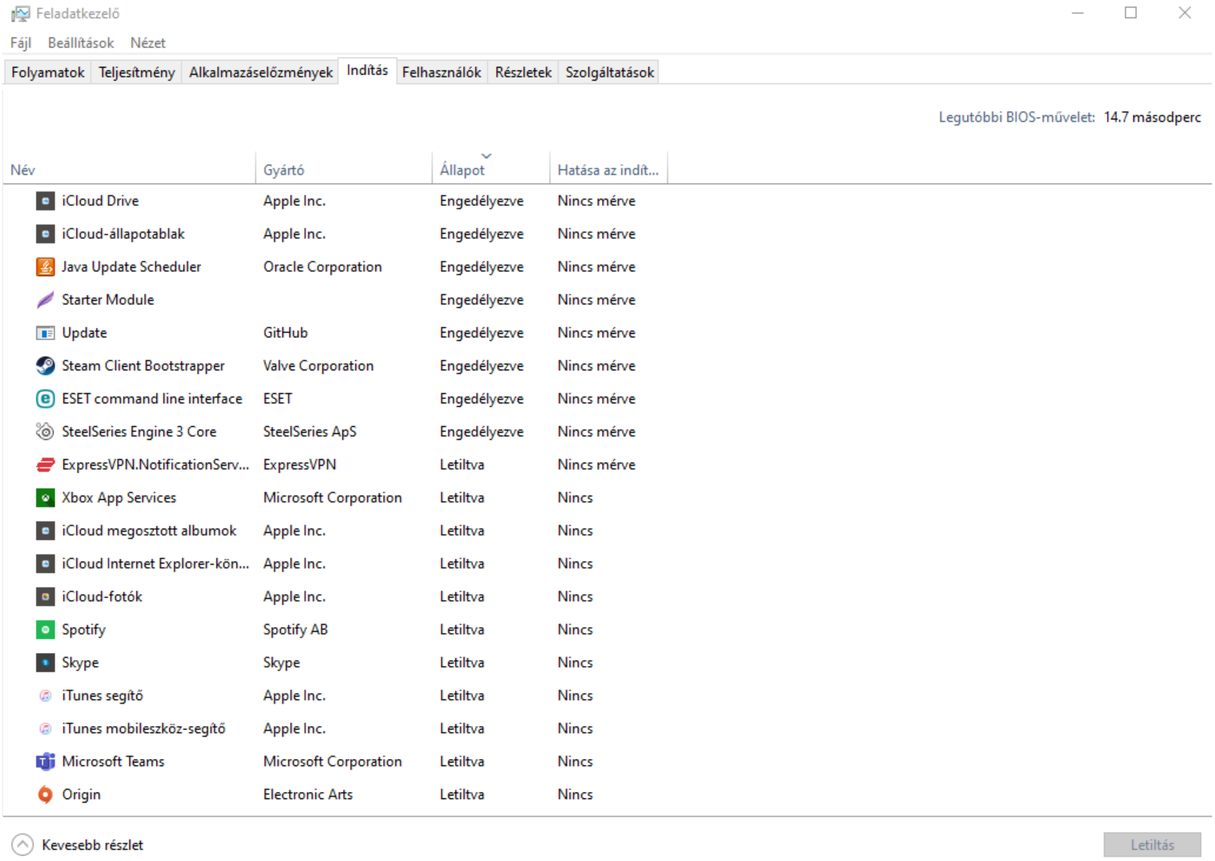
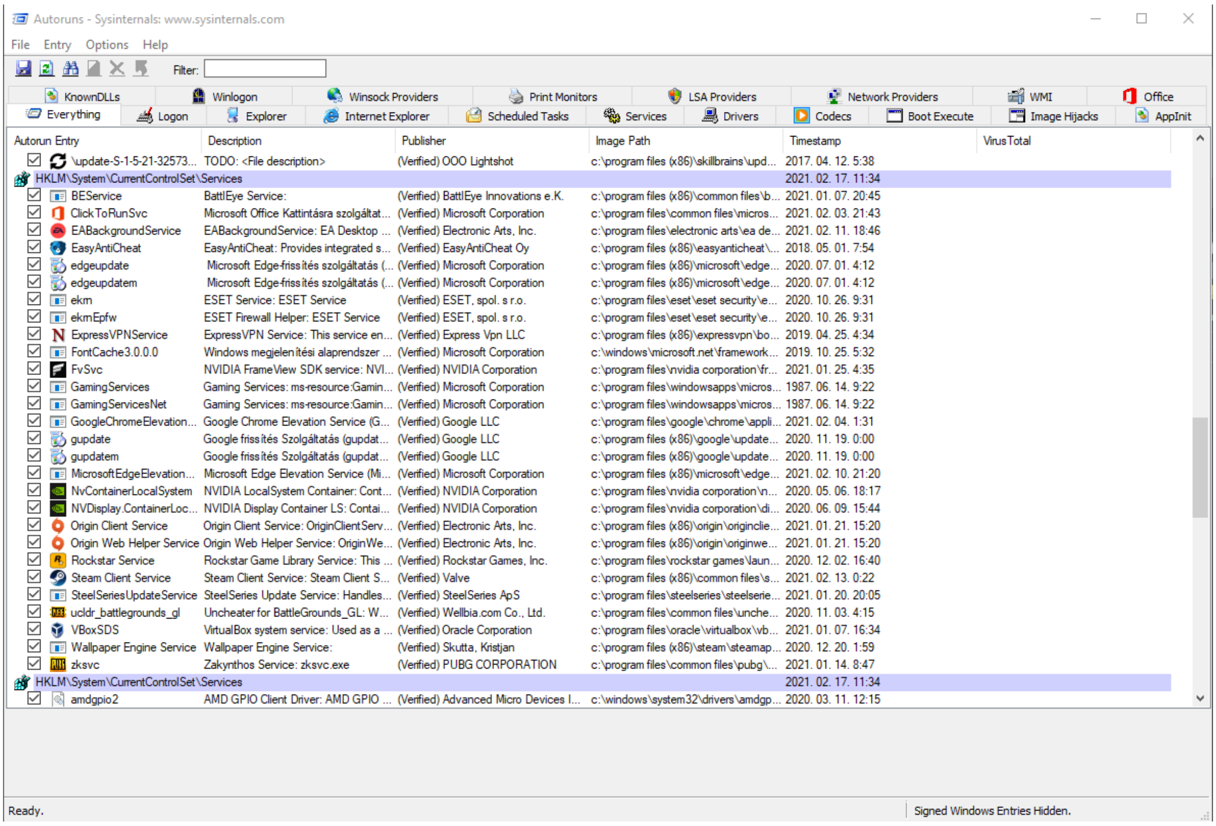
Babik Szilárd Kristóf – A6NQW1 – OS 2. gyakorlat

