

# **Operációs rendszerek BSc**

2. Gyak.

2022.02.15.

Készítette:

Karczub Roland Bsc

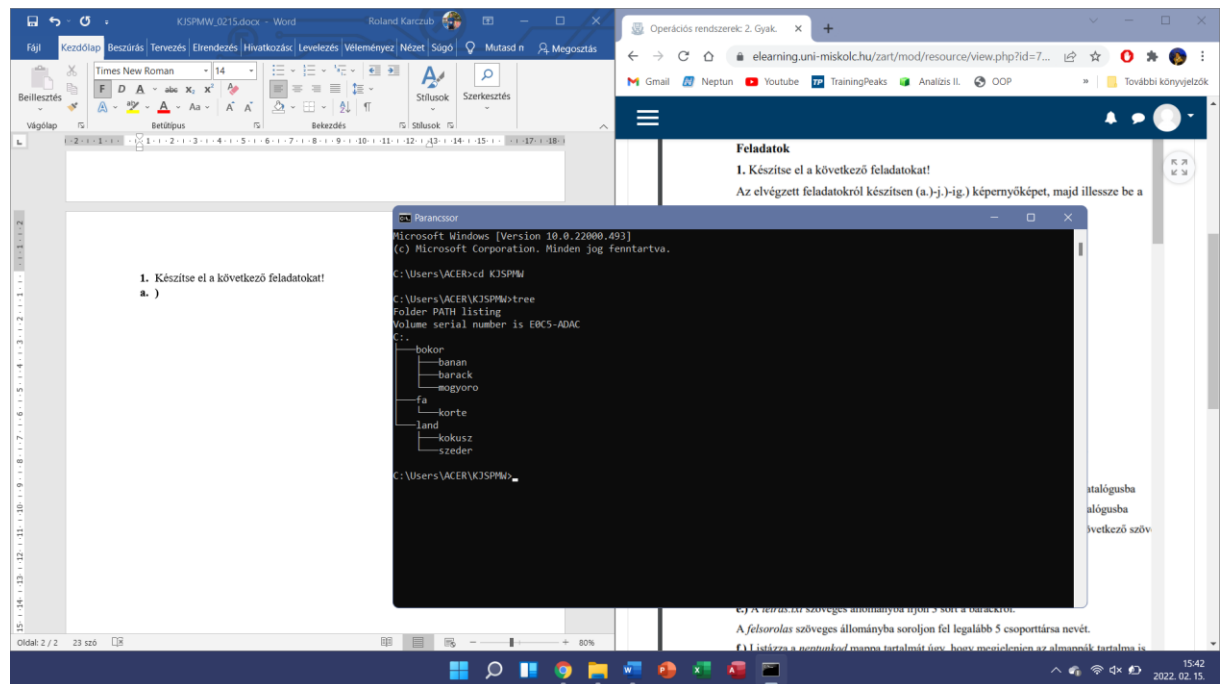
Programtervező informatikus

KJSPMW

**Miskolc, 2022**

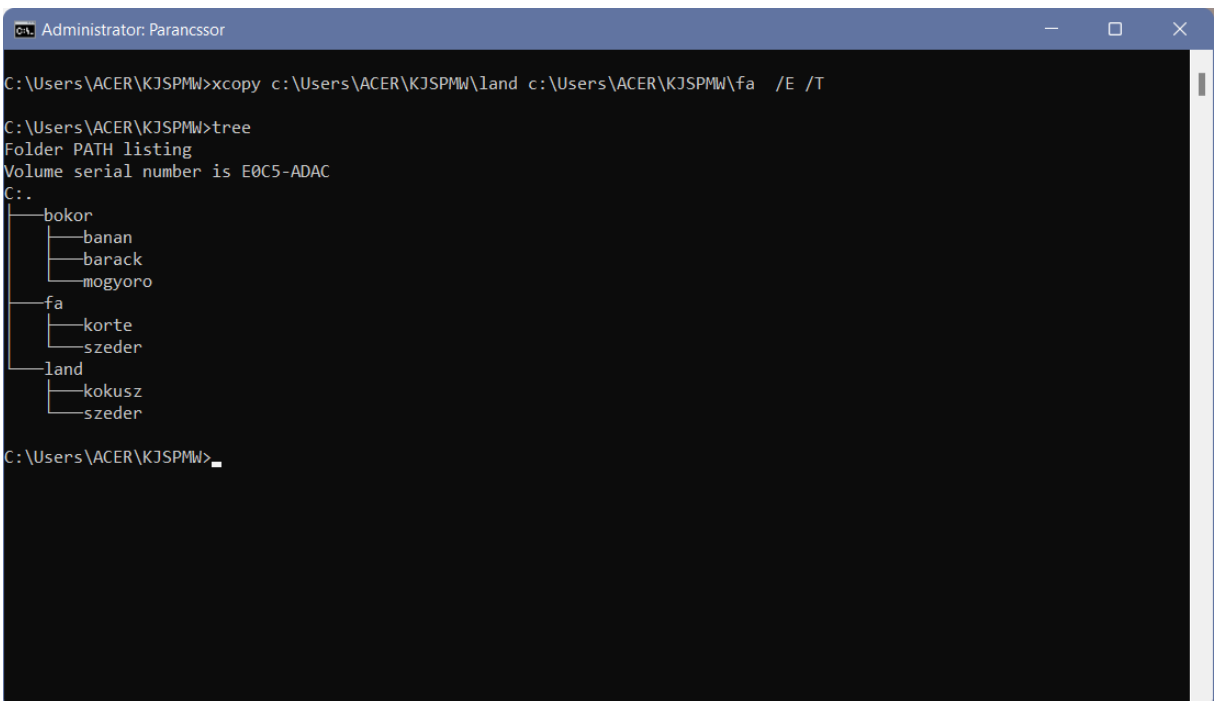
# 1. Készítse el a következő feladatokat!

