

Operációs rendszerek Bsc

2. Gyak.

2022. 02. 15.

Készítette:

Keresztes Iulia Bsc

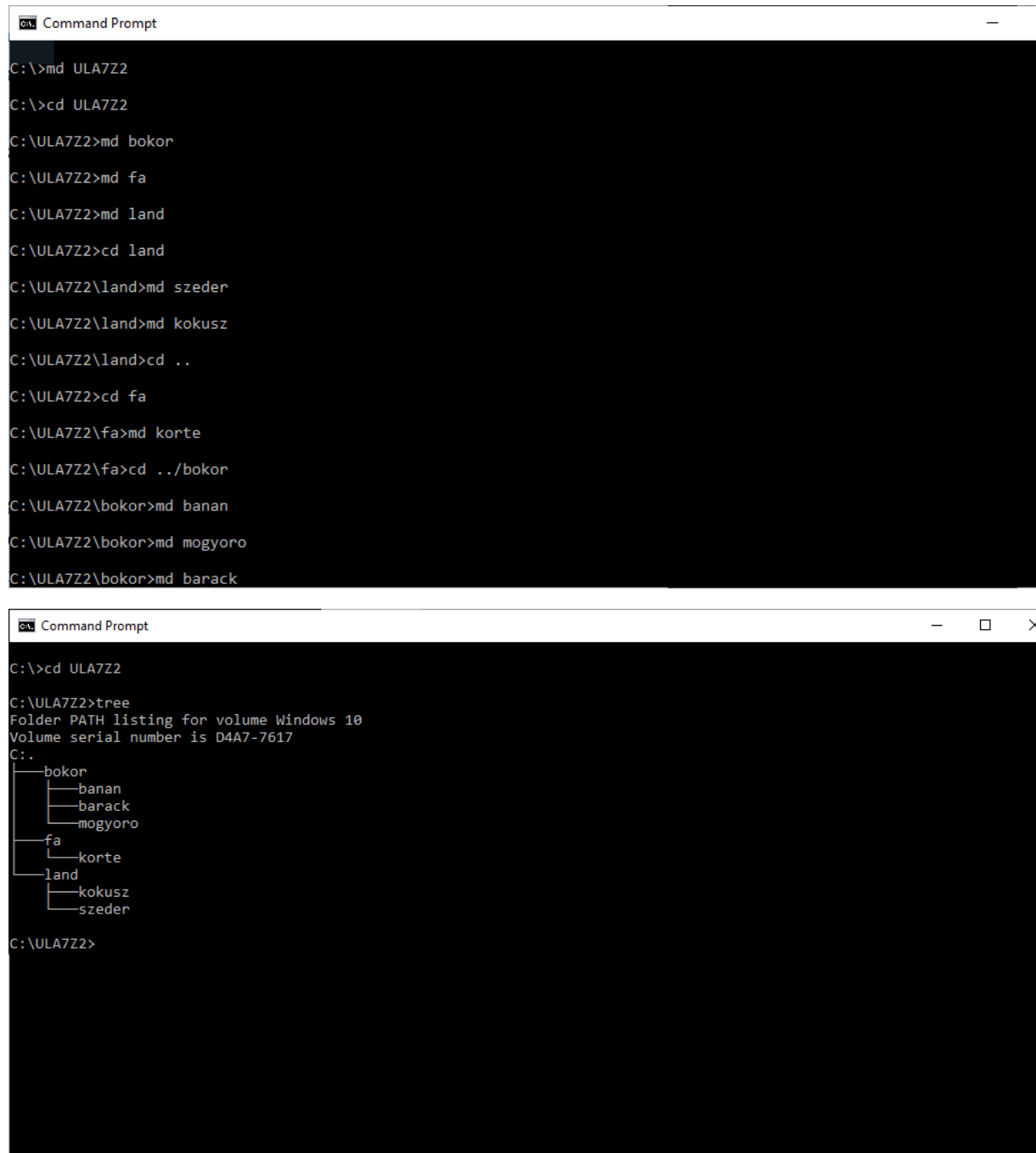
Programtervező informatikus szak

ULA7Z2

Miskolc, 2022

1. feladat:

a) Hozza létre a következő mappa szerkezetet!



```
Command Prompt
C:\>md ULA7Z2
C:\>cd ULA7Z2
C:\ULA7Z2>md bokor
C:\ULA7Z2>md fa
C:\ULA7Z2>md land
C:\ULA7Z2>cd land
C:\ULA7Z2\land>md szeder
C:\ULA7Z2\land>md kokusz
C:\ULA7Z2\land>cd ..
C:\ULA7Z2>cd fa
C:\ULA7Z2\fa>md korte
C:\ULA7Z2\fa>cd ../bokor
C:\ULA7Z2\bokor>md banan
C:\ULA7Z2\bokor>md mogyoro
C:\ULA7Z2\bokor>md barack

Command Prompt
C:\>cd ULA7Z2
C:\ULA7Z2>tree
Folder PATH listing for volume Windows 10
Volume serial number is D4A7-7617
C:.
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   └── korte
└── land
    ├── kokusz
    └── szeder
C:\ULA7Z2>
```

b) Készítsen másolatot:

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

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

```

Command Prompt

C:\ULA7Z2>xcopy land fa /s /t

C:\ULA7Z2>xcopy bokor fa /s /t

```

Hogy ez működhessen, a land/szeder és bokor/banan jegyzékekbe szükséges volt beletenni egy fájlt.