A számítógépemen az automatikusan induló programok listája a Feladatkezelő „Indítás” ablakából és az Autoruns segédprogramból (részlet):



Legutóbbi BIOS-művelet: 14.7 másodperc

Név	Gyártó	Állapot	Hatása az indít...
iCloud Drive	Apple Inc.	Engedélyezve	Nincs mérve
iCloud-állapotablak	Apple Inc.	Engedélyezve	Nincs mérve
Java Update Scheduler	Oracle Corporation	Engedélyezve	Nincs mérve
Starter Module		Engedélyezve	Nincs mérve
Update	GitHub	Engedélyezve	Nincs mérve
Steam Client Bootstrapper	Valve Corporation	Engedélyezve	Nincs mérve
ESET command line interface	ESET	Engedélyezve	Nincs mérve
SteelSeries Engine 3 Core	SteelSeries ApS	Engedélyezve	Nincs mérve
ExpressVPN.NotificationServ...	ExpressVPN	Letiltva	Nincs mérve
Xbox App Services	Microsoft Corporation	Letiltva	Nincs
iCloud megosztott albumok	Apple Inc.	Letiltva	Nincs
iCloud Internet Explorer-kön...	Apple Inc.	Letiltva	Nincs
iCloud-fotók	Apple Inc.	Letiltva	Nincs
Spotify	Spotify AB	Letiltva	Nincs
Skype	Skype	Letiltva	Nincs
iTunes segítő	Apple Inc.	Letiltva	Nincs
iTunes mobileszköz-segítő	Apple Inc.	Letiltva	Nincs
Microsoft Teams	Microsoft Corporation	Letiltva	Nincs
Origin	Electronic Arts	Letiltva	Nincs

