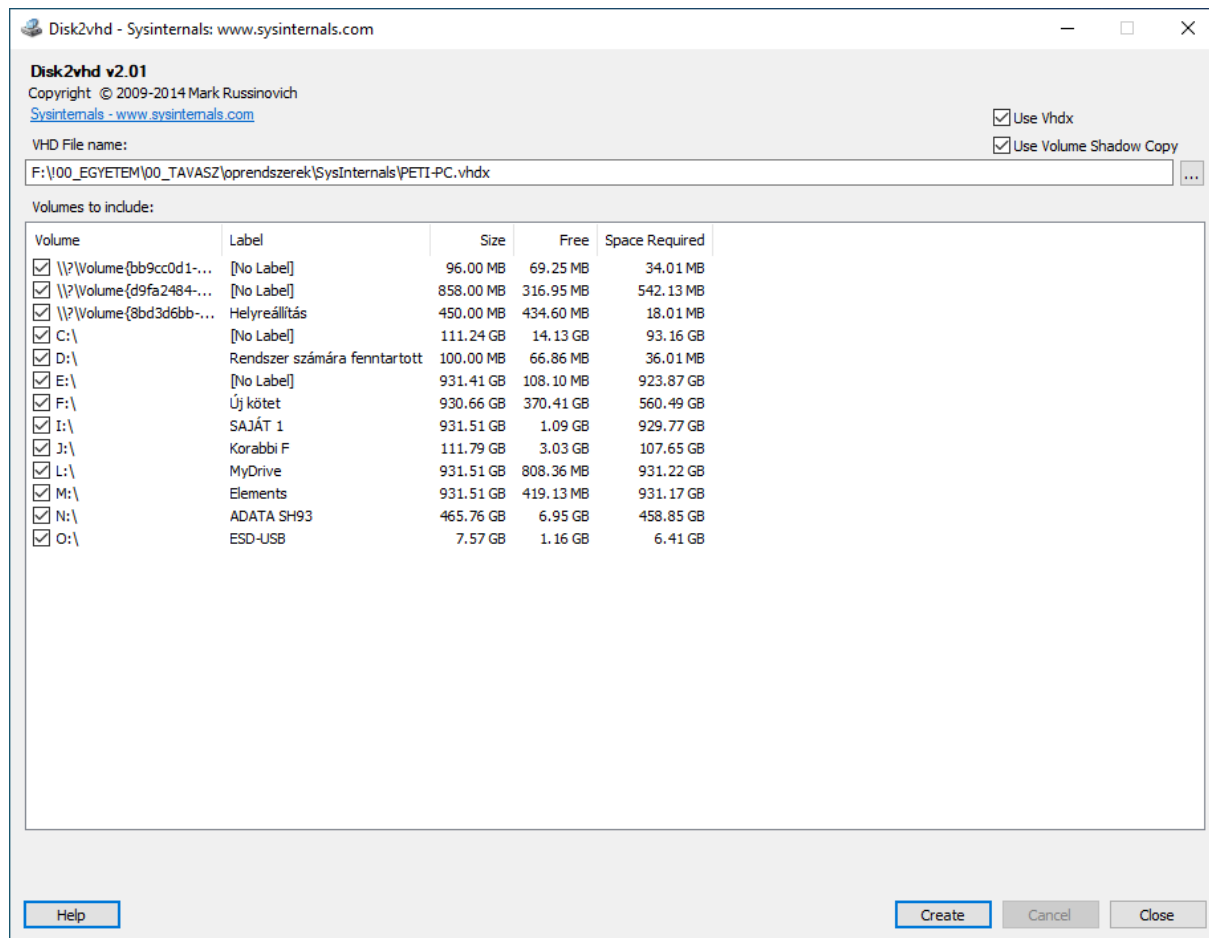


Windows külső segédprogramok

Disk2vhd:

Listázza a rendszerben létező köteteket. Fizikai lemezek virtuális verzióinak létrehozására alkalmas, mely virtuális lemezeket aztán Microsoft Virtual PC vagy Hyper-V virtuális gépeken használhatunk.



TCPView:

Részletes listát ad minden aktív TCP illetve UDP kapcsolatáról (végpontról), mely tartalmazza a kapcsolatot használó processz nevét, azonosítóját (PID), a helyi és távoli címet, portot, TCP kapcsolatok aktuális állapotát (TIME_WAIT, LISTENING, ESTABLISHED), hálózati forgalmat, stb. A távoli címeket névfeloldással is nézhetjük, ha be van kapcsolva ez az opció. A folyamatokat leállíthatjuk, megszakíthatjuk a kapcsolatot, a WHOIS szolgáltatás használatával pedig további információhoz juthatunk a távoli címekről.