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

```

Command Prompt

C:\ULA7Z2>move bokor/barack fa
1 dir(s) moved.

C:\ULA7Z2>move land/kokusz fa
1 dir(s) moved.

```

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

C:\ULA7Z2>rd land /s
land, Are you sure (Y/N)? y

C:\ULA7Z2>copy NUL bokor/banan/leiras.txt
1 file(s) copied.

C:\ULA7Z2>copy NUL fa/felsorolas.txt
The syntax of the command is incorrect.

C:\ULA7Z2>copy NUL fa\felsorolas.txt
1 file(s) copied.

```

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

```
Command Prompt
C:\ULA7Z2>cd bokor\banan
C:\ULA7Z2\bokor\banan>echo A barack egy gyumolcs, ami fan no. > leiras.txt
C:\ULA7Z2\bokor\banan>echo A fa latin megnevezese Prunus persica. >> leiras.txt
C:\ULA7Z2\bokor\banan>echo Olyan gyumolcsfa, amely a Rosaceae csaladba tartozik, tehat rozsafele. >> leiras.txt
```

```
Command Prompt
C:\>cd ULA7Z2/fa
C:\ULA7Z2\fa>echo szilva > felsorolas.txt
C:\ULA7Z2\fa>echo meggy >> felsorolas.txt
C:\ULA7Z2\fa>echo alma >> felsorolas.txt
C:\ULA7Z2\fa>echo korte >> felsorolas.txt
C:\ULA7Z2\fa>echo mandula >> felsorolas.txt
C:\ULA7Z2\fa>
```

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

```
Command Prompt
C:\ULA7Z2>dir /s
Volume in drive C has no label.
Volume Serial Number is CEE1-0D68

Directory of C:\ULA7Z2
02/19/2022 10:35 <DIR> .
02/19/2022 10:35 <DIR> ..
02/19/2022 10:31 <DIR> bokor
02/19/2022 10:47 <DIR> fa
0 File(s) 0 bytes

Directory of C:\ULA7Z2\bokor
02/19/2022 10:31 <DIR> .
02/19/2022 10:31 <DIR> ..
02/19/2022 11:11 <DIR> banan
02/19/2022 10:09 <DIR> mogyoro
0 File(s) 0 bytes

Directory of C:\ULA7Z2\bokor\banan
02/19/2022 11:11 <DIR> .
02/19/2022 11:11 <DIR> ..
02/19/2022 10:59 151 leiras.txt
1 File(s) 151 bytes

Directory of C:\ULA7Z2\bokor\mogyoro
02/19/2022 10:09 <DIR> .
02/19/2022 10:09 <DIR> ..
0 File(s) 0 bytes

Directory of C:\ULA7Z2\fa
02/19/2022 10:47 <DIR> .
02/19/2022 10:47 <DIR> ..
02/19/2022 10:21 <DIR> banan
02/19/2022 10:09 <DIR> barack
02/19/2022 11:07 141 felsorolas.txt
02/19/2022 10:09 <DIR> kokusz
02/19/2022 10:09 <DIR> korte
02/19/2022 10:19 <DIR> szeder
1 File(s) 141 bytes

Directory of C:\ULA7Z2\fa\banan
02/19/2022 10:21 <DIR> .
02/19/2022 10:21 <DIR> ..
```

```
Command Prompt
Directory of C:\ULA7Z2\fa\banan
02/19/2022 10:21 <DIR> .
02/19/2022 10:21 <DIR> ..
0 File(s) 0 bytes

Directory of C:\ULA7Z2\fa\barack
02/19/2022 10:09 <DIR> .
02/19/2022 10:09 <DIR> ..
0 File(s) 0 bytes

Directory of C:\ULA7Z2\fa\kokusz
02/19/2022 10:09 <DIR> .
02/19/2022 10:09 <DIR> ..
0 File(s) 0 bytes

Directory of C:\ULA7Z2\fa\korte
02/19/2022 10:09 <DIR> .
02/19/2022 10:09 <DIR> ..
0 File(s) 0 bytes

Directory of C:\ULA7Z2\fa\szeder
02/19/2022 10:19 <DIR> .
02/19/2022 10:19 <DIR> ..
0 File(s) 0 bytes

Total Files Listed:
2 File(s) 292 bytes
29 Dir(s) 55,171,485,696 bytes free

C:\ULA7Z2>
```

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

```
Command Prompt
C:\>dir /s ?e*
```

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

```
Command Prompt
C:\ULA7Z2\fa>icacls felsorolas.txt /grant Everyone:R
processed file: felsorolas.txt
Successfully processed 1 files; Failed processing 0 files
```

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

```
Command Prompt
Directory of C:\ULA7Z2\fa\kokusz
02/19/2022 10:09 <DIR> .
02/19/2022 10:09 <DIR> ..
0 File(s) 0 bytes

Directory of C:\ULA7Z2\fa\korte
02/19/2022 10:09 <DIR> .
02/19/2022 10:09 <DIR> ..
0 File(s) 0 bytes

Directory of C:\ULA7Z2\fa\szeder
02/19/2022 10:19 <DIR> .
02/19/2022 10:19 <DIR> ..
0 File(s) 0 bytes

