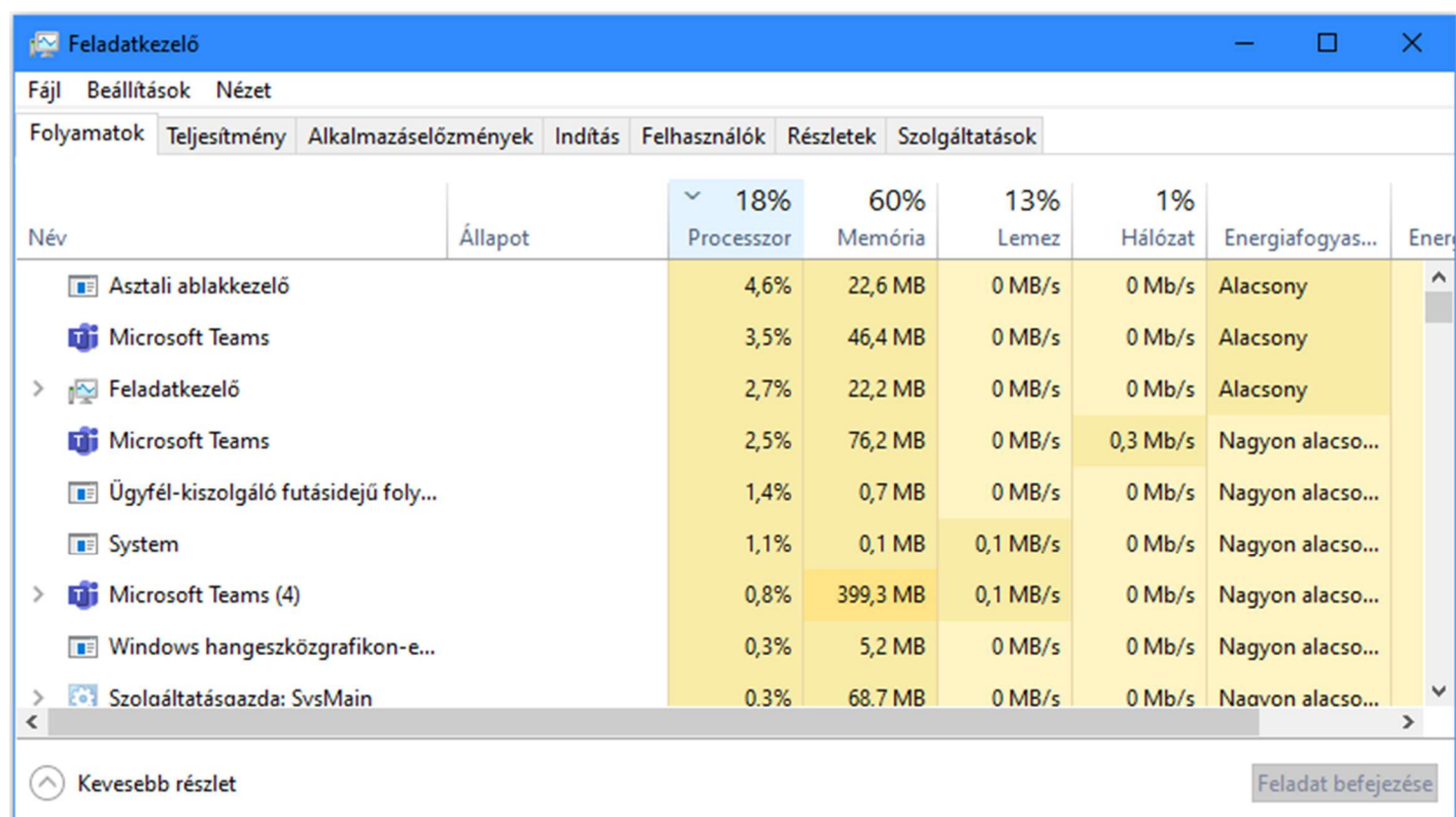
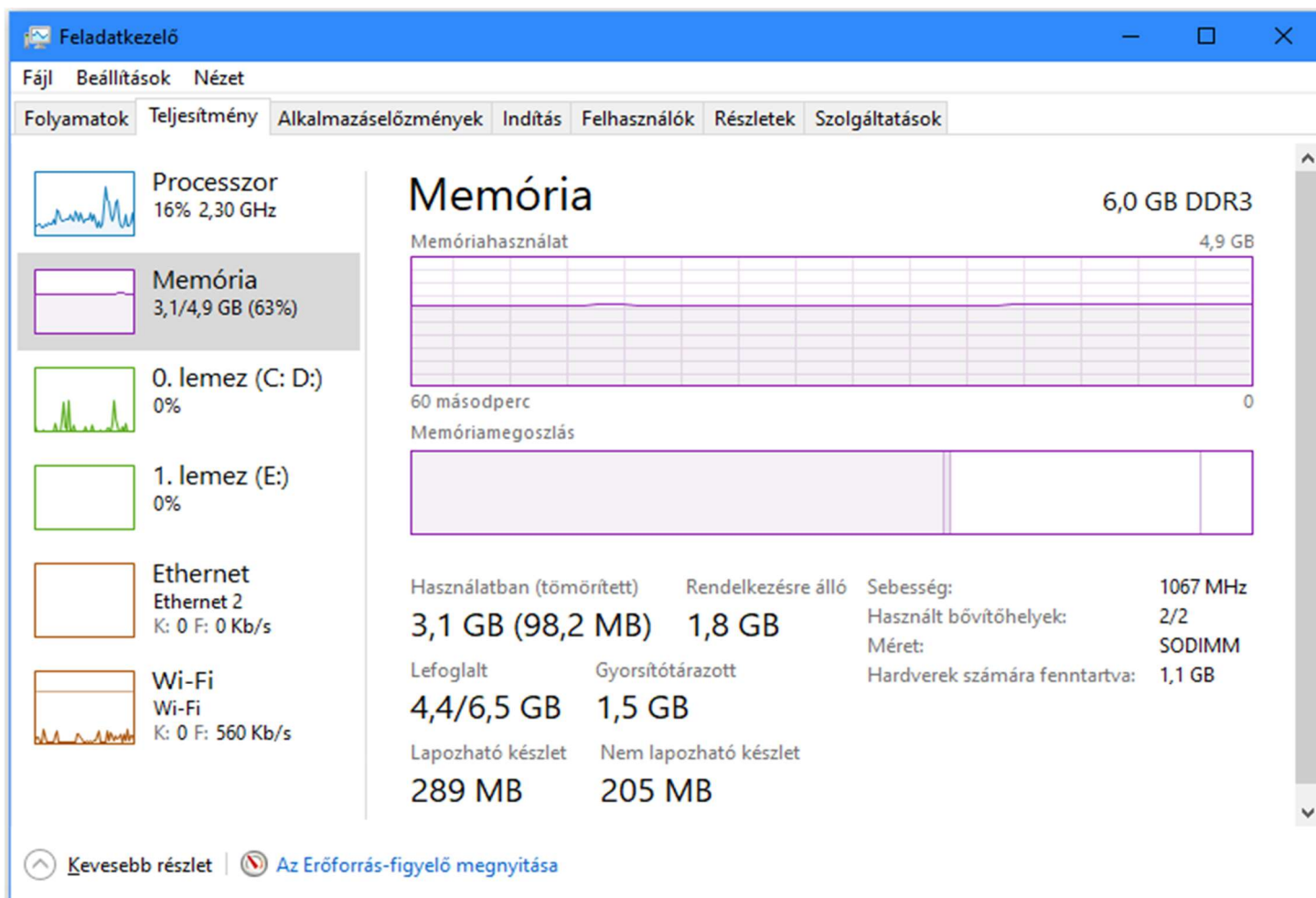