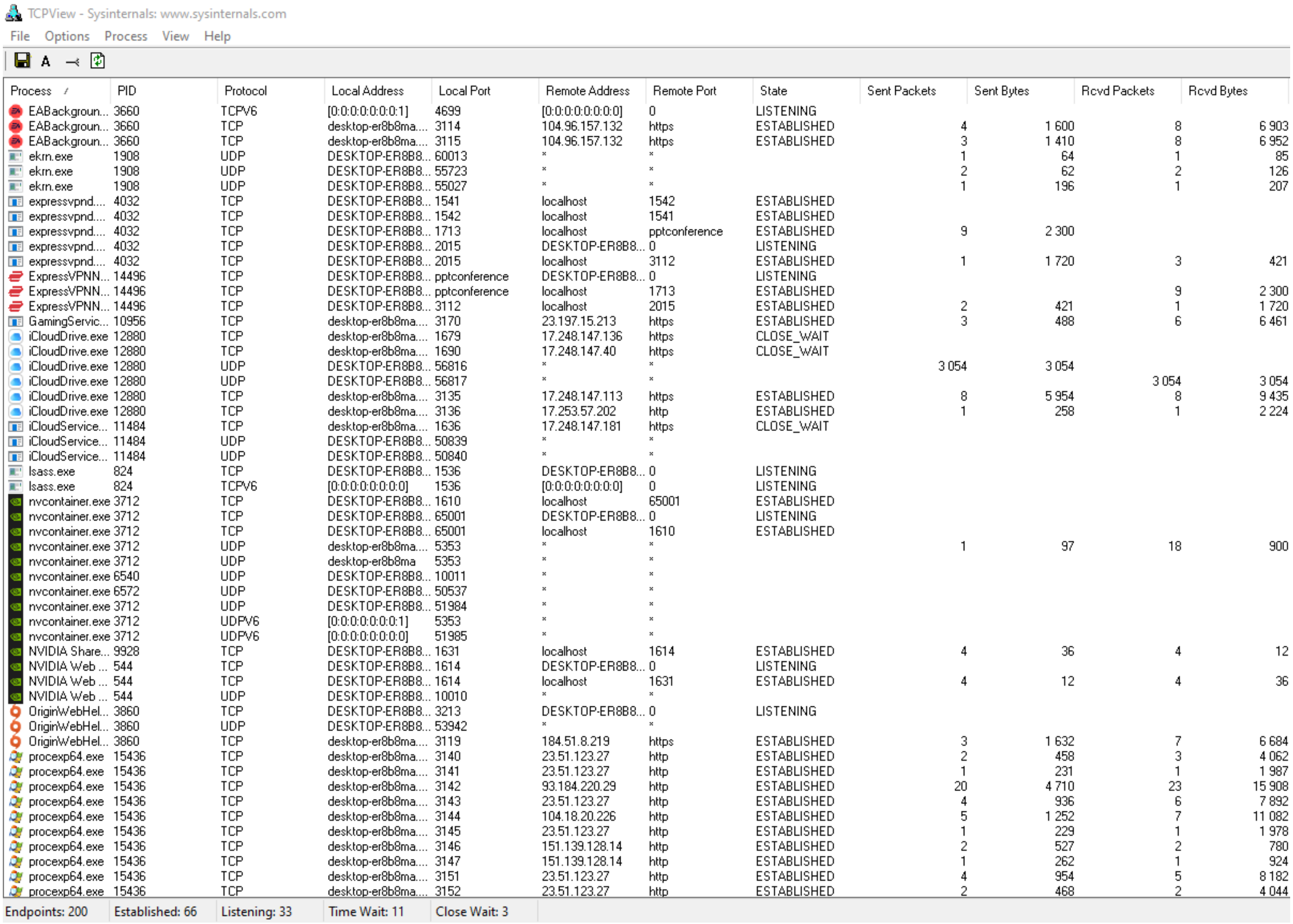


Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
☑ \update-S-1-5-21-32573...	TODO: <File description>	(Verified) OOO Lightshot	c:\program files (x86)\skillbrains\upd...	2017. 04. 12. 5:38	
HKLM\System\CurrentControlSet\Services				2021. 02. 17. 11:34	
☑ BEService	BattlEye Service:	(Verified) BattlEye Innovations e.K.	c:\program files (x86)\common files\b...	2021. 01. 07. 20:45	
☑ ClickToRunSvc	Microsoft Office Kattintásra szolgáltat...	(Verified) Microsoft Corporation	c:\program files\common files\micros...	2021. 02. 03. 21:43	
☑ EABackgroundService	EABackgroundService: EA Desktop ...	(Verified) Electronic Arts, Inc.	c:\program files\electronic arts\ea de...	2021. 02. 11. 18:46	
☑ EasyAntiCheat	EasyAntiCheat: Provides integrated s...	(Verified) EasyAntiCheat Oy	c:\program files (x86)\easyanticheat\...	2018. 05. 01. 7:54	
☑ edgeupdate	Microsoft Edge-frissítés szolgáltatás (...	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge...	2020. 07. 01. 4:12	
☑ edgeupdatem	Microsoft Edge-frissítés szolgáltatás (...	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge...	2020. 07. 01. 4:12	
☑ ekrn	ESET Service: ESET Service	(Verified) ESET, spol. s r.o.	c:\program files\eset\eset security\e...	2020. 10. 26. 9:31	
☑ ekrnEpfw	ESET Firewall Helper: ESET Service	(Verified) ESET, spol. s r.o.	c:\program files\eset\eset security\e...	2020. 10. 26. 9:31	
☑ ExpressVPNService	ExpressVPN Service: This service en...	(Verified) Express Vpn LLC	c:\program files (x86)\expressvpn\bo...	2019. 04. 25. 4:34	
☑ FontCache3.0.0.0	Windows megjelenítési alaprendszer ...	(Verified) Microsoft Corporation	c:\windows\microsoft.net\framework...	2019. 10. 25. 5:32	
☑ FvSvc	NVIDIA FrameView SDK service: NVI...	(Verified) NVIDIA Corporation	c:\program files\nvidia corporation\fr...	2021. 01. 25. 4:35	
☑ GamingServices	Gaming Services: ms-resource:Gamin...	(Verified) Microsoft Corporation	c:\program files\windowsapps\micros...	1987. 06. 14. 9:22	
☑ GamingServicesNet	Gaming Services: ms-resource:Gamin...	(Verified) Microsoft Corporation	c:\program files\windowsapps\micros...	1987. 06. 14. 9:22	
☑ GoogleChromeElevation...	Google Chrome Elevation Service (G...	(Verified) Google LLC	c:\program files\google\chrome\appli...	2021. 02. 04. 1:31	
☑ gupdate	Google frissítés Szolgáltatás (gupdat...	(Verified) Google LLC	c:\program files (x86)\google\update...	2020. 11. 19. 0:00	
☑ gupdatem	Google frissítés Szolgáltatás (gupdat...	(Verified) Google LLC	c:\program files (x86)\google\update...	2020. 11. 19. 0:00	
☑ MicrosoftEdgeElevation...	Microsoft Edge Elevation Service (Mi...	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge...	2021. 02. 10. 21:20	
☑ NvContainerLocalSystem	NVIDIA LocalSystem Container: Cont...	(Verified) NVIDIA Corporation	c:\program files\nvidia corporation\n...	2020. 05. 06. 18:17	
☑ NVDisplay.ContainerLoc...	NVIDIA Display Container LS: Contai...	(Verified) NVIDIA Corporation	c:\program files\nvidia corporation\di...	2020. 06. 09. 15:44	
☑ Origin Client Service	Origin Client Service: OriginClientServ...	(Verified) Electronic Arts, Inc.	c:\program files (x86)\origin\originclie...	2021. 01. 21. 15:20	
☑ Origin Web Helper Service	Origin Web Helper Service: OriginWe...	(Verified) Electronic Arts, Inc.	c:\program files (x86)\origin\originwe...	2021. 01. 21. 15:20	
☑ Rockstar Service	Rockstar Game Library Service: This ...	(Verified) Rockstar Games, Inc.	c:\program files\rockstar games\laun...	2020. 12. 02. 16:40	
☑ Steam Client Service	Steam Client Service: Steam Client S...	(Verified) Valve	c:\program files (x86)\common files\s...	2021. 02. 13. 0:22	
☑ SteelSeriesUpdateService	SteelSeries Update Service: Handles...	(Verified) SteelSeries ApS	c:\program files\steelseries\steelserie...	2021. 01. 20. 20:05	
☑ ucldr_battlegrounds_gl	Uncheater for BattleGrounds_GL: W...	(Verified) Wellbia.com Co., Ltd.	c:\program files\common files\unche...	2020. 11. 03. 4:15	
☑ VBoxSDS	VirtualBox system service: Used as a ...	(Verified) Oracle Corporation	c:\program files\oracle\virtualbox\vb...	2021. 01. 07. 16:34	
☑ Wallpaper Engine Service	Wallpaper Engine Service:	(Verified) Skutta, Kristjan	c:\program files (x86)\steam\steamap...	2020. 12. 20. 1:59	
☑ zksvc	Zakynthos Service: zksvc.exe	(Verified) PUBG CORPORATION	c:\program files\common files\pubg\...	2021. 01. 14. 8:47	
HKLM\System\CurrentControlSet\Services				2021. 02. 17. 11:34	
☑ amdgpio2	AMD GPIO Client Driver: AMD GPIO ...	(Verified) Advanced Micro Devices I...	c:\windows\system32\drivers\amdgp...	2020. 03. 11. 12:15	

Ready.

Signed Windows Entries Hidden.

