

Operációs Rendszerek BSC

3. gyakorlat

2021.február 24.

Készítette:

Kércsi Bence

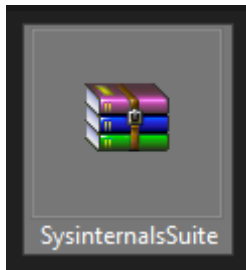
Programtervező Informatikus

ILVIYV

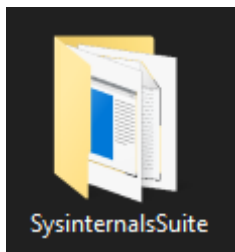
1.feladat:

Tölts le a *Sysinternals Suite* csomagot, majd csomagolja ki. A Windows belső működését lehet tanulmányozni, vagy a hibakeresésben segít.

<https://docs.microsoft.com/hu-hu/sysinternals/downloads/sysinternals-suite>



Letöltést követően ez a tömörített file jelent meg, amit aztán kicsomagoltam:



2. A Sysinternals weboldalon kategóriákba sorolva hasznos programok érhetők el:

a) File and Disk Utilities (Disk2vhd)

b) Networking Utilities (TCPView)

c) Process Utilities (Process Explorer, Process Monitor, AutoRuns)

d) Security Utilities (LogonSession)

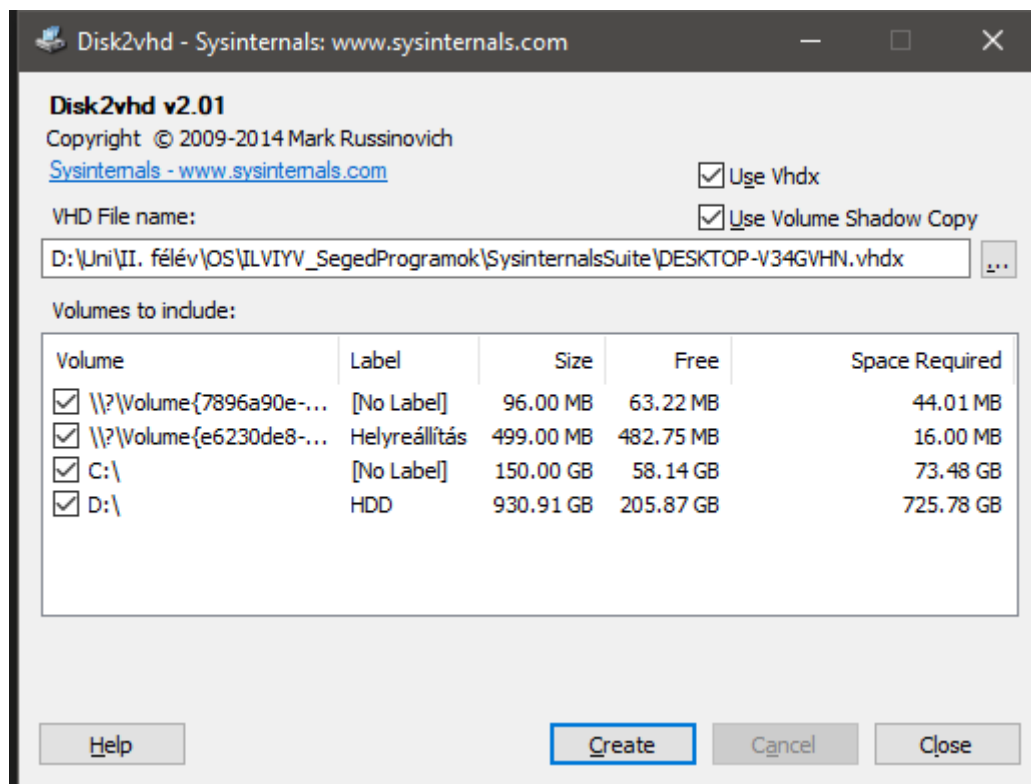
e) Information Utilities (RAMMap)

A felsorolt eszközök közül minden eszköz esetén tölts le, futtassa - és írja le a program szolgáltatásait és a futtatás eredményét egy-egy mondattal - majd mentse el a megadott dokumentumba (képernyőkép).

Megj: a zárójelben lévő eszközön felül válasszon még egy eszközt is.

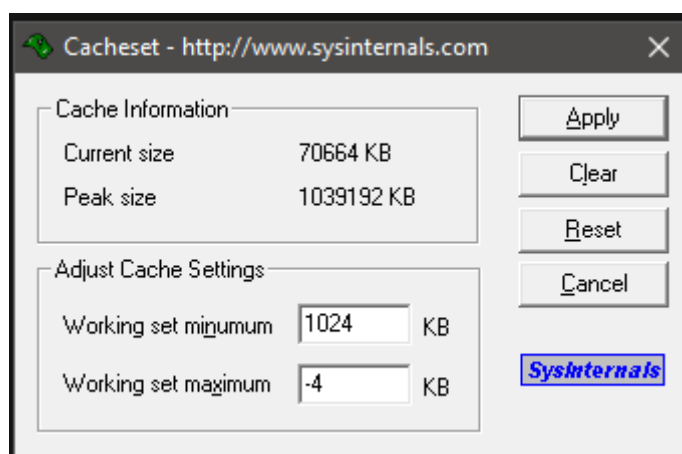
A, File and Disk Utilities:

Disk2vhd:



Kilistázza jelenleg milyen partíciókra van osztva, ezeknek mennyi a limitjük, illetve virtuális merevlemez tudunk vele létrehozni.

Cacheset:



Tudjuk vele állítani a cache méretét.

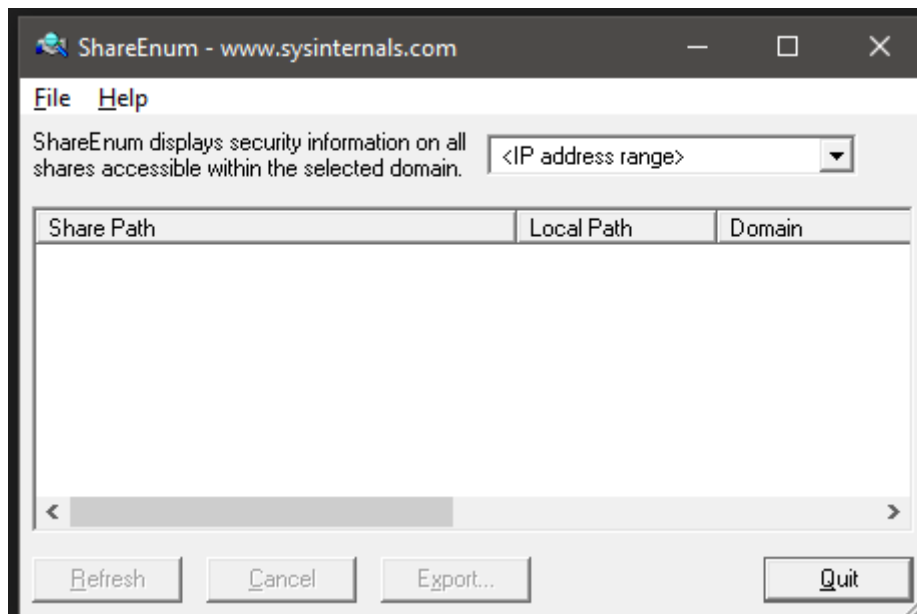
B, Networking Utilities:

TCPView:

