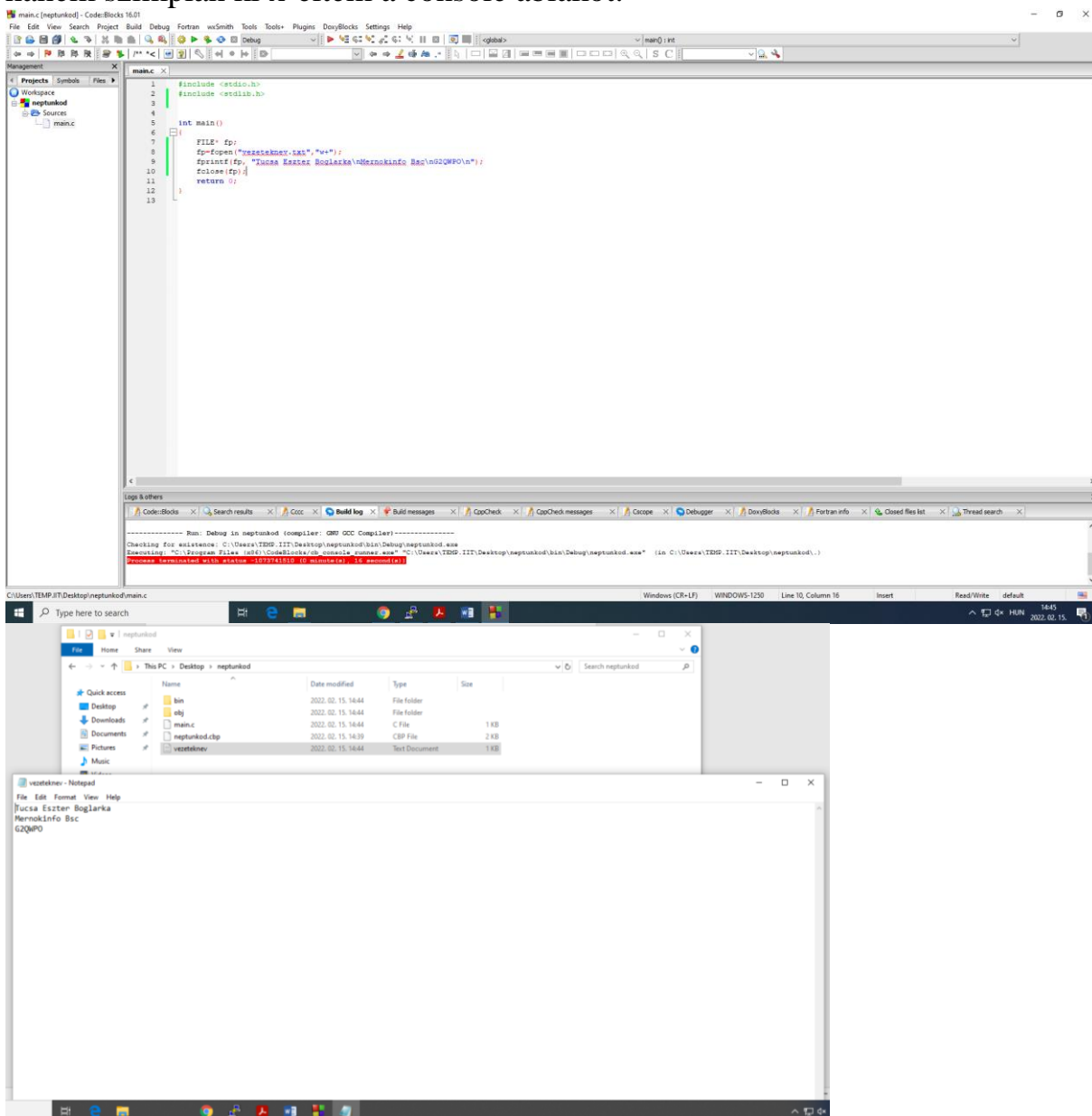
A Dependency Walker segítségével végezze el a következő feladatokat.

Nyissa meg a *neptunkod.exe* fájlt!