Total Files Listed:
2 File(s) 292 bytes
29 Dir(s) 54,504,062,976 bytes free
```

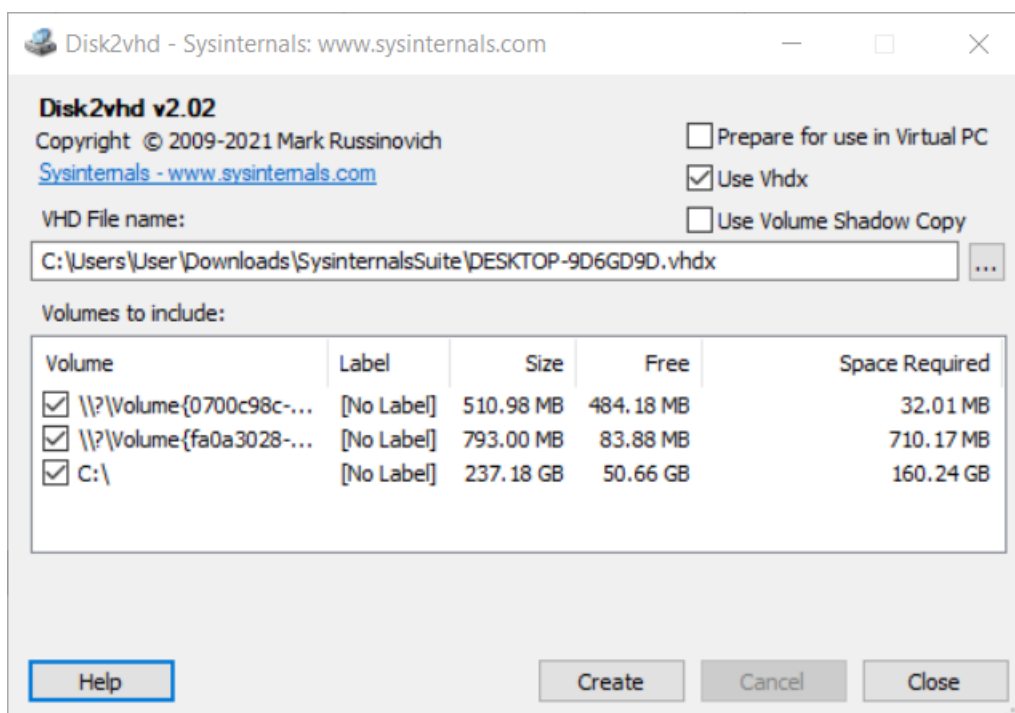
j) Rendezze ABC-szerint a felsorolas.txt file tartalmát.

