

Operációs rendszerek Bsc

2. Gyak.
2022.02.20.

Készítette:

Mezei Gréta

Gazdaságinformatikus

WY9VBO

Miskolc, 2022

1.feladat

a,

```
PS C:\Users\mezei> tree C:\WY9VB0
Folder PATH listing for volume OS
Volume serial number is 0000000C EC74:258A
C:\WY9VB0
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   └── korte
└── land
    ├── kokusz
    └── szeder
PS C:\Users\mezei>
```

b,

```
PS C:\Users\mezei> cp c:\WY9VB0\land\szeder C:\WY9VB0\fa
PS C:\Users\mezei> tree C:\WY9VB0
Folder PATH listing for volume OS
Volume serial number is 00000067 EC74:258A
C:\WY9VB0
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   ├── korte
│   └── szeder
└── land
    ├── kokusz
    └── szeder
PS C:\Users\mezei> cp C:\WY9VB0\bokor\banan C:\WY9VB0\fa
PS C:\Users\mezei> tree C:\WY9VB0
Folder PATH listing for volume OS
Volume serial number is 000000A0 EC74:258A
C:\WY9VB0
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   ├── banan
│   ├── korte
│   └── szeder
└── land
    ├── kokusz
    └── szeder
PS C:\Users\mezei>
```

C,

```
PS C:\Users\mezei> move-item C:\WY9VB0\bokor\barack C:\WY9VB0\fa
PS C:\Users\mezei> tree C:\WY9VB0
Folder PATH listing for volume OS
Volume serial number is 00000061 EC74:258A
C:\WY9VB0
├── bokor
│   ├── banan
│   └── mogyoro
├── fa
│   ├── banan
│   ├── barack
│   ├── korte
│   └── szeder
└── land
    ├── kokusz
    └── szeder

PS C:\Users\mezei> move-item C:\WY9VB0\land\kokusz C:\WY9VB0\fa
PS C:\Users\mezei> tree C:\WY9VB0
Folder PATH listing for volume OS
Volume serial number is 0000007C EC74:258A
C:\WY9VB0
├── bokor
│   ├── banan
│   └── mogyoro
├── fa
│   ├── banan
│   ├── barack
│   ├── kokusz
│   ├── korte
│   └── szeder
└── land
    └── szeder

PS C:\Users\mezei>
```

d,

```
PS C:\Users\mezei> remove-item C:\WY9VB0\land
PS C:\Users\mezei> tree C:\WY9VB0
Folder PATH listing for volume OS
Volume serial number is 000000F6 EC74:258A
C:\WY9VB0
├── bokor
│   ├── banan
│   └── mogyoro
├── fa
│   ├── banan
│   ├── barack
│   ├── kokusz
│   ├── korte
│   └── szeder
└── land

PS C:\Users\mezei>
```

f,

```
PS C:\Users\mezei> Get-ChildItem C:\WY9VB0 -Force -Recurse
```

Directory: C:\WY9VB0

Mode	LastWriteTime	Length	Name
d-----	2022. 04. 01. 19:59		bokor
d-----	2022. 04. 12. 16:37		fa

Directory: C:\WY9VB0\bokor

Mode	LastWriteTime	Length	Name
d-----	2022. 04. 12. 16:33		banan
d-----	2022. 04. 01. 19:41		mogyoro

