

**Operációs rendszerek BSc**  
**2. Gyak.**  
**2022. 02. 15.**

**Készítette:**

Nemesi Gergely Tibor

Üzemmérnök-informatikus

ILZGJC

**Miskolc, 2022**

# 1. feladat:

## A, Hozza létre a következő mappa szerkezetet!

```
Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Robo>cd Documents

C:\Users\Robo\Documents>mkdir ILZGJC

C:\Users\Robo\Documents>cd ILZGJC

C:\Users\Robo\Documents\ILZGJC>mkdir bokor

C:\Users\Robo\Documents\ILZGJC>cd bokor

C:\Users\Robo\Documents\ILZGJC\bokor>mkdir banan

C:\Users\Robo\Documents\ILZGJC\bokor>mkdir mogyoro

C:\Users\Robo\Documents\ILZGJC\bokor>mkdir barack

C:\Users\Robo\Documents\ILZGJC\bokor>cd ..

C:\Users\Robo\Documents\ILZGJC>mkdir fa

C:\Users\Robo\Documents\ILZGJC>cd fa

C:\Users\Robo\Documents\ILZGJC\fa>mkdir korte

C:\Users\Robo\Documents\ILZGJC\fa>cd ..

C:\Users\Robo\Documents\ILZGJC>mkdir land

C:\Users\Robo\Documents\ILZGJC>cd land

C:\Users\Robo\Documents\ILZGJC\land>mkdir szeder

C:\Users\Robo\Documents\ILZGJC\land>mkdir kokusz

C:\Users\Robo\Documents\ILZGJC\land>cd ..

C:\Users\Robo\Documents\ILZGJC>tree
```

```
Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Robo\Documents\ILZGJC>mkdir fa

C:\Users\Robo\Documents\ILZGJC>cd fa

C:\Users\Robo\Documents\ILZGJC\fa>mkdir korte

C:\Users\Robo\Documents\ILZGJC\fa>cd ..

C:\Users\Robo\Documents\ILZGJC>mkdir land

C:\Users\Robo\Documents\ILZGJC>cd land

C:\Users\Robo\Documents\ILZGJC\land>mkdir szeder

C:\Users\Robo\Documents\ILZGJC\land>mkdir kokusz

C:\Users\Robo\Documents\ILZGJC\land>cd ..

C:\Users\Robo\Documents\ILZGJC>tree
Folder PATH listing
Volume serial number is 96A4-B342
C:.
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   └── korte
├── land
│   ├── kokusz
│   └── szeder
└──
```

# 1. feladat

B, Készítsen másolatot:

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

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

```
Command Prompt
29/12/2021 13:22 <DIR> Adobe
08/02/2022 14:26 <DIR> Egyéni Office-sablonok
15/02/2022 13:27 <DIR> ILZGJC
14/02/2022 12:40 <DIR> ILZGJC0sGyak
14/02/2022 10:07 <DIR> Java
07/02/2022 11:13 <DIR> My Games
09/02/2022 08:05 <DIR> OneNote-jegyzetfüzetek
02/02/2022 12:16 <DIR> programs
15/02/2022 00:18 <DIR> ShareX
15/02/2022 11:23 120 template_Article.aux
15/02/2022 11:23 3,341 template_Article.log
15/02/2022 11:23 39,852 template_Article.pdf
15/02/2022 11:23 915 template_Article.synctex.gz
15/02/2022 11:23 184 template_Article.tex
5 File(s) 44,412 bytes
11 Dir(s) 371,831,549,952 bytes free

C:\Users\Robo\Documents>cd ILZGJC

C:\Users\Robo\Documents\ILZGJC>xcopy "C:\Users\Robo\Documents\ILZGJC\land\szeder" "C:\Users\Robo\Documents\ILZGJC\fa" /t /e

C:\Users\Robo\Documents\ILZGJC>xcopy "C:\Users\Robo\Documents\ILZGJC\bokor\banan" "C:\Users\Robo\Documents\ILZGJC\fa" /t /e

C:\Users\Robo\Documents\ILZGJC>tree
Folder PATH listing
Volume serial number is 96A4-B342
C:.
|_ bokor
|   |_ banan
|   |_ barack
|   |_ mogyoro
|_ fa
|   |_ banan
|   |_ korte
|   |_ szeder
|_ land
|   |_ kokusz
|   |_ szeder

C:\Users\Robo\Documents\ILZGJC>
```

1. feladat:

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

```
Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Robo>cd Documents

C:\Users\Robo\Documents>cd ILZGJC

C:\Users\Robo\Documents\ILZGJC>move bokor\barack fa
1 dir(s) moved.

C:\Users\Robo\Documents\ILZGJC>move land\kokusz fa
1 dir(s) moved.

C:\Users\Robo\Documents\ILZGJC>tree
Folder PATH listing
Volume serial number is 96A4-B342
C:.
├── bokor
│   ├── banan
│   └── mogyoro
├── fa
│   ├── banan
│   ├── barack
│   ├── kokusz
│   ├── korte
│   └── szeder
└── land
    └── szeder

C:\Users\Robo\Documents\ILZGJC>
```

1. feladat:

D, Törölje a *neptunkod/land* katalógust a teljes tartalmával.

Hozza létre a következő szöveges állományokat:

*neptunkod/bokor/banan/ leiras.txt*

*neptunkod/tree/felsorolas.txt*

```
Command Prompt
Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Robo>cd Documents

C:\Users\Robo\Documents>cd ilzq
The system cannot find the path specified.

C:\Users\Robo\Documents>cd ILZGJC

C:\Users\Robo\Documents\ILZGJC>rmdir /S land
land, Are you sure (Y/N)? y

C:\Users\Robo\Documents\ILZGJC>tree
'tree' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Robo\Documents\ILZGJC>tree
Folder PATH listing
Volume serial number is 96A4-B342
C:.
├── bokor
│   ├── banan
│   └── mogyoro
└── fa
    ├── banan
    ├── barack
    ├── kokusz
    ├── korte
    └── szeder

C:\Users\Robo\Documents\ILZGJC>
```

```
Command Prompt
(c) Microsoft Corporation. All rights reserved.

C:\Users\Robo>cd Documents

C:\Users\Robo\Documents>cd ILZGJC

C:\Users\Robo\Documents\ILZGJC>cd bokor

C:\Users\Robo\Documents\ILZGJC\bokor>cd banan

C:\Users\Robo\Documents\ILZGJC\bokor\banan>notepad leiras.txt

C:\Users\Robo\Documents\ILZGJC\bokor\banan>cd ..

C:\Users\Robo\Documents\ILZGJC\bokor>cd ..

C:\Users\Robo\Documents\ILZGJC>cd tree
The system cannot find the path specified.

C:\Users\Robo\Documents\ILZGJC>cd fa

C:\Users\Robo\Documents\ILZGJC\fa>notepad felsorolas.txt

C:\Users\Robo\Documents\ILZGJC\fa>cd ..

C:\Users\Robo\Documents\ILZGJC>tree
Folder PATH listing
Volume serial number is 96A4-B342
C:.
├── bokor
│   ├── banan
│   └── mogyoro
└── fa
    ├── banan
    ├── barack
    ├── kokusz
    ├── korte
    └── szeder

C:\Users\Robo\Documents\ILZGJC>
```

1. feladat:

E, A *leiras.txt* szöveges állományba írjon 3 sort a barackról.