```
Command Prompt
C:\ULA7Z2\fa>sort felsorolas.txt
alma
korte
mandula
meggy
szilva
```

2. feladat: Tölts le a Sysinternals Suite csomagot, majd csomagolja ki.

A felsorolt eszközök közül minden eszköz esetén tölts le, futtassa - és írja le a program szolgáltatásait és a futtatás eredményét

a) File and Disk Utilities (Disk2vhd)



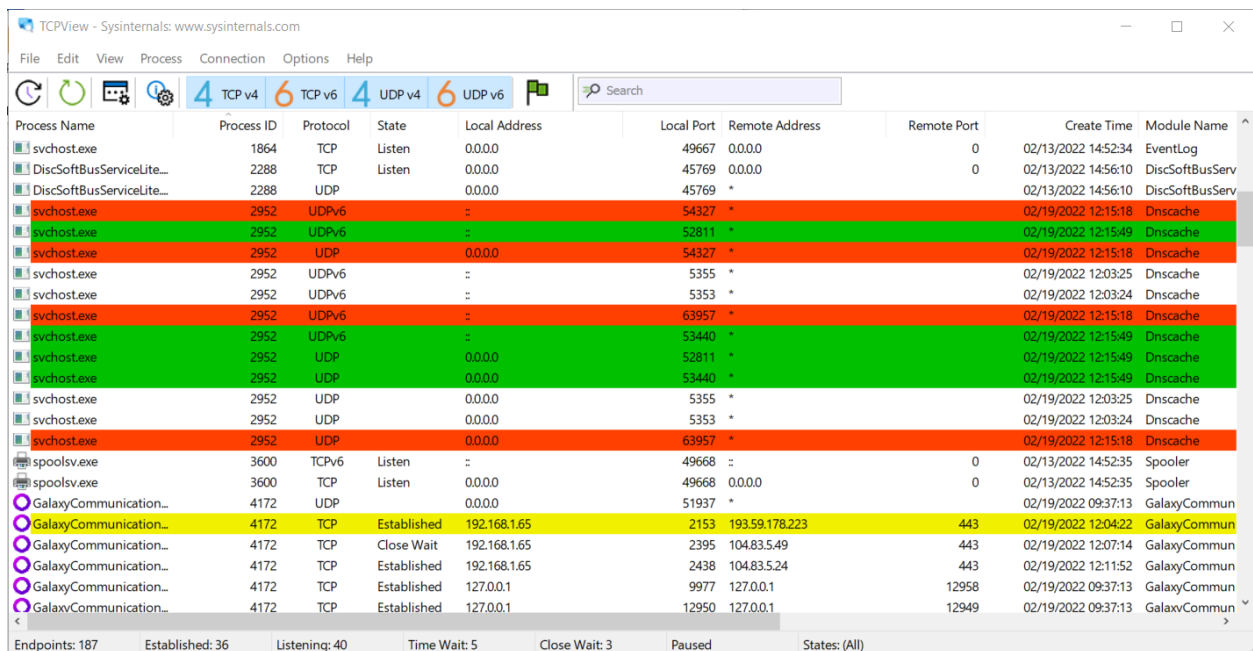
Szolgáltatás: Fizikai lemezekről virtuális másolatot készít. Futtatáskor a „VHD File name” részen megadott útvonalra, a megadott néven készíti el a vhdx kiterjesztésű virtuális lemezt.

Ha a „Use vhdx” négyzet nincs kipipálva, a lemez vhd kiterjesztéssel jön létre.

A „Prepare for use in Virtual PC” opció kompatibilitást biztosít a Microsoft Virtual PC alkalmazásával.

A „Use Volume Shadow Copy” opció kiválasztásával a Disk2vhd a virtuális lemezt a lemez aktuális állapotával hozza létre, tehát ha a másolat készítése alatt valami változik a Windowson (például új programot telepít a felhasználó), ez a változás nem lesz része a virtuális lemeznek.

b) Networking Utilities (TCPView)



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	1864	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	02/13/2022 14:52:34	EventLog
DiscSoftBusServiceLite...	2288	TCP	Listen	0.0.0.0	45769	0.0.0.0	0	02/13/2022 14:56:10	DiscSoftBusServ
DiscSoftBusServiceLite...	2288	UDP		0.0.0.0	45769	*		02/13/2022 14:56:10	DiscSoftBusServ
svchost.exe	2952	UDPv6		::	54327	*		02/19/2022 12:15:18	Dnscache
svchost.exe	2952	UDPv6		::	52811	*		02/19/2022 12:15:49	Dnscache
svchost.exe	2952	UDP		0.0.0.0	54327	*		02/19/2022 12:15:18	Dnscache
svchost.exe	2952	UDPv6		::	5355	*		02/19/2022 12:03:25	Dnscache
svchost.exe	2952	UDPv6		::	5353	*		02/19/2022 12:03:24	Dnscache
svchost.exe	2952	UDPv6		::	63957	*		02/19/2022 12:15:18	Dnscache
svchost.exe	2952	UDPv6		::	53440	*		02/19/2022 12:15:49	Dnscache
svchost.exe	2952	UDP		0.0.0.0	52811	*		02/19/2022 12:15:49	Dnscache
svchost.exe	2952	UDP		0.0.0.0	53440	*		02/19/2022 12:15:49	Dnscache
svchost.exe	2952	UDP		0.0.0.0	5355	*		02/19/2022 12:03:25	Dnscache
svchost.exe	2952	UDP		0.0.0.0	5353	*		02/19/2022 12:03:24	Dnscache
svchost.exe	2952	UDP		0.0.0.0	63957	*		02/19/2022 12:15:18	Dnscache
spoolsv.exe	3600	TCPv6	Listen	::	49668	::	0	02/13/2022 14:52:35	Spooler
spoolsv.exe	3600	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	02/13/2022 14:52:35	Spooler
GalaxyCommunication...	4172	UDP		0.0.0.0	51937	*		02/19/2022 09:37:13	GalaxyCommun
GalaxyCommunication...	4172	TCP	Established	192.168.1.65	2153	193.59.178.223	443	02/19/2022 12:04:22	GalaxyCommun
GalaxyCommunication...	4172	TCP	Close Wait	192.168.1.65	2395	104.83.5.49	443	02/19/2022 12:07:14	GalaxyCommun
GalaxyCommunication...	4172	TCP	Established	192.168.1.65	2438	104.83.5.24	443	02/19/2022 12:11:52	GalaxyCommun
GalaxyCommunication...	4172	TCP	Established	127.0.0.1	9977	127.0.0.1	12958	02/19/2022 09:37:13	GalaxyCommun
GalaxyCommunication...	4172	TCP	Established	127.0.0.1	12950	127.0.0.1	12949	02/19/2022 09:37:13	GalaxyCommun

