

Operációs rendszerek BSc

1. Gyak.

2022. 02. 16.

Készítette:

Szelényi Szabolcs Bsc

Mérnökinformatikus hallgató

TYNYS9

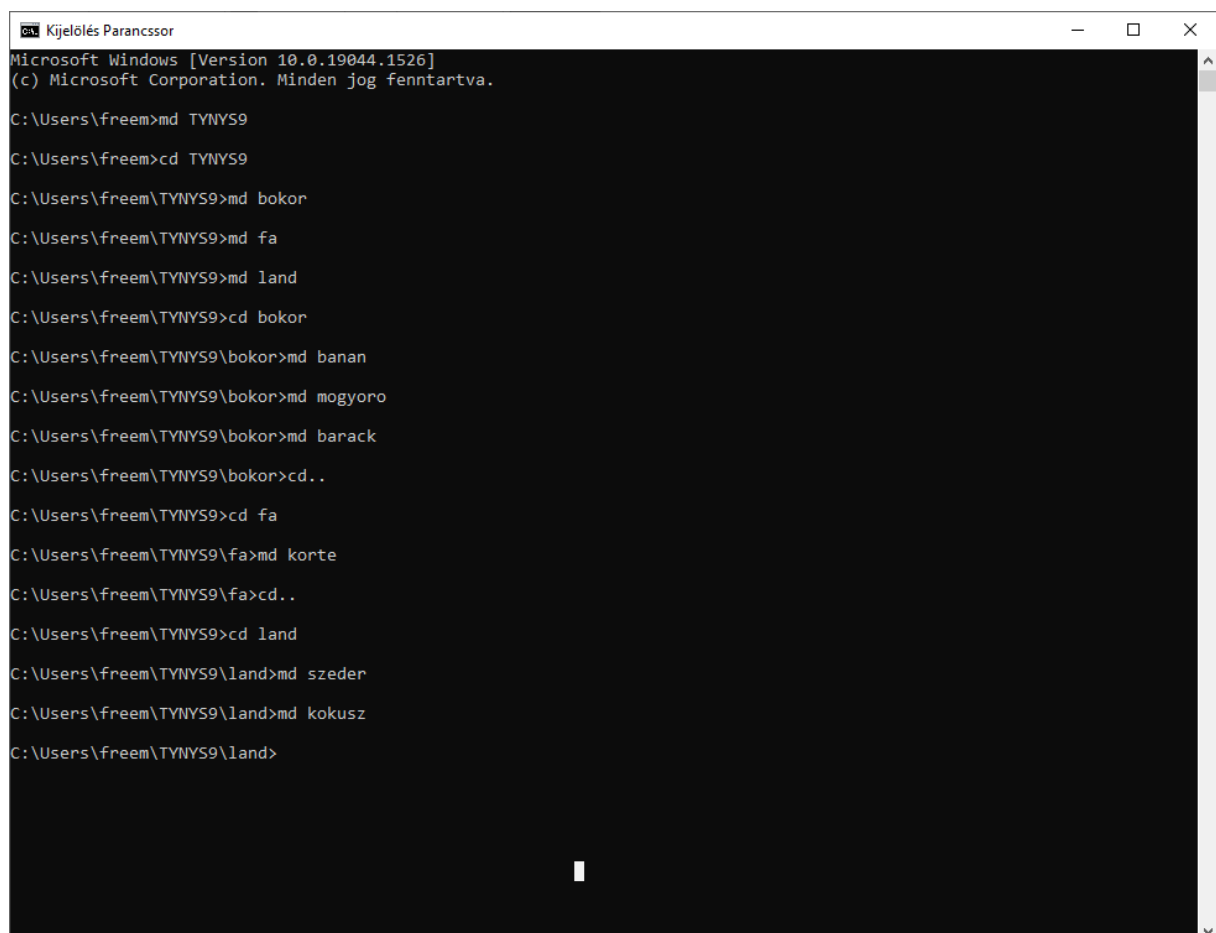
Miskolc, 2022

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
```



```
Kijelölés Parancssor
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. Minden jog fenntartva.

C:\Users\freem>md TYNYS9
C:\Users\freem>cd TYNYS9
C:\Users\freem\TYNYS9>md bokor
C:\Users\freem\TYNYS9>md fa
C:\Users\freem\TYNYS9>md land
C:\Users\freem\TYNYS9>cd bokor
C:\Users\freem\TYNYS9\bokor>md banan
C:\Users\freem\TYNYS9\bokor>md mogyoro
C:\Users\freem\TYNYS9\bokor>md barack
C:\Users\freem\TYNYS9\bokor>cd..
C:\Users\freem\TYNYS9>cd fa
C:\Users\freem\TYNYS9\fa>md korte
C:\Users\freem\TYNYS9\fa>cd..
C:\Users\freem\TYNYS9>cd land
C:\Users\freem\TYNYS9\land>md szeder
C:\Users\freem\TYNYS9\land>md kokusz
C:\Users\freem\TYNYS9\land>
```

b.) Készítsen másolatot:

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

```
Parancssor
C:\Users\freem\TYNYS9>robocopy C:\Users\freem\TYNYS9\land\szeder C:\Users\freem\TYNYS9\fa /e /xf

