

Operációs rendszerek BSc

3. gyak

2021.02.24.

Készítette:

Varga-Molnár Bertalan

PY7QFH

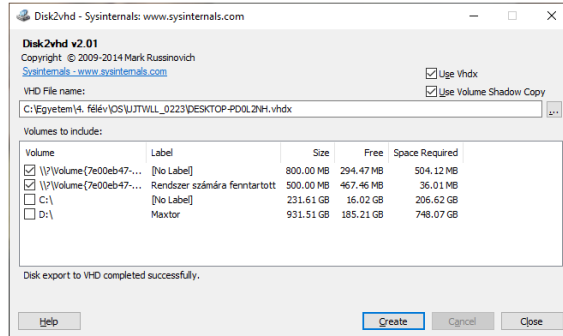
Programtervező informatikus

1. Windows belső működésének tanulmányozása:
Sysinternals Suite fájlcsomag letöltésre került.

2. Sysinternals néhány programjának futtatása:

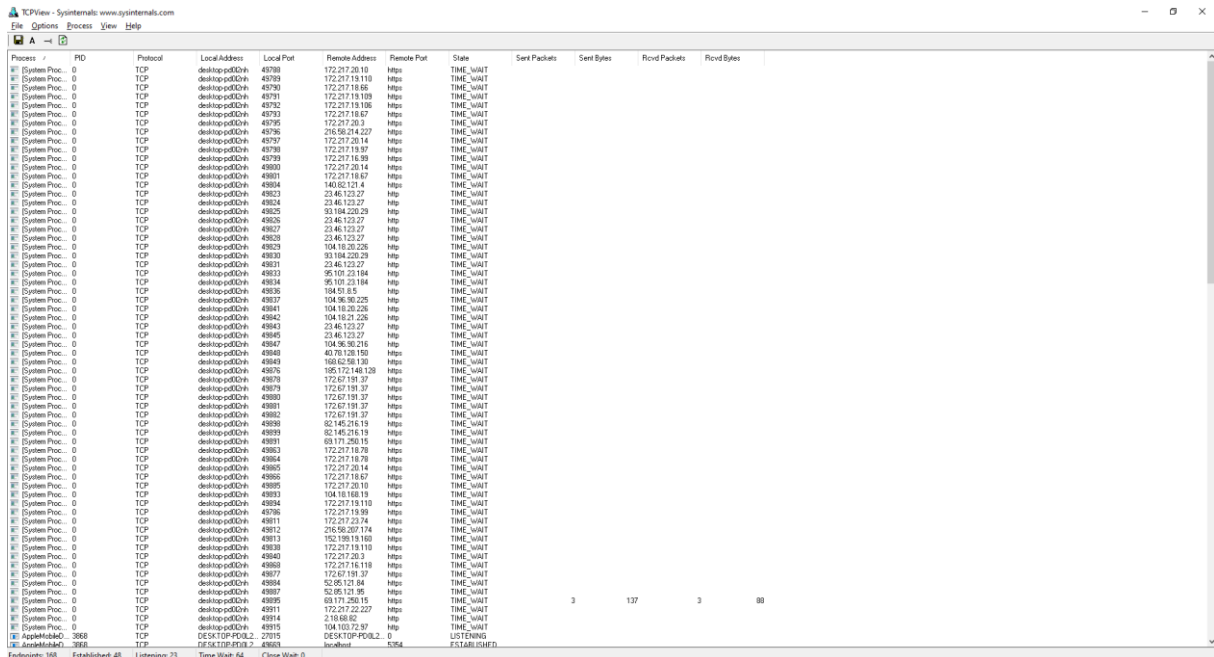
a. File and Disk Utilities:

Célja egy lemezképfájl létrehozása adott meghajtó(k)ról.



b. Networking Utilities:

Célja a processzekhez tartozó hálózati kapcsolatok adatainak összesítése.



c. Process Utilities:

Célja a processzek és adatainak listázása.