A *felsorolas* szöveges állományba soroljon fel legalább 5 csoporttársa nevét.



```
leiras.txt - Notepad
File Edit Format View Help
A magyar nyelvben „őszibarack” néven említjük összes termesztett és magról kelt változatát
de a kényesebb, általában késői külföldi fajták „francia barack” néven is ismertek.
Voltaképpen mindkét elnevezés helytelen, mert nem „ősz”i
```



```
felsorolas.txt - Notepad
File Edit Format View Help
Kocsis Zoltán
Juhász Balázs
Nyíri Levente
Rakaczki Dániel
Tisza Marcell
```

1. feladat:

F, Listázza a *neptunkod* mappa tartalmát úgy, hogy megjelenjen az almappák tartalma is.

```
C:\Users\Robo\Documents\ILZGJC>tree
Folder PATH listing
Volume serial number is 96A4-B342
C:..
|
+--- bokor
|
|   +--- banan
|   +--- mogyoro
|
+--- fa
|
|   +--- banan
|   +--- barack
|   +--- kokusz
|   +--- korte
|   +--- szeder
```

1. feladat:

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

```
Command Prompt
Volume Serial Number is 96A4-B342

Directory of C:\Users\Robo\Documents\ILZGJC\fa

15/02/2022  13:26    <DIR>          korte
               0 File(s)              0 bytes

Total Files Listed:
               0 File(s)              0 bytes
               1 Dir(s)  371,446,685,696 bytes free

C:\Users\Robo\Documents\ILZGJC>dir *e*  /s
Volume in drive C has no label.
Volume Serial Number is 96A4-B342

Directory of C:\Users\Robo\Documents\ILZGJC\bokor\banan

15/02/2022  14:08                267 leiras.txt
               1 File(s)              267 bytes

Directory of C:\Users\Robo\Documents\ILZGJC\fa

15/02/2022  14:13                80 felsorolas.txt
15/02/2022  13:26    <DIR>          korte
15/02/2022  13:27    <DIR>          szeder
               1 File(s)              80 bytes

Total Files Listed:
               2 File(s)              347 bytes
               2 Dir(s)  371,446,685,696 bytes free

C:\Users\Robo\Documents\ILZGJC>dir *e  /b /s
C:\Users\Robo\Documents\ILZGJC\fa\korte

C:\Users\Robo\Documents\ILZGJC>dir *e*  /b /s
C:\Users\Robo\Documents\ILZGJC\bokor\banan\leiras.txt
C:\Users\Robo\Documents\ILZGJC\fa\felsorolas.txt
C:\Users\Robo\Documents\ILZGJC\fa\szeder

C:\Users\Robo\Documents\ILZGJC>
```



1. feladat:

H, Tegye mindenki számára olvashatóvá a *felsorolas.txt* file-t.

```
Command Prompt
C:\Users\Robo\Documents\ILZGJC\fa>sort felsorolas.txt /o felsorolas.txt
C:\Users\Robo\Documents\ILZGJC\fa>icacls felsorolas /t /grant Everyone:R
Successfully processed 0 files; Failed processing 0 files
C:\Users\Robo\Documents\ILZGJC\fa>
```

1. feladat:

I, Jelenítse meg, hogy mennyi helyet foglal a merevlemezen a *neptunkod* mappa az al-mappáival együtt.

```
Command Prompt
C:\Users\Robo\Documents\ILZGJC>dir
Volume in drive C has no label.
Volume Serial Number is 96A4-B342

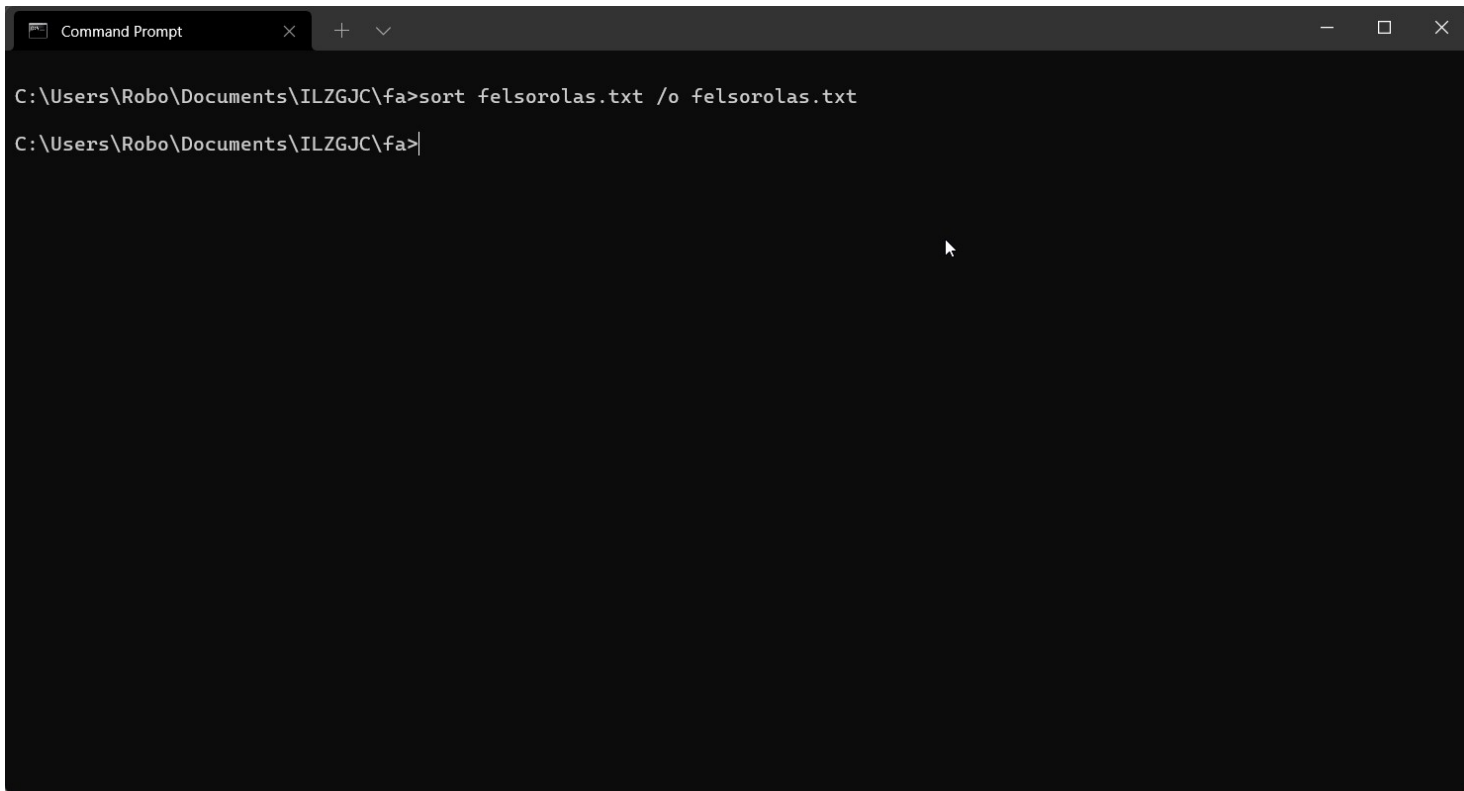
Directory of C:\Users\Robo\Documents\ILZGJC

15/02/2022  13:45    <DIR>        .
15/02/2022  14:38    <DIR>        ..
15/02/2022  13:40    <DIR>        bokor
15/02/2022  14:09    <DIR>        fa
               0 File(s)                0 bytes
               4 Dir(s)  371,440,738,304 bytes free

C:\Users\Robo\Documents\ILZGJC>
```

1. feladat:

J, Rendezze ABC-szerint a *felsorolas.txt* file tartalmát.