Endpoints: 187 Established: 36 Listening: 40 Time Wait: 5 Close Wait: 3 Paused States: (All)

Szolgáltatás: A TCPView kilistázza az aktuális processzekhez tartozó TCP és UDP portokat, további részletekkel, mint például IP-cím, létrejövés dátuma és a processz azonosítója. Másodpercenként frissül a lista, és színek jelzik a változások jellegét: a sárga sorok a megváltozott állapotú portokra vonatoznak, a pirosak a kitöröltekre, a zöldek pedig az éppen létrejöttekre.

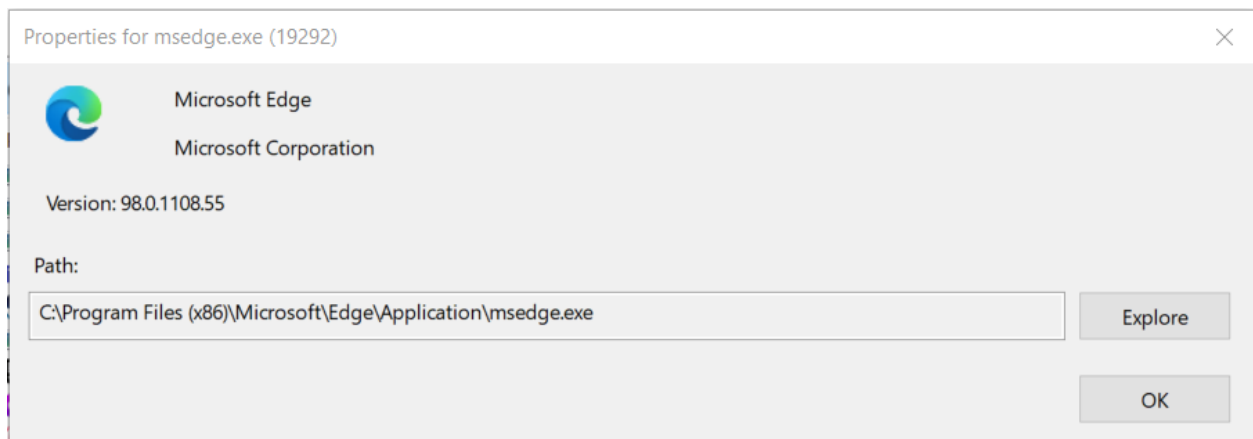
Az ikonsorban további funkciók érhetők el. A TCP v4, v6, UDP v4, v6 gombokra kattintva kijelölhető, hogy milyen protokollokat használó processzekről jelenjenek meg adatok.

Az első ikon arra szolgál, hogy a felhasználó leállítsa vagy folytassa az automatikus frissítéseket, bár ez a Space billentyűvel is változatható.

A második ikon frissítésre szolgál az automatikus frissítések aktiválása nélkül.

A harmadik ikonnal beállítható, hogy címekeként IP-címek vagy pedig Domain nevek jelenjenek meg.

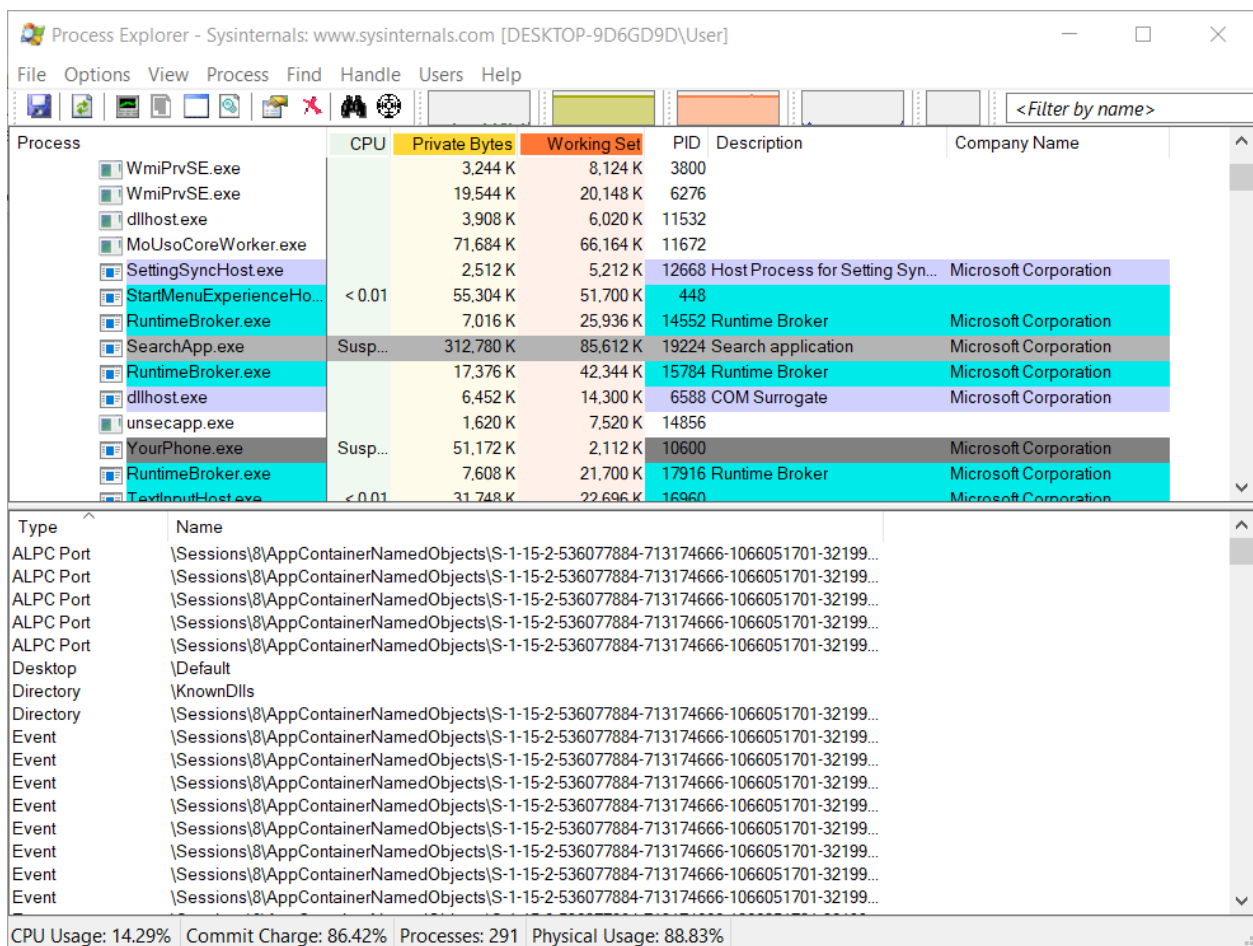
A negyedik ikon akkor nyomható meg, ha kiválasztunk egy processzt a listából. Ekkor a következő ablak jelenik meg:



Itt további információkat tudhatunk meg az adott processzről, például a verziószámát.

Az utolsó ikon, a zöld zászló, állapotok szűrésére szolgál.

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



A Process Explorer egyféle részletesebb Task Manager, amely számon tartja az adott processzek által használt DLL-eket és egyéb erőforrásokat is.

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

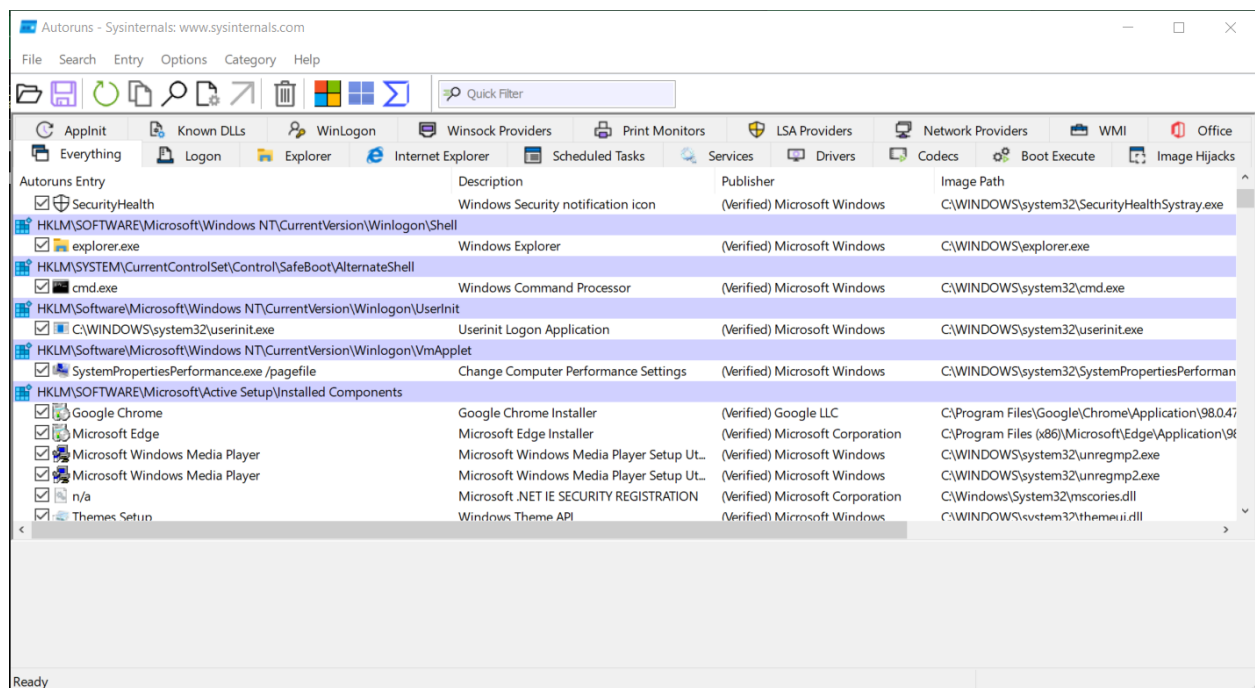
Time o...	Process Name	PID	Operation	Path	Result	Detail
12:45:19...	lsass.exe	944	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1,607,680, Le...
12:45:19...	lsass.exe	944	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1,591,296, Le...
12:45:19...	Explorer.EXE	6352	ReadFile	C:\Windows\System32\shlwapi.dll	SUCCESS	Offset 312,832, Len...
12:45:19...	lsass.exe	944	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1,513,984, Le...
12:45:19...	Explorer.EXE	6352	ReadFile	C:\Windows\System32\shlwapi.dll	SUCCESS	Offset 253,440, Le...
12:45:19...	lsass.exe	944	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1,579,008, Le...
12:45:19...	lsass.exe	944	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset 1,497,600, Le...
12:45:19...	Explorer.EXE	6352	ReadFile	C:\Windows\System32\windows.storage...	SUCCESS	Offset 6,910,464, Le...
12:45:19...	lsass.exe	944	QueryNameInfo...	C:\Users\User\Downloads\Sysinternals...	SUCCESS	Name: (Users\User...
12:45:19...	lsass.exe	944	QueryNameInfo...	C:\Users\User\Downloads\Sysinternals...	SUCCESS	Name: (Users\User...
12:45:19...	Explorer.EXE	6352	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset 3,581,440, Le...
12:45:19...	ctfmon.exe	13348	ReadFile	C:\Windows\System32\inputService.dll	SUCCESS	Offset 4,089,856, Le...
12:45:19...	ctfmon.exe	13348	ReadFile	C:\Windows\System32\TextInputFramew...	SUCCESS	Offset 900,608, Len...
12:45:19...	Explorer.EXE	6352	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset 3,532,288, Le...