A TCP View segédprogram ablaka (szintén részlet), ahol láthatóak a TCP/UDP kapcsolatok a számítógép illetve külső szerverek között, illetve a helyi localhost kapcsolatok is:

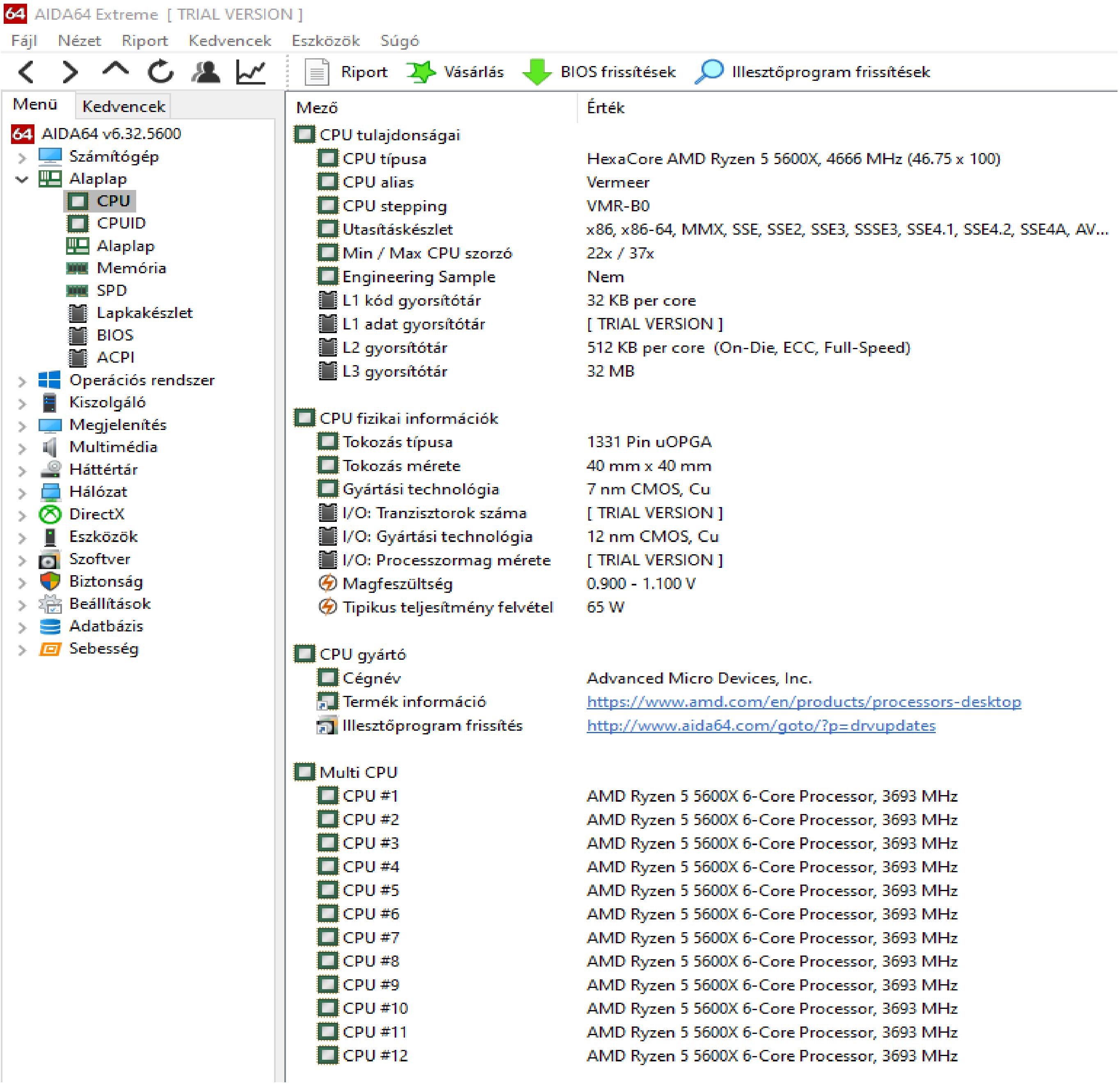


Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
EABackgroun...	3660	TCPV6	[0:0:0:0:0:0:0:1]	4699	[0:0:0:0:0:0:0:0]	0	LISTENING				
EABackgroun...	3660	TCP	desktop-er8b8ma....	3114	104.96.157.132	https	ESTABLISHED	4	1 600	8	6 903
EABackgroun...	3660	TCP	desktop-er8b8ma....	3115	104.96.157.132	https	ESTABLISHED	3	1 410	8	6 952
ekrn.exe	1908	UDP	DESKTOP-ER8B8...	60013	*	*		1	64	1	85
ekrn.exe	1908	UDP	DESKTOP-ER8B8...	55723	*	*		2	62	2	126
ekrn.exe	1908	UDP	DESKTOP-ER8B8...	55027	*	*		1	196	1	207
expressvpnd....	4032	TCP	DESKTOP-ER8B8...	1541	localhost	1542	ESTABLISHED				
expressvpnd....	4032	TCP	DESKTOP-ER8B8...	1542	localhost	1541	ESTABLISHED				
expressvpnd....	4032	TCP	DESKTOP-ER8B8...	1713	localhost	pptconference	ESTABLISHED	9	2 300		
expressvpnd....	4032	TCP	DESKTOP-ER8B8...	2015	DESKTOP-ER8B8...	0	LISTENING				
expressvpnd....	4032	TCP	DESKTOP-ER8B8...	2015	localhost	3112	ESTABLISHED	1	1 720	3	421
ExpressVPNN...	14496	TCP	DESKTOP-ER8B8...	pptconference	DESKTOP-ER8B8...	0	LISTENING				
ExpressVPNN...	14496	TCP	DESKTOP-ER8B8...	pptconference	localhost	1713	ESTABLISHED			9	2 300
ExpressVPNN...	14496	TCP	DESKTOP-ER8B8...	3112	localhost	2015	ESTABLISHED	2	421	1	1 720
GamingServic...	10956	TCP	desktop-er8b8ma....	3170	23.197.15.213	https	ESTABLISHED	3	488	6	6 461
iCloudDrive.exe	12880	TCP	desktop-er8b8ma....	1679	17.248.147.136	https	CLOSE_WAIT				
iCloudDrive.exe	12880	TCP	desktop-er8b8ma....	1690	17.248.147.40	https	CLOSE_WAIT				
iCloudDrive.exe	12880	UDP	DESKTOP-ER8B8...	56816	*	*		3 054	3 054		
iCloudDrive.exe	12880	UDP	DESKTOP-ER8B8...	56817	*	*				3 054	3 054
iCloudDrive.exe	12880	TCP	desktop-er8b8ma....	3135	17.248.147.113	https	ESTABLISHED	8	5 954	8	9 435
iCloudDrive.exe	12880	TCP	desktop-er8b8ma....	3136	17.253.57.202	http	ESTABLISHED	1	258	1	2 224
iCloudService...	11484	TCP	desktop-er8b8ma....	1636	17.248.147.181	https	CLOSE_WAIT				
iCloudService...	11484	UDP	DESKTOP-ER8B8...	50839	*	*					
iCloudService...	11484	UDP	DESKTOP-ER8B8...	50840	*	*					
lsass.exe	824	TCP	DESKTOP-ER8B8...	1536	DESKTOP-ER8B8...	0	LISTENING				