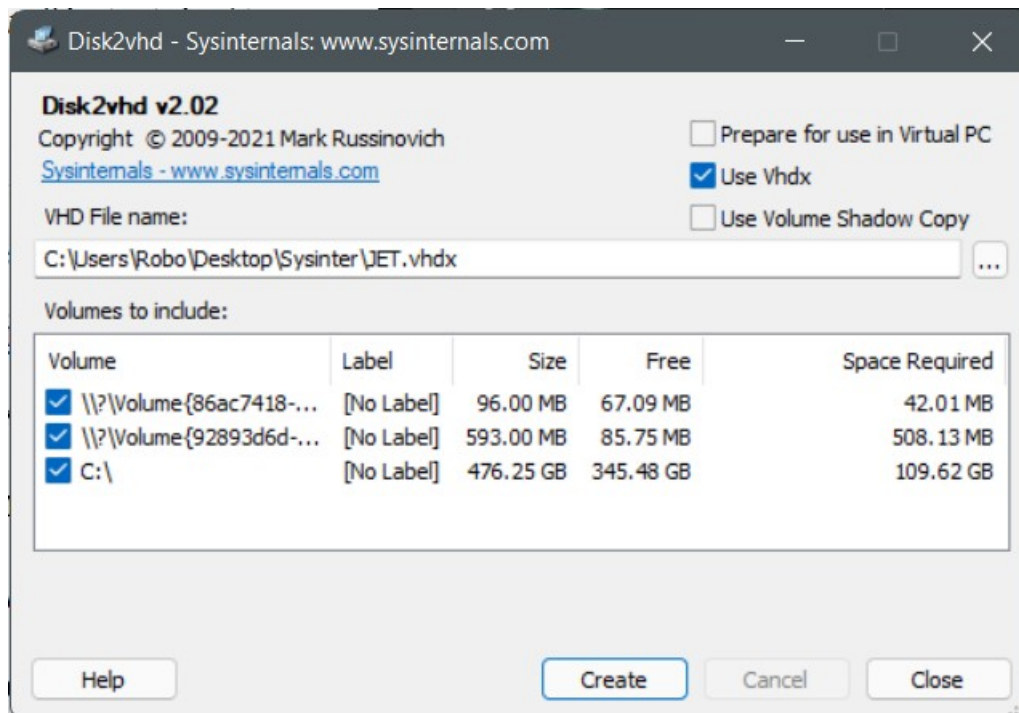


```
Command Prompt
C:\Users\Robo\Documents\ILZGJC\fa>sort felsorolas.txt /o felsorolas.txt
C:\Users\Robo\Documents\ILZGJC\fa>
```

2, feladat:

Tölts le a *Sysinternals Suite* csomagot, majd csomagolja ki. A Windows belső működését lehet tanulmányozni, vagy a hibakeresésben segít.

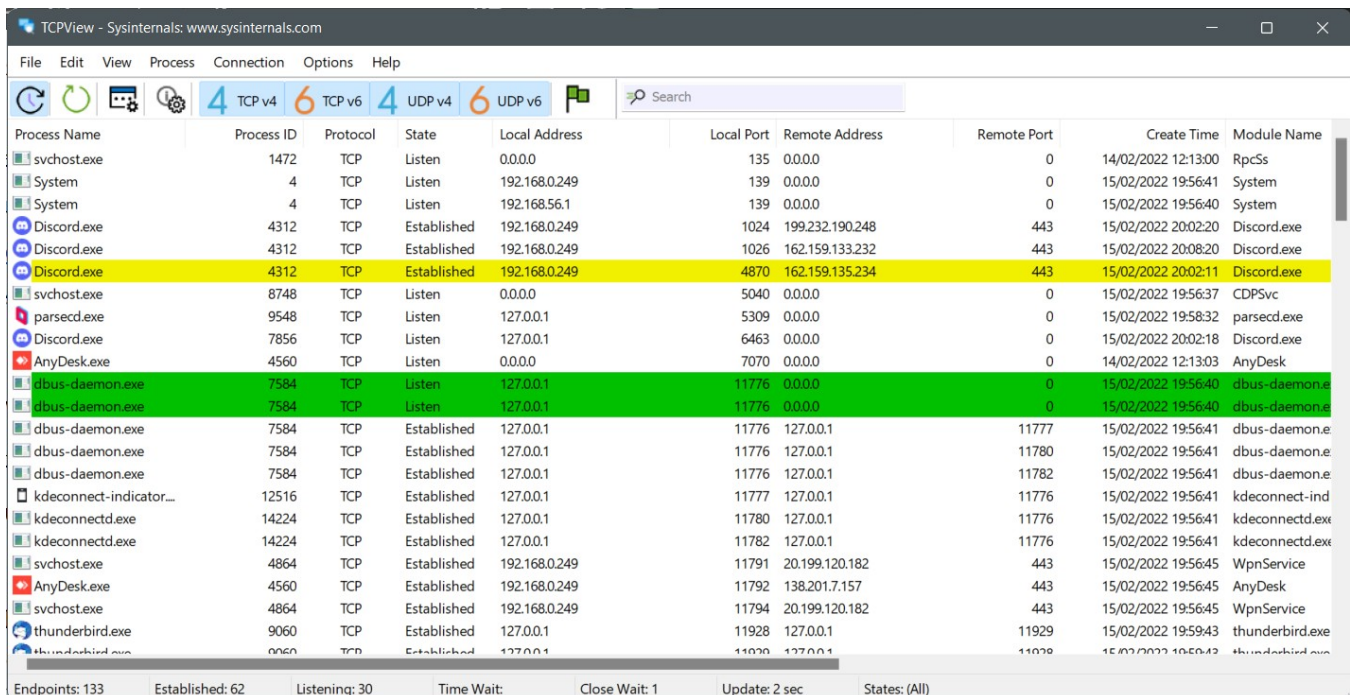
A, File and Disk Utilities (Disk2vhd)



A Disk2vhd egy olyan segédprogram, amely létrehozza a fizikai lemezek VHD-változatait (Virtual Hard Disk – Microsoft Virtual Machine disk format).

## 2. feladat

### B, Networking Utilities (TCPView)



The screenshot shows the TCPView application window. The title bar reads 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Edit', 'View', 'Process', 'Connection', 'Options', and 'Help'. Below the menu is a toolbar with icons for refreshing, pausing, settings, and a search bar. The main display is a table of network connections. The table has columns for Process Name, Process ID, Protocol, State, Local Address, Local Port, Remote Address, Remote Port, Create Time, and Module Name. The table lists various processes and their network activity. At the bottom, a status bar shows summary statistics: Endpoints: 133, Established: 62, Listening: 30, Time Wait: 1, Close Wait: 1, Update: 2 sec, States: (All).

