

# Operációs rendszerek BSc

## 2.Gyak.

2022.02.15.

**Készítette:**

Stremler László Bsc

Programtervező Informatikus

AQYO8L

**Miskolc, 2022**

### 1. Feladat:

a.) Hozza létre a következő mappa szerkezetet!

GitBash-ben csináltam meg a mappaszerkezetet, mivel ezt tartottam a legegyszerűbb megoldásnak.

```
MINGW64; c:/Users/László/Desktop/OS/AQY08L0sGyak/AQY08L_0215
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ mkdir bokor
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ mkdir bokor/banan
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ mkdir bokor/mogyoro
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ mkdir bokor/barack
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ ls
bokor/
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ cd bokor
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215/bokor (MAPPA)
$ ls
banan/  barack/  mogyoro/
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215/bokor (MAPPA)
$ cd ../
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ mkdir fa
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ mkdir fa/korte
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ mkdir land
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ mkdir land/szeder
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ mkdir land/kokusz
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ ls
bokor/  fa/  land/
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ |
```

b.) Készítsen másolatot:

- a neptunkod/ land/szeder katalógusról a neptunkod/fa katalógusba
  - a neptunkod /bokor/banan katalógusról a neptunkod /fa katalógusba
- Itt a cp parancs rekurzív kapcsolójával másoltam át a katalógust és a tartalmakat a kijelölt helyre. Enélkül a kapcsoló nélkül nem lehetett másolatot készíteni, mivel nem voltak üresek.

```
László@DESKTOP-GFIIQG6 MINGW64 ~/Desktop/OS/AQY08LOsGyak/AQY08L_0215 (MAPPA)
$ cp -r land/szeder fa/

László@DESKTOP-GFIIQG6 MINGW64 ~/Desktop/OS/AQY08LOsGyak/AQY08L_0215 (MAPPA)
$ cd fa

László@DESKTOP-GFIIQG6 MINGW64 ~/Desktop/OS/AQY08LOsGyak/AQY08L_0215/fa (MAPPA)
$ ls
korte/  szeder/

László@DESKTOP-GFIIQG6 MINGW64 ~/Desktop/OS/AQY08LOsGyak/AQY08L_0215/fa (MAPPA)
$ cp -r bokor/banan fa
cp: cannot stat 'bokor/banan': No such file or directory

László@DESKTOP-GFIIQG6 MINGW64 ~/Desktop/OS/AQY08LOsGyak/AQY08L_0215/fa (MAPPA)
$ cd ../

László@DESKTOP-GFIIQG6 MINGW64 ~/Desktop/OS/AQY08LOsGyak/AQY08L_0215 (MAPPA)
$ cp -r bokor/banan fa

László@DESKTOP-GFIIQG6 MINGW64 ~/Desktop/OS/AQY08LOsGyak/AQY08L_0215 (MAPPA)
$ cd fa

László@DESKTOP-GFIIQG6 MINGW64 ~/Desktop/OS/AQY08LOsGyak/AQY08L_0215/fa (MAPPA)
$ ls
banan/  korte/  szeder/
```

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

```
László@DESKTOP-GFIIQG6 MINGW64 ~/Desktop/OS/AQY08LOsGyak/AQY08L_0215 (MAPPA)
$ mv bokor/barack fa

László@DESKTOP-GFIIQG6 MINGW64 ~/Desktop/OS/AQY08LOsGyak/AQY08L_0215 (MAPPA)
$ mv land/kokusz fa

László@DESKTOP-GFIIQG6 MINGW64 ~/Desktop/OS/AQY08LOsGyak/AQY08L_0215 (MAPPA)
$ cd fa

László@DESKTOP-GFIIQG6 MINGW64 ~/Desktop/OS/AQY08LOsGyak/AQY08L_0215/fa (MAPPA)
$ ls
banan/  barack/  kokusz/  korte/  szeder/
```

Az mv parancsot használva teljesítettem a feladatot, majd a végén a fa mappába belépve az ls paranccsal megnéztem hogy minden oda került-e, ahova a feladat kérte.

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

- neptunkod/bokor/banan/ leiras.txt
- neptunkod/tree/felsorolas.txt

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

A felsorolas szöveges állományba soroljon fel legalább 5 csoporttársa nevét.

```
László@DESKTOP-GF11QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ rm -r land

László@DESKTOP-GF11QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ ls
bokor/  fa/
```

Ezen a képen a land mappa törlése látható, amit rekurzív módon hajtottam végre az rm parancs -r kapcsolója segítségével. A művelet után az ls paranccsal megnéztem, hogy tényleg törölve lett-e a mappa.

```
László@DESKTOP-GF11QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215/bokor/banan (MAPPA)
$ nano leiras.txt

László@DESKTOP-GF11QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215/bokor/banan (MAPPA)
$ cat leiras.txt
A baracknak több fajtája is van, többek között az őszi és a sárgabarack. A barack fán terem. A gyümölcsök osztályába tartozik. Nagyon zamatos, finom, édes húsa van.

László@DESKTOP-GF11QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215/bokor/banan (MAPPA)
$ cd ../

László@DESKTOP-GF11QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215/bokor (MAPPA)
$ cd ../

László@DESKTOP-GF11QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ cd tree
bash: cd: tree: No such file or directory

László@DESKTOP-GF11QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ cd /tree
bash: cd: /tree: No such file or directory

László@DESKTOP-GF11QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ ls
bokor/  fa/

László@DESKTOP-GF11QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ cd fa

László@DESKTOP-GF11QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215/fa (MAPPA)
$ nano felsorolas.txt

László@DESKTOP-GF11QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215/fa (MAPPA)
$ cat felsorolas.txt
Benedek Elek
Fekete László
Zöld Piroska
Kék Elemér
Árpádházi Árpád Tibor
```

Én a d és e betűjelű feladatokat egyszerre csináltam meg, mivel ezt találtam a leghatékonyabb megoldásnak. Közvetlen a fájl létrehozása után beleírtam a tartalmukat, amit azonnal mentettem is. A képernyőképen látszik, hogy utána a cat paranccsal megnéztem a tartalmukat a biztonság kedvéért.

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

```
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ ls -R
.:
bokor/  fa/

./bokor:
banan/  mogyoro/

./bokor/banan:
leiras.txt

./bokor/mogyoro:

./fa:
banan/  barack/  felsorolas.txt  kokusz/  korte/  szeder/

./fa/banan:

./fa/barack:

./fa/kokusz:

./fa/korte:

./fa/szeder:

László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ |
```

Az ls parancs -R kapcsolójával listáztam az összes almappát, valamint a bennük lévő fájlokat.

