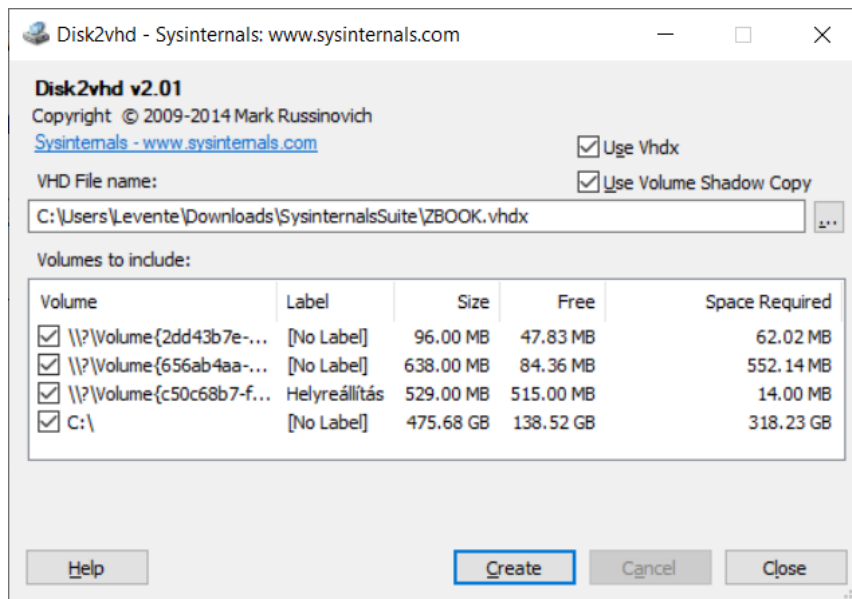
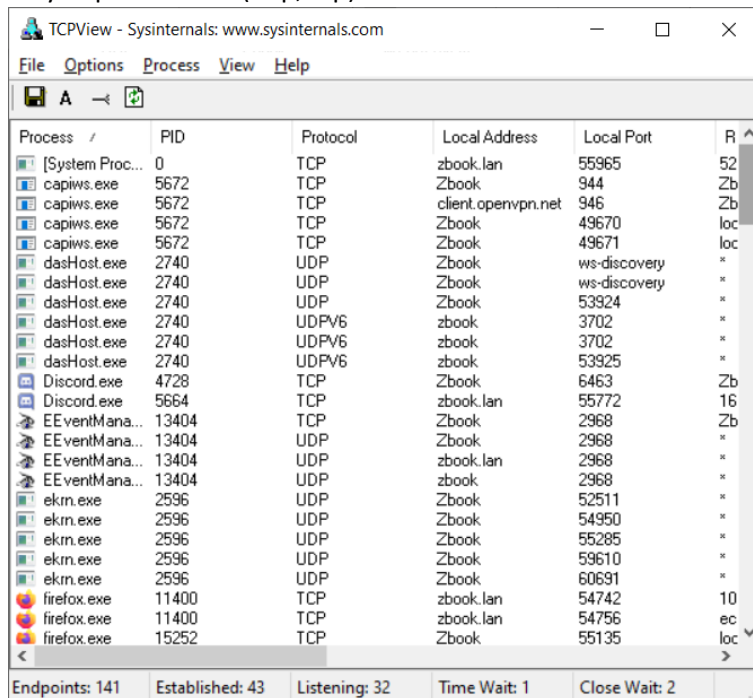


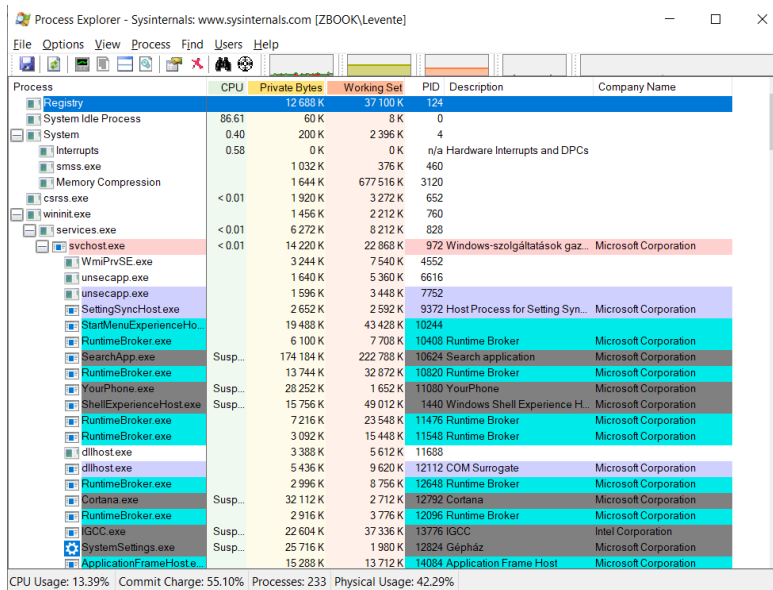
- a) A disk2vhd-val lehet megnézni a háttértárakat, azok méretét, köteteit, címkeit.



