

# Operációs rendszerek Bsc

2 Gyak.

2022.02.08

**Készítette:**

Veres Balázs László Bsc

GÉIK

ZKY1YM

## Feladatok

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!

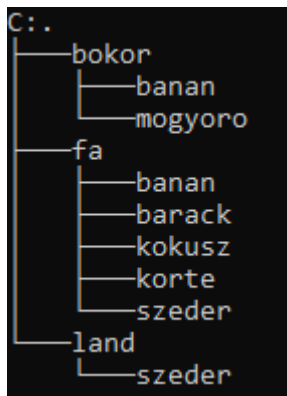
```
C:\Users\veres\Desktop\veres>mkdir bokor  
  
C:\Users\veres\Desktop\veres>cd bokor  
  
C:\Users\veres\Desktop\veres\bokor>mkdir banan  
  
C:\Users\veres\Desktop\veres\bokor>mkdir mogyoro  
  
C:\Users\veres\Desktop\veres\bokor>mkdir barack
```

```
C:.  
├── bokor  
│   ├── banan  
│   ├── barack  
│   └── mogyoro  
├── fa  
│   └── korte  
└── land  
    ├── kokusz  
    └── szeder
```

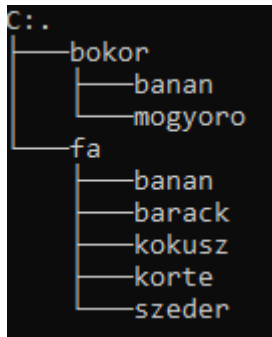
b.) Készítsen másolatot:

```
C:.  
├── bokor  
│   ├── banan  
│   ├── barack  
│   └── mogyoro  
├── fa  
│   ├── banan  
│   ├── korte  
│   └── szeder  
└── land  
    ├── kokusz  
    └── szeder
```

c.) Végezze el a következő áthelyezéseket:



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



e.) A leiras.txt szöveges állományba írjon 3 sort a barackról.

```
C:\Users\veres\Desktop\zky1m\bokor\banan>echo A banán a trópusokon elterjedt és termesztett egyszikű, lágy szárú, bár gyakran fatermetű növények nemzetsége a banánfélék (Musaceae) róluk elnevezett cs aládjában. A világ legmagasabb egyszikű, lágy szárú növénye. > leiras.txt
```

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

```
C:\Users\veres\Desktop\zky1m>dir
Volume in drive C has no label.
Volume Serial Number is 705E-371F

Directory of C:\Users\veres\Desktop\zky1m

2022. 02. 20.  17:38    <DIR>          .
2022. 02. 20.  17:38    <DIR>          ..
2022. 02. 20.  17:22    <DIR>          bokor
2022. 02. 20.  17:23    <DIR>          fa
2022. 02. 20.  17:39    <DIR>          tree
                0 File(s)              0 bytes
                5 Dir(s)  154 249 224 192 bytes free
```

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

```
C:\Users\veres\Desktop\zky1ym>dir ?e*
Volume in drive C has no label.
Volume Serial Number is 705E-371F

Directory of C:\Users\veres\Desktop\zky1ym

File Not Found

C:\Users\veres\Desktop\zky1ym>_
```

Nincs ilyen.

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

```
C:\Users\veres\Desktop\zky1ym>attrib -r C:\Users\veres\Desktop\zky1ym\tree\felsorolas.txt
```