TCPView - Sysinternals: www.sysinternals.com												
File Options Process View Help												
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	desktop-v34gvhn	63653	52.109.88.174	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-v34gvhn	63654	52.109.88.174	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-v34gvhn	63655	52.113.193.103	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-v34gvhn	63656	52.109.88.174	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-v34gvhn	63658	52.109.88.174	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-v34gvhn	63660	edge-star-shv-01-p...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-v34gvhn	63661	157.240.30.35	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-v34gvhn	63662	edge-star-shv-01-p...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-v34gvhn	63663	157.240.30.35	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-v34gvhn	63657	52.109.32.32	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-v34gvhn	63659	52.109.32.32	https	TIME_WAIT					
DiscSoftBusS...	14348	TCP	DESKTOP-V34GV...	45769	DESKTOP-V34GV...	0	LISTENING					
DiscSoftBusS...	14348	UDP	DESKTOP-V34GV...	45769	"	"						
lsass.exe	952	TCP	DESKTOP-V34GV...	49664	DESKTOP-V34GV...	0	LISTENING					
lsass.exe	952	TCPV6	[0.0.0.0:0.0.0.0]	49664	[0.0.0.0:0.0.0.0]	0	LISTENING					
nvcontainer.exe	17188	UDP	DESKTOP-V34GV...	52537	"	"						
NVIDIA Web...	8716	TCP	DESKTOP-V34GV...	63167	DESKTOP-V34GV...	0	LISTENING					
NVIDIA Web...	8716	UDP	DESKTOP-V34GV...	10030	"	"						
obs64.exe	13208	TCP	desktop-v34gvhn	63079	"	"	CLOSE_WAIT					
OneApp.IGCC...	3920	TCP	DESKTOP-V34GV...	808	DESKTOP-V34GV...	0	LISTENING					
OneApp.IGCC...	3920	TCPV6	[0.0.0.0:0.0.0.0]	808	[0.0.0.0:0.0.0.0]	0	LISTENING					
opera.exe	16172	TCP	desktop-v34gvhn	60816	edge-star-shv-01-p...	https	ESTABLISHED	1	51	1	30	
opera.exe	16172	TCP	desktop-v34gvhn	60918	edge-star-shv-01-p...	https	ESTABLISHED	1	52	1	30	
opera.exe	16172	TCP	desktop-v34gvhn	62983	142.250.27.188	5228	ESTABLISHED					
Razer Synaps...	14400	TCPV6	[0.0.0.0:0.0.0.1]	60895	[0.0.0.0:0.0.0.1]	5426	ESTABLISHED					
Razer Synaps...	14400	TCPV6	[0.0.0.0:0.0.0.1]	62002	[0.0.0.0:0.0.0.1]	5426	ESTABLISHED					
Razer Synaps...	14400	TCPV6	[0.0.0.0:0.0.0.1]	62007	[0.0.0.0:0.0.0.1]	5426	ESTABLISHED					
Razer Synaps...	14400	TCPV6	[0.0.0.0:0.0.0.1]	62010	[0.0.0.0:0.0.0.1]	5426	ESTABLISHED					
Razer Synaps...	14400	TCPV6	[0.0.0.0:0.0.0.1]	62028	[0.0.0.0:0.0.0.1]	5426	ESTABLISHED					
Razer Synaps...	14400	TCPV6	[0.0.0.0:0.0.0.1]	62033	[0.0.0.0:0.0.0.1]	5426	ESTABLISHED					
Razer Synaps...	14400	TCPV6	[0.0.0.0:0.0.0.1]	62035	[0.0.0.0:0.0.0.1]	5426	ESTABLISHED					
Razer Synaps...	14400	TCPV6	[0.0.0.0:0.0.0.1]	62039	[0.0.0.0:0.0.0.1]	5426	ESTABLISHED					
Razer Synaps...	6712	TCPV6	[0.0.0.0:0.0.0.1]	60738	[0.0.0.0:0.0.0.1]	5426	ESTABLISHED					
Razer Synaps...	6712	TCPV6	[0.0.0.0:0.0.0.1]	60742	[0.0.0.0:0.0.0.1]	5426	ESTABLISHED	2	167	2	28	
Razer Synaps...	6712	TCPV6	[0.0.0.0:0.0.0.1]	60746	[0.0.0.0:0.0.0.1]	5426	ESTABLISHED					
Razer Synaps...	6712	TCPV6	[0.0.0.0:0.0.0.1]	60749	[0.0.0.0:0.0.0.1]	5426	ESTABLISHED					
RzSDKServer...	4208	TCP	DESKTOP-V34GV...	13339	DESKTOP-V34GV...	0	LISTENING					
RzSDKServer...	4208	TCP	DESKTOP-V34GV...	1337	DESKTOP-V34GV...	0	LISTENING					
RzSDKServer...	4208	TCPV6	[0.0.0.0:0.0.0.0]	1337	[0.0.0.0:0.0.0.0]	0	LISTENING					
services.exe	324	TCP	DESKTOP-V34GV...	49670	DESKTOP-V34GV...	0	LISTENING					
services.exe	324	TCPV6	[0.0.0.0:0.0.0.0]	49670	[0.0.0.0:0.0.0.0]	0	LISTENING					
spoolsv.exe	6703	TCP	DESKTOP-V34GV...	5353	DESKTOP-V34GV...	0	LISTENING					
spoolsv.exe	3768	TCPV6	[0.0.0.0:0.0.0.0]	49663	[0.0.0.0:0.0.0.0]	0	LISTENING					
svchost.exe	1136	TCP	DESKTOP-V34GV...	epmap	DESKTOP-V34GV...	0	LISTENING					
svchost.exe	1328	TCP	DESKTOP-V34GV...	ms-wbt-server	DESKTOP-V34GV...	0	LISTENING					
svchost.exe	8368	TCP	DESKTOP-V34GV...	5040	DESKTOP-V34GV...	0	LISTENING					
svchost.exe	1608	TCP	DESKTOP-V34GV...	49666	DESKTOP-V34GV...	0	LISTENING					
svchost.exe	2052	TCP	DESKTOP-V34GV...	49667	DESKTOP-V34GV...	0	LISTENING					
svchost.exe	3140	TCP	DESKTOP-V34GV...	49668	DESKTOP-V34GV...	0	LISTENING					
svchost.exe	4080	TCP	desktop-v34gvhn	60689	51.103.5.159	https	ESTABLISHED					
svchost.exe	5664	TCP	DESKTOP-V34GV...	ms-do	DESKTOP-V34GV...	0	LISTENING					
svchost.exe	10792	UDP	DESKTOP-V34GV...	ssdp	"	"						
svchost.exe	10792	UDP	desktop-v34gvhn	ssdp	"	"						
svchost.exe	10792	UDP	desktop-v34gvhn	ssdp	"	"						
svchost.exe	15832	UDP	desktop-v34gvhn	qwave	"	"						
svchost.exe	15832	UDP	desktop-v34gvhn	qwave	"	"						
svchost.exe	1328	UDP	DESKTOP-V34GV...	ms-wbt-server	"	"						
svchost.exe	8368	UDP	DESKTOP-V34GV...	5050	"	"						
svchost.exe	3264	UDP	DESKTOP-V34GV...	5353	"	"						
svchost.exe	3264	UDP	DESKTOP-V34GV...	llmnr	"	"						
svchost.exe	4752	UDP	DESKTOP-V34GV...	49664	"	"						
svchost.exe	10792	UDP	desktop-v34gvhn	65525	"	"						
svchost.exe	10792	UDP	desktop-v34gvhn	65526	"	"						
svchost.exe	10792	UDP	DESKTOP-V34GV...	65527	"	"						
svchost.exe	1136	TCPV6	[0.0.0.0:0.0.0.0]	epmap	[0.0.0.0:0.0.0.0]	0	LISTENING					
svchost.exe	1328	TCPV6	[0.0.0.0:0.0.0.0]	ms-wbt-server	[0.0.0.0:0.0.0.0]	0	LISTENING					
svchost.exe	5664	TCPV6	[0.0.0.0:0.0.0.0]	ms-do	[0.0.0.0:0.0.0.0]	0	LISTENING					
svchost.exe	1608	TCPV6	[0.0.0.0:0.0.0.0]	49666	[0.0.0.0:0.0.0.0]	0	LISTENING					
svchost.exe	2052	TCPV6	[0.0.0.0:0.0.0.0]	49667	[0.0.0.0:0.0.0.0]	0	LISTENING					

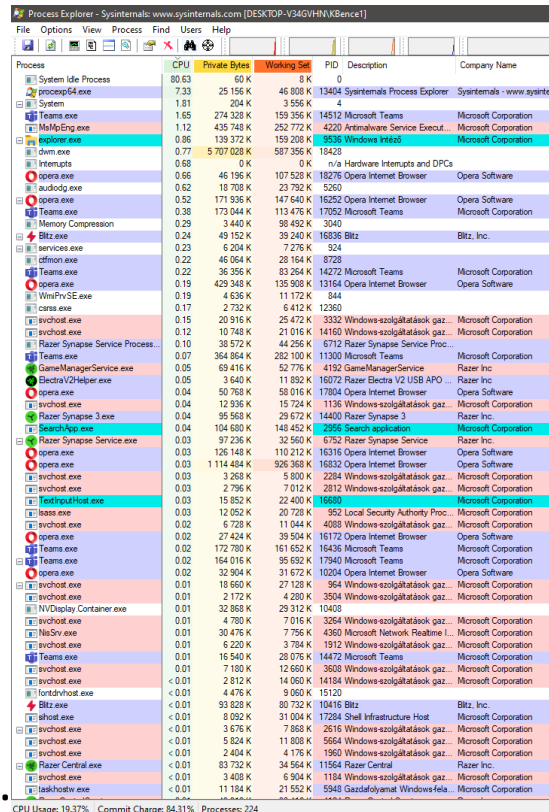
Kilistázza részletesen, a TCP és UDP kapcsolatok végpontját, az azokat használó processzek nevét, és címét.