## a. ) Hozza létre a következő mappa szerkezetet!



## b.) Készítsen másolatot:

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



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

```
Administrator: Parancssor

C:\Users\ACER\KJSPMW>tree
Folder PATH listing
Volume serial number is E0C5-ADAC
C:.
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   ├── banan
│   ├── korte
│   └── szeder
└── land
    ├── kokusz
    └── szeder

C:\Users\ACER\KJSPMW>
```

c.) Végezze el a következő áthelyezéseket!

- a neptunkod /bokor/barack katalógust helyezze át a neptunkod /fa katalógusba:

```
Administrator: Parancssor

├── barack
└── mogyoro
fa
├── banan
├── korte
└── szeder
land
├── kokusz
└── szeder

C:\Users\ACER\KJSPMW>move c:\Users\ACER\KJSPMW\bokor\barack c:\Users\ACER\KJSPMW\fa
1 dir(s) moved.

C:\Users\ACER\KJSPMW>tree
Folder PATH listing
Volume serial number is E0C5-ADAC
C:.
├── bokor
│   ├── banan
│   └── mogyoro
├── fa
│   ├── banan
│   ├── barack
│   ├── korte
│   └── szeder
└── land
    ├── kokusz
    └── szeder

C:\Users\ACER\KJSPMW>
```

- a neptunkod /land /kokusz katalógust helyezze át a neptunkod/fa katalógusba:

```
Administrator: Parancssor

C:\Users\ACER\KJSPM\>tree
.
├── mogyoro
├── fa
│   ├── banan
│   ├── barack
│   ├── korte
│   └── szeder
└── land
    ├── kokusz
    └── szeder

C:\Users\ACER\KJSPM\>move c:\Users\ACER\KJSPM\land\kokusz c:\Users\ACER\KJSPM\fa
1 dir(s) moved.

C:\Users\ACER\KJSPM\>tree
Folder PATH listing
Volume serial number is E0C5-ADAC
C:.
├── bokor
│   ├── banan
│   └── mogyoro
├── fa
│   ├── banan
│   ├── barack
│   ├── kokusz
│   ├── korte
│   └── szeder
└── land
    └── szeder

C:\Users\ACER\KJSPM\>
```

d.) Törölje a neptunkod/land/katalógust a teljes tartalmával.

- Hozza létre a következő szöveges állományokat:

neptunkod/bokor/banan/leiras.txt

neptunkod/tree/felsorolas.txt

```
Administrator: Parancssor

C:\Users\ACER\KJSPM\>cd bokor
C:\Users\ACER\KJSPM\bokor>cd banan
C:\Users\ACER\KJSPM\bokor\banan>type nul > leiras.txt
C:\Users\ACER\KJSPM\bokor\banan>cd/
C:\>cd Users
C:\Users>cd ACER
C:\Users\ACER>cd KJSPM
C:\Users\ACER\KJSPM>cd fa
C:\Users\ACER\KJSPM\fa>type nul > felsorolas.txt
A rendszer nem találja a megadott fájlt.
Error occurred while processing: felsorolas.txt.
C:\Users\ACER\KJSPM\fa>type nul > felsorolas.txt
C:\Users\ACER\KJSPM\fa>tree
Folder PATH listing
Volume serial number is E0C5-ADAC
C:.
├── banan
├── barack
├── kokusz
├── korte
└── szeder

C:\Users\ACER\KJSPM\fa>cd..
C:\Users\ACER\KJSPM>tree
Folder PATH listing
Volume serial number is E0C5-ADAC
C:.
├── bokor
│   ├── banan
│   └── mogyoro
├── fa
│   ├── banan
│   ├── barack
│   ├── kokusz
│   ├── korte
│   └── szeder
└── land
    └── szeder

C:\Users\ACER\KJSPM>cd KJSPM
```

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

```
Administrator: Parancssor

C:\Users\ACER\KJSPMW>cd bokor

C:\Users\ACER\KJSPMW\bokor>cd banan

C:\Users\ACER\KJSPMW\bokor\banan>copy con leiras.txt
Sarga
Overwrite leiras.txt? (Yes/No/All): yes
Kajszí
Őszi
1 file(s) copied.

C:\Users\ACER\KJSPMW\bokor\banan>cd..

C:\Users\ACER\KJSPMW\bokor>cd..

C:\Users\ACER\KJSPMW>cd fa

C:\Users\ACER\KJSPMW\fa>copy con felsorolas.txt
Laci
Overwrite felsorolas.txt? (Yes/No/All): yes
Gabi
Viktor
Mate
Kevin
1 file(s) copied.

C:\Users\ACER\KJSPMW\fa>
```

