

Operációs rendszerek BSc

2. Gyak.

2022. 02. 20.

Készítette:

Sárosi Bence BProf
Üzemtechnikus-informatikus
DQ1Q17

Miskolc, 2022

1.feladat:

a) Hozza létre a következő mappa szerkezetet!

```
Microsoft Windows [Version 10.0.19043.1466]
(c) Microsoft Corporation. Minden jog fenntartva.

C:\Users\Roland>mkdir DQ1Q17

C:\Users\Roland>dc DQ1Q17
'dc' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Roland>cd DQ1Q17

C:\Users\Roland\DQ1Q17>mkdir bokor

C:\Users\Roland\DQ1Q17>mkdir fa
'mkdir' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Roland\DQ1Q17>mkdir fa

C:\Users\Roland\DQ1Q17>mkdir land

C:\Users\Roland\DQ1Q17>cd bokor

C:\Users\Roland\DQ1Q17\bokor>mkdir banan

C:\Users\Roland\DQ1Q17\bokor>mkdir barack

C:\Users\Roland\DQ1Q17\bokor>mkdir mogyor

C:\Users\Roland\DQ1Q17\bokor>d..
'd..' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Roland\DQ1Q17\bokor>cd..

C:\Users\Roland\DQ1Q17>cd fa

C:\Users\Roland\DQ1Q17\fa>mkdir korte

C:\Users\Roland\DQ1Q17\fa>cd..

C:\Users\Roland\DQ1Q17>cd land

C:\Users\Roland\DQ1Q17\land>mkdir kokusz

C:\Users\Roland\DQ1Q17\land>mkdir szeder

C:\Users\Roland\DQ1Q17\land>cd..
```

```
C:\Users\Roland\DQ1Q17>mkdir land

C:\Users\Roland\DQ1Q17>cd bokor

C:\Users\Roland\DQ1Q17\bokor>mkdir banan

C:\Users\Roland\DQ1Q17\bokor>mkdir barack

C:\Users\Roland\DQ1Q17\bokor>mkdir mogyor

C:\Users\Roland\DQ1Q17\bokor>d..
'd..' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Roland\DQ1Q17\bokor>cd..

C:\Users\Roland\DQ1Q17>cd fa

C:\Users\Roland\DQ1Q17\fa>mkdir korte

C:\Users\Roland\DQ1Q17\fa>cd..

C:\Users\Roland\DQ1Q17>cd land

C:\Users\Roland\DQ1Q17\land>mkdir kokusz

C:\Users\Roland\DQ1Q17\land>mkdir szeder

C:\Users\Roland\DQ1Q17\land>cd..

C:\Users\Roland\DQ1Q17>tree
Folder PATH listing for volume Boot
Volume serial number is 5414-9A70
C:.
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyor
├── 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

```
C:\Users\Roland\DQ1Q17>xcopy "C:\Users\Roland\DQ1Q17\land\szeder" "C:\Users\Roland\DQ1Q17\fa" /t /e_
```

```
C:\Users\Roland\DQ1Q17>xcopy "C:\Users\Roland\DQ1Q17\bokor\banan" "C:\Users\Roland\DQ1Q17\fa" /t /e_
```

```
C:\Users\Roland>cd DQ1Q17
C:\Users\Roland\DQ1Q17>tree
Folder PATH listing for volume Boot
Volume serial number is 5414-9A70
C:.
├── bokor
│   ├── banan
│   └── mogyoró
├── fa
│   ├── banan
│   ├── barack
│   ├── kokusz
│   ├── korte
│   └── szeder
├── land
│   └── szeder
└──
```

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

```
C:\Users\Roland\DQ1Q17>move bokor\barack fa
1 dir(s) moved.
```

```
C:\Users\Roland\DQ1Q17>move land\kokusz fa
1 dir(s) moved.
```

```
C:\Users\Roland\DQ1Q17>tree
Folder PATH listing for volume Boot
Volume serial number is 5414-9A70
```

```
C:..
|
|---bokor
|   |
|   |---banan
|   |---mogyor
|
|---fa
|   |
|   |---banan
|   |---barack
|   |---kokusz
|   |---korte
|   |---szeder
|
|---land
|   |
|   |---szeder
```

```
C:\Users\Roland\DQ1Q17>
```

1.feladat:

d) Törölje a neptunkod/land katalógust a teljes tartalmával. Hozza létre a következő szöveges allományokat:

neptunkod/bokor/banan/ leiras.txt

neptunkod/tree/felsorolas.txt

```
C:\Users\Roland\DQ1Q17>rmdir /s land
land, Are you sure (Y/N)? y

C:\Users\Roland\DQ1Q17>tree
Folder PATH listing for volume Boot
Volume serial number is 5414-9A70
C:.
|
|_ bokor
|   |
|   |_ banan
|   |_ mogyor
|
|_ fa
    |
    |_ banan
    |_ barack
    |_ kokusz
    |_ korte
    |_ szeder

C:\Users\Roland\DQ1Q17>

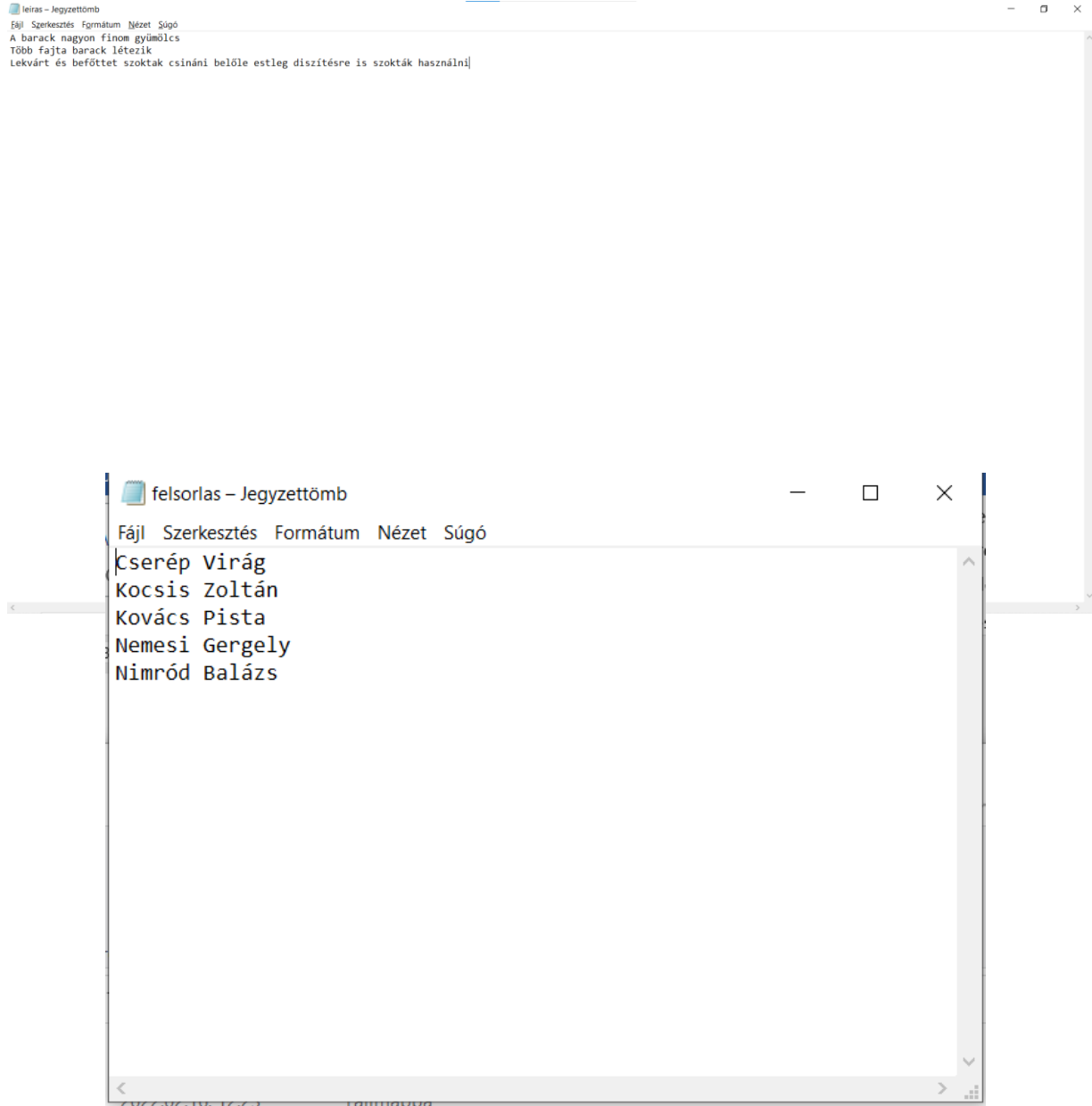
C:\Users\Roland\DQ1Q17>cd bokor
C:\Users\Roland\DQ1Q17\bokor>cd banan
C:\Users\Roland\DQ1Q17\bokor\banan>notepad leiras.txt
C:\Users\Roland\DQ1Q17\bokor\banan>cd..
C:\Users\Roland\DQ1Q17\bokor>cd..
C:\Users\Roland\DQ1Q17>cd fa
C:\Users\Roland\DQ1Q17\fa>cd fa
A rendszer nem találja a megadott elérési utat.
C:\Users\Roland\DQ1Q17\fa>notepad leiras.txt
C:\Users\Roland\DQ1Q17\fa>tree
Folder PATH listing for volume Boot
Volume serial number is 5414-9A70
C:.
|_ banan
|_ barack
|_ kokusz
|_ korte
|_ szeder