lsass.exe	824	TCPV6	[0:0:0:0:0:0:0:0]	1536	[0:0:0:0:0:0:0:0]	0	LISTENING				
nvcontainer.exe	3712	TCP	DESKTOP-ER8B8...	1610	localhost	65001	ESTABLISHED				
nvcontainer.exe	3712	TCP	DESKTOP-ER8B8...	65001	DESKTOP-ER8B8...	0	LISTENING				
nvcontainer.exe	3712	TCP	DESKTOP-ER8B8...	65001	localhost	1610	ESTABLISHED				
nvcontainer.exe	3712	UDP	desktop-er8b8ma....	5353	*	*		1	97	18	900
nvcontainer.exe	3712	UDP	desktop-er8b8ma	5353	*	*					
nvcontainer.exe	6540	UDP	DESKTOP-ER8B8...	10011	*	*					
nvcontainer.exe	6572	UDP	DESKTOP-ER8B8...	50537	*	*					
nvcontainer.exe	3712	UDP	DESKTOP-ER8B8...	51984	*	*					
nvcontainer.exe	3712	UDPV6	[0:0:0:0:0:0:0:1]	5353	*	*					
nvcontainer.exe	3712	UDPV6	[0:0:0:0:0:0:0:0]	51985	*	*					
NVIDIA Share...	9928	TCP	DESKTOP-ER8B8...	1631	localhost	1614	ESTABLISHED	4	36	4	12
NVIDIA Web ...	544	TCP	DESKTOP-ER8B8...	1614	DESKTOP-ER8B8...	0	LISTENING				
NVIDIA Web ...	544	TCP	DESKTOP-ER8B8...	1614	localhost	1631	ESTABLISHED	4	12	4	36
NVIDIA Web ...	544	UDP	DESKTOP-ER8B8...	10010	*	*					
OriginWebHel...	3860	TCP	DESKTOP-ER8B8...	3213	DESKTOP-ER8B8...	0	LISTENING				
OriginWebHel...	3860	UDP	DESKTOP-ER8B8...	53942	*	*					
OriginWebHel...	3860	TCP	desktop-er8b8ma....	3119	184.51.8.219	https	ESTABLISHED	3	1 632	7	6 684
procexp64.exe	15436	TCP	desktop-er8b8ma....	3140	23.51.123.27	http	ESTABLISHED	2	458	3	4 062
procexp64.exe	15436	TCP	desktop-er8b8ma....	3141	23.51.123.27	http	ESTABLISHED	1	231	1	1 987
procexp64.exe	15436	TCP	desktop-er8b8ma....	3142	93.184.220.29	http	ESTABLISHED	20	4 710	23	15 908
procexp64.exe	15436	TCP	desktop-er8b8ma....	3143	23.51.123.27	http	ESTABLISHED	4	936	6	7 892
procexp64.exe	15436	TCP	desktop-er8b8ma....	3144	104.18.20.226	http	ESTABLISHED	5	1 252	7	11 082
procexp64.exe	15436	TCP	desktop-er8b8ma....	3145	23.51.123.27	http	ESTABLISHED	1	229	1	1 978
procexp64.exe	15436	TCP	desktop-er8b8ma....	3146	151.139.128.14	http	ESTABLISHED	2	527	2	780
procexp64.exe	15436	TCP	desktop-er8b8ma....	3147	151.139.128.14	http	ESTABLISHED	1	262	1	924
procexp64.exe	15436	TCP	desktop-er8b8ma....	3151	23.51.123.27	http	ESTABLISHED	4	954	5	8 182
procexp64.exe	15436	TCP	desktop-er8b8ma....	3152	23.51.123.27	http	ESTABLISHED	2	468	2	4 044

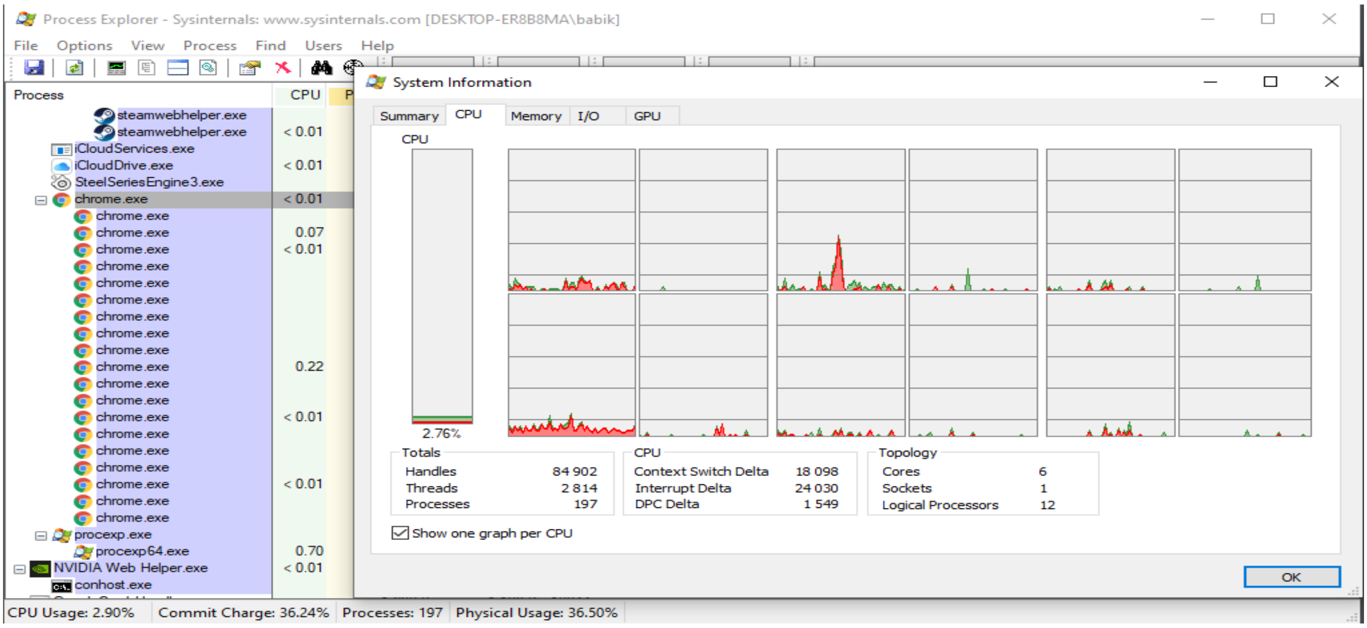
Endpoints: 200 | Established: 66 | Listening: 33 | Time Wait: 11 | Close Wait: 3