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

```
Administrator: Parancssor

C:\Users\ACER\KJSPMW>tree /f
Folder PATH listing
Volume serial number is E0C5-ADAC
C:.
├── bokor
│   ├── banan
│   │   └── leiras.txt
│   └── mogyoro
└── fa
    ├── felsorolas.txt
    ├── banan
    ├── barack
    ├── kokusz
    ├── korte
    └── szeder

C:\Users\ACER\KJSPMW>
```

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

```
Administrator: Parancssor
C:\Users\ACER\KJSPMW>dir ?e* /B /S
C:\Users\ACER\KJSPMW\bokor\banan\leiras.txt
C:\Users\ACER\KJSPMW\fa\felsorolas.txt
C:\Users\ACER\KJSPMW>
```

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

```
Administrator: Parancssor
C:\Users\ACER\KJSPMW>cd bokor
C:\Users\ACER\KJSPMW\bokor>cd banan
C:\Users\ACER\KJSPMW\bokor\banan>cd ..
C:\Users\ACER\KJSPMW\bokor>cd ..
C:\Users\ACER\KJSPMW>cd fa
C:\Users\ACER\KJSPMW\fa>icacls felsorolas.txt /reset /t /c /q
Successfully processed 1 files; Failed processing 0 files
C:\Users\ACER\KJSPMW\fa>
```

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

```
Administrator: Parancssor
2022. 02. 16. 14:11 <DIR> ..
0 File(s) 0 bytes

Directory of C:\Users\ACER\KJSPMW\fa\barack
2022. 02. 15. 15:26 <DIR> .
2022. 02. 16. 14:11 <DIR> ..
0 File(s) 0 bytes

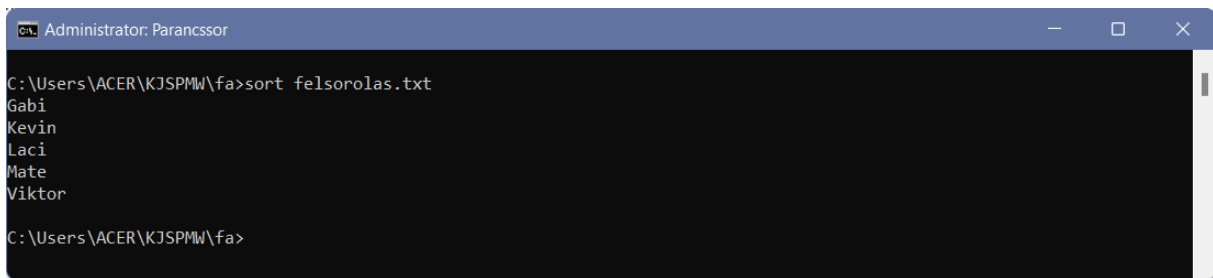
Directory of C:\Users\ACER\KJSPMW\fa\kokusz
2022. 02. 15. 15:30 <DIR> .
2022. 02. 16. 14:11 <DIR> ..
0 File(s) 0 bytes

Directory of C:\Users\ACER\KJSPMW\fa\korte
2022. 02. 15. 15:30 <DIR> .
2022. 02. 16. 14:11 <DIR> ..
0 File(s) 0 bytes

Directory of C:\Users\ACER\KJSPMW\fa\szeder
2022. 02. 15. 15:30 <DIR> .
2022. 02. 16. 14:11 <DIR> ..
0 File(s) 0 bytes

Total Files Listed:
2 File(s) 54 bytes
29 Dir(s) 312 685 735 936 bytes free
C:\Users\ACER>dir /s "KJSPMW"
```