i.) Jelenítse meg, hogy mennyi helyet foglal a merevlemezen a neptunkod mappa az al-mappáival: **216 byte**.

```
C:\Users\veres\Desktop\zky1ym>dir /a/s
Volume in drive C has no label.
Volume Serial Number is 705E-371F

Directory of C:\Users\veres\Desktop\zky1ym

2022. 02. 20. 17:38 <DIR>      .
2022. 02. 20. 17:38 <DIR>      ..
2022. 02. 20. 17:22 <DIR>      bokor
2022. 02. 20. 17:23 <DIR>      fa
2022. 02. 20. 17:39 <DIR>      tree
                        0 File(s)          0 bytes

Directory of C:\Users\veres\Desktop\zky1ym\bokor

2022. 02. 20. 17:22 <DIR>      .
2022. 02. 20. 17:22 <DIR>      ..
2022. 02. 20. 17:35 <DIR>      banan
2022. 02. 20. 17:09 <DIR>      mogyoro
                        0 File(s)          0 bytes

Directory of C:\Users\veres\Desktop\zky1ym\bokor\banan

2022. 02. 20. 17:35 <DIR>      .
2022. 02. 20. 17:35 <DIR>      ..
2022. 02. 20. 17:35          216 leiras.txt
                        1 File(s)        216 bytes

Directory of C:\Users\veres\Desktop\zky1ym\bokor\mogyoro

2022. 02. 20. 17:09 <DIR>      .
2022. 02. 20. 17:09 <DIR>      ..
                        0 File(s)          0 bytes

Directory of C:\Users\veres\Desktop\zky1ym\fa

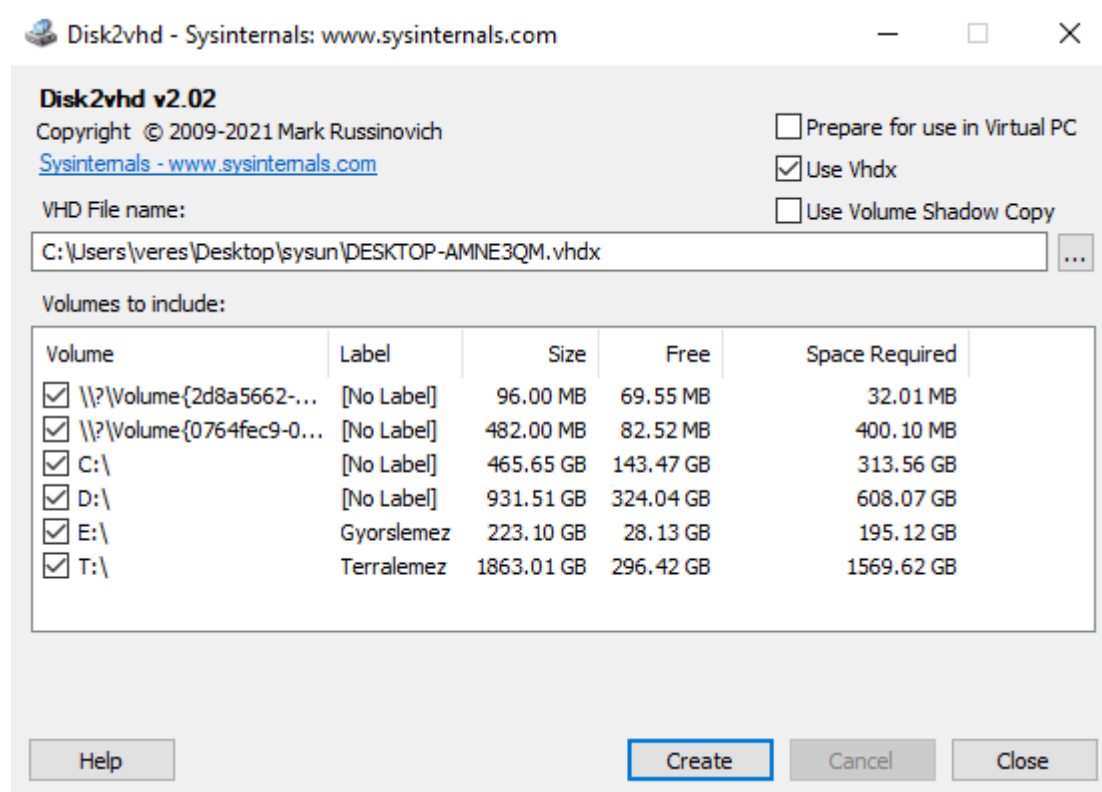
2022. 02. 20. 17:23 <DIR>      .
2022. 02. 20. 17:23 <DIR>      ..
2022. 02. 20. 17:19 <DIR>      banan
```

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

```
C:\Users\veres\Desktop\zky1ym\tree>sort felsorolas.txt
Ferenc
Janos
Kata
Peter
Reka
```

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

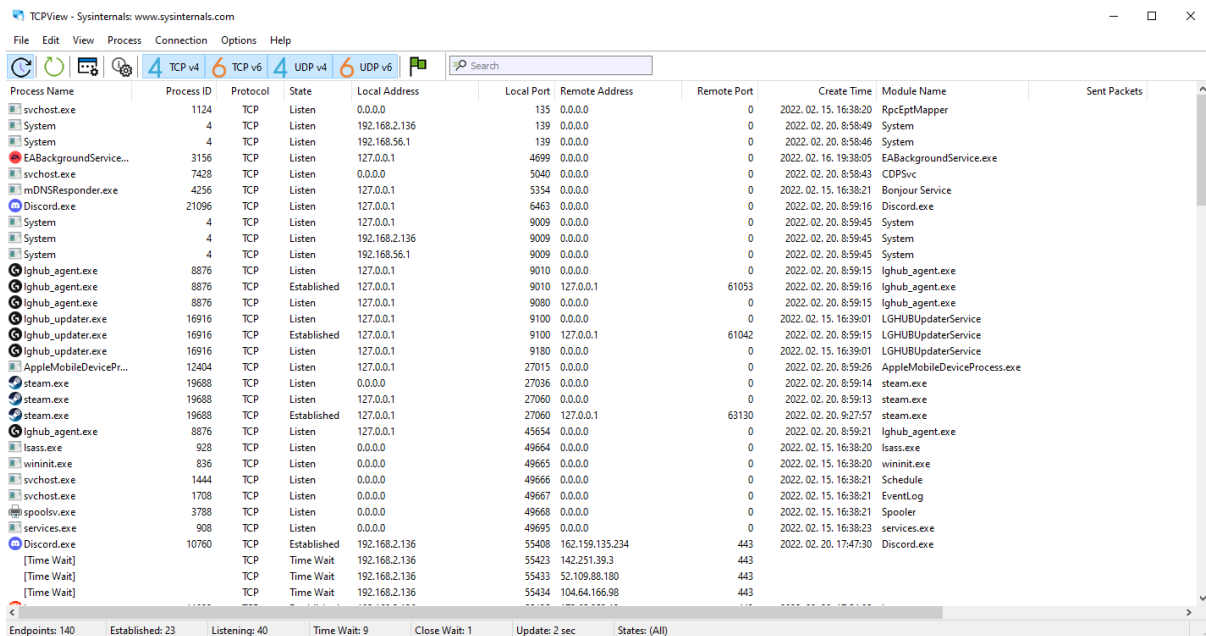
a) File and Disk Utilities (Disk2vhd)



A Disk2vhd egy olyan segédprogram, amely a fizikai lemezek VHD (Virtual Hard Disk - a Microsoft virtuális gépek lemezformátuma) változatait hozza létre a Microsoft Virtual PC vagy Microsoft Hyper-V virtuális gépekben (VM) való használatra. A Disk2vhd és más fizikai-virtuális eszközök között az a különbség, hogy a Disk2vhd-t online rendszerben futtathatja. A Disk2vhd a Windows XP-ben bevezetett Windows Volume Snapshot funkciót használja a konverzióba bevonni kívánt kötetek konzisztens pillanatfelvételeinek létrehozására.