-----
ROBOCOPY      ::      Robust File Copy for Windows
-----

Started : 2022. február 17., csütörtök 14:35:28
Source  : C:\Users\freem\TYNYS9\land\szeder\
Dest    : C:\Users\freem\TYNYS9\fa\

Files : *.*

Options : *.* /S /E /DCOPY:DA /COPY:DAT /R:1000000 /W:30

-----

*EXTRA Dir      0      C:\Users\freem\TYNYS9\land\szeder\
                -1      C:\Users\freem\TYNYS9\fa\korte\

-----

      Total    Copied    Skipped    Mismatch    FAILED    Extras
Dirs  :        1         0         1         0         0         1
Files :         0         0         0         0         0         0
Bytes :         0         0         0         0         0         0
Times :  0:00:00   0:00:00                0:00:00   0:00:00
Ended : 2022. február 17., csütörtök 14:35:28

C:\Users\freem\TYNYS9>robocopy C:\Users\freem\TYNYS9\bokor\banan C:\Users\freem\TYNYS9\fa /e /xf

-----
ROBOCOPY      ::      Robust File Copy for Windows
-----

Started : 2022. február 17., csütörtök 14:35:51
Source  : C:\Users\freem\TYNYS9\bokor\banan\
Dest    : C:\Users\freem\TYNYS9\fa\

Files : *.*

Options : *.* /S /E /DCOPY:DA /COPY:DAT /R:1000000 /W:30

-----

*EXTRA Dir      0      C:\Users\freem\TYNYS9\bokor\banan\
                -1      C:\Users\freem\TYNYS9\fa\korte\

-----

      Total    Copied    Skipped    Mismatch    FAILED    Extras
Dirs  :        1         0         1         0         0         1
Files :         0         0         0         0         0         0
Bytes :         0         0         0         0         0         0
Times :  0:00:00   0:00:00                0:00:00   0:00:00
Ended : 2022. február 17., csütörtök 14:35:51
```

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

```
Kijelölés Parancssor

C:\Users\freem\TYNYS9>move C:\Users\freem\TYNYS9\bokor\barack C:\Users\freem\TYNYS9\fa
1 dir(s) moved.

C:\Users\freem\TYNYS9>move C:\Users\freem\TYNYS9\land\kokusz C:\Users\freem\TYNYS9\fa
1 dir(s) moved.

C:\Users\freem\TYNYS9>
```

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.

```
Parancssor

C:\Users\freem\TYNYS9>del C:\Users\freem\TYNYS9\land
C:\Users\freem\TYNYS9\land\*, Are you sure (Y/N)? y

C:\Users\freem\TYNYS9>copycon C:\Users\freem\TYNYS9\bokor\banan\leiras.txt
'copycon' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\freem\TYNYS9>copy con C:\Users\freem\TYNYS9\bokor\banan\leiras.txt
sárga
magvas
finom do
^Z
1 file(s) copied.

C:\Users\freem\TYNYS9>copy con C:\Users\freem\TYNYS9\fa\felsorolas.txt
Kazsi
Bazsi
Krisz
Danda
Tetya
^Z
1 file(s) copied.

C:\Users\freem\TYNYS9>
```

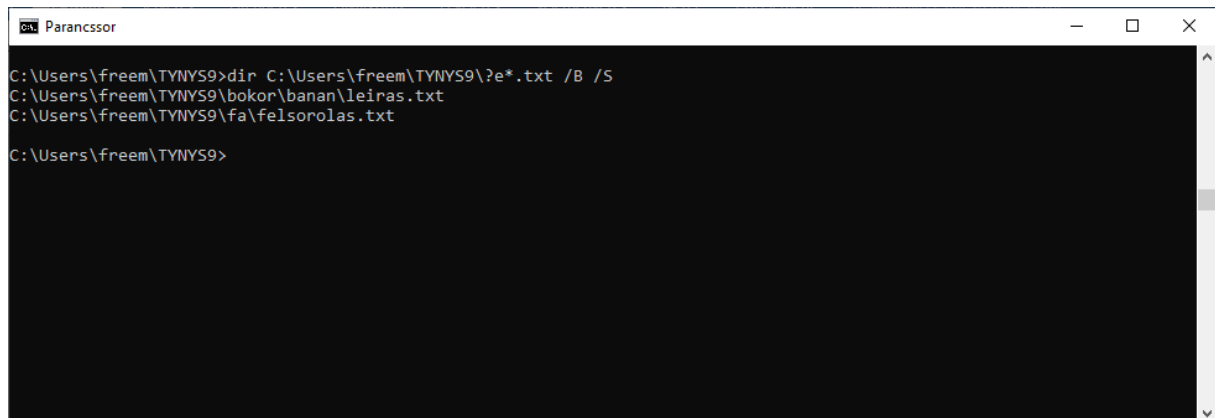
f.) Listázza a neptunkod mappa tartalmát úgy, hogy megjelenjen az almappák tartalma is.