C:\Users\Roland\DQ1Q17\fa>cd..
C:\Users\Roland\DQ1Q17>treeü
'treeü' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Roland\DQ1Q17>tree
Folder PATH listing for volume Boot
Volume serial number is 5414-9A70
C:.
|_ bokor
|   |_ banan
|   |_ mogyor
|
|_ fa
    |_ banan
    |_ barack
    |_ kokusz
    |_ korte
    |_ szeder

C:\Users\Roland\DQ1Q17>
```

1.feladat:

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



1.feladat:

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

```
C:\Users\Roland\DQ1Q17>tree
Folder PATH listing for volume Boot
Volume serial number is 5414-9A70
C:.\
├── bokor
│   ├── banan
│   └── mogyor
└── fa
    ├── banan
    ├── barack
    ├── kokusz
    ├── korte
    └── szeder

C:\Users\Roland\DQ1Q17>s
```

1.feladat:

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

```
C:\Users\Roland\DQ1Q17>dir *e* /s
Volume in drive C is Boot
Volume Serial Number is 5414-9A70

Directory of C:\Users\Roland\DQ1Q17\bokor\banan

2022.02.16.  12:48                85 leiras.txt
               1 File(s)                85 bytes

Directory of C:\Users\Roland\DQ1Q17\fa

2022.02.16.  12:24    <DIR>          korte
2022.02.16.  12:50                78 leiras.txt
2022.02.16.  12:25    <DIR>          szeder
               1 File(s)                78 bytes

Total Files Listed:
               2 File(s)                163 bytes
               2 Dir(s)  15 309 602 816 bytes free

C:\Users\Roland\DQ1Q17>dir *e* /b /s
C:\Users\Roland\DQ1Q17\bokor\banan\leiras.txt
C:\Users\Roland\DQ1Q17\fa\korte
C:\Users\Roland\DQ1Q17\fa\leiras.txt
C:\Users\Roland\DQ1Q17\fa\szeder

C:\Users\Roland\DQ1Q17>
```


1.feladat:

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

```
C:\Users\Roland\DQ1Q17\fa>sort felsorlas.txt /o felsorlas.txt

C:\Users\Roland\DQ1Q17\fa>icacls felsorlas.txt /t /grant Everyone:R
Everyone: A fióknevek és a biztonsági azonosítók között nem jött létre egymáshoz rendelés.
Successfully processed 0 files; Failed processing 1 files
```

1.feladat:

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

```
C:\Users\Roland\DQ1Q17\fa>cd..

C:\Users\Roland\DQ1Q17>dir
Volume in drive C is Boot
Volume Serial Number is 5414-9A70

Directory of C:\Users\Roland\DQ1Q17

2022.02.16.  12:39    <DIR>          .
2022.02.16.  12:39    <DIR>          ..
2022.02.16.  12:36    <DIR>          bokor
2022.02.16.  12:57    <DIR>          fa
               0 File(s)                0 bytes
               4 Dir(s)  15 311 863 808 bytes free

C:\Users\Roland\DQ1Q17>
```

1.feladat:

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

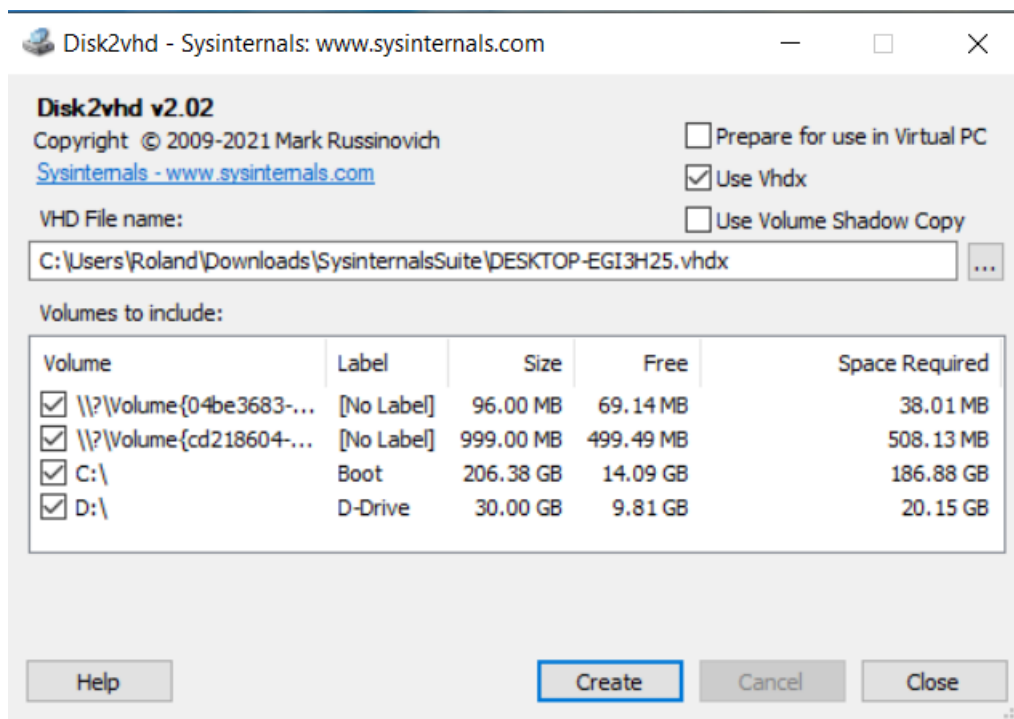
```
C:\Users\Roland\DQ1Q17\fa>sort felsorlas.txt /o felsorlas.txt
```