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



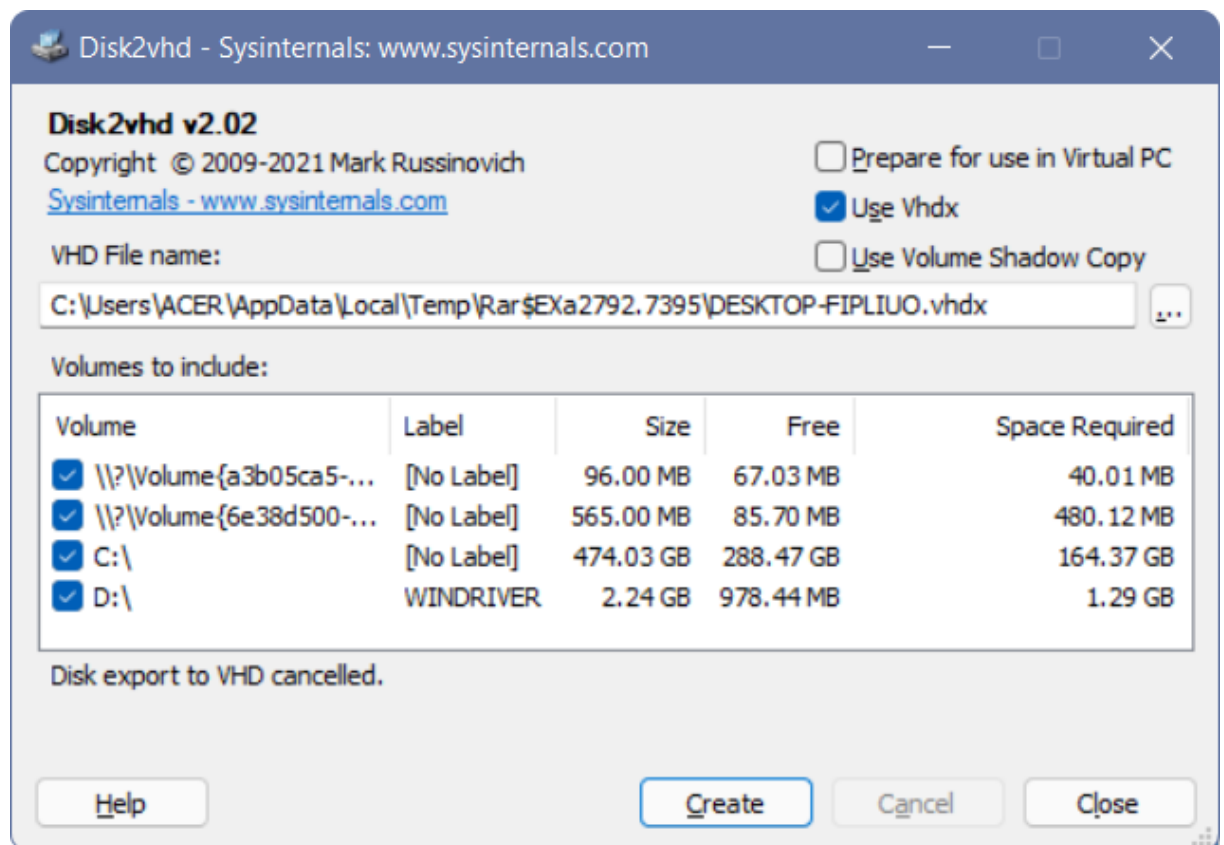
```
C:\Users\ACER\KJSPMW\fa>sort felsorolas.txt
Gabi
Kevin
Laci
Mate
Viktor
C:\Users\ACER\KJSPMW\fa>
```

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

- **File and Disk Utilities (Disk2vhd):**

A Disk2vhd egy olyan segédprogram, amely létrehozza a fizikai lemezek VHD-verzióit a Microsoft Virtual PC-n vagy Microsoft Hyper-V virtuális gépeken való használatra.

A Disk2vhd felhasználói felület felsorolja a rendszeren található köteteket:

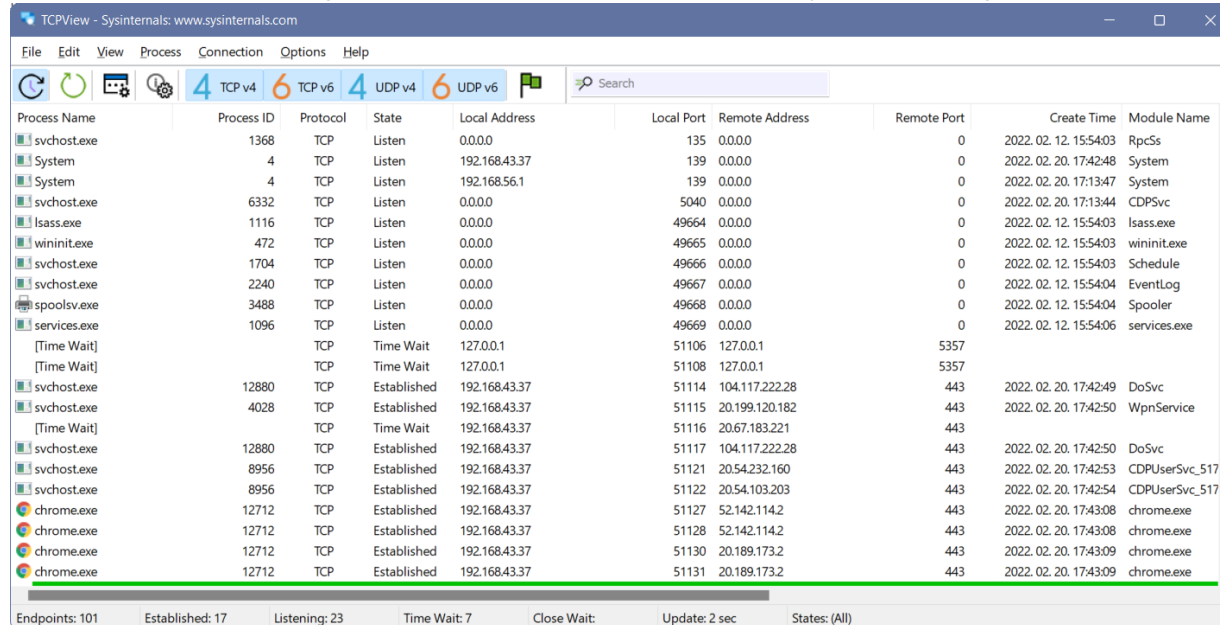


Minden olyan lemezhez létrehoz egy VHD-t, amelyen a kiválasztott kötetek találhatóak. Megőrzi a lemez particionálási adatait, de csak a kiválasztott lemezen lévő kötetek adattartalmait másolja.