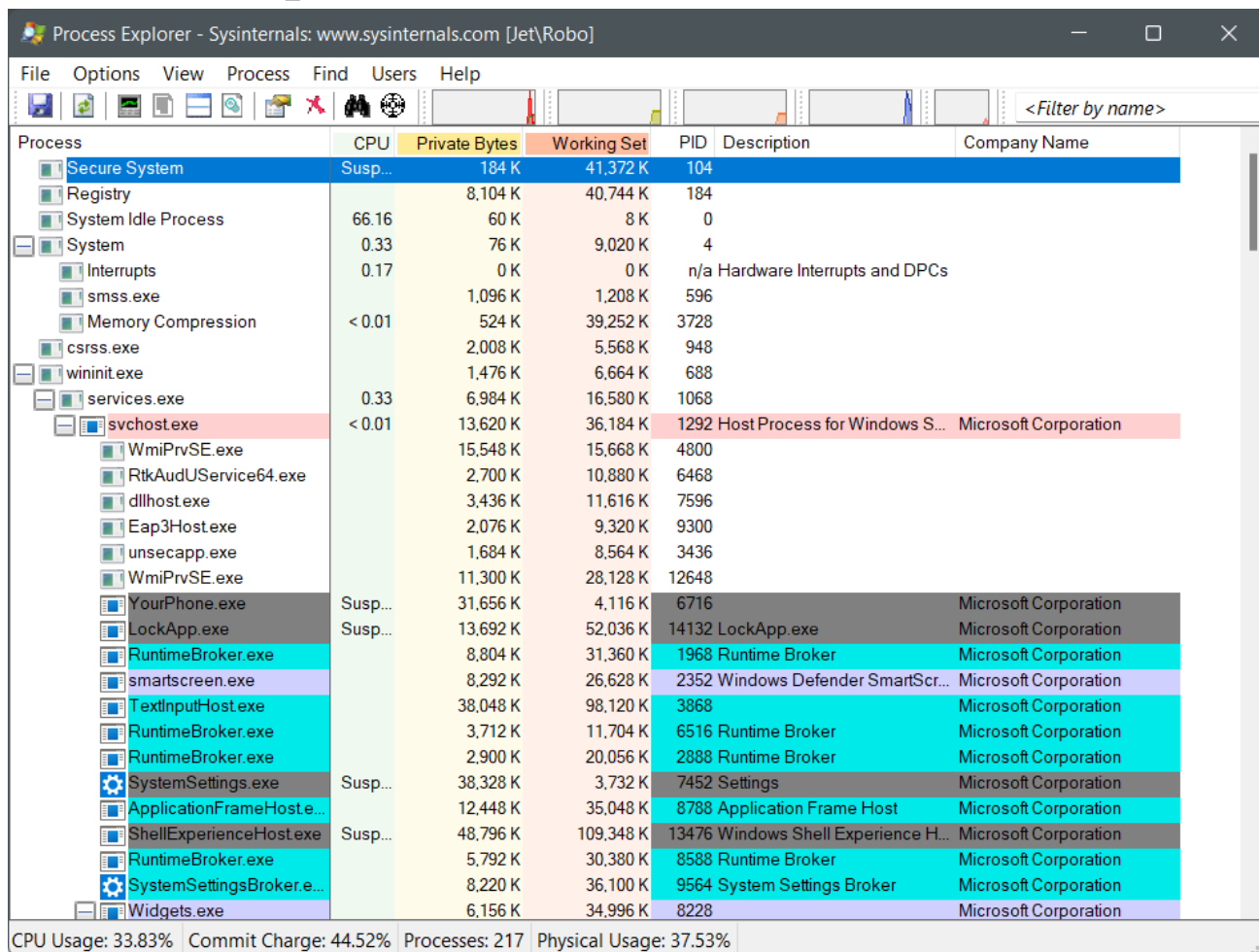
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	1472	TCP	Listen	0.0.0.0	135	0.0.0.0	0	14/02/2022 12:13:00	RpcSs
System	4	TCP	Listen	192.168.0.249	139	0.0.0.0	0	15/02/2022 19:56:41	System
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	15/02/2022 19:56:40	System
Discord.exe	4312	TCP	Established	192.168.0.249	1024	199.232.190.248	443	15/02/2022 20:02:20	Discord.exe
Discord.exe	4312	TCP	Established	192.168.0.249	1026	162.159.133.232	443	15/02/2022 20:08:20	Discord.exe
Discord.exe	4312	TCP	Established	192.168.0.249	4870	162.159.135.234	443	15/02/2022 20:02:11	Discord.exe
svchost.exe	8748	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	15/02/2022 19:56:37	CDPSvc
parsecd.exe	9548	TCP	Listen	127.0.0.1	5309	0.0.0.0	0	15/02/2022 19:58:32	parsecd.exe
Discord.exe	7856	TCP	Listen	127.0.0.1	6463	0.0.0.0	0	15/02/2022 20:02:18	Discord.exe
AnyDesk.exe	4560	TCP	Listen	0.0.0.0	7070	0.0.0.0	0	14/02/2022 12:13:03	AnyDesk
dbus-daemon.exe	7584	TCP	Listen	127.0.0.1	11776	0.0.0.0	0	15/02/2022 19:56:40	dbus-daemon.e
dbus-daemon.exe	7584	TCP	Listen	127.0.0.1	11776	0.0.0.0	0	15/02/2022 19:56:40	dbus-daemon.e
dbus-daemon.exe	7584	TCP	Established	127.0.0.1	11776	127.0.0.1	11777	15/02/2022 19:56:41	dbus-daemon.e
dbus-daemon.exe	7584	TCP	Established	127.0.0.1	11776	127.0.0.1	11780	15/02/2022 19:56:41	dbus-daemon.e
dbus-daemon.exe	7584	TCP	Established	127.0.0.1	11776	127.0.0.1	11782	15/02/2022 19:56:41	dbus-daemon.e
kdeconnect-indicator...	12516	TCP	Established	127.0.0.1	11777	127.0.0.1	11776	15/02/2022 19:56:41	kdeconnect-ind
kdeconnectd.exe	14224	TCP	Established	127.0.0.1	11780	127.0.0.1	11776	15/02/2022 19:56:41	kdeconnectd.exe
kdeconnectd.exe	14224	TCP	Established	127.0.0.1	11782	127.0.0.1	11776	15/02/2022 19:56:41	kdeconnectd.exe
svchost.exe	4864	TCP	Established	192.168.0.249	11791	20.199.120.182	443	15/02/2022 19:56:45	WpnService
AnyDesk.exe	4560	TCP	Established	192.168.0.249	11792	138.201.7.157	443	15/02/2022 19:56:45	AnyDesk
svchost.exe	4864	TCP	Established	192.168.0.249	11794	20.199.120.182	443	15/02/2022 19:56:45	WpnService
thunderbird.exe	9060	TCP	Established	127.0.0.1	11928	127.0.0.1	11929	15/02/2022 19:59:43	thunderbird.exe
thunderbird.exe	9060	TCP	Established	127.0.0.1	11928	127.0.0.1	11928	15/02/2022 19:59:43	thunderbird.exe

Endpoints: 133   Established: 62   Listening: 30   Time Wait: 1   Close Wait: 1   Update: 2 sec   States: (All)

Ez a szoftver leírást ad bizonyos folyamatokról, pontosan azok, amelyek TCP vagy UDP protokollok szerint dolgoznak. A szoftver segít beazonosítani, hogy mely programok csatlakoznak az internetre, és mennyi adatot fogadtak/küldtek, lokálisan hol találhatóak meg, milyen a státuszuk.