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

```
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ ls -R | grep "^e"
leiras.txt
felsorolas.txt

László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ |
```

A gyökérmappába való visszatérés után, az ls parancs -R kapcsolóját, valamint a grep parancsot ötvöztem, így tudtam kiírni a feladat megoldását. Az ls parancs kilistázza a dolgokat, a -R kapcsolóval az összes almappát és tartalmát. A grep parancs megnézi hogy tartalmaz-e valamilyen elemet, ami megfelel a kritériumnak a csővezeték bal oldalának kimenetele. A grep parancs paramétere a következőt jelenti: ^-fájlnév eleje; . – első karakter lehet bármi; e – második karakter.

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

```
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ cd fa

László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215/fa (MAPPA)
$ chmod a+r felsorolas.txt

László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215/fa (MAPPA)
$ |
```

A chmod parancs segítségével adtam jogosultságot az összes felhasználónak olvasásra. (Az “a” jelöli az összes felhasználót – all user, a “+r” pedig hogy az olvasást (read) adom hozzá jogosultságként az adott felhasználóhoz.)

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

```
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ du -h
1.0K    ./bokor/banan
0       ./bokor/mogyoro
1.0K    ./bokor
0       ./fa/banan
0       ./fa/barack
0       ./fa/kokusz
0       ./fa/korte
0       ./fa/szeder
5.0K    ./fa
6.0K    .

László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ |
```

Itt a du parancsot használtam, a -h kapcsolójával pedig ember által értelmezhető értéket adott vissza.

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

```
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ sort fa/felsorolas.txt
Benedek Elek
Fekete László
Kék Elemér
Zöld Piroska
Árpádházi Árpád Tibor

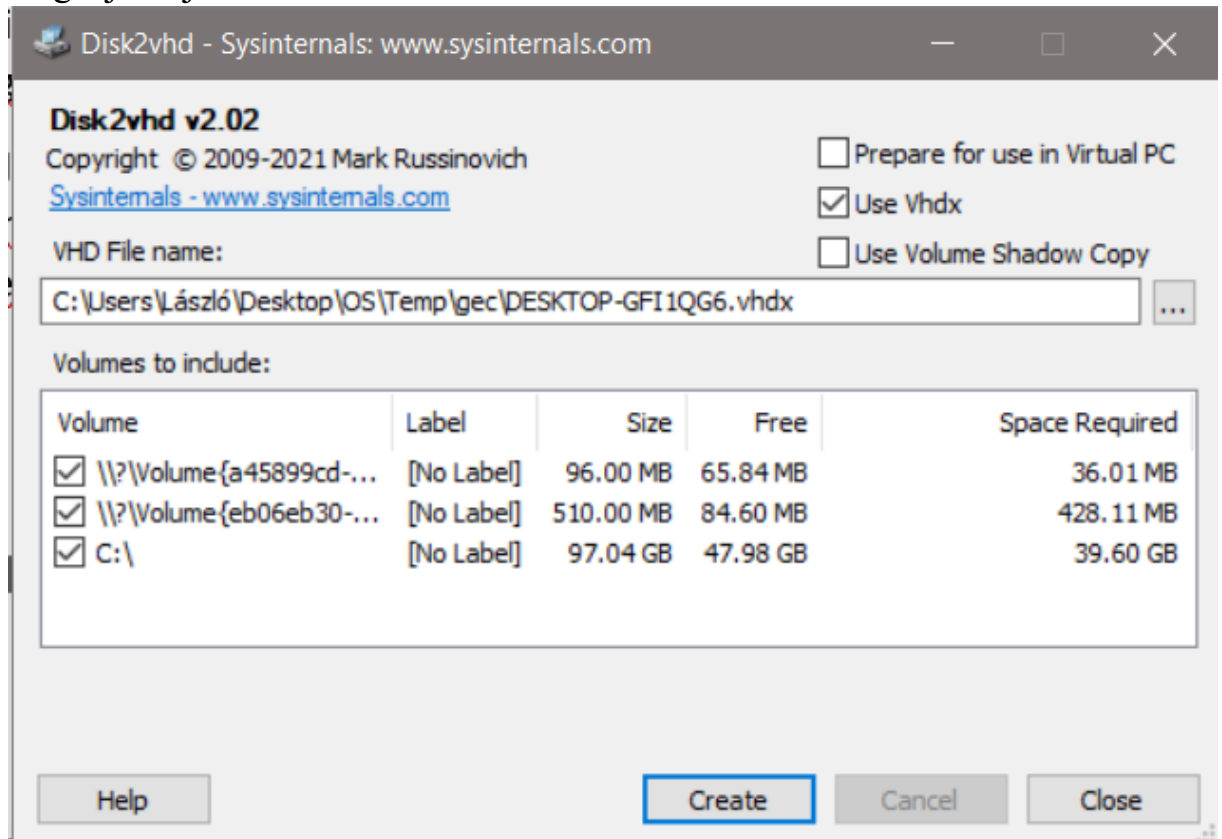
László@DESKTOP-GFI1QG6 MINGW64 ~/Desktop/OS/AQY08L0sGyak/AQY08L_0215 (MAPPA)
$ sort -c fa/felsorolas.txt
sort: fa/felsorolas.txt:4: disorder: Kék Elemér
```

A sort parancs segítségével az angol ABC-nek megfelelően sorbarendeztem a fájl tartalmát.

## 2. Feladat:

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): Képes a fizikai meghajtóból virtuális meghajtó fájlt csinálni .vhd formátumban.



- b) Networking Utilities (TCPView): Kijelzi a futó folyamatokat, a folyamat azonosítójukat (process id), az internetes protokollját, a kapcsolat állapotát, a helyi (interfész) IP címet amit használ a folyamat, a helyi portot, a távoli IP címet, ami felé kommunikál a folyamat, a távoli portot, a kapcsolat létrejöttének időpontját, a küldött és fogadott csomagokat, valamint bájtokat.