12:45:19...	ctfmon.exe	13348	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
12:45:19...	ctfmon.exe	13348	RegOpenKey	HKLM\Software\Microsoft\Input\Setti...	SUCCESS	Desired Access: R...
12:45:19...	ctfmon.exe	13348	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
12:45:19...	ctfmon.exe	13348	RegOpenKey	HKCU\Software\Microsoft\Input\Setti...	SUCCESS	Desired Access: R...
12:45:19...	ctfmon.exe	13348	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Query: HandleTag...
12:45:19...	ctfmon.exe	13348	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Desired Access: Q...
12:45:19...	ctfmon.exe	13348	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Type: REG_DWO...
12:45:19...	Explorer.EXE	6352	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset 3,499,520, Le...
12:45:19...	ctfmon.exe	13348	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	
12:45:19...	ctfmon.exe	13348	RegQueryKey	HKCU\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Query: HandleTag...
12:45:19...	ctfmon.exe	13348	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Desired Access: Q...
12:45:19...	lsass.exe	944	ReadFile	C:\Windows\System32\samsrv.dll	SUCCESS	Offset 826,880, Len...
12:45:19...	ctfmon.exe	13348	RegQueryValue	HKCU\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Type: REG_DWO...
12:45:19...	ctfmon.exe	13348	RegCloseKey	HKCU\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	
12:45:19...	ctfmon.exe	13348	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	
12:45:19...	ctfmon.exe	13348	RegCloseKey	HKCU\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	
12:45:19...	ctfmon.exe	13348	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
12:45:19...	ctfmon.exe	13348	RegOpenKey	HKLM\Software\Microsoft\Input\Setti...	SUCCESS	Desired Access: R...

Showing 466,837 of 1,045,716 events (44%) Backed by virtual memory

A Process Monitor kilistázza az aktuális processzeket, és további információkat szolgáltat róluk, mint például az elvégzett művelet típusát (Operation oszlop), a szálát, amelyen fut, felhasznált registryket és fájlokat, vagy a hálózati aktivitást. A processzek és a róluk szóló információk folyamatosan adódnak hozzá a listához, így mindig össze lehet hasonlítani korábbi állapotokat az aktuálissal. Az első oszlopban az időpont jelenik meg, amikor az állapot fel lett jegyezve.

A Process Monitor lehetőséget ad rengeteg különböző szempont alapján szűrni vagy kiemelni a listában megjelenő elemeket.

Egy processz fa is megjeleníthető, hogy kiválaszthassuk azokat a processzeket, amelyeket meg szeretnénk jeleníteni a listában.



Az Autoruns kilistáz minden automatikusan induló alkalmazást, legyen az olyan, amely gép indításával indul vagy bejelentkezéskor, még a registry kulcsokat is megjeleníti. A program lehetőséget ad elrejtetni a Windowshoz vagy a Microsofthoz tartozó alkalmazásokat és processzeket, hogy könnyebben átláthatóak legyenek a harmadik féltől származó software-ek.

d) Security Utilities (LogonSession)