```
Kijelölés Parancssor

C:\Users\freem\TYNYS9>dir /b /s
C:\Users\freem\TYNYS9\bokor
C:\Users\freem\TYNYS9\fa
C:\Users\freem\TYNYS9\land
C:\Users\freem\TYNYS9\bokor\banan
C:\Users\freem\TYNYS9\bokor\mogoró
C:\Users\freem\TYNYS9\bokor\banan\leiras.txt
C:\Users\freem\TYNYS9\fa\barack
C:\Users\freem\TYNYS9\fa\felsorolas.txt
C:\Users\freem\TYNYS9\fa\kokusz
C:\Users\freem\TYNYS9\fa\korte
C:\Users\freem\TYNYS9\land\szeder

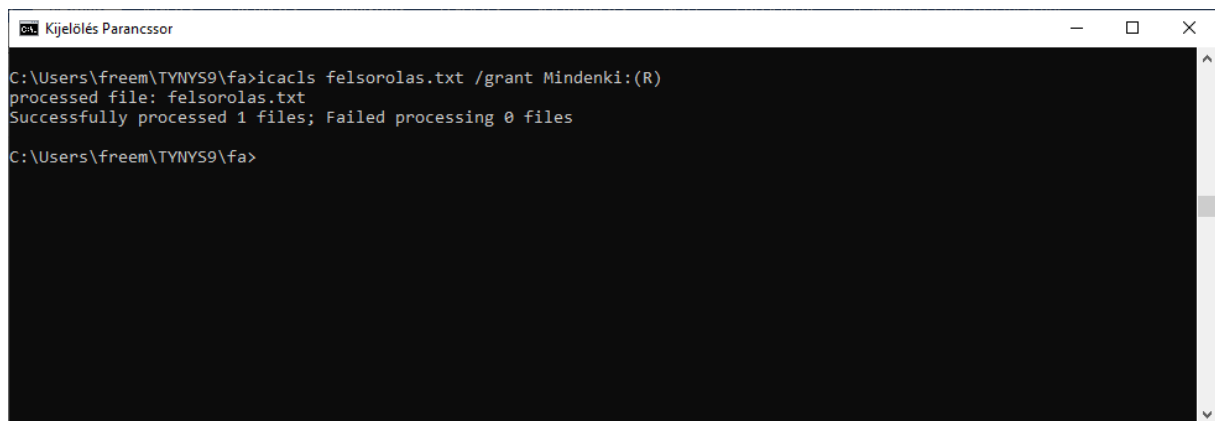
C:\Users\freem\TYNYS9>
```

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



```
Parancssor
C:\Users\freem\TYNYS9>dir C:\Users\freem\TYNYS9\?e*.txt /B /S
C:\Users\freem\TYNYS9\bokor\banan\leiras.txt
C:\Users\freem\TYNYS9\fa\felsorolas.txt
C:\Users\freem\TYNYS9>
```

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



```
Kijelölés Parancssor
C:\Users\freem\TYNYS9\fa>icacls felsorolas.txt /grant Mindenki:(R)
processed file: felsorolas.txt
Successfully processed 1 files; Failed processing 0 files
C:\Users\freem\TYNYS9\fa>
```

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

```
Parancssor
C:\Users\freem>dir /s TYNYS9
Volume in drive C has no label.
Volume Serial Number is 2A2D-7243

Directory of C:\Users\freem\TYNYS9

2022. 02. 17. 14:04 <DIR>      .
2022. 02. 17. 14:04 <DIR>      ..
2022. 02. 17. 14:40 <DIR>      bokor
2022. 02. 17. 14:55 <DIR>      fa
2022. 02. 17. 14:40 <DIR>      land
0 File(s)              0 bytes

Directory of C:\Users\freem\TYNYS9\bokor

2022. 02. 17. 14:40 <DIR>      .
2022. 02. 17. 14:40 <DIR>      ..
2022. 02. 17. 14:53 <DIR>      banan
2022. 02. 17. 14:05 <DIR>      mogyoro
0 File(s)              0 bytes

Directory of C:\Users\freem\TYNYS9\bokor\banan

2022. 02. 17. 14:53 <DIR>      .
2022. 02. 17. 14:53 <DIR>      ..
2022. 02. 17. 14:54      25 leiras.txt
1 File(s)              25 bytes

Directory of C:\Users\freem\TYNYS9\bokor\mogyoro

2022. 02. 17. 14:05 <DIR>      .
2022. 02. 17. 14:05 <DIR>      ..
0 File(s)              0 bytes

Directory of C:\Users\freem\TYNYS9\fa

2022. 02. 17. 14:55 <DIR>      .
2022. 02. 17. 14:55 <DIR>      ..
2022. 02. 17. 14:05 <DIR>      barack
2022. 02. 17. 14:55      35 felsorolas.txt
2022. 02. 17. 14:06 <DIR>      kokusz
2022. 02. 17. 14:05 <DIR>      korte
1 File(s)              35 bytes

Directory of C:\Users\freem\TYNYS9\fa\barack

2022. 02. 17. 14:05 <DIR>      .
2022. 02. 17. 14:05 <DIR>      ..
0 File(s)              0 bytes