```
C:\Users\Roland\DQ1Q17\fa>
```

2.feladat:

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

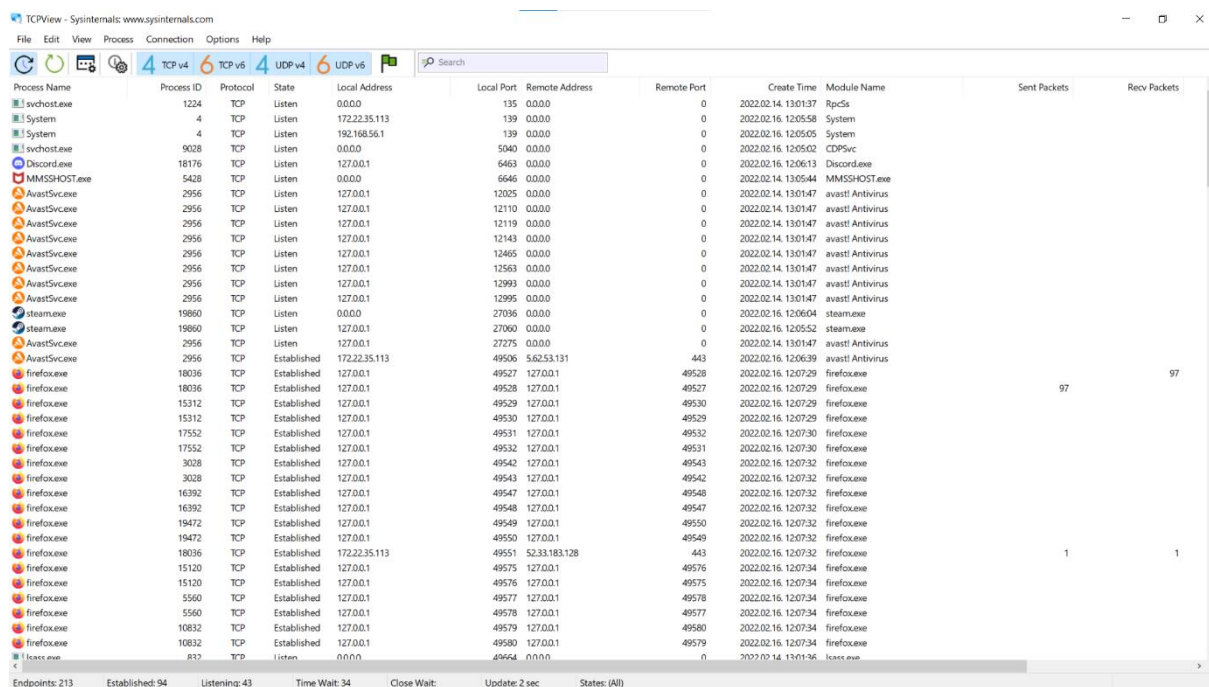
a) File and Disk Utilities (Disk2vhd)



A Disk2vhd egy olyan segédprogram, amely létrehozza a fizikai lemezek VHD-változatait (Virtual Hard Disk – Microsoft Virtual Machine lemezformátuma) Microsoft Virtual PC-ben vagy Microsoft Hyper-V virtuális gépekben (VM-ekben) való használatra[1]

2.feladat

b) Networking Utilities (TCPView)



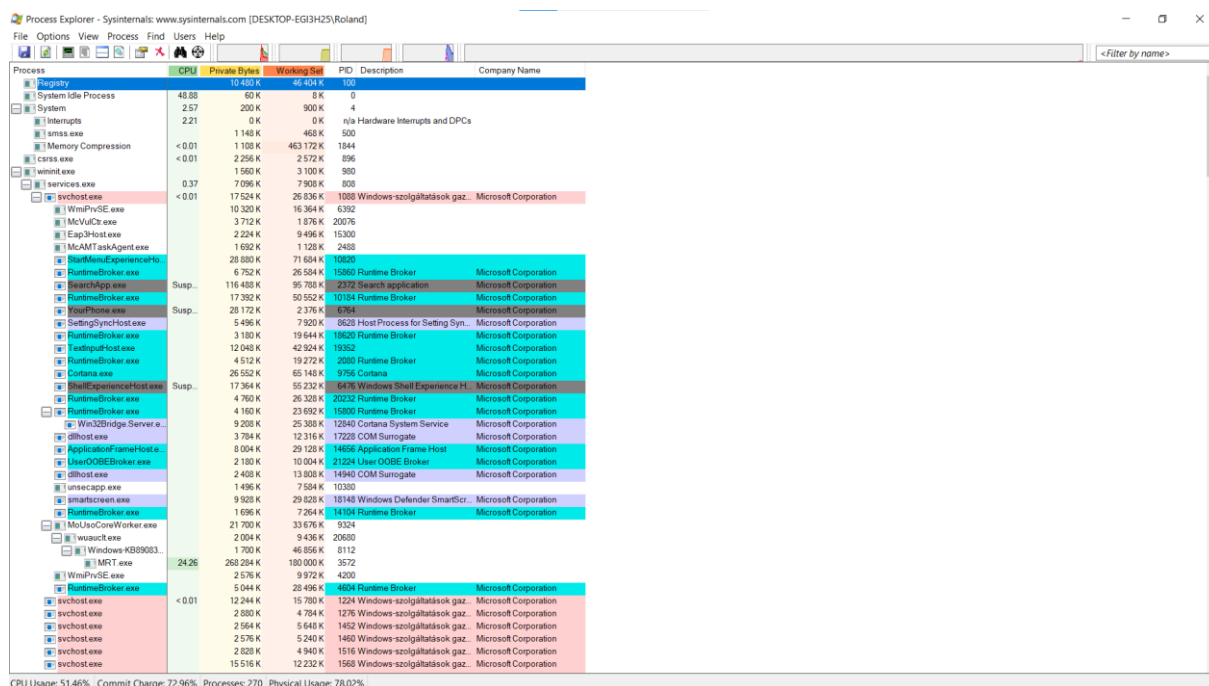
The screenshot shows the TCPView application window. The title bar reads 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes File, Edit, View, Process, Connection, Options, and Help. The toolbar has icons for refreshing, pausing, and other functions. Below the toolbar, there are tabs for TCP v4, TCP v6, UDP v4, and UDP v6, with a search bar. The main table displays network connections with columns: Process Name, Process ID, Protocol, State, Local Address, Local Port, Remote Address, Remote Port, Create Time, Module Name, Sent Packets, and Recv Packets. The table lists various processes like svchost.exe, System, and several instances of AvastSvc.exe and Firefox.exe. At the bottom, a status bar shows statistics: Endpoints: 213, Established: 94, Listening: 43, Time Wait: 34, Close Wait: , Update: 2 sec, States: (All).

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets	Recv Packets
svchost.exe	1224	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2022.02.14. 13:01:37	RpcSs		
System	4	TCP	Listen	172.22.35.113	139	0.0.0.0	0	2022.02.16. 12:05:58	System		
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	2022.02.16. 12:05:05	System		
svchost.exe	9028	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2022.02.16. 12:05:02	CDPSvc		
Discord.exe	18176	TCP	Listen	127.0.0.1	6463	0.0.0.0	0	2022.02.16. 12:06:13	Discord.exe		
MMSSHST.exe	5428	TCP	Listen	0.0.0.0	6646	0.0.0.0	0	2022.02.14. 13:05:44	MMSSHST.exe		
AvastSvc.exe	2956	TCP	Listen	127.0.0.1	12025	0.0.0.0	0	2022.02.14. 13:01:47	avast! Antivirus		
AvastSvc.exe	2956	TCP	Listen	127.0.0.1	12110	0.0.0.0	0	2022.02.14. 13:01:47	avast! Antivirus		
AvastSvc.exe	2956	TCP	Listen	127.0.0.1	12119	0.0.0.0	0	2022.02.14. 13:01:47	avast! Antivirus		
AvastSvc.exe	2956	TCP	Listen	127.0.0.1	12143	0.0.0.0	0	2022.02.14. 13:01:47	avast! Antivirus		
AvastSvc.exe	2956	TCP	Listen	127.0.0.1	12465	0.0.0.0	0	2022.02.14. 13:01:47	avast! Antivirus		
AvastSvc.exe	2956	TCP	Listen	127.0.0.1	12563	0.0.0.0	0	2022.02.14. 13:01:47	avast! Antivirus		
AvastSvc.exe	2956	TCP	Listen	127.0.0.1	12993	0.0.0.0	0	2022.02.14. 13:01:47	avast! Antivirus		
AvastSvc.exe	2956	TCP	Listen	127.0.0.1	12995	0.0.0.0	0	2022.02.14. 13:01:47	avast! Antivirus		
steam.exe	19860	TCP	Listen	0.0.0.0	27086	0.0.0.0	0	2022.02.16. 12:06:04	steam.exe		
steam.exe	19860	TCP	Listen	127.0.0.1	27060	0.0.0.0	0	2022.02.16. 12:05:52	steam.exe		
AvastSvc.exe	2956	TCP	Listen	127.0.0.1	27275	0.0.0.0	0	2022.02.14. 13:01:47	avast! Antivirus		
AvastSvc.exe	2956	TCP	Established	172.22.35.113	49506	562.53.131	443	2022.02.16. 12:06:39	avast! Antivirus		
Firefox.exe	18036	TCP	Established	127.0.0.1	49527	127.0.0.1	49528	2022.02.16. 12:07:29	Firefox.exe		97
Firefox.exe	18036	TCP	Established	127.0.0.1	49528	127.0.0.1	49527	2022.02.16. 12:07:29	Firefox.exe	97	
Firefox.exe	15312	TCP	Established	127.0.0.1	49529	127.0.0.1	49530	2022.02.16. 12:07:29	Firefox.exe		
Firefox.exe	15312	TCP	Established	127.0.0.1	49530	127.0.0.1	49529	2022.02.16. 12:07:29	Firefox.exe		
Firefox.exe	17552	TCP	Established	127.0.0.1	49531	127.0.0.1	49532	2022.02.16. 12:07:30	Firefox.exe		
Firefox.exe	17552	TCP	Established	127.0.0.1	49532	127.0.0.1	49531	2022.02.16. 12:07:30	Firefox.exe		
Firefox.exe	3028	TCP	Established	127.0.0.1	49542	127.0.0.1	49543	2022.02.16. 12:07:32	Firefox.exe		
Firefox.exe	3028	TCP	Established	127.0.0.1	49543	127.0.0.1	49542	2022.02.16. 12:07:32	Firefox.exe		
Firefox.exe	16392	TCP	Established	127.0.0.1	49547	127.0.0.1	49548	2022.02.16. 12:07:32	Firefox.exe		
Firefox.exe	16392	TCP	Established	127.0.0.1	49548	127.0.0.1	49547	2022.02.16. 12:07:32	Firefox.exe		
Firefox.exe	19472	TCP	Established	127.0.0.1	49549	127.0.0.1	49550	2022.02.16. 12:07:32	Firefox.exe		
Firefox.exe	19472	TCP	Established	127.0.0.1	49550	127.0.0.1	49549	2022.02.16. 12:07:32	Firefox.exe		
Firefox.exe	18036	TCP	Established	172.22.35.113	49551	52.83.183.128	443	2022.02.16. 12:07:32	Firefox.exe	1	1
Firefox.exe	15120	TCP	Established	127.0.0.1	49575	127.0.0.1	49576	2022.02.16. 12:07:34	Firefox.exe		
Firefox.exe	15120	TCP	Established	127.0.0.1	49576	127.0.0.1	49575	2022.02.16. 12:07:34	Firefox.exe		
Firefox.exe	5560	TCP	Established	127.0.0.1	49577	127.0.0.1	49578	2022.02.16. 12:07:34	Firefox.exe		
Firefox.exe	5560	TCP	Established	127.0.0.1	49578	127.0.0.1	49577	2022.02.16. 12:07:34	Firefox.exe		