ShareEnum:



A hálózathoz csatlakoztatott gépek közt lehetséges vele megnézni „megosztott” fileokat. Részletesebben nem tudom bemutatni ugyanis nem csatlakozok olyan hálózathoz amiben ez lehetséges lenne.

C, Process Utilities:



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	0.00	0 K	0 K	0		
smss64.exe	7.33	25 156 K	46 808 K	13494	Sysinternals Process Explorer	Sysinternals - www.sysinter...
System	1.81	204 K	3 556 K	4		
Teams.exe	1.65	274 328 K	159 356 K	14512	Microsoft Teams	Microsoft Corporation
MsMpEng.exe	1.12	435 748 K	252 772 K	4220	Antimalware Service Execut...	Microsoft Corporation
explorer.exe	0.86	139 372 K	159 208 K	9536	Windows Explorer	Microsoft Corporation
dmv.exe	0.77	5 707 028 K	587 356 K	18428		
Interrupts	0.68	0 K	0 K	n/a	Hardware Interrupts and DPCs	
opera.exe	0.66	46 196 K	107 528 K	18276	Opera Internet Browser	Opera Software
audiodg.exe	0.62	18 708 K	23 782 K	5260		
opera.exe	0.52	171 936 K	147 640 K	16292	Opera Internet Browser	Opera Software
Teams.exe	0.38	173 044 K	113 476 K	17052	Microsoft Teams	Microsoft Corporation
Memory Compression	0.29	3 440 K	38 492 K	3040		
Blitz.exe	0.24	49 152 K	39 340 K	18638	Blitz	Blitz, Inc.
services.exe	0.23	6 204 K	7 276 K	924		
ctfmon.exe	0.22	46 064 K	28 164 K	8728		
Teams.exe	0.22	36 356 K	83 264 K	14272	Microsoft Teams	Microsoft Corporation
opera.exe	0.19	429 348 K	135 980 K	13164	Opera Internet Browser	Opera Software
WinPrvSE.exe	0.19	4 636 K	11 172 K	844		
csrss.exe	0.17	2 732 K	6 412 K	12360		
svchost.exe	0.15	20 916 K	25 472 K	3332	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe	0.12	10 748 K	21 016 K	14160	Windows-szolgáltatások gaz...	Microsoft Corporation
Razer Synapse Service Process...	0.10	38 572 K	44 256 K	6712	Razer Synapse Service Proc...	
Teams.exe	0.07	364 864 K	282 100 K	11300	Microsoft Teams	Microsoft Corporation
GameManagerService.exe	0.06	69 416 K	52 776 K	4192	GameManagerService	Razer Inc.
Electra/Helper.exe	0.05	3 640 K	11 892 K	16072	Razer Electra V2 USB APO...	Razer Inc.
opera.exe	0.04	50 768 K	58 016 K	17804	Opera Internet Browser	Opera Software
svchost.exe	0.04	12 936 K	15 724 K	1136	Windows-szolgáltatások gaz...	Microsoft Corporation
Razer Synapse 3.exe	0.04	95 568 K	29 672 K	14400	Razer Synapse 3	Razer Inc.
SearchIndexer.exe	0.04	104 680 K	148 452 K	2956	Search application	Microsoft Corporation
Razer Synapse Service.exe	0.03	97 236 K	32 560 K	6752	Razer Synapse Service	Razer Inc.
opera.exe	0.03	126 148 K	110 212 K	16316	Opera Internet Browser	Opera Software
opera.exe	0.03	1 114 484 K	926 368 K	16332	Opera Internet Browser	Opera Software
svchost.exe	0.03	3 258 K	5 800 K	2284	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe	0.03	2 796 K	7 012 K	2812	Windows-szolgáltatások gaz...	Microsoft Corporation
TextInputHost.exe	0.03	15 852 K	22 400 K	16680		Microsoft Corporation
lsass.exe	0.03	12 052 K	20 728 K	362	Local Security Authority Proc...	Microsoft Corporation
svchost.exe	0.02	6 728 K	11 044 K	4082	Windows-szolgáltatások gaz...	Microsoft Corporation
opera.exe	0.02	27 424 K	39 504 K	16172	Opera Internet Browser	Opera Software
Teams.exe	0.02	172 780 K	161 652 K	16436	Microsoft Teams	Microsoft Corporation
Teams.exe	0.02	164 016 K	95 692 K	17940	Microsoft Teams	Microsoft Corporation
opera.exe	0.02	32 904 K	31 672 K	10204	Opera Internet Browser	Opera Software
svchost.exe	0.01	18 660 K	27 128 K	964	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe	0.01	2 172 K	4 280 K	3504	Windows-szolgáltatások gaz...	Microsoft Corporation
NVDisplay Container.exe	0.01	32 868 K	29 312 K	10408		
svchost.exe	0.01	4 780 K	7 016 K	3064	Windows-szolgáltatások gaz...	Microsoft Corporation
NisSrv.exe	0.01	30 476 K	7 756 K	4360	Microsoft Network Realtime I...	Microsoft Corporation
svchost.exe	0.01	6 220 K	3 784 K	1912	Windows-szolgáltatások gaz...	Microsoft Corporation
Teams.exe	0.01	16 540 K	28 076 K	14472	Microsoft Teams	Microsoft Corporation
svchost.exe	0.01	7 180 K	12 660 K	3608	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe	< 0.01	2 812 K	14 060 K	14184	Windows-szolgáltatások gaz...	Microsoft Corporation
fontdrvhost.exe	< 0.01	4 476 K	9 060 K	15120		
Blitz.exe	< 0.01	93 628 K	80 732 K	18418	Blitz	Blitz, Inc.
ssh.exe	< 0.01	8 692 K	31 004 K	17284	Shell Infrastructure Host	Microsoft Corporation
svchost.exe	< 0.01	3 676 K	7 868 K	2616	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe	< 0.01	5 824 K	11 808 K	5684	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe	< 0.01	2 404 K	4 176 K	1590	Windows-szolgáltatások gaz...	Microsoft Corporation
Razer Central.exe	< 0.01	83 732 K	34 564 K	11564	Razer Central	Razer Inc.
svchost.exe	< 0.01	3 408 K	6 904 K	1184	Windows-szolgáltatások gaz...	Microsoft Corporation
taskhostv.exe	< 0.01	11 184 K	21 552 K	5948	Gazdálkodási Windows-fel...	Microsoft Corporation

CPU Usage: 19.37% | Commit Charge: 84.31% | Processes: 224








Process Explorer:


















Megmutatja, hogy milyen DLL processzek futnak vagy vannak betöltve. Láthatjuk a processzek nevét, a CPU használatukat, egy rövid leírást, ahol van ott gyártó/tulaj nevét.

Process Monitor:

Process Monitor - Sysinternals: www.sysinternals.com

FileEditEventFilterToolsOptionsHelp





Time	Process Name	PID	Operation	Path	Result	Detail
13:03...	svchost.exe	2388	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI...	NAME NOT FOUND	Desired Access: R...
13:03...	svchost.exe	2388	RegOpenKey	HKU\S-1-5-18	REPARSE	Desired Access: M...
13:03...	svchost.exe	2388	RegOpenKey	HKU\DEFAULT	SUCCESS	Desired Access: M...
13:03...	svchost.exe	2388	RegOpenKey	HKU\DEFAULT\Software\Policies\Mic...	NAME NOT FOUND	Desired Access: R...
13:03...	svchost.exe	2388	RegOpenKey	HKU\DEFAULT\Control Panel\Desktop	SUCCESS	Desired Access: R...
13:03...	svchost.exe	2388	RegQueryValue	HKU\DEFAULT\Control Panel\Desktop...	BUFFER OVERFL...	Length: 12
13:03...	svchost.exe	2388	RegQueryValue	HKU\DEFAULT\Control Panel\Desktop...	SUCCESS	Type: REG_MULT...
13:03...	svchost.exe	2388	RegCloseKey	HKU\DEFAULT\Control Panel\Desktop	SUCCESS	
13:03...	svchost.exe	2388	RegOpenKey	HKU\DEFAULT	SUCCESS	
13:03...	svchost.exe	2388	ReadFile	C:\Windows\System32\ntdll.dll	SUCCESS	Offset: 1 502 720, ...
13:03...	svchost.exe	2388	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 690 688, Le...
13:03...	svchost.exe	2388	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI...	NAME NOT FOUND	Desired Access: R...
13:03...	svchost.exe	2388	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 678 400, Le...
13:03...	svchost.exe	2388	RegOpenKey	HKU\S-1-5-18	REPARSE	Desired Access: M...
13:03...	svchost.exe	2388	RegOpenKey	HKU\DEFAULT	SUCCESS	Desired Access: M...
13:03...	svchost.exe	2388	RegOpenKey	HKU\DEFAULT\Software\Policies\Mic...	NAME NOT FOUND	Desired Access: R...
13:03...	svchost.exe	2388	RegOpenKey	HKU\DEFAULT\Control Panel\Desktop...	NAME NOT FOUND	Desired Access: R...
13:03...	svchost.exe	2388	RegCloseKey	HKU\DEFAULT	SUCCESS	
13:03...	svchost.exe	2388	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 635 904, Le...
13:03...	svchost.exe	2388	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 312 832, Le...
13:03...	svchost.exe	2388	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 623 616, Le...
13:03...	svchost.exe	2388	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 257 536, Le...
13:03...	svchost.exe	2388	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
13:03...	svchost.exe	2388	QueryStandardI...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 3 1...
13:03...	svchost.exe	2388	QueryStandardI...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 3 1...
13:03...	svchost.exe	2388	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
13:03...	svchost.exe	2388	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI...	NAME NOT FOUND	Desired Access: R...
13:03...	svchost.exe	2388	RegOpenKey	HKU\S-1-5-18	REPARSE	Desired Access: M...
13:03...	svchost.exe	2388	RegOpenKey	HKU\DEFAULT	SUCCESS	Desired Access: M...
13:03...	svchost.exe	2388	RegOpenKey	HKU\DEFAULT\Software\Policies\Mic...	NAME NOT FOUND	Desired Access: R...
13:03...	svchost.exe	2388	RegOpenKey	HKU\DEFAULT\Control Panel\Desktop	SUCCESS	Desired Access: R...
13:03...	svchost.exe	2388	RegQueryValue	HKU\DEFAULT\Control Panel\Desktop...	BUFFER OVERFL...	Length: 12
13:03...	svchost.exe	2388	RegQueryValue	HKU\DEFAULT\Control Panel\Desktop...	SUCCESS	Type: REG_MULT...
13:03...	svchost.exe	2388	RegCloseKey	HKU\DEFAULT\Control Panel\Desktop	SUCCESS	
13:03...	svchost.exe	2388	RegCloseKey	HKU\DEFAULT	SUCCESS	
13:03...	svchost.exe	2388	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI...	NAME NOT FOUND	Desired Access: R...
13:03...	svchost.exe	2388	RegOpenKey	HKU\S-1-5-18	REPARSE	Desired Access: M...
13:03...	svchost.exe	2388	RegOpenKey	HKU\DEFAULT	SUCCESS	Desired Access: M...
13:03...	svchost.exe	2388	RegOpenKey	HKU\DEFAULT\Software\Policies\Mic...	NAME NOT FOUND	Desired Access: R...
13:03...	svchost.exe	2388	RegOpenKey	HKU\DEFAULT\Control Panel\Desktop...	NAME NOT FOUND	Desired Access: R...
13:03...	svchost.exe	2388	RegCloseKey	HKU\DEFAULT	SUCCESS	
13:03...	svchost.exe	2388	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
13:03...	svchost.exe	2388	QueryStandardI...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 3 1...
13:03...	svchost.exe	2388	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
13:03...	svchost.exe	2388	ReadFile	C:\Windows\System32\windows.storag...	SUCCESS	Offset: 6 918 144, ...
13:03...	svchost.exe	2388	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
13:03...	svchost.exe	2388	QueryStandardI...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 3 1...
13:03...	svchost.exe	2388	QueryStandardI...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 3 1...
13:03...	svchost.exe	2388	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
13:03...	svchost.exe	2388	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
13:03...	svchost.exe	2388	QueryStandardI...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 3 1...
13:03...	svchost.exe	2388	ReadFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 1 319 936, ...
13:03...	svchost.exe	2388	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
13:03...	svchost.exe	2388	ReadFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 1 300 480, ...
13:03...	svchost.exe	2388	ReadFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 1 299 968, ...
13:03...	svchost.exe	2388	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
13:03...	svchost.exe	2388	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
13:03...	svchost.exe	2388	ReadFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 1 295 360, ...
13:03...	svchost.exe	2388	RegOpenKey	HKCU\Software\Classes\CLSID\{1165... NAME NOT FOUND	Desired Access: R...	
13:03...	svchost.exe	2388	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
13:03...	svchost.exe	2388	RegOpenKey	HKCR\CLSID\{11659A23-5884-4D1B-9... SUCCESS	Desired Access: R...	
13:03...	svchost.exe	2388	RegQueryKey	HKCR\CLSID\{11659A23-5884-4D1B-9... SUCCESS	Query: Name	
13:03...	svchost.exe	2388	RegQueryKey	HKCR\CLSID\{11659A23-5884-4D1B-9... SUCCESS	Query: HandleTag...	
13:03...	svchost.exe	2388	RegOpenKey	HKCU\Software\Classes\CLSID\{1165... NAME NOT FOUND	Desired Access: R...	

Showing 138 494 of 291 168 events (47%) Backed by virtual memory

Itt futó processzek nevét láthatjuk, elindulásuk idejét, feladatukat, elérési útjukat

AutoRuns:

Autoruns - Sysinternals: www.sysinternals.com					
File Entry Options Help					
Filter:					
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit KnownDLLs Winlogon Winsock					
Autorun Entry	Description	Publisher	Image Path	Timestamp	Virus Total
<input checked="" type="checkbox"/> 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	
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021.02.22. 7:46	
<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\	2020.09.23. 4:18	
<input checked="" type="checkbox"/> Riot Vanguard	Vanguard tray notification.	(Verified) Riot Games, Inc.	c:\program files\riot\vanguard\vgtray.exe	2021.01.22. 21:31	
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2021.01.20. 13:17	
<input checked="" type="checkbox"/> Acrobat Assistant 8.0	AcroTray	(Not verified) Adobe Systems Inc.	c:\program files (x86)\adobe\acrobat\	2020.07.30. 23:29	
<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"/> ElectraV2Helper	Razer Electra V2 USB APO Helper	(Verified) Razer USA Ltd.	c:\program files (x86)\razer\razer_ele...	2017.09.06. 2:53	
<input checked="" type="checkbox"/> Razer Synapse	Razer Synapse	(Verified) Razer USA Ltd.	c:\program files (x86)\razer\synapse\	2020.05.13. 13:32	
<input checked="" type="checkbox"/> Razer Cortex	CortexLauncher.exe	(Verified) Razer USA Ltd.	c:\program files (x86)\razer\razer cort...	2020.02.05. 9:20	
<input checked="" type="checkbox"/> HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021.02.19. 15:43	
<input checked="" type="checkbox"/> BitTorrent	BitTorrent	(Verified) BitTorrent Inc	c:\users\qwert\appdata\roaming\bit...	2020.08.12. 0:08	
<input checked="" type="checkbox"/> btweb			File not found: C:\Users\qwert\AppData...		
<input checked="" type="checkbox"/> com.blitz.app	Blitz	(Verified) Swift Media Entertainment, L...	c:\users\qwert\appdata\local\progra...	2021.01.23. 1:18	
<input checked="" type="checkbox"/> DAEMON Tools Lite Aut...	DAEMON Tools Lite Agent	(Verified) AVB Disc Soft, SIA	d:\program files\daemon tools lite\tda...	2020.09.03. 10:47	
<input checked="" type="checkbox"/> EpicGamesLauncher	EpicGamesLauncher	(Verified) Epic Games Inc.	d:\program files\epic games\launche...	2020.09.24. 16:11	
<input checked="" type="checkbox"/> Facebook MessengerDe...	Messenger	(Verified) Facebook, Inc.	c:\users\qwert\appdata\local\progra...	2020.07.06. 21:07	
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	c:\users\qwert\appdata\local\micros...	2021.03.10. 16:03	
<input checked="" type="checkbox"/> Opera Browser Assistant	Opera Browser Assistant	(Verified) Opera Software AS	c:\users\qwert\appdata\local\progra...	2020.11.24. 15:56	
<input checked="" type="checkbox"/> Synapse3	Razer Synapse 3	(Verified) Razer USA Ltd.	c:\program files (x86)\razer\synapse3...	1969.07.19. 15:08	
<input checked="" type="checkbox"/> Web Companion			File not found: C:\Program Files (x86)...		
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2020.11.05. 18:21	
<input checked="" type="checkbox"/> Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge...	2021.02.17. 4:41	
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	2019.10.25. 4:45	
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				2020.09.25. 8:05	
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\syswow64\mscories.dll	2019.10.25. 9:48	
<input checked="" type="checkbox"/> HKLM\Software\Classes\Protocols\Filter				2021.02.03. 22:24	
<input checked="" type="checkbox"/> text/xml	Microsoft Office XML MIME Filter	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft office...	2020.12.28. 23:39	
<input checked="" type="checkbox"/> HKLM\Software\Classes\ShellEx\ContextMenuHandlers				2020.10.19. 9:34	
<input checked="" type="checkbox"/> AccExt	Core Sync	(Verified) Adobe Systems Incorporated	c:\program files (x86)\common files\ad...	2018.02.27. 15:24	
<input checked="" type="checkbox"/> Adobe Acrobat Context...	Adobe Acrobat Context Menu	(Verified) Adobe Inc.	c:\program files (x86)\adobe\acrobat...	2020.07.30. 23:14	
<input checked="" type="checkbox"/> WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	d:\program files\winrar\varext.dll	2016.08.14. 20:15	
<input checked="" type="checkbox"/> HKLM\Software\Classes\Drive\ShellEx\ContextMenuHandlers				2020.09.18. 14:06	
<input checked="" type="checkbox"/> DaemonShellExtDriveLite	DAEMON Tools Lite	(Verified) AVB Disc Soft, SIA	d:\program files\daemon tools lite\tds...	2020.09.03. 10:47	
<input checked="" type="checkbox"/> HKLM\Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers				2020.09.18. 14:06	
<input checked="" type="checkbox"/> DaemonShellExtImageLite	DAEMON Tools Lite	(Verified) AVB Disc Soft, SIA	d:\program files\daemon tools lite\tds...	2020.09.03. 10:47	
<input checked="" type="checkbox"/> HKLM\Software\Classes\Directory\ShellEx\CopyHookHandlers				2020.10.26. 5:57	
<input checked="" type="checkbox"/> WinSCPCopyHook	Drag&Drop shell extension for WinSC...	(Verified) Martin Prikyl	d:\program files\winscp\dragext64.dll	2020.10.15. 12:05	
<input checked="" type="checkbox"/> HKLM\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers				2020.09.18. 12:37	
<input checked="" type="checkbox"/> NvCplDesktopContext	NVIDIA Display Shell Extension	(Verified) NVIDIA Corporation	c:\windows\system32\driverstore\file...	2020.10.01. 5:17	
<input checked="" type="checkbox"/> HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers				2020.10.19. 9:34	
<input checked="" type="checkbox"/> AccExt	Core Sync	(Verified) Adobe Systems Incorporated	c:\program files (x86)\common files\ad...	2018.02.27. 15:24	
<input checked="" type="checkbox"/> Adobe Acrobat Context...	Adobe Acrobat Context Menu	(Verified) Adobe Inc.	c:\program files (x86)\adobe\acrobat...	2020.07.30. 23:14	
<input checked="" type="checkbox"/> WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	d:\program files\winrar\varext.dll	2016.08.14. 20:15	
<input checked="" type="checkbox"/> HKLM\Software\Classes\Folder\ShellEx\DragDropHandlers				2020.09.18. 13:43	
<input checked="" type="checkbox"/> WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	d:\program files\winrar\varext.dll	2016.08.14. 20:15	
<input checked="" type="checkbox"/> HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers				2020.12.04. 16:21	
<input checked="" type="checkbox"/> AccExtIco1	Core Sync	(Verified) Adobe Systems Incorporated	c:\program files (x86)\common files\ad...	2018.02.27. 15:24	

Ez az automatikusan gép indítással induló processzeket listázza ki, indulásuk helyét, egy rövid leírást ad róluk, gyártójukat.

ListDDL:

```
File: C:\Program Files (x86)\Sysinternals\Suite\blitz.exe
0x0000000000000000 0x40000 C:\Windows\System32\powrprof.dll
0x0000000000000000 0x20000 C:\Windows\System32\UPDC.dll
0x0000000000000000 0x70000 C:\Windows\System32\Windows.UI.dll
0x0000000000000000 0x70000 C:\Windows\System32\WindowManagementAPI.dll
0x0000000000000000 0x20000 C:\Windows\System32\TextInputFramework.dll
0x0000000000000000 0x20000 C:\Windows\System32\inputhost.dll
0x0000000000000000 0x20000 C:\Windows\System32\wintypes.dll
0x0000000000000000 0x10000 C:\Windows\System32\Winapi_appcore.dll
0x0000000000000000 0x20000 C:\Windows\System32\combaseapi.dll
0x0000000000000000 0x30000 C:\Windows\System32\WS2_32.dll
0x0000000000000000 0x20000 C:\Windows\System32\comctl32.dll
0x0000000000000000 0x30000 C:\Windows\System32\PROPSYS.dll
0x0000000000000000 0x20000 C:\Windows\System32\ntmarta.dll
-----
blitz.exe pid: 7812
Command line: C:\Users\qwert\AppData\Local\Programs\Blitz\blitz.exe --user-data-dir=C:\Users\qwert\AppData\Local\Programs\Blitz\prefetch7 --no-rate-limit --monitor-self-annotation-type=crashpad-handler --database=C:\Users\qwert\AppData\Local\Programs\Blitz\Crashpad --url=https://sentry.blitz.rs/api/2/minidump/?entry_key=598e2f1b41249b84e0fcdcb04e45 --annotation_productName=Blitz --annotation_version=1.10.127 --annotation-prod=electron --annotation-ve
r=11.2.1 --initial-client-data=0x4dc,0x510,0x514,0x474,0x518,0x6b31000,0x6b31010,0x6b3101c
Base      Size      Path
0x0000000000000000 0x40000 C:\Users\qwert\AppData\Local\Programs\Blitz\blitz.exe
0x0000000000000000 0x10000 C:\Windows\System32\ntdll.dll
0x0000000000000000 0x50000 C:\Windows\System32\wow64.dll
0x0000000000000000 0x10000 C:\Windows\System32\wow64cpu.dll
0x0000000000000000 0x40000 C:\Windows\System32\wow64cpu.dll
0x0000000000000000 0x40000 C:\Users\qwert\AppData\Local\Programs\Blitz\blitz.exe
0x0000000000000000 0x20000 C:\Windows\System32\kernel32.dll
0x0000000000000000 0x10000 C:\Windows\System32\USER32.dll
0x0000000000000000 0x214000 C:\Windows\System32\USER32.dll
0x0000000000000000 0x20000 C:\Windows\System32\ole32.dll
0x0000000000000000 0x70000 C:\Windows\System32\ole32.dll
0x0000000000000000 0x10000 C:\Users\qwert\AppData\Local\Programs\Blitz\ffmpeg.dll
0x0000000000000000 0x120000 C:\Windows\System32\userbase.dll
0x0000000000000000 0x20000 C:\Windows\System32\combase.dll
0x0000000000000000 0x10000 C:\Windows\System32\ole32.dll
0x0000000000000000 0x20000 C:\Windows\System32\RPCRT4.dll
0x0000000000000000 0x20000 C:\Windows\System32\RSING32.dll
0x0000000000000000 0x20000 C:\Windows\System32\WS2_32.dll
0x0000000000000000 0x20000 C:\Windows\System32\GDI32.dll
0x0000000000000000 0xf0000 C:\Windows\System32\CRYPT32.dll
0x0000000000000000 0x10000 C:\Windows\System32\WinSxS.dll
0x0000000000000000 0x40000 C:\Windows\System32\gdi32full.dll
0x0000000000000000 0x10000 C:\Windows\System32\USER32.dll
0x0000000000000000 0x10000 C:\Windows\System32\WinSxS.dll
0x0000000000000000 0xf0000 C:\Windows\System32\advapi32.dll
0x0000000000000000 0x20000 C:\Windows\System32\RPCRT4.dll
0x0000000000000000 0x80000 C:\Windows\System32\VERSION.dll
0x0000000000000000 0x20000 C:\Windows\System32\USERENV.dll
0x0000000000000000 0x20000 C:\Windows\System32\WinSxS.dll
0x0000000000000000 0x60000 C:\Windows\System32\WINPOOL.DRV
0x0000000000000000 0x20000 C:\Windows\System32\WINHTTP.dll
0x0000000000000000 0x40000 C:\Windows\System32\Secur32.dll
0x0000000000000000 0x70000 C:\Windows\System32\sechost.dll
0x0000000000000000 0x10000 C:\Windows\System32\ole32.dll
0x0000000000000000 0x274000 C:\Windows\System32\UIAutomationCore.dll
0x0000000000000000 0x20000 C:\Windows\System32\SSPICLI.dll
0x0000000000000000 0x20000 C:\Windows\System32\PROPSYS.dll
0x0000000000000000 0x20000 C:\Windows\System32\RPCRT4.dll
0x0000000000000000 0x20000 C:\Windows\System32\cryptprimitives.dll
0x0000000000000000 0x40000 C:\Windows\System32\powrprof.dll
0x0000000000000000 0x20000 C:\Windows\System32\UPDC.dll
0x0000000000000000 0x70000 C:\Windows\System32\Windows.UI.dll
0x0000000000000000 0x70000 C:\Windows\System32\WindowManagementAPI.dll
0x0000000000000000 0x20000 C:\Windows\System32\TextInputFramework.dll
0x0000000000000000 0x20000 C:\Windows\System32\inputhost.dll
0x0000000000000000 0x20000 C:\Windows\System32\wintypes.dll
0x0000000000000000 0x10000 C:\Windows\System32\Winapi_appcore.dll
0x0000000000000000 0x20000 C:\Windows\System32\combaseapi.dll
0x0000000000000000 0x30000 C:\Windows\System32\WS2_32.dll
0x0000000000000000 0x20000 C:\Windows\System32\comctl32.dll
0x0000000000000000 0x30000 C:\Windows\System32\PROPSYS.dll
0x0000000000000000 0x20000 C:\Windows\System32\ntmarta.dll
```