- **Networking Utilities (TCPView):**

A TCPView egy Windows program, amely részletes listában mutatja be a rendszer összes TCP- és UDP-végpontját, beleértve a helyi és távoli címeket, valamint a TCP-kapcsolatok állapotát.

A TCPView indítani fogja az összes aktív TCP- és UDP-végpont felsorolását, és feloldja az összes IP-címet a tartománynév-verziójukra:



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	1368	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2022.02.12.15:54:03	RpcSs
System	4	TCP	Listen	192.168.43.37	139	0.0.0.0	0	2022.02.20.17:42:48	System
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	2022.02.20.17:13:47	System
svchost.exe	6332	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2022.02.20.17:13:44	CDPSvc
lsass.exe	1116	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2022.02.12.15:54:03	lsass.exe
wininit.exe	472	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2022.02.12.15:54:03	wininit.exe
svchost.exe	1704	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2022.02.12.15:54:03	Schedule
svchost.exe	2240	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2022.02.12.15:54:04	EventLog
spoolsv.exe	3488	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	2022.02.12.15:54:04	Spooler
services.exe	1096	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	2022.02.12.15:54:06	services.exe
[Time Wait]		TCP	Time Wait	127.0.0.1	51106	127.0.0.1	5357		
[Time Wait]		TCP	Time Wait	127.0.0.1	51108	127.0.0.1	5357		
svchost.exe	12880	TCP	Established	192.168.43.37	51114	104.117.222.28	443	2022.02.20.17:42:49	DoSvc
svchost.exe	4028	TCP	Established	192.168.43.37	51115	20.199.120.182	443	2022.02.20.17:42:50	WpnService
[Time Wait]		TCP	Time Wait	192.168.43.37	51116	20.67.183.221	443		
svchost.exe	12880	TCP	Established	192.168.43.37	51117	104.117.222.28	443	2022.02.20.17:42:50	DoSvc
svchost.exe	8956	TCP	Established	192.168.43.37	51121	20.54.232.160	443	2022.02.20.17:42:53	CDPUserSvc_517
svchost.exe	8956	TCP	Established	192.168.43.37	51122	20.54.103.203	443	2022.02.20.17:42:54	CDPUserSvc_517
chrome.exe	12712	TCP	Established	192.168.43.37	51127	52.142.114.2	443	2022.02.20.17:43:08	chrome.exe
chrome.exe	12712	TCP	Established	192.168.43.37	51128	52.142.114.2	443	2022.02.20.17:43:08	chrome.exe
chrome.exe	12712	TCP	Established	192.168.43.37	51130	20.189.173.2	443	2022.02.20.17:43:09	chrome.exe
chrome.exe	12712	TCP	Established	192.168.43.37	51131	20.189.173.2	443	2022.02.20.17:43:09	chrome.exe

- **Process Utilities (Process Explorer, Process Monitor, AutoRuns):**

A Process Explorer egy hatékony keresési képességgel is rendelkezik, amely gyorsan megmutatja, hogy mely folyamatokhoz vannak megnyitva adott leírók vagy betöltött DLL-ek.

A Folyamatkezelő egyedi képességei hasznosak a DLL-verzióproblémák nyomon követéséhez vagy a szivárgások kezeléséhez, és betekintést nyújtanak a Windows és alkalmazásokba.



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-FIPLIUO\ACER]

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		8 940 K	57 808 K	160		
System Idle Process	99.56	60 K	8 K	0		
System	< 0.01	92 K	17 672 K	4		
Interrupts	0.19	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 076 K	1 236 K	624		
Memory Compression		560 K	84 308 K	2972		
csrss.exe		1 936 K	6 396 K	876		
wininit.exe		1 524 K	7 660 K	472		
services.exe		5 692 K	10 624 K	1096		
svchost.exe		17 764 K	48 916 K	1240	Windows-szolgáltatások gaz...	Microsoft Corporation
dllhost.exe		3 972 K	12 552 K	8044		
Eap3Host.exe		2 892 K	10 080 K	6748		
WmiPrvSE.exe		2 408 K	10 236 K	640		
SearchHost.exe	Susp...	86 952 K	150 016 K	9788		Microsoft Corporation
StartMenuExperienceHo...		27 884 K	76 100 K	14140		
RuntimeBroker.exe		6 160 K	30 328 K	4920	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		3 264 K	21 108 K	6452	Runtime Broker	Microsoft Corporation
dllhost.exe		5 488 K	14 700 K	14120	COM Surrogate	Microsoft Corporation
YourPhone.exe	Susp...	30 468 K	26 232 K	11680		Microsoft Corporation
RuntimeBroker.exe		2 760 K	19 424 K	9592	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	Susp...	31 036 K	87 248 K	12668	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		5 428 K	24 612 K	13780	Runtime Broker	Microsoft Corporation
SystemSettingsBroker.e...		8 228 K	36 336 K	5560	System Settings Broker	Microsoft Corporation
ApplicationFrameHost.e...		15 124 K	38 796 K	13804	Application Frame Host	Microsoft Corporation
Video.UI.exe	Susp...	20 380 K	2 432 K	9924		
RuntimeBroker.exe		1 428 K	7 636 K	11600	Runtime Broker	Microsoft Corporation
Widgets.exe		7 268 K	38 800 K	4316		Microsoft Corporation
msedgewebview2.exe	< 0.01	30 684 K	19 060 K	4664	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		1 908 K	8 056 K	13264	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		73 352 K	14 400 K	9816	Microsoft Edge WebView2	Microsoft Corporation