Firefox.exe	10832	TCP	Established	127.0.0.1	49579	127.0.0.1	49580	2022.02.16. 12:07:34	Firefox.exe		
Firefox.exe	10832	TCP	Established	127.0.0.1	49580	127.0.0.1	49579	2022.02.16. 12:07:34	Firefox.exe		
lsass.exe	832	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2022.02.14. 13:01:36	lsass.exe		

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 Windows Server 2008, Vista és XP rendszeren a TCPView a végpont tulajdonában található folyamat nevét is jelenti. A TCPView a Netstat program egy informatívabb és kényelmesebben bemutatott részkészletét biztosítja, amely a Windows. A TCPView-letöltés tartalmazza a Tcpsvcon parancssori verziót, amely ugyanazokkal a funkciókkal rendelkezik[2].

2.feladat

c) Process Explorer



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-EG3H25/Roland]

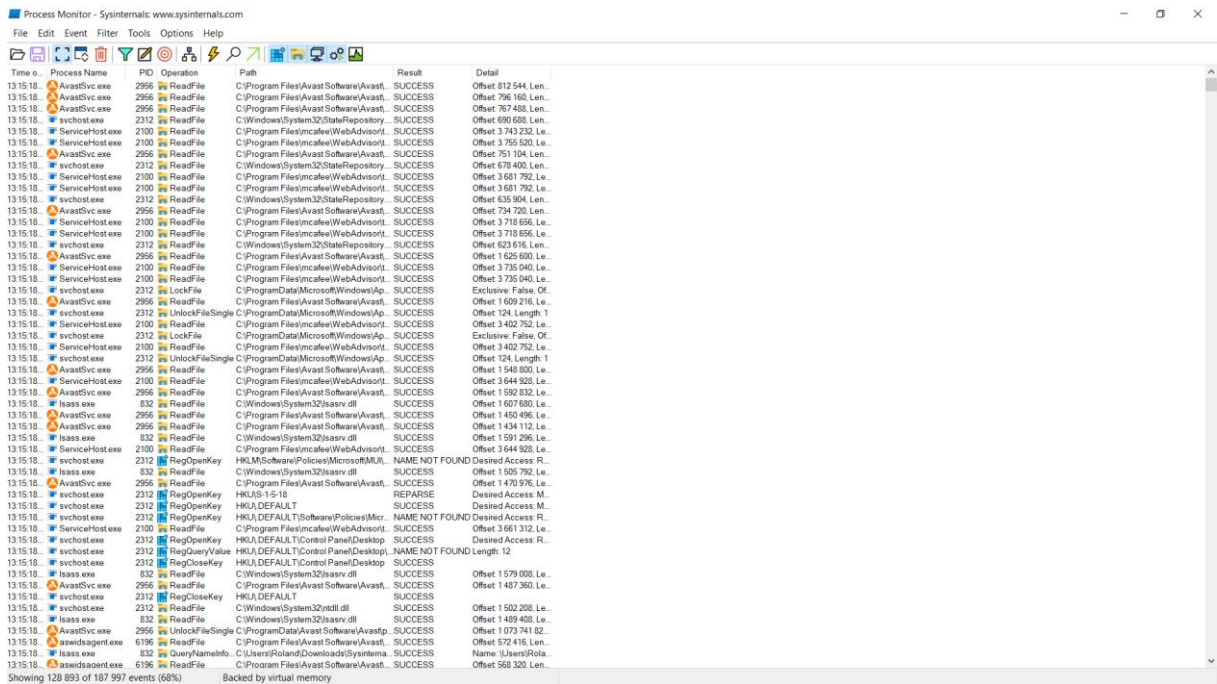
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		10 480 K	46 404 K	100		
System Idle Process	48.88	60 K	8 K	0		
System	2.57	200 K	900 K	4		
smss.exe		1 148 K	468 K	500		
Memory Compression	< 0.01	1 108 K	463 172 K	1844		
csrss.exe	< 0.01	2 256 K	2 572 K	896		
svchost.exe		1 560 K	3 100 K	980		
services.exe	0.37	7 096 K	7 908 K	808		
svchost.exe	< 0.01	17 524 K	26 836 K	1088	Windows szolgáltatások gaz.	Microsoft Corporation
WmiPrvSE.exe		10 320 K	16 364 K	6392		
McVc2.exe		3 712 K	1 876 K	20076		
EsapHost.exe		2 224 K	9 496 K	15300		
McAMTaskAgent.exe		1 682 K	1 128 K	2488		
StartMenuExperienceHost.exe		28 880 K	71 684 K	10020		
RuntimeBroker.exe		6 752 K	26 584 K	15860	Runtime Broker	Microsoft Corporation
SearchIndexing.exe	Susp.	116 488 K	95 788 K	2212	Search application	Microsoft Corporation
RuntimeBroker.exe		17 382 K	50 552 K	10184	Runtime Broker	Microsoft Corporation
YotaPhone.exe	Susp.	28 172 K	2 376 K	6764		Microsoft Corporation
SettingsSyncHost.exe		5 496 K	7 920 K	8628	Host Process for Setting Syn...	Microsoft Corporation
RuntimeBroker.exe		3 180 K	19 644 K	18620	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		12 048 K	42 924 K	19352		Microsoft Corporation
RuntimeBroker.exe		4 512 K	19 272 K	2080	Runtime Broker	Microsoft Corporation
Cortana.exe		26 552 K	65 148 K	9756	Cortana	Microsoft Corporation
ShellExperienceHost.exe	Susp.	17 364 K	55 232 K	6476	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		4 768 K	26 328 K	20232	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		4 160 K	23 692 K	15900	Runtime Broker	Microsoft Corporation
Win32BridgeServer.exe		9 208 K	25 388 K	12940	Cortana System Service	Microsoft Corporation
dllhost.exe		3 784 K	12 316 K	17228	COM Surrogate	Microsoft Corporation
ApplicationFrameHost.exe		8 004 K	29 128 K	14656	Application Frame Host	Microsoft Corporation
UserOSD.exe		2 180 K	10 004 K	21224	User OSDE Broker	Microsoft Corporation
dllhost.exe		2 408 K	13 808 K	14940	COM Surrogate	Microsoft Corporation
unsecapp.exe		1 486 K	7 584 K	10380		
smartscreen.exe		9 920 K	29 828 K	18148	Windows Defender SmartScr...	Microsoft Corporation
RuntimeBroker.exe		1 696 K	7 254 K	14104	Runtime Broker	Microsoft Corporation
MsUserCovWorker.exe		21 700 K	33 676 K	9324		
wscntcl.exe		2 004 K	9 436 K	20680		
Windows KB890803...		1 700 K	46 856 K	8112		
MRT.exe	24.26	268 284 K	180 000 K	3572		
WmiPrvSE.exe		2 576 K	9 972 K	4280		
RuntimeBroker.exe		5 044 K	26 496 K	4604	Runtime Broker	Microsoft Corporation
svchost.exe	< 0.01	12 244 K	15 780 K	1224	Windows szolgáltatások gaz.	Microsoft Corporation
svchost.exe		2 880 K	4 784 K	1276	Windows szolgáltatások gaz.	Microsoft Corporation
svchost.exe		2 564 K	5 648 K	1462	Windows szolgáltatások gaz.	Microsoft Corporation
svchost.exe		2 576 K	5 240 K	1460	Windows szolgáltatások gaz.	Microsoft Corporation
svchost.exe		2 820 K	4 940 K	1516	Windows szolgáltatások gaz.	Microsoft Corporation
svchost.exe		15 516 K	12 232 K	1568	Windows szolgáltatások gaz.	Microsoft Corporation

CPU Usage: 51.46% Commit Charge: 72.96% Processes: 270 Physical Usage: 78.02%

A *Process Explorer* információkat jelenít meg arról, hogy mely leírók és DLL-ek folyamatai nyitottak vagy betöltöttek. A felső ablakban mindig megjelenik az aktuálisan aktív folyamatok listája, beleértve a tulajdonos fiókjaik nevét is, míg az alsó ablakban megjelenő információ attól függ, hogy a *Process Explorer* milyen módban van: ha kezelő módban van, akkor a kezelő, hogy a felső ablakban kiválasztott folyamat megnyílt; ha a *Process Explorer* DLL módban van, látni fogja a folyamat által betöltött DLL-eket és memórialékepezett fájlokat. A *Process Explorer* hatékony keresési funkcióval is rendelkezik, amely gyorsan megmutatja, hogy mely folyamatokban van megnyitva adott leíró vagy DLL-ek betöltve.[3]

2.feladat

c) Process Monitor

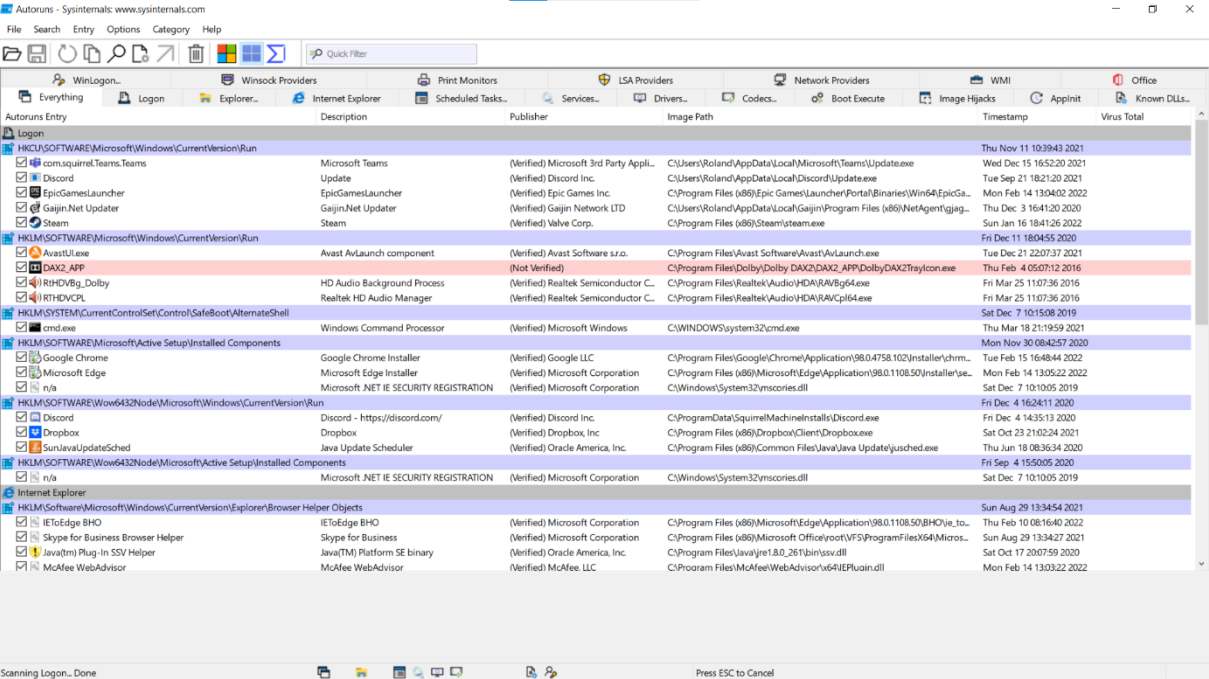