Az alábbi képeken a Process Explorer segédprogram CPU használati statisztikái láthatóak, továbbá a Coreinfo segédprogramon keresztül *-al jelölve láthatóak a CPU által támogatott instrukciókészletek (instruction set). Érdekességképpen az AIDA64 program CPU tulajdonság ablakát is mellékeltem. A számítógépem 2021 elején lett összeállítva, és a legújabb generációs, 7 nm-es gyártási technológiával készült AMD Ryzen 5600X található benne. A processzor 6 magos, és 12 szálon fut, gyári maximális órajele pedig 4,6 Ghz, amelyet a maximális teljesítmény elérése érdekében 4,8 Ghz-re túlhajtottam. A virtualizálási képességek be vannak kapcsolva, így a VirtualBoxon lévő Linux is jóval jobban fut.

Szerencsére az órán említett programok nagy részét eddig is ismertem, és némelyik ilyen segédprogram (AIDA64, CPU-Z, GPU-Z, Autoruns, stb.) gyakorlott is vagyok és kéznél voltak a gyakorlatra.



Mező	Érték
CPU tulajdonságai	
CPU típusa	HexaCore AMD Ryzen 5 5600X, 4666 MHz (46.75 x 100)
CPU alias	Vermeer
CPU stepping	VMR-B0
Utasításkészlet	x86, x86-64, MMX, SSE, SSE2, SSE3, SSSE3, SSE4.1, SSE4.2, SSE4A, AV...
Min / Max CPU szorzó	22x / 37x
Engineering Sample	Nem
L1 kód gyorsítótár	32 KB per core
L1 adat gyorsítótár	[TRIAL VERSION]
L2 gyorsítótár	512 KB per core (On-Die, ECC, Full-Speed)
L3 gyorsítótár	32 MB
CPU fizikai információk	
Tokozás típusa	1331 Pin uOPGA
Tokozás mérete	40 mm x 40 mm
Gyártási technológia	7 nm CMOS, Cu
I/O: Tranzisztorok száma	[TRIAL VERSION]
I/O: Gyártási technológia	12 nm CMOS, Cu
I/O: Processzormag mérete	[TRIAL VERSION]
Magfeszültség	0.900 - 1.100 V
Tipikus teljesítmény felvétel	65 W
CPU gyártó	
Cégnév	Advanced Micro Devices, Inc.
Termék információ	https://www.amd.com/en/products/processors-desktop
Illesztőprogram frissítés	http://www.aida64.com/goto/?p=drvupdates
Multi CPU	
CPU #1	AMD Ryzen 5 5600X 6-Core Processor, 3693 MHz
CPU #2	AMD Ryzen 5 5600X 6-Core Processor, 3693 MHz
CPU #3	AMD Ryzen 5 5600X 6-Core Processor, 3693 MHz
CPU #4	AMD Ryzen 5 5600X 6-Core Processor, 3693 MHz
CPU #5	AMD Ryzen 5 5600X 6-Core Processor, 3693 MHz
CPU #6	AMD Ryzen 5 5600X 6-Core Processor, 3693 MHz
CPU #7	AMD Ryzen 5 5600X 6-Core Processor, 3693 MHz
CPU #8	AMD Ryzen 5 5600X 6-Core Processor, 3693 MHz
CPU #9	AMD Ryzen 5 5600X 6-Core Processor, 3693 MHz
CPU #10	AMD Ryzen 5 5600X 6-Core Processor, 3693 MHz
CPU #11	AMD Ryzen 5 5600X 6-Core Processor, 3693 MHz
CPU #12	AMD Ryzen 5 5600X 6-Core Processor, 3693 MHz

