

Virtuális merevlemez hoz létre a kijelölt helyen (segíti a VM-eket)

TCPView - Sysinternals: www.sysinternals.com												
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes	
chrome.exe	17384	TCP	sans	55089	ec2-18-194-178-2...	https	ESTABLISHED			375	18 000	
chrome.exe	17384	TCP	sans	55125	142.250.27.188	5228	ESTABLISHED	2	52	2	52	
chrome.exe	9256	UDP	Sans	5353	*	*				514	31 767	
chrome.exe	9256	UDP	Sans	5353	*	*						
chrome.exe	9256	UDP	Sans	5353	*	*						
chrome.exe	9256	UDP	Sans	5353	*	*						
chrome.exe	9256	UDPV6	sans	5353	*	*						
chrome.exe	9256	UDPV6	sans	5353	*	*						
Discord.exe	11760	TCP	Sans	6463	Sans	0	LISTENING					
Discord.exe	13076	TCP	sans	58507	162.159.133.234	https	ESTABLISHED	53	3 310	509	67 197	
Discord.exe	13076	TCP	sans	58521	162.159.128.235	https	ESTABLISHED	384	29 499	141	8 037	
Discord.exe	13076	TCP	sans	62263	162.159.135.232	https	ESTABLISHED	5	1 021	4	1 726	
Discord.exe	13076	TCP	sans	62265	162.159.135.232	https	ESTABLISHED	5	1 090	5	1 589	
Discord.exe	11760	UDP	Sans	63904	*	*		11	494	309	40 399	
EpicGamesLa...	4300	TCP	sans	55028	ec2-54-162-217-2...	https	ESTABLISHED	34	8 942	68	9 520	
EpicGamesLa...	4300	TCP	sans	62311	ec2-3-231-45-219...	https	CLOSE_WAIT	4	2 075	6	5 573	
GamingServic...	7128	TCP	sans	62331	a88-221-62-148.d...	https	ESTABLISHED	3	488	5	6 461	
ihl_service.exe	3992	TCPV6	[0.0.0.0:0.0.0.1]	49669	sans	0	LISTENING					
lghub.exe	7848	TCP	Sans	54724	localhost	9010	ESTABLISHED					
lghub.exe	10944	TCP	Sans	54726	localhost	9010	ESTABLISHED					
lghub_agent...	1196	TCP	Sans	9010	localhost	54726	ESTABLISHED					
lghub_agent...	1196	TCP	Sans	9010	Sans	0	LISTENING					
lghub_agent...	1196	TCP	Sans	9010	localhost	54724	ESTABLISHED					
lghub_agent...	1196	TCP	Sans	9080	Sans	0	LISTENING					
lghub_agent...	1196	TCP	Sans	45654	Sans	0	LISTENING					
lghub_agent...	1196	TCP	Sans	54728	localhost	9100	ESTABLISHED					
Endpoints: 155 Established: 32 Listening: 39 Time Wait: 0 Close Wait: 12												

A TCPview a TCP és UDP végpontjának részletes felsorolása, beleértve a helyi és távoli címeket és a TCP kapcsolatok állapotát.

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
14:23:...	MsMpEng.exe	4008	CreateFile	C:\Windows\System32\drivers\PROCM...	SUCCESS	Desired Access: R...
14:23:...	MsMpEng.exe	4008	QueryBasicInfor...	C:\Windows\System32\drivers\PROCM...	SUCCESS	CreationTime: 202...
14:23:...	MsMpEng.exe	4008	CloseFile	C:\Windows\System32\drivers\PROCM...	SUCCESS	
14:23:...	MsMpEng.exe	4008	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 2 736 128, ...
14:23:...	svchost.exe	3096	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 690 688, Le...
14:23:...	MsMpEng.exe	4008	FileSystemControl	C:\Windows\System32	SUCCESS	Control: FSCTL_IS...
14:23:...	MsMpEng.exe	4008	CreateFile	C:\	SUCCESS	Desired Access: R...
14:23:...	MsMpEng.exe	4008	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 2 711 552, ...
14:23:...	MsMpEng.exe	4008	QueryBasicInfor...	C:\	SUCCESS	CreationTime: 201...
14:23:...	MsMpEng.exe	4008	CloseFile	C:\	SUCCESS	
14:23:...	svchost.exe	3096	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 678 400, Le...
14:23:...	MsMpEng.exe	4008	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 2 695 168, ...
14:23:...	svchost.exe	3096	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 635 904, Le...
14:23:...	MsMpEng.exe	4008	CreateFile	C:\Windows\System32\drivers\PROCM...	SUCCESS	Desired Access: R...
14:23:...	MsMpEng.exe	4008	QueryBasicInfor...	C:\Windows\System32\drivers\PROCM...	SUCCESS	CreationTime: 202...
14:23:...	MsMpEng.exe	4008	CloseFile	C:\Windows\System32\drivers\PROCM...	SUCCESS	
14:23:...	MsMpEng.exe	4008	CreateFile	C:\	SUCCESS	Desired Access: R...
14:23:...	MsMpEng.exe	4008	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 2 678 784, ...
14:23:...	MsMpEng.exe	4008	QueryBasicInfor...	C:\	SUCCESS	CreationTime: 201...
14:23:...	MsMpEng.exe	4008	CloseFile	C:\	SUCCESS	
14:23:...	Skype.exe	16936	UDP Receive	Sans:47449->13.69.134.231:3480	SUCCESS	Length: 72, sequ...