TCPView - Sysinternals.com: www.sysinternals.com

FileOptionsProcessViewHelp

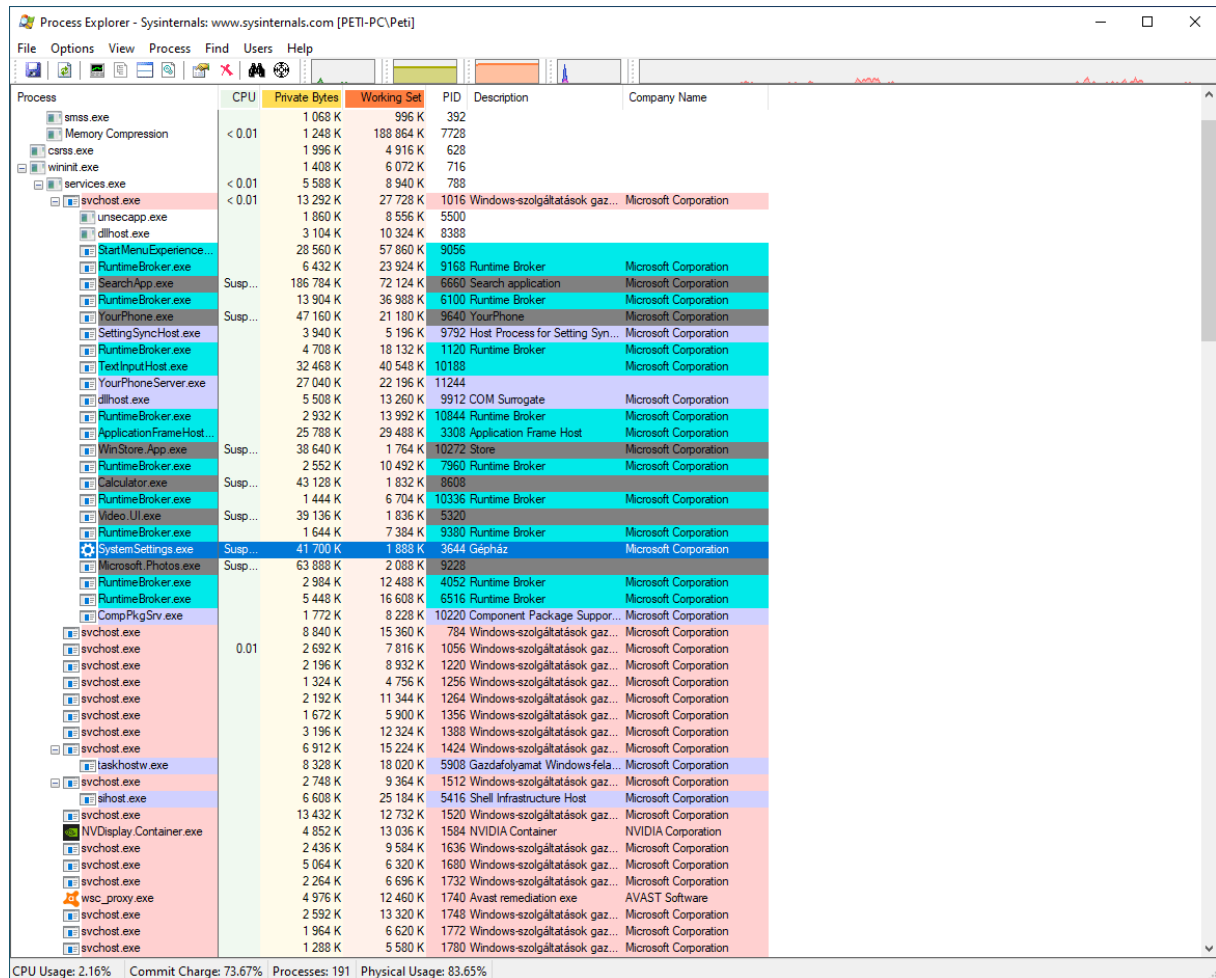
A

→

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes	
System Proc...	0	TCP	pet-pc	63127	a89-221-187-122.deploy.static.akam...	http	TIME_WAIT	1	213	3	4 549	
System Proc...	0	TCP	pet-pc	63125	52.103.8.20	https	TIME_WAIT	3	1 122	4	6 226	
System Proc...	0	TCP	pet-pc	63129	52.113.139.102	https	TIME_WAIT	6	3 032	7	6 156	
AvastSvc.exe	2932	TCP	PETI-PC	12025	PETI-PC	0	LISTENING	0				
AvastSvc.exe	2932	TCP	PETI-PC	12110	PETI-PC	0	LISTENING	0				
AvastSvc.exe	2932	TCP	PETI-PC	12119	PETI-PC	0	LISTENING	0				
AvastSvc.exe	2932	TCP	PETI-PC	12143	PETI-PC	0	LISTENING	0				
AvastSvc.exe	2932	TCP	PETI-PC	12465	PETI-PC	0	LISTENING	0				
AvastSvc.exe	2932	TCP	PETI-PC	12563	PETI-PC	0	LISTENING	0				
AvastSvc.exe	2932	TCP	PETI-PC	12993	PETI-PC	0	LISTENING	0				
AvastSvc.exe	2932	TCP	PETI-PC	12995	PETI-PC	0	LISTENING	0				
AvastSvc.exe	2932	TCP	PETI-PC	27275	PETI-PC	0	LISTENING	0				
AvastSvc.exe	2932	TCP	pet-pc	49673	prog39-010.lf.avast.com	http	ESTABLISHED	2		6	4 754	
AvastSvc.exe	2932	TCP	pet-pc	49675	5.62.53.131	https	ESTABLISHED					
AvastSvc.exe	2932	UDP	PETI-PC	56607	PETI-PC	*						
AvastSvc.exe	2932	UDP	PETI-PC	56609	*	*						
AvastSvc.exe	2932	TCPSV6	[0.0.0.0.0.0.0.1]	12025	pet-pc	0	LISTENING	0				
AvastSvc.exe	2932	TCPSV6	[0.0.0.0.0.0.0.1]	12110	pet-pc	0	LISTENING	0				
AvastSvc.exe	2932	TCPSV6	[0.0.0.0.0.0.0.1]	12119	pet-pc	0	LISTENING	0				
AvastSvc.exe	2932	TCPSV6	[0.0.0.0.0.0.0.1]	12143	pet-pc	0	LISTENING	0				
AvastSvc.exe	2932	TCPSV6	[0.0.0.0.0.0.0.1]	12465	pet-pc	0	LISTENING	0				
AvastSvc.exe	2932	TCPSV6	[0.0.0.0.0.0.0.1]	12563	pet-pc	0	LISTENING	0				
AvastSvc.exe	2932	TCPSV6	[0.0.0.0.0.0.0.1]	12993	pet-pc	0	LISTENING	0				
AvastSvc.exe	2932	TCPSV6	[0.0.0.0.0.0.0.1]	12995	pet-pc	0	LISTENING	0				
AvastSvc.exe	2932	TCPSV6	[0.0.0.0.0.0.0.1]	27275	pet-pc	0	LISTENING	0				
dashHost.exe	7940	UDP	PETI-PC	we-discovery	*	*						
dashHost.exe	7940	UDP	PETI-PC	we-discovery	*	*						
dashHost.exe	7940	UDP	PETI-PC	50412	*	*						
dashHost.exe	7940	UDPSV6	pet-pc	3702	*	*						
dashHost.exe	7940	UDPSV6	pet-pc	3702	*	*						
dashHost.exe	7940	UDPSV6	pet-pc	50413	*	*						
firefox.exe	11168	TCP	PETI-PC	49856	localhost	49857	ESTABLISHED					
firefox.exe	11168	TCP	PETI-PC	49857	localhost	49856	ESTABLISHED	1 202		1 202	1 202	
firefox.exe	3396	TCP	PETI-PC	49859	localhost	49860	ESTABLISHED					
firefox.exe	3396	TCP	PETI-PC	49860	localhost	49859	ESTABLISHED	60		60	60	
firefox.exe	10612	TCP	PETI-PC	49864	localhost	49865	ESTABLISHED					
firefox.exe	10612	TCP	PETI-PC	49865	localhost	49864	ESTABLISHED					
firefox.exe	2612	TCP	PETI-PC	49867	localhost	49868	ESTABLISHED					
firefox.exe	2612	TCP	PETI-PC	49868	localhost	49867	ESTABLISHED					
firefox.exe	11168	TCP	pet-pc	49869	ec2-234-214-16-178.us-west-2.compu...	https	ESTABLISHED	1	35	1	31	
firefox.exe	12392	TCP	PETI-PC	49873	localhost	49874	ESTABLISHED					
firefox.exe	12392	TCP	PETI-PC	49874	localhost	49873	ESTABLISHED					
firefox.exe	11168	TCP	pet-pc	50013	edge-star-shv-01-cdf1.facebook.com	https	ESTABLISHED	52	1 876	55	3 241	
firefox.exe	10952	TCP	PETI-PC	62766	localhost	62767	ESTABLISHED					
firefox.exe	10952	TCP	PETI-PC	62767	localhost	62766	ESTABLISHED					
firefox.exe	11168	TCP	pet-pc	62795	edge-star-mini-shv-01-cdf1.faceboo...	https	ESTABLISHED	13	3 021	14	2 403	
firefox.exe	11168	TCP	pet-pc	63060	lb-140-62-114-26-usd.github.com	https	ESTABLISHED	11	2 179	12	3 680	
firefox.exe	10072	TCP	PETI-PC	63110	localhost	63111	ESTABLISHED					
firefox.exe	10072	TCP	PETI-PC	63111	localhost	63110	ESTABLISHED					
lsass.exe	808	TCP	PETI-PC	49664	PETI-PC	0	LISTENING	0				
lsass.exe	808	TCPSV6	pet-pc	49664	pet-pc	0	LISTENING	0				
ServerAdmin.exe	6660	TCP	pet-pc	62466	netelinc...	https	ESTABLISHED					
Endpoints: 118Established: 24Listening: 42Time Wait: 3Close Wait: 1												