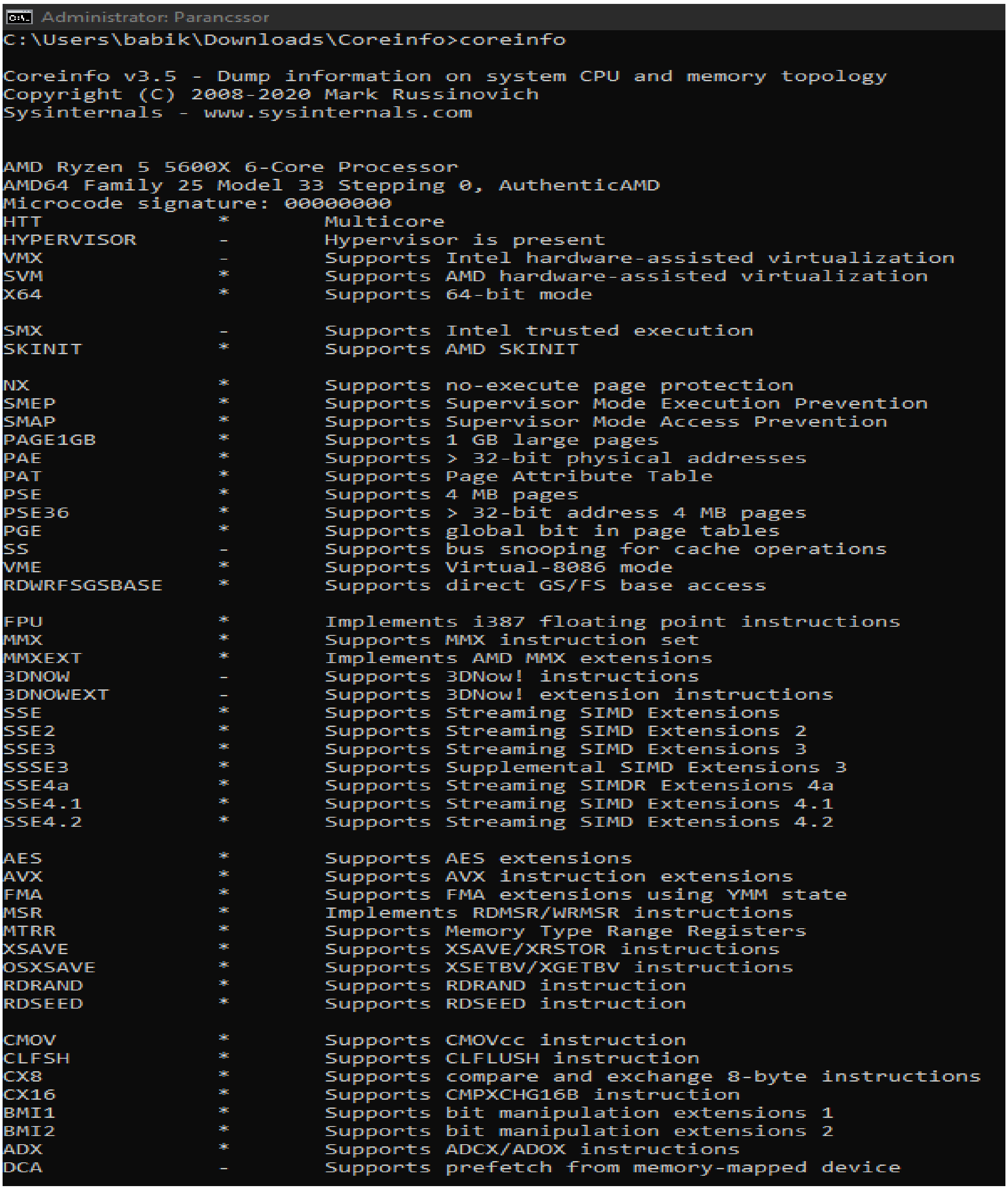


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-ER8B8MA\babik]
File Options View Process Find Users Help
System Information
Summary CPU Memory I/O GPU
CPU
2.76%
☑ Show one graph per CPU
OK

Process	CPU
steamwebhelper.exe	
steamwebhelper.exe	< 0.01
iCloudServices.exe	
iCloudDrive.exe	< 0.01
SteelSeriesEngine3.exe	
chrome.exe	< 0.01
chrome.exe	
chrome.exe	0.07
chrome.exe	< 0.01
chrome.exe	
chrome.exe	
chrome.exe	
chrome.exe	
chrome.exe	
chrome.exe	
chrome.exe	0.22
chrome.exe	
chrome.exe	
chrome.exe	< 0.01
chrome.exe	
chrome.exe	
chrome.exe	
chrome.exe	< 0.01
chrome.exe	
chrome.exe	
procexp.exe	
procexp64.exe	0.70
NVIDIA Web Helper.exe	< 0.01
conhost.exe	

Totals		CPU		Topology	
Handles	84 902	Context Switch Delta	18 098	Cores	6
Threads	2 814	Interrupt Delta	24 030	Sockets	1
Processes	197	DPC Delta	1 549	Logical Processors	12

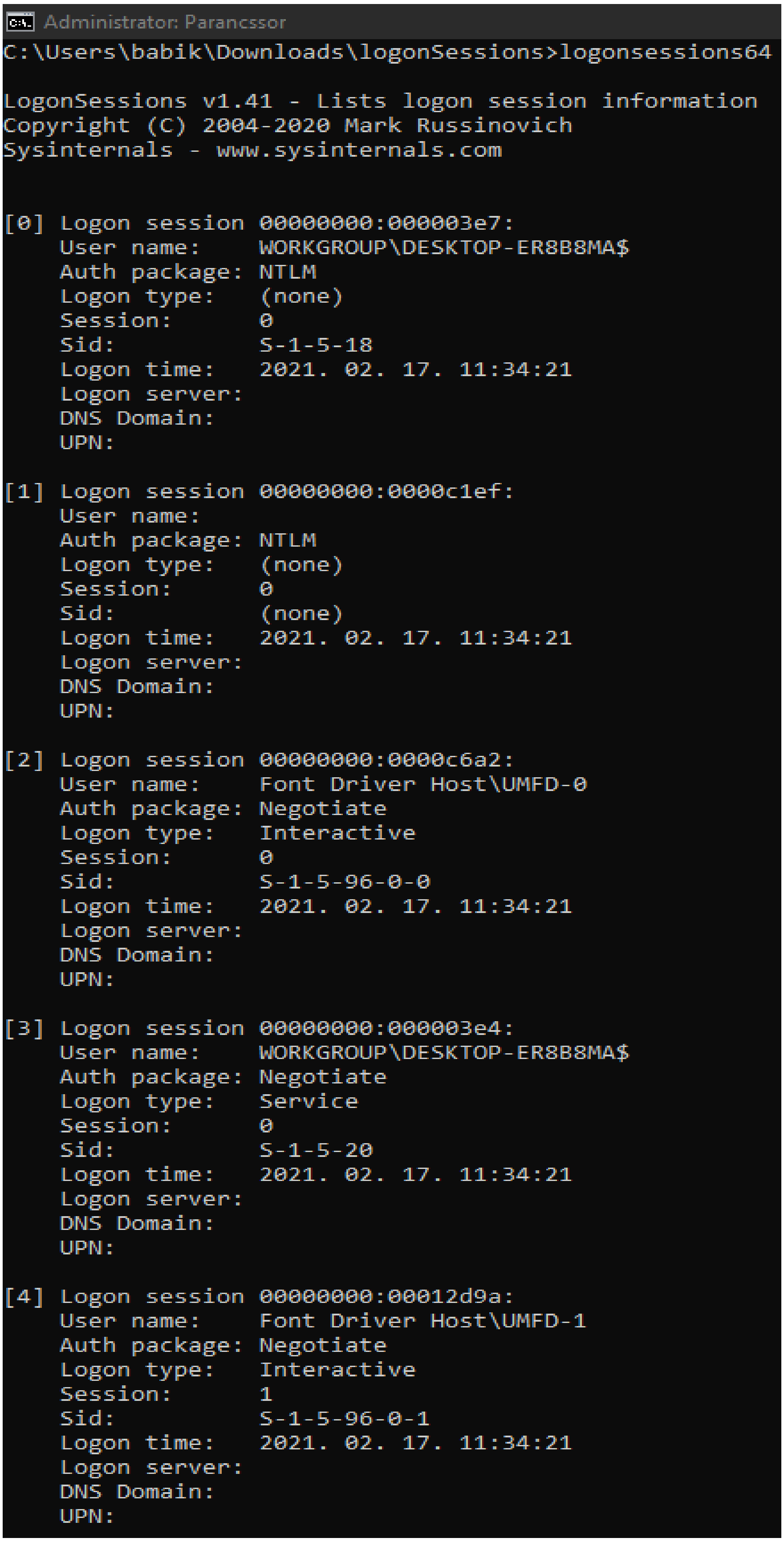
CPU Usage: 2.90% Commit Charge: 36.24% Processes: 197 Physical Usage: 36.50%