Az első részben azt vizsgáltam, hogy a teams beszélgetés közben mi az aminek a legtöbb energiaigénye van.



Másodiknak a komponensek terheltségét vizsgáltam a beszélgetés közben.



Következőnek azt néztem, hogy indításkor mik indulnak el és elég sok felesleges dolog indult amiket le is tiltottam.

Feladatkezelő

Fájl Beállítások Nézet

Folyamatok Teljesítmény Alkalmazáselemlmények Indítás Felhasználók Részletek Szolgáltatások

Legutóbbi BIOS-művelet: 0.0 másodperc

Név	Gyártó	Állapot	Hatása az indít...
CCleaner	Piriform Software Ltd	Letiltva	Nincs
DAEMON Tools Lite Agent	Disc Soft Ltd	Letiltva	Nincs
EpicGamesLauncher	Epic Games, Inc.	Letiltva	Nincs
Hamachi Client Application	LogMeln Inc.	Letiltva	Nincs
Microsoft OneDrive	Microsoft Corporation	Letiltva	Nincs
Microsoft Teams	Microsoft Corporation	Letiltva	Nincs
ScanToPCActivationApp	HP Inc.	Letiltva	Nincs
Send to OneNote Tool	Microsoft Corporation	Letiltva	Nincs
Skype	Skype	Letiltva	Nincs
Spotify	Spotify AB	Letiltva	Nincs
Steam Client Bootstrapper	Valve Corporation	Letiltva	Nincs
Tablet Client Driver	Tablet Driver	Engedélyezve	Alacsony
Windows Security notificati...	Microsoft Corporation	Engedélyezve	Alacsony
X-Mouse Button Control	Highresolution Enterpris...	Letiltva	Nincs

Kevesebb részlet

Letiltás

A következő részben azt vizsgáltam, hogy mik azok a programok amiket a windows és mik azok amiket én indítottam a használat közben, viszont találtam olyat is amit valamilyen harmadik szoftver indíthatott.

Feladatkezelő

Fájl Beállítások Nézet

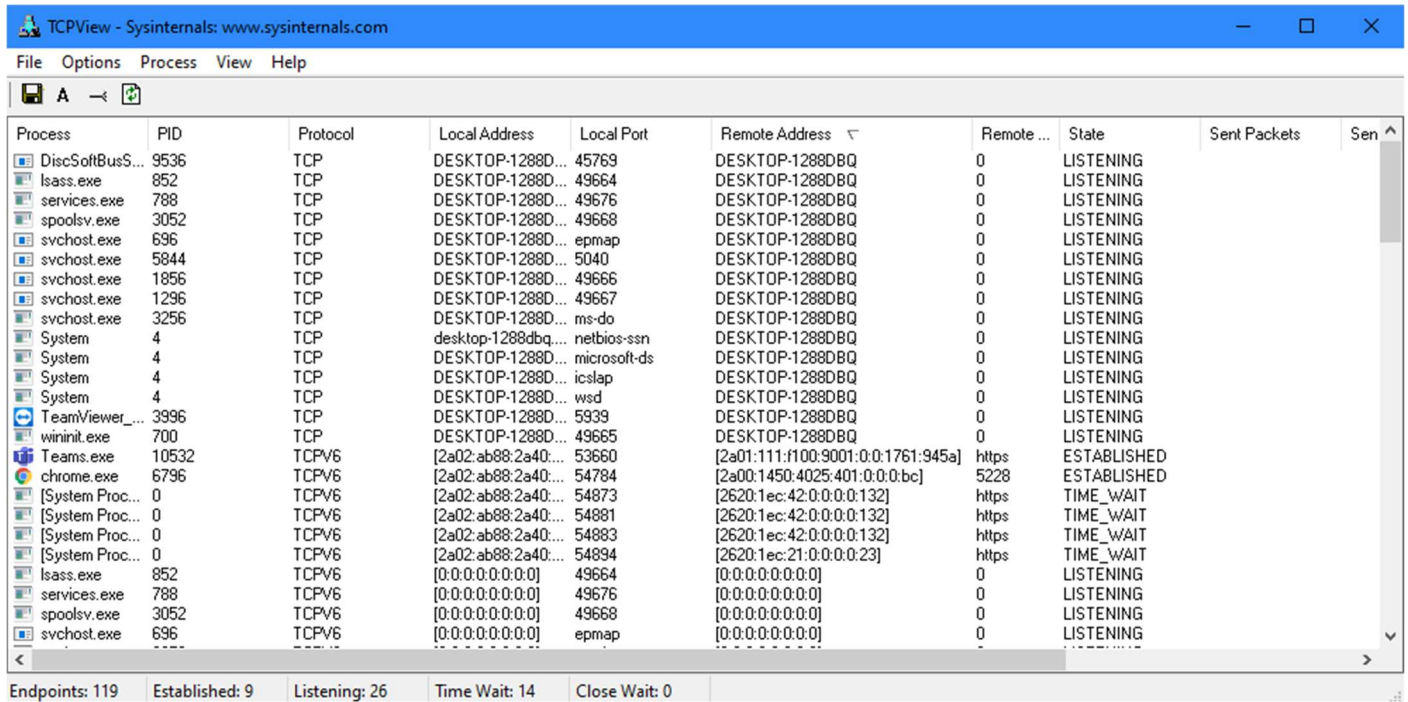
Folyamatok Teljesítmény Alkalmazáselemlmények Indítás Felhasználók Részletek Szolgáltatások