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-PD0L2NH;Mark]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry	11.292 K	108 228 K	124			
System Idle Process	86.84	60 K	8 K	0		
System	0.26	200 K	1 268 K	4		
smss.exe	0.20	0 K	n/a		Hardware Interrupts and DPCs	
Memory Compression		1 124 K	1 212 K	460		
csrss.exe		76 K	4 236 K	2668		
carss.exe	< 0.01	1 816 K	5 404 K	668		
winit.exe		1 720 K	6 840 K	1008		
services.exe	0.36	5 376 K	10 188 K	728		
WinFhVSE.exe	< 0.01	12 300 K	31 096 K	932	Windows-szolgáltatások gaz...	Microsoft Corporation
WinFhVSE.exe		5 760 K	13 552 K	4848		
StartMenuExperience		58 372 K	95 676 K	8676		
RuntimeBroker.exe	< 0.01	7 340 K	27 464 K	7244	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	153 792 K	222 604 K	7436	Search application	Microsoft Corporation
RuntimeBroker.exe		8 256 K	29 072 K	7540	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	32 692 K	32 476 K	7624	YourPhone	Microsoft Corporation
LockApp.exe	Susp...	22 372 K	53 196 K	5620	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		9 820 K	34 480 K	8388	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		4 240 K	17 632 K	8644	Runtime Broker	Microsoft Corporation
dlhost.exe		5 816 K	12 768 K	9068	COM Surrogate	Microsoft Corporation
dlhost.exe		3 848 K	10 788 K	2992		
RuntimeBroker.exe		2 924 K	13 548 K	8292	Runtime Broker	Microsoft Corporation
Calculator.exe	Susp...	31 724 K	48 448 K	10864		
ApplicationFrameHost...		20 028 K	33 792 K	10876	Application Frame Host	Microsoft Corporation
RuntimeBroker.exe		1 844 K	8 424 K	10984	Runtime Broker	Microsoft Corporation
TextInputHost.exe	< 0.01	20 900 K	48 776 K	11208		
RuntimeBroker.exe		8 264 K	35 504 K	11040	Runtime Broker	Microsoft Corporation
BackgroundTaskHost	Susp...	6 784 K	28 960 K	11224	Background Task Host	Microsoft Corporation
BackgroundTaskHost	Susp...	11 636 K	31 140 K	9504	Background Task Host	Microsoft Corporation

