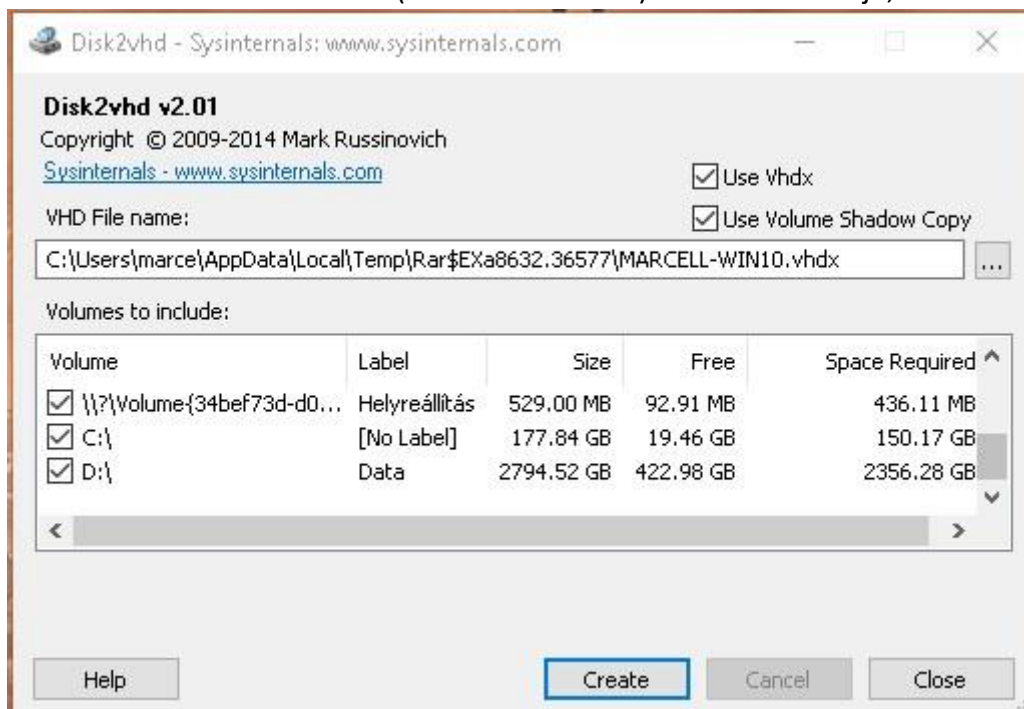


## Disk2vhd

A Disk2vhd program segítségével a számítógépünkben lévő HDD-ről(Hard Disk Drive) készít egy virtuális változatot. Ez a VHD (Virtual Hard Disk). Ez arra lehet jó, ha szeretnénk a