## b) Networking Utilities (TCPView):

A TCPView egy Windows program, amely részletes listát mutat a rendszerében lévő összes TCP és UDP végpontról, beleértve a helyi és távoli címeket és a TCP-kapcsolatok állapotát. A Windows Server 2008, Vista és XP rendszereken a TCPView a végpontot birtokló folyamat nevét is jelzi.



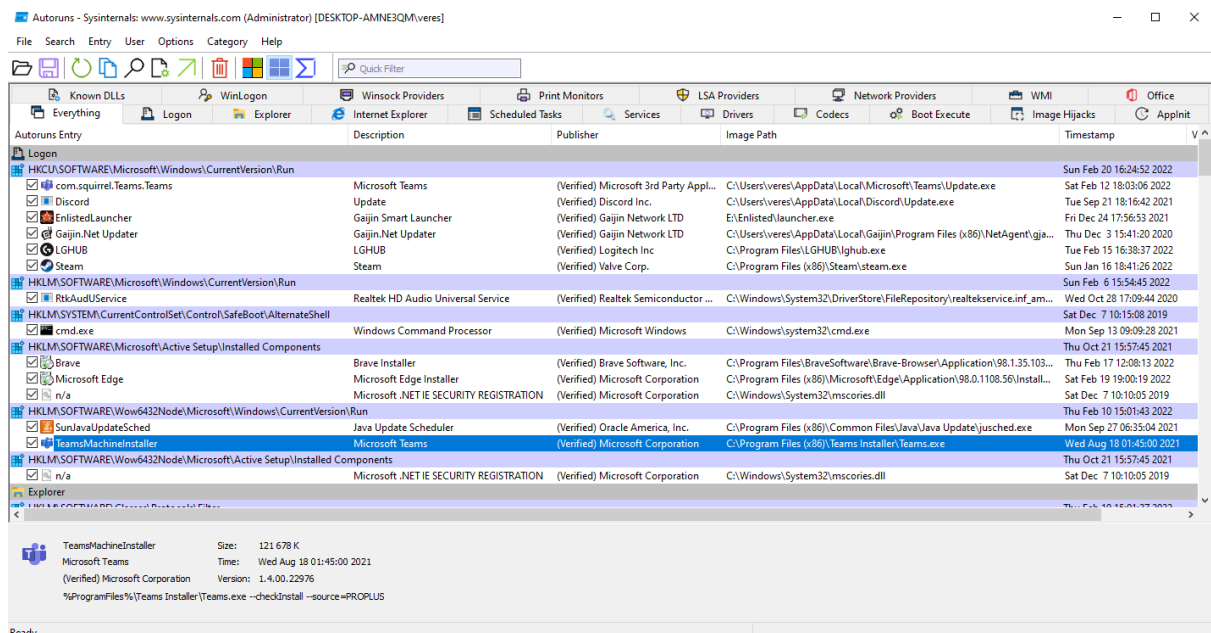
The screenshot shows the TCPView application window. The title bar reads 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes File, Edit, View, Process, Connection, Options, and Help. Below the menu is a toolbar with icons for refreshing, pausing, and other functions. A search bar is present. The main window 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, EABackgroundService..., mDNSResponder.exe, Discord.exe, lghub\_agent.exe, lghub\_updater.exe, AppleMobileDeviceProcess..., steam.exe, wininit.exe, svchost.exe, spoolsv.exe, services.exe, and Discord.exe. The bottom status bar shows statistics: Endpoints: 140, Established: 23, Listening: 40, Time Wait: 9, Close Wait: 1, 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
svchost.exe	1124	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2022.02.15.16:38:20	RpcEptMapper	
System	4	TCP	Listen	192.168.2.136	139	0.0.0.0	0	2022.02.20.8:58:49	System	
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	2022.02.20.8:58:46	System	
EABackgroundService...	3156	TCP	Listen	127.0.0.1	4699	0.0.0.0	0	2022.02.16.19:38:05	EABackgroundService.exe	
svchost.exe	7428	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2022.02.20.8:58:43	CDPSvc	
mDNSResponder.exe	4256	TCP	Listen	127.0.0.1	5354	0.0.0.0	0	2022.02.15.16:38:21	Bonjour Service	
Discord.exe	21096	TCP	Listen	127.0.0.1	6463	0.0.0.0	0	2022.02.20.8:59:16	Discord.exe	
System	4	TCP	Listen	127.0.0.1	9009	0.0.0.0	0	2022.02.20.8:59:45	System	
System	4	TCP	Listen	192.168.2.136	9009	0.0.0.0	0	2022.02.20.8:59:45	System	
System	4	TCP	Listen	192.168.56.1	9009	0.0.0.0	0	2022.02.20.8:59:45	System	
lghub_agent.exe	8876	TCP	Listen	127.0.0.1	9010	0.0.0.0	0	2022.02.20.8:59:15	lghub_agent.exe	
lghub_agent.exe	8876	TCP	Established	127.0.0.1	9010	127.0.0.1	61053	2022.02.20.8:59:16	lghub_agent.exe	
lghub_agent.exe	8876	TCP	Listen	127.0.0.1	9080	0.0.0.0	0	2022.02.20.8:59:15	lghub_agent.exe	
lghub_updater.exe	16916	TCP	Listen	127.0.0.1	9100	0.0.0.0	0	2022.02.15.16:39:01	LGHUBUpdaterService	
lghub_updater.exe	16916	TCP	Established	127.0.0.1	9100	127.0.0.1	61042	2022.02.20.8:59:15	LGHUBUpdaterService	
lghub_updater.exe	16916	TCP	Listen	127.0.0.1	9180	0.0.0.0	0	2022.02.15.16:39:01	LGHUBUpdaterService	
AppleMobileDevicePr...	12404	TCP	Listen	127.0.0.1	27015	0.0.0.0	0	2022.02.20.8:59:26	AppleMobileDeviceProcess.exe	
steam.exe	19688	TCP	Listen	0.0.0.0	27036	0.0.0.0	0	2022.02.20.8:59:14	steam.exe	
steam.exe	19688	TCP	Listen	127.0.0.1	27060	0.0.0.0	0	2022.02.20.8:59:13	steam.exe	
steam.exe	19688	TCP	Established	127.0.0.1	27060	127.0.0.1	63130	2022.02.20.9:27:57	steam.exe	
lghub_agent.exe	8876	TCP	Listen	127.0.0.1	45654	0.0.0.0	0	2022.02.20.8:59:21	lghub_agent.exe	
lsass.exe	928	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2022.02.15.16:38:20	lsass.exe	
wininit.exe	836	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2022.02.15.16:38:20	wininit.exe	
svchost.exe	1444	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2022.02.15.16:38:21	Schedule	
svchost.exe	1708	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2022.02.15.16:38:21	EventLog	
spoolsv.exe	3788	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	2022.02.15.16:38:21	Spooler	
services.exe	908	TCP	Listen	0.0.0.0	49695	0.0.0.0	0	2022.02.15.16:38:23	services.exe	
Discord.exe	10760	TCP	Established	192.168.2.136	55408	162.159.135.234	443	2022.02.20.17:47:30	Discord.exe	
[Time Wait]		TCP	Time Wait	192.168.2.136	55423	142.251.39.3	443			
[Time Wait]		TCP	Time Wait	192.168.2.136	55433	102.109.88.180	443			
[Time Wait]		TCP	Time Wait	192.168.2.136	55434	104.64.166.98	443			