Time	Process Name	PID	Operation	Path	Result	Detail
13:15:18	AvastSvc.exe	2956	ReadFile	C:\Program Files\Avast Software\Avast\	SUCCESS	Offset 812 544, Len...
13:15:18	AvastSvc.exe	2956	ReadFile	C:\Program Files\Avast Software\Avast\	SUCCESS	Offset 796 160, Len...
13:15:18	AvastSvc.exe	2956	ReadFile	C:\Program Files\Avast Software\Avast\	SUCCESS	Offset 767 480, Len...
13:15:18	svchost.exe	2312	ReadFile	C:\Windows\System32\StateRepository\	SUCCESS	Offset 690 680, Len...
13:15:18	ServiceHost.exe	2100	ReadFile	C:\Program Files\incalweb\WebAdvisor\	SUCCESS	Offset 3 743 232, Le...
13:15:18	ServiceHost.exe	2100	ReadFile	C:\Program Files\incalweb\WebAdvisor\	SUCCESS	Offset 3 755 520, Le...
13:15:18	AvastSvc.exe	2956	ReadFile	C:\Program Files\Avast Software\Avast\	SUCCESS	Offset 751 104, Len...
13:15:18	svchost.exe	2312	ReadFile	C:\Windows\System32\StateRepository\	SUCCESS	Offset 678 400, Len...
13:15:18	ServiceHost.exe	2100	ReadFile	C:\Program Files\incalweb\WebAdvisor\	SUCCESS	Offset 3 681 792, Le...
13:15:18	ServiceHost.exe	2100	ReadFile	C:\Program Files\incalweb\WebAdvisor\	SUCCESS	Offset 3 681 792, Le...
13:15:18	svchost.exe	2312	ReadFile	C:\Windows\System32\StateRepository\	SUCCESS	Offset 635 904, Len...
13:15:18	AvastSvc.exe	2956	ReadFile	C:\Program Files\Avast Software\Avast\	SUCCESS	Offset 734 720, Len...
13:15:18	ServiceHost.exe	2100	ReadFile	C:\Program Files\incalweb\WebAdvisor\	SUCCESS	Offset 3 718 856, Le...
13:15:18	ServiceHost.exe	2100	ReadFile	C:\Program Files\incalweb\WebAdvisor\	SUCCESS	Offset 3 718 856, Le...
13:15:18	svchost.exe	2312	ReadFile	C:\Windows\System32\StateRepository\	SUCCESS	Offset 623 616, Len...
13:15:18	AvastSvc.exe	2956	ReadFile	C:\Program Files\Avast Software\Avast\	SUCCESS	Offset 1 625 600, Le...
13:15:18	ServiceHost.exe	2100	ReadFile	C:\Program Files\incalweb\WebAdvisor\	SUCCESS	Offset 3 735 040, Le...
13:15:18	ServiceHost.exe	2100	ReadFile	C:\Program Files\incalweb\WebAdvisor\	SUCCESS	Offset 3 735 040, Le...
13:15:18	svchost.exe	2312	LockFile	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Exclusive False, Of...
13:15:18	AvastSvc.exe	2956	ReadFile	C:\Program Files\Avast Software\Avast\	SUCCESS	Offset 1 609 216, Le...
13:15:18	svchost.exe	2312	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Offset 124, Length 1
13:15:18	ServiceHost.exe	2100	ReadFile	C:\Program Files\incalweb\WebAdvisor\	SUCCESS	Offset 3 402 752, Le...
13:15:18	svchost.exe	2312	LockFile	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Exclusive False, Of...
13:15:18	ServiceHost.exe	2100	ReadFile	C:\Program Files\incalweb\WebAdvisor\	SUCCESS	Offset 3 402 752, Le...
13:15:18	svchost.exe	2312	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Offset 124, Length 1
13:15:18	AvastSvc.exe	2956	ReadFile	C:\Program Files\Avast Software\Avast\	SUCCESS	Offset 1 540 800, Le...
13:15:18	ServiceHost.exe	2100	ReadFile	C:\Program Files\incalweb\WebAdvisor\	SUCCESS	Offset 3 544 928, Le...
13:15:18	AvastSvc.exe	2956	ReadFile	C:\Program Files\Avast Software\Avast\	SUCCESS	Offset 1 592 832, Le...
13:15:18	lsass.exe	832	ReadFile	C:\Windows\System32\lsassrv.dll	SUCCESS	Offset 1 607 680, Le...
13:15:18	AvastSvc.exe	2956	ReadFile	C:\Program Files\Avast Software\Avast\	SUCCESS	Offset 1 450 496, Le...
13:15:18	AvastSvc.exe	2956	ReadFile	C:\Program Files\Avast Software\Avast\	SUCCESS	Offset 1 434 112, Le...
13:15:18	lsass.exe	832	ReadFile	C:\Windows\System32\lsassrv.dll	SUCCESS	Offset 1 591 296, Le...
13:15:18	ServiceHost.exe	2100	ReadFile	C:\Program Files\incalweb\WebAdvisor\	SUCCESS	Offset 3 644 928, Le...
13:15:18	svchost.exe	2312	RegOpenKey	HKLM\Software\Policies\Microsoft\B...	NAME NOT FOUND	Desired Access: R...
13:15:18	lsass.exe	832	ReadFile	C:\Windows\System32\lsassrv.dll	SUCCESS	Offset 1 505 792, Le...
13:15:18	AvastSvc.exe	2956	ReadFile	C:\Program Files\Avast Software\Avast\	SUCCESS	Offset 1 470 976, Le...
13:15:18	svchost.exe	2312	RegOpenKey	HKU\S-1-5-18	REPARSE	Desired Access: M...
13:15:18	svchost.exe	2312	RegOpenKey	HKU\DEFAULT	SUCCESS	Desired Access: M...
13:15:18	svchost.exe	2312	RegOpenKey	HKU\DEFAULT\Software\Policies\Micr...	NAME NOT FOUND	Desired Access: R...
13:15:18	ServiceHost.exe	2100	ReadFile	C:\Program Files\incalweb\WebAdvisor\	SUCCESS	Offset 3 661 312, Le...
13:15:18	svchost.exe	2312	RegOpenKey	HKU\DEFAULT\Control Panel\Desktop	SUCCESS	Desired Access: R...
13:15:18	svchost.exe	2312	RegQueryValue	HKU\DEFAULT\Control Panel\Desktop	NAME NOT FOUND	Length: 12
13:15:18	svchost.exe	2312	RegCloseKey	HKU\DEFAULT\Control Panel\Desktop	SUCCESS	
13:15:18	lsass.exe	832	ReadFile	C:\Windows\System32\lsassrv.dll	SUCCESS	Offset 1 579 008, Le...
13:15:18	AvastSvc.exe	2956	ReadFile	C:\Program Files\Avast Software\Avast\	SUCCESS	Offset 1 457 360, Le...
13:15:18	svchost.exe	2312	RegCloseKey	HKU\DEFAULT	SUCCESS	
