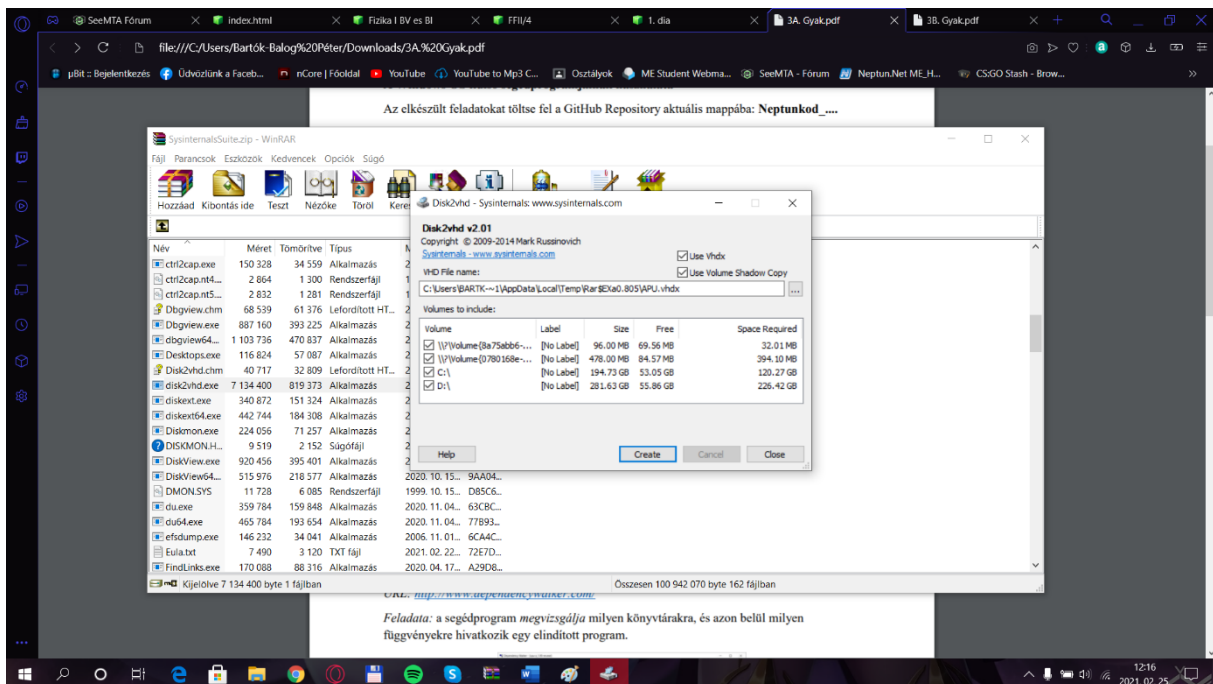


Disk2vhd: Virtuális merevlemez létrehozása.