## 2. feladat

### C, Process Explorer



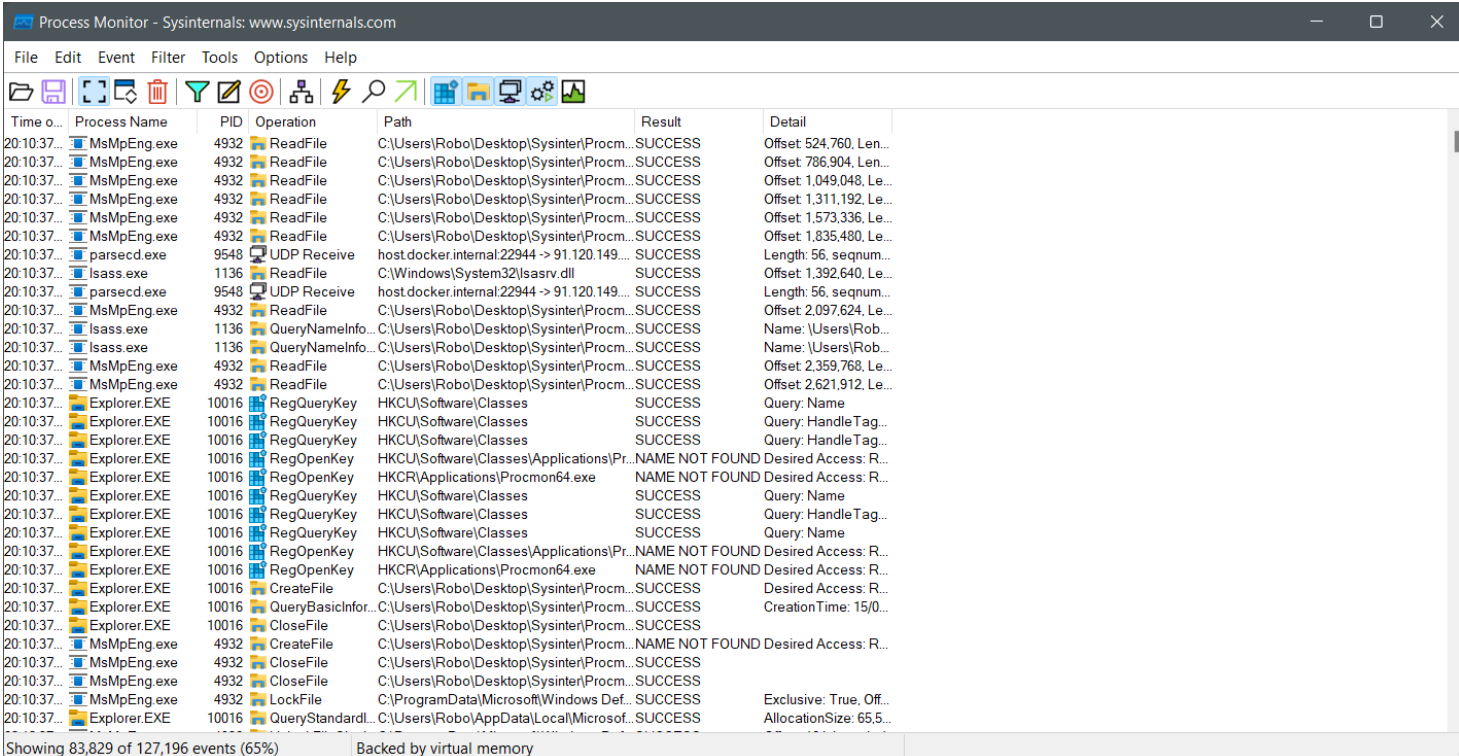
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System	Susp...	184 K	41,372 K	104		
Registry		8,104 K	40,744 K	184		
System Idle Process	66.16	60 K	8 K	0		
System	0.33	76 K	9,020 K	4		
Interrupts	0.17	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,096 K	1,208 K	596		
Memory Compression	< 0.01	524 K	39,252 K	3728		
csrss.exe		2,008 K	5,568 K	948		
wininit.exe		1,476 K	6,664 K	688		
services.exe	0.33	6,984 K	16,580 K	1068		
svchost.exe	< 0.01	13,620 K	36,184 K	1292	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		15,548 K	15,668 K	4800		
RtkAudUService64.exe		2,700 K	10,880 K	6468		
dllhost.exe		3,436 K	11,616 K	7596		
Eap3Host.exe		2,076 K	9,320 K	9300		
unsecapp.exe		1,684 K	8,564 K	3436		
WmiPrvSE.exe		11,300 K	28,128 K	12648		
YourPhone.exe	Susp...	31,656 K	4,116 K	6716		Microsoft Corporation
LockApp.exe	Susp...	13,692 K	52,036 K	14132	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		8,804 K	31,360 K	1968	Runtime Broker	Microsoft Corporation
smartscreen.exe		8,292 K	26,628 K	2352	Windows Defender SmartScr...	Microsoft Corporation
TextInputHost.exe		38,048 K	98,120 K	3868		Microsoft Corporation
RuntimeBroker.exe		3,712 K	11,704 K	6516	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2,900 K	20,056 K	2888	Runtime Broker	Microsoft Corporation
SystemSettings.exe	Susp...	38,328 K	3,732 K	7452	Settings	Microsoft Corporation
ApplicationFrameHost.exe		12,448 K	35,048 K	8788	Application Frame Host	Microsoft Corporation
ShellExperienceHost.exe	Susp...	48,796 K	109,348 K	13476	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		5,792 K	30,380 K	8588	Runtime Broker	Microsoft Corporation
SystemSettingsBroker.exe		8,220 K	36,100 K	9564	System Settings Broker	Microsoft Corporation
Widgets.exe		6,156 K	34,996 K	8228		Microsoft Corporation

CPU Usage: 33.83% | Commit Charge: 44.52% | Processes: 217 | Physical Usage: 37.53%

Ez a szoftver egy folyamat megfigyelő, mely a Task Manager-hez képest sokkal részletesebb leírást nyújt az adott processekről, rendszer információkról. Leginkább DLL verzió hibakezelésre alkalmazzák a leggyakrabban, mert ez a program segít abban, hogy kiszűrje mely processzek milyen DLL fájlt töltenek be.

## 2. feladat

# C, Process Monitor



The screenshot shows the Process Monitor application window. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Edit", "Event", "Filter", "Tools", "Options", and "Help". Below the menu is a toolbar with various icons for file operations, filtering, and viewing. The main area displays a list of system events in a table format. The table has columns for "Time o...", "Process Name", "PID", "Operation", "Path", "Result", and "Detail". The events are filtered to show only those from "MsMpEng.exe" and "Explorer.EXE". The status bar at the bottom indicates "Showing 83,829 of 127,196 events (65%)" and "Backed by virtual memory".