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

### Autoruns:

Megmutatja, mely programok vannak beállítva úgy, hogy automatikusan elinduljanak a rendszer indításakor és a bejelentkezéskor. Az Autoruns megmutatja a registry és a fájlhelyszínek teljes listáját is, ahol az alkalmazások konfigurálhatják az automatikus indítási beállításokat.

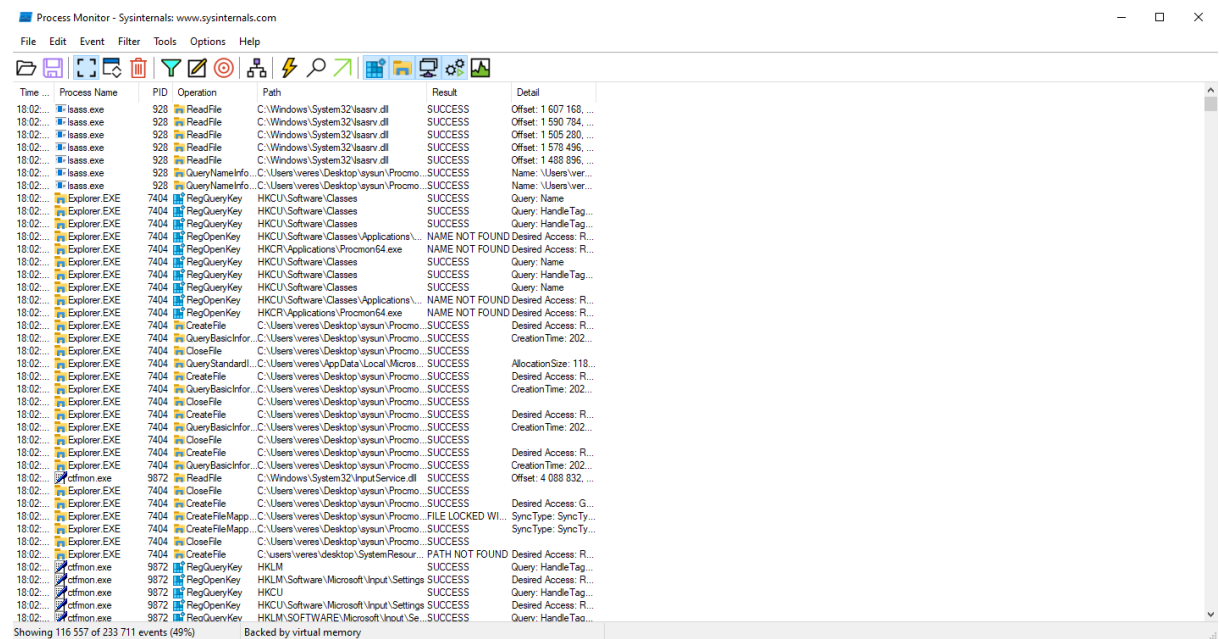


The screenshot shows the Autoruns application window. The title bar reads 'Autoruns - Sysinternals: www.sysinternals.com (Administrator) [DESKTOP-AMNE3QM\veres]'. The menu bar includes File, Search, Entry, User, Options, Category, and Help. Below the menu is a toolbar with icons for refreshing, pausing, and other functions. The main window displays a table of startup programs with columns: Logon, Description, Publisher, Image Path, and Timestamp. The table lists various system and user programs, including Logon, HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell, HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components, HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run, and Explorer. The bottom status bar shows 'Ready'.