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6 Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	872	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2021.12.06.20:54:50	RpcEptMapper
System	4	TCP	Listen	192.168.1.4	139	0.0.0.0	0	2022.02.15.18:24:24	System
svchost.exe	6300	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2022.02.15.18:24:20	CDPSvc
WINWORD.EXE	5140	TCP	Fin Wait 2	192.168.1.4	49185	52.109.88.56	443	2022.02.15.18:53:51	WINWORD.EXE
opera.exe	6480	TCP	Established	192.168.1.4	49205	140.82.112.25	443	2022.02.15.18:58:55	opera.exe
lsass.exe	816	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2021.12.06.20:54:50	lsass.exe
wininit.exe	656	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2021.12.06.20:54:50	wininit.exe
svchost.exe	1516	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2021.12.06.20:54:50	EventLog
svchost.exe	1508	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2021.12.06.20:54:51	Schedule
spoolsv.exe	3528	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	2021.12.06.20:54:53	Spooler
services.exe	796	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	2021.12.06.20:54:54	services.exe
svchost.exe	3640	TCP	Established	192.168.1.4	53397	20.199.120.85	443	2022.02.15.18:24:30	WpnService
opera.exe	6480	TCP	Established	192.168.1.4	53524	185.60.218.19	443	2022.02.15.18:25:18	opera.exe
opera.exe	6480	TCP	Established	192.168.1.4	53545	142.250.102.188	5228	2022.02.15.18:25:22	opera.exe
WinStore.App.exe	7068	TCP	Close Wait	192.168.1.4	54821	92.122.253.130	443	2022.02.15.18:28:38	WinStore.App.exe
WinStore.App.exe	7068	TCP	Close Wait	192.168.1.4	54822	92.122.253.130	443	2022.02.15.18:28:38	WinStore.App.exe
WinStore.App.exe	7068	TCP	Close Wait	192.168.1.4	54823	92.122.253.130	443	2022.02.15.18:28:38	WinStore.App.exe
WinStore.App.exe	7068	TCP	Close Wait	192.168.1.4	54824	92.122.253.130	443	2022.02.15.18:28:38	WinStore.App.exe
WinStore.App.exe	7068	TCP	Close Wait	192.168.1.4	54825	92.122.253.130	443	2022.02.15.18:28:39	WinStore.App.exe
WinStore.App.exe	7068	TCP	Close Wait	192.168.1.4	54826	92.122.253.130	443	2022.02.15.18:28:39	WinStore.App.exe
WinStore.App.exe	7068	TCP	Close Wait	192.168.1.4	54828	92.122.253.130	443	2022.02.15.18:28:50	WinStore.App.exe
opera.exe	6480	TCP	Established	192.168.1.4	54882	185.60.218.12	443	2022.02.15.18:34:15	opera.exe
WINWORD.EXE	5140	TCP	Established	192.168.1.4	55689	13.107.138.9	443	2022.02.15.19:02:09	WINWORD.EXE
WINWORD.EXE	5140	TCP	Established	192.168.1.4	55875	13.107.136.9	443	2022.02.15.19:19:57	WINWORD.EXE

Endpoints: 61 Established: 9 Listening: 21 Time Wait: 3 Close Wait: 7 Update: 2 sec States: (All)

c) Process Utilities (Process Explorer, Process Monitor, AutoRuns): A Process Explorer kiírja az éppen futó folyamatokat és alfolyamataikat, a processzor idejüket, az általuk használt és lefoglalt memóriát, a PID-jüket, a leírásukat és a folyamatok gyártóját.

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-GF11QG6\László]

File Options View Process Find Users Help

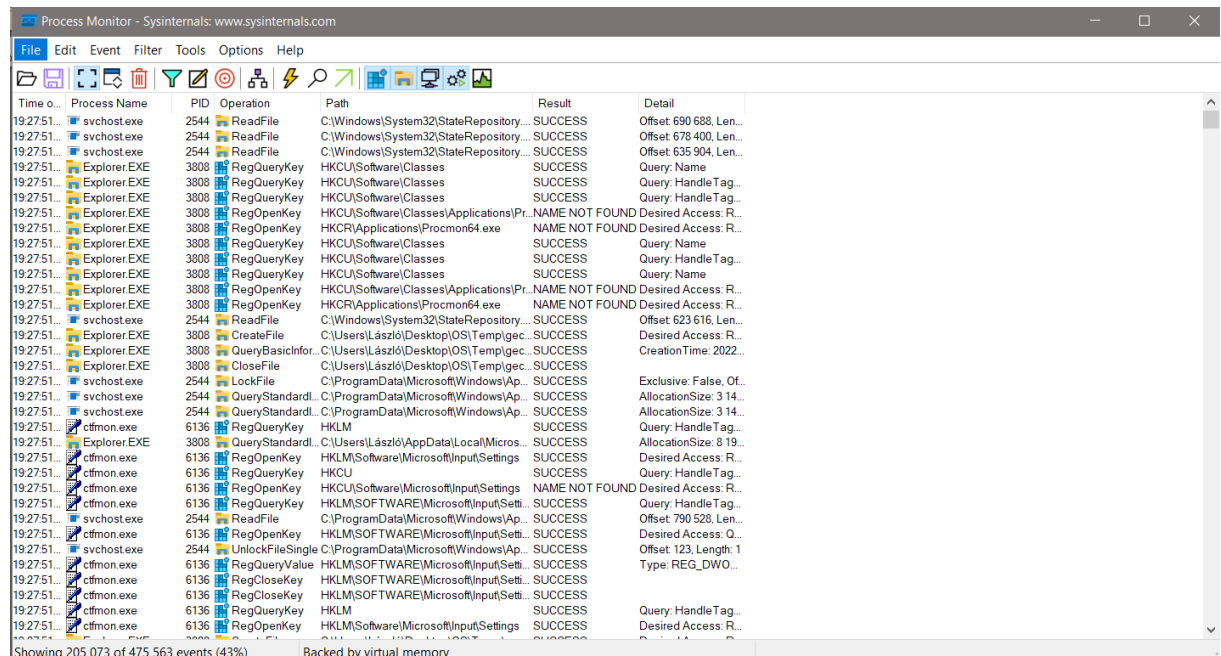
<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		10 424 K	58 876 K	100		
System Idle Process	72.99	60 K	8 K	0		
System	0.74	192 K	32 K	4		
Interrupts	2.21	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 072 K	500 K	380		
Memory Compression	< 0.01	472 K	137 700 K	2612		
csrss.exe		848 K	4 060 K	572		
wininit.exe		620 K	3 928 K	656		
services.exe	< 0.01	5 572 K	7 128 K	796		
svchost.exe	< 0.01	13 904 K	24 500 K	940	Windows-szolgáltatások gaz...	Microsoft Corporation
dllhost.exe		3 652 K	5 920 K	2928		
StartMenuExperienceHo...		20 268 K	61 136 K	8672		
RuntimeBroker.exe		7 056 K	28 068 K	9724	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	178 020 K	255 748 K	6636	Search application	Microsoft Corporation
RuntimeBroker.exe	< 0.01	12 100 K	37 036 K	7136	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	28 016 K	2 536 K	3776	YourPhone	Microsoft Corporation
RuntimeBroker.exe		6 056 K	24 364 K	8784	Runtime Broker	Microsoft Corporation
SettingSyncHost.exe		2 240 K	6 020 K	6988	Host Process for Setting Syn...	Microsoft Corporation
dllhost.exe		5 468 K	14 472 K	9812	COM Surrogate	Microsoft Corporation
RuntimeBroker.exe		1 992 K	11 276 K	4168	Runtime Broker	Microsoft Corporation
TextInputHost.exe	< 0.01	11 008 K	42 080 K	8992		Microsoft Corporation
WinStore.App.exe	Susp...	59 476 K	3 144 K	7068	Store	Microsoft Corporation
ApplicationFrameHoste...		15 620 K	36 428 K	11048	Application Frame Host	Microsoft Corporation
RuntimeBroker.exe		4 920 K	18 540 K	9444	Runtime Broker	Microsoft Corporation
SystemSettings.exe	Susp...	22 660 K	2 880 K	7580	Gépház	Microsoft Corporation
UserOOBEBroker.exe		2 052 K	9 140 K	8720	User OOBEBroker	Microsoft Corporation
Calculator.exe	Susp...	20 492 K	2 448 K	10336		
RuntimeBroker.exe		1 560 K	6 512 K	2832	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	8.48	33 668 K	83 096 K	10900	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe	1.47	5 928 K	29 376 K	11008	Runtime Broker	Microsoft Corporation