Process Explorer:

Azon túl, hogy részletes információt nyújt a futó processzekről (ikon, CPU-használat, PID, leírás, cégnév, felhasználó, stb) haladó processzkezelő programként funkcionál.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
smss.exe		1 068 K	996 K	392		
Memory Compression	< 0.01	1 248 K	188 864 K	7728		
cars.exe		1 996 K	4 916 K	628		
wininit.exe		1 408 K	6 072 K	716		
services.exe	< 0.01	5 588 K	8 940 K	788		
svchost.exe	< 0.01	13 292 K	27 728 K	1016	Windows-szolgáltatások gaz...	Microsoft Corporation
unsecapp.exe		1 860 K	8 556 K	5500		
dlhst.exe		3 104 K	10 324 K	8388		
StartMenuExperience...		28 560 K	57 860 K	9056		
RuntimeBroker.exe		6 432 K	23 924 K	9168	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	186 784 K	72 124 K	6660	Search application	Microsoft Corporation
RuntimeBroker.exe		13 904 K	36 988 K	6100	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	47 160 K	21 180 K	9640	YourPhone	Microsoft Corporation
SettingSyncHost.exe		3 940 K	5 196 K	9792	Host Process for Setting Syn...	Microsoft Corporation
RuntimeBroker.exe		4 708 K	18 132 K	1120	Runtime Broker	Microsoft Corporation
TextInputHost.exe		32 468 K	40 548 K	10188		Microsoft Corporation
YourPhoneServer.exe		27 040 K	22 196 K	11244		
dlhst.exe		5 508 K	13 260 K	9912	COM Surrogate	Microsoft Corporation
RuntimeBroker.exe		2 932 K	13 992 K	10844	Runtime Broker	Microsoft Corporation
ApplicationFrameHost...		25 788 K	29 488 K	3308	Application Frame Host	Microsoft Corporation
WinStore.App.exe	Susp...	38 640 K	1 764 K	10272	Store	Microsoft Corporation
RuntimeBroker.exe		2 552 K	10 492 K	7960	Runtime Broker	Microsoft Corporation
Calculator.exe	Susp...	43 128 K	1 832 K	8668		
RuntimeBroker.exe		1 444 K	6 704 K	10336	Runtime Broker	Microsoft Corporation
Video.UI.exe	Susp...	39 136 K	1 836 K	5320		
RuntimeBroker.exe		1 644 K	7 384 K	9380	Runtime Broker	Microsoft Corporation
SystemSettings.exe	Susp...	41 700 K	1 888 K	3644	Gépház	Microsoft Corporation
Microsoft.Photos.exe	Susp...	63 888 K	2 088 K	9228		
RuntimeBroker.exe		2 984 K	12 488 K	4052	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		5 448 K	16 608 K	6516	Runtime Broker	Microsoft Corporation
CompPkgSrv.exe		1 772 K	8 228 K	10220	Component Package Suppor...	Microsoft Corporation
svchost.exe		8 840 K	15 360 K	784	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe	0.01	2 692 K	7 816 K	1056	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		2 196 K	8 932 K	1220	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		1 324 K	4 756 K	1256	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		2 192 K	11 344 K	1264	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		1 672 K	5 900 K	1356	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		3 196 K	12 324 K	1388	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		6 912 K	15 224 K	1424	Windows-szolgáltatások gaz...	Microsoft Corporation
taskhostw.exe		8 328 K	18 020 K	5908	Gazdalfolyamat Windows-fela...	Microsoft Corporation
svchost.exe		2 748 K	9 364 K	1512	Windows-szolgáltatások gaz...	Microsoft Corporation
shost.exe		6 608 K	25 184 K	5416	Shell Infrastructure Host	Microsoft Corporation
svchost.exe		13 432 K	12 732 K	1520	Windows-szolgáltatások gaz...	Microsoft Corporation
NVDisplay.Container.exe		4 852 K	13 036 K	1584	NVIDIA Container	NVIDIA Corporation
svchost.exe		2 436 K	9 584 K	1636	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		5 064 K	6 320 K	1680	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		2 264 K	6 696 K	1732	Windows-szolgáltatások gaz...	Microsoft Corporation
wsc_proxy.exe		4 976 K	12 460 K	1740	Avast remediation exe	AVAST Software
svchost.exe		2 592 K	13 320 K	1748	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		1 964 K	6 620 K	1772	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe		1 288 K	5 580 K	1780	Windows-szolgáltatások gaz...	Microsoft Corporation

CPU Usage: 2.16% Commit Charge: 73.67% Processes: 191 Physical Usage: 83.65%

Process Monitor:

Fejlett „rendszermonitorozó” program, melynek segítségével valós idejű visszajelzést kapunk a processzekről, a rendszerleíró adatbázisban és a fájlrendszerben zajló eseményekről.

