

Operációs rendszerek Bsc

2.Gyak

2022.02.15

Készítette:

Garay Gabriel

Programtervező informatika

GJ2N7R

Miskolc, 2022

1. a) Mappa szerkezet létrehozása

- A fájlokat az **mkdir** paranccsal hoztam létre.

```
C:\>tree GJ2N7R
Folder PATH listing
Volume serial number is 00000211 F829:DC09
C:\GJ2N7R
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   └── korte
├── land
│   ├── kokusz
│   └── szeder
└──
```

b) A „szeder” fájl átmásolása a fa mappába

- A fájlok átmásolásához az **Xcopy** parancsot használtam. Ahhoz, hogy ne másoljam át az egész fájlt, létre kellett hozni egy kivételeket tartalmazó txt fájlt, beleírni a mellőzendő mappákat, és a **/exclude** kapcsoló segítségével kihagyni őket a másolás során. A txt fájl tartalmának cseréjéhez használt parancs az **echo >**.

- A parancs: **Xcopy land fa /E /T /EXCLUDE:excludelist.txt**, illetve

Xcopy bokor fa /E /T /EXCLUDE:excludelist.txt

```
C:\GJ2N7R>echo kokusz > excludelist.txt

C:\GJ2N7R>Xcopy land fa /E /T /EXCLUDE:excludelist.txt

C:\GJ2N7R>tree
Folder PATH listing
Volume serial number is F829-DC09
C:..
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   ├── korte
│   └── szeder
├── land
│   ├── kokusz
│   └── szeder
└──
```

```

C:\GJ2N7R>echo barack >> excludelist.txt

C:\GJ2N7R>Xcopy bokor fa /E /T /EXCLUDE:excludelist.txt

C:\GJ2N7R>cd..

C:\>tree GJ2N7R
Folder PATH listing
Volume serial number is F829-DC09
C:\GJ2N7R
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   ├── banan
│   ├── korte
│   └── szeder
└── land
    ├── kokusz
    └── szeder

```

c) Fájlok áthelyezése

- A használt parancs a **move**.

```

C:\GJ2N7R>move bokor/barack fa
1 dir(s) moved.

C:\GJ2N7R>cd..

C:\>tree GJ2N7R
Folder PATH listing
Volume serial number is 0000028E F829:DC09
C:\GJ2N7R
├── bokor
│   ├── banan
│   └── mogyoro
├── fa
│   ├── banan
│   ├── barack
│   ├── korte
│   └── szeder
└── land
    ├── kokusz
    └── szeder

```

```

C:\>move GJ2N7R/land/kokusz GJ2N7R/fa
1 dir(s) moved.

C:\>tree GJ2N7R
Folder PATH listing
Volume serial number is F829-DC09
C:\GJ2N7R
├── bokor
│   ├── banan
│   └── mogyoro
├── fa
│   ├── banan
│   ├── barack
│   ├── kokusz
│   ├── korte
│   └── szeder
└── land
    └── szeder

```

d) Land katalógus törlése, és szöveges fájlok létrehozása

- A törléshez használt parancs az **rmdir**.

```
C:\GJ2N7R>rmdir land /S /Q

C:\GJ2N7R>cd..

C:\>tree GJ2N7R
Folder PATH listing
Volume serial number is F829-DC09
C:\GJ2N7R
├── bokor
│   ├── banan
│   └── mogyoro
└── fa
    ├── banan
    ├── barack
    ├── kokusz
    ├── korte
    └── szeder
```

-A szöveges fájl létrehozáshoz használt parancs a **copy con**

```
C:\>copy con GJ2N7R\bokor\banan\leiras.txt
^Z
        1 file(s) copied.
```

```
C:\>copy con GJ2N7R\fa\felsorolas.txt
^Z
        1 file(s) copied.

C:\>
```

e) 3 mondat a barackról a leiras.txt fájlba

```
C:\>copy con GJ2N7R\bokor\banan\leiras.txt
A barack hazankban is termo gyumolcs.
Overwrite GJ2N7R\bokor\banan\leiras.txt? (Yes/No/All): y
Atlagosan julius környeken erik.
Kozepeben mag talalhato
^Z
        1 file(s) copied.
```

```
C:\>copy con GJ2N7R\fa\felsorolas.txt
Berki Viktor
Overwrite GJ2N7R\fa\felsorolas.txt? (Yes/No/All): y
Csonka Patrik
David Rebeka
Kartczub Roland
Kormos Balazs
^7
```

f) Neptunkód mappa listázása az almappakkal is

- A használt parancs a **dir /S /B**

```
C:\GJ2N7R>dir /B /S
C:\GJ2N7R\bokor
C:\GJ2N7R\excludelist.txt
C:\GJ2N7R\fa
C:\GJ2N7R\bokor\banan
C:\GJ2N7R\bokor\mogyor
C:\GJ2N7R\bokor\banan\leiras.txt
C:\GJ2N7R\fa\banan
C:\GJ2N7R\fa\barack
C:\GJ2N7R\fa\felsorolas.txt
C:\GJ2N7R\fa\kokusz
C:\GJ2N7R\fa\korte
C:\GJ2N7R\fa\szeder
```

g) A gyökérmappa összes olyan fájljának kikeresése, amelyeknek a második betűje „e”.