Név	Folya...	Állapot	Felhasznál...	Processzor	Memória ...	UAC virtualizálás
A rendszer üresjárat...	0	Fut	SYSTEM	86	8 K	
AcroRd32.exe	7924	Fut	Marci	00	2 748 K	Letiltva
AcroRd32.exe	2724	Fut	Marci	00	26 680 K	Letiltva
ApplicationFrameHo...	6244	Fut	Marci	00	712 K	Letiltva
AppVShNotify.exe	2868	Fut	SYSTEM	00	28 K	Nem engedély...
armsvc.exe	3836	Fut	SYSTEM	00	36 K	Nem engedély...
atieclxx.exe	10272	Fut	SYSTEM	00	416 K	Nem engedély...
atiesrxx.exe	1612	Fut	SYSTEM	00	52 K	Nem engedély...
audiodg.exe	4988	Fut	HELYI SZO...	00	5 408 K	Nem engedély...
csrss.exe	604	Fut	SYSTEM	00	664 K	Nem engedély...
csrss.exe	6664	Fut	SYSTEM	00	704 K	Nem engedély...
ctfmon.exe	1316	Fut	Marci	00	2 028 K	Letiltva
dasHost.exe	3304	Fut	HELYI SZO...	00	2 240 K	Nem engedély...
dasHost.exe	5064	Fut	HÁLÓZATI...	00	28 K	Nem engedély...
DiscSoftBusServiceLi...	9536	Fut	SYSTEM	00	672 K	Nem engedély...
dllhost.exe	5668	Fut	SYSTEM	00	836 K	Nem engedély...
dllhost.exe	6288	Fut	Marci	00	1 820 K	Letiltva
dllhost.exe	6784	Fut	Marci	00	1 844 K	Letiltva
DSDFunctionKeyCtIS...	3472	Fut	SYSTEM	00	28 K	Nem engedély...
DSDFunctionKeyCtIS...	188	Fut	Marci	00	480 K	Letiltva
DTSHELL.exe	8964	Fut	Marci	00	864 K	Letiltva
dwm.exe	4364	Fut	DWM-7	01	24 576 K	Letiltva
dynamabookSystemSer...	4016	Fut	SYSTEM	00	100 K	Nem engedély...
explorer.exe	1864	Fut	Marci	00	57 024 K	Letiltva

Kevesebb részlet

Feladat befejezése

A következőknek a tcp protokoll vizsgálatot csináltam és meglepődésemre nagyon sok minden csinál kapcsolatot miközben használok a számítógépet.