CPU Usage: 27.28% Commit Charge: 50.05% Processes: 171 Physical Usage: 48.32%



A Process Monitor úgyszintén az éppen futó folyamatokat mutatja, azonban ez az előzővel ellentétben mutatja a folyamat által végrehajtott műveletet, a folyamat elérési útvonalát, a folyamat művelet eredményét, valamint a részleteket. Továbbá képes folyamat fát is előállítani, ami az előző program alap nézete volt.

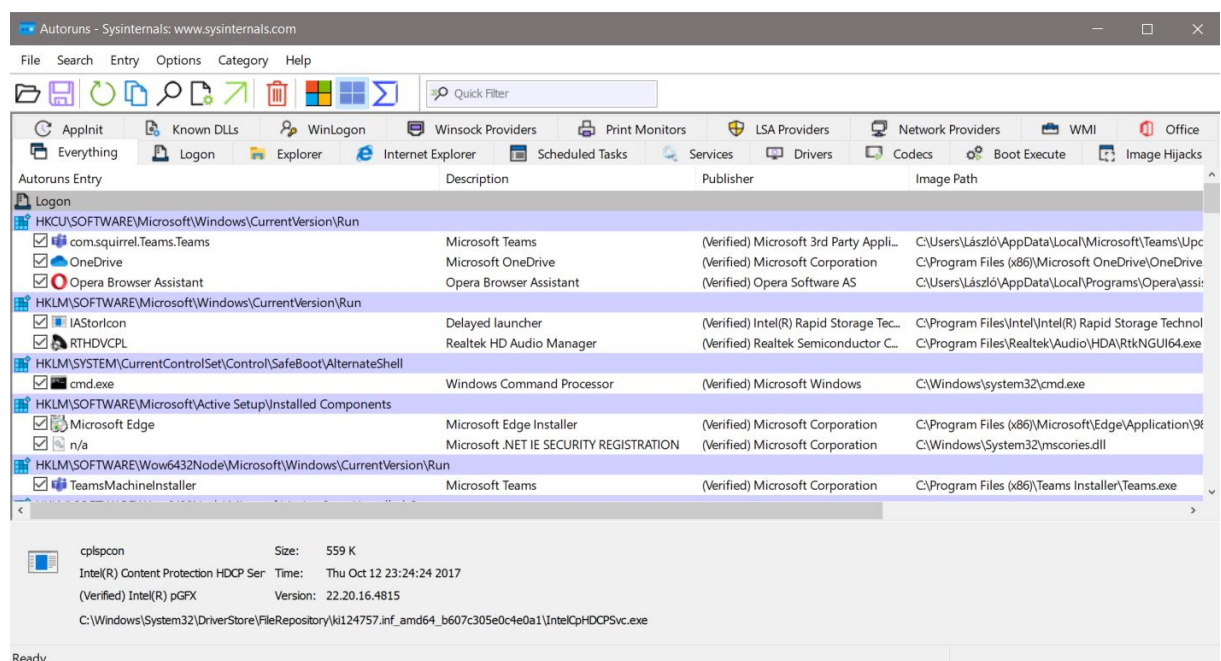


Process Monitor - Sysinternals: www.sysinternals.com

Time o...	Process Name	PID	Operation	Path	Result	Detail
19:27:51...	svchost.exe	2544	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 690 688, Len...
19:27:51...	svchost.exe	2544	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 678 400, Len...
19:27:51...	svchost.exe	2544	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 635 904, Len...
19:27:51...	Explorer.EXE	3808	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
19:27:51...	Explorer.EXE	3808	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
19:27:51...	Explorer.EXE	3808	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
19:27:51...	Explorer.EXE	3808	RegOpenKey	HKCU\Software\Classes\Applications\Pr...	NAME NOT FOUND	Desired Access: R...
19:27:51...	Explorer.EXE	3808	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
19:27:51...	Explorer.EXE	3808	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
19:27:51...	Explorer.EXE	3808	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
19:27:51...	Explorer.EXE	3808	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
19:27:51...	Explorer.EXE	3808	RegOpenKey	HKCU\Software\Classes\Applications\Pr...	NAME NOT FOUND	Desired Access: R...
19:27:51...	Explorer.EXE	3808	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
19:27:51...	svchost.exe	2544	CreateFile	C:\Users\László\Desktop\OS\Templge...	SUCCESS	Offset: 623 616, Len...
19:27:51...	svchost.exe	2544	CreateFile	C:\Users\László\Desktop\OS\Templge...	SUCCESS	Desired Access: R...
19:27:51...	svchost.exe	2544	QueryBasicInfor...	C:\Users\László\Desktop\OS\Templge...	SUCCESS	CreationTime: 2022...
19:27:51...	svchost.exe	2544	CloseFile	C:\Users\László\Desktop\OS\Templge...	SUCCESS	
19:27:51...	svchost.exe	2544	LockFile	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Exclusive: False, Of...
19:27:51...	svchost.exe	2544	QueryStandardl...	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	AllocationSize: 3 14...
19:27:51...	svchost.exe	2544	QueryStandardl...	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	AllocationSize: 3 14...
19:27:51...	ctfmon.exe	6136	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
19:27:51...	Explorer.EXE	3808	QueryStandardl...	C:\Users\László\AppData\Local\Micros...	SUCCESS	AllocationSize: 8 19...