Directory of C:\Users\freem\TYNYS9\fa\kokusz

2022. 02. 17. 14:06 <DIR>      .
2022. 02. 17. 14:06 <DIR>      ..
0 File(s)              0 bytes
```

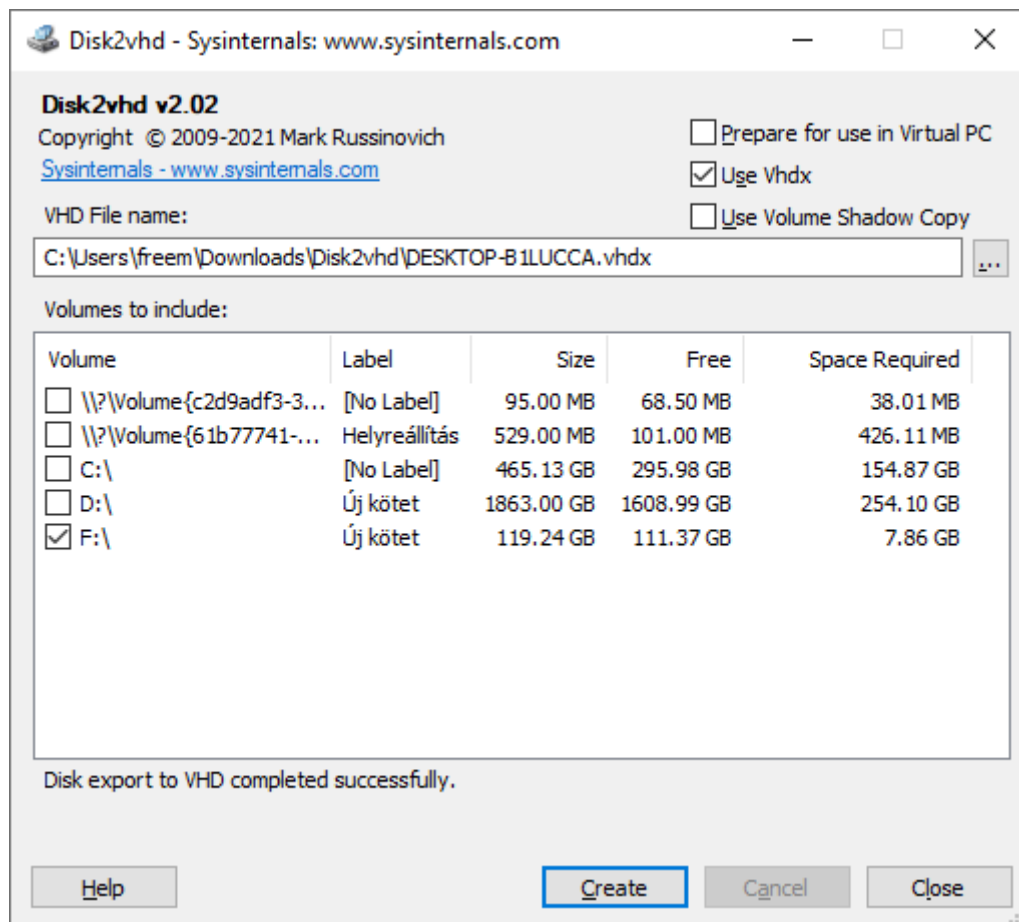
j.) Rendezze ABC-szerint a felsorolas.txt file tartalmát.

```
Parancssor
C:\Users\freem\TYNYS9\fa>sort felsorolas.txt
Bazsi
Danda
Kazsi
Krisz
Tetya