CPU Usage: 13.16% Commit Charge: 21.78% Processes: 165 Physical Usage: 23.40%

Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
18:44...	svchost.exe	2228	ReadFile	C:\Windows\System32\StateRepository\...	SUCCESS	Offset: 690 688, Le...
18:44...	svchost.exe	2228	ReadFile	C:\Windows\System32\StateRepository\...	SUCCESS	Offset: 678 400, Le...
18:44...	svchost.exe	2228	ReadFile	C:\Windows\System32\StateRepository\...	SUCCESS	Offset: 635 904, Le...
18:44...	svchost.exe	2228	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
18:44...	svchost.exe	2228	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 124, Length...
18:44...	svchost.exe	2228	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
18:44...	svchost.exe	2228	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 124, Length...
18:44...	Explorer.EXE	920	ReadFile	C:\Windows\System32\shlwapi.dll	SUCCESS	Offset: 312 832, Le...
18:44...	MsMpEng.exe	3268	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 942 208...
18:44...	Core.exe	8808	ReadFile	C:\Windows\System32\IHLAPI.DLL	SUCCESS	Offset: 210 432, Le...
18:44...	MsMpEng.exe	3268	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 446 592...
18:44...	Core.exe	8808	ReadFile	C:\Windows\System32\IHLAPI.DLL	SUCCESS	Offset: 187 904, Le...
18:44...	MsMpEng.exe	3268	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 151 680...
18:44...	Core.exe	8808	ReadFile	C:\Program Files\Logitech Gaming Soft...	SUCCESS	Offset: 1 036 336...
18:44...	svchost.exe	2228	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
18:44...	MsMpEng.exe	3268	UnlockFileSingle	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 124, Length...
18:44...	svchost.exe	2228	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 124, Length...
18:44...	Core.exe	8808	ReadFile	C:\Program Files\Logitech Gaming Soft...	SUCCESS	Offset: 1 021 952...
18:44...	Core.exe	3268	LockFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Exclusive: False, O...
18:44...	Explorer.EXE	920	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
18:44...	MsMpEng.exe	3268	UnlockFileSingle	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 124, Length...
18:44...	Core.exe	8808	LockFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Exclusive: False, O...
18:44...	Explorer.EXE	920	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
18:44...	MsMpEng.exe	3268	LockFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Exclusive: True, Of...
18:44...	Explorer.EXE	920	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
18:44...	Core.exe	8808	ReadFile	C:\Program Files\Logitech Gaming Soft...	SUCCESS	Offset: 865 280, Le...
18:44...	Explorer.EXE	920	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND Desired Access: R...	
18:44...	Explorer.EXE	920	RegOpenKey	HKCR\Applications\Promon64.exe	NAME NOT FOUND Desired Access: R...	
18:44...	Explorer.EXE	920	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
18:44...	Explorer.EXE	920	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
18:44...	Core.exe	8808	ReadFile	C:\Program Files\Logitech Gaming Soft...	SUCCESS	Offset: 5 403 648...
18:44...	Explorer.EXE	920	RegOpenKey	HKCR\Applications\Promon64.exe	NAME NOT FOUND Desired Access: R...	
18:44...	MsMpEng.exe	3268	WriteFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 654 472...
18:44...	MsMpEng.exe	3268	WriteFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 654 496...
18:44...	MsMpEng.exe	3268	WriteFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 658 592...
18:44...	MsMpEng.exe	3268	WriteFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 658 616...
18:44...	Core.exe	8808	ReadFile	C:\Program Files\Logitech Gaming Soft...	SUCCESS	Offset: 3 342 208...
18:44...	MsMpEng.exe	3268	WriteFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 662 712...
18:44...	MsMpEng.exe	3268	WriteFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 662 736...
18:44...	MsMpEng.exe	3268	WriteFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 666 832...
18:44...	MsMpEng.exe	3268	WriteFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 3 666 856...
18:44...	Core.exe	8808	ReadFile	C:\Program Files\Logitech Gaming Soft...	SUCCESS	Offset: 5 379 072...

Showing 65 017 of 194 689 events (33%) Backed by virtual memory

Autounst - Sysinternals: www.sysinternals.com

Autounst Entry	Description	Publisher	Image Path	Timestamp	ViruTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	2019.12.07.10:15	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Logitech Gaming Framework	(Verified) Logitech Inc	c:\program files\logitech gaming soft...	2021.03.02.18:31	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Pentabest Service	(Verified) Guangzhou Ugee Computer...	c:\program files\pentabest\pentabest...	2019.08.31.2:50	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	Java Update Scheduler	(Verified) Oracle America, Inc.	c:\program files (x86)\common files\j...	2020.12.07.0:33	
HKCU\Software\Teams	Microsoft Teams	(Verified) Microsoft 3rd Party Applicat...	c:\users\mark\appdata\local\microso...	2020.09.15.19:07	
Opera Browser Assistant	Opera Browser Assistant	(Verified) Opera Software AS	c:\users\mark\appdata\local\progra...	2020.11.24.15:56	
ProtonVPN	ProtonVPN	(Verified) ProtonVPN AG	c:\program files (x86)\proton technol...	2020.02.17.9:24	
Skype for Desktop	Skype	(Verified) Skype Software Sarl	c:\program files (x86)\microsoft\skyp...	2019.12.06.2:09	
uTorrent	uTorrent	(Verified) BitTorrent Inc	c:\users\mark\appdata\roaming\utor...	2020.08.21.20:01	
Wargaming.net Game C...	Wargaming.net Game Center	(Verified) Wargaming.net Limited	c:\programdata\wargaming.net\gam...	2020.12.02.12:26	
C:\Users\Mark\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	Kuldes a(z) OneNote pro... Send to OneNote Tool	(Verified) Microsoft Corporation	c:\program files\microsoft office\vo...	2020.12.07.19:58	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components	Google Chrome	(Verified) Google LLC	c:\program files (x86)\google\chrome...	2021.02.15.20:31	
Microsoft Edge	Microsoft Edge	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge...	2021.02.25.1:49	
n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	2019.10.25.4:45	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	2020.12.07.3:13	
text/xml	Microsoft Office XML MIME Filter	(Verified) Microsoft Corporation	c:\program files\microsoft office\vo...	2020.12.28.23:39	
HKLM\Software\Classes\Protocols\Handler	Microsoft® Help Data Services Module	(Verified) Microsoft Corporation	c:\program files\common files\microso...	2012.11.07.13:17	
ms-help	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft office\vo...	2020.12.28.23:33	
ms-minib-16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft office\vo...	2020.12.28.23:33	
oef-16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft office\vo...	2020.12.28.23:33	
HKLM\Software\Classes\ShellEx\ContextMenuHandlers	ShellHandler for Notepad++ (64 bit)	(Verified) Notepad++	c:\notepad++\nppsh64.dll	2020.12.07.0:31	

