

Operációs rendszerek BSc

1. Gyak.

2022. 02. 08.

Készítette:

Zarándi Ákos Bsc

Gazdaságinformatikus

DX6C4R

1.

a)

```
D:\>md D:\DX6C4R\bokor\mogyoro

D:\>md D:\DX6C4R\bokor\barack

D:\>md D:\DX6C4R\fa\korte

D:\>md D:\DX6C4R\land\szeder

D:\>md D:\DX6C4R\land\kokusz

D:\>tree DX6C4R
Folder PATH listing
Volume serial number is 000000B1 D6E7:8ABB
D:\DX6C4R
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
├── land
│   ├── kokusz
│   └── szeder
└──
```

D:\>md D:\DX6C4R\fa\korte

```
D:\>tree DX6C4R
Folder PATH listing
Volume serial number is 000000B9 D6E7:8ABB
D:\DX6C4R
├── bokor
│   ├── banan
│   ├── barack
│   └── mogyoro
├── fa
│   └── korte
├── land
│   ├── kokusz
│   └── szeder
└──
```

2. feladat

Disk2vhd v2.02
 Copyright © 2009-2021 Mark Russinovich
[Sysinternals - www.sysinternals.com](http://www.sysinternals.com)

VHD File name: ☐ Prepare for use in Virtual PC
☒ Use Vhdx
☐ Use Volume Shadow Copy

Volumes to include:

Volume	Label	Size	Free	Space Required
<input checked="" type="checkbox"/> \\?\Volume{4e8ad122-...}	[No Label]	96.00 MB	45.51 MB	56.01 MB
<input checked="" type="checkbox"/> \\?\Volume{f877a36b-...}	[No Label]	506.00 MB	82.78 MB	420.10 MB
<input checked="" type="checkbox"/> C:\	[No Label]	237.86 GB	13.24 GB	204.67 GB
<input checked="" type="checkbox"/> D:\	[No Label]	931.48 GB	110.47 GB	821.35 GB

A fizikai tárhelyet átalakítja virtuális tárhellyé és mint látható nekem van még bőven helyem