Directory: C:\WY9VB0\bokor\banan

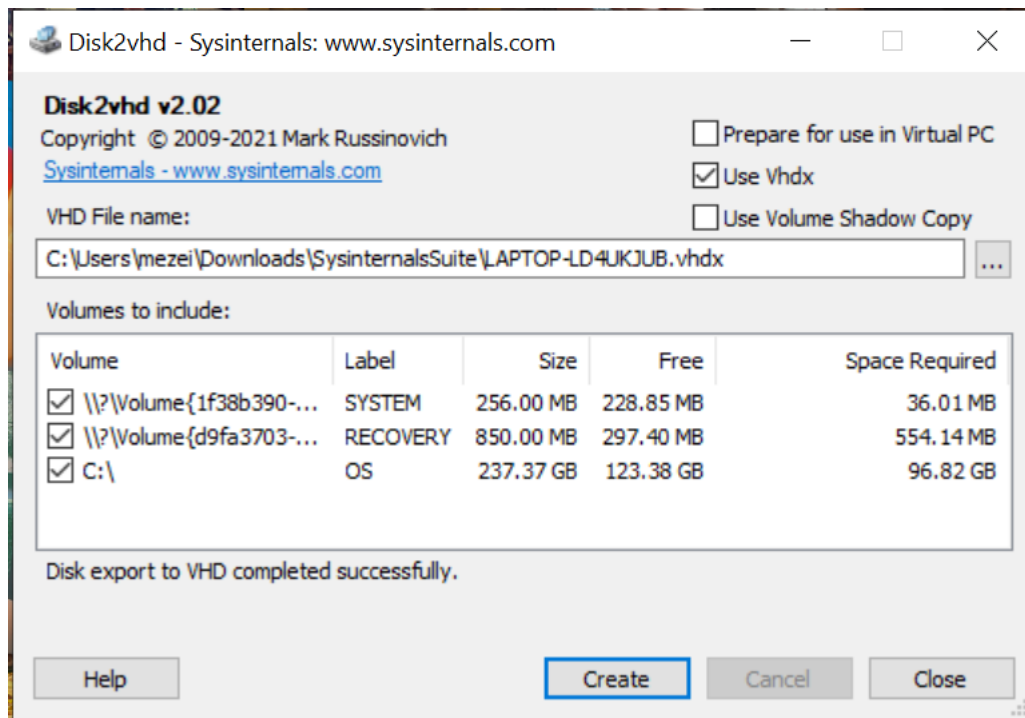
Mode	LastWriteTime	Length	Name
-a----	2022. 04. 12. 16:35	193	leiras.txt

Directory: C:\WY9VB0\fa

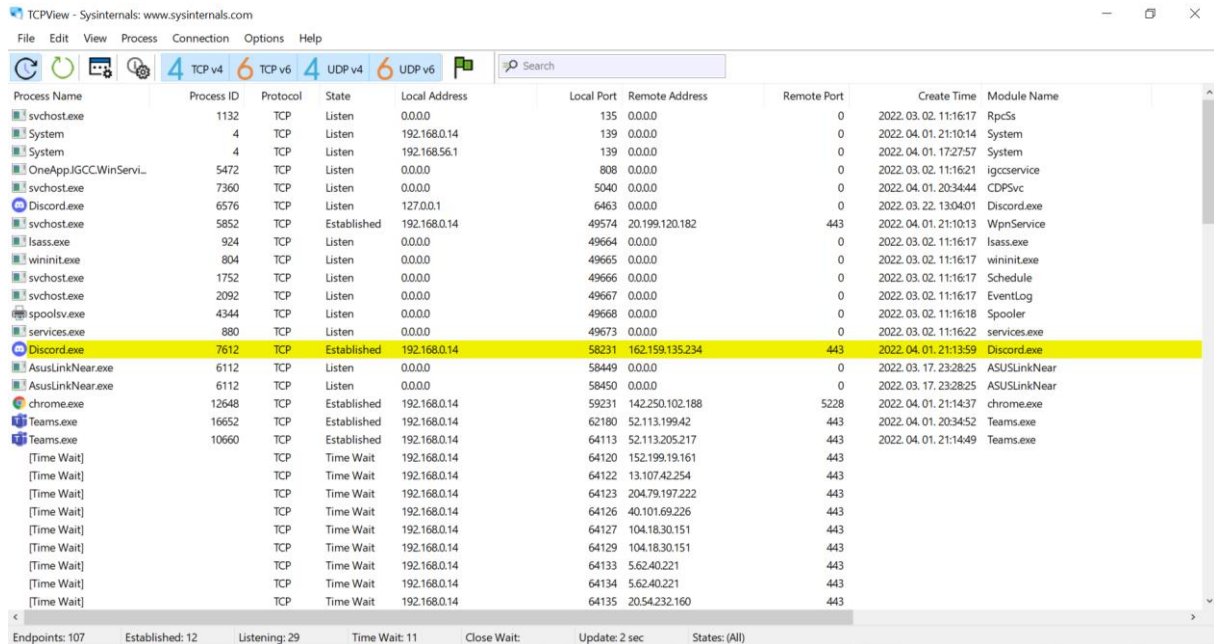
Mode	LastWriteTime	Length	Name
d-----	2022. 04. 01. 19:53		banan
d-----	2022. 04. 01. 19:41		barack
d-----	2022. 04. 01. 19:42		kokusz
d-----	2022. 04. 01. 19:42		korte
d-----	2022. 04. 01. 19:52		szeder
-a----	2022. 04. 12. 16:39	80	felsorolas.txt

2.feladat

a,



b,



C,

Process Explorer - Sysinternals: www.sysinternals.com [LAPTOP-LD4UKJUB\mezei]