Miskolc, 2021

d. Security Utilities:

Célja a bejelentkezési időszakok adatainak listázása.

```
Kijelölte Administrator Parancsok
C:\Vegyes\4 - felder\05\UjTul_0223\logonsessions64.exe

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

[0] Logon session 00000000-00000007:
User name: WORKGROUP\DESKTOP-P0BL2MH$
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: S-1-5-18
Logon time: 2021. 03. 02. 18:40:56
Logon server:
DNS Domain:
UPN:

[1] Logon session 00000000-00000007:
User name:
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: (none)
Logon time: 2021. 03. 02. 18:40:56
Logon server:
DNS Domain:
UPN:

[2] Logon session 00000000-00000007:
User name: Font Driver Host\UMFD-0
Auth package: Negotiate
Logon type: Interactive
Session: 0
Sid: S-1-5-96-0-0
Logon time: 2021. 03. 02. 18:40:56
Logon server:
DNS Domain:
UPN:

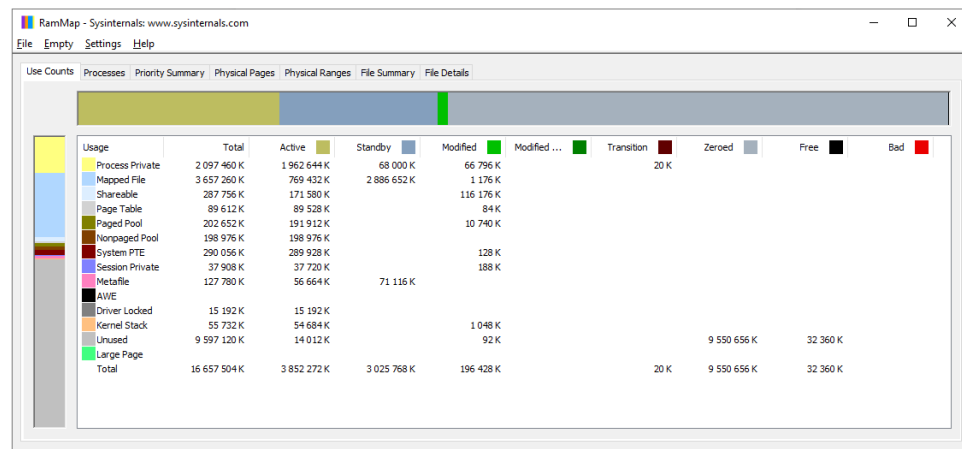
[3] Logon session 00000000-00000007:
User name: Font Driver Host\UMFD-1
Auth package: Negotiate
Logon type: Interactive
Session: 1
Sid: S-1-5-96-0-1
Logon time: 2021. 03. 02. 18:40:56
Logon server:
DNS Domain:
UPN:

[4] Logon session 00000000-00000007:
User name: WORKGROUP\DESKTOP-P0BL2MH$
Auth package: Negotiate
Logon type: Service
Session: 0
Sid: S-1-5-20
Logon time: 2021. 03. 02. 18:40:57
Logon server:
DNS Domain:
UPN:

[5] Logon session 00000000-00010002:
```

e. Information Utilities:

Célja a számítógépről (ez esetben a RAM-ról) kapott információk listázása.