19:27:51...	ctfmon.exe	6136	RegOpenKey	HKLM\Software\Microsoft\Input\Setti...	SUCCESS	Desired Access: R...
19:27:51...	ctfmon.exe	6136	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
19:27:51...	ctfmon.exe	6136	RegOpenKey	HKCU\Software\Microsoft\Input\Setti...	NAME NOT FOUND	Desired Access: R...
19:27:51...	ctfmon.exe	6136	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Query: HandleTag...
19:27:51...	svchost.exe	2544	ReadFile	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Offset: 790 528, Len...
19:27:51...	ctfmon.exe	6136	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Desired Access: Q...
19:27:51...	svchost.exe	2544	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Offset: 123, Length: 1
19:27:51...	ctfmon.exe	6136	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Type: REG_DWORD...
19:27:51...	ctfmon.exe	6136	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	
19:27:51...	ctfmon.exe	6136	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	
19:27:51...	ctfmon.exe	6136	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
19:27:51...	ctfmon.exe	6136	RegOpenKey	HKLM\Software\Microsoft\Input\Setti...	SUCCESS	Desired Access: R...

Showing 205 073 of 475 563 events (43%) Backed by virtual memory

Az AutoRuns megmutatja, hogy egy-egy folyamat mely registrybejegyzést használja. Le lehet tiltani a folyamatok automatikus futását ezzel a programmal. Az ablakban csoportokra bontja Microsoft termékek, ismert termékek, stb. néven. Lényegében egy grafikus felületet biztosít a Registry-nek.

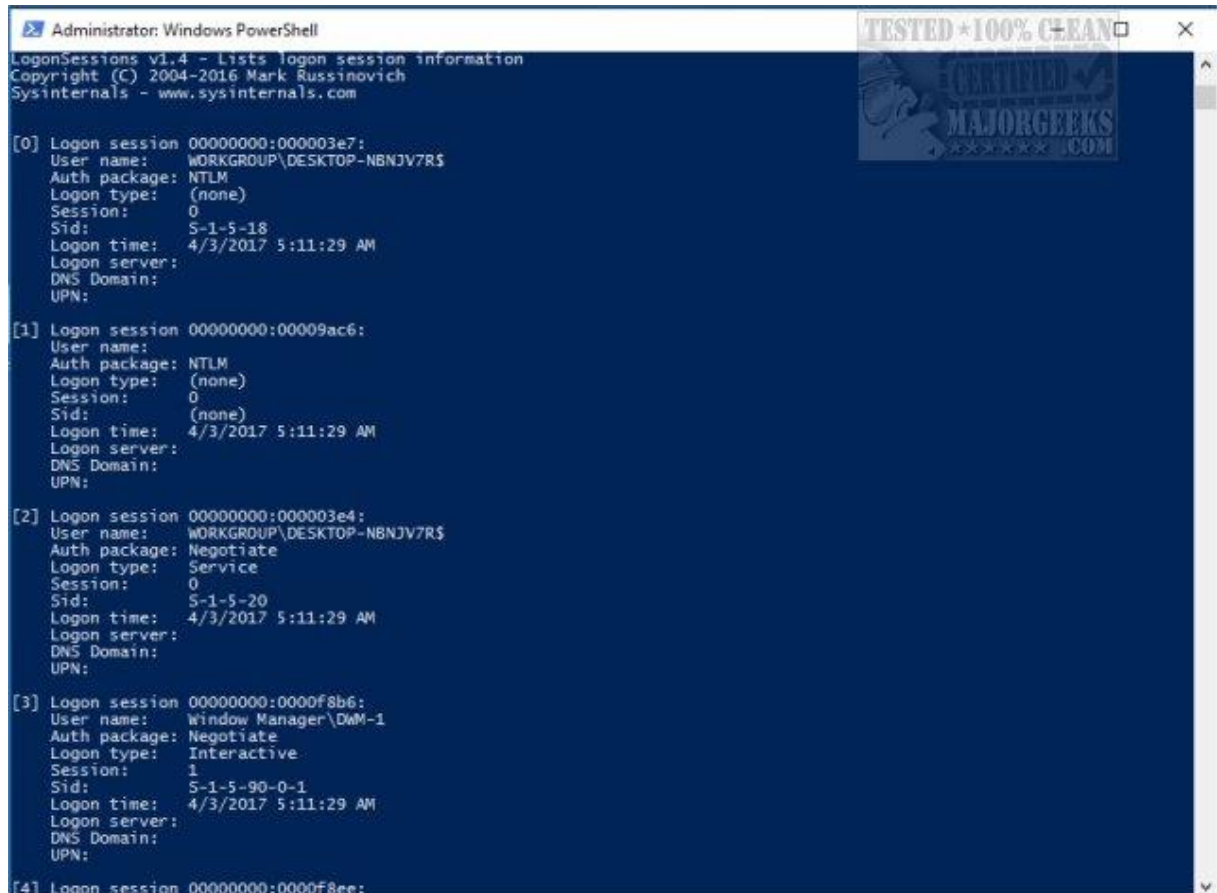


Autoruns - Sysinternals: www.sysinternals.com

Auturuns Entry	Description	Publisher	Image Path
Logon			
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> com.squirrel.Teams.Teams	Microsoft Teams	(Verified) Microsoft 3rd Party Appli...	C:\Users\László\AppData\Local\Microsoft\Teams\Upd...
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft OneDrive\OneDrive...
<input checked="" type="checkbox"/> Opera Browser Assistant	Opera Browser Assistant	(Verified) Opera Software AS	C:\Users\László\AppData\Local\Programs\Opera\assi...
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> IASstoricon	Delayed launcher	(Verified) Intel(R) Rapid Storage Tec...	C:\Program Files\Intel\Intel(R) Rapid Storage Technol...
<input checked="" type="checkbox"/> RTHDVCPL	Realtek HD Audio Manager	(Verified) Realtek Semiconductor C...	C:\Program Files\Realtek\Audio\HDA\RtkNGUI64.exe
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell			
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			
<input checked="" type="checkbox"/> Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\96...
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> TeamsMachineInstaller	Microsoft Teams	(Verified) Microsoft Corporation	C:\Program Files (x86)\Teams Installer\Teams.exe