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		8 864 K	51 540 K	100		
System Idle Process		60 K	8 K	0		
System	2.25	224 K	528 K	4		
Interrupts	7.88	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 064 K	0 K	472		
Memory Compression	0.38	3 368 K	150 772 K	2884		
csrss.exe		2 176 K	1 732 K	612		
wininit.exe		1 592 K	0 K	804		
services.exe	0.75	6 748 K	5 860 K	880		
svchost.exe	1.13	25 100 K	25 616 K	584	Windows-szolgáltatások gaz...	Microsoft Corporation
WmiPrvSE.exe		33 348 K	7 424 K	6960		
MoUsCoreWorker.exe		65 980 K	3 312 K	7704		
unsecapp.exe		1 540 K	1 772 K	11320		
StartMenuExperienceHos...		42 688 K	16 788 K	11892		
RuntimeBroker.exe		7 988 K	2 496 K	604	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	161 972 K	60 664 K	15596	Search application	Microsoft Corporation
RuntimeBroker.exe		19 428 K	23 888 K	13396	Runtime Broker	Microsoft Corporation
SettingSyncHost.exe		13 804 K	8 016 K	13372	Host Process for Setting Syn...	Microsoft Corporation
LockApp.exe	Susp...	14 932 K	340 K	13932	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		10 840 K	6 668 K	10732	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		8 204 K	9 748 K	15176	Runtime Broker	Microsoft Corporation
TextInputHost.exe		13 452 K	10 704 K	3672		Microsoft Corporation
ApplicationFrameHost.exe		15 664 K	3 784 K	11852	Application Frame Host	Microsoft Corporation
dllhost.exe		5 928 K	7 320 K	11372	COM Surrogate	Microsoft Corporation
SystemSettings.exe	Susp...	25 408 K	572 K	3576	Gépház	Microsoft Corporation
UserOOBEBroker.exe		2 716 K	3 384 K	5216	User OOBEBroker	Microsoft Corporation
dllhost.exe		2 368 K	9 728 K	5680	COM Surrogate	Microsoft Corporation
SDXHelperBgt.exe	Susp...	3 088 K	156 K	15632	Office SDX Helper Backgrou...	Microsoft Corporation
RuntimeBroker.exe		2 964 K	2 064 K	11180	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	Susp...	25 024 K	4 784 K	18052	Windows Shell Experience H...	Microsoft Corporation

CPU Usage: 38.77% Commit Charge: 52.32% Processes: 232 Physical Usage: 70.76%

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\windows.storage.dll	SUCCESS	Offset: 6 962 688, ...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\windows.storage.dll	SUCCESS	Offset: 6 962 688, ...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\ExplorerFrame.dll	SUCCESS	Offset: 1 937 920, ...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\shell32.dll	SUCCESS	Offset: 6 725 632, ...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\ExplorerFrame.dll	SUCCESS	Offset: 1 933 824, ...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\ExplorerFrame.dll	SUCCESS	Offset: 1 937 920, ...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\ExplorerFrame.dll	SUCCESS	Offset: 1 937 920, ...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\ExplorerFrame.dll	SUCCESS	Offset: 1 954 304, ...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\ExplorerFrame.dll	SUCCESS	Offset: 1 954 304, ...
21:20.3...	Explorer.EXE	10492	CreateFile	C:\Users\mezei\Downloads\Sysinternals...	SUCCESS	Desired Access: R...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\ExplorerFrame.dll	SUCCESS	Offset: 1 954 304, ...
21:20.3...	Explorer.EXE	10492	QueryBasicInfor...	C:\Users\mezei\Downloads\Sysinternals...	SUCCESS	CreationTime: 2022...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\ExplorerFrame.dll	SUCCESS	Offset: 1 954 304, ...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Users\mezei\Downloads\Sysinternals...	SUCCESS	Offset: 1 954 304, ...
21:20.3...	Explorer.EXE	10492	RegOpenKey	HKCU\Software\Microsoft\Windows\Curr...	NAME NOT FOUND	Desired Access: R...
21:20.3...	Explorer.EXE	10492	RegOpenKey	HKCU\Software\Microsoft\Windows\Curr...	NAME NOT FOUND	Desired Access: R...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 2 702 848, ...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 2 702 848, ...
21:20.3...	Isass.exe	924	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 607 168, ...
21:20.3...	Isass.exe	924	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 590 784, ...
21:20.3...	Isass.exe	924	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 513 472, ...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\user.dll	SUCCESS	Offset: 536 576, Le...
21:20.3...	Explorer.EXE	10492	RegOpenKey	HKCU	SUCCESS	Query: HandleTags...
21:20.3...	Explorer.EXE	10492	RegOpenKey	HKCU\Software\Microsoft\Windows\Curr...	NAME NOT FOUND	Desired Access: R...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 2 702 848, ...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\shlwapi.dll	SUCCESS	Offset: 312 832, Le...
21:20.3...	Isass.exe	924	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 578 496, ...
21:20.3...	Explorer.EXE	10492	CreateFile	C:\Users\mezei\Downloads\Sysinternals...	SUCCESS	Desired Access: R...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 2 711 040, ...
21:20.3...	Explorer.EXE	10492	QueryBasicInfor...	C:\Users\mezei\Downloads\Sysinternals...	SUCCESS	CreationTime: 2022...
21:20.3...	Explorer.EXE	10492	CloseFile	C:\Users\mezei\Downloads\Sysinternals...	SUCCESS	
21:20.3...	Isass.exe	924	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1 497 088, ...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 2 547 200, ...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\user.dll	SUCCESS	Offset: 524 288, Le...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 3 480 064, ...
21:20.3...	Explorer.EXE	10492	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 2 551 296, ...