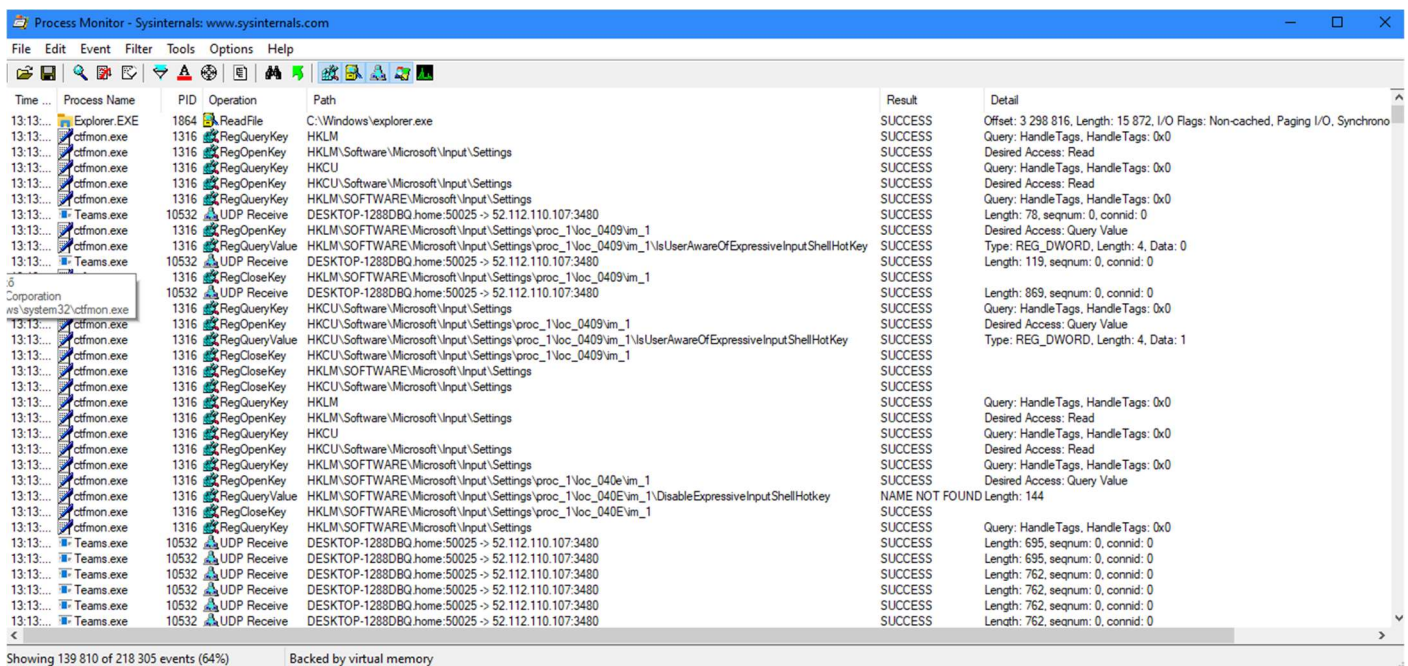


The screenshot shows the TCPView application window. The title bar reads 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Options', 'Process', 'View', and 'Help'. The main window displays a table of network connections with columns: Process, PID, Protocol, Local Address, Local Port, Remote Address, Remote Port, State, Sent Packets, and Sent Bytes. The table lists various system processes like 'DiscSoftBus...', 'lsass.exe', 'services.exe', 'spoolsv.exe', 'svchost.exe', 'System', 'TeamViewer...', 'wininit.exe', 'Teams.exe', 'chrome.exe', and '[System Proc...]' along with their respective network activity. At the bottom, a summary bar shows: Endpoints: 119, Established: 9, Listening: 26, Time Wait: 14, Close Wait: 0.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes
DiscSoftBus...	9536	TCP	DESKTOP-1288D...	45769	DESKTOP-1288DBQ	0	LISTENING		
lsass.exe	852	TCP	DESKTOP-1288D...	49664	DESKTOP-1288DBQ	0	LISTENING		
services.exe	788	TCP	DESKTOP-1288D...	49676	DESKTOP-1288DBQ	0	LISTENING		
spoolsv.exe	3052	TCP	DESKTOP-1288D...	49668	DESKTOP-1288DBQ	0	LISTENING		
svchost.exe	696	TCP	DESKTOP-1288D...	epmap	DESKTOP-1288DBQ	0	LISTENING		
svchost.exe	5844	TCP	DESKTOP-1288D...	5040	DESKTOP-1288DBQ	0	LISTENING		
svchost.exe	1856	TCP	DESKTOP-1288D...	49666	DESKTOP-1288DBQ	0	LISTENING		
svchost.exe	1296	TCP	DESKTOP-1288D...	49667	DESKTOP-1288DBQ	0	LISTENING		
svchost.exe	3256	TCP	DESKTOP-1288D...	ms-do	DESKTOP-1288DBQ	0	LISTENING		
System	4	TCP	desktop-1288dbq...	netbios-ssn	DESKTOP-1288DBQ	0	LISTENING		
System	4	TCP	DESKTOP-1288D...	microsoft-ds	DESKTOP-1288DBQ	0	LISTENING		
System	4	TCP	DESKTOP-1288D...	icslap	DESKTOP-1288DBQ	0	LISTENING		
System	4	TCP	DESKTOP-1288D...	wscd	DESKTOP-1288DBQ	0	LISTENING		
TeamViewer...	3996	TCP	DESKTOP-1288D...	5939	DESKTOP-1288DBQ	0	LISTENING		
wininit.exe	700	TCP	DESKTOP-1288D...	49665	DESKTOP-1288DBQ	0	LISTENING		
Teams.exe	10532	TCPV6	[2a02:ab88:2a40...	53660	[2a01:111:f100:9001:0:0:1761:945a]	https	ESTABLISHED		
chrome.exe	6796	TCPV6	[2a02:ab88:2a40...	54784	[2a00:1450:4025:401:0:0:0:bc]	5228	ESTABLISHED		
[System Proc...	0	TCPV6	[2a02:ab88:2a40...	54873	[2620:1ec:42:0:0:0:0:132]	https	TIME_WAIT		
[System Proc...	0	TCPV6	[2a02:ab88:2a40...	54881	[2620:1ec:42:0:0:0:0:132]	https	TIME_WAIT		
[System Proc...	0	TCPV6	[2a02:ab88:2a40...	54883	[2620:1ec:42:0:0:0:0:132]	https	TIME_WAIT		
[System Proc...	0	TCPV6	[2a02:ab88:2a40...	54894	[2620:1ec:21:0:0:0:0:23]	https	TIME_WAIT		
lsass.exe	852	TCPV6	[0:0:0:0:0:0:0:0]	49664	[0:0:0:0:0:0:0:0]	0	LISTENING		
services.exe	788	TCPV6	[0:0:0:0:0:0:0:0]	49676	[0:0:0:0:0:0:0:0]	0	LISTENING		
spoolsv.exe	3052	TCPV6	[0:0:0:0:0:0:0:0]	49668	[0:0:0:0:0:0:0:0]	0	LISTENING		
svchost.exe	696	TCPV6	[0:0:0:0:0:0:0:0]	epmap	[0:0:0:0:0:0:0:0]	0	LISTENING		

Endpoints: 119   Established: 9   Listening: 26   Time Wait: 14   Close Wait: 0

A processz monitort próbáltam ki következőknek és láttam, hogy nagyon sok processz zajlik le másodpercenként.