CPU Usage: 0.38% Commit Charge: 37.63% Processes: 177 Physical Usage: 28.29%

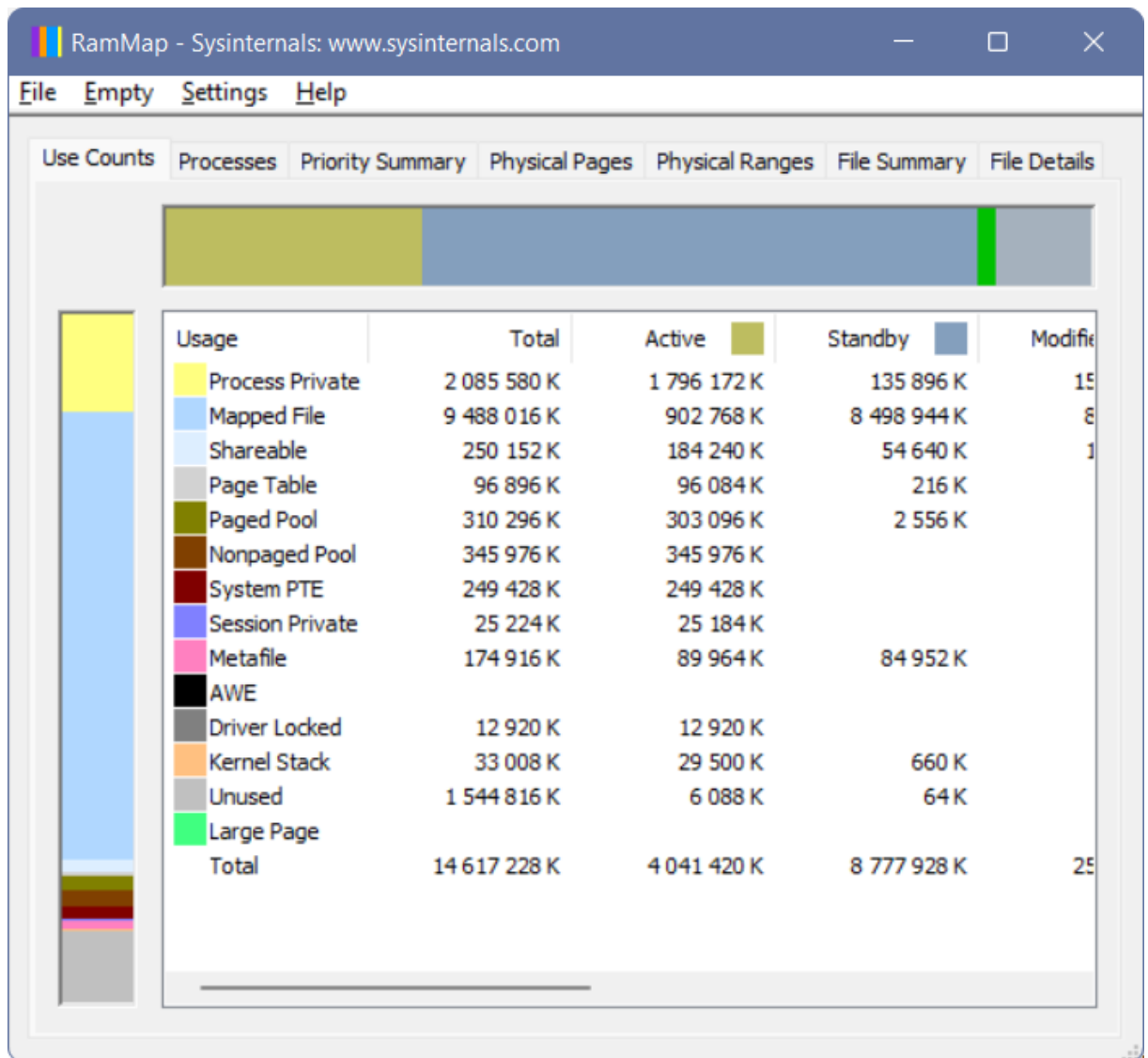
- **Security Utilities (LogonSession):**

Aktív bejelentkezési munkamenetek listázása.