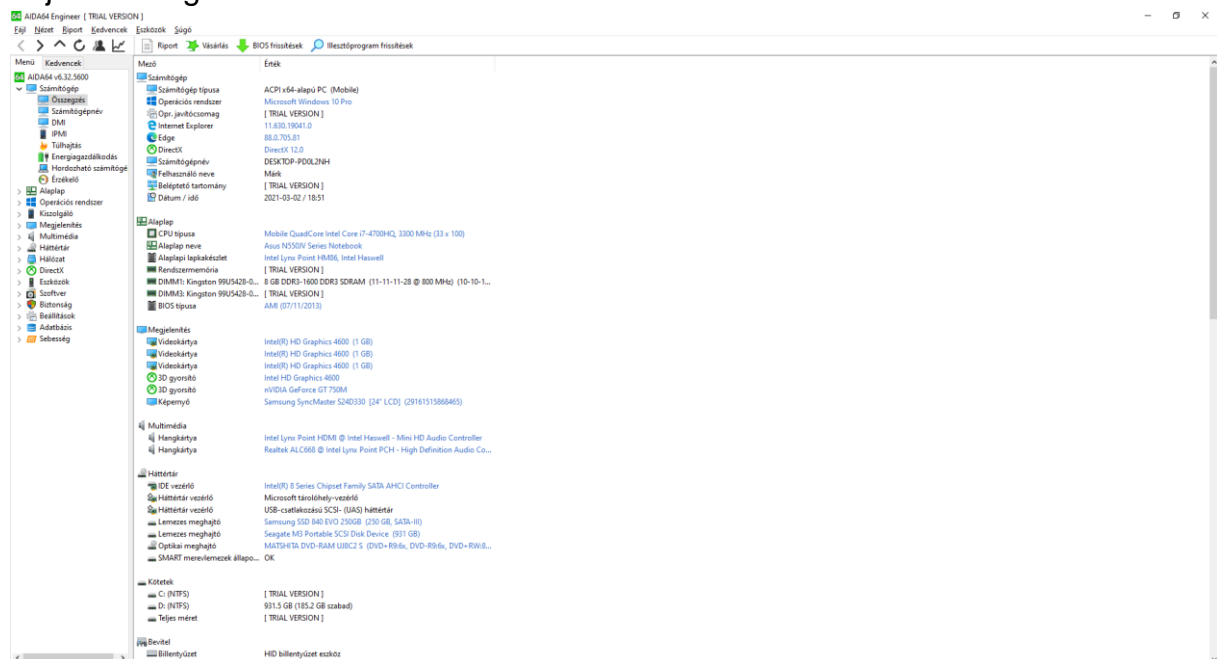


3. A számítógépet elemző szoftverek futtatása:

a. AIDA64:

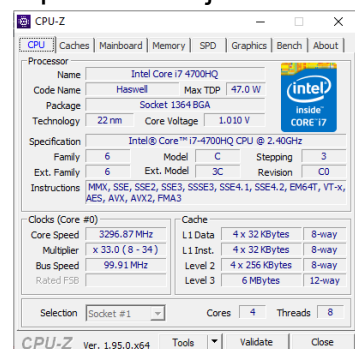
A számítógépről ad egy átfogó leírást, valamint különböző parancsok

hajthatók végre vele.



b. CPU-Z:

A processzor jellemzőinek részletes leírása.



c. GPU-Z:

A videokártya adatainak átfogó bemutatása.

