

A **Process Explorer** a Sysinternals Suite programcsomag része, melyben a futó programokról részleteket láthatunk, mint például a processzorból hány százalékot használ ki, mennyi memóriát használ a program, mi a program neve, melyik céghez tartozik a program. A legelső sávban látható, hogy hány százalékban van kihasználva a CPU, hány processz fut, stb.

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-PFNURUS\Sándor]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Teams.exe	2.27	248 056 K	303 028 K	5152	Microsoft Teams	Microsoft Corporation
dwm.exe	1.92	100 784 K	131 968 K	3748		
explorer.exe	1.03	83 028 K	172 536 K	16700	Windows Intéző	Microsoft Corporation
Interrupts	0.98	0 K	0 K	n/a	Hardware Interrupts and DPCs	
Teams.exe	0.88	320 332 K	348 040 K	5272	Microsoft Teams	Microsoft Corporation
System	0.85	220 K	6 012 K	4		
procexp64.exe	0.82	34 920 K	57 208 K	15208	Sysinternals Process Explorer	Sysinternals - www.sysinter...
chrome.exe	0.57	400 912 K	428 556 K	13744	Google Chrome	Google LLC
Viber.exe	0.41	124 440 K	201 956 K	20140	Viber	Viber Media S.Á r.l.
Teams.exe	0.40	185 912 K	235 048 K	17808	Microsoft Teams	Microsoft Corporation
audiodg.exe	0.30	21 428 K	31 744 K	13352		
ArmouryCrate.UserSessionHelp...	0.30	33 032 K	51 228 K	1460		
steam.exe	0.25	57 812 K	77 216 K	2368	Steam Client Bootstrapper	Valve Corporation
csrss.exe	0.24	2 584 K	6 812 K	16504		
svchost.exe	0.23	9 304 K	25 772 K	12724	Windows-szolgáltatások gaz...	Microsoft Corporation
asus_framework.exe	0.21	24 080 K	23 068 K	17744		
MsMpEng.exe	0.20	582 464 K	504 552 K	4572	Antimalware Service Executa...	Microsoft Corporation
XtuService.exe	0.19	46 676 K	42 732 K	4328	XtuService	Intel(R) Corporation
NVIDIA Share.exe	0.19	22 184 K	65 408 K	8464	NVIDIA Share	NVIDIA Corporation
AutoConnectHelper.exe	0.15	28 636 K	41 688 K	17900	AutoConnectHelper	
ctfmon.exe	0.13	12 704 K	29 860 K	19548		
WINWORD.EXE	0.10	77 844 K	126 416 K	15892	Microsoft Word	Microsoft Corporation
svchost.exe	0.10	4 168 K	7 100 K	1964	Windows-szolgáltatások gaz...	Microsoft Corporation
lsass.exe	0.07	9 232 K	18 388 K	884	Local Security Authority Proc...	Microsoft Corporation
qbittorrent.exe	0.06	62 784 K	26 164 K	10544	qBittorrent - A Bittorrent Client	The qBittorrent Project
obs-fimpeg-mux.exe	0.06	17 212 K	13 212 K	16340		
svchost.exe	0.05	14 288 K	19 676 K	1360	Windows-szolgáltatások gaz...	Microsoft Corporation
asus_framework.exe	0.05	186 876 K	31 420 K	15660		
Origin.exe	0.04	59 744 K	108 416 K	4480	Origin	Electronic Arts
nvsp-helper64.exe	0.03	2 844 K	13 748 K	7880		

CPU Usage: 21.12% Commit Charge: 32.09% Processes: 240 Physical Usage: 31.66%

TCPView – A futó programokról és szolgáltatásokról ad leírást, hogy melyik hálózaton fut, melyik porton található, stb.