- b) A tcpview-val lehet megnézni egyes folyamatok/processzek kommunikációját. Első körben a névvel, pid-de (process iD) azonosítjuk a folyamatot, és megnézzük, hogy milyen portokat, milyen protokollon (udp, tcp) kommunikál.



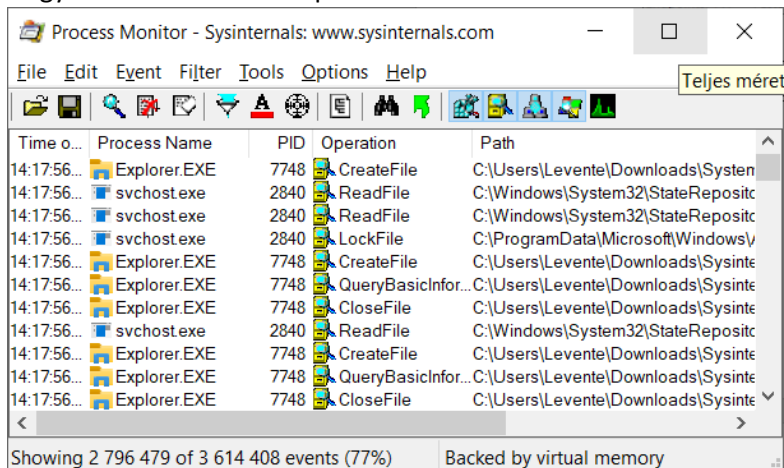
- c) A process explorer-rel lehet egyes processzekről részletes információt kapni (név, pid, processzor kihasználtság, leírás, készítő neve, foglalt hely)



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		12 688 K	37 100 K	124		
System Idle Process	86.61	60 K	8 K	0		
System	0.40	200 K	2 396 K	4		
Interrupts	0.58	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 032 K	376 K	460		
Memory Compression		1 644 K	677 516 K	3120		
csrss.exe	< 0.01	1 920 K	3 272 K	652		
wininit.exe		1 456 K	2 212 K	760		
services.exe	< 0.01	6 272 K	8 212 K	828		
svchost.exe	< 0.01	14 220 K	22 868 K	972	Windows-szolgáltatások gaz...	Microsoft Corporation
WmiPrvSE.exe		3 244 K	7 540 K	4552		
unsecapp.exe		1 640 K	5 360 K	6616		
unsecapp.exe		1 596 K	3 448 K	7752		
SettingSyncHost.exe		2 652 K	2 592 K	9372	Host Process for Setting Syn...	Microsoft Corporation
StartMenuExperienceHost.exe		19 488 K	43 428 K	10244		
RuntimeBroker.exe		6 100 K	7 708 K	10408	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	174 184 K	222 788 K	10624	Search application	Microsoft Corporation
RuntimeBroker.exe		13 744 K	32 872 K	10820	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	28 252 K	1 652 K	11050	YourPhone	Microsoft Corporation
ShellExperienceHost.exe	Susp...	15 756 K	49 012 K	1440	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		7 216 K	23 548 K	11476	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		3 092 K	15 448 K	11548	Runtime Broker	Microsoft Corporation
dllhost.exe		3 388 K	5 612 K	11658		
dllhost.exe		5 436 K	9 620 K	12112	COM Surrogate	Microsoft Corporation
RuntimeBroker.exe		2 996 K	8 756 K	12648	Runtime Broker	Microsoft Corporation
Cortana.exe	Susp...	32 112 K	2 712 K	12792	Cortana	Microsoft Corporation
RuntimeBroker.exe		2 916 K	3 776 K	12096	Runtime Broker	Microsoft Corporation
IGCC.exe	Susp...	22 604 K	37 336 K	13776	IGCC	Intel Corporation
SystemSettings.exe	Susp...	25 716 K	1 980 K	12824	Gépház	Microsoft Corporation
ApplicationFrameHost.exe		15 288 K	13 712 K	14084	Application Frame Host	Microsoft Corporation

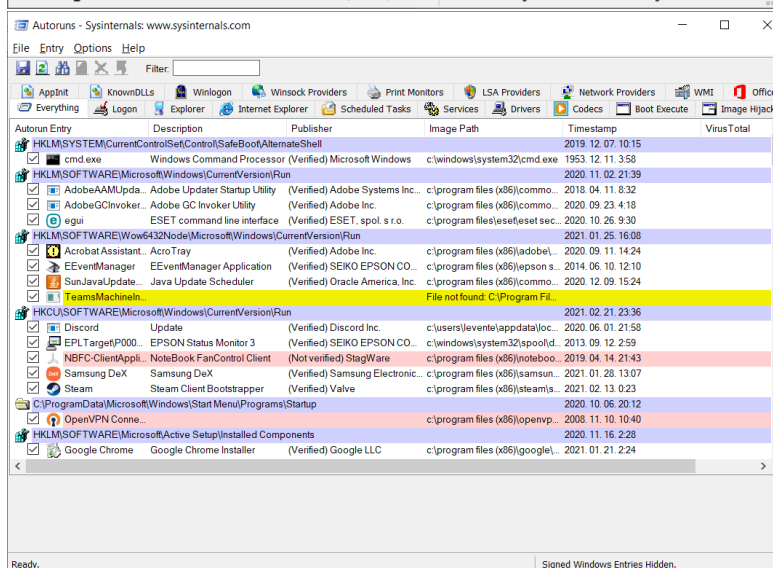
CPU Usage: 13.39% Commit Charge: 55.10% Processes: 233 Physical Usage: 42.29%

Nagyon hasonló tudású a process monitor és az autoruns is.