13:15:18	svchost.exe	2312	ReadFile	C:\Windows\System32\ntdll.dll	SUCCESS	Offset 1 502 208, Le...
13:15:18	lsass.exe	832	ReadFile	C:\Windows\System32\lsassrv.dll	SUCCESS	Offset 1 480 480, Le...
13:15:18	AvastSvc.exe	2956	UnlockFileSingle	C:\ProgramData\Avast Software\Avast\	SUCCESS	Offset 1 073 744, Le...
13:15:18	avastagent.exe	6196	ReadFile	C:\Program Files\Avast Software\Avast\	SUCCESS	Offset 572 416, Len...
13:15:18	lsass.exe	832	QueryNameInfo	C:\Users\Roland\Downloads\System...	SUCCESS	Name: \lsass\Root...
13:15:18	avastagent.exe	6196	ReadFile	C:\Program Files\Avast Software\Avast\	SUCCESS	Offset 568 320, Len...

A Folyamatfigyelő egy fejlett monitorozási eszköz Windows, amely valós idejű fájlrendszer-, beállításjegyzék- és folyamat-/száltevékenységet mutat be. Kombinálja két örökölt Sysinternals segédprogram, a *Filemon* és a *Regmon* funkcióit, és számos fejlesztést tartalmaz, többek között gazdag és nem kipusztító szűrést, átfogó eseménytulajdonságokat, például munkamenet-azonosítókat és felhasználóneveket, megbízható folyamatinformációkat, teljes szálkészleteket az egyes műveletek integrált szimbólumtámogatásával, a fájlba történő egyidejű naplózást. Egyedi funkciókkal a Folyamatfigyelő a rendszer hibaelhárítási és kártevőkeresési eszközkészletének egyik alapvető segédprogramja lesz.

2.feladat

c) AutoRuns

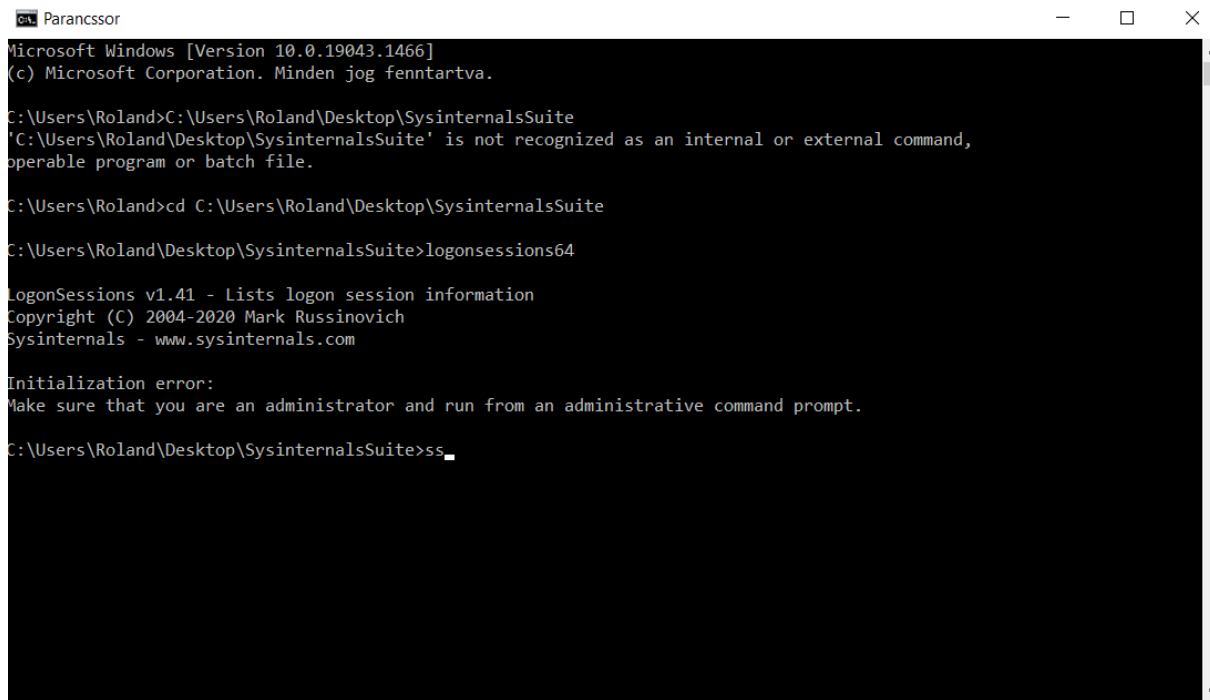


Name	Description	Publisher	Image Path	Timestamp
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Thu Nov 11 10:39:43 2021
com.squirrel.Teams.Teams	Microsoft Teams	(Verified) Microsoft 3rd Party Appli..	C:\Users\Roland\AppData\Local\Microsoft\Teams\Update.exe	Wed Dec 15 16:52:20 2021
Discord	Update	(Verified) Discord Inc.	C:\Users\Roland\AppData\Local\Discord\Update.exe	Tue Sep 21 18:21:20 2021
EpicGamesLauncher	EpicGamesLauncher	(Verified) Epic Games Inc.	C:\Program Files (x86)\Epic Games\Launcher\Portal\Binaries\Win64\EpicGa..	Mon Feb 14 13:04:02 2022
Gajjin.Net Updater	Gajjin.Net Updater	(Verified) Gajjin Network LTD	C:\Users\Roland\AppData\Local\Gajjin\Program Files (x86)\NetAgent\gajg..	Thu Dec 3 16:41:20 2020
Steam	Steam	(Verified) Valve Corp.	C:\Program Files (x86)\Steam\steam.exe	Sun Jan 16 18:41:26 2022
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Fri Dec 11 18:04:55 2020
Avast!Launch	Avast!Launch component	(Verified) Avast Software s.r.o.	C:\Program Files\Avast\Software\Avast\AvLaunch.exe	Tue Dec 21 22:07:37 2021
DAX2_APP	(Not Verified)	(Not Verified)	C:\Program Files\Realtek\Audio\HDA\RAVb64.exe	Thu Feb 4 05:07:12 2016
HD Audio Background Process	Realtek HD Audio Manager	(Verified) Realtek Semiconductor C..	C:\Program Files\Realtek\Audio\HDA\RAVb64.exe	Fri Mar 25 11:07:36 2016
IRTHDEVCL	Realtek HD Audio Manager	(Verified) Realtek Semiconductor C..	C:\Program Files\Realtek\Audio\HDA\RAVb64.exe	Fri Mar 25 11:07:36 2016
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Sat Dec 7 10:15:08 2019
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				Thu Mar 18 21:19:59 2021
Google Chrome	Google Chrome Installer	(Verified) Google LLC	C:\Program Files\Google\Chrome\Application\98.0.4758.102\Installer\chrm..	Mon Nov 30 08:42:57 2020
Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\98.0.1108.50\Installer\se..	Tue Feb 15 16:48:44 2022
n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Mon Feb 14 13:05:22 2022
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				Sat Dec 7 10:10:05 2019
Discord	Discord - https://discord.com/	(Verified) Discord Inc.	C:\ProgramData\SquirrelMachine\installs\Discord.exe	Fri Dec 4 14:35:13 2020
Dropbox	Dropbox	(Verified) Dropbox, Inc.	C:\Program Files (x86)\Dropbox\Client\Dropbox.exe	Sat Oct 23 21:02:24 2021
SunJavaUpdateSched	Java Update Scheduler	(Verified) Oracle America, Inc.	C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	Thu Jun 18 08:36:34 2020
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				Fri Sep 4 15:50:05 2020
n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Sat Dec 7 10:10:05 2019
Internet Explorer				Sat Dec 7 10:10:05 2019
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				Sun Aug 29 13:34:54 2021
IEToEdge BHO	IEToEdge BHO	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\98.0.1108.50\BHO\Ie_to..	Thu Feb 10 08:16:40 2022
Skype for Business Browser Helper	Skype for Business	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft Office\root\VF9\ProgramFiles\X64\Micros..	Sun Aug 29 13:34:27 2021
Java(TM) Plug-In SSV Helper	Java(TM) Platform SE binary	(Verified) Oracle America, Inc.	C:\Program Files\Java\jre1.8.0_261\bin\ssv.dll	Sat Oct 17 20:07:59 2020
McAfee WebAdvisor	McAfee WebAdvisor	(Verified) McAfee, LLC	C:\Program Files\McAfee\WebAdvisor\sv64\IEPlugin.dll	Mon Feb 14 13:03:22 2022

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