- A használt parancs **dir ?e***

```
C:\>dir ?e*
Volume in drive C has no label.
Volume Serial Number is F829-DC09

Directory of C:\

2017. 01. 02. 13:18 <DIR> OEM
2018. 04. 12. 00:38 <DIR> PerfLogs
                0 File(s)          0 bytes
                2 Dir(s)  36 639 014 912 bytes free

C:\>
```

h) A felsorolas.txt fájl olvashatóvá tétele

```
C:\>attrib -r GJ2N7R\fa\felsorolas.txt
```

i)A neptunkod fájl teljes méretének megjelenítése

```
Directory of C:\GJ2N7R\fa
2022. 02. 16. 19:14 <DIR> .
2022. 02. 16. 19:14 <DIR> ..
2022. 02. 16. 18:01 <DIR> banan
2022. 02. 16. 18:01 <DIR> barack
2022. 02. 16. 19:27 75 felsorolas.txt
2022. 02. 16. 18:02 <DIR> kokusz
2022. 02. 16. 18:02 <DIR> korte
2022. 02. 16. 18:02 <DIR> szeder
                1 File(s)          75 bytes

Directory of C:\GJ2N7R\fa\banan
2022. 02. 16. 18:01 <DIR> .
2022. 02. 16. 18:01 <DIR> ..
                0 File(s)          0 bytes

Directory of C:\GJ2N7R\fa\barack
2022. 02. 16. 18:01 <DIR> .
2022. 02. 16. 18:01 <DIR> ..
                0 File(s)          0 bytes

Directory of C:\GJ2N7R\fa\kokusz
2022. 02. 16. 18:02 <DIR> .
2022. 02. 16. 18:02 <DIR> ..
                0 File(s)          0 bytes

Directory of C:\GJ2N7R\fa\korte
2022. 02. 16. 18:02 <DIR> .
2022. 02. 16. 18:02 <DIR> ..
                0 File(s)          0 bytes

Directory of C:\GJ2N7R\fa\szeder
2022. 02. 16. 18:02 <DIR> .
2022. 02. 16. 18:02 <DIR> ..
                0 File(s)          0 bytes

Total Files Listed:
        3 File(s)          192 bytes
       29 Dir(s)  36 605 284 352 bytes free
```

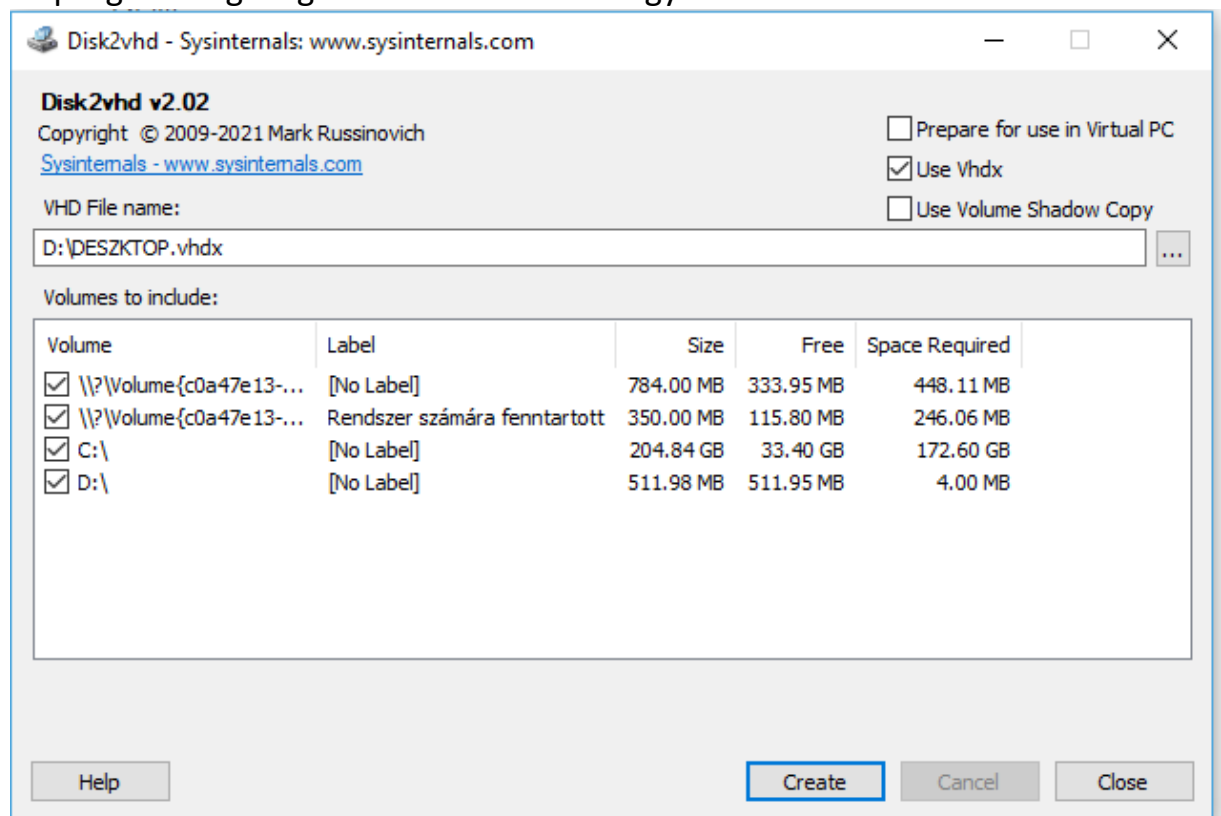
j) A felsorolas.txt fájl tartalmának rendezése ABC sorrendben

```
C:\>sort GJ2N7R\fa\felsorolas.txt
Berki Viktor
Csonka Patrik
David Rebeka
Kartczub Roland
Kormos Balazs
```