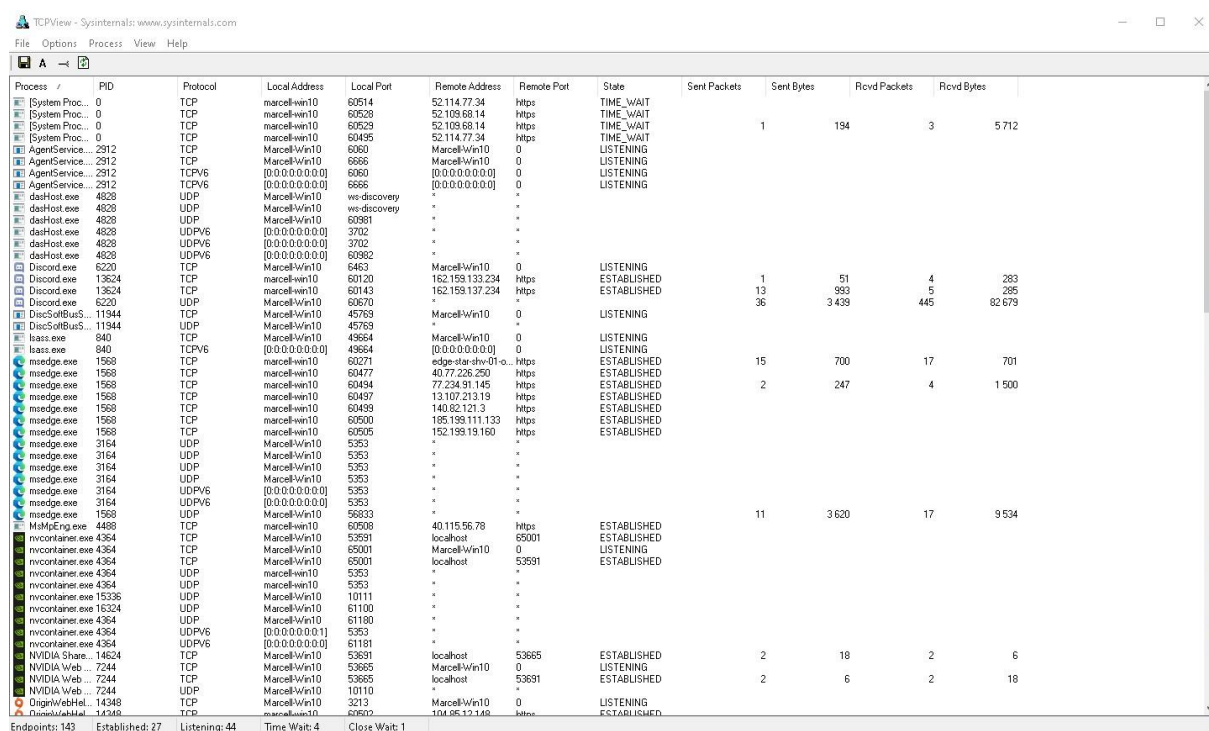


számítógépünkről virtuális klónt készíteni.

A *VHD File Name* alatt megadhatjuk, hova készítsen VHD fájlt. Kiválasztjuk a meghajtónk betűjelét, majd a *Create* gombra kattintva a konvertálás megkezdődik.

## TCPView

A TCPView segítségével megnézhetjük az éppen futó programok és szolgáltatások által felépített összes létező TCP és UDP kapcsolatát, igen részletesen.



De ha nem kell nekünk ennyire részletes információ az éppen élő TCP és UDP kapcsolatokról, akkor a parancssort megnyitva a *netstat* parancs is kilistázza, de az nem fogja odaírni a program nevét.

## Process Explorer

Hasonló a Windows feladatkezelőjéhez. Annyiban különbözik, hogy két részből áll az ablak. A felső részben listázza ki az éppen futó folyamatokat úgy, mint a feladatkezelő. Az alsó

The screenshot shows the Process Explorer window. The top pane displays a list of running processes with columns for CPU usage, Private Bytes, Working Set, PID, Description, and Company Name. The bottom pane shows the loaded DLLs for the selected process, with columns for Name, Description, Company Name, and Path.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
csrss.exe	< 0.01	2 244 K	11 440 K	652		
wininit.exe	< 0.01	1 960 K	14 160 K	748		
services.exe	< 0.01	7 428 K	27 052 K	824		
svchost.exe	< 0.01	27 464 K	59 404 K	972	Windows-szolgáltatások gaz...	Microsoft Corporation
dllhost.exe		3 448 K	3 028 K	10196		
MoUsoCoreWorker.exe		29 736 K	18 396 K	17048		
StartMenuExperience...		79 912 K	67 992 K	11612		
RuntimeBroker.exe		6 176 K	25 064 K	16280	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	234 504 K	103 036 K	12720	Search application	Microsoft Corporation
RuntimeBroker.exe		53 280 K	42 208 K	13252	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	74 560 K	3 024 K	14744	YourPhone	Microsoft Corporation
SettingSyncHost.exe		5 476 K	6 468 K	11176	Host Process for Setting Syn...	Microsoft Corporation
LockApp.exe	Susp...	61 788 K	45 928 K	9760	LockApp.exe	Microsoft Corporation