Process Monitor - Sysinternals: www.sysinternals.com					
File Edit Events Filter Tools Options Help					
Time ...	Process Name	PID	Operation	Path	Result
16:43...	ctfmon.exe	6200	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS
16:43...	ctfmon.exe	6200	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS
16:43...	ctfmon.exe	6200	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS
16:43...	ctfmon.exe	6200	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS
16:43...	Explorer.EXE	6856	ReadFile	C:\Windows\System32\UIAnimation.dll	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKCU	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS
16:43...	ctfmon.exe	6200	RegQueryValue	HKCU\SOFTWARE\Microsoft\Input\Settings\MultilingualEnabled	SUCCESS
16:43...	ctfmon.exe	6200	RegCloseKey	HKCU\SOFTWARE\Microsoft\Input\Settings	SUCCESS
16:43...	Explorer.EXE	6856	ReadFile	C:\Windows\System32\UIAnimation.dll	SUCCESS
16:43...	Explorer.EXE	6856	ReadFile	C:\Windows\System32\UIAnimation.dll	SUCCESS
16:43...	Explorer.EXE	6856	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS
16:43...	Explorer.EXE	6856	RegOpenKey	HKCU	SUCCESS
16:43...	Explorer.EXE	6856	RegCloseKey	HKCU	SUCCESS
16:43...	ctfmon.exe	6200	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS
16:43...	ctfmon.exe	6200	ReadFile	C:\Windows\System32\TextInputFramework.dll	SUCCESS
16:43...	ctfmon.exe	6200	ReadFile	C:\Windows\System32\CoreUIComponents.dll	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKLM	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKCU	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS
16:43...	ctfmon.exe	6200	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1\loc_0409\im_1	SUCCESS
16:43...	ctfmon.exe	6200	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1\loc_0409\im_1\UsUserAv...	SUCCESS
16:43...	ctfmon.exe	6200	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1\loc_0409\im_1	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Settings	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Settings\proc_1\loc_0409\im_1	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Settings\proc_1\loc_0409\im_1\UsUserAv...	SUCCESS
16:43...	ctfmon.exe	6200	RegCloseKey	HKCU\SOFTWARE\Microsoft\Input\Settings\proc_1\loc_0409\im_1	SUCCESS
16:43...	ctfmon.exe	6200	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Settings	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKLM	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKCU	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Settings	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1\loc_040e\im_1	SUCCESS
16:43...	ctfmon.exe	6200	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1\loc_040e\im_1\DisableEx...	NAME NOT FOUND Length: 144
16:43...	ctfmon.exe	6200	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1\loc_040e\im_1	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Settings	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1\loc_040e	SUCCESS
16:43...	ctfmon.exe	6200	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1\loc_040e\DisableExpress...	NAME NOT FOUND Length: 144
16:43...	ctfmon.exe	6200	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1\loc_040e	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Settings	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1	SUCCESS
16:43...	ctfmon.exe	6200	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1\DisableExpress\inputSh...	NAME NOT FOUND Length: 144
16:43...	ctfmon.exe	6200	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1	SUCCESS
16:43...	ctfmon.exe	6200	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Settings\DisableExpress\inputShellHokey	NAME NOT FOUND Length: 144
16:43...	ctfmon.exe	6200	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Settings	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKCU	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Settings	SUCCESS
16:43...	ctfmon.exe	6200	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Settings\EnableExpress\inputEmojiMult...	NAME NOT FOUND Length: 16