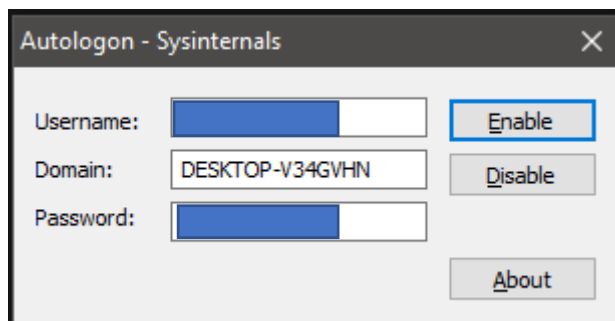
Kilistázza az elindított vagy beöltött DLL-eket.

D, Security Utilities:

LogonSession:

Valamilyen oknál fogva akár milyen módon próbáltam indítani nem indul.

AutoLogon:



Azt lehet megvalósítani vele, hogy egy adott felhasználói fiókba automatikusan belépjen, ha

megadjuk az ahhoz tartozó helyes felhasználónév, jelszó kombinációt.

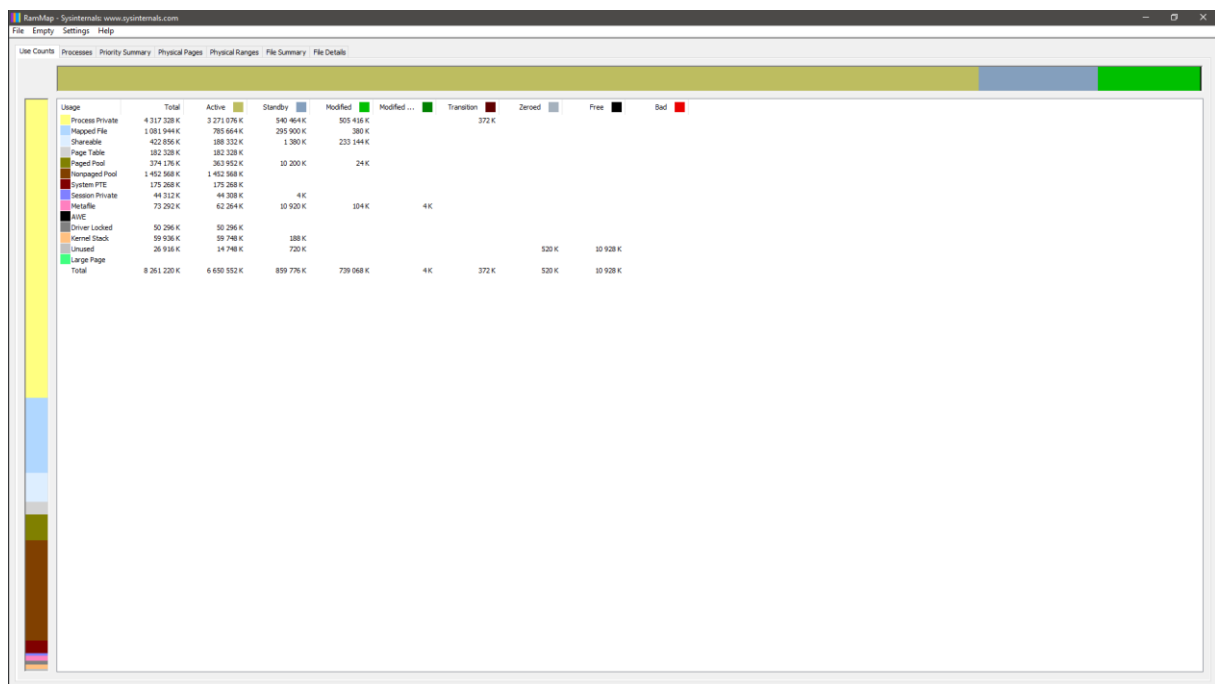
AccesEnum:



Megmutatja egy adott mappába melyik felhasználó csoportoknak milyen jogosultságaik vannak.

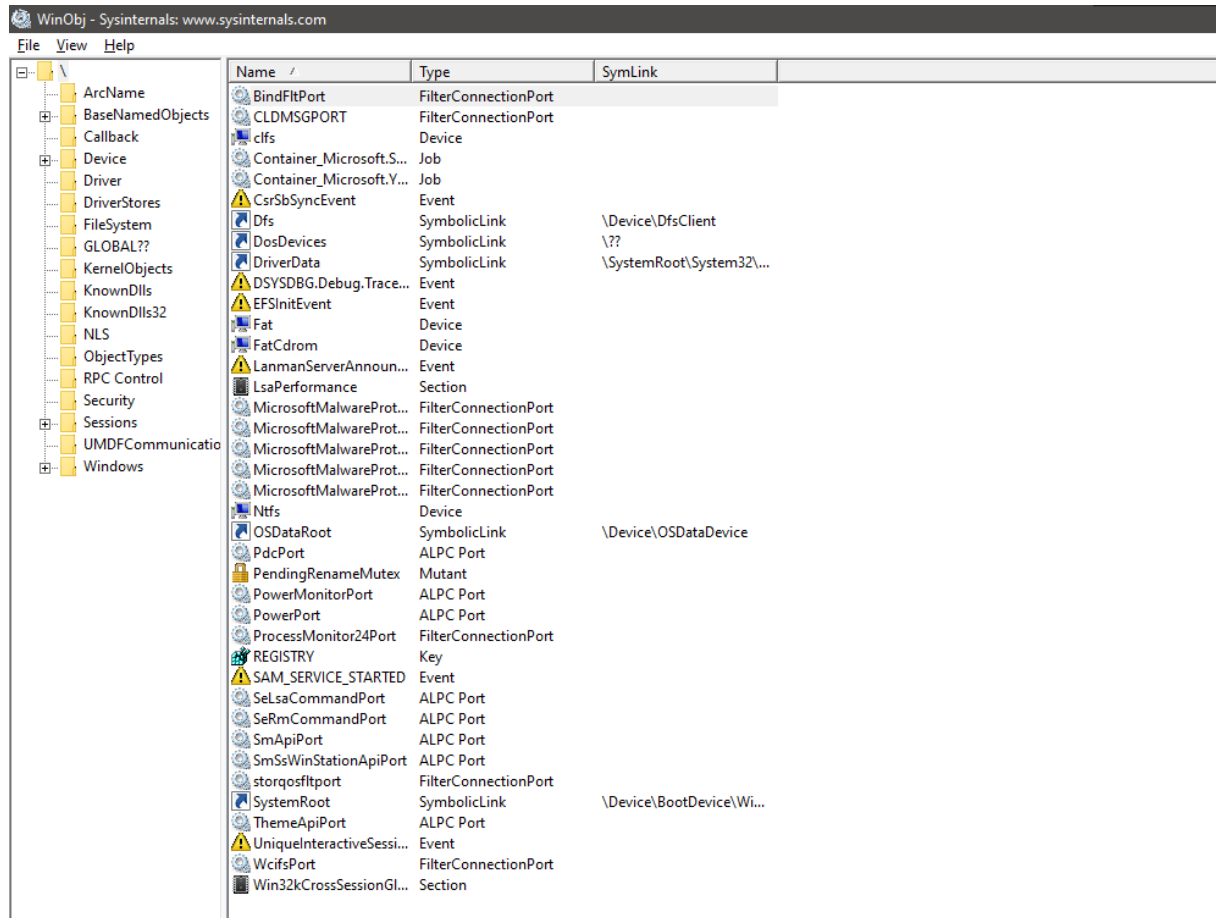
E, Information Utilities:

RAMMap:



Megmutatja, hogy mennyi RAM-ot használ a kernel illetve a driverek. Fizikai memóriáról is több információt is nyújt.