- **Information Utilities (RAMMap):**

A RAMMap egy speciális fizikai memóriahasználat-elemzési segédprogram a Windows Vista és újabb verziókhoz.

A RAMMap használatával megértheti, hogyan kezeli Windows a memóriahasználatot, elemezheti az alkalmazás memóriahasználatát, vagy választ ad a RAM kiosztásával kapcsolatos konkrét kérdésekre.

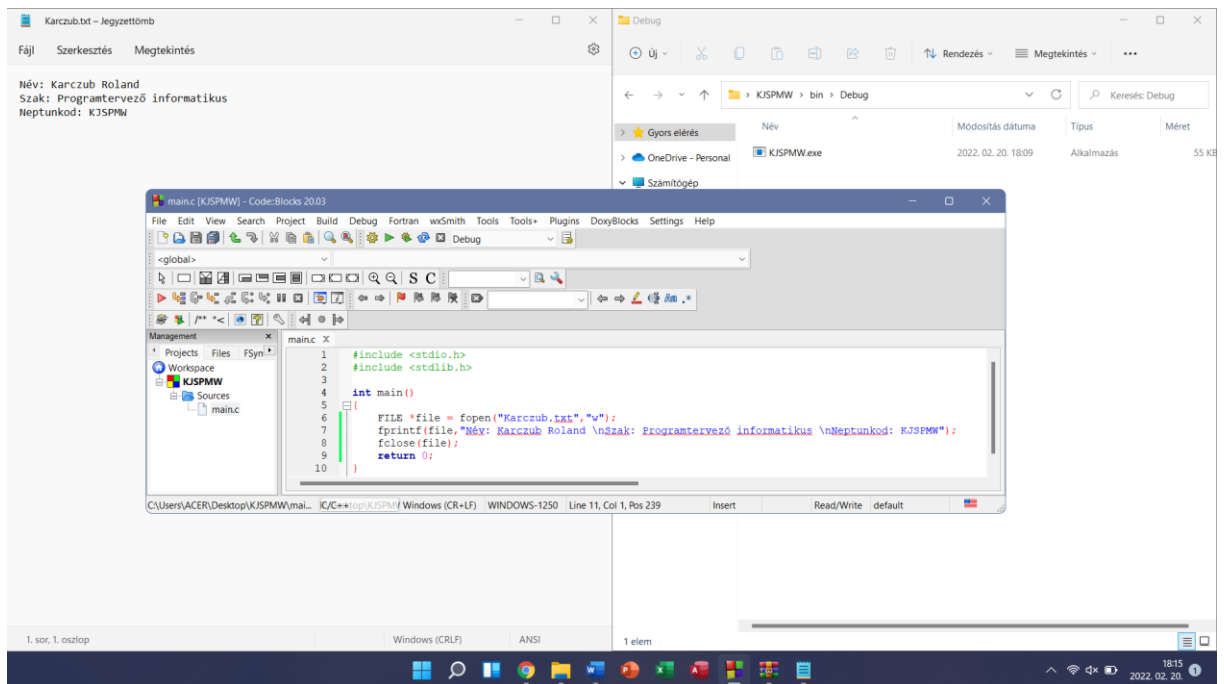


### 3.) Töltse le a következő programot: Dependency Walker:

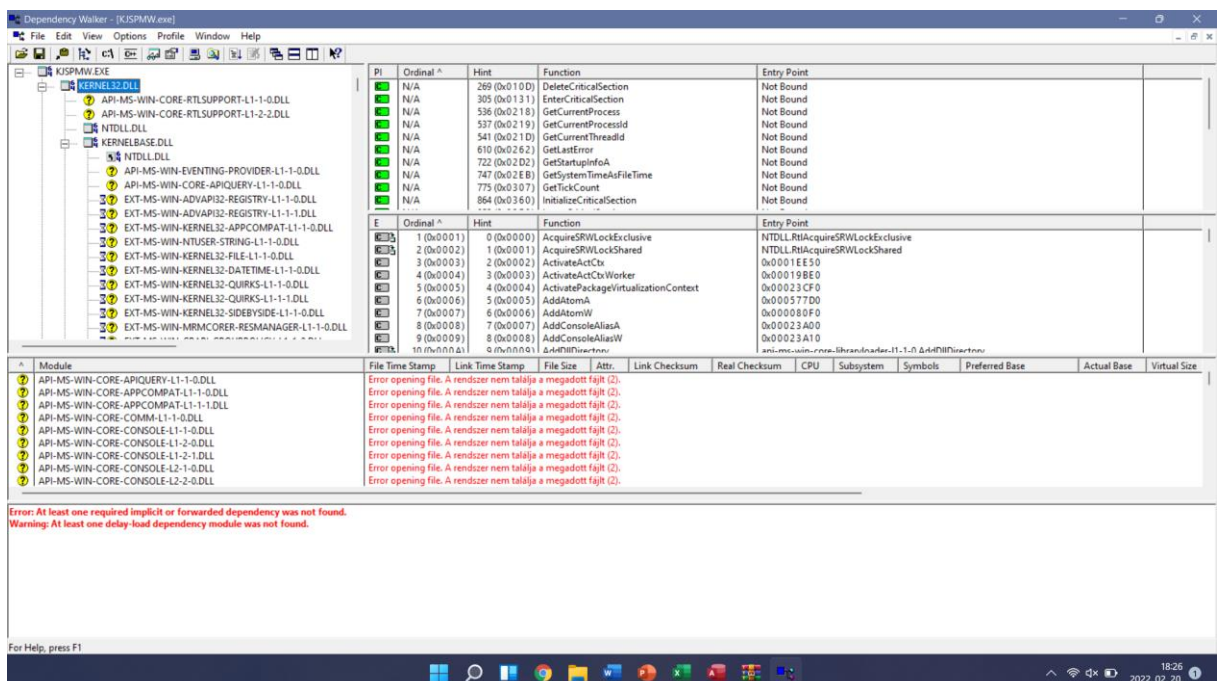
Feladata: a segédprogram megvizsgálja milyen mappákra, és azon belül milyen függvényekre hivatkozik egy elindított program.