Name	Description	Company Name	Path
{3DA71D5A-20CC-...			C:\Users\marce\AppData\Local\Microsoft\Windows\Cach...
*FontCache-FontFa...			C:\Windows\ServiceProfiles\LocalService\AppData\Local\...
*FontCache-S-1-5-...			C:\Windows\ServiceProfiles\LocalService\AppData\Local\...
*FontCache-Syste...			C:\Windows\ServiceProfiles\LocalService\AppData\Local\...
3060710702.pri			C:\Windows\rescache\_merged\2583045284\3060710702...
3060710702.pri			C:\Windows\rescache\_merged\2583045284\3060710702...
3896405323.pri			C:\Windows\rescache\_merged\24768367\3896405323.pri
actxprxy.dll	ActiveX Interface Marshaling Library	Microsoft Corporation	C:\Windows\System32\actxprxy.dll
advapi32.dll	Speciális 32 bites Windows API	Microsoft Corporation	C:\Windows\System32\advapi32.dll
AppResolver.dll	Alkalmazásfeloldó	Microsoft Corporation	C:\Windows\System32\AppResolver.dll
BCP47Langs.dll	BCP47 Language Classes	Microsoft Corporation	C:\Windows\System32\BCP47Langs.dll
BCP47mm.dll	BCP47 Language Classes for Res...	Microsoft Corporation	C:\Windows\System32\BCP47mm.dll
bcrypt.dll	Windows kriptográfiai primitívek kö...	Microsoft Corporation	C:\Windows\System32\bcrypt.dll
bcryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll
biwinrt.dll	Windows Background Broker Infra...	Microsoft Corporation	C:\Windows\System32\biwinrt.dll

CPU Usage: 5.38% | Commit Charge: 33.78% | Processes: 233 | Physical Usage: 46.41%

részében van részletes információ adott folyamatról, például hogy milyen DLL fájlokat használ.

A View fület lenyitva a *Low Panel View* menüponton belül lehet kiválasztani mit szeretnénk látni az alsó részben.

## Process Monitor

Hasonlóan a Windows Feladatkezelőjéhez, kilistázza az éppen futó folyamatokat.