Winobj:



WinObj - Sysinternals: www.sysinternals.com

File View Help

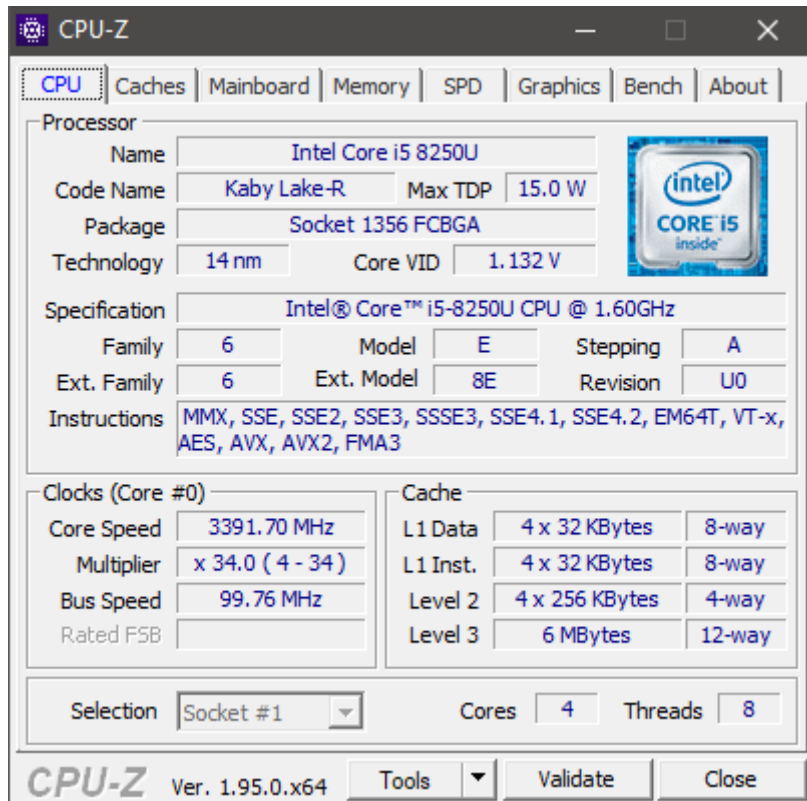
Name	Type	SymLink
ArcName		
BaseNamedObjects		
Callback		
Device		
Driver		
DriverStores		
FileSystem		
GLOBAL??		
KernelObjects		
KnownDlls		
KnownDlls32		
NLS		
ObjectTypes		
RPC Control		
Security		
Sessions		
UMDFCommunicatio		
Windows		
BindFtPort	FilterConnectionPort	
CLDMSGPORT	FilterConnectionPort	
clfs	Device	
Container_Microsoft.S...	Job	
Container_Microsoft.V...	Job	
CsrSbSyncEvent	Event	
Dfs	SymbolicLink	\Device\DfsClient
DosDevices	SymbolicLink	\??
DriverData	SymbolicLink	\SystemRoot\System32\...
DSYSDBG.Debug.Trace...	Event	
EFSInitEvent	Event	
Fat	Device	
FatCdrom	Device	
LanmanServerAnnoun...	Event	
LsaPerformance	Section	
MicrosoftMalwareProt...	FilterConnectionPort	
MicrosoftMalwareProt...	FilterConnectionPort	
MicrosoftMalwareProt...	FilterConnectionPort	
MicrosoftMalwareProt...	FilterConnectionPort	
MicrosoftMalwareProt...	FilterConnectionPort	
Ntfs	Device	
OSDataRoot	SymbolicLink	\Device\OSDataDevice
PdcPort	ALPC Port	
PendingRenameMutex	Mutant	
PowerMonitorPort	ALPC Port	
PowerPort	ALPC Port	
ProcessMonitor24Port	FilterConnectionPort	
REGISTRY	Key	
SAM_SERVICE_STARTED	Event	
SeLsaCommandPort	ALPC Port	
SeRmCommandPort	ALPC Port	
SmApiPort	ALPC Port	
SmSsWinStationApiPort	ALPC Port	
storqosfltport	FilterConnectionPort	
SystemRoot	SymbolicLink	\Device\BootDevice\Wi...
ThemeApiPort	ALPC Port	
UniqueInteractiveSessi...	Event	
WcifsPort	FilterConnectionPort	
Win32kCrossSessionGl...	Section	

Megmutatja az objektumokkal kapcsolatos információkat. Jó résskeresésre is a biztonsági rendszerben.

3. Töltse le és végezzen vizsgálatot az *AIDA64_Engineer_v5.98.4800_Portable*, *CPU-Z*, *GPU-Z* programokkal.

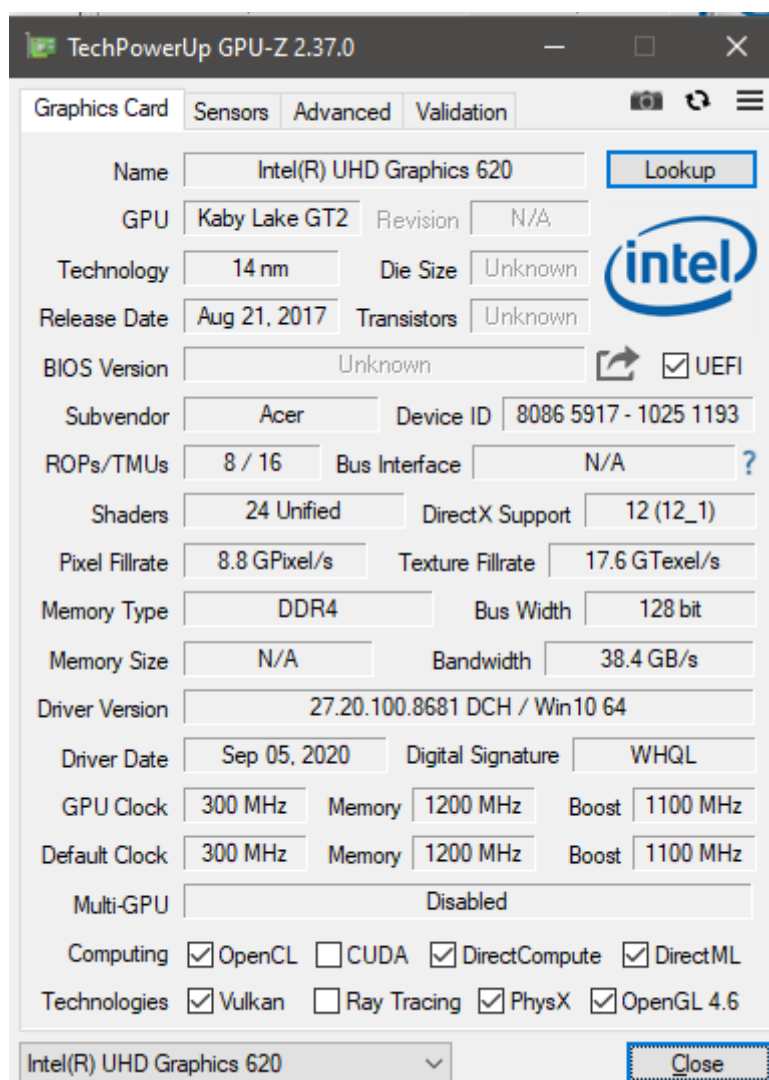
A felsorolt segédprogramoknak írja le a szolgáltatásait és a futtatás eredményét egy-egy mondattal - majd mentse el az alábbi dokumentumba (képernyőkép is).