TCP: Folyamatok vizsgálata

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	apu.home	61979	40.126.31.143	https	TIME_WAIT				
[System Proc...]	0	TCP	apu.home	62000	52.109.76.124	https	TIME_WAIT				
[System Proc...]	0	TCP	apu.home	62008	52.109.76.124	https	TIME_WAIT				
[System Proc...]	0	TCP	apu.home	62015	52.109.76.124	https	TIME_WAIT				
[System Proc...]	0	TCP	apu.home	62034	52.109.76.124	https	TIME_WAIT				
[GameManage...]	4704	TCP	apu.home	61985	a104.103.72.26.d...	http	ESTABLISHED				
[GameManage...]	4704	TCP	apu.home	61986	a104.103.72.26.d...	http	ESTABLISHED				
[j_h_service.e...	4264	TCPV6	[0.0.0.0.0.0.1]	48669	apu	0	LISTENING				
[LCore.exe]	14732	UDP	apu	54915				1138	299 294	1138	299 294
[LCore.exe]	14732	UDPV6	apu	54915							
[IaaS.exe]	1016	TCP	apu	49664	apu	0	LISTENING				
[IaaS.exe]	1016	TCPV6	apu	49664	apu	0	LISTENING				
[MicrosoftEdg...	7940	TCP	apu.home	61674	a2.16.10.138.depl...	https	CLOSE_WAIT				
[nvcontainer.e...	4304	TCP	apu	64254	localhost	65001	ESTABLISHED				
[nvcontainer.e...	4304	TCP	apu	65001	apu	0	LISTENING				
[nvcontainer.e...	4304	TCP	apu	65001	localhost	64254	ESTABLISHED				
[nvcontainer.e...	4304	UDP	apu	5353				1	85	17	677
[nvcontainer.e...	4304	UDP	apu	5353							
[nvcontainer.e...	3620	UDP	apu	10071							
[nvcontainer.e...	395	UDP	apu	49354							
[nvcontainer.e...	4304	UDP	apu	61242							
[nvcontainer.e...	4304	UDPV6	[0.0.0.0.0.0.1]	5353							
[nvcontainer.e...	4304	UDPV6	apu	61243							
[NVIDIA Share...	11796	TCP	apu	61207	localhost	62874	ESTABLISHED	23	207	23	69
[NVIDIA Web ...]	1616	TCP	apu	62874	localhost	61207	ESTABLISHED	23	69	23	207
[NVIDIA Web ...]	1616	UDP	apu	10070	apu	0	LISTENING				
[opera.exe]	6836	TCP	apu.home	61723	ec2-18-209-90-15...	https	ESTABLISHED	67	13 483	40	5 634
[opera.exe]	6836	TCP	apu.home	61740	142.250.27.189	5228	ESTABLISHED			2	1 679
[opera.exe]	6836	TCP	apu.home	61952	bud02c24-nv41...	https	CLOSE_WAIT	1	64	6	4 695
[opera.exe]	6836	TCP	apu.home	61954	bud02c24-nv41...	https	CLOSE_WAIT	2	581	5	3 392
[opera.exe]	6836	TCP	apu.home	61958	edge-star-hv-01-...	https	ESTABLISHED	88	6 678	87	3 168
[opera.exe]	6836	TCP	apu.home	61959	edge-star-hv-01-...	https	ESTABLISHED	88	6 683	88	3 190
[opera.exe]	6836	TCP	apu.home	61960	edge-star-hv-01-...	https	ESTABLISHED	88	6 624	88	3 190
[OriginWebHel...	4436	TCP	apu	3213	apu	0	LISTENING				
[OriginWebHel...	4436	UDP	apu	59667							
[OriginWebHel...	4436	TCP	apu.home	62016	184.51.8.219	https	ESTABLISHED	3	1 633	7	6 685
[Razer Synaps...	1596	TCPV6	[0.0.0.0.0.0.1]	61186	[0.0.0.0.0.0.1]	5426	ESTABLISHED			57	228
[Razer Synaps...	1596	TCPV6	[0.0.0.0.0.0.1]	61253	[0.0.0.0.0.0.1]	5426	ESTABLISHED			57	228
[Razer Synaps...	1596	TCPV6	[0.0.0.0.0.0.1]	61254	[0.0.0.0.0.0.1]	5426	ESTABLISHED			57	228
[Razer Synaps...	1596	TCPV6	[0.0.0.0.0.0.1]	61213	[0.0.0.0.0.0.1]	5426	ESTABLISHED			57	228
[Razer Synaps...	1596	TCPV6	[0.0.0.0.0.0.1]	64252	[0.0.0.0.0.0.1]	5426	ESTABLISHED			57	228
[Razer Synaps...	7304	TCPV6	[0.0.0.0.0.0.1]	61223	[0.0.0.0.0.0.1]	5426	ESTABLISHED			57	228
[Razer Synaps...	7304	TCPV6	[0.0.0.0.0.0.1]	61263	[0.0.0.0.0.0.1]	5426	ESTABLISHED			57	228
[Razer Synaps...	7304	TCPV6	[0.0.0.0.0.0.1]	61264	[0.0.0.0.0.0.1]	5426	ESTABLISHED	136	10 526	133	1 596
[Razer Synaps...	7304	TCPV6	[0.0.0.0.0.0.1]	61265	[0.0.0.0.0.0.1]	5426	ESTABLISHED			57	228
[RazerCentra...	4636	TCP	apu.home	61205	ec2-3-232-144-13...	https	ESTABLISHED	5	370	10	185
[RazerCentra...	4636	TCP	apu.home	61963	a104.103.72.128...	https	ESTABLISHED	3	577	8	4 533
[RazerCentra...	4636	TCP	apu.home	61964	a104.103.72.123...	https	ESTABLISHED	4	1 079	6	4 135
[RGLiveServ...	4684	TCP	apu	13030	apu	0	LISTENING				