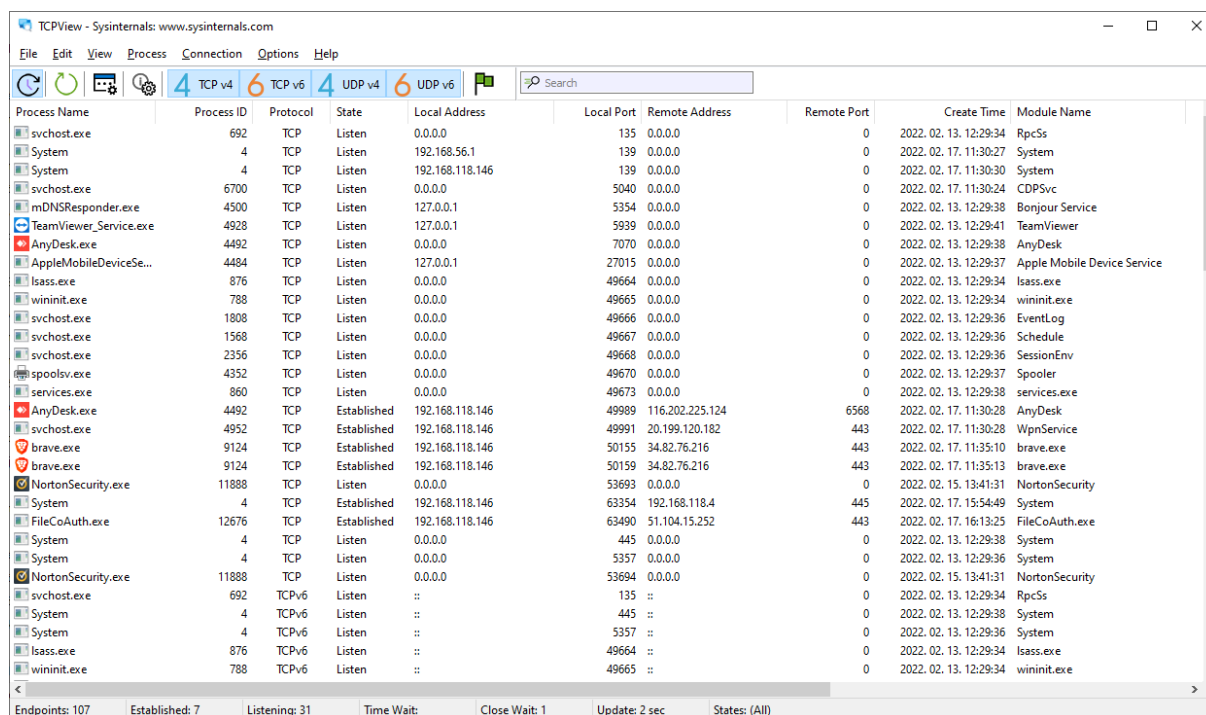
C:\Users\freem\TYNYS9\fa>
```

2. A Sysinternals weboldalán kategóriákba sorolva hasznos programok érhetőek el:

a) File and Disk Utilities (Disk2vhd)



b) Networking Utilities (TCPView)



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

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-B1LUCCA\freem]

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		12 732 K	128 816 K	108		
System Idle Process	66.06	60 K	8 K	0		
System	0.38	212 K	2 660 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 056 K	628 K	456		
Memory Compression		244 K	19 836 K	3068		
csrss.exe		2 100 K	3 764 K	668		
wininit.exe		1 564 K	4 444 K	788		
services.exe	1.13	7 440 K	10 924 K	860		
svchost.exe		17 148 K	26 180 K	996	Windows-szolgáltatások gaz...	Microsoft Corporation
MoUsCoreWorker.exe		16 148 K	27 756 K	9648		
WmiPrvSE.exe		3 372 K	8 456 K	5936		
WmiPrvSE.exe		2 396 K	5 996 K	8104		
unsecapp.exe		1 720 K	9 616 K	13388		
SettingSyncHost.exe		3 536 K	6 468 K	4052	Host Process for Setting Syn...	Microsoft Corporation
StartMenuExperience...		29 560 K	76 896 K	6376		
RuntimeBroker.exe		6 792 K	27 956 K	8112	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	140 088 K	203 948 K	9676	Search application	Microsoft Corporation
RuntimeBroker.exe		13 428 K	46 212 K	5584	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	32 172 K	19 092 K	10980		Microsoft Corporation
LockApp.exe	Susp...	15 484 K	51 068 K	8776	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		8 600 K	33 476 K	12452	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		7 256 K	28 632 K	1328	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		3 116 K	21 248 K	5896	Runtime Broker	Microsoft Corporation
TextInputHost.exe		16 240 K	46 980 K	964		Microsoft Corporation