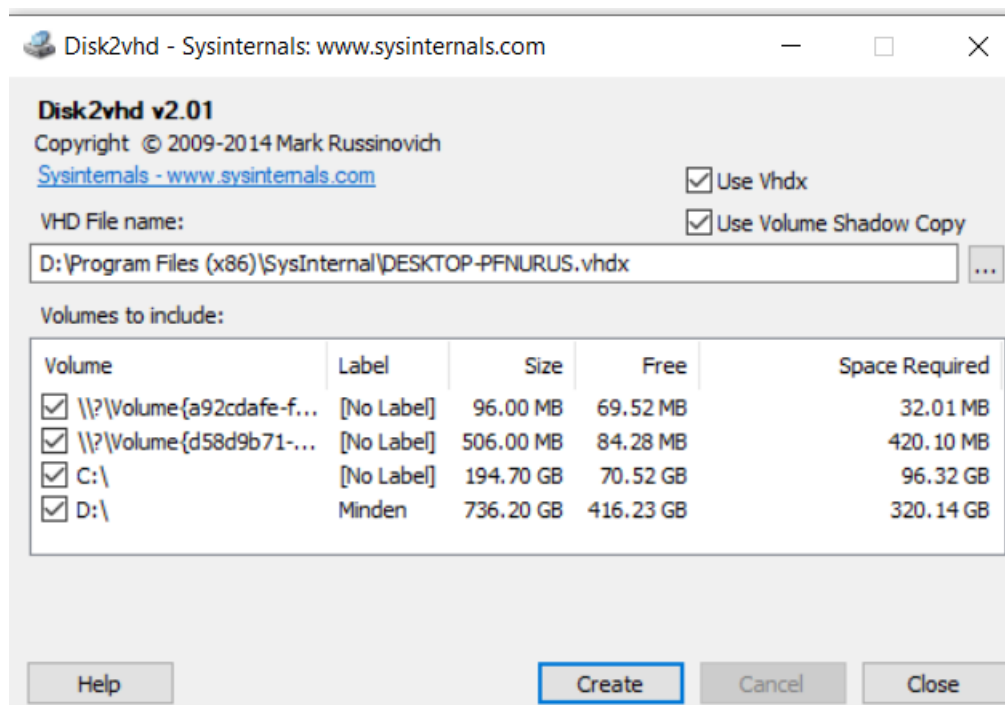
TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52674	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52675	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52676	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52677	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52678	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52679	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52680	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52681	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52682	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52683	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52684	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52685	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52686	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52687	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52688	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52689	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52690	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52691	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52692	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52693	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52694	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52695	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52696	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52697	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52698	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52699	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52700	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52701	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52702	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52703	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52704	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52705	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52706	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52707	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52708	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52709	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52710	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52711	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52712	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52713	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52714	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52715	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52716	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52717	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52718	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52719	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52720	localhost	1043	TIME_WAIT				
[System Proc...]	0	TCP	DESKTOP-PFNUR...	52721	localhost	1043	TIME_WAIT				

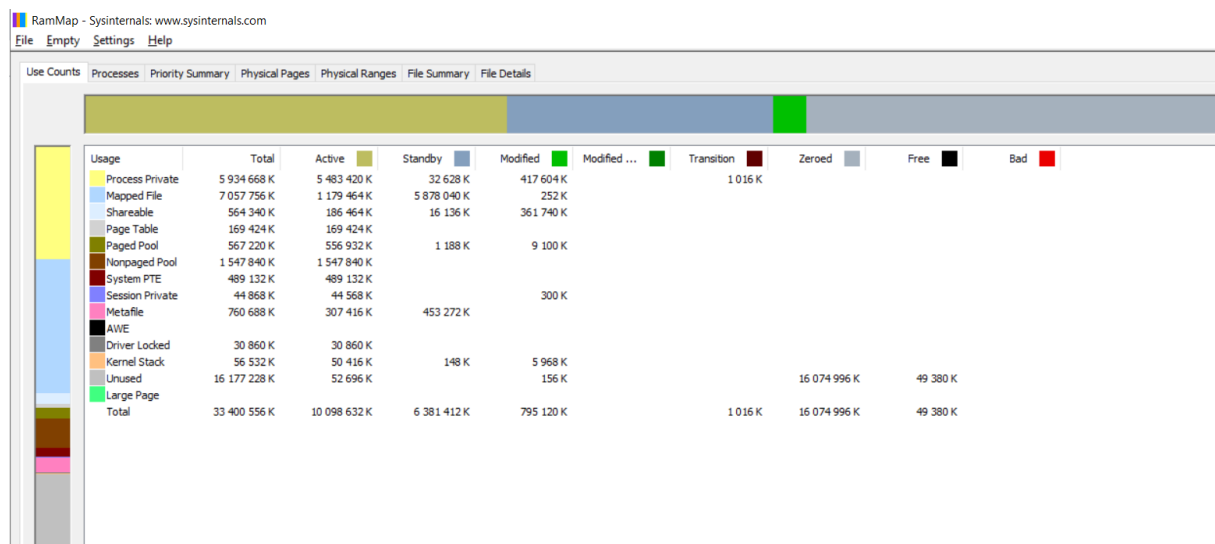
Endpoints: 932 Established: 58 Listening: 54 Time Wait: 315 Close Wait: 6

Disk2vhd – segítséget nyújt a fájlok átirányítására virtuális rendszerekre a számítógépünkről



LogonSessions - Listát ad ki arról, hogy kik jelentkeztek be a számítógépre, és ezekről a felhasználókról ad bővebb információt.

RAMMAP – A memóriáról ad bővebb leírást, mi használja, mennyit használ belőle, folyamatokról külön ad leírást melyik mennyi memóriát fogyaszt, stb.



Autoruns – Autómatikusan induló programok, folyamatok, szolgáltatásokról ad bővebb leírást.