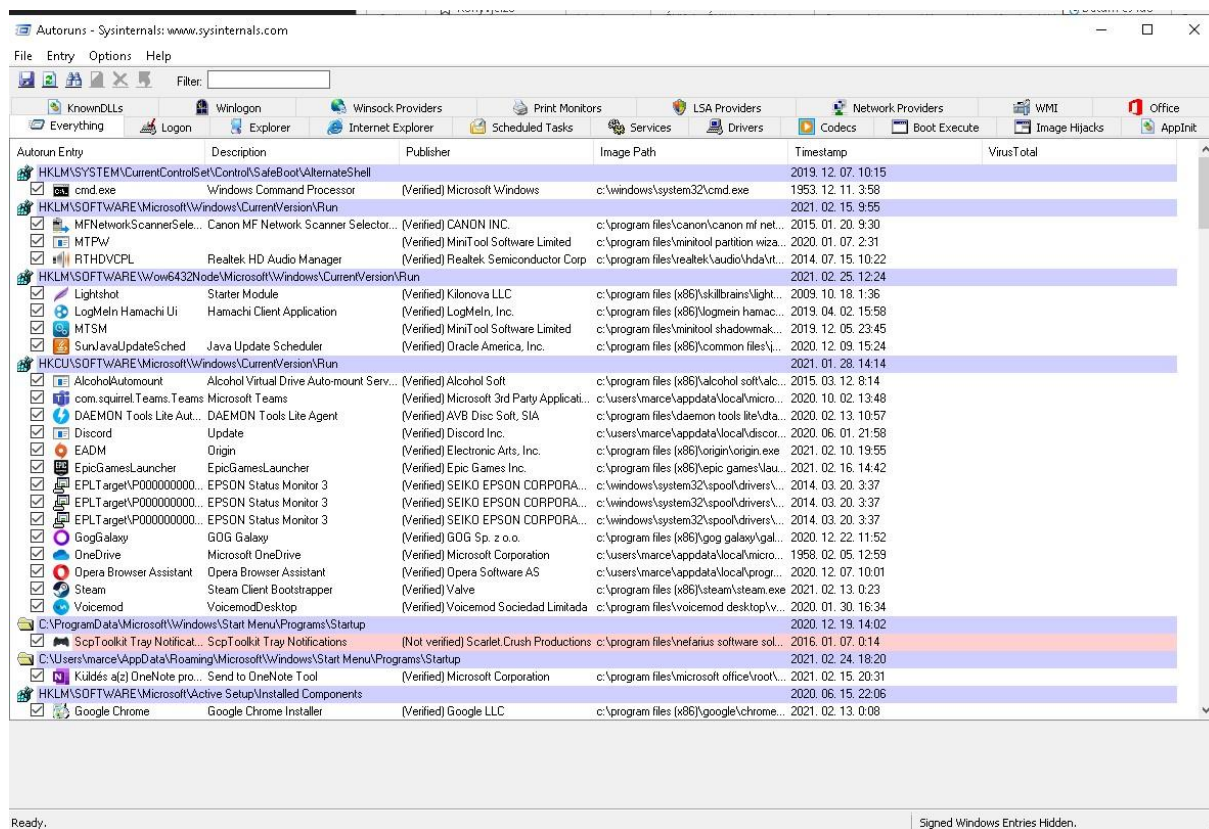
The screenshot shows the Process Monitor window. The top pane displays a list of running processes. The bottom pane shows a list of system events with columns for Time, Process Name, PID, Operation, Path, Result, and Detail.

Time	Process Name	PID	Operation	Path	Result	Detail
13:49...	svchost.exe	2688	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 690 688, Le...
13:49...	MsmPng.exe	4488	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 069 760...
13:49...	MsmPng.exe	4488	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 163 968...
13:49...	svchost.exe	2688	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 678 400, Le...
13:49...	MsmPng.exe	4488	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 434 304...
13:49...	svchost.exe	2688	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 635 904, Le...
13:49...	Explorer.EXE	12800	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
13:49...	Explorer.EXE	12800	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
13:49...	MsmPng.exe	4488	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 147 584...
13:49...	svchost.exe	2688	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 623 616, Le...
13:49...	Explorer.EXE	12800	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
13:49...	Explorer.EXE	12800	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
13:49...	Explorer.EXE	12800	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
13:49...	Explorer.EXE	12800	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
13:49...	Explorer.EXE	12800	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
13:49...	Explorer.EXE	12800	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
13:49...	Explorer.EXE	12800	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
13:49...	MsmPng.exe	4488	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 479 360...
13:49...	svchost.exe	2688	ReadFile	C:\Windows\System32\Windows State...	SUCCESS	Offset: 5 478 400...
13:49...	Explorer.EXE	12800	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
13:49...	svchost.exe	2688	QueryOpen	D:\2020_21_2\OS\System32\Suite\Pr...	SUCCESS	CreationTime: 202...
13:49...	svchost.exe	2688	ReadFile	C:\Windows\System32\Windows State...	SUCCESS	Offset: 5 544 960...
13:49...	MsmPng.exe	4488	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Exclusive: False, O...
13:49...	Explorer.EXE	12800	QueryStandard...	C:\Users\marce\AppData\Local\Micros...	SUCCESS	AllocationSize: 7 4...
13:49...	Explorer.EXE	12800	ReadFile	C:\Users\marce\AppData\Local\Micros...	SUCCESS	Offset: 3 485 696...
13:49...	svchost.exe	2688	ReadFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
13:49...	MsmPng.exe	4488	UnlockFileSingle	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 124, Length...
13:49...	svchost.exe	2688	QueryStandard...	C:\ProgramData\Microsoft\Windows De...	SUCCESS	AllocationSize: 4 1...
13:49...	svchost.exe	2688	ReadFile	C:\Windows\System32\Windows State...	SUCCESS	Offset: 5 470 208...
13:49...	svchost.exe	2688	ReadFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 2 821 632...
13:49...	MsmPng.exe	4488	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Exclusive: False, O...
13:49...	MsmPng.exe	4488	UnlockFileSingle	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 124, Length...
13:49...	svchost.exe	2688	RegOpenKey	HKLM\Software\Policies\Microsoft\VMU...	NAME NOT FOUND	Desired Access: R...
13:49...	svchost.exe	2688	RegOpenKey	HKU\S-1-5-18	REPARSE	Desired Access: M...
13:49...	svchost.exe	2688	RegOpenKey	HKU\DEFAULT	SUCCESS	Desired Access: M...