Time o...	Process Name	PID	Operation	Path	Result	Detail
20:10:37...	MsMpEng.exe	4932	ReadFile	C:\Users\Robo\Desktop\Sysinterl\Procm...	SUCCESS	Offset 524,760, Len...
20:10:37...	MsMpEng.exe	4932	ReadFile	C:\Users\Robo\Desktop\Sysinterl\Procm...	SUCCESS	Offset 786,904, Len...
20:10:37...	MsMpEng.exe	4932	ReadFile	C:\Users\Robo\Desktop\Sysinterl\Procm...	SUCCESS	Offset 1,049,048, Le...
20:10:37...	MsMpEng.exe	4932	ReadFile	C:\Users\Robo\Desktop\Sysinterl\Procm...	SUCCESS	Offset 1,311,192, Le...
20:10:37...	MsMpEng.exe	4932	ReadFile	C:\Users\Robo\Desktop\Sysinterl\Procm...	SUCCESS	Offset 1,573,336, Le...
20:10:37...	MsMpEng.exe	4932	ReadFile	C:\Users\Robo\Desktop\Sysinterl\Procm...	SUCCESS	Offset 1,835,480, Le...
20:10:37...	parsecd.exe	9548	UDP Receive	host.docker.internal:22944 -> 91.120.149...	SUCCESS	Length: 56, seqnum...
20:10:37...	lsass.exe	1136	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1,392,640, Le...
20:10:37...	parsecd.exe	9548	UDP Receive	host.docker.internal:22944 -> 91.120.149...	SUCCESS	Length: 56, seqnum...
20:10:37...	MsMpEng.exe	4932	ReadFile	C:\Users\Robo\Desktop\Sysinterl\Procm...	SUCCESS	Offset 2,097,624, Le...
20:10:37...	lsass.exe	1136	QueryNameInfo...	C:\Users\Robo\Desktop\Sysinterl\Procm...	SUCCESS	Name: \Users\Rob...
20:10:37...	lsass.exe	1136	QueryNameInfo...	C:\Users\Robo\Desktop\Sysinterl\Procm...	SUCCESS	Name: \Users\Rob...
20:10:37...	MsMpEng.exe	4932	ReadFile	C:\Users\Robo\Desktop\Sysinterl\Procm...	SUCCESS	Offset 2,359,768, Le...
20:10:37...	MsMpEng.exe	4932	ReadFile	C:\Users\Robo\Desktop\Sysinterl\Procm...	SUCCESS	Offset 2,621,912, Le...
20:10:37...	Explorer.EXE	10016	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
20:10:37...	Explorer.EXE	10016	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
20:10:37...	Explorer.EXE	10016	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
20:10:37...	Explorer.EXE	10016	RegOpenKey	HKCU\Software\Classes\Applications\Pr...	NAME NOT FOUND	Desired Access: R...
20:10:37...	Explorer.EXE	10016	RegOpenKey	HKCR\Applications\Procm64.exe	NAME NOT FOUND	Desired Access: R...
20:10:37...	Explorer.EXE	10016	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
20:10:37...	Explorer.EXE	10016	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
20:10:37...	Explorer.EXE	10016	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
20:10:37...	Explorer.EXE	10016	RegOpenKey	HKCU\Software\Classes\Applications\Pr...	NAME NOT FOUND	Desired Access: R...
20:10:37...	Explorer.EXE	10016	RegOpenKey	HKCR\Applications\Procm64.exe	NAME NOT FOUND	Desired Access: R...
20:10:37...	Explorer.EXE	10016	CreateFile	C:\Users\Robo\Desktop\Sysinterl\Procm...	SUCCESS	Desired Access: R...
20:10:37...	Explorer.EXE	10016	QueryBasicInfor...	C:\Users\Robo\Desktop\Sysinterl\Procm...	SUCCESS	CreationTime: 15/0...
20:10:37...	Explorer.EXE	10016	CloseFile	C:\Users\Robo\Desktop\Sysinterl\Procm...	SUCCESS	
20:10:37...	MsMpEng.exe	4932	CreateFile	C:\Users\Robo\Desktop\Sysinterl\Procm...	NAME NOT FOUND	Desired Access: R...
20:10:37...	MsMpEng.exe	4932	CloseFile	C:\Users\Robo\Desktop\Sysinterl\Procm...	SUCCESS	
20:10:37...	MsMpEng.exe	4932	CloseFile	C:\Users\Robo\Desktop\Sysinterl\Procm...	SUCCESS	
20:10:37...	MsMpEng.exe	4932	LockFile	C:\ProgramData\Microsoft\Windows Def...	SUCCESS	Exclusive: True, Off...
20:10:37...	Explorer.EXE	10016	QueryStandardI...	C:\Users\Robo\AppData\Local\Microsof...	SUCCESS	AllocationSize: 65.5...

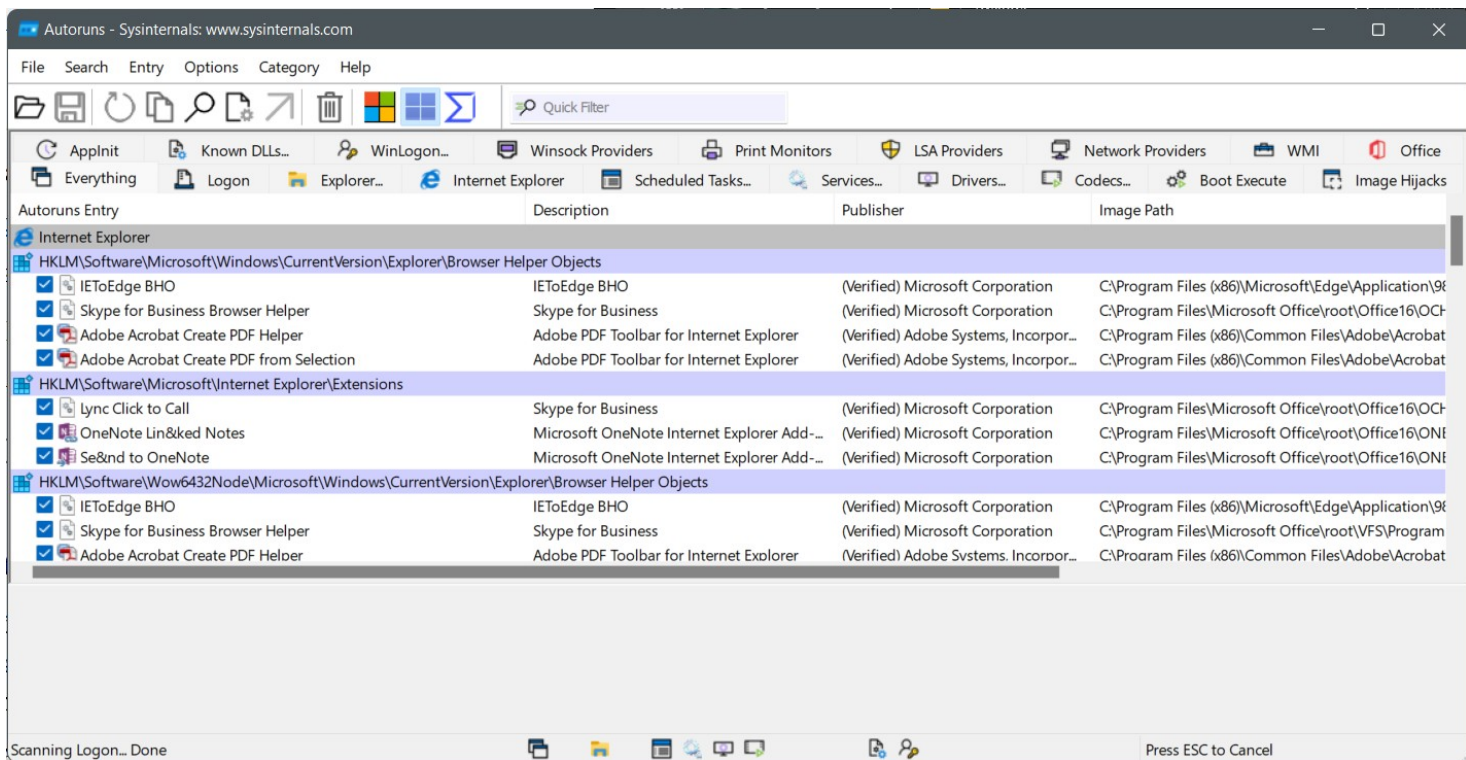
Showing 83,829 of 127,196 events (65%)      Backed by virtual memory