Endpoints: 163 Established: 74 Listening: 35 Time Wait: 5 Close Wait: 4

Process Expoler, Autoruns: Folyamat kezelések.

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codes WMI Boot Execute Image Hijacks Apphit KnownDLLs Winlog Winsock Providers Print Monitors LSA Providers

Autoun Entry	Description	Publisher	Image Path	Timestamp	Virus Total
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\Shell				2019.11.20.14.10	
cmd.exe	Windows Command Processor (Verified)	Microsoft Windows	c:\windows\system32\cmd.exe	1996.06.08.13.13	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021.02.21.16.34	
Launch LCore	Logitech Gaming Framework (Verified)	Logitech Inc.	c:\program files\logitech gami...	2018.10.05.9.27	
Riot Vanguard	Vanguard tray notification (Verified)	Riot Games, Inc.	c:\program files\riot vanguard...	2021.01.22.21.31	
R2ShareHelper			File not found: C:\Windows\...		
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021.01.19.19.27	
BitTorrent	BitTorrent Inc (Verified)	BitTorrent Inc	c:\users\bartok-balog\peteria...	2014.06.21.0.54	
com blitz app	Blitz (Verified)	Swift Media Entertai...	c:\users\bartok-balog\peteria...	2021.01.23.1.18	
com squirrel Tea	Microsoft Teams (Verified)	Microsoft 3rd Party...	c:\users\bartok-balog\peteria...	2020.10.02.13.48	
OneDrive	Microsoft OneDrive (Verified)	Microsoft Corporation	c:\users\bartok-balog\peteria...	1968.02.05.12.59	
Steam	Steam Client Bootstrapper (Verified)	Valve	c:\program files (x86)\steam...	2020.12.21.0.10	
Synapse3	Razer Synapse 3 (Verified)	Razer USA Ltd.	c:\program files (x86)\razer...	1968.07.19.15.08	
uTorrent	BitTorrent Inc (Verified)	BitTorrent Inc	c:\program files (x86)\utorren...	2011.03.10.3.36	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2021.01.19.19.26	
Google Chrome	Google Chrome Installer (Verified)	Google LLC	c:\program files (x86)\google...	2021.02.13.0.08	
nla	Microsoft .NET IE SECURITY...	Microsoft Corporation	c:\windows\system32\mscon...	2019.10.25.4.45	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				2019.11.26.20.00	
nla	Microsoft .NET IE SECURITY...	Microsoft Corporation	c:\windows\system32\mscon...	2019.10.25.4.45	
HKLM\SOFTWARE\Classes\Protocols\Filer				2021.02.01.13.23	
textml	Microsoft Office XML MIME Fil...	Microsoft Corporation	c:\program files\microsoft offi...	2020.12.28.23.39	
HKLM\SOFTWARE\Classes\Protocols\Handler				2021.02.01.13.23	
ms-office-roam	Microsoft Office component (Verified)	Microsoft Corporation	c:\program files\microsoft offi...	2020.12.28.23.33	
ms-office-16	Microsoft Office component (Verified)	Microsoft Corporation	c:\program files\microsoft offi...	2020.12.28.23.33	
ms-office-16	Microsoft Office component (Verified)	Microsoft Corporation	c:\program files\microsoft offi...	2020.12.28.23.33	
ms-office-16	Microsoft Office component (Verified)	Microsoft Corporation	c:\program files\microsoft offi...	2020.12.28.23.33	
HKLM\Software\Classes\Shell\ExContextMenu\Handlers				2020.09.19.11.37	
Notepad++	ShellHandler for Notepad++ (Verified)	Notepad++	c:\program files\notepad++\n...	2014.05.12.10.49	
WinRAR	WinRAR shell extension (Verified)	win.rar GmbH	c:\program files\winrar\raet.dl	2014.06.10.18.11	
HKLM\Software\Classes\Directory\Background\Shell\ExContextMenu\Handlers				2020.10.13.17.52	
WinSCP	Drag&Drop shell extension fo...	Martin Piskyl	c:\program files (x86)\winscp...	2020.07.24.15.49	
HKLM\Software\Classes\Directory\Background\Shell\ExContextMenu\Handlers				2020.01.07.16.42	
NVIDIA Desktop Co.	NVIDIA Display Shell Extensi...	NVIDIA Corporation	c:\windows\system32\driverst...	2021.01.22.19.59	
HKLM\Software\Classes\Folder\Shell\ExContextMenu\Handlers				2020.01.07.18.04	
WinRAR	WinRAR shell extension (Verified)	win.rar GmbH	c:\program files\winrar\raet.dl	2014.06.10.18.11	