Showing 474 598 of 1 114 333 events (42%) | Backed by virtual memory

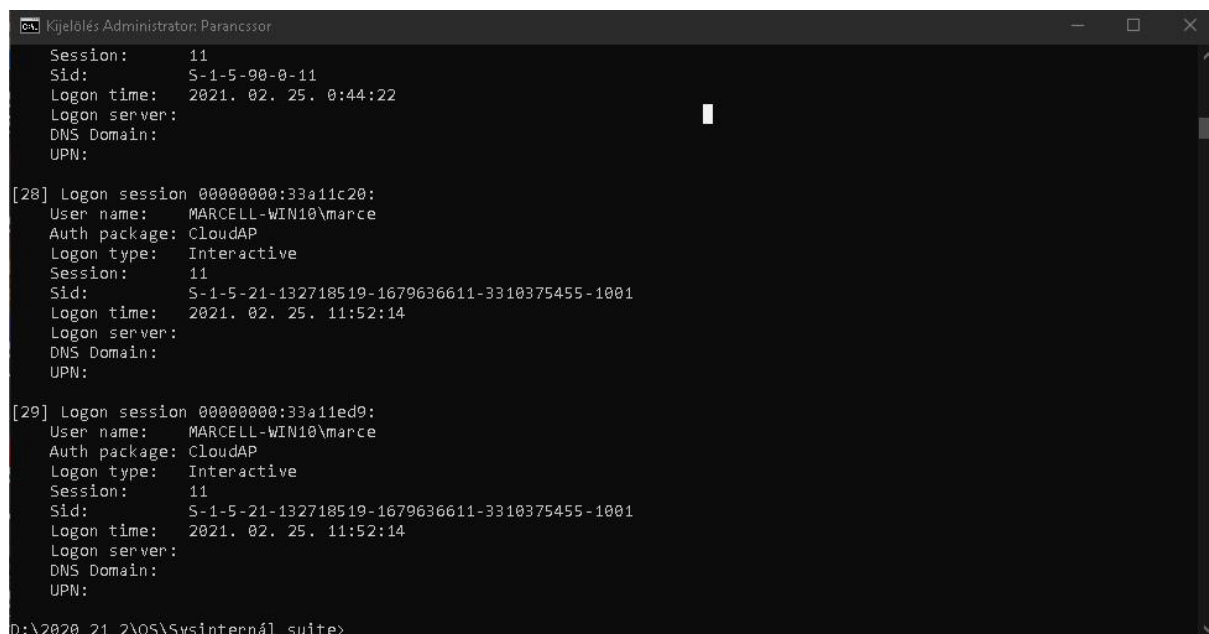
## AutoRuns

Ez a program, azt mutatja meg, hogy mely programok és szolgáltatások indulnak el automatikusan a Windows betöltésekor, illetve amikor belépünk.