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!  
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-L1-2-2.DLL



**Keresse meg NTDLL.DLL-t! Mi ennek a szerepe? Vizsgálja meg az exportált függvényeket, milyen információkat kap az NT API-ról! Dynamic Link Library fájlok, mint ntdll.dll, alapvetően "útmutató könyvek", amelyek információkat és útmutatásokat tartalmaznak a**

Dependency Walker - [NTDLL.DLL]
File Edit View Options Profile Window Help

NTDLL.DLL

PI	Ordinal ^	Hint	Function	Entry Point
E	Ordinal ^	Hint	Function	Entry Point
228 (0x00E4)	219 (0x00DB)		NtAlpcAcceptConnectPort	0x000A4610
229 (0x00E5)	220 (0x00DC)		NtAlpcCancelMessage	0x000A4630
230 (0x00E6)	221 (0x00DD)		NtAlpcConnectPort	0x000A4650
231 (0x00E7)	222 (0x00DE)		NtAlpcConnectPortEx	0x000A4670
232 (0x00E8)	223 (0x00DF)		NtAlpcCreatePort	0x000A4690
233 (0x00E9)	224 (0x00E0)		NtAlpcCreatePortSection	0x000A46B0
234 (0x00EA)	225 (0x00E1)		NtAlpcCreateResourceReserve	0x000A46D0
235 (0x00EB)	226 (0x00E2)		NtAlpcCreateSectionView	0x000A46F0
236 (0x00EC)	227 (0x00E3)		NtAlpcCreateSecurityContext	0x000A4710
237 (0x00ED)	228 (0x00E4)		NtAlpcDeletePortSection	0x000A4730
238 (0x00EE)	229 (0x00E5)		NtAlpcDeleteResourceReserve	0x000A4750
239 (0x00EF)	230 (0x00E6)		NtAlpcDeleteSectionView	0x000A4770
240 (0x00F0)	231 (0x00E7)		NtAlpcDeleteSecurityContext	0x000A4790
241 (0x00F1)	232 (0x00E8)		NtAlpcDisconnectPort	0x000A47B0
242 (0x00F2)	233 (0x00E9)		NtAlpcImpersonateClientContainerOfPort	0x000A47D0
243 (0x00F3)	234 (0x00EA)		NtAlpcImpersonateClientOfPort	0x000A47F0
244 (0x00F4)	235 (0x00EB)		NtAlpcOpenSenderProcess	0x000A4810
245 (0x00F5)	236 (0x00EC)		NtAlpcOpenSenderThread	0x000A4830
246 (0x00F6)	237 (0x00ED)		NtAlpcQueryInformation	0x000A4850
247 (0x00F7)	238 (0x00EE)		NtAlpcQueryInformationMessage	0x000A4870
248 (0x00F8)	239 (0x00EF)		NtAlpcRevokeSecurityContext	0x000A4890
249 (0x00F9)	240 (0x00F0)		NtAlpcSendMailReceivePort	0x000A48B0
250 (0x00FA)	241 (0x00F1)		NtAlpcSetInformation	0x000A48D0
251 (0x00FB)	242 (0x00F2)		NtApphelpCacheControl	0x000A48F0
252 (0x00FC)	243 (0x00F3)		NtAreMappedFilesTheSame	0x000A4910
253 (0x00FD)	244 (0x00F4)		NtAssignProcessToJobObject	0x000A4930
254 (0x00FE)	245 (0x00F5)		NtAssociateWaitCompletionPacket	0x000A4950
255 (0x00FF)	246 (0x00F6)		NtCallNtLdr	0x000A4970

Module	File Time Stamp	Link Time Stamp	File Size	Attr	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size	Load Order	File Ver	Product Ver	Image Ver	Li
NTDLL.DLL	2022/02/11 14:35	2048/03/18 11:55	2 128 360	A	0x00208607	0x00208607	x64	Console	CV,Unknown	0x0000001800000000	Unknown	0x00209000	Not Loaded	10.0.22000.469	10.0.22000.469	10.0	14

For Help, press F1