TCPView - Sysinternals: www.sysinternals.com

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets	Recv Packets
svchost.exe	1296	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2022.02.04.17:53:35	RpcSs		
System	4	TCP	Listen	192.168.122.142	139	0.0.0.0	0	2022.02.15.14:05:38	System		
System	4	TCP	Listen	192.168.122.142	139	0.0.0.0	0	2022.02.15.14:05:37	System		
OriginWebHelperServ...	4936	TCP	Listen	127.0.0.1	3213	0.0.0.0	0	2022.02.04.17:53:39	Origin Web Helper Service		
svchost.exe	7244	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2022.02.15.14:05:35	CDPSvc		
mDNSResponder.exe	4636	TCP	Listen	127.0.0.1	5354	0.0.0.0	0	2022.02.04.17:53:36	Bonjour Service		
TeamViewer_Service.exe	4952	TCP	Listen	127.0.0.1	5939	0.0.0.0	0	2022.02.04.17:53:39	TeamViewer		
Discord.exe	8080	TCP	Listen	127.0.0.1	6463	0.0.0.0	0	2022.02.15.14:11:48	Discord.exe		
AppleMobileDeviceSer...	4592	TCP	Listen	127.0.0.1	27015	0.0.0.0	0	2022.02.04.17:53:36	Apple Mobile Device Service		
AppleMobileDeviceSer...	4592	TCP	Established	127.0.0.1	27015	127.0.0.1	52615	2022.02.15.14:06:02	Apple Mobile Device Service		
steam.exe	14716	TCP	Listen	0.0.0.0	27036	0.0.0.0	0	2022.02.15.14:05:39	steam.exe		
steam.exe	14716	TCP	Listen	127.0.0.1	27060	0.0.0.0	0	2022.02.15.14:39:34	steam.exe		
DiscSoftBusServiceLite...	16752	TCP	Listen	0.0.0.0	45769	0.0.0.0	0	2022.02.04.17:54:09	DiscSoftBusServiceLite.exe		
svchost.exe	4920	TCP	Established	192.168.122.142	49474	20.199.120.85	443	2022.02.15.14:05:39	WpnService		
lsass.exe	1004	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2022.02.04.17:53:35	lsass.exe		
wininit.exe	948	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2022.02.04.17:53:35	wininit.exe		
svchost.exe	1672	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2022.02.04.17:53:35	Schedule		
svchost.exe	1460	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2022.02.04.17:53:35	Eventlog		
spoolsv.exe	3348	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	2022.02.04.17:53:36	Spooler		
nvcontainer.exe	4864	TCP	Established	127.0.0.1	49671	127.0.0.1	65001	2022.02.15.14:05:38	nvcontainer.exe		
services.exe	996	TCP	Listen	0.0.0.0	49672	0.0.0.0	0	2022.02.04.17:53:39	services.exe		
NVIDIA Web Helper.exe	21372	TCP	Listen	127.0.0.1	51244	0.0.0.0	0	2022.02.15.14:05:56	NVIDIA Web Helper.exe		
NVIDIA Web Helper.exe	21372	TCP	Established	127.0.0.1	51244	127.0.0.1	53990	2022.02.15.14:05:59	NVIDIA Web Helper.exe		
iTunesHelper.exe	23524	TCP	Established	127.0.0.1	52615	127.0.0.1	27015	2022.02.15.14:06:02	iTunesHelper.exe		
Discord.exe	14892	TCP	Established	192.168.122.142	53015	162.158.130.234	443	2022.02.15.14:57:05	Discord.exe	48	
NVIDIA Share.exe	9016	TCP	Established	127.0.0.1	53990	127.0.0.1	51244	2022.02.15.14:05:59	NVIDIA Share.exe		
Skype.exe	21768	TCP	Established	192.168.122.142	56427	52.149.21.60	443	2022.02.15.15:42:26	Skype.exe		
WINWORD.EXE	3412	TCP	Established	192.168.122.142	56428	52.109.12.20	443	2022.02.15.15:45:59	WINWORD.EXE		
svchost.exe	4608	TCP	Established	192.168.122.142	56429	84.53.161.186	80	2022.02.15.15:35:00	CryptSvc		
chrome.exe	22192	TCP	Established	192.168.122.142	56430	52.149.21.60	443	2022.02.15.15:35:11	chrome.exe		
OriginWebHelperServ...	4936	TCP	Established	192.168.122.142	56432	104.80.234.144	443	2022.02.15.15:35:33	Origin Web Helper Service	3	8
Skype.exe	21768	TCP	Established	192.168.122.142	56436	52.149.21.60	443	2022.02.15.15:42:12	Skype.exe	1	1
WINWORD.EXE	3412	TCP	Established	192.168.122.142	56437	2.22.22.112	443	2022.02.15.15:43:13	WINWORD.EXE		
WINWORD.EXE	3412	TCP	Established	192.168.122.142	56438	2.22.22.112	443	2022.02.15.15:43:13	WINWORD.EXE		
WINWORD.EXE	3412	TCP	Established	192.168.122.142	56439	2.22.22.112	443	2022.02.15.15:43:13	WINWORD.EXE		
WINWORD.EXE	3412	TCP	Established	192.168.122.142	56440	2.22.22.112	443	2022.02.15.15:43:13	WINWORD.EXE		

Endpoints: 184 Established: 63 Listening: 34 Time Wait: 11 Close Wait: 2 Update: 2 sec States: (All)

Részletesen megmutatja a TCP és az UDP végpontokat a rendszeren

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

Network Providers | Scheduled Tasks | Services | Drivers | Codex | Boot Execute | Image Hijacks | AppBirt | KnowIDLLs | Winlogon | Winsock Providers | Print Monitors | LSA Providers