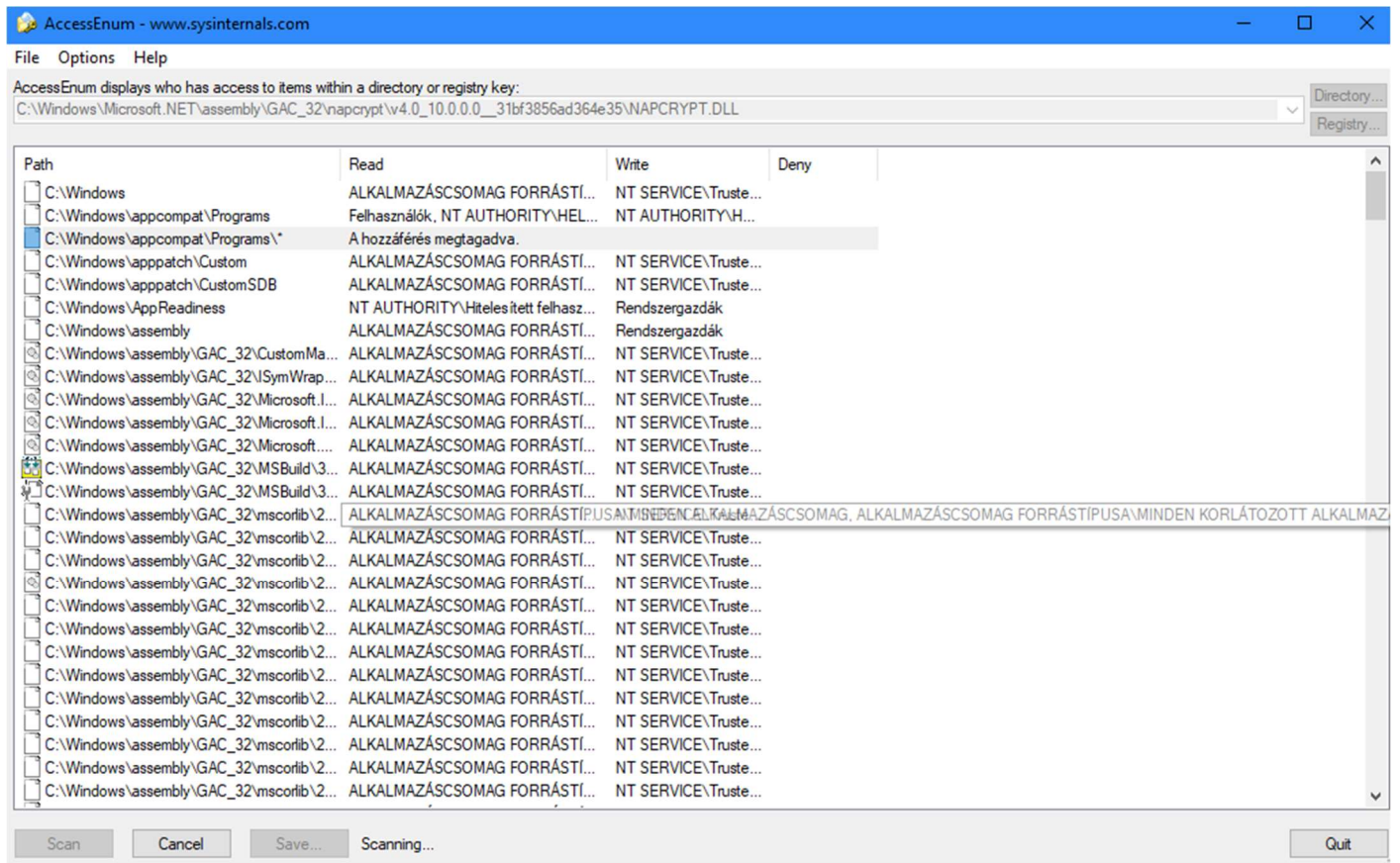


The screenshot shows the Process Monitor application window. The title bar reads 'Process Monitor - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Edit', 'Event', 'Filter', 'Tools', 'Options', and 'Help'. The main window displays a list of system events with columns: Time, Process Name, PID, Operation, Path, Result, and Detail. The events show various registry operations (ReadFile, RegOpenKey, RegQueryValue, RegCloseKey) and network activity (UDP Receive) for processes like 'Explorer.EXE', 'ctfmon.exe', 'Teams.exe', and 'System32\ctfmon.exe'. At the bottom, a status bar indicates 'Showing 139 810 of 218 305 events (64%)' and 'Backed by virtual memory'.