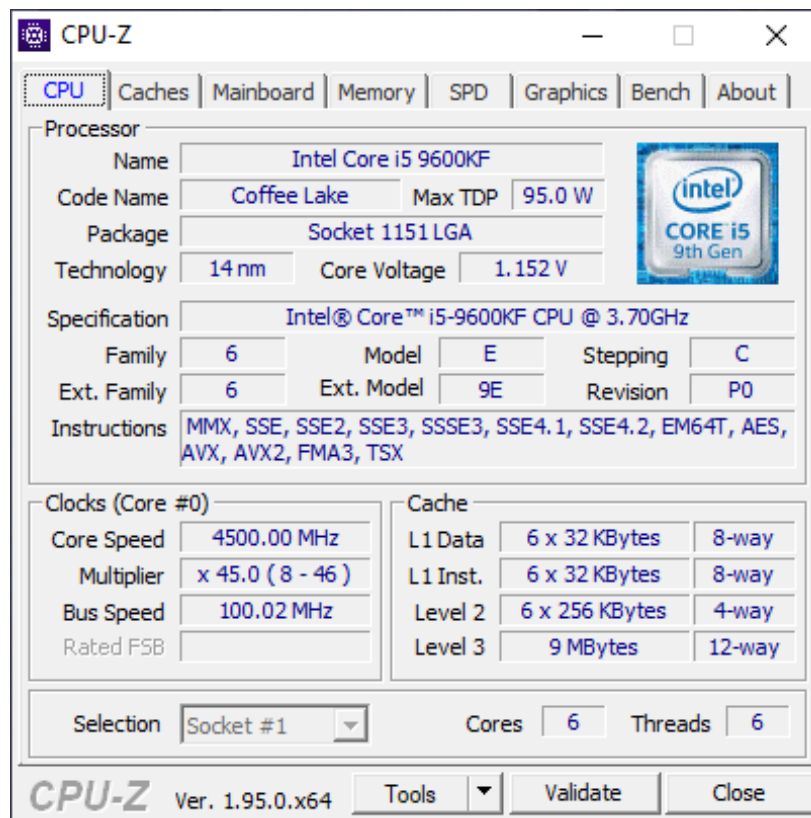
Showing 38 498 918 of 45 194 190 events (85%) Backed by virtual memory

Process Monitor valós idejű fájlrendszert, nyilvántartást és folyamat / szál tevékenységet mutat.