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

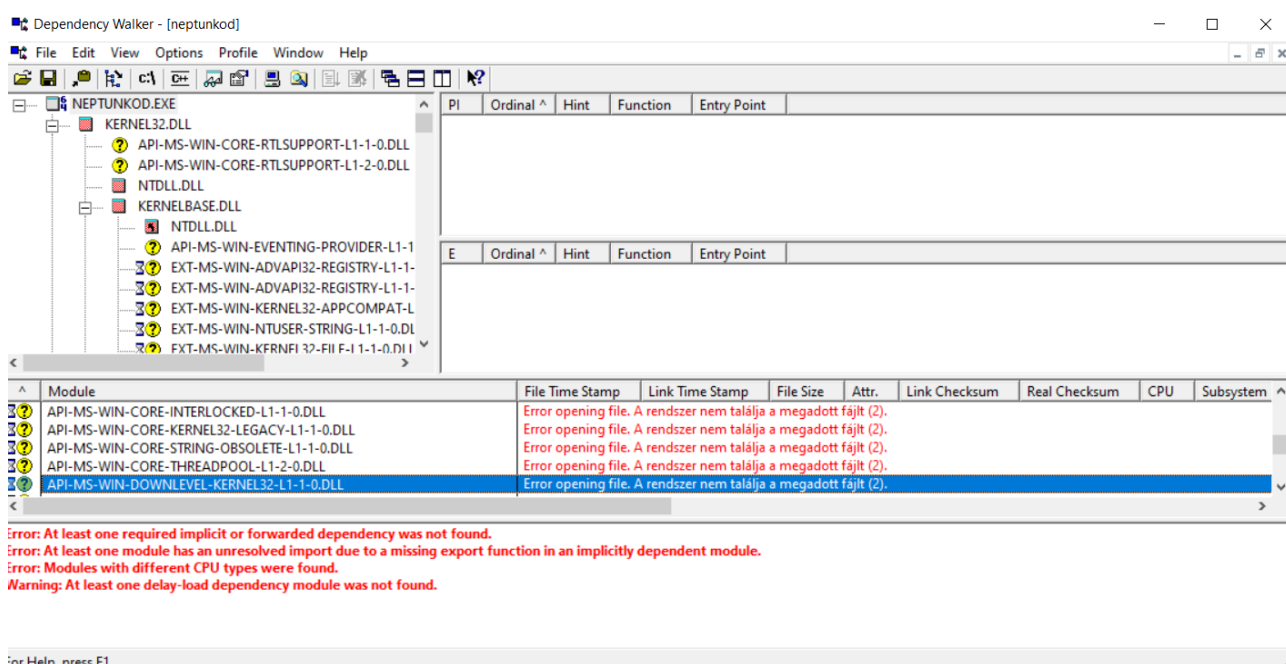
b.) Keresse meg *NTDLL.DLL*-t! Mi ennek a szerepe? Vizsgálja meg az exportált függvényeket, milyen információkat kap az NT API-ról! „

A C kód: //A piros „process terminated” csak amiatt van, hogy nem entert nyomtam, hanem szimplán ki x-eltem a console ablakot.



A fájl létrejött a megfelelő névvel, és a megadott adatokkal.

a)



Az itt látható 2 API-t használja.

b) Az előbbi képernyőképen látszik az NTDLL.dll is.

Az NTDLL.dll az NT rendszerfüggvényeit, kernel függvényeit tartalmazza, gépi kód formában. Programként futtatható, a feladatkezelőben is processként megtekinthető. Szükséges a Windows operációs rendszert futtató gépek megfelelő működéséhez.

Az NT APIk a jogosultságok engedélyezéséért, letiltásáért, munkafolyamatokon belül távoli szálakat létrehozásáért, natív alkalmazások futtatásáért és kényszerleállításért felelős. Eventeket készít, megnyit, bezár, kezel bizonyos folyamatokat. Több fajta NT API van, pl.: Nt/Zw, Rtl, Csr, Dbg, Ki, Ldr, Nls, Pfx, Tp. Ezek mind bizonyos részekért felelnek a fentebb említett folyamatokban.