## LogonSessions

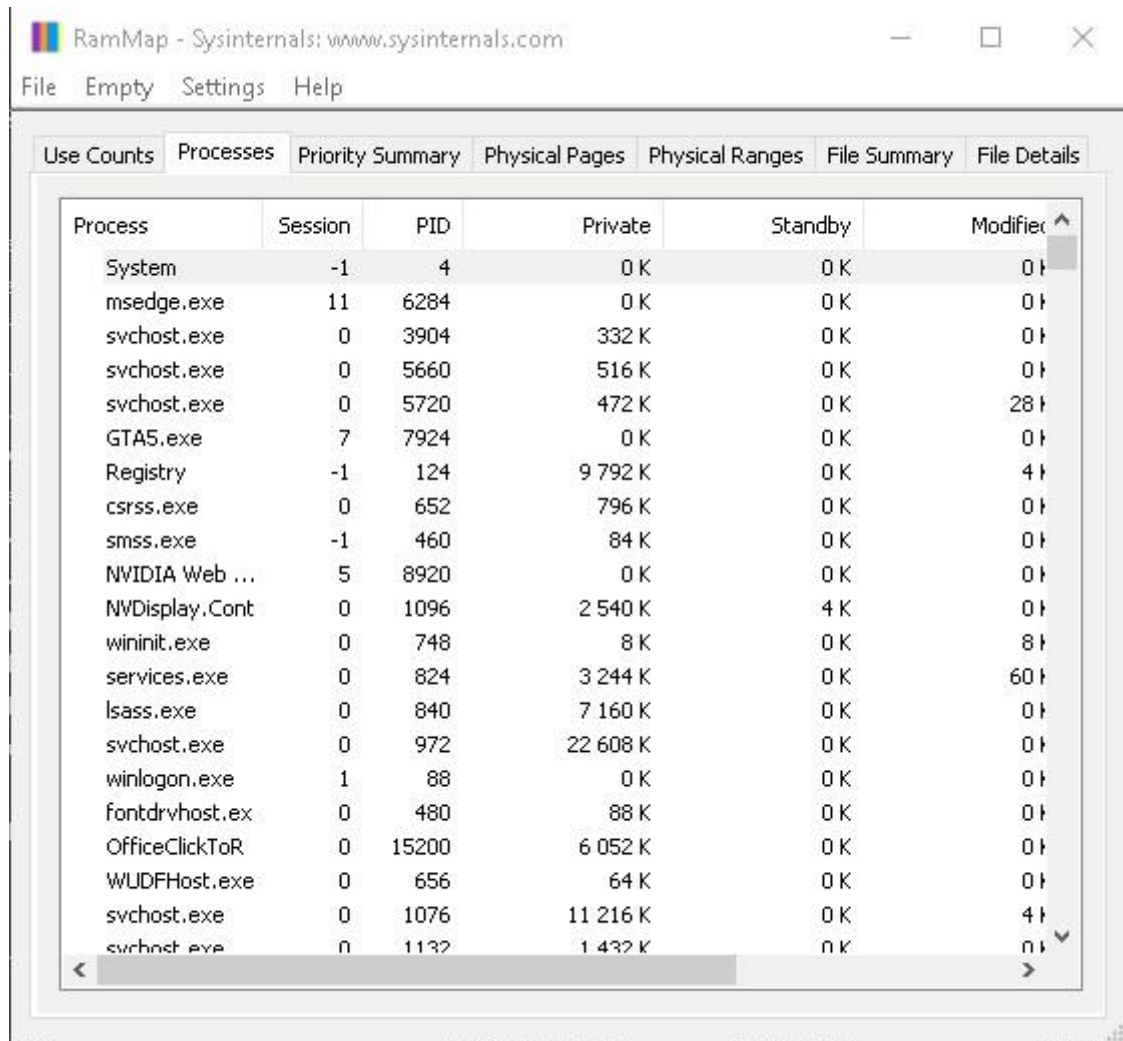
Parancssorra kiírja ki és mikor jelentkezett be a számítógépen.