```
Parancssor
Microsoft Windows [Version 10.0.19043.1466]
(c) Microsoft Corporation. Minden jog fenntartva.

C:\Users\Roland>C:\Users\Roland\Desktop\SysinternalsSuite
'C:\Users\Roland\Desktop\SysinternalsSuite' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Roland>cd C:\Users\Roland\Desktop\SysinternalsSuite

C:\Users\Roland\Desktop\SysinternalsSuite>logonsessions64

LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

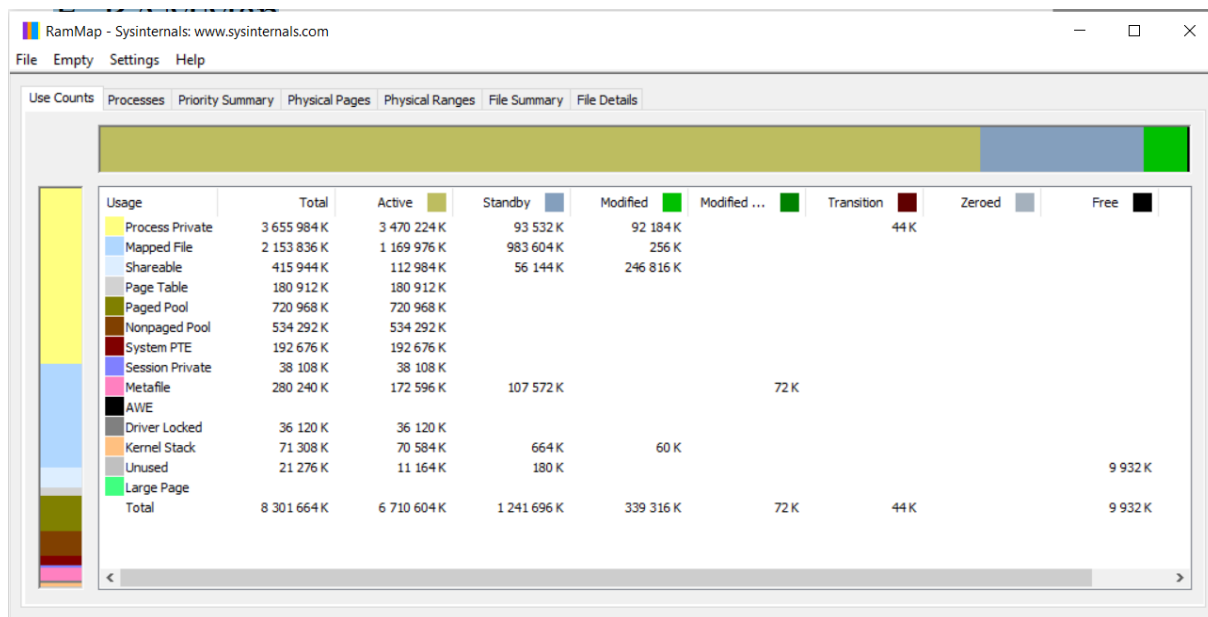
Initialization error:
Make sure that you are an administrator and run from an administrative command prompt.

C:\Users\Roland\Desktop\SysinternalsSuite>ss_
```

A LogonSessions segédprogram felsorolja a helyi biztonsági hatóság (LSA) által létrehozott és kezelt aktív bejelentkezési munkameneteket. A bejelentkezési munkamenet akkor jön létre, amikor egy felhasználói fiókot vagy szolgáltatásfiókot hitelesítenek a Windows rendszerben. A hitelesítés sokféleképpen történhet.

2.feladat

e) RAMMap



A RAMMap megkönnyíti ezekre a kérdésekre a választ. A RAMMap egy fejlett fizikai memóriahasználat-elemző segédprogram Windows Vista és újabb verziókhoz. Különbőféle módon jeleníti meg a használati információkat több különböző lapján:

Használati számok: a használat összegzése típus és lapozási lista szerint

Folyamat: folyamat munkakészlet méretek

Prioritásösszegzés: prioritásos készenléti listaméretek

Fizikai oldalak: oldalankénti használat az összes fizikai memória számára

Fizikai tartományok: fizikai memóriacímek

Fájlösszegzés: a RAM-ban lévő fájladatok fájlonként

Fájl részletei: egyes fizikai oldalak fájlonként

A RAMMap segítségével megértheti, hogyan kezeli a Windows memóriát, elemezze az alkalmazások memóriahasználatát, vagy válaszoljon a RAM lefoglalásával kapcsolatos konkrét kérdésekre. A RAMMap frissítési funkciója lehetővé teszi a kijelző frissítését, és támogatja a memória pillanatképeinek mentését és betöltését.

3.feladat:

C programkód

```
C:\Users\Roland\Desktop\Progyak\neptunkod\bin\Debug\neptunkod.exe
Vezeteknev : Sarosi
Keresztnev : Bence
Szak : GUI
Neptunkod : WX3RG6