A Process Monitor egy fejlett megfigyelő eszköz a Windows számára, amely valós idejű fájlrendszer, rendszerleíró adatbázis és folyamat/szál tevékenységet mutat.



## 2. feladat

### C, AutoRuns



Ez a program leírást ad, hogy mely szoftverek indulnak el miután az operációs rendszer bootolása befejeződött. Nem feltétlenül csak szoftverek listáját adja meg, hanem emellé megnézhetjük mely DLL fájlok, szolgáltatások, driverek, Codec-ek indulnak el. A lista indulás sorrendje szerint van prezentálva, és minden esetben a cmd.exe lesz az az alapprogram ami legelőször elindul.

## 2. feladat

### D, LogonSession

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Robo\Desktop\Sysinter

C:\Users\Robo\Desktop\Sysinter>logonsessions.exe

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\JET$
    Auth package:   NTLM
    Logon type:     (none)
    Session:        0
    Sid:            S-1-5-18
    Logon time:     14/02/2022 12:13:00
    Logon server:
    DNS Domain:
    UPN:

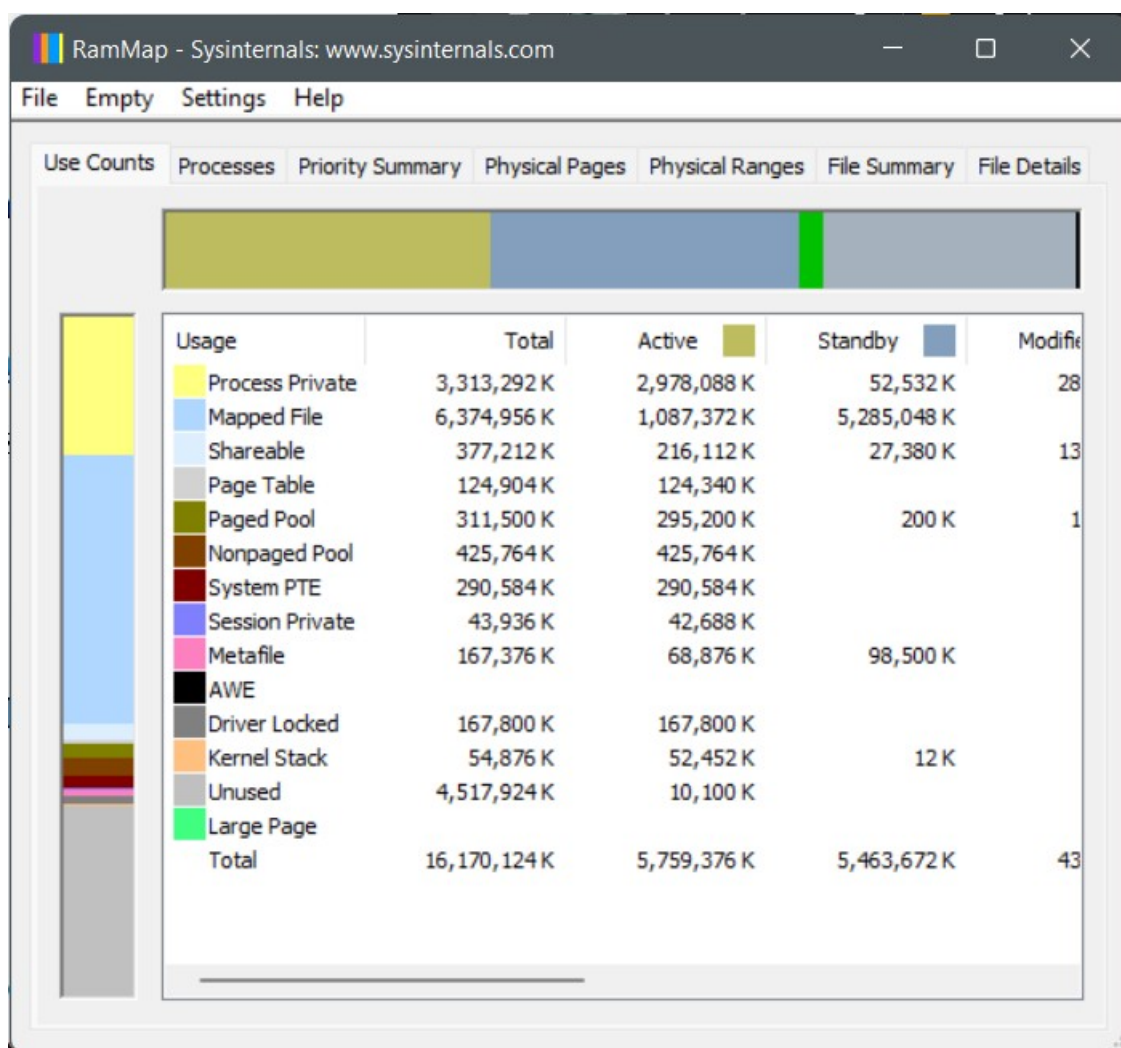
[1] Logon session 00000000:0000e384:
    User name:
    Auth package:   NTLM
    Logon type:     (none)
    Session:        0
    Sid:            (none)
    Logon time:     14/02/2022 12:13:00
```

A program információt arról, hogy az adott végberendezés sessionjeit melyik felhasználó használja, mióta, milyen módon, melyik szerveren (ha a számítógép esetlegesen egy belső hálózatban lenne felkonfigurálva).



## 2. feladat

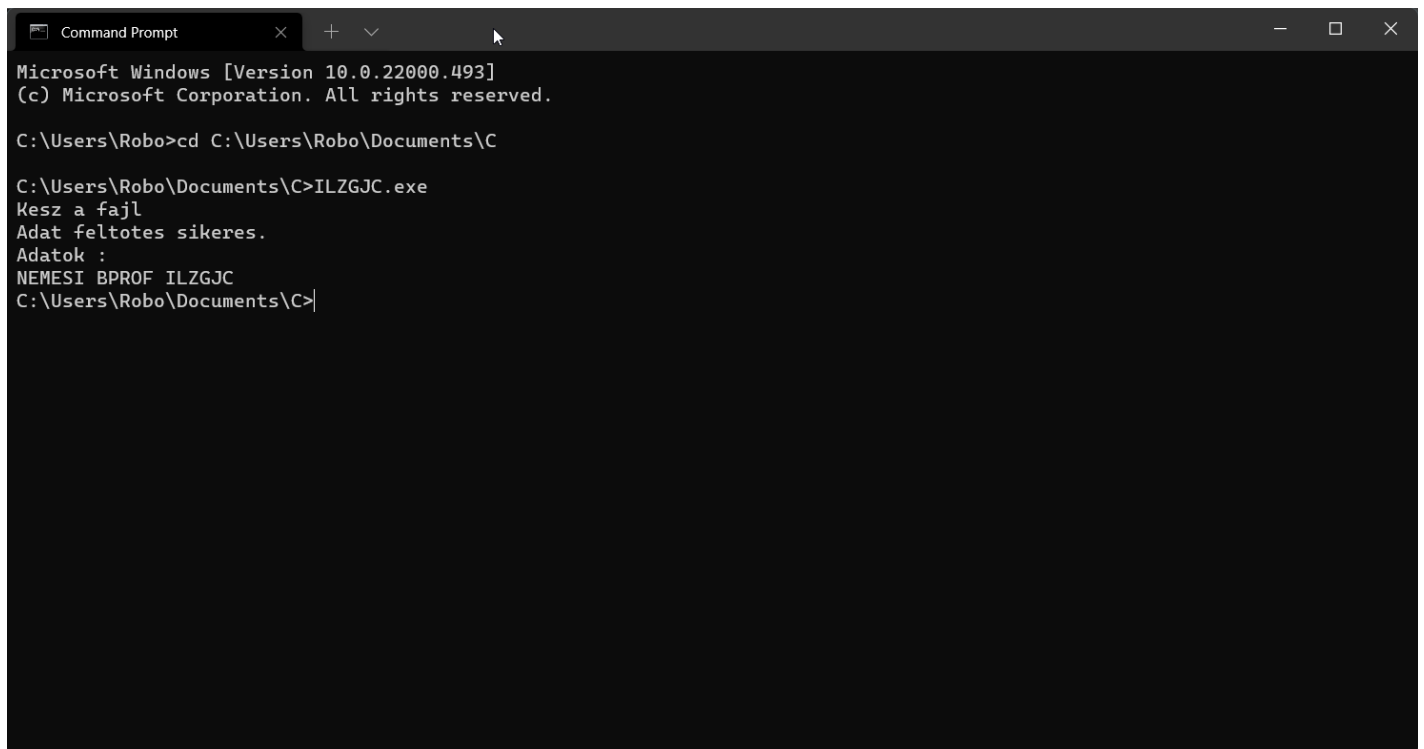
### E, RAMMap



A program segít megértetni velünk, hogy a Windows hogyan kezeli a fizikai memóriát. Megmutatja, hogy az összes RAM-ból (az én esetemben 8 GB – 8 345 936 K) bizonyos részei milyen használat alatt van, mint például 3 GB körüli memóriaterület mapped file által lefoglalt terület van jelen, melyből ennek az 1/3-ad része aktív, azaz adott fájlok tárgya a virtuális memóriában aktív feldolgozás alatt vannak, míg a maradék 2/3-ad része még sorban áll.

### 3. feladat:

## C programkód