SystemSettings.exe	Susp...	25 328 K	3 512 K	5560	Gépház	Microsoft Corporation
ApplicationFrameHost...		12 060 K	32 132 K	14260	Application Frame Host	Microsoft Corporation
UserOOBEBroker.exe		1 904 K	10 032 K	9832	User OOBEBroker	Microsoft Corporation
Video.UI.exe	Susp...	20 184 K	3 096 K	1384		

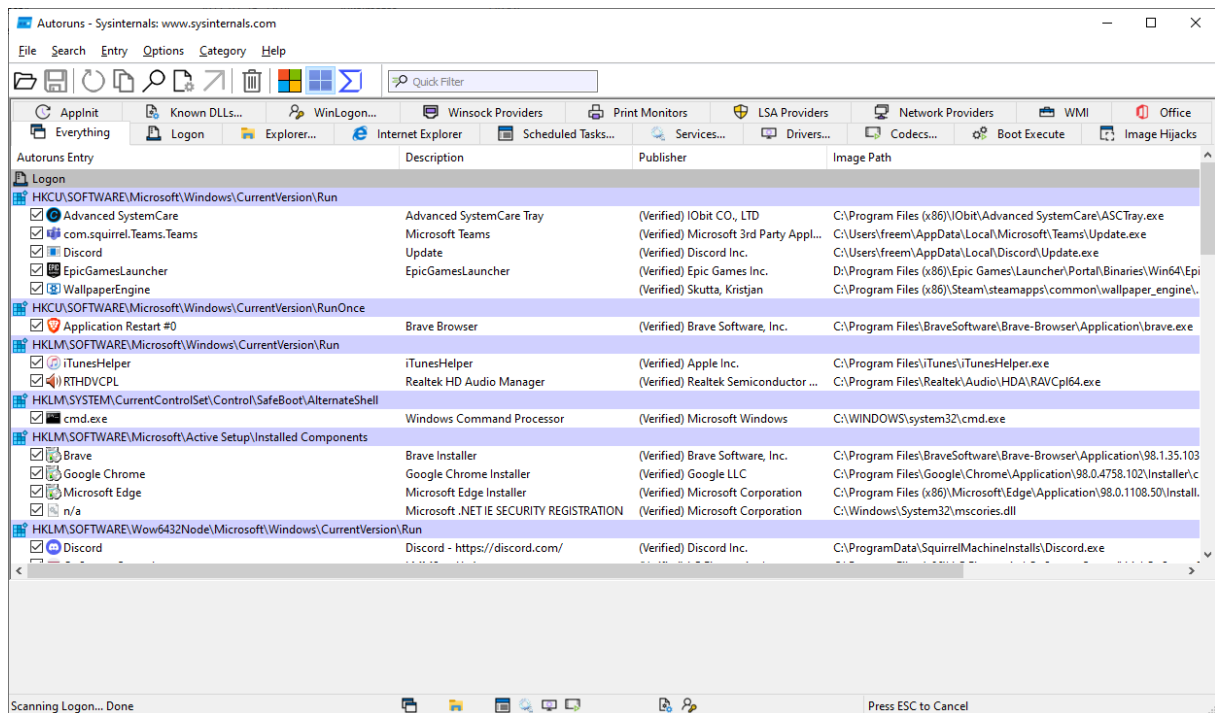
CPU Usage: 33.03% Commit Charge: 27.86% Processes: 202 Physical Usage: 23.14%

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

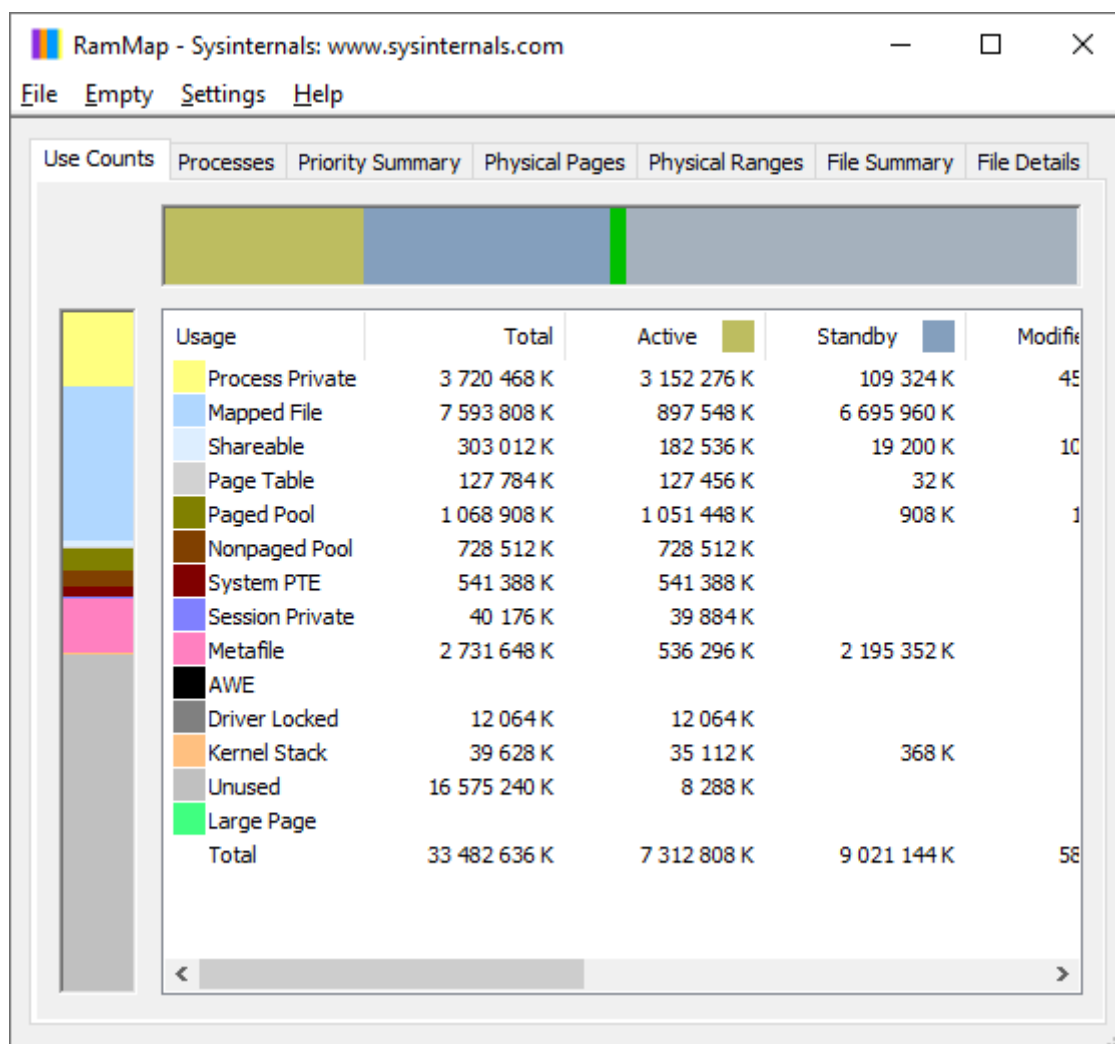
Time ...	Process Name	PID	Operation	Path	Result	Detail
16:16:...	svchost.exe	3712	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 690 688, Le...
16:16:...	svchost.exe	3712	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 678 400, Le...
16:16:...	svchost.exe	3712	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 635 904, Le...
16:16:...	lsass.exe	876	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 607 168, ...
16:16:...	lsass.exe	876	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 590 784, ...
16:16:...	svchost.exe	3712	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 627 712, Le...
16:16:...	lsass.exe	876	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 505 280, ...
16:16:...	svchost.exe	3712	Lock File	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
16:16:...	lsass.exe	876	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 578 496, ...
16:16:...	lsass.exe	876	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 488 896, ...
16:16:...	lsass.exe	876	QueryNameInfo...	C:\Users\freem\Downloads\ProcessMo...	SUCCESS	Name: \Users\free...
16:16:...	lsass.exe	876	QueryNameInfo...	C:\Users\freem\Downloads\ProcessMo...	SUCCESS	Name: \Users\free...
16:16:...	Explorer.EXE	9700	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query: Name