2. Sysinternals Suite csomag letöltése, felsorolt programok futtatása.

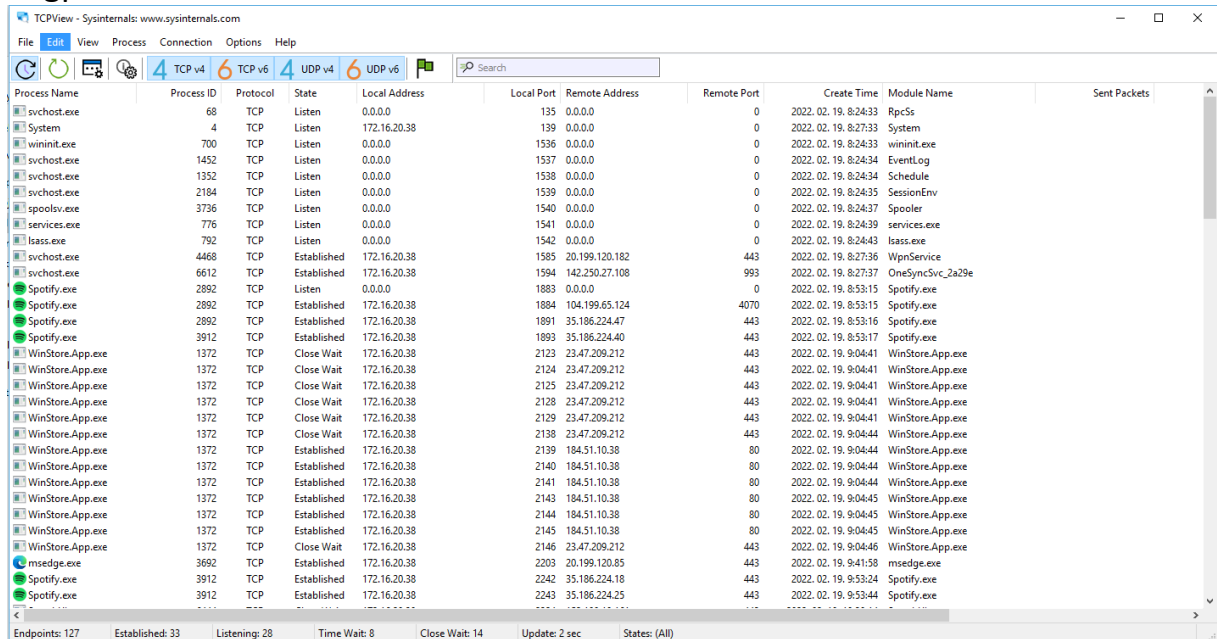
a) File and Disk Utilities(Disk2vhd)

-A program segítségével létrehozhatunk egy virtuális merevlemezt.



b) Networking utilities(TCPView)

-A program feladata, hogy kilistázza az összes TCP- és UDP-végpontokat a rendszerben.