Logon	Description	Publisher	Image Path	Timestamp
Logon				
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Microsoft Teams	(Verified) Microsoft 3rd Party Appl...	C:\Users\veres\AppData\Local\Microsoft\Teams\Update.exe	Sun Feb 20 16:24:52 2022
Discord	Update	(Verified) Discord Inc.	C:\Users\veres\AppData\Local\Discord\Update.exe	Sat Feb 12 18:03:06 2022
EnlistedLauncher	Gajjin Smart Launcher	(Verified) Gajjin Network LTD	E:\Enlisted\launcher.exe	Sat Sep 21 18:16:42 2021
Gajjin.Net Updater	Gajjin.Net Updater	(Verified) Gajjin Network LTD	C:\Users\veres\AppData\Local\Gajjin\Program Files (x86)\NetAgent\gja...	Fri Dec 24 17:56:53 2021
LGHUB	LGHUB	(Verified) Logitech Inc	C:\Program Files\LGHUB\Lghub.exe	Fri Dec 24 15:41:20 2020
Steam	Steam	(Verified) Valve Corp.	C:\Program Files (x86)\Steam\steam.exe	Tue Feb 15 16:38:37 2022
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Sun Jan 16 18:41:26 2022
RtkAudUService	Realtek HD Audio Universal Service	(Verified) Realtek Semiconductor ...	C:\Windows\System32\DriverStore\FileRepository\realtekservice.inf_am...	Sun Feb 6 15:54:45 2022
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				Wed Oct 28 17:09:44 2020
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe	Sat Dec 7 10:10:09 2019
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				Mon Sep 13 09:09:28 2021
Brave	Brave Installer	(Verified) Brave Software, Inc.	C:\Program Files\BraveSoftware\Brave-Browser\Application\98.1.35.103...	Thu Oct 21 15:57:45 2021
Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\98.0.1108.56\Install...	Thu Feb 17 12:08:13 2022
n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Sat Feb 19 19:00:19 2022
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				Sat Dec 7 10:10:05 2019
SunJavaUpdateSched	Java Update Scheduler	(Verified) Oracle America, Inc.	C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	Thu Feb 10 15:01:43 2022
TeamsMachineInstaller	Microsoft Teams	(Verified) Microsoft Corporation	C:\Program Files (x86)\Teams Installer\Teams.exe	Mon Sep 27 06:35:04 2021
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				Wed Aug 18 01:45:00 2021
n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Thu Oct 21 15:57:45 2021
Explorer				Sat Dec 7 10:10:05 2019

## Process Monitor

A fájlrendszer, a registry, a folyamatok, a szálak és a DLL-aktivitás valós idejű figyelését teszi lehetővé



Process Monitor - Sysinternals: www.sysinternals.com

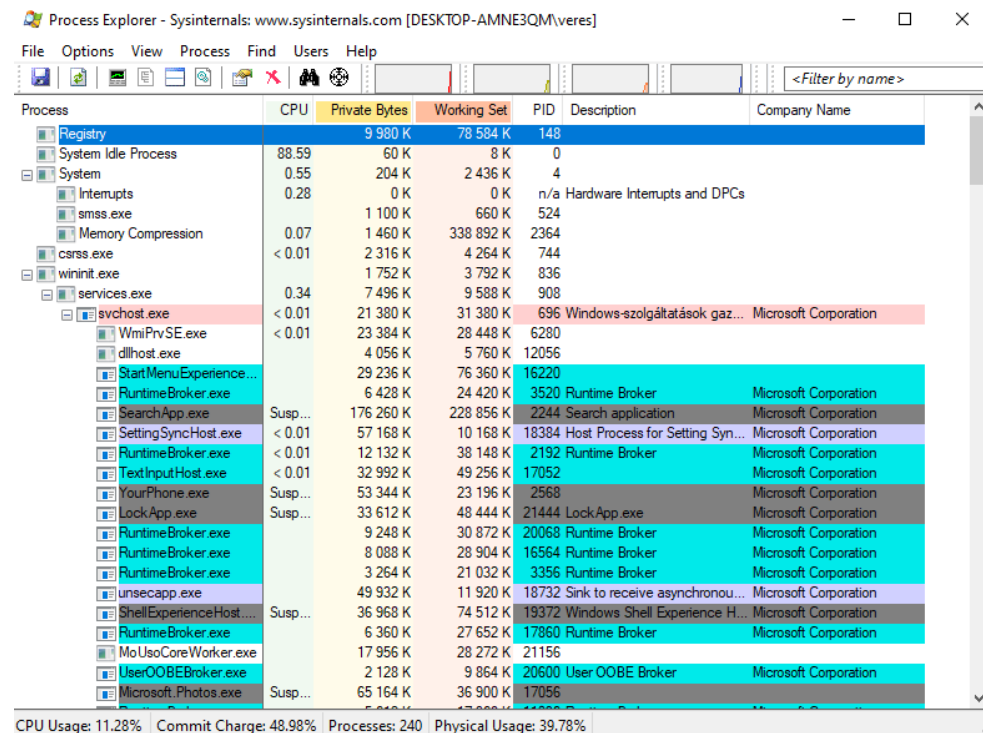
File Edit Event Filter Tools Options Help