Ready.

Signed Windows Entries Hidden.

12:19
2021.02.25

Process Explorer - Sysinternals: www.sysinternals.com [APU] Bartók-Balog Péter

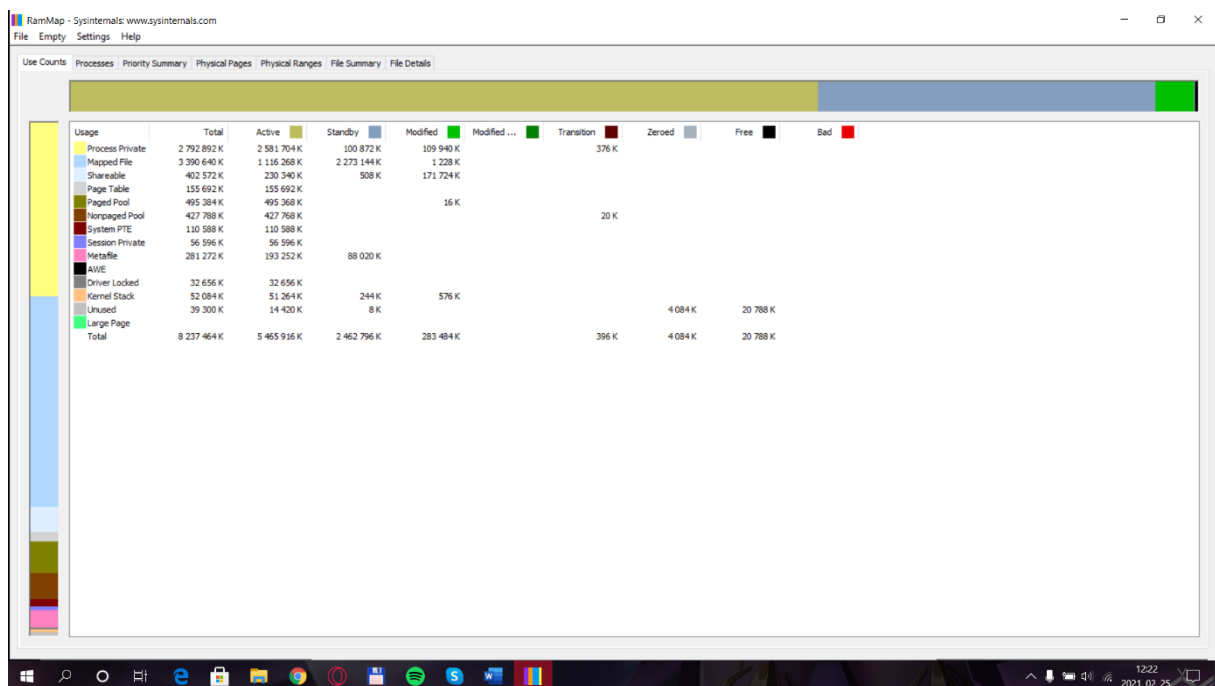
File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	83.16	60 K	40,492 K	0		
System	0.56	220 K	5,412 K	4		
Interrupts	0.52	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,048 K	456 K	552		
Memory Compression	< 0.01	1,348 K	198,896 K	2676		
csrss.exe	< 0.01	2,716 K	3,752 K	816		
wininit.exe		1,732 K	3,608 K	916		
services.exe	0.01	6,952 K	8,400 K	908		
svchost.exe		812 K	1,372 K	1128	Windows szolgáltatások gaz...	Microsoft Corporation
svchost.exe		15,948 K	24,424 K	1156	Windows szolgáltatások gaz...	Microsoft Corporation
WmPrvSE.exe		12,944 K	9,448 K	650		
dlhost.exe		3,344 K	4,244 K	8196		
unsecapp.exe		1,676 K	3,836 K	3352		
WmPrvSE.exe		10,624 K	19,280 K	14628		
RuntimeBroker.exe		27,320 K	69,060 K	17948		Microsoft Corporation
SearchApp.exe	Susp.	184,112 K	104,476 K	16280	Search application	Microsoft Corporation
RuntimeBroker.exe		12,204 K	37,744 K	11404	Runtime Broker	Microsoft Corporation
SettingsSyncHost.exe		4,532 K	6,796 K	10704	Host Process for Setting Syn...	Microsoft Corporation
RuntimeBroker.exe	Susp.	14,032 K	42,224 K	12816	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		6,932 K	26,384 K	12884	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		9,228 K	34,032 K	16564	Runtime Broker	Microsoft Corporation
dlhost.exe		11,404 K	19,712 K	17096	COM Surrogate	Microsoft Corporation
ApplicationFrameHost.exe		24,600 K	39,844 K	17624	Application Frame Host	Microsoft Corporation