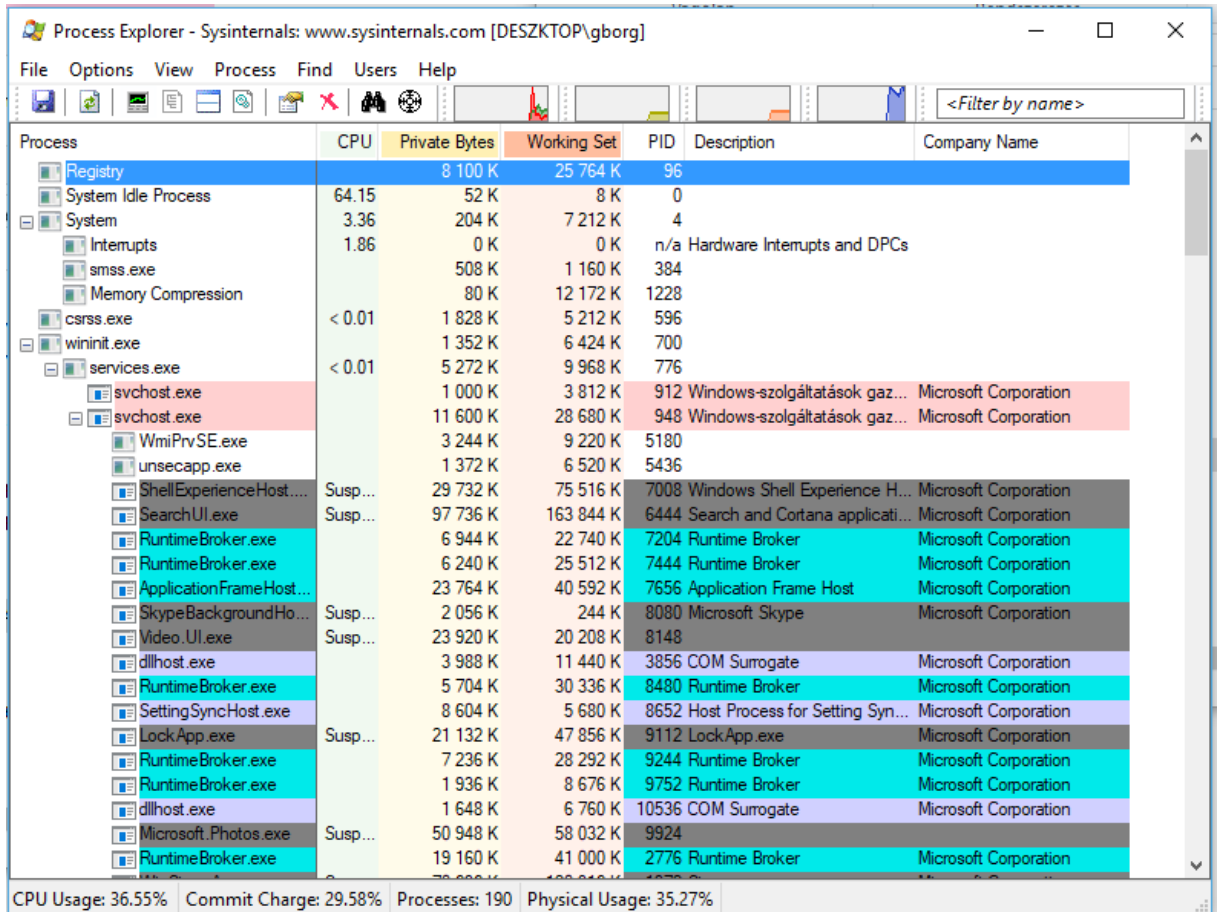
The screenshot shows the TCPView application window. The interface includes a menu bar (File, Edit, View, Process, Connection, Options, Help), a toolbar with icons for refreshing, pausing, and other functions, and a tabbed interface with 'TCP v4', 'TCP v6', 'UDP v4', and 'UDP v6' tabs. The 'TCP v4' tab is selected. A search bar is located on the right side of the toolbar. The main area displays a table of network connections with columns: Process Name, Process ID, Protocol, State, Local Address, Local Port, Remote Address, Remote Port, Create Time, Module Name, and Sent Packets. The table lists various system and user processes, including svchost.exe, System, wininit.exe, EventLog, SessionEnv, Spooler, services.exe, lsass.exe, WpnService, OneSyncSvc_2a29e, and several instances of WinStore.App.exe. The status bar at the bottom shows summary statistics: Endpoints: 127, Established: 33, Listening: 28, Time Wait: 8, Close Wait: 14, Update: 2 sec, and States: (All).