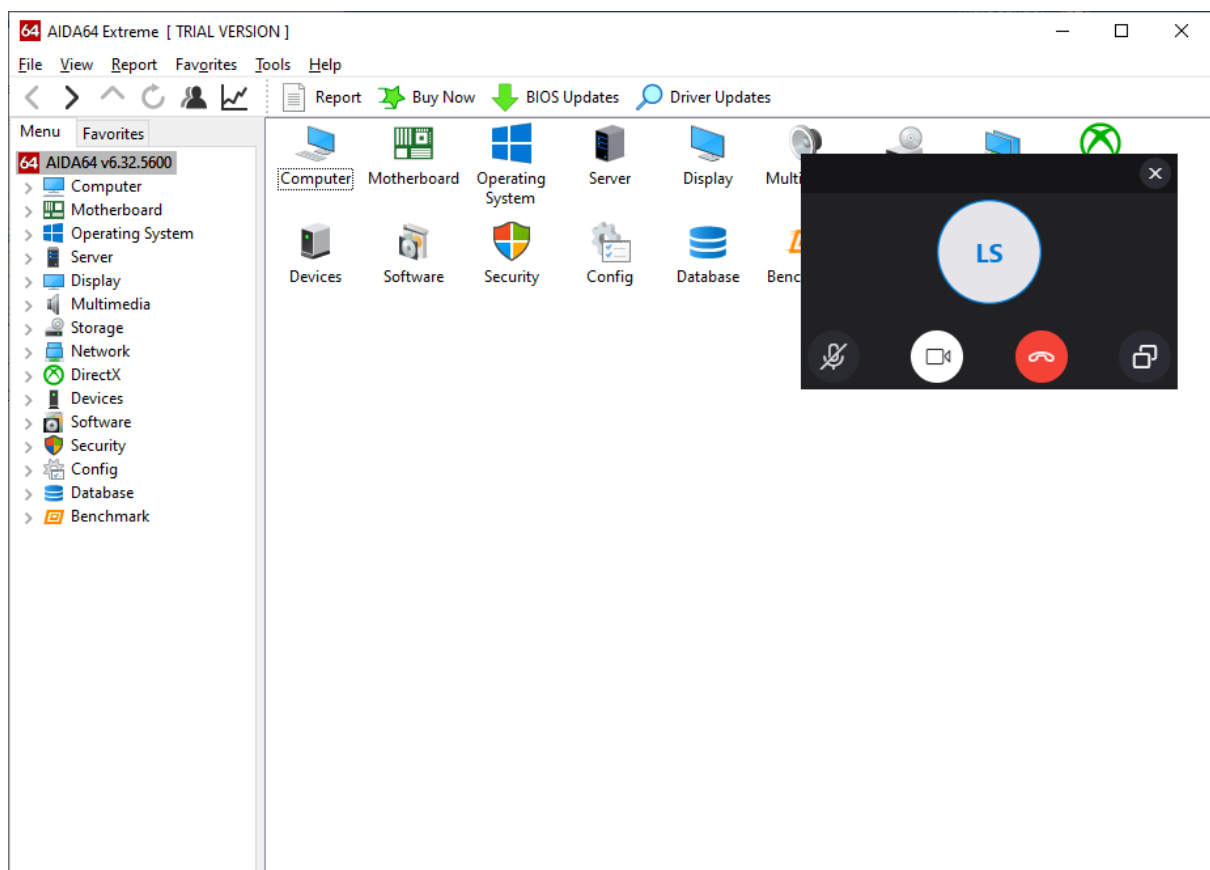
```
[12] Logon session 00000000:013c7b57:
  User name: SANS\Gery
  Auth package: NTLM
  Logon type: Interactive
  Session: 3
  Sid: S-1-5-21-1122759742-2121758638-2393287594-1002
  Logon time: 2021. 02. 23. 8:25:15
  Logon server: SANS
  DNS Domain:
  UPN:

[13] Logon session 00000000:013c7b87:
  User name: SANS\Gery
  Auth package: NTLM
  Logon type: Interactive
  Session: 3
  Sid: S-1-5-21-1122759742-2121758638-2393287594-1002
  Logon time: 2021. 02. 23. 8:25:15
  Logon server: SANS
  DNS Domain:
  UPN:
```

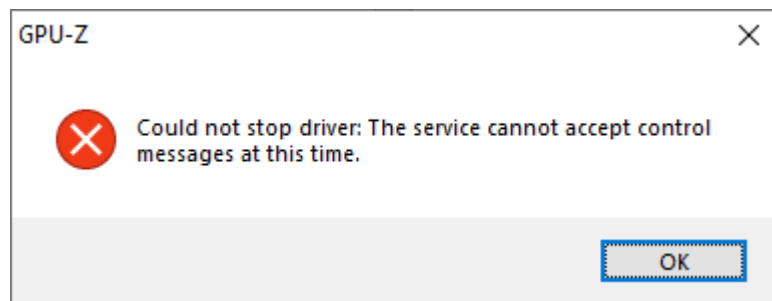
A múltban történt bejelentkezéseket jeleníti meg



A CPU élő adatait mutatja



Reportot lehet írni szinte mindenről ami a rendszerben van



GPU-Z nem működik valamiért az első futtatás után nem nyílik meg többé

De a GPU élő adatait adná vissza