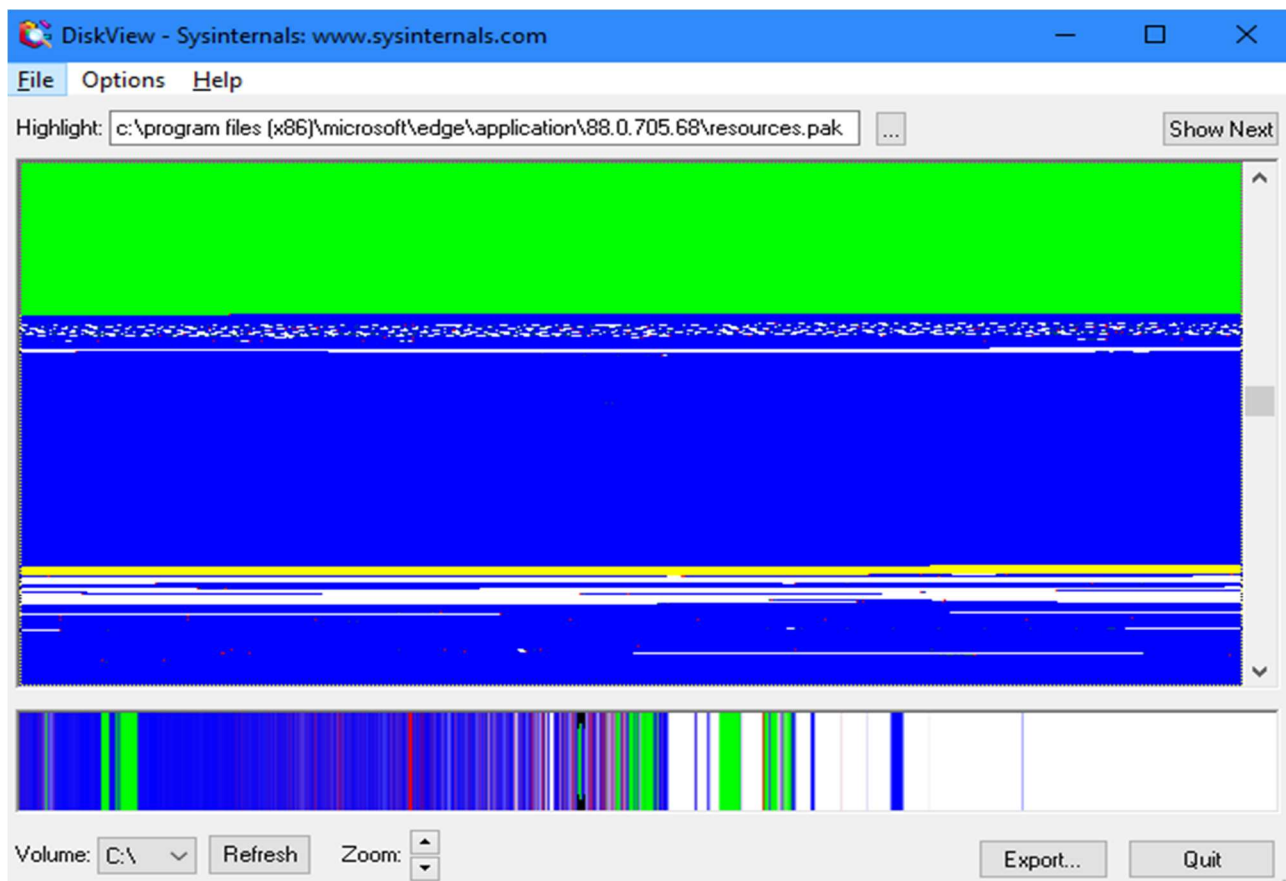
Time	Process Name	PID	Operation	Path	Result	Detail
13:13:...	Explorer.EXE	1864	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 3 298 816, Length: 15 872, I/O Flags: Non-cached, Paging I/O, Synchron...
13:13:...	ctfmon.exe	1316	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	ctfmon.exe	1316	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: Read
13:13:...	ctfmon.exe	1316	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	ctfmon.exe	1316	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Settings	SUCCESS	Desired Access: Read
13:13:...	ctfmon.exe	1316	RegOpenKey	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	ctfmon.exe	1316	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1Voc_0409\im_1	SUCCESS	Length: 78, sequum: 0, connid: 0
13:13:...	ctfmon.exe	1316	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1Voc_0409\im_1	SUCCESS	Desired Access: Query Value
13:13:...	ctfmon.exe	1316	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1Voc_0409\im_1	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Length: 119, sequum: 0, connid: 0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Length: 869, sequum: 0, connid: 0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Query: HandleTags, HandleTags: 0x0
13:13:...	Teams.exe	10532	UDP Receive	DESKTOP-1288DBQ.home:50025 -> 52.112.110.107:3480	SUCCESS	Desired Access: Read



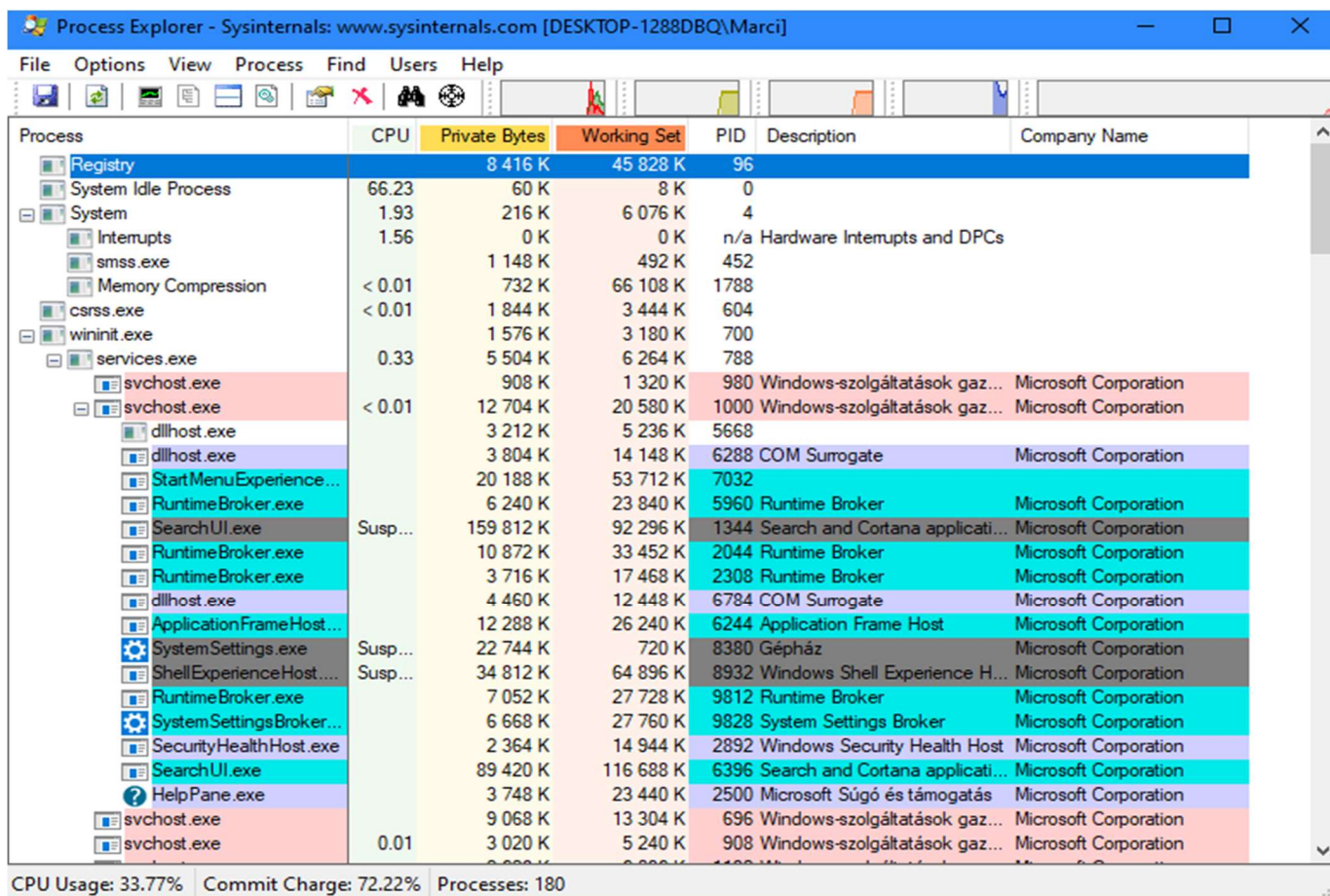
Az AccesEnum futtatásakor észrevettem, hogy a sok filehoz mennyi programnak van hozzáférése.