Autorun Entry	Description	Publisher	Image Path	Timestamp	Virus Total
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				2019.12.07.10.15	
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	1953.12.11.3.58	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021.07.28.23.11	
<input checked="" type="checkbox"/> iTunesHelper	iTunesHelper	(Verified) Apple Inc.	c:\program files\itunes\itunesh...	2020.11.12.13.42	
<input checked="" type="checkbox"/> Riot Vanguard	Vanguard tray notification	(Verified) Riot Games, Inc.	c:\program files\riot vanguard...	2021.11.30.3.43	
<input checked="" type="checkbox"/> RtkAudService	Realtek HD Audio Universal ...	(Verified) Realtek Semiconductor	c:\windows\system32\rtkaudi...	2020.02.06.8.58	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2020.11.25.12.13	
<input checked="" type="checkbox"/> LogMeln Hamac...	Hamachi Client Application	(Verified) LogMeln, Inc.	c:\program files (x86)\logmei...	2019.04.02.15.58	
<input checked="" type="checkbox"/> SunJavaUpdate	Java Update Scheduler	(Verified) Oracle America, Inc.	c:\program files (x86)\commo...	2020.09.16.21.51	
<input checked="" type="checkbox"/> TeamViewer	TeamViewer		File not found: C:\Program Fi...		
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021.12.27.8.05	
<input checked="" type="checkbox"/> CCXProcess	CCXProcess	(Verified) Adobe Inc.	c:\program files (x86)\adobe\...	2019.11.27.0.11	
<input checked="" type="checkbox"/> com.blitz.app	Blitz	(Not verified) Blitz, Inc.	c:\users\b3lga\appdata\local...	2021.12.16.18.41	
<input checked="" type="checkbox"/> DAEMON Tools ...	DAEMON Tools Lite Agent	(Verified) AVB Disc Soft, SIA	c:\program files\daemon tool...	2021.10.19.8.52	
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	c:\users\b3lga\appdata\local...	1946.05.04.20.33	
<input checked="" type="checkbox"/> Overwolf	Overwolf Launcher	(Verified) Overwolf Ltd	c:\program files (x86)\overwo...	2021.12.14.13.57	
<input checked="" type="checkbox"/> Steam	Steam	(Verified) Valve Corp.	c:\program files (x86)\steam\...	2022.01.16.18.37	
<input checked="" type="checkbox"/> MWeb			File not found: C:\Users\b3lga...		
<input checked="" type="checkbox"/> Web Companion			File not found: C:\Program Fi...		
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2020.11.08.8.40	
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	(Verified) Google LLC	c:\program files\google\chro...	2022.02.11.21.56	
<input checked="" type="checkbox"/> Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	c:\program files (x86)\microso...	2022.03.01.19.43	
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY ...	(Verified) Microsoft Corporation	c:\windows\system32\mscon...	2019.10.25.4.45	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				2020.09.04.15.35	
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY ...	(Verified) Microsoft Corporation	c:\windows\syswow64\mscon...	2019.10.25.9.48	
HKLM\SOFTWARE\Classes\Protocols\Run				2022.03.05.10.56	
<input checked="" type="checkbox"/> iwdnt	Microsoft Office XML MME Fil...	(Verified) Microsoft Corporation	c:\program files\microsoft off...	2022.02.01.17.29	
HKLM\SOFTWARE\Classes\Protocols\Handler				2022.03.05.10.56	
<input checked="" type="checkbox"/> mso-minib-roam...	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft off...	2022.02.01.17.08	
<input checked="" type="checkbox"/> mso-minib.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft off...	2022.02.01.17.08	
<input checked="" type="checkbox"/> mso-roaming.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft off...	2022.02.01.17.08	
<input checked="" type="checkbox"/> mso.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft off...	2022.02.01.17.08	
HKLM\Software\Classes\ShellEx\ContextMenuHandlers				2020.09.16.19.22	
<input checked="" type="checkbox"/> AccExt	Core Sync	(Verified) Adobe Systems Inc.	c:\program files (x86)\commo...	2018.03.05.16.02	
<input checked="" type="checkbox"/> ANotead++64	ShellHandler for Notead++ (...)	(Verified) Notead++	c:\oroom files (x86)\notead...	2014.05.12.10.49	

Ready.

Signed Windows Entries Hidden.

Megmutatja mely programok indulnak automatikusan amikor a rendszer beindul.

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	4 284 908 K	4 075 912 K	72 836 K	136 136 K					
Mapped File	9 222 636 K	1 543 112 K	7 562 876 K	116 648 K					
Shareable	397 544 K	182 996 K	73 096 K	141 452 K					
Page Table	147 044 K	147 044 K							
Paged Pool	460 544 K	419 200 K	14 984 K	26 360 K					
Nonpaged Pool	492 300 K	492 300 K							
System PTE	372 804 K	372 676 K	128 K						
Session Private	89 992 K	89 856 K	16 K	120 K					
Metafile	534 844 K	139 628 K	395 216 K						
AWE									
Driver Locked	32 900 K	32 900 K							
Kernel Stack	77 348 K	74 476 K	880 K	1 992 K					
Unused	433 092 K	9 720 K	68 K	8 K			398 636 K	24 660 K	
Large Page									
Total	16 565 956 K	7 599 820 K	8 120 100 K	422 716 K			398 636 K	24 660 K	

Megmutatja a ram használatát különböző alkalmazásokban/helyeken.