Time	Process Name	PID	Operation	Path	Result	Detail
18:02	lsass.exe	928	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 607 168, ...
18:02	lsass.exe	928	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 590 784, ...
18:02	lsass.exe	928	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 505 280, ...
18:02	lsass.exe	928	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 578 496, ...
18:02	lsass.exe	928	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1 488 896, ...
18:02	lsass.exe	928	QueryNameInfo	C:\Users\veres\Desktop\lsasun\Proco...	SUCCESS	Name: \Users\ver...
18:02	lsass.exe	928	QueryNameInfo	C:\Users\veres\Desktop\lsasun\Proco...	SUCCESS	Name: \Users\ver...
18:02	Explorer.EXE	7404	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
18:02	Explorer.EXE	7404	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
18:02	Explorer.EXE	7404	RegOpenKey	HKCU\Software\Classes\Applications...	NAME NOT FOUND	Desired Access: R...
18:02	Explorer.EXE	7404	RegOpenKey	HKCR\Applications\Procom64.exe	SUCCESS	Query: Name
18:02	Explorer.EXE	7404	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
18:02	Explorer.EXE	7404	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
18:02	Explorer.EXE	7404	RegOpenKey	HKCU\Software\Classes\Applications...	NAME NOT FOUND	Desired Access: R...
18:02	Explorer.EXE	7404	RegOpenKey	HKCR\Applications\Procom64.exe	SUCCESS	Desired Access: R...
18:02	Explorer.EXE	7404	CreateFile	C:\Users\veres\Desktop\lsasun\Proco...	SUCCESS	Creation Time: 202...
18:02	Explorer.EXE	7404	QueryBasicInfo	C:\Users\veres\Desktop\lsasun\Proco...	SUCCESS	Creation Time: 202...
18:02	Explorer.EXE	7404	CloseFile	C:\Users\veres\Desktop\lsasun\Proco...	SUCCESS	
18:02	Explorer.EXE	7404	QueryStandard	C:\Users\veres\AppData\Local\Micros...	SUCCESS	AllocationSize: 118...
18:02	Explorer.EXE	7404	QueryBasicInfo	C:\Users\veres\Desktop\lsasun\Proco...	SUCCESS	Desired Access: R...
18:02	Explorer.EXE	7404	CloseFile	C:\Users\veres\Desktop\lsasun\Proco...	SUCCESS	Creation Time: 202...
18:02	Explorer.EXE	7404	CreateFile	C:\Users\veres\Desktop\lsasun\Proco...	SUCCESS	Desired Access: R...
18:02	Explorer.EXE	7404	QueryBasicInfo	C:\Users\veres\Desktop\lsasun\Proco...	SUCCESS	Creation Time: 202...
18:02	Explorer.EXE	7404	CloseFile	C:\Users\veres\Desktop\lsasun\Proco...	SUCCESS	Desired Access: R...
18:02	Explorer.EXE	7404	CreateFile	C:\Users\veres\Desktop\lsasun\Proco...	SUCCESS	Creation Time: 202...
18:02	Explorer.EXE	7404	QueryBasicInfo	C:\Users\veres\Desktop\lsasun\Proco...	SUCCESS	Creation Time: 202...
18:02	dfmon.exe	9872	ReadFile	C:\Windows\System32\inputService.dll	SUCCESS	Offset: 4 088 832, ...
18:02	Explorer.EXE	7404	CloseFile	C:\Users\veres\Desktop\lsasun\Proco...	SUCCESS	Desired Access: G...
18:02	Explorer.EXE	7404	CreateFile	C:\Users\veres\Desktop\lsasun\Proco...	FILE LOCKED WI...	SyncType: SyncTy...
18:02	Explorer.EXE	7404	CreateFile	C:\Users\veres\Desktop\lsasun\Proco...	SUCCESS	SyncType: SyncTy...
18:02	Explorer.EXE	7404	CloseFile	C:\Users\veres\Desktop\lsasun\Proco...	SUCCESS	
18:02	Explorer.EXE	7404	CreateFile	C:\Users\veres\Desktop\SystemResour...	PATH NOT FOUND	Desired Access: R...
18:02	dfmon.exe	9872	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTag...
18:02	dfmon.exe	9872	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
18:02	dfmon.exe	9872	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
18:02	dfmon.exe	9872	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...

Showing 116 557 of 233 711 events (49%) Backed by virtual memory

## Process Explorer:

Megtudhatjuk, hogy milyen fájlok, registry-ik és egyéb objektumok vannak megnyitva a folyamatokban, milyen DLL-eket töltöttek be, és még sok minden mást. Ez a segédprogram még azt is megmutatja, hogy ki a tulajdonosa az egyes folyamatoknak.