Ready

d) Security Utilities (LogonSession): Megmutatja, hogy hány aktív bejelentkezés van a számítógépen. Egy parancssoros programról van szó. Az én számítógémemen ahogy megnyitottam, egyből be is zárult, így a következő képet erről a [linkről](#) szúrtam be.



```
Administrator: Windows PowerShell
LogonSessions v1.4 - Lists logon session information
Copyright (C) 2004-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
    User name: WORKGROUP\DESKTOP-NBNJV7R$
    Auth package: NTLM
    Logon type: (none)
    Session: 0
    Sid: S-1-5-18
    Logon time: 4/3/2017 5:11:29 AM
    Logon server:
    DNS Domain:
    UPN:

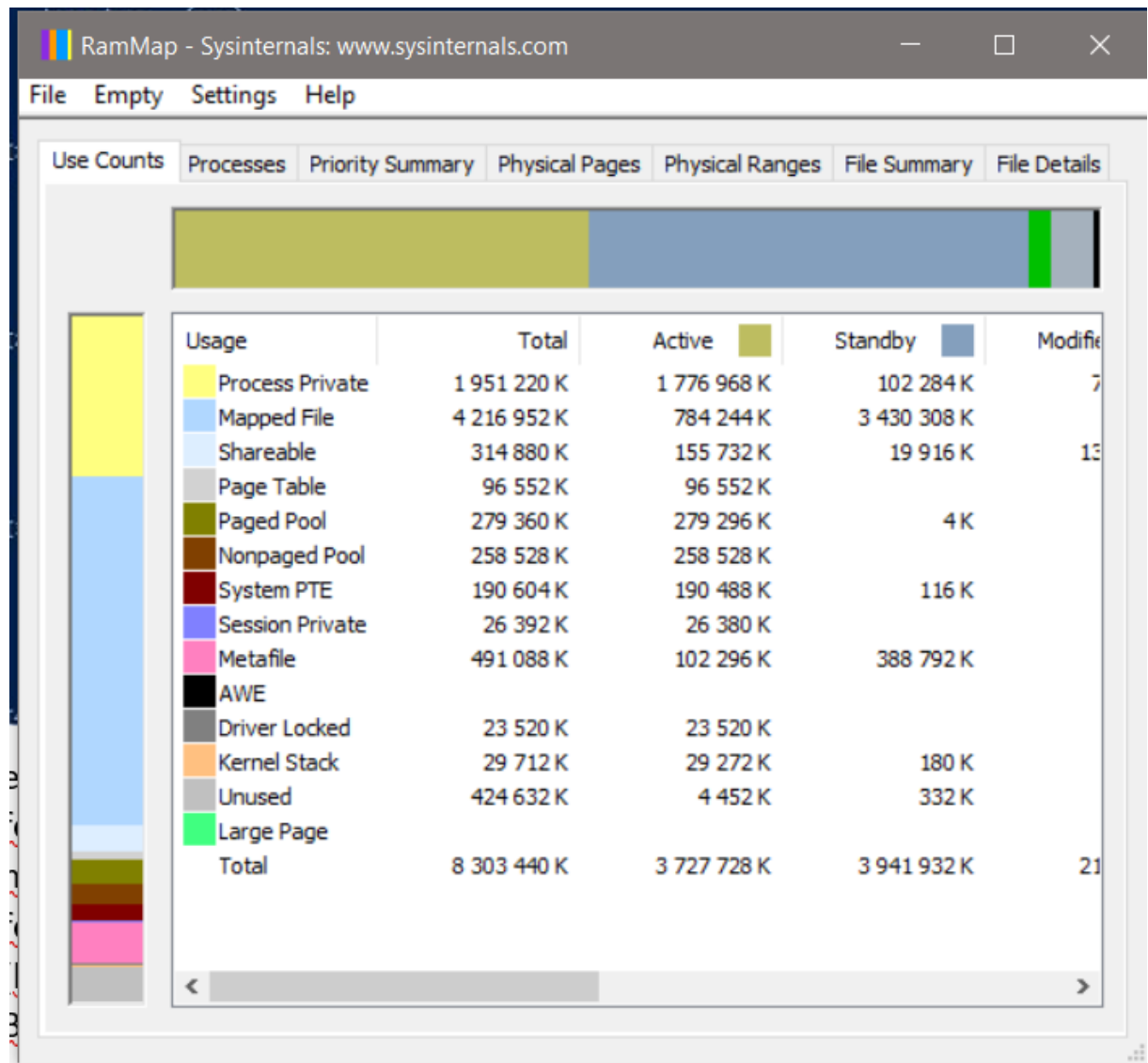
[1] Logon session 00000000:00009ac6:
    User name:
    Auth package: NTLM
    Logon type: (none)
    Session: 0
    Sid: (none)
    Logon time: 4/3/2017 5:11:29 AM
    Logon server:
    DNS Domain:
    UPN:

[2] Logon session 00000000:000003e4:
    User name: WORKGROUP\DESKTOP-NBNJV7R$
    Auth package: Negotiate
    Logon type: Service
    Session: 0
    Sid: S-1-5-20
    Logon time: 4/3/2017 5:11:29 AM
    Logon server:
    DNS Domain:
    UPN:

[3] Logon session 00000000:0000f8b6:
    User name: Window Manager\DM-1
    Auth package: Negotiate
    Logon type: Interactive
    Session: 1
    Sid: S-1-5-90-0-1
    Logon time: 4/3/2017 5:11:29 AM
    Logon server:
    DNS Domain:
    UPN:

[4] Logon session 00000000:0000f8ee:
```