Process Tree						
<input type="checkbox"/> Only show processes still running at end of current trace <input checked="" type="checkbox"/> Timelines cover displayed events only						
	File	Company	Ver	Command	Start Time	End Time
[-] System (4)	System		NT AUTHORITY\...		2021 03 15 13:4... n/a	
[-] Registry (100)	Registry		NT AUTHORITY\...		2021 03 15 13:4... n/a	
[-] smss.exe (392)	Windows munkam...	Microsoft Corporat...	NT AUTHORITY\...SystemRoot\Syst...		2021 03 15 13:4... n/a	
[-] MemCompression (7728)	MemCompression		NT AUTHORITY\...		2021 03 15 13:4... n/a	
[-] csrss.exe (620)	Ugráfizetési f... C:\WINDOWS\sy...	Microsoft Corporat...	NT AUTHORITY\...SystemRoot\%a...		2021 03 15 13:4... n/a	
[-] wininit.exe (715)	Windows-end.kd...	Microsoft Corporat...	NT AUTHORITY\...wininit.exe		2021 03 15 13:4... n/a	
[-] services.exe (788)	Szolgáltatási vez...	Microsoft Corporat...	NT AUTHORITY\...C:\WINDOWS\sy...		2021 03 15 13:4... n/a	
[-] lvchost.exe (1016)	Windows szolgá...	Microsoft Corporat...	NT AUTHORITY\...C:\WINDOWS\sy...		2021 03 15 13:4... n/a	
[-] lsirpcss.exe (5503)	Link to receive as...	Microsoft Corporat...	NT AUTHORITY\...C:\WINDOWS\sy...		2021 03 15 13:4... n/a	
[-] DllHost.exe (8388)	COM Surrogate	Microsoft Corporat...	NT AUTHORITY\...C:\WINDOWS\sy...		2021 03 15 13:4... n/a	
[-] StartMenuExperienceH...	C:\WINDOWS\S...		PETI-PC\Peti	"C:\WINDOWS\...	2021 03 15 13:4... n/a	
[-] RuntimeBroker.exe (916)	Runtime Broker	Microsoft Corporat...	C:\Windows\Syst...	C:\Windows\Syst...	2021 03 15 13:4... n/a	
[-] SearchApp.exe (6682)	Search application	Microsoft Corporat...	C:\Windows\Syst...	"C:\Windows\Sy...	2021 03 15 13:4... n/a	
[-] RuntimeBroker.exe (610)	Runtime Broker	Microsoft Corporat...	C:\Windows\Syst...	PETI-PC\Peti	2021 03 15 13:4... n/a	
[-] YourPhone.exe (9648)	YourPhone	Microsoft Corporat...	C:\Program Files\...	"C:\Program Fie...	2021 03 15 13:4... n/a	
[-] SettingSyncHost.exe (9)	Hot Process for...	Microsoft Corporat...	C:\WINDOWS\sy...	PETI-PC\Peti	2021 03 15 13:4... n/a	
[-] RuntimeBroker.exe (112)	Runtime Broker	Microsoft Corporat...	C:\Windows\Syst...	C:\Windows\Syst...	2021 03 15 13:4... n/a	
[-] TestinputHost.exe (1016)	C:\WINDOWS\S...	Microsoft Corporat...	PETI-PC\Peti	"C:\WINDOWS\...	2021 03 15 13:4... n/a	
[-] YourPhoneServer.exe (1)	PETI-PC\Peti		C:\Program Fie...	"C:\Program Fie...	2021 03 15 13:4... n/a	
[-] DllHost.exe (9912)	COM Surrogate	Microsoft Corporat...	C:\WINDOWS\sy...	PETI-PC\Peti	2021 03 15 13:4... n/a	
[-] RuntimeBroker.exe (108)	Runtime Broker	Microsoft Corporat...	C:\Windows\Syst...	C:\Windows\Syst...	2021 03 15 13:4... n/a	
[-] ApplicationFrameHost.exe	Application Frame...	Microsoft Corporat...	C:\WINDOWS\sy...	PETI-PC\Peti	2021 03 15 13:4... n/a	
[-] WinStoreApp.exe (1023)	Store	Microsoft Corporat...	C:\Program Fie...	PETI-PC\Peti	2021 03 15 13:4... n/a	
[-] RuntimeBroker.exe (796)	Runtime Broker	Microsoft Corporat...	C:\Windows\Syst...	C:\Windows\Syst...	2021 03 15 13:4... n/a	
[-] Calculator.exe (8608)	C:\Program Files\...		PETI-PC\Peti	"C:\Program Fie...	2021 03 15 13:4... n/a	
[-] RuntimeBroker.exe (103)	Runtime Broker	Microsoft Corporat...	C:\Windows\Syst...	C:\Windows\Syst...	2021 03 15 13:4... n/a	
[-] Video UI.exe (5320)	C:\Program Fie...		PETI-PC\Peti	"C:\Program Fie...	2021 03 15 13:4... n/a	
[-] RuntimeBroker.exe (930)	Runtime Broker	Microsoft Corporat...	C:\Windows\Syst...	C:\Windows\Syst...	2021 03 15 13:5... n/a	
[-] SystemSettings.exe (634)	Gépfázis	Microsoft Corporat...	C:\Windows\Im...	"C:\Windows\Im...	2021 03 15 13:5... n/a	
[-] Microsoft.Photos.exe (92)	C:\Program Fie...		PETI-PC\Peti	"C:\Program Fie...	2021 03 15 14:1... n/a	
[-] RuntimeBroker.exe (651)	Runtime Broker	Microsoft Corporat...	C:\Windows\Syst...	C:\Windows\Syst...	2021 03 15 14:1... n/a	
[-] CompHgs32v.exe (1028)	Component Pack...	Microsoft Corporat...	C:\Windows\Syst...	PETI-PC\Peti	2021 03 15 14:2... n/a	
[-] Wmi.exe (636)	WMI Provider Host	Microsoft Corporat...	NT AUTHORITY\...	C:\WINDOWS\sy...	2021 03 15 16:4... 2021 03 15 16:5...	
[-] DllHost.exe (3344)	COM Surrogate	Microsoft Corporat...	C:\WINDOWS\sy...	PETI-PC\Peti	2021 03 15 16:4... 2021 03 15 16:4...	
[-] DllHost.exe (4232)	COM Surrogate	Microsoft Corporat...	C:\WINDOWS\sy...	PETI-PC\Peti	2021 03 15 16:4... 2021 03 15 16:4...	
[-] Wmi.exe (9764)	WMI Provider Host	Microsoft Corporat...	NT AUTHORITY\...	C:\WINDOWS\sy...	2021 03 15 16:4... 2021 03 15 16:4...	
[-] BackgroundTaskHost.exe	Background Task...	Microsoft Corporat...	C:\WINDOWS\sy...	PETI-PC\Peti	2021 03 15 16:4... 2021 03 15 16:4...	
[-] RuntimeBroker.exe (325)	Runtime Broker	Microsoft Corporat...	C:\Windows\Syst...	C:\Windows\Syst...	2021 03 15 16:4... 2021 03 15 16:5...	
[-] LocalBridge.exe (109)	LocalBridge		C:\Program Fie...	"C:\Program Fie...	2021 03 15 16:4... 2021 03 15 16:4...	
[-] mousoconworker.exe (3)	MoJoSO Core Wor...	Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\Syst...	2021 03 15 16:4... 2021 03 15 16:4...	
[-] HsTm.exe (7782)	Microsoft Outbo...	Microsoft Corporat...	C:\Program Fie...	PETI-PC\Peti	2021 03 15 16:5... 2021 03 15 16:5...	
[-] RuntimeBroker.exe (761)	Runtime Broker	Microsoft Corporat...	C:\Windows\Syst...	C:\Windows\Syst...	2021 03 15 16:5... 2021 03 15 16:5...	
[-] MoJoSO Core Wor...	C:\Windows\Syst...	Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\Syst...	2021 03 15 16:5... 2021 03 15 16:5...	
Description: Company: Path: Idle Command: User: PID: 0 Started: 2021 03 15 13:46:42						
<input type="button" value="Go To Event"/> <input type="button" value="Include Process"/> <input type="button" value="Include Subtree"/> <input type="button" value="Close"/>						

AutoRuns:

Ez a segédprogram bőséges információt nyújt a rendszerindításkor vagy bejelentkezéskor induló programokról illetve folyamatokról.

Autoruns - Sysinternals - www.sysinternals.com
File Entry Options Help

Filter:

AppInit KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
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				2020. 07. 18. 18:44	
<input checked="" type="checkbox"/> AdobeAAMUpdater-1.0	Adobe Updater Startup Utility	(Verified) Adobe Systems Incorporated	c:\program files (x86)\common files\adobe\...	2018. 04. 11. 8:32	
<input checked="" type="checkbox"/> AdobeGCInvoker-1.0	Adobe GC Invoker Utility	(Verified) Adobe Inc.	c:\program files (x86)\common files\adobe\...	2021. 02. 17. 4:27	
<input checked="" type="checkbox"/> AvastUI.exe	Avast AvLaunch component	(Verified) Avast Software s.r.o.	c:\program files\avast software\avast\...	2021. 02. 10. 0:58	
<input checked="" type="checkbox"/> RTHDVCPL	Realtek HD Audio Manager	(Verified) Realtek Semiconductor Corp.	c:\program files\realtek\audio\hda\rt... \	2018. 10. 15. 11:17	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2021. 02. 01. 16:42	
<input checked="" type="checkbox"/> Adobe Creative Cloud	Adobe Creative Cloud	(Verified) Adobe Systems Incorporated	c:\program files (x86)\adobe\adobe ...	2018. 04. 24. 15:29	
<input checked="" type="checkbox"/> HDD Regenerator		(Verified) Abstradrome	c:\program files (x86)\hdd regenerato...	2012. 10. 06. 22:01	
<input checked="" type="checkbox"/> SunJavaUpdateSched	Java Update Scheduler	(Verified) Oracle America, Inc.	c:\program files (x86)\common files\j... \	2020. 12. 09. 15:24	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021. 02. 19. 12:31	
<input checked="" type="checkbox"/> AllerCalc	AllerCalc MFC Application	(Not verified) AllerSoft	c:\program files (x86)\allercalc\allerc...	2000. 08. 22. 23:09	
<input checked="" type="checkbox"/> CCleaner Smart Cleaning	CCleaner	(Verified) Piriform Software Ltd	c:\program files\ccleaner\ccleaner64...	2020. 12. 08. 14:29	
<input checked="" type="checkbox"/> com.squirrel.Teams.Teams	Microsoft Teams	(Verified) Microsoft 3rd Party Applicati...	c:\users\peti\appdata\local\microsof...	2020. 10. 02. 13:48	
<input checked="" type="checkbox"/> EpicGamesLauncher	EpicGamesLauncher	(Verified) Epic Games Inc.	c:\program files (x86)\epic games\lau...	2021. 01. 14. 20:11	
<input checked="" type="checkbox"/> HEXelon MAX	HEXelon MAX	(Not verified) Jerzy Znamowski	c:\program files (x86)\hexelon max 6...	1992. 06. 19. 23:22	
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	c:\users\peti\appdata\local\microsof...	1941. 12. 22. 4:35	
<input checked="" type="checkbox"/> SmileboxTray	Smilebox Tray	(Verified) Smilebox, Inc.	c:\users\peti\appdata\local\smile...	2019. 03. 12. 8:59	
<input checked="" type="checkbox"/> TypografFontSets	Typograf - Fontmanager	(Verified) A. & M. Neuber Software	c:\program files (x86)\typograf\fontse...	1992. 06. 19. 23:22	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce				2021. 03. 15. 14:17	
<input checked="" type="checkbox"/> Delete Cached Standalo...			File not found: del		
<input checked="" type="checkbox"/> Delete Cached Update ...			File not found: del		
<input checked="" type="checkbox"/> Uninstall 21.016.0124.0...			File not found: mdir		
<input checked="" type="checkbox"/> Uninstall 21.016.0124.0...			File not found: mdir		
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2020. 08. 30. 1:46	
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	(Verified) Google LLC	c:\program files (x86)\google\chrome...	2021. 03. 05. 2:07	
<input checked="" type="checkbox"/> Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge...	2021. 03. 13. 9:33	
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\system32\msicories.dll	2019. 10. 25. 4:45	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2020. 07. 18. 18:57	

Ready.
Signed Windows Entries Hidden.

LogonSessions:

Listázza az aktuális bejelentkezéseket (sessions) a felhasználó vagy a szolgáltatás nevével, a bejelentkezés típusával, idejével, azonosítójával.

```
Administrator: C:\WINDOWS\system32\cmd.exe
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:00003e7:
User name: WORKGROUP\PETI-PC$
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: S-1-5-18
Logon time: 2021. 03. 15. 18:22:32
Logon server:
DNS Domain:
UPN:

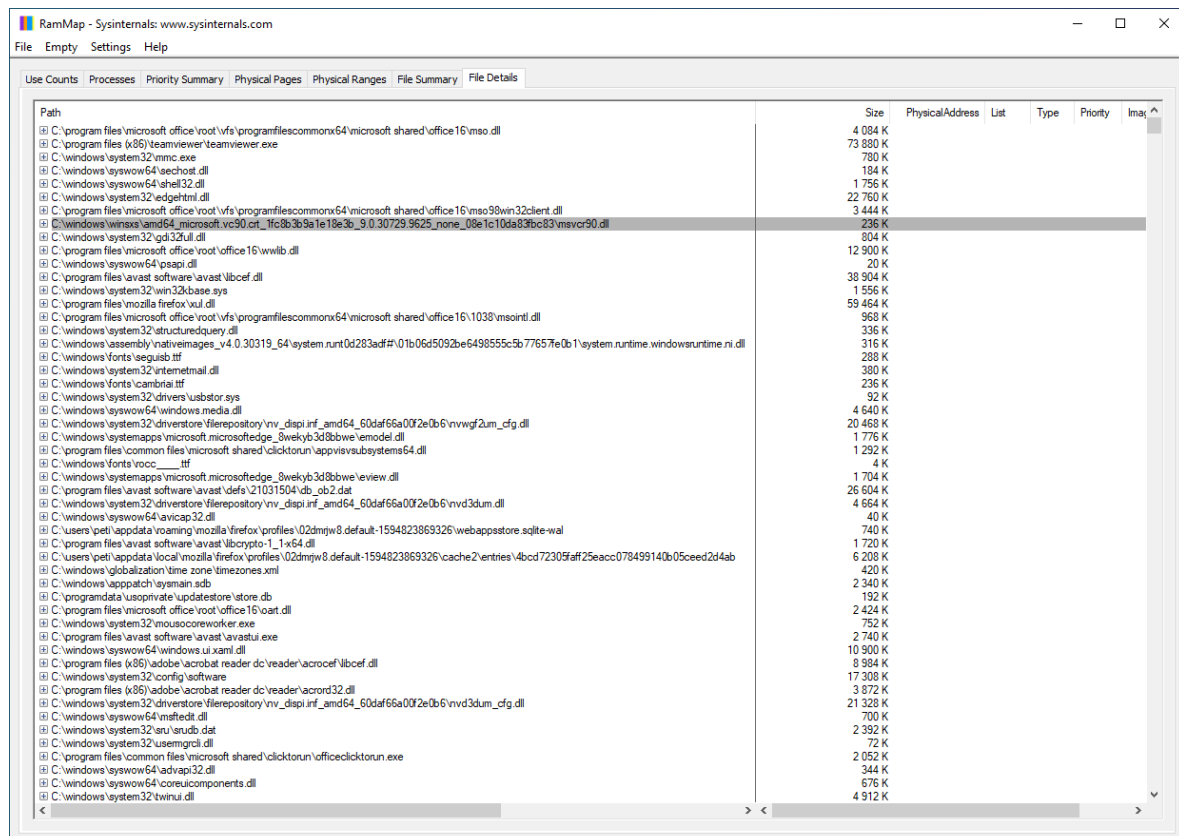
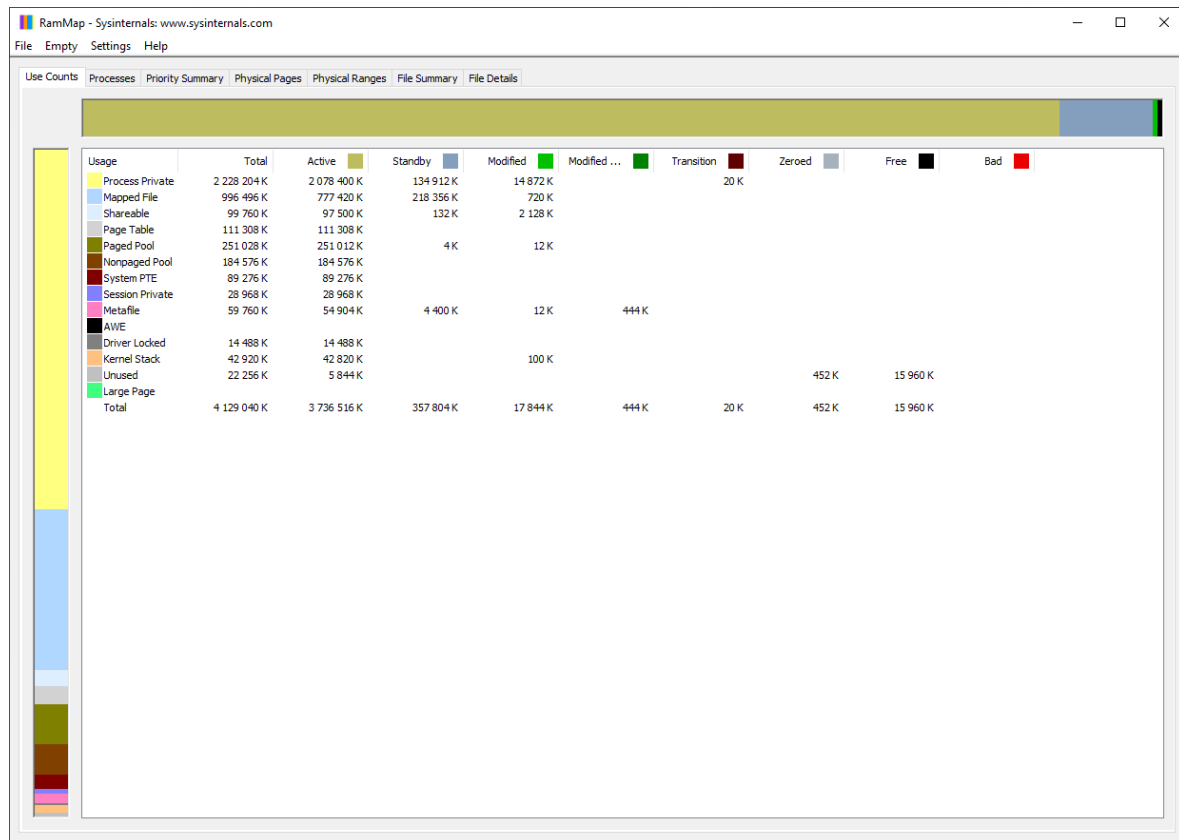
[1] Logon session 00000000:0000f378:
User name:
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: (none)
Logon time: 2021. 03. 15. 18:22:32
Logon server:
DNS Domain:
UPN:

[2] Logon session 00000000:0000fba6:
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. 15. 18:22:32
Logon server:
DNS Domain:
UPN:

[3] Logon session 00000000:0000fbb1:
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. 15. 18:22:32
```