RuntimeBroker.exe		6,320 K	25,944 K	18004	Runtime Broker	Microsoft Corporation
MicrosoftEdgeWebUI.exe	Susp.	4,684 K	13,572 K	18204	Microsoft Edge Web Platform	Microsoft Corporation
SystemSettings.exe	Susp.	21,568 K	2,396 K	14324	Galphaz	Microsoft Corporation
dlhost.exe		1,652 K	7,340 K	9564	COM Surrogate	Microsoft Corporation
dlhost.exe		1,672 K	7,440 K	6652	COM Surrogate	Microsoft Corporation
RuntimeBroker.exe		13,000 K	41,756 K	10828		Microsoft Corporation
UserOOBEBroker.exe		1,952 K	8,808 K	7524	User OOBEBroker	Microsoft Corporation
ShellExperienceHost.exe	Susp.	30,828 K	50,280 K	14116	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		5,272 K	26,024 K	4740	Runtime Broker	Microsoft Corporation
SystemSettingsBroker.exe		9,480 K	32,520 K	11644	System Settings Broker	Microsoft Corporation
MicrosoftPhotos.exe	Susp.	52,976 K	3,272 K	16428		
RuntimeBroker.exe		10,708 K	32,012 K	9012	Runtime Broker	Microsoft Corporation
RealtekAudioControlPanel.exe	Susp.	9,276 K	33,644 K	2324	Realtek Audio Console	Realtek Semiconductor
RuntimeBroker.exe		2,400 K	14,036 K	14160	Runtime Broker	Microsoft Corporation
RealTime.exe	Susp.	70,992 K	2,260 K	10200	RealTime	Microsoft Corporation
RuntimeBroker.exe		2,136 K	9,856 K	15344	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2,104 K	9,880 K	16580	Runtime Broker	Microsoft Corporation
MicrosoftEdge.exe	Susp.	24,904 K	60,200 K	1124	Microsoft Edge	Microsoft Corporation
InternetExplorer.exe		1,536 K	15,008 K	1232	Internet Explorer	Microsoft Corporation
MicrosoftEdgeCP.exe	Susp.	150,416 K	55,572 K	7840	Microsoft Edge Console Proc...	Microsoft Corporation