## RAMMap



Memória használat analizátor. Szépen megmutatja, hogy mennyi memória van használatban éppen és mennyi van készenlétben. Megnézhetjük hogy a processek mennyi memóriát használnak



RamMap - Sysinternals: www.sysinternals.com

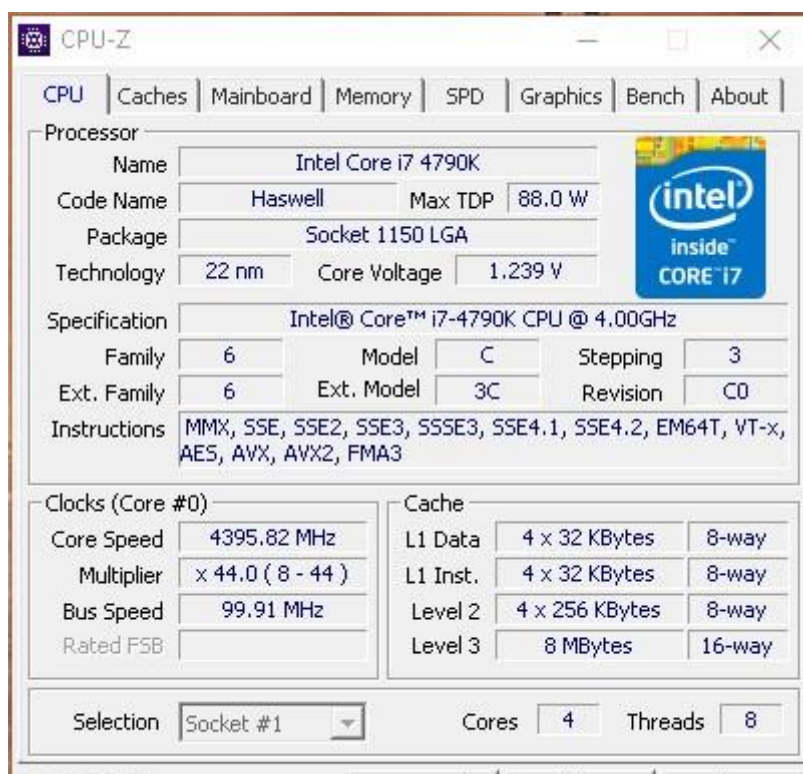
File Empty Settings Help

Use Counts Processes Priority Summary Physical Pages Physical Ranges File Summary File Details

Process	Session	PID	Private	Standby	Modifier
System	-1	4	0 K	0 K	0 K
msedge.exe	11	6284	0 K	0 K	0 K
svchost.exe	0	3904	332 K	0 K	0 K
svchost.exe	0	5660	516 K	0 K	0 K
svchost.exe	0	5720	472 K	0 K	28 K
GTA5.exe	7	7924	0 K	0 K	0 K
Registry	-1	124	9 792 K	0 K	4 K
csrss.exe	0	652	796 K	0 K	0 K
smss.exe	-1	460	84 K	0 K	0 K
NVIDIA Web ...	5	8920	0 K	0 K	0 K
NVDisplay.Cont	0	1096	2 540 K	4 K	0 K
wininit.exe	0	748	8 K	0 K	8 K
services.exe	0	824	3 244 K	0 K	60 K
lsass.exe	0	840	7 160 K	0 K	0 K
svchost.exe	0	972	22 608 K	0 K	0 K
winlogon.exe	1	88	0 K	0 K	0 K
fontdrvhost.ex	0	480	88 K	0 K	0 K
OfficeClickToR	0	15200	6 052 K	0 K	0 K
WUDFHost.exe	0	656	64 K	0 K	0 K
svchost.exe	0	1076	11 216 K	0 K	4 K
svchost.exe	0	1132	1 432 K	0 K	0 K

## CPU-Z

E csodás programmal, részletes információkat kapunk a számítógépünk konfigurációjáról pl.:  
cpu típusa,  
száma,  
magok  
mekkora a