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
svchost.exe	68	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2022.02.19.8:24:33	RpcCs	
System	4	TCP	Listen	172.16.20.38	139	0.0.0.0	0	2022.02.19.8:27:33	System	
wininit.exe	700	TCP	Listen	0.0.0.0	1536	0.0.0.0	0	2022.02.19.8:24:33	wininit.exe	
svchost.exe	1452	TCP	Listen	0.0.0.0	1537	0.0.0.0	0	2022.02.19.8:24:34	EventLog	
svchost.exe	1352	TCP	Listen	0.0.0.0	1538	0.0.0.0	0	2022.02.19.8:24:34	Schedule	
svchost.exe	2184	TCP	Listen	0.0.0.0	1539	0.0.0.0	0	2022.02.19.8:24:35	SessionEnv	
spoolsv.exe	3736	TCP	Listen	0.0.0.0	1540	0.0.0.0	0	2022.02.19.8:24:37	Spooler	
services.exe	776	TCP	Listen	0.0.0.0	1541	0.0.0.0	0	2022.02.19.8:24:39	services.exe	
lsass.exe	792	TCP	Listen	0.0.0.0	1542	0.0.0.0	0	2022.02.19.8:24:43	lsass.exe	
svchost.exe	4468	TCP	Established	172.16.20.38	1585	20.199.120.182	443	2022.02.19.8:27:36	WpnService	
svchost.exe	6612	TCP	Established	172.16.20.38	1594	142.250.27.108	993	2022.02.19.8:27:37	OneSyncSvc_2a29e	
Spotify.exe	2892	TCP	Listen	0.0.0.0	1883	0.0.0.0	0	2022.02.19.8:53:15	Spotify.exe	
Spotify.exe	2892	TCP	Established	172.16.20.38	1884	104.199.65.124	4070	2022.02.19.8:53:15	Spotify.exe	
Spotify.exe	2892	TCP	Established	172.16.20.38	1891	35.186.234.47	443	2022.02.19.8:53:16	Spotify.exe	
Spotify.exe	3912	TCP	Established	172.16.20.38	1893	35.186.234.40	443	2022.02.19.8:53:17	Spotify.exe	
WinStore.App.exe	1372	TCP	Close Wait	172.16.20.38	2123	23.47.209.212	443	2022.02.19.9:04:41	WinStore.App.exe	
WinStore.App.exe	1372	TCP	Close Wait	172.16.20.38	2124	23.47.209.212	443	2022.02.19.9:04:41	WinStore.App.exe	
WinStore.App.exe	1372	TCP	Close Wait	172.16.20.38	2125	23.47.209.212	443	2022.02.19.9:04:41	WinStore.App.exe	
WinStore.App.exe	1372	TCP	Close Wait	172.16.20.38	2128	23.47.209.212	443	2022.02.19.9:04:41	WinStore.App.exe	
WinStore.App.exe	1372	TCP	Close Wait	172.16.20.38	2129	23.47.209.212	443	2022.02.19.9:04:41	WinStore.App.exe	
WinStore.App.exe	1372	TCP	Close Wait	172.16.20.38	2138	23.47.209.212	443	2022.02.19.9:04:44	WinStore.App.exe	
WinStore.App.exe	1372	TCP	Established	172.16.20.38	2139	184.51.10.38	80	2022.02.19.9:04:44	WinStore.App.exe	
WinStore.App.exe	1372	TCP	Established	172.16.20.38	2140	184.51.10.38	80	2022.02.19.9:04:44	WinStore.App.exe	
WinStore.App.exe	1372	TCP	Established	172.16.20.38	2141	184.51.10.38	80	2022.02.19.9:04:44	WinStore.App.exe	
WinStore.App.exe	1372	TCP	Established	172.16.20.38	2143	184.51.10.38	80	2022.02.19.9:04:45	WinStore.App.exe	
WinStore.App.exe	1372	TCP	Established	172.16.20.38	2144	184.51.10.38	80	2022.02.19.9:04:45	WinStore.App.exe	
WinStore.App.exe	1372	TCP	Established	172.16.20.38	2145	184.51.10.38	80	2022.02.19.9:04:45	WinStore.App.exe	
WinStore.App.exe	1372	TCP	Established	172.16.20.38	2146	23.47.209.212	443	2022.02.19.9:04:46	WinStore.App.exe	
msedge.exe	3692	TCP	Established	172.16.20.38	2203	20.199.120.65	443	2022.02.19.9:41:58	msedge.exe	
Spotify.exe	3912	TCP	Established	172.16.20.38	2242	35.186.224.18	443	2022.02.19.9:53:24	Spotify.exe	
Spotify.exe	3912	TCP	Established	172.16.20.38	2243	35.186.224.25	443	2022.02.19.9:53:44	Spotify.exe	

Endpoints: 127 Established: 33 Listening: 28 Time Wait: 8 Close Wait: 14 Update: 2 sec States: (All)

c) Process Utilities (Process Explorer)

-A szoftver a számítógépes hibák javításáért felelős és megvédi a felhasználót a fájlvesztésektől, hardverhibáktól.