```
Administrator: Command Prompt
C:\Users\User\Downloads\SysinternalsSuite>logonsessions

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\DESKTOP-9D6GD9D$
  Auth package: NTLM
  Logon type: (none)
  Session: 0
  Sid: S-1-5-18
  Logon time: 02/13/2022 14:52:34
  Logon server:
  DNS Domain:
  UPN:

[1] Logon session 00000000:00012455:
  User name:
  Auth package: NTLM
  Logon type: (none)
  Session: 0
  Sid: (none)
  Logon time: 02/13/2022 14:52:34
  Logon server:
  DNS Domain:
  UPN:

[2] Logon session 00000000:00012825:
  User name: Font Driver Host\UMFD-0
  Auth package: Negotiate
  Logon type: Interactive
  Session: 0
  Sid: S-1-5-96-0-0
  Logon time: 02/13/2022 14:52:34
  Logon server:
  DNS Domain:
  UPN:

[3] Logon session 00000000:000003e5:
```

A LogonSessions kilistázza az aktuális bejelentkezési csoportokat (logon session-ok), és lehetőséget ad az adott csoportokhoz tartozó processzek megtekintésére is, például:

```
Administrator: Command Prompt

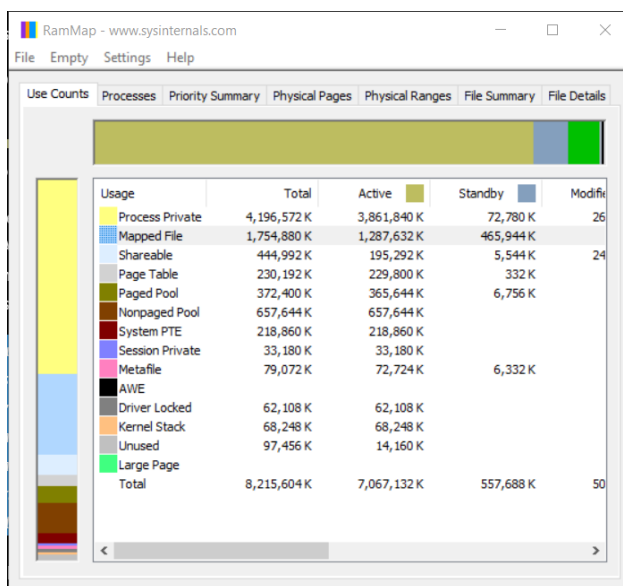
UPN:

[21] Logon session 00000000:220156c4:
User name: Window Manager\DWM-8
Auth package: Negotiate
Logon type: Interactive
Session: 8
Sid: S-1-5-90-0-8
Logon time: 02/18/2022 23:41:29
Logon server:
DNS Domain:
UPN:
10088: dwm.exe

[22] Logon session 00000000:22092af3:
User name: DESKTOP-9D6GD9D\User
Auth package: NTLM
Logon type: Interactive
Session: 8
Sid: S-1-5-21-3331196124-3159364482-3019219141-1001
Logon time: 02/19/2022 09:33:46
Logon server: DESKTOP-9D6GD9D
DNS Domain:
UPN:
6916: Wacom_TouchUser.exe
9680: Adobe Installer.exe
22768: steam.exe
9076: ACCStd.exe
7200: DTAgent.exe
4544: steamwebhelper.exe
9552: steamwebhelper.exe
12684: steamwebhelper.exe
21928: steamwebhelper.exe
13548: steamwebhelper.exe
11400: steamwebhelper.exe
13120: steamwebhelper.exe
7252: cmd.exe
13180: conhost.exe
23412: logonsessions.exe

[23] Logon session 00000000:22092b67:
```

e) Information Utilities (RAMMap)

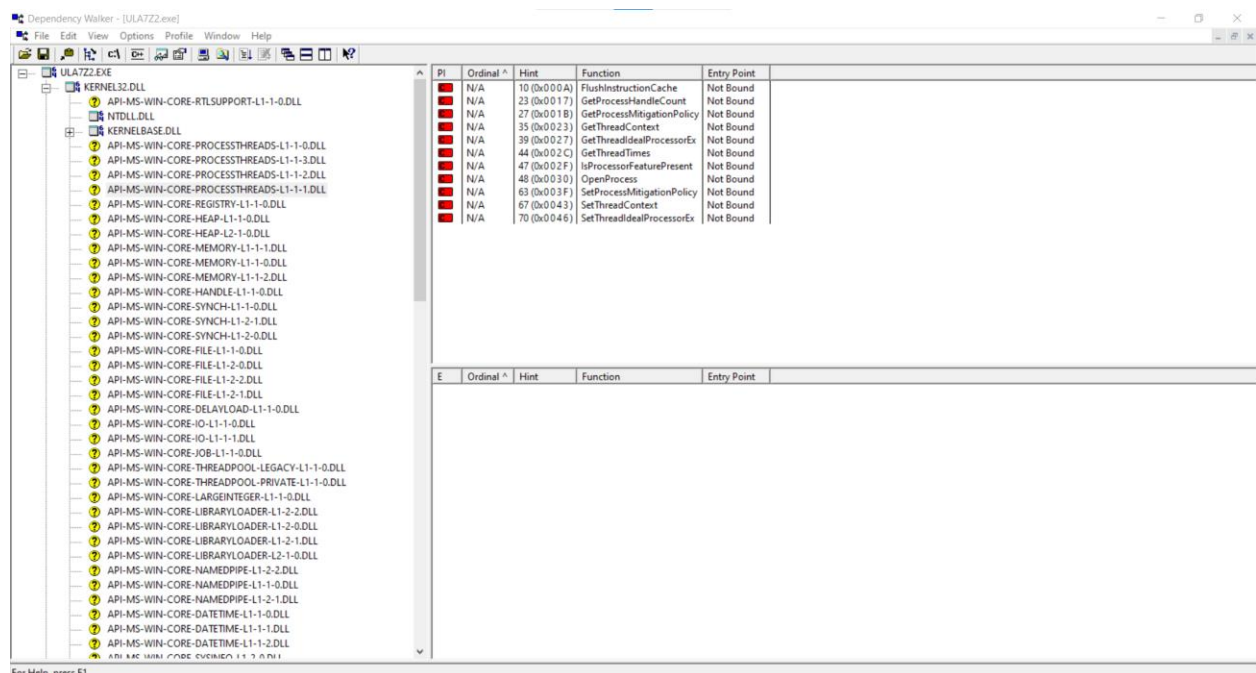


A RAMMap arra szolgál, hogy részletes listát adjon arról, ahogy a Windows hogyan kezeli a memóriát. Többféle megvizsgálási szempontot is biztosít a különböző fülökön:

- Use Counts: memóriahasználati összefoglaló típus és paging (lapozás) szerint csoportosítva
- Processes: processzek részletes memóriahasználata
- Priority Summary: prioritás szerint csoportosított memóriahasználat
- Physical Pages: kilistázott fizikai memóriacímek, és hozzá tartozó részletes információk (pl. milyen processz használja, milyen virtuális cím tartozik hozzá)
- Physical Ranges: memóriacím-tartományok szerint csoportosított memória foglalkozás
- File Summary: fájlankénti RAM használat
- File Details: fájlok memóriahasználatra utaló részletes adatai

3. feladat: Töltse le a következő programot: Dependency Walker

a) Vizsgálja meg, hogy a neptunkod.exe milyen API hívásokat használ a kernel32.dll-ből



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

A NTDLL.DLL-hez tartozó exportált függvények alapján látszólag ez a dll tartalmazza a programhoz (és a forrásfájl lefordításához) szükséges gépi kódokat,

számos olyan függvényt tartalmazva, amely szorosan kapcsolódik a program működéséhez, például NtDrawText, NtLockFile, NtReadFile.