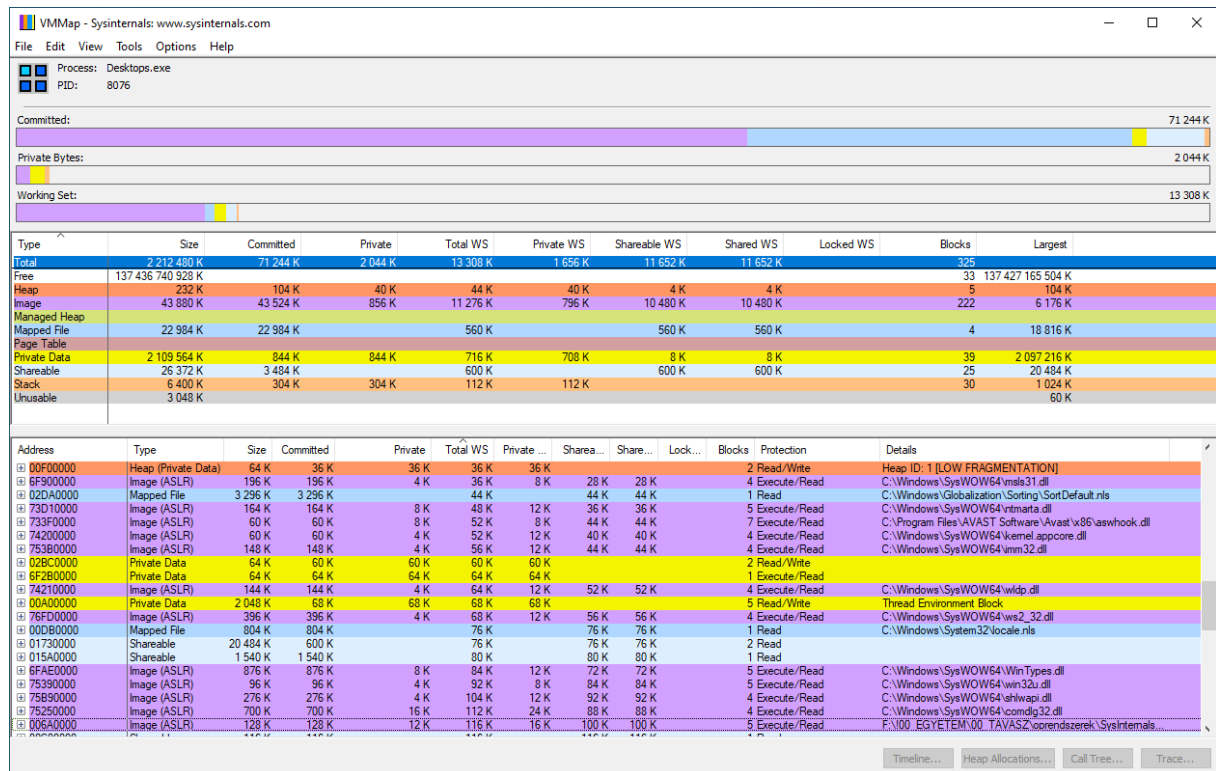
RamMap:

Részletes információt nyújt a fizikai memória használatáról, pl. mennyi memóriát használ a rendszermag vagy a driverek, stb.