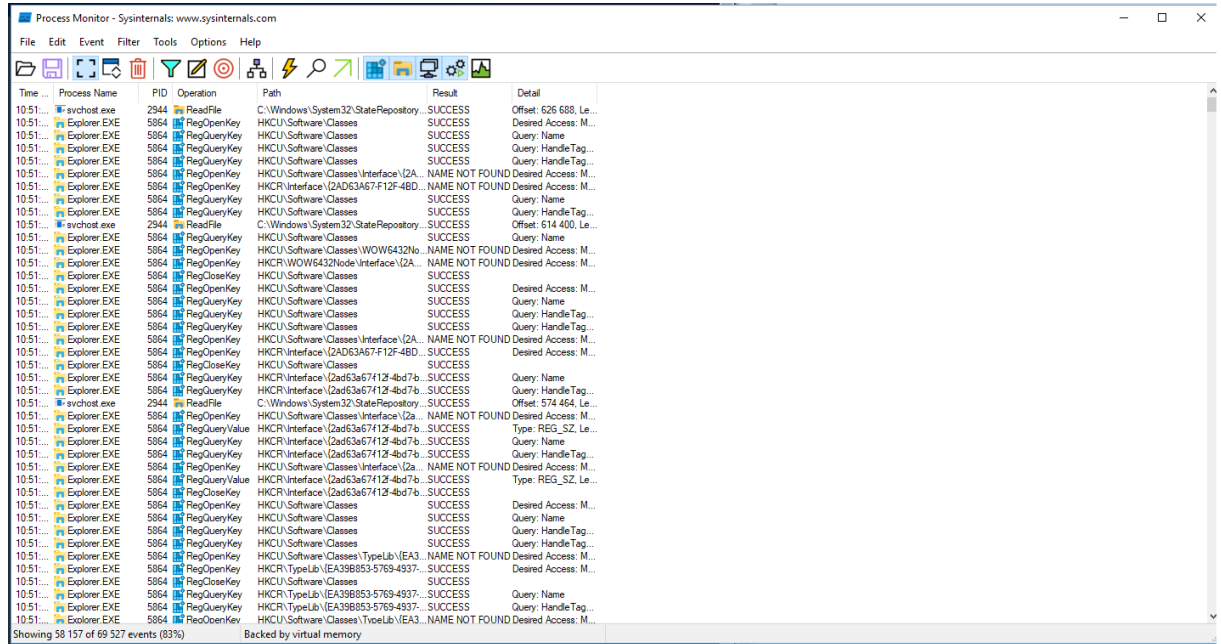
The screenshot shows the Process Explorer window from Sysinternals. The title bar reads 'Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP\gborg]'. The menu bar includes File, Options, View, Process, Find, Users, and Help. The toolbar contains icons for file operations, process management, and search. A search filter box on the right says '<Filter by name>'. The main table lists processes with columns for Process, CPU, Private Bytes, Working Set, PID, Description, and Company Name. The 'Process' column has a tree view on the left showing the hierarchy from Registry to System, and then individual processes. The 'CPU' column shows usage percentages, some with status like 'Susp...'. The 'Private Bytes' and 'Working Set' columns show memory usage in K. The 'PID' column shows the process ID. The 'Description' column shows the full name of the process. The 'Company Name' column shows the manufacturer. At the bottom, a status bar displays 'CPU Usage: 36.55%', 'Commit Charge: 29.58%', 'Processes: 190', and 'Physical Usage: 35.27%'.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		8 100 K	25 764 K	96		
System Idle Process	64.15	52 K	8 K	0		
System	3.36	204 K	7 212 K	4		
Interrupts	1.86	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		508 K	1 160 K	384		
Memory Compression		80 K	12 172 K	1228		
csrss.exe	< 0.01	1 828 K	5 212 K	596		
wininit.exe	< 0.01	1 352 K	6 424 K	700		
services.exe	< 0.01	5 272 K	9 968 K	776		
svchost.exe		1 000 K	3 812 K	912	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		11 600 K	28 680 K	948	Windows-szolgáltatások gaz...	Microsoft Corporation
WmiPrvSE.exe		3 244 K	9 220 K	5180		
unsecapp.exe		1 372 K	6 520 K	5436		
ShellExperienceHost.exe	Susp...	29 732 K	75 516 K	7008	Windows Shell Experience H...	Microsoft Corporation
SearchUI.exe	Susp...	97 736 K	163 844 K	6444	Search and Cortana applicati...	Microsoft Corporation
RuntimeBroker.exe		6 944 K	22 740 K	7204	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		6 240 K	25 512 K	7444	Runtime Broker	Microsoft Corporation
ApplicationFrameHost.exe		23 764 K	40 592 K	7656	Application Frame Host	Microsoft Corporation
SkypeBackgroundHost.exe	Susp...	2 056 K	244 K	8080	Microsoft Skype	Microsoft Corporation
Video.UI.exe	Susp...	23 920 K	20 208 K	8148		
dllhost.exe		3 988 K	11 440 K	3856	COM Surrogate	Microsoft Corporation
RuntimeBroker.exe		5 704 K	30 336 K	8480	Runtime Broker	Microsoft Corporation
SettingSyncHost.exe		8 604 K	5 680 K	8652	Host Process for Setting Syn...	Microsoft Corporation
LockApp.exe	Susp...	21 132 K	47 856 K	9112	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		7 236 K	28 292 K	9244	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		1 936 K	8 676 K	9752	Runtime Broker	Microsoft Corporation
dllhost.exe		1 648 K	6 760 K	10536	COM Surrogate	Microsoft Corporation
Microsoft.Photos.exe	Susp...	50 948 K	58 032 K	9924		
RuntimeBroker.exe		19 160 K	41 000 K	2776	Runtime Broker	Microsoft Corporation

CPU Usage: 36.55% | Commit Charge: 29.58% | Processes: 190 | Physical Usage: 35.27%

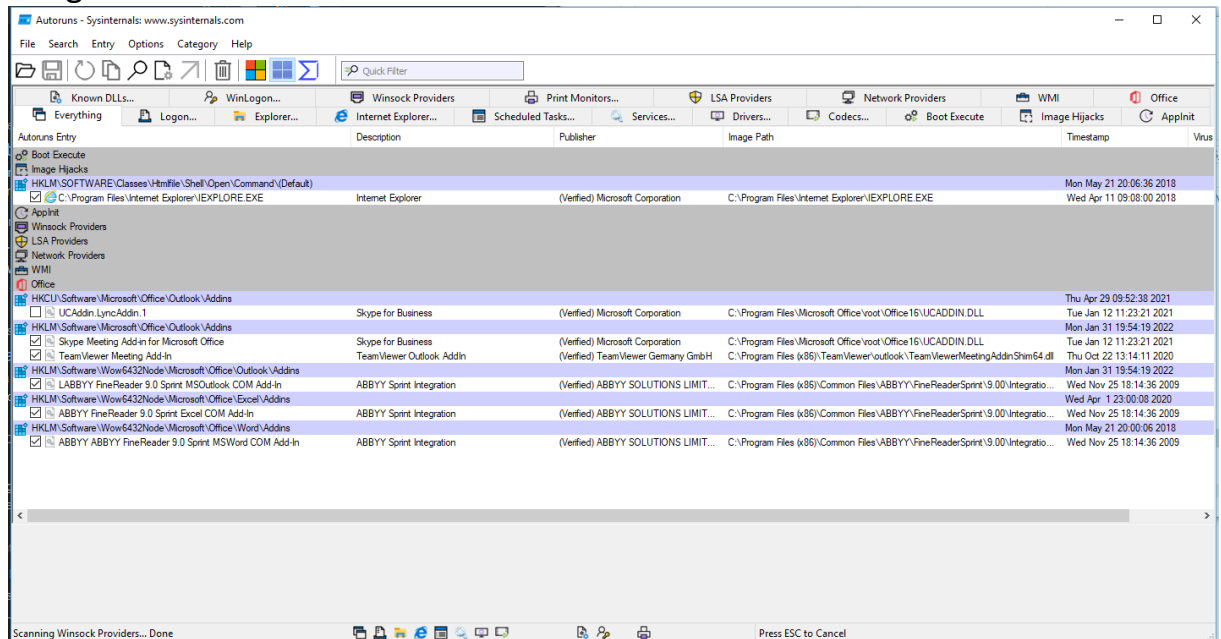
(Process Monitor)