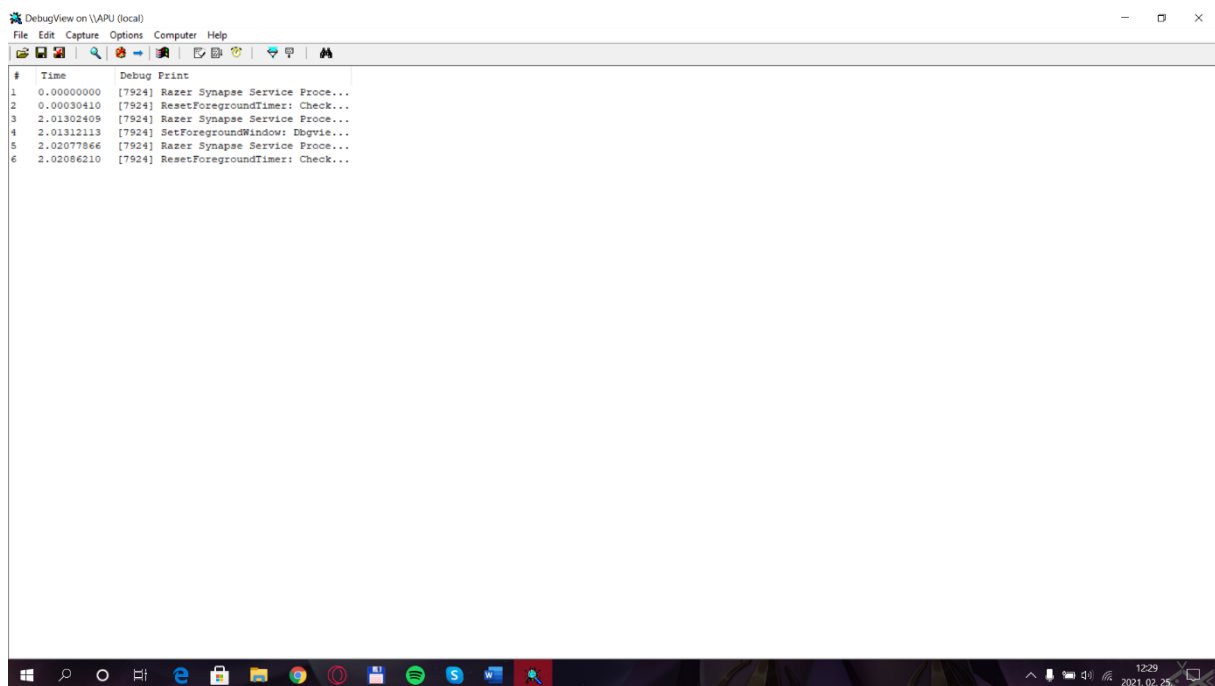
CPU Usage: 16.84% Commit Charge: 64.60% Processes: 241 Physical Usage: 69.55%

12:18
2021.02.25

Rammap: RAM terheltsége, ellenőrzése, működése.



Debugview: megfigyelheti eszközökről vagy böngészőkből érkező eseményeket, ahol engedélyezte a hibakeresést.



Aida, Gpu-u, Cpu-z: Részletes elemzés a hardverekről, oprendszeréről, hálózatról, i/o állományokról.