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help					
Filter:					
Network Providers					
Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks Appinit KnownDLLs					
Autorun Entry	Description	Publisher	Image Path	Timestamp	Virus Total
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				2020. 10. 03. 13:06	
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor (Verified)	Microsoft Windows	c:\windows\system32\cmd.exe	1953. 12. 11. 3:58	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2020. 10. 03. 14:06	
<input checked="" type="checkbox"/> Discord	Discord - https://discord.com/ (Verified)	Discord Inc.	c:\programdata\squirrelmachi...	2020. 06. 01. 21:52	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2020. 12. 26. 19:24	
<input checked="" type="checkbox"/> Discord	Update (Verified)	Discord Inc.	c:\users\balog\appdata\local...	2020. 06. 01. 21:58	
<input checked="" type="checkbox"/> EADM	Origin (Verified)	Electronic Arts, Inc.	d:\games\origin\origin.exe	2021. 02. 02. 14:01	
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive (Verified)	Microsoft Corporation	c:\users\balog\appdata\local...	1958. 02. 05. 12:59	
<input checked="" type="checkbox"/> qBittorrent	qBittorrent - A Bittorrent Client (Not verified)	The qBittorrent ...	c:\program files\qBittorrent\qb...	2020. 04. 25. 0:56	
<input checked="" type="checkbox"/> Steam	Steam Client Bootstrapper (Verified)	Valve	d:\games\steam\steam.exe	2021. 02. 13. 0:23	
<input checked="" type="checkbox"/> Viber	Viber (Verified)	Viber Media S.à.r.l.	c:\users\balog\appdata\local...	2021. 01. 25. 17:45	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2020. 10. 03. 14:06	
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer (Verified)	Google LLC	c:\program files\google\chro...	2021. 02. 04. 1:31	
<input checked="" type="checkbox"/> Microsoft Edge	Microsoft Edge Installer (Verified)	Microsoft Corporation	c:\program files (x86)\microso...	2021. 02. 10. 21:20	
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY ... (Verified)	Microsoft Corporation	c:\windows\system32\mscori...	2019. 10. 25. 4:45	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				2020. 10. 03. 13:07	
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY ... (Verified)	Microsoft Corporation	c:\windows\syswow64\mscori...	2019. 10. 25. 9:48	
HKLM\SOFTWARE\Classes\Protocols\Filter				2020. 10. 14. 15:28	
<input checked="" type="checkbox"/> text/xml	Microsoft Office XML MIME Fil... (Verified)	Microsoft Corporation	c:\program files\common files...	2015. 07. 30. 13:21	
HKLM\SOFTWARE\Classes\Protocols\Handler				2020. 10. 14. 15:30	
<input checked="" type="checkbox"/> ms-help	Microsoft® Help Data Service... (Verified)	Microsoft Corporation	c:\program files\common files...	2015. 07. 30. 13:30	
<input checked="" type="checkbox"/> mso-minsb.16	Microsoft Office 2016 compon... (Verified)	Microsoft Corporation	c:\program files\microsoft offic...	2015. 07. 30. 13:04	
<input checked="" type="checkbox"/> osf16	Microsoft Office 2016 compon... (Verified)	Microsoft Corporation	c:\program files\microsoft offic...	2015. 07. 30. 13:04	
HKLM\Software\Classes\ShellEx\ContextMenu-Handlers				2020. 10. 03. 14:06	
<input checked="" type="checkbox"/> ANotepad++64	ShellHandler for Notepad++ (... (Verified)	Notepad++	c:\program files (x86)\notepad...	2014. 05. 12. 10:49	
<input checked="" type="checkbox"/> WinRAR	WinRAR shell extension (Verified)	win.rar GmbH	c:\program files\winrar\rarext.dll	2020. 06. 25. 11:38	
HKLM\Software\Classes\Directory\Background\ShellEx\ContextMenu-Handlers				2020. 10. 03. 13:54	
<input checked="" type="checkbox"/> NvCpDesktopCo...	NVIDIA Display Shell Extensi... (Verified)	NVIDIA Corporation	c:\windows\system32\diverst...	2020. 01. 02. 15:06	
HKLM\Software\Classes\Folder\ShellEx\ContextMenu-Handlers				2020. 10. 03. 14:06	
<input checked="" type="checkbox"/> WinRAR	WinRAR shell extension (Verified)	win.rar GmbH	c:\program files\winrar\rarext.dll	2020. 06. 25. 11:38	
HKLM\Software\Classes\Folder\ShellEx\DragDrop-Handlers				2020. 10. 03. 14:06	
<input checked="" type="checkbox"/> WinRAR	WinRAR shell extension (Verified)	win.rar GmbH	c:\program files\winrar\rarext.dll	2020. 06. 25. 11:38	
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers				2020. 10. 14. 15:30	
<input checked="" type="checkbox"/> SkyDrivePro1 (E...	Microsoft OneDrive for Busine... (Verified)	Microsoft Corporation	c:\program files\microsoft offic...	2015. 07. 30. 13:23	
<input checked="" type="checkbox"/> SkyDrivePro2 (S...	Microsoft OneDrive for Busine... (Verified)	Microsoft Corporation	c:\program files\microsoft offic...	2015. 07. 30. 13:23	

Készítette: Balogh Sándor (GVVASJ)

2021.02.17