-A Process Monitor feladata, hogy segítse az alkalmazásokkal kapcsolatos problémák kezelését a számítógépen.



(AutoRuns)

-Az AutoRuns program fő használati célja a windows indításánál a programok automatikus futtatásának bekapcsolása/kikapcsolása. Ezen kívül megmutatja az induló menü elemeket, illesztőprogramokat, szolgáltatásokat és sok más.



- d) Security Utilities(LogonSession)[Képernyőkép a következő lapon]**
- Kilstázza a jelenlegi aktív bejelentkezéseket.

```
Sid: S-1-5-96-0-1
Logon time: 2022. 02. 19. 8:24:34
Logon server:
DNS Domain:
UPN:

[5] Logon session 00000000:00015246:
User name: Window Manager\DWM-1
Auth package: Negotiate
Logon type: Interactive
Session: 1
Sid: S-1-5-90-0-1
Logon time: 2022. 02. 19. 8:24:34
Logon server:
DNS Domain:
UPN:

[6] Logon session 00000000:000152b3:
User name: Window Manager\DWM-1
Auth package: Negotiate
Logon type: Interactive
Session: 1
Sid: S-1-5-90-0-1
Logon time: 2022. 02. 19. 8:24:34
Logon server:
DNS Domain:
UPN:

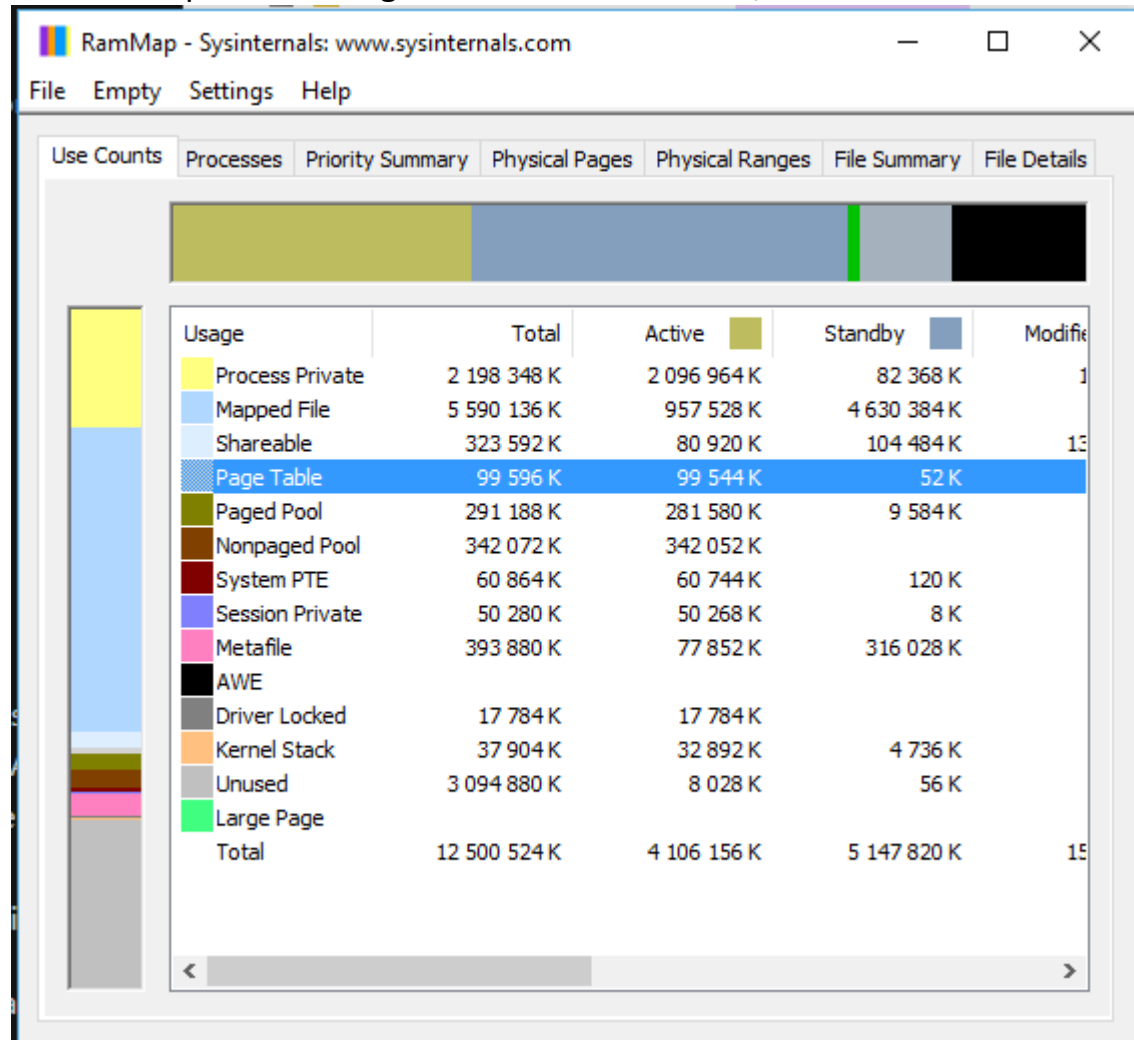
[7] Logon session 00000000:000003e5:
User name: NT AUTHORITY\HELYI SZOLGLTATLS
Auth package: Negotiate
Logon type: Service
Session: 0
Sid: S-1-5-19
Logon time: 2022. 02. 19. 8:24:34
Logon server:
DNS Domain:
UPN:

[8] Logon session 00000000:00024fd2:
User name: DESZKTOP\gborg
Auth package: CloudAP
Logon type: Interactive
Session: 1
Sid: S-1-5-21-3706558226-4134771054-4219173159-1001
Logon time: 2022. 02. 19. 8:24:36
Logon server:
DNS Domain:
UPN:

[9] Logon session 00000000:00025181:
User name: DESZKTOP\gborg
Auth package: CloudAP
Logon type: Interactive
Session: 1
Sid: S-1-5-21-3706558226-4134771054-4219173159-1001
Logon time: 2022. 02. 19. 8:24:36
Logon server:
DNS Domain:
UPN:
```