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-AMNE3QM\veres]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		9 980 K	78 584 K	148		
System Idle Process	88.59	60 K	8 K	0		
System	0.55	204 K	2 436 K	4		
Interrupts	0.28	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 100 K	660 K	524		
Memory Compression	0.07	1 460 K	338 892 K	2364		
csrss.exe	< 0.01	2 316 K	4 264 K	744		
wininit.exe		1 752 K	3 792 K	836		
services.exe	0.34	7 496 K	9 588 K	908		
svchost.exe	< 0.01	21 380 K	31 380 K	696	Windows-szolgáltatások gaz...	Microsoft Corporation
WmiPrvSE.exe	< 0.01	23 384 K	28 448 K	6280		
dllhost.exe		4 056 K	5 760 K	12056		
StartMenuExperienceHost.exe		29 236 K	76 360 K	16220		
RuntimeBroker.exe		6 428 K	24 420 K	3520	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	176 260 K	228 856 K	2244	Search application	Microsoft Corporation
SettingSyncHost.exe	< 0.01	57 168 K	10 168 K	18384	Host Process for Setting Syn...	Microsoft Corporation
RuntimeBroker.exe	< 0.01	12 132 K	38 148 K	2192	Runtime Broker	Microsoft Corporation
TextInputHost.exe	< 0.01	32 992 K	49 256 K	17052		Microsoft Corporation
YourPhone.exe	Susp...	53 344 K	23 196 K	2568		Microsoft Corporation
LockApp.exe	Susp...	33 612 K	48 444 K	21444	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		9 248 K	30 872 K	20068	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		8 088 K	28 904 K	16564	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		3 264 K	21 032 K	3356	Runtime Broker	Microsoft Corporation
unsecapp.exe		49 932 K	11 920 K	18732	Sink to receive asynchronou...	Microsoft Corporation
ShellExperienceHost.exe	Susp...	36 968 K	74 512 K	19372	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		6 360 K	27 652 K	17860	Runtime Broker	Microsoft Corporation
MoUsoCoreWorker.exe		17 956 K	28 272 K	21156		
UserOOBEBroker.exe		2 128 K	9 864 K	20600	User OOBEBroker	Microsoft Corporation
Microsoft.Photos.exe	Susp...	65 164 K	36 900 K	17056		

CPU Usage: 11.28% Commit Charge: 48.98% Processes: 240 Physical Usage: 39.78%

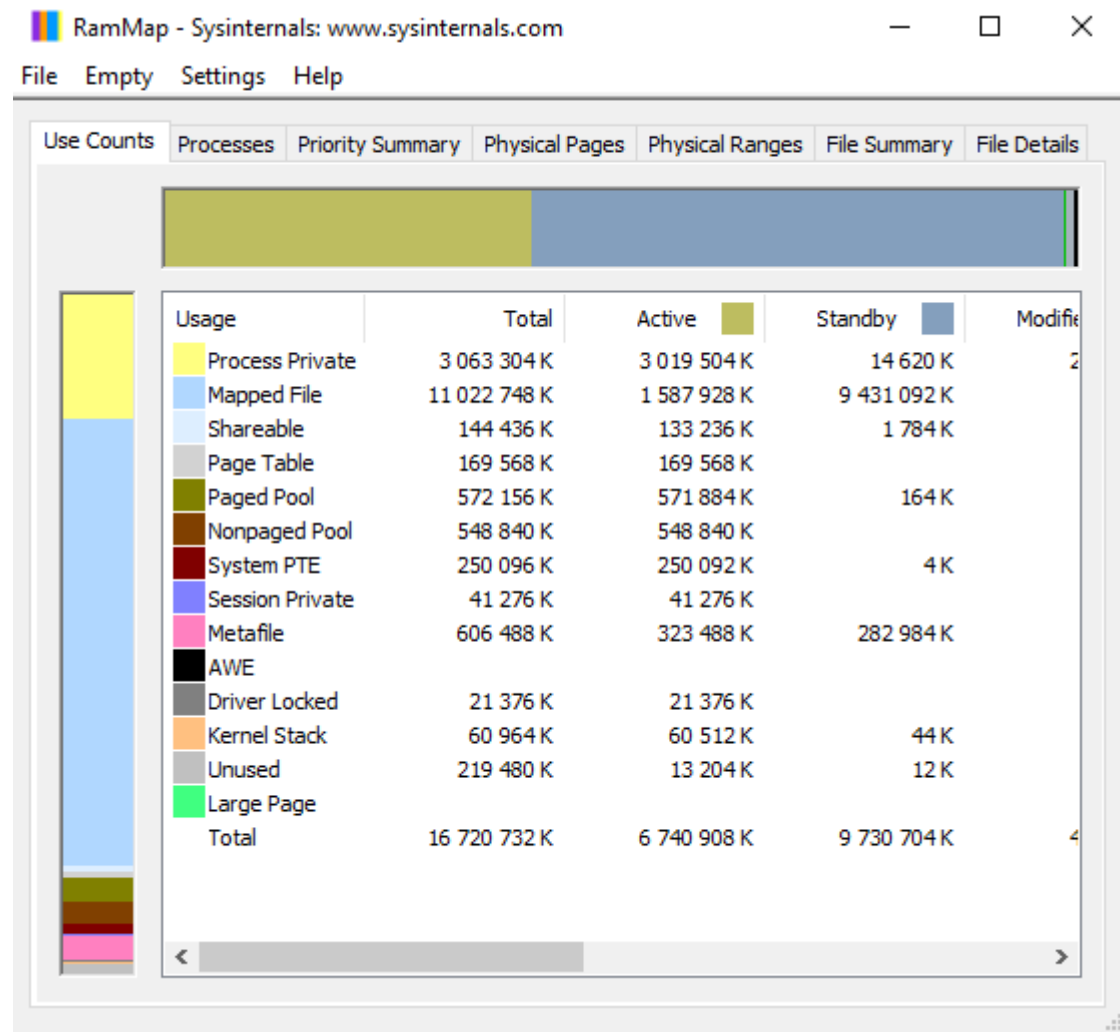
d) Security Utilities (LogonSession)