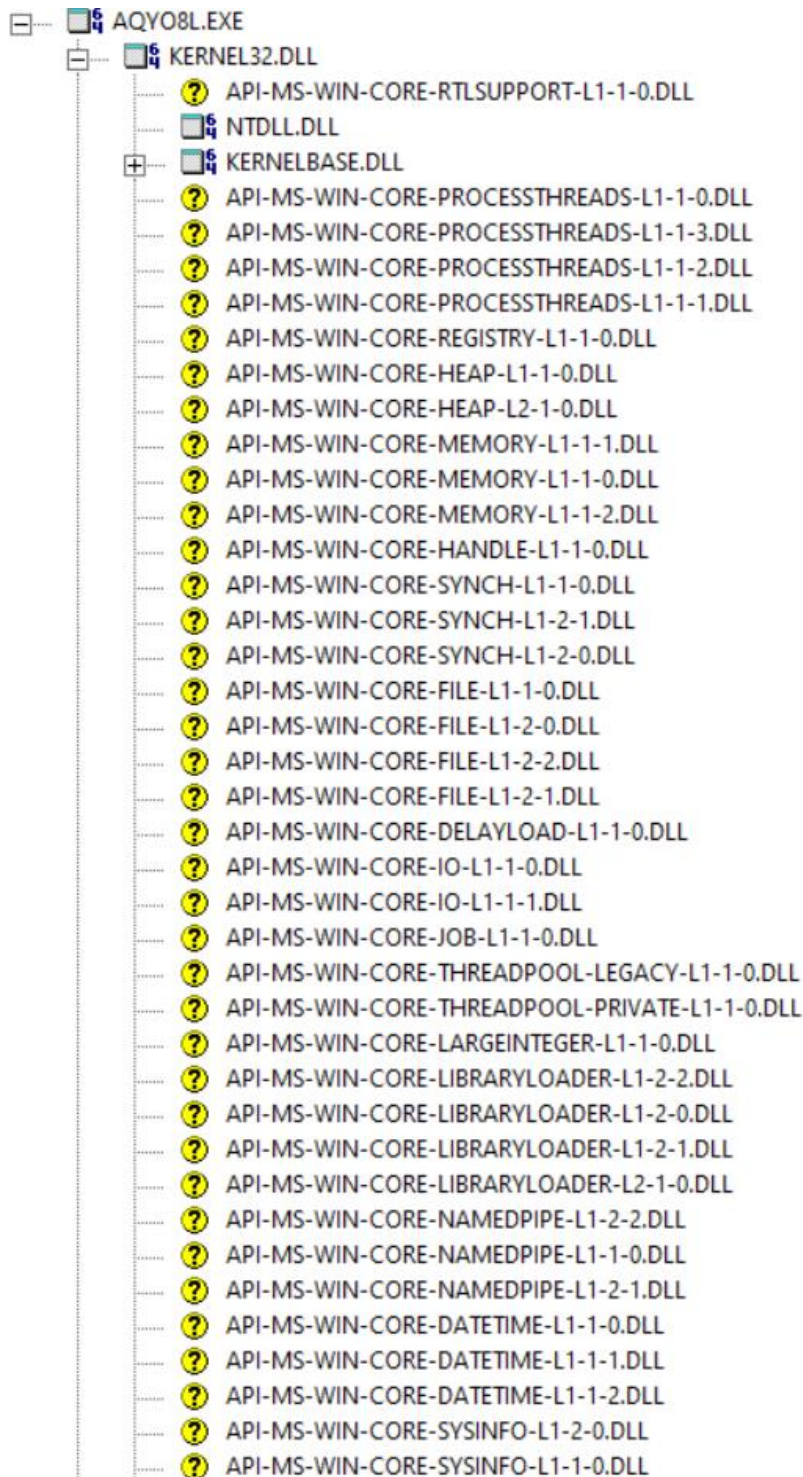
e) Information Utilities (RAMMap): A RAMMap megmutatja folyamattípusokra bontva a memóriahasználatot, lefoglalt és aktívan használt memóriaterület szempontjából. Meg lehet benne tekinteni folyamatokra lebontva a memóriahasználatot. Megmutatja egy-egy fizikai (hexadecimális) memóriacím állapotát, prioritását, folyamat típusát. Betekintést nyújt a fizikai memóriacímek tartományába, ahol megnézhetjük melyik tartomány mekkora területet foglal el a memórián. Kiírja a folyamatok és az általuk használt fájlok memóriahasználatát. Valamint megtudhatjuk, hogy melyik fájl mely memóriacímeket birtokolja.



### 3. Feladat:

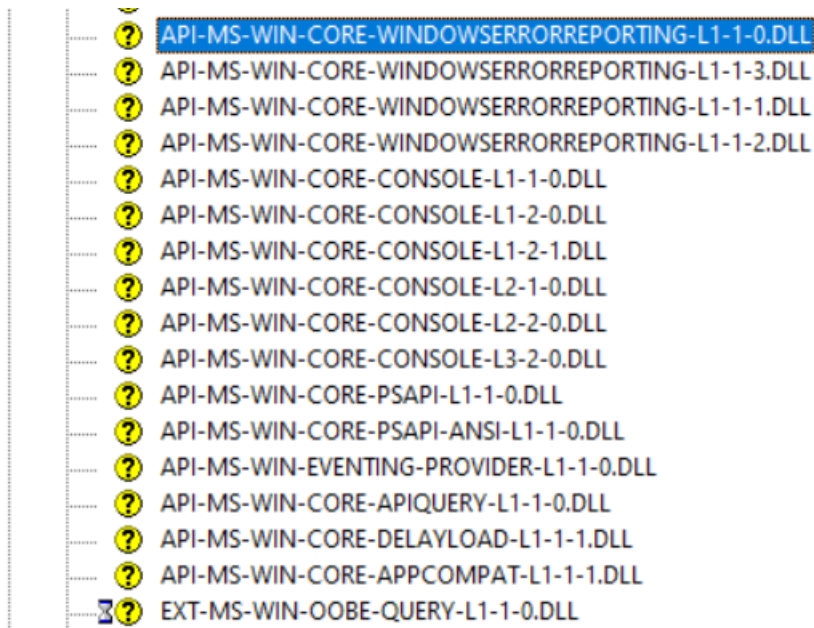
Töltse le a következő programot: Dependency Walker

a) AQYO8L.exe a következő hívásokat használja a Kernel-ből:



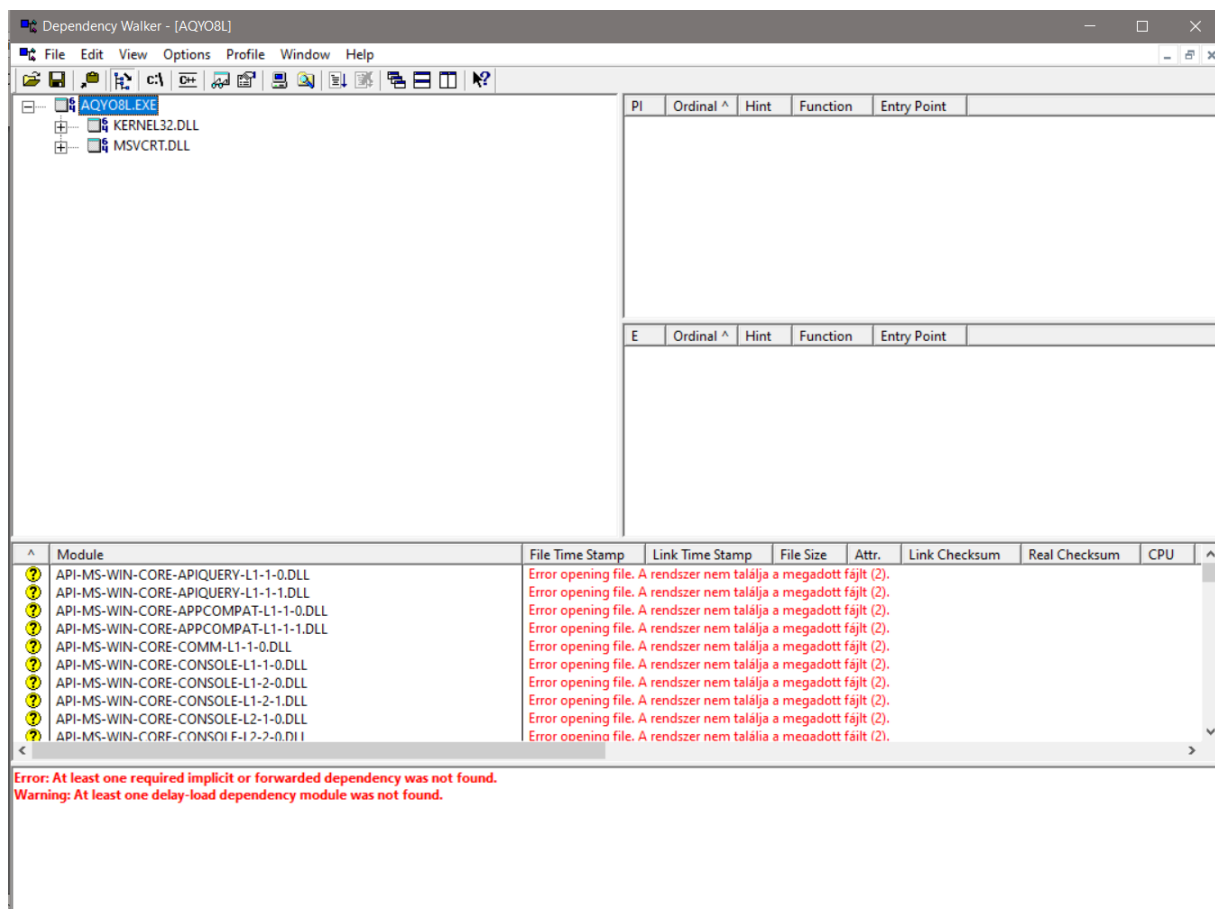


..... ? API-MS-WIN-CORE-SYSINFO-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-SYSINFO-L1-2-3.DLL  
..... ? API-MS-WIN-CORE-SYSINFO-L1-2-1.DLL  
..... ? API-MS-WIN-CORE-TIMEZONE-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-LOCALIZATION-L1-2-0.DLL  
..... ? API-MS-WIN-CORE-PROCESSSNAPSHOT-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-PROCESSENVIRONMENT-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-PROCESSENVIRONMENT-L1-2-0.DLL  
..... ? API-MS-WIN-CORE-STRING-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-DEBUG-L1-1-1.DLL  
..... ? API-MS-WIN-CORE-DEBUG-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-ERRORHANDLING-L1-1-3.DLL  
..... ? API-MS-WIN-CORE-FIBERS-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-UTIL-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-PROFILE-L1-1-0.DLL  
..... ? API-MS-WIN-SECURITY-BASE-L1-1-0.DLL  
..... ? API-MS-WIN-SECURITY-BASE-L1-2-0.DLL  
..... ? API-MS-WIN-SECURITY-APPCONTAINER-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-COMM-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-REALTIME-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-WOW64-L1-1-1.DLL  
..... ? API-MS-WIN-CORE-WOW64-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-WOW64-L1-1-3.DLL  
..... ? API-MS-WIN-CORE-SYSTEMTOPOLOGY-L1-1-1.DLL  
..... ? API-MS-WIN-CORE-SYSTEMTOPOLOGY-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-PROCESSTOPOLOGY-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-NAMESPACE-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-FILE-L2-1-2.DLL  
..... ? API-MS-WIN-CORE-FILE-L2-1-0.DLL  
..... ? API-MS-WIN-CORE-FILE-L2-1-3.DLL  
..... ? API-MS-WIN-CORE-FILE-L2-1-1.DLL  
..... ? API-MS-WIN-CORE-XSTATE-L2-1-0.DLL  
..... ? API-MS-WIN-CORE-XSTATE-L2-1-1.DLL  
..... ? API-MS-WIN-CORE-LOCALIZATION-L2-1-0.DLL  
..... ? API-MS-WIN-CORE-NORMALIZATION-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-FIBERS-L2-1-0.DLL  
..... ? API-MS-WIN-CORE-FIBERS-L2-1-1.DLL  
..... ? API-MS-WIN-CORE-LOCALIZATION-PRIVATE-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-SIDEBYSIDE-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL  
..... ? API-MS-WIN-CORE-WINDOWSErrorReporting-L1-1-0.DLL



Látható a képeken, hogy nagyon sok API hívást használ egy egyszerű C-ben megírt program.

- b) NTDLL.dll szerepe: Az NTDLL.dll az NT rendszer funkciókat tartalmazza, gépi kódon megírva. NT Layer DLL folyamatként fut a számítógépen és indításkor a RAM-ba töltődik be.



Ahogy a képen is látható, a Kernel-ből és az MSVCRT.DLL-ből hív meg függvényeket a program.

A Dependency Walker képes .exe fájlok futtatásához szükséges függvények kimutatására, megmutatja milyen API-k meghívása szükséges a program futásához és kiírja az API-k hexadecimális kódját is. Ezenkívül ha kétszer kattintunk egy elemre, akkor megnyitja a böngészőben az adott elem leírását a Microsoft oldalán. (Ez csak elmélet, Windows 10-en csak a Microsoft oldal keresőjét hozza be.)