CPU-Z

CPU Caches Mainboard Memory SPD Graphics Bench About

Processor

Name	Intel Core i7 4790K		
Code Name	Haswell	Max TDP	88.0 W
Package	Socket 1150 LGA		
Technology	22 nm	Core Voltage	1.239 V

Specification

Intel® Core™ i7-4790K CPU @ 4.00GHz

Family	6	Model	C	Stepping	3
Ext. Family	6	Ext. Model	3C	Revision	C0

Instructions

MMX, SSE, SSE2, SSE3, SSE4.1, SSE4.2, EM64T, VT-x, AES, AVX, AVX2, FMA3

Clocks (Core #0)

Core Speed	4395.82 MHz
Multiplier	x 44.0 ( 8 - 44 )
Bus Speed	99.91 MHz
Rated FSB	

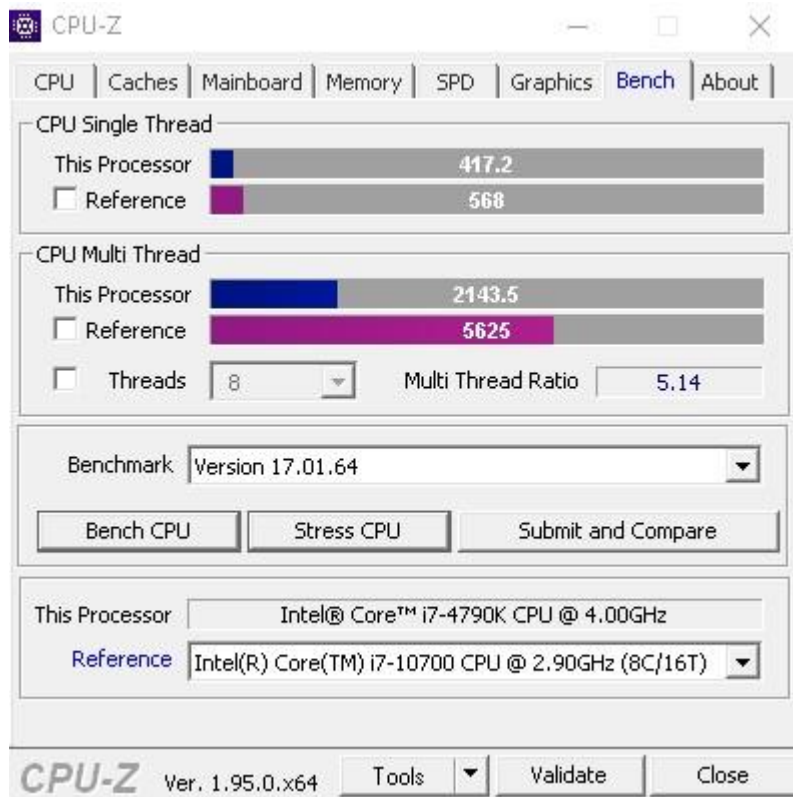
Cache

L1 Data	4 x 32 KBytes	8-way
L1 Inst.	4 x 32 KBytes	8-way
Level 2	4 x 256 KBytes	8-way
Level 3	8 MBytes	16-way

Selection

Socket #1 Cores 4 Threads 8

teljesítménye, mekkora feszültséget vesz fel éppen stb. De az alaplapról, a RAM-ról és a grafikus kártyáról is kapunk egy kisebb leírást. Sőt, a CPU-Z segítségével stress testet is tudunk csinálni. Egy 10. generációs i7-es processzorral hasonlítottam össze az én 4. generációs i7-es processzoromat.



## GPU-Z

Ez a program a videokártyánkról ad részletes információkat, hasonlóan mint CPU-Z-ben a processzorról. Megnézhetjük a kártyának a típusát, grafikus memóriakapacitását és típusát, teljesítményét, hőmérsékletét stb.