A jelenleg aktív bejelentkezett munkameneteket listázza ki.

```
[27] Logon session 00000000:28691b39:  
User name:      DESKTOP-AMNE3QM\veres  
Auth package:   CloudAP  
Logon type:     Interactive  
Session:       10  
Sid:           S-1-5-21-3144379037-549243845-4022684298-1001  
Logon time:     2022. 02. 20. 8:58:43  
Logon server:  
DNS Domain:  
UPN:
```

e) Information Utilities (RAMMap)

Egy fejlett fizikai memóriahasználat-elemző segédprogram, amely különböző módon mutatja be a használati információkat több különböző lapon.



3. Töltse le a következő programot: Dependency Walker

A Dependency Walker segítségével végezze el a következő feladatokat.



Dependency Walker - [skytime.exe]

File Edit View Options Profile Window Help

The screenshot shows the Dependency Walker application interface. On the left, a tree view lists loaded modules: skytime.exe, KERNEL32.DLL, API-MS-WIN-CORE-RTSSUPPORT-L1-1-0.DLL, NTDLL.dll, USER32.dll, GDI32.dll, ADVAPI32.dll, SHLWAPI.dll, and SHELL32.dll. The main pane displays a detailed list of module dependencies. Each row includes a checkbox, a green status icon, the ordinal number, a hint, the function name, and the entry point.

	PI	Ordinal ^	Hint	Function	Entry Point
		N/A	269 (0x01D0)	DeleteCriticalSection	Not Bound
		N/A	305 (0x0131)	EnterCriticalSection	Not Bound
		N/A	556 (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 (0x02C2)	GetStartupInfo	Not Bound
		N/A	747 (0x02EB)	GetSystemTimeAsFileTime	Not Bound
		N/A	775 (0x0307)	GetTickCount	Not Bound
		N/A	864 (0x03A0)	InitializeCriticalSection	Not Bound
		N/A	952 (0x03B8)	LeaveCriticalSection	Not Bound
		N/A	1004 (0x0446)	QueryPerformanceCounter	Not Bound
		N/A	1180 (0x04FC)	RtlAddFunctionTable	Not Bound
		N/A	1181 (0x04FD)	RtlCaptureContext	Not Bound
		N/A	1188 (0x04A4)	RtlLookupFunctionEntry	Not Bound
		N/A	1195 (0x04A8)	RtlUnwindInvid	Not Bound
		N/A	1347 (0x0543)	SetUnhandledExceptionFilter	Not Bound
		N/A	1361 (0x0551)	Sleep	Not Bound
		N/A	1376 (0x0560)	TerminateProcess	Not Bound
		N/A	1396 (0x0574)	SetUnhandledExceptionFilter	Not Bound
		N/A	1470 (0x05B2)	UnhandledExceptionFilter	Not Bound
		N/A	1444 (0x05A4)	VirtualProtect	Not Bound
		N/A	1446 (0x05A6)	VirtualQuery	Not Bound

	E	Ordinal ^	Hint	Function	Entry Point
	1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive	

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
Module														
EXT-MS-WIN-RT-DEVICE-ACCESS-L1-1-0.DLL									Error opening file. A rendszert nem találja a megadott fájlt (2).					
EXT-MS-WIN32-SUBSYSTEM-QUERY-L1-1-0.DLL									Error opening file. A rendszert nem találja a megadott fájlt (2).					
KERNELBASE.dll	2022/02/11 10:59	2021/12/12 7:32	770 136 A		0x000BF847	0x000BF847	x64	Console	CY\Unknown	0x0000000180000000	Unknown	0x000BE000	Not Loaded	10.0.19041.1503
KERNEL32.dll	2022/02/11 10:59	2064/12/28 4:42	2 922 912 A		0x002D8009	0x002D8009	x64	Console	CY\Unknown	0x0000000180000000	Unknown	0x002C8000	Not Loaded	10.0.19041.1503
MSVCRT.dll	2021/09/18 8:09	2015/11/20 23:31	637 360 A		0x000E9F5D	0x000E9F5D	x64	GUI	CY\Unknown	0x0000000110100000	Unknown	0x000E9000	Not Loaded	7.0.19041.546
NTDLL.dll	2022/01/13 17:59	2090/09/01 14:26	2 028 296 A		0x001FF8C2	0x001FF8C2	x64	Console	CY\Unknown	0x0000000180000000	Unknown	0x001F5000	Not Loaded	10.0.19041.1466
EXT-MS-WIN-SECURITY-CAPATHNZ-L1-1-0.DLL	2022/02/20 18:15	2021/02/28 15:58	56 089 A		0x00019102	0x00019102	x64	Console	None	0x0000000000000000	Unknown	0x00013000	Not Loaded	N/A

Szerepe: Az Ntdll.dll többnyire a rendszerfeladatokkal foglalkozik, és számos kernel-módú funkciót tartalmaz, amelyek lehetővé teszik a "Windows alkalmazásprogramozási felületet (API)" működését. Az ntdll.dll felelős az üzenetekért, az ütemezésért, a szálkezelésért és a szinkronizálásért is az operációs rendszerben.

Mentés: Írja le a program szolgáltatásait és a futtatás eredményét a feladat számával a megadott jegyzőkönyvbe (képernyőkép is).