A DiskView program nagyon érdekes volt, mert mutatja hogy egyes programok mennyi helyet foglal el a merevlemezemen és ezt mind vizuálisan.



Process Explorer-ben sokkal több mindent megtudtam az adott processzekről.



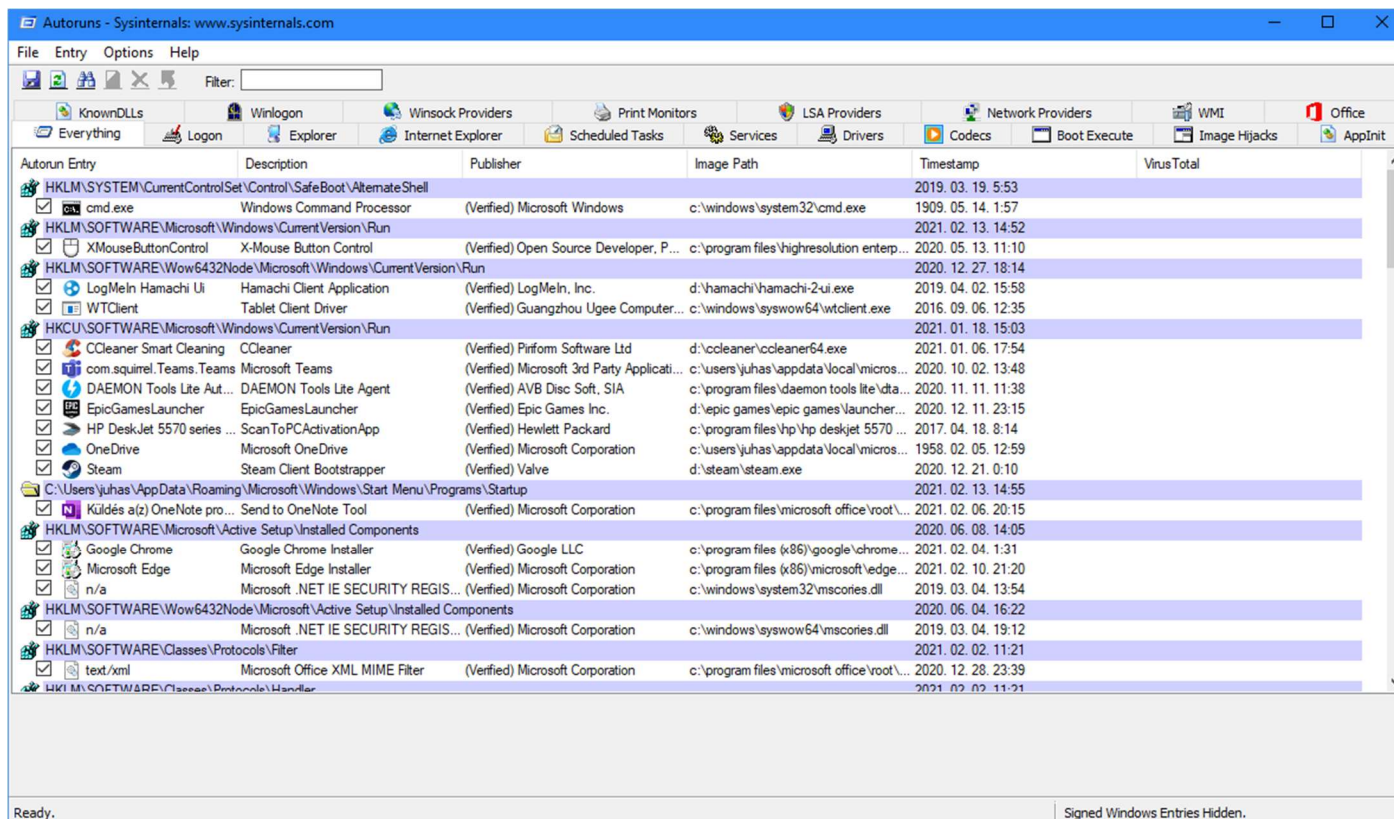
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-1288DBQ\Marci]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		8 416 K	45 828 K	96		
System Idle Process		60 K	8 K	0		
System	1.93	216 K	6 076 K	4		
Interrupts	1.56	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 148 K	492 K	452		
Memory Compression	< 0.01	732 K	66 108 K	1788		
csrss.exe	< 0.01	1 844 K	3 444 K	604		
wininit.exe		1 576 K	3 180 K	700		
services.exe	0.33	5 504 K	6 264 K	788		
svchost.exe		908 K	1 320 K	980	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe	< 0.01	12 704 K	20 580 K	1000	Windows-szolgáltatások gaz...	Microsoft Corporation
dllhost.exe		3 212 K	5 236 K	5668		
dllhost.exe		3 804 K	14 148 K	6288	COM Surrogate	Microsoft Corporation
StartMenuExperienceHost.exe		20 188 K	53 712 K	7032		
RuntimeBroker.exe		6 240 K	23 840 K	5960	Runtime Broker	Microsoft Corporation
SearchUI.exe	Susp...	159 812 K	92 296 K	1344	Search and Cortana applicati...	Microsoft Corporation
RuntimeBroker.exe		10 872 K	33 452 K	2044	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		3 716 K	17 468 K	2308	Runtime Broker	Microsoft Corporation
dllhost.exe		4 460 K	12 448 K	6784	COM Surrogate	Microsoft Corporation
ApplicationFrameHost.exe		12 288 K	26 240 K	6244	Application Frame Host	Microsoft Corporation
SystemSettings.exe	Susp...	22 744 K	720 K	8380	Gépház	Microsoft Corporation
ShellExperienceHost.exe	Susp...	34 812 K	64 896 K	8932	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		7 052 K	27 728 K	9812	Runtime Broker	Microsoft Corporation
SystemSettingsBroker.exe		6 668 K	27 760 K	9828	System Settings Broker	Microsoft Corporation
SecurityHealthHost.exe		2 364 K	14 944 K	2892	Windows Security Health Host	Microsoft Corporation
SearchUI.exe		89 420 K	116 688 K	6396	Search and Cortana applicati...	Microsoft Corporation
HelpPane.exe		3 748 K	23 440 K	2500	Microsoft Súlyó és támogatás	Microsoft Corporation
svchost.exe		9 068 K	13 304 K	696	Windows-szolgáltatások gaz...	Microsoft Corporation
svchost.exe	0.01	3 020 K	5 240 K	908	Windows-szolgáltatások gaz...	Microsoft Corporation