16:16:...	Explorer.EXE	9700	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
16:16:...	Explorer.EXE	9700	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
16:16:...	Explorer.EXE	9700	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
16:16:...	Explorer.EXE	9700	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
16:16:...	Explorer.EXE	9700	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query: Name
16:16:...	Explorer.EXE	9700	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
16:16:...	Explorer.EXE	9700	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query: Name
16:16:...	Explorer.EXE	9700	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
16:16:...	Explorer.EXE	9700	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
16:16:...	ctfmon.exe	10816	RegQueryValue	HKLM	SUCCESS	Query: HandleTag...
16:16:...	ctfmon.exe	10816	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
16:16:...	ctfmon.exe	10816	RegQueryValue	HKCU	SUCCESS	Query: HandleTag...
16:16:...	Explorer.EXE	9700	CreateFile	C:\Users\freem\Downloads\ProcessMo...	SUCCESS	Desired Access: R...
16:16:...	ctfmon.exe	10816	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
16:16:...	ctfmon.exe	10816	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
16:16:...	Explorer.EXE	9700	QueryBasicInfo...	C:\Users\freem\Downloads\ProcessMo...	SUCCESS	CreationTime: 202...
16:16:...	ctfmon.exe	10816	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
16:16:...	Explorer.EXE	9700	CloseFile	C:\Users\freem\Downloads\ProcessMo...	SUCCESS	
16:16:...	ctfmon.exe	10816	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Type: REG_DWORD...
16:16:...	ctfmon.exe	10816	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
16:16:...	ctfmon.exe	10816	RegQueryValue	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