```
Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Robo>cd C:\Users\Robo\Documents\C

C:\Users\Robo\Documents\C>ILZGJC.exe
Kesz a fajl
Adat feltotes sikeres.
Adatok :
NEMESI BPROF ILZGJC
C:\Users\Robo\Documents\C>
```



```
nemesi.txt - Notepad
File Edit Format View Help
NEMESI BPROF ILZGJC

Ln 1, Col 1    100%    Windows (CRLF)    UTF-8
```

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

For Help, press F1

### 3. feladat:

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

Dependency Walker - (ILZGJC.exe)

File Edit View Options Profile Window Help

Module List:

- KERNEL32.DLL
- API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
- API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL
- NTDLL.DLL
- KERNELBASE.DLL
- API-MS-WIN-CORE-PROCESSSTHEADS-L1-1-0.DLL
- API-MS-WIN-CORE-PROCESSSTHEADS-L1-1-3.DLL
- API-MS-WIN-CORE-PROCESSSTHEADS-L1-1-2.DLL
- API-MS-WIN-CORE-PROCESSSTHEADS-L1-1-1.DLL
- API-MS-WIN-CORE-REGISTRY-L1-1-0.DLL
- API-MS-WIN-CORE-HEAP-L1-1-0.DLL
- API-MS-WIN-CORE-MEMORY-L1-1-0.DLL
- API-MS-WIN-CORE-MEMORY-L1-2.DLL
- API-MS-WIN-CORE-HANDLE-L1-1-0.DLL
- API-MS-WIN-CORE-SYNCH-L1-1-0.DLL
- API-MS-WIN-CORE-SYNCH-L1-2-1.DLL
- API-MS-WIN-CORE-SYNCH-L1-2-0.DLL

Export Table:

Ordinal	Hint	Function	Entry Point
8 (0x0008)	934 (0x03A6)	RtlDispatchAPC	0x0002A140
9 (0x0009)	723 (0x02D3)	RtlActivateActivationContextUnsafeFast	0x0003F240
10 (0x000A)	891 (0x037B)	RtlDeactivateActivationContextUnsafeFast	0x0003EF80
11 (0x000B)	1185 (0x04A1)	RtlInterlockedPushListSList	0x000C2700
12 (0x000C)	1534 (0x05FE)	RtlUlongByteSwap	0x000C2780
13 (0x000D)	1535 (0x05FF)	RtlUlongLongByteSwap	0x000C27C0
14 (0x000E)	1579 (0x062B)	RtlUshortByteSwap	0x000C27E0
15 (0x000F)	0 (0x0000)	A_SHAFinal	0x0006AE80
16 (0x0010)	1 (0x0001)	A_SHAInit	0x00098DD0
17 (0x0011)	2 (0x0002)	A_SHAUpdate	0x0006AF60

Module List:

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).											
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).											
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL	Error opening file. The system cannot find the file specified (2).											
API-MS-WIN-CORE-COMM-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).											
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL	Error opening file. The system cannot find the file specified (2).											
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL	Error opening file. The system cannot find the file specified (2).											
API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL	Error opening file. The system cannot find the file specified (2).											
API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL	Error opening file. The system cannot find the file specified (2).											
API-MS-WIN-CORE-CRT-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).											

Errors:

- Error: At least one required implicit or forwarded dependency was not found.
- Error: At least one module has an unresolved import due to a missing export function in an implicitly dependent module.
- Error: Modules with different CPU types were found.
- Error: A circular dependency was detected.
- Warning: At least one delay-load dependency module was not found.
- Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

For Help, press F1

Az NTDLL.DLL a Windows Native API-t exportálja. A natív API az operációs rendszer felhasználói módú összetevői által használt interfész, amelynek a Win32 vagy más API-alrendszerek támogatása nélkül kell futnia.