CPU Usage: 33.77% Commit Charge: 72.22% Processes: 180

Az autoruns nekem nagyon hasonlított a feladatkezelő indítás opcióhoz viszont sokkal részletesebb.



Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

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 AppInit

Autorun Entry	Description	Publisher	Image Path	Timestamp	Virus Total
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				2019. 03. 19. 5:53	
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	1909. 05. 14. 1:57	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021. 02. 13. 14:52	
XMouseButtonControl	X-Mouse Button Control	(Verified) Open Source Developer, P...	c:\program files\highresolution enter...	2020. 05. 13. 11:10	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2020. 12. 27. 18:14	
LogMeIn Hamachi UI	Hamachi Client Application	(Verified) LogMeIn, Inc.	d:\hamachi\hamachi-2-ui.exe	2019. 04. 02. 15:58	
WTClient	Tablet Client Driver	(Verified) Guangzhou Ugee Computer...	c:\windows\syswow64\wtclient.exe	2016. 09. 06. 12:35	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021. 01. 18. 15:03	
CCleaner Smart Cleaning	CCleaner	(Verified) Piriform Software Ltd	d:\ccleaner\ccleaner64.exe	2021. 01. 06. 17:54	
com.squirrel.Teams.Teams	Microsoft Teams	(Verified) Microsoft 3rd Party Applicati...	c:\users\juhas\appdata\local\microso...	2020. 10. 02. 13:48	
DAEMON Tools Lite Aut...	DAEMON Tools Lite Agent	(Verified) AVB Disc Soft, SIA	c:\program files\daemon tools lite\lta...	2020. 11. 11. 11:38	
EpicGamesLauncher	EpicGamesLauncher	(Verified) Epic Games Inc.	d:\epic games\epic games\launcher...	2020. 12. 11. 23:15	
HP DeskJet 5570 series ...	ScanToPCActivationApp	(Verified) Hewlett Packard	c:\program files\hp\hp deskjet 5570 ...	2017. 04. 18. 8:14	
OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	c:\users\juhas\appdata\local\microso...	1958. 02. 05. 12:59	
Steam	Steam Client Bootstrapper	(Verified) Valve	d:\steam\steam.exe	2020. 12. 21. 0:10	
C:\Users\juhas\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				2021. 02. 13. 14:55	
Küldés a(z) OneNote pro...	Send to OneNote Tool	(Verified) Microsoft Corporation	c:\program files\microsoft office\root\...	2021. 02. 06. 20:15	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2020. 06. 08. 14:05	
Google Chrome	Google Chrome Installer	(Verified) Google LLC	c:\program files (x86)\google\chrome...	2021. 02. 04. 1:31	
Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge...	2021. 02. 10. 21:20	
n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	2019. 03. 04. 13:54	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				2020. 06. 04. 16:22	
n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\syswow64\mscories.dll	2019. 03. 04. 19:12	
HKLM\SOFTWARE\Classes\Protocols\Filer				2021. 02. 02. 11:21	
text/xml	Microsoft Office XML MIME Filter	(Verified) Microsoft Corporation	c:\program files\microsoft office\root\...	2020. 12. 28. 23:39	
HKLM\SOFTWARE\Classes\Protocols\Handler				2021. 02. 02. 11:21	

Ready. Signed Windows Entries Hidden.