Hallgato azonosito : 2
Vezeteknev : Kiss
Keresztnev : Katoka
Szak : GDE
Neptunkod : BL2YX1

Hallgato azonosito : 3
Vezeteknev : Nemoda
Keresztnev : Buda
Szak : VIL
Neptunkod : LAQ1GH

Nem sikerült megnyitni a fájlt: Permission denied

Kerem a fájl nevet (vezeteknev.txt) : sarosi.txt

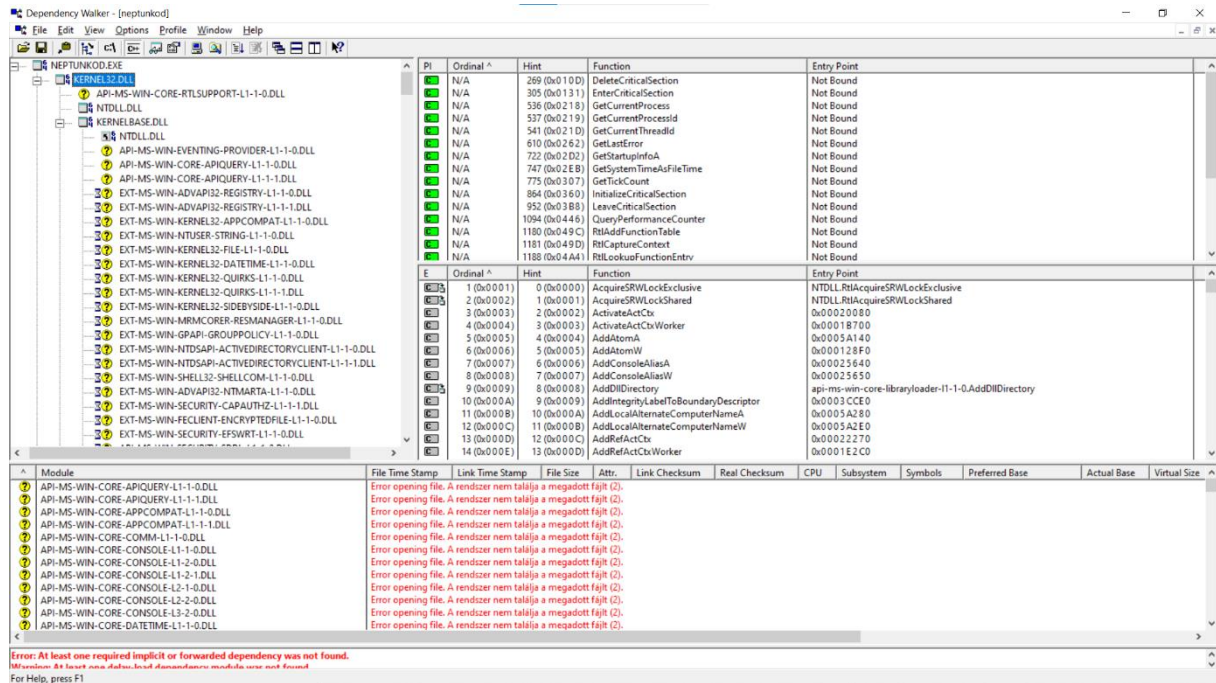
1. 1 Sarosi Bence GUI WX3RG6
2. 2 Kiss Katoka GDE BL2YX1
3. 3 Nemoda Buda VIL LAQ1GH

Process returned 0 (0x0)   execution time : 12.211 s
Press any key to continue.
```

```
sarosi - Jegyzetömb
Fájl Szerkesztés Formátum Nézet Súgó
1 Sarosi Bence GUI WX3RG6
2 Kiss Katoka GDE BL2YX1
3 Nemoda Buda VIL LAQ1GH
```

3.feladat:

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



The screenshot shows the Dependency Walker (NEPTUNKOD.EXE) window. The left pane lists the loaded DLLs, including kernel32.dll. The right pane shows the list of imported functions from kernel32.dll. The bottom pane shows the list of imported modules, including API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL, API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL, API-MS-WIN-CORE-COMM-L1-1-0.DLL, API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL, API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL, API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL, API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL, API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL, and API-MS-WIN-CORE-DATETIME-L1-1-0.DLL. The bottom status bar indicates an error: "Error: At least one required implicit or forwarded dependency was not found. (Warning: At least one data access structure module was not found. For Help, press F1).

PI	Ordinal	Hint	Function	Entry Point
N/A	269 (0x010D)		DeleteCriticalSection	Not Bound
N/A	305 (0x0131)		EnterCriticalSection	Not Bound
N/A	536 (0x0218)		GetCurrentProcess	Not Bound
N/A	537 (0x0219)		GetCurrentProcessId	Not Bound
N/A	541 (0x021D)		GetCurrentThreadId	Not Bound
N/A	610 (0x0262)		GetLastError	Not Bound
N/A	722 (0x02D2)		GetStartupInfoA	Not Bound
N/A	747 (0x02E8)		GetSystemTimeAsFileTime	Not Bound
N/A	775 (0x0307)		GetTickCount	Not Bound
N/A	864 (0x0360)		InitializeCriticalSection	Not Bound
N/A	952 (0x03B8)		LeaveCriticalSection	Not Bound
N/A	1094 (0x0446)		QueryPerformanceCounter	Not Bound
N/A	1180 (0x049C)		RtlAddFunctionTable	Not Bound
N/A	1181 (0x049D)		RtlCaptureContext	Not Bound
N/A	1188 (0x04A4)		RtlLookupFunctionEntry	Not Bound

E	Ordinal	Hint	Function	Entry Point
1	0 (0x0000)		AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
2	1 (0x0001)		AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
3	2 (0x0002)		ActivateActCtx	0x00020080
4	3 (0x0003)		ActivateActCtxWorker	0x0001B700
5	4 (0x0004)		AddAtomA	0x0005A140
6	5 (0x0005)		AddAtomW	0x000128F0
7	6 (0x0006)		AddConsoleAliasA	0x00025640
8	7 (0x0007)		AddConsoleAliasW	0x00025650
9	8 (0x0008)		AddDllDirectory	api-ms-win-core-libraryloader-l1-1-0.AddDllDirectory
10	9 (0x0009)		AddIntegrityLabelToBoundaryDescriptor	0x0003CCE0
11	10 (0x000A)		AddLocalAlternateComputerNameA	0x0005A280
12	11 (0x000B)		AddLocalAlternateComputerNameW	0x0005A2E0
13	12 (0x000C)		AddRefActCtx	0x00022270
14	13 (0x000D)		AddRefActCtxWorker	0x0001E2C0

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. A rendszert nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-COMM-L1-1-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).											
API-MS-WIN-CORE-DATETIME-L1-1-0.DLL	Error opening file. A rendszert nem találja a megadott fájlt (2).											

Error: At least one required implicit or forwarded dependency was not found.
Warning: At least one data access structure module was not found.
For Help, press F1

3.feladat:

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

Dependency Walker - [ntpqunkod]

Module: NTDLL.DLL

Ordinal	Hint	Function	Entry Point
20 (0x0014)	N/A	CsrAllocateCaptureBuffer	Not Bound
21 (0x0015)	N/A	CsrAllocateMessagePointer	Not Bound
23 (0x0017)	N/A	CsrCaptureMessageMultiUnicodeStringsInPlace	Not Bound
24 (0x0018)	N/A	CsrCaptureMessageString	Not Bound
25 (0x001A)	N/A	CsrClientCallServer	Not Bound
28 (0x001C)	N/A	CsrFreeCaptureBuffer	Not Bound
32 (0x0020)	N/A	CsrVerifyRegion	Not Bound
34 (0x0022)	N/A	DbgPrint	Not Bound
35 (0x0023)	N/A	DbgPrintEx	Not Bound
45 (0x002D)	N/A	DbgUiGetThreadDebugObject	Not Bound
46 (0x002E)	N/A	DbgUiIssueRemoteBreakin	Not Bound
57 (0x0039)	N/A	EtwEventEnabled	Not Bound
59 (0x003B)	N/A	EtwEventRegister	Not Bound
61 (0x003D)	N/A	EtwEventUnregister	Not Bound
62 (0x003E)	N/A	EtwEventWrite	Not Bound

Error: At least one required implicit or forwarded dependency was not found.
Warning: At least one data-load dependency module was not found.
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.