Administrator: Parancssor

```
C:\Users\babik\Downloads\Coreinfo>coreinfo

Coreinfo v3.5 - Dump information on system CPU and memory topology
Copyright (C) 2008-2020 Mark Russinovich
Sysinternals - www.sysinternals.com


AMD Ryzen 5 5600X 6-Core Processor
AMD64 Family 25 Model 33 Stepping 0, AuthenticAMD
Microcode signature: 00000000
HTT             *       Multicore
HYPERVISOR      -       Hypervisor is present
VMX             -       Supports Intel hardware-assisted virtualization
SVM             *       Supports AMD hardware-assisted virtualization
X64             *       Supports 64-bit mode

SMX             -       Supports Intel trusted execution
SKINIT          *       Supports AMD SKINIT

NX              *       Supports no-execute page protection
SMEP            *       Supports Supervisor Mode Execution Prevention
SMAP            *       Supports Supervisor Mode Access Prevention
PAGE1GB         *       Supports 1 GB large pages
PAE             *       Supports > 32-bit physical addresses
PAT             *       Supports Page Attribute Table
PSE             *       Supports 4 MB pages
PSE36           *       Supports > 32-bit address 4 MB pages
PGE             *       Supports global bit in page tables
SS              -       Supports bus snooping for cache operations
VME             *       Supports Virtual-8086 mode
RDWRFSGSBASE    *       Supports direct GS/FS base access

FPU             *       Implements i387 floating point instructions
MMX             *       Supports MMX instruction set
MMXEXT          *       Implements AMD MMX extensions
3DNOW           -       Supports 3DNow! instructions
3DNOWEXT        -       Supports 3DNow! extension instructions
SSE             *       Supports Streaming SIMD Extensions
SSE2            *       Supports Streaming SIMD Extensions 2
SSE3            *       Supports Streaming SIMD Extensions 3
SSSE3           *       Supports Supplemental SIMD Extensions 3
SSE4a           *       Supports Streaming SIMDR Extensions 4a
SSE4.1          *       Supports Streaming SIMD Extensions 4.1
SSE4.2          *       Supports Streaming SIMD Extensions 4.2

AES             *       Supports AES extensions
AVX             *       Supports AVX instruction extensions
FMA             *       Supports FMA extensions using YMM state
MSR             *       Implements RDMSR/WRMSR instructions
MTRR            *       Supports Memory Type Range Registers
XSAVE           *       Supports XSAVE/XRSTOR instructions
OSXSAVE         *       Supports XSETBV/XGETBV instructions
RDRAND          *       Supports RDRAND instruction
RDSEED          *       Supports RDSEED instruction

CMOV            *       Supports CMOVcc instruction
CLFSH           *       Supports CLFLUSH instruction
CX8             *       Supports compare and exchange 8-byte instructions
CX16            *       Supports CMPXCHG16B instruction
BMI1            *       Supports bit manipulation extensions 1
BMI2            *       Supports bit manipulation extensions 2
ADX             *       Supports ADCX/ADOX instructions
DCA             -       Supports prefetch from memory-mapped device
```

Utolsóként a LogonSessions segédprogram segítségével láthatóak a számítógépen bejelentkezett és még ki nem jelentkezett, futó folyamatok. A -p kapcsolóval láthatóak, hogy egyes folyamatok alatt mely processzek futnak a számítógépen:



```
C:\Users\babik\Downloads\logonSessions>logonsessions64

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


[0] Logon session 00000000:000003e7:
    User name:    WORKGROUP\DESKTOP-ER8B8MA$
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          S-1-5-18
    Logon time:   2021. 02. 17. 11:34:21
    Logon server:
    DNS Domain:
    UPN:

[1] Logon session 00000000:0000c1ef:
    User name:
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          (none)
    Logon time:   2021. 02. 17. 11:34:21
    Logon server:
    DNS Domain:
    UPN:

[2] Logon session 00000000:0000c6a2:
    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. 02. 17. 11:34:21
    Logon server:
    DNS Domain:
    UPN:

[3] Logon session 00000000:000003e4:
    User name:    WORKGROUP\DESKTOP-ER8B8MA$
    Auth package: Negotiate
    Logon type:   Service
    Session:      0
    Sid:          S-1-5-20
    Logon time:   2021. 02. 17. 11:34:21
    Logon server:
    DNS Domain:
    UPN:

[4] Logon session 00000000:00012d9a:
    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. 02. 17. 11:34:21
    Logon server:
    DNS Domain:
    UPN:
```