VMMap:

Processzek memóriahasználatának (fizikai és virtuális memória) elemzésére szolgáló program.



AIDA64 Engineer:

Professzionális rendszerinformációs és rendszerdiagnosztikai program. Szolgáltatásai többek között: hardverfelismerés, teljesítménymérés, hardverdiagnosztika, stabilitásteszt, érzékelőfigyelés, szoftveranalitika, jelentéskészítés.

The screenshot displays the AIDA64 Engineer software interface, which is used for system information and diagnostics. The main window is titled "AIDA64 Engineer [TRIAL VERSION]". It features a menu bar with options like Fáj, Nézet, Riport, Kedvencek, Eszközök, and Súgó. Below the menu bar, there are icons for navigation and actions such as Riport, Vásárlás, BIOS frissítések, and Illesztőprogram frissítések.

The main content area is divided into two panes. The left pane, titled "Menü", shows a tree view of system components including Számítógép, Alaplap, CPU, CPUID, Alaplap, Memória, SPD, Lapkakészlet, BIOS, ACPI, Operációs rendszer, Operációs rendszer, Folyamatok, Illesztőprogramok, Szolgáltatások, AX fájlok, DLL fájlok, Tanúsítványok, Üzemidő, Kiszolgáló, Megjelenítés, Multimédia, Háttértár, Hálózat, DirectX, Eszközök, Szoftver, Biztonság, Beállítások, Adatbázis, and Sebesség. The right pane, titled "Mező", displays detailed information for selected components, including their values and units.

The "Mező" pane shows the following information:

- Utasításkészlet:** x86, x86-64, MMX, SSE, SSE2, SSE3, SSSE3, SSE4.1, SSE4.2, AVX
- Eredeti órajel:** [TRIAL VERSION]
- Min / Max CPU szorzó:** 16x / 33x
- Engineering Sample:** Nem
- L1 kód gyorsítótár:** 32 KB per core
- L1 adat gyorsítótár:** [TRIAL VERSION]
- L2 gyorsítótár:** 256 KB per core (On-Die, ECC, Full-Speed)
- L3 gyorsítótár:** 3 MB (On-Die, ECC, Full-Speed)
- CPU fizikai információk:**
 - Tokozás típusa:** 1155 Contact FC-LGA
 - Tokozás mérete:** 37.5 mm x 37.5 mm
 - Gyártási technológia:** 22 nm, CMOS, Cu, High-K + Metal Gate
 - Processzormag mérete:** [TRIAL VERSION]
 - Tipikus teljesítmény felvétel:** 55 W
- CPU gyártó:**
 - Cégnév:** Intel Corporation
 - Termék információ:** <https://ark.intel.com/content/www/us/en/ark/search.html?q=Inte...>
 - Illesztőprogram frissítés:** <http://www.aida64.com/goto/?p=drvupdates>
- Multi CPU:**
 - Alaplap azonosítója:** A M I ALASKA
 - CPU #1:** Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz, 3293 MHz
 - CPU #2:** Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz, 3293 MHz
 - CPU #3:** Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz, 3293 MHz
 - CPU #4:** Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz, 3293 MHz
- CPU kihasználtság:**
 - 1. CPU / 1. mag / 1. SMT egy...:** 0%
 - 1. CPU / 1. mag / 2. SMT egy...:** 1%
 - 1. CPU / 2. mag / 1. SMT egy...:** 1%
 - 1. CPU / 2. mag / 2. SMT egy...:** 1%

The bottom pane, titled "Riport - AIDA64", shows a summary of system information and a list of components. It includes fields for Verzió, Sebességmérő modul, Honlap, Riport típusa, Számítógép, Riport készítő, Operációs rendszer, Célum, and Idő. The "Összegzés" section provides a detailed overview of the system's hardware and software configuration, including the motherboard, CPU, memory, and storage details.

CPU-Z:

Rendszerinformációs, rendszerprofil-készítő program. Információt nyújt a különböző összetevőkről (processzor, gyorsítótár, memória, alaplap, lapkakészlet stb.), valós idejű mérési adatokat szolgáltat (pl. a processzormagok belső frekvenciájáról), „benchmark” jellegű összehasonlítást, jelentést készíthetünk vele, stb.

CPU-Z Ver. 1.95.0.x64

CPU | Caches | Mainboard | Memory | SPD | Graphics | Bench | About

Processor

Name	Intel Core i3 3220		
Code Name	Ivy Bridge	Max TDP	55.0 W
Package	Socket 1155 LGA		
Technology	22 nm	Core Voltage	1.000 V

Specification Intel® Core™ i3-3220 CPU @ 3.30GHz

Family	6	Model	A	Stepping	9
Ext. Family	6	Ext. Model	3A	Revision	L1

Instructions: MMX, SSE, SSE2, SSE3, SSSE3, SSE4.1, SSE4.2, EM64T, VT-x, AVX

Clocks (Core #0)

Core Speed	3292.14 MHz
Multiplier	x 33.0 (16 - 33)
Bus Speed	99.76 MHz
Rated FSB	

Cache

L1 Data	2 x 32 KBytes	8-way
L1 Inst.	2 x 32 KBytes	8-way
Level 2	2 x 256 KBytes	8-way
Level 3	3 MBytes	12-way

Selection: Socket #1 Cores: 2 Threads: 4

CPU-Z Ver. 1.95.0.x64 Tools Validate Close

CPU-Z Ver. 1.95.0.x64

CPU | Caches | Mainboard | Memory | SPD | Graphics | **Bench** | About

CPU Single Thread

This Processor	59 %
<input checked="" type="checkbox"/> Reference	100 %

CPU Multi Thread

This Processor	158 %
<input type="checkbox"/> Reference	1748 %

☐ Threads: 4 Multi Thread Ratio: 2.68

Benchmark: Version 17.01.64

Bench CPU Stress CPU Submit and Compare

This Processor: Intel® Core™ i3-3220 CPU @ 3.30GHz

Reference: Intel(R) Core(TM) i9-7980XE CPU @ 2.60GHz (18C/36T)

CPU-Z Ver. 1.95.0.x64 Tools Validate Close

GPU-Z:

A videokártyára ill. grafikus processzorra specializált rendszerinformációs és diagnosztikai program. Valós időben megfigyelhetjük pl. a GPU hőmérsékletét, a hűtő fordulatszámát, az eszköz memóriahasználatát, stb. Érdekesség, hogy a Lookup gomb segítségével a techpowerup.com weboldalán a videokártyánk technikai jellemzőit ismertető lapra jutunk, ahol más hasonló termékekkel is összehasonlíthatjuk azt.