16:16:...	ctfmon.exe	10816	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Desired Access: Q...
16:16:...	ctfmon.exe	10816	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
16:16:...	ctfmon.exe	10816	RegCloseKey	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
16:16:...	ctfmon.exe	10816	RegQueryValue	HKLM	SUCCESS	Query: HandleTag...
16:16:...	ctfmon.exe	10816	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...

Showing 38 078 of 139 144 events (27%) Backed by virtual memory

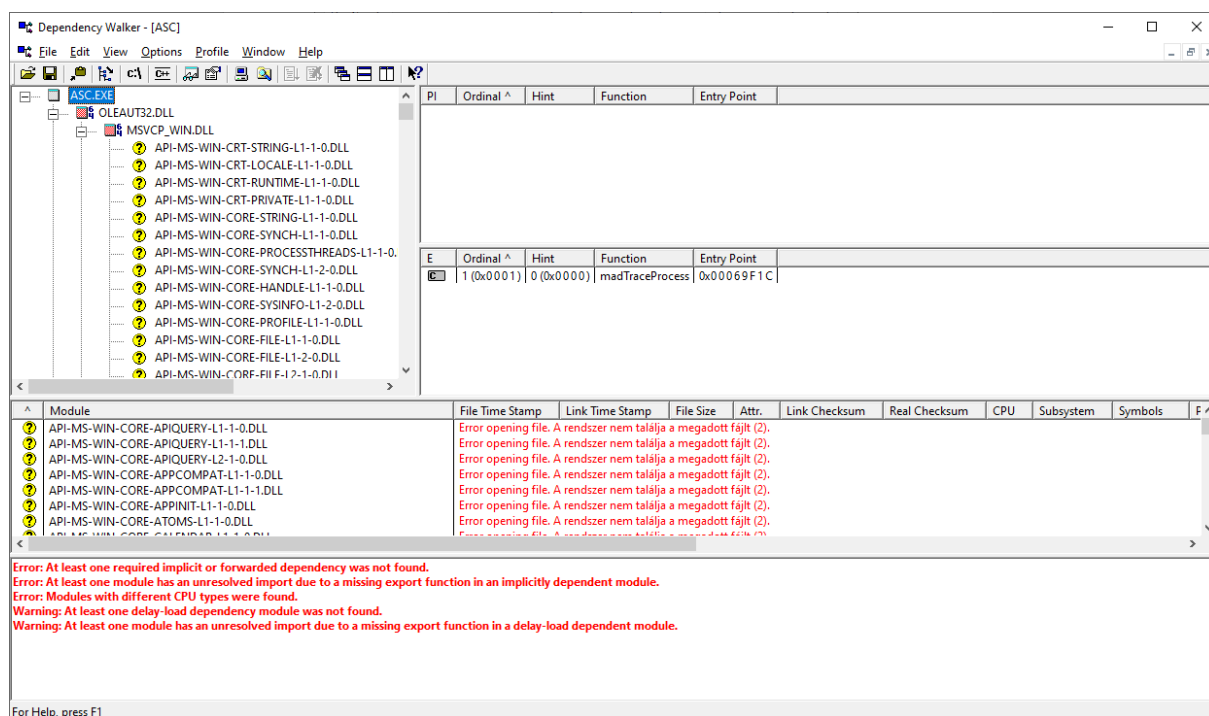


d) Security Utilities (LogonSession)

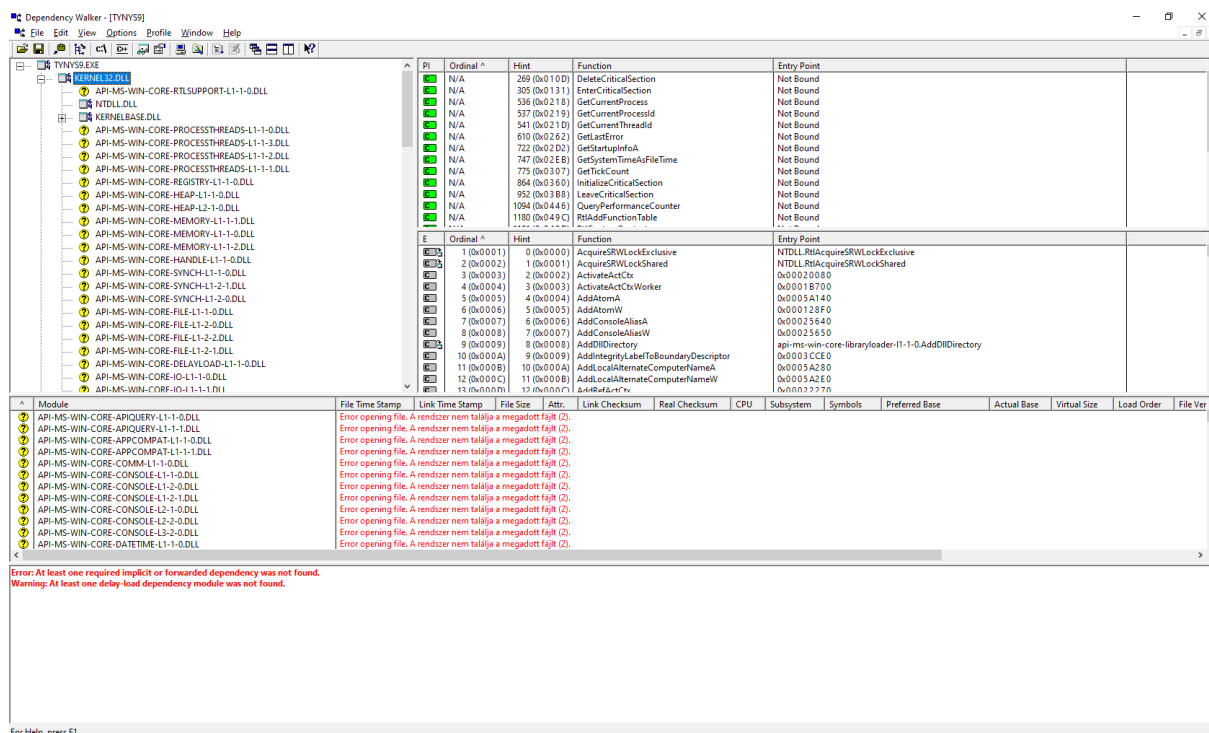
e) Information Utilities (RAMMap)



3. Töltse le a következő programot: Dependency Walker



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



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

Az ntdll.dll a rendszerkönyvtár, amely felelős az operációs rendszer mozgatásáért, másolásáért, összehasonlításáért és más hasonló műveleteiért.

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
111 (0x006F)	102 (0x0066)		LdrAddLoadAsDataTable	0x00073000
112 (0x0070)	103 (0x0067)		LdrAddRefDll	0x00010140
113 (0x0071)	104 (0x0068)		LdrAppxHandleIntegrityFailure	0x000CB430
114 (0x0072)	105 (0x0069)		LdrCallEnclave	0x000CCA10
115 (0x0073)	106 (0x006A)		LdrControlFlowGuardEnforced	0x00033520
116 (0x0074)	107 (0x006B)		LdrCreateEnclave	0x000CCA20
117 (0x0075)	108 (0x006C)		LdrDeleteEnclave	0x000CCB30
118 (0x0076)	109 (0x006D)		LdrDisableThreadCalloutsForDll	0x0000EF70

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size	Load Orde
NTDLL.DLL	2022/01/14 12:57	2090/09/01 14:26	2 026 296	A	0x001FBCE0	0x001FBCE0	x64	Console	CV,Unknown	0x0000000180000000	Unknown	0x001F5000	Not Loade

For Help, press F1