CPU-Z:



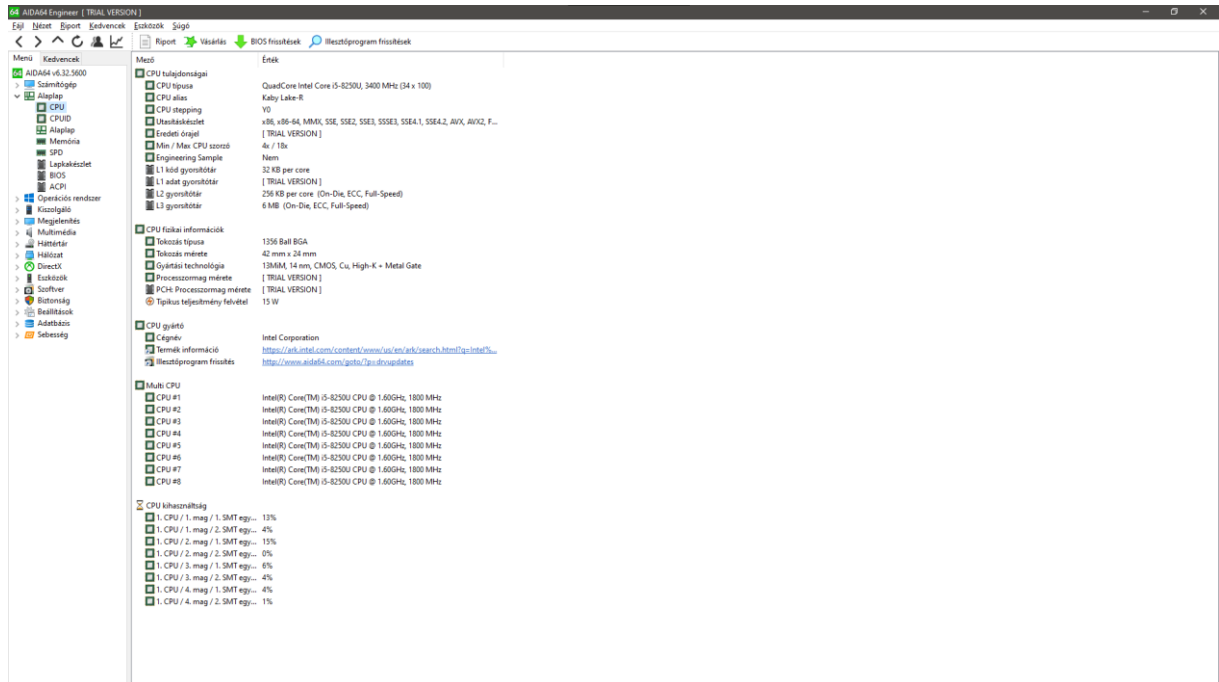
Információkat tartalmaz a CPU-ról. Milyen CPU van benne, hanyadik generációs, milyen órajelű, milyen technológiával készült, illetve további információkat is nézhetünk vele, például alaplap, memória, gpu stb.

GPU-Z:



Részletesebb információkkal szolgál a GPU-ról. Milyen típusú, milyen technikával készült, kiadásának ideje stb.

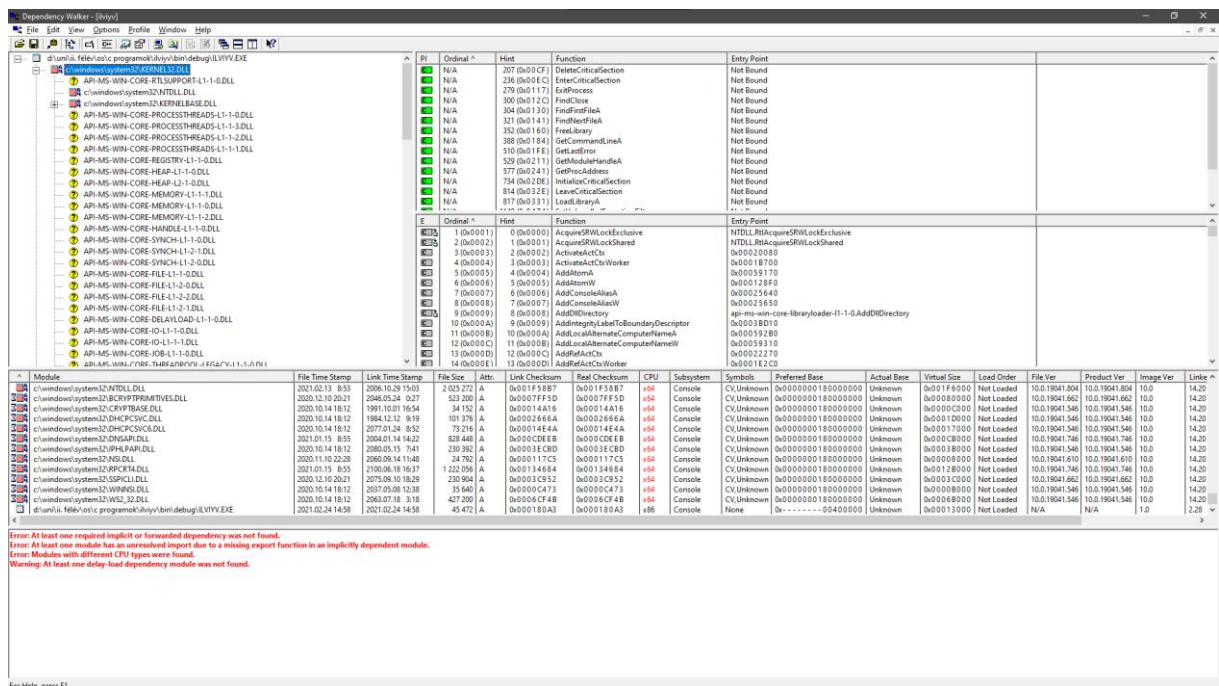
AIDA:



Nagyon részletes leírást ad minden bal sávban felsorolt elemről.

4. Tölts le a következő programot: Dependency Walker

Feladata: a segédprogram *megvizsgálja* milyen könyvtárakra, és azon belül milyen függvényekre hivatkozik egy elindított program.



Rengeteg api fut.

Ordinal	Hint	Function	Entry Point
N/A	70 (0x0046)	EtwGetTraceEnableFlags	Not Bound
N/A	71 (0x0047)	EtwGetTraceEnableLevel	Not Bound
N/A	72 (0x0048)	EtwGetTraceLoggerHandle	Not Bound
N/A	79 (0x004F)	EtwRegisterTraceGuidsW	Not Bound
N/A	84 (0x0054)	EtwTraceMessage	Not Bound
N/A	86 (0x0056)	EtwUnregisterTraceGuids	Not Bound
N/A	253 (0x01FD)	NtClose	Not Bound
N/A	416 (0x01A0)	NtOpenFile	Not Bound
N/A	419 (0x01A3)	NtOpenKey	Not Bound
N/A	477 (0x01DD)	NtQueryInformationProcess	Not Bound
N/A	510 (0x01FE)	NtQueryValueKey	Not Bound
N/A	627 (0x0273)	NtTerminateProcess	Not Bound
N/A	723 (0x02D3)	RtlAllocateHeap	Not Bound
N/A	755 (0x02F3)	RtlCaptureContext	Not Bound
8 (0x0009)	N/A	A_SHAFinal	0x0007E8B0
9 (0x0009)	0 (0x0000)	A_SHAInit	0x0007C290
10 (0x000A)	1 (0x0001)	A_SHAUpdate	0x0005D0C0
11 (0x000B)	2 (0x0002)	AlpcAdjustCompletionListConcurrencyCount	0x0005D100
12 (0x000C)	3 (0x0003)	AlpcFreeCompletionListMessage	0x000E0700
13 (0x000D)	4 (0x0004)	AlpcGetCompletionListMessageInformation	0x000E9200
14 (0x000E)	5 (0x0005)	AlpcGetCompletionListMessageAttributes	0x000E9230
15 (0x000F)	6 (0x0006)	AlpcGetHeaderSize	0x000E0750
16 (0x0010)	7 (0x0007)	AlpcGetMessageAttribute	0x000E9550
17 (0x0011)	8 (0x0008)	AlpcGetMessageFromCompletionList	0x000E9610
18 (0x0012)	9 (0x0009)	AlpcGetOutstandingCompletionListMessageCount	0x000E9F00
19 (0x0013)	10 (0x000A)	AlpcInitializeMessageAttribute	0x000E96C0
20 (0x0014)	11 (0x000B)	AlpcMaxAllowedMessageLength	0x000E9580
21 (0x0015)	12 (0x000C)		0x000E44E0

b,c:Nem tudom, akár hogy próbáltam értelmezni, nincs meg a szükséges előzetes informatikai tudásom ahhoz, hogy az épp működő folyamatokat értelmezni tudjam.