Autoruns - Sysinternals: www.sysinternals.com

File Search Entry Options Category Help

Quick Filter

Autoruns Entry	Description	Publisher	Image Path	Tir ^
Logon				
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Th
<input checked="" type="checkbox"/> AvastBrowserAutoLaunch_905F062F31CC832A770572A6BCB2FCB	Avast Secure Browser	(Verified) Avast Software s.r.o.	C:\Program Files (x86)\AVAST Software\Browser\Application\AvastBrowser...	Mc
<input checked="" type="checkbox"/> btweb	File not found: "C:\Users\mezei\AppData\Roaming\BitTorrent Web\btweb..."			
<input checked="" type="checkbox"/> MicrosoftEdgeAutoLaunch_1DDC428AA738F73EB30050C1A598CF...	Microsoft Edge	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Su
<input checked="" type="checkbox"/> Taskbar system	Taskbar system	(Verified) Globalhop Ltd TOO	C:\Users\mezei\AppData\Local\Programs\Taskbar system\TaskbarSystem.exe	W
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce				
<input checked="" type="checkbox"/> Delete Cached Standalone Update Binary	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Th
<input checked="" type="checkbox"/> Delete Cached Update Binary	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Th
<input checked="" type="checkbox"/> Uninstall 22.045.0227.0004	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Th
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Sa
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				
<input checked="" type="checkbox"/> Avast Secure Browser	Avast Browser Installer	(Verified) Avast Software s.r.o.	C:\Program Files (x86)\AVAST Software\Browser\Application\99.0.15399.85\...	Mc
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	(Verified) Google LLC	C:\Program Files (x86)\Google\Chrome\Application\100.0.4896.75\Installer...	Mc
<input checked="" type="checkbox"/> Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\100.0.1185.39\Installer...	Tu
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Sa
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				
<input checked="" type="checkbox"/> CanonQuickMenu	Canon Quick Menu	(Verified) Canon Inc.	C:\Program Files (x86)\Canon\Quick Menu\CNQMMAIN.EXE	W

e,

RamMap - Sysinternals: www.sysinternals.com

File Empty Settings Help

Use Counts Processes Priority Summary Physical Pages Physical Ranges File Summary File Details

Usage	Total	Active	Standby	Modified	Modified ...	Transition	Zeroed	Free	Bad
Process Private	1 372 180 K	1 139 772 K	114 656 K	117 624 K		128 K			
Mapped File	1 265 624 K	401 532 K	862 536 K	1 556 K					
Shareable	187 300 K	65 976 K	7 428 K	113 896 K					
Page Table	116 712 K	116 712 K							
Paged Pool	189 716 K	184 244 K	4 820 K	652 K					
Nonpaged Pool	385 912 K	385 912 K							
System PTE	157 104 K	157 016 K	88 K						
Session Private	49 268 K	48 660 K	608 K						
Metafile	32 780 K	23 460 K	9 304 K	4 K	12 K				
AWE									
Driver Locked	43 508 K	43 508 K							
Kernel Stack	40 460 K	40 132 K	64 K	264 K					
Unused	165 004 K	10 932 K	52 K				124 208 K	29 812 K	
Large Page									
Total	4 005 568 K	2 617 856 K	999 556 K	233 996 K	12 K	128 K	124 208 K	29 812 K	