e) Information Utilities(RAMMap)

- A RAMMap analízist végez a memóriakezelésről, RAM allokációról.



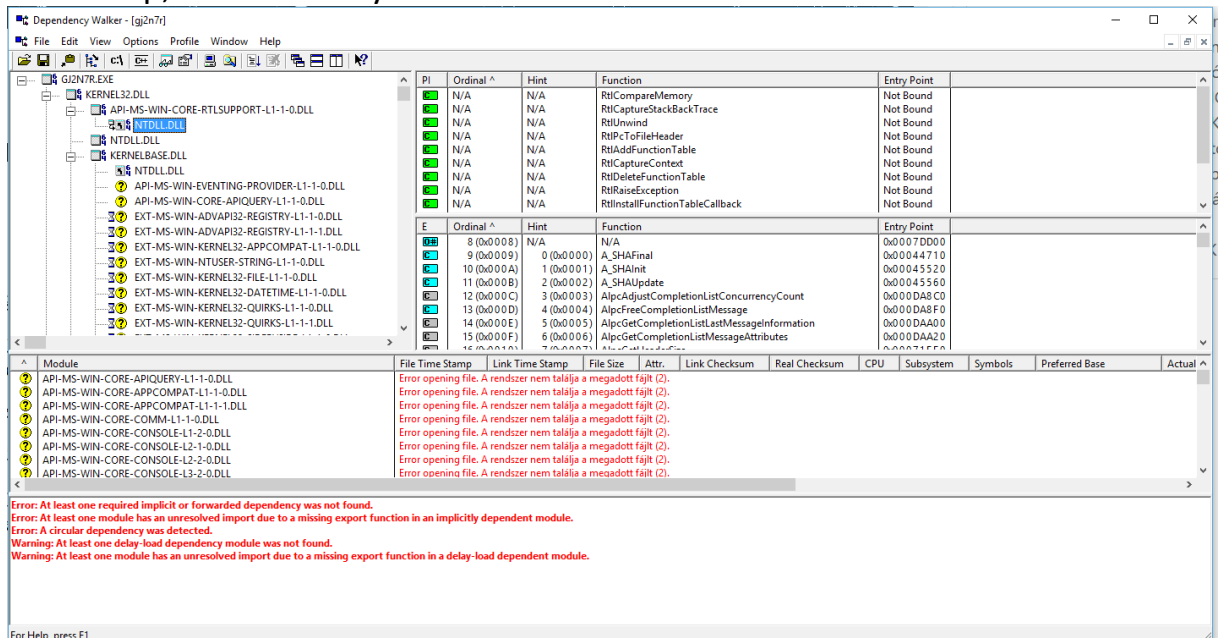
3. neptunkod.c nevű forráskód elkészítése, futtatása.

```
C:\Users\gborg\Desktop\Egyetem 2021-22 2>gcc gj2n7r.c -o gj2n7r.exe

C:\Users\gborg\Desktop\Egyetem 2021-22 2>gj2n7r
Garay Gabriel,
Programtervezo informatika,
GJ2N7R
C:\Users\gborg\Desktop\Egyetem 2021-22 2>
```

a)

- A program rengeteg API hívást használ, például: win-eventing, ntuser, core-heap, core-memory...



b)

Az NTDLL.DLL szerepe, hogy exportálja az alapértelmezett API-t, ami egy operációs rendszer által használt felület.