Time o...	Process Name	PID	Operation	Path
14:17:56...	Explorer.EXE	7748	CreateFile	C:\Users\Levente\Downloads\System
14:17:56...	svchost.exe	2840	ReadFile	C:\Windows\System32\StateRepositc
14:17:56...	svchost.exe	2840	ReadFile	C:\Windows\System32\StateRepositc
14:17:56...	svchost.exe	2840	LockFile	C:\ProgramData\Microsoft\Windows\y
14:17:56...	Explorer.EXE	7748	CreateFile	C:\Users\Levente\Downloads\Sysinte
14:17:56...	Explorer.EXE	7748	QueryBasicInfor...	C:\Users\Levente\Downloads\Sysinte
14:17:56...	Explorer.EXE	7748	CloseFile	C:\Users\Levente\Downloads\Sysinte
14:17:56...	svchost.exe	2840	ReadFile	C:\Windows\System32\StateRepositc
14:17:56...	Explorer.EXE	7748	CreateFile	C:\Users\Levente\Downloads\Sysinte
14:17:56...	Explorer.EXE	7748	QueryBasicInfor...	C:\Users\Levente\Downloads\Sysinte
14:17:56...	Explorer.EXE	7748	CloseFile	C:\Users\Levente\Downloads\Sysinte

Showing 2 796 479 of 3 614 408 events (77%) Backed by virtual memory



Name	Description	Publisher	Image Path	Timestamp
HKLM\SYSTEM\CurrentControlSet\SafeBoot\AlternateShell				2019.12.07.10.15
cmd.exe	Windows Command Processor (Verified)	Microsoft Windows	c:\windows\system32\cmd.exe	1953.12.11.3.58
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2020.11.02.21.39
AdobeAAMUpda...	Adobe Updater Startup Utility (Verified)	Adobe Systems Inc.	c:\program files (x86)\commo...	2018.04.11.8.32
AdobeGCInvoker...	Adobe GC Invoker Utility (Verified)	Adobe Inc.	c:\program files (x86)\commo...	2020.09.23.4.18
egui	ESET command line interface (Verified)	ESET, spol. s r.o.	c:\program files\eset\eset sec...	2020.10.26.9.30
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2021.01.25.16.08
Acrobat Assistant...	AcroTray (Verified)	Adobe Inc.	c:\program files (x86)\adobe\...	2020.09.11.14.24
EEventManager	EEventManager Application (Verified)	SEIKO EPSON CO...	c:\program files (x86)\epson s...	2014.06.10.12.10
SunJavaUpdate...	Java Update Scheduler (Verified)	Oracle America, Inc.	c:\program files (x86)\commo...	2020.12.09.15.24
TeamsMachineIn...			File not found: C:\Program Fil...	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021.02.21.23.36
Discord	Update (Verified)	Discord Inc.	c:\users\levente\appdata\loc...	2020.06.01.21.58
EPLTargetP000...	EPSON Status Monitor 3 (Verified)	SEIKO EPSON CO...	c:\windows\system32\pool\d...	2013.09.12.2.59
NBFC-ClientAppl...	NoteBook FanControl Client (Not verified)	StagWare	c:\program files (x86)\noteboo...	2019.04.14.21.43
Samsung DeX	Samsung DeX (Verified)	Samsung Electronic...	c:\program files (x86)\samsun...	2021.01.28.13.07
Steam	Steam Client Bootstrapper (Verified)	Valve	c:\program files (x86)\steam\...	2021.02.13.0.23
OpenVPN Connect	OpenVPN Connect (Verified)	OpenVPN LLC	c:\program files (x86)\openvp...	2020.10.06.20.12
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2020.11.10.10.40
Google Chrome	Google Chrome Installer (Verified)	Google LLC	c:\program files (x86)\google\...	2021.01.21.2.24

Ready. Signed Windows Entries Hidden.

d) A logonsession a bejelentkezett felhasználókat és az ahhoz tartozó időpontot mutatja

```
Administrator: Parancssor

DMS Domain:
UPN:

[6] Logon session 00000000:0001c8bf:
User name: Window Manager\DMH-1
Auth package: Negotiate
Logon type: Interactive
Session: 1
Sid: S-1-5-90-0-1
Logon time: 2021. 02. 22. 12:11:35
Logon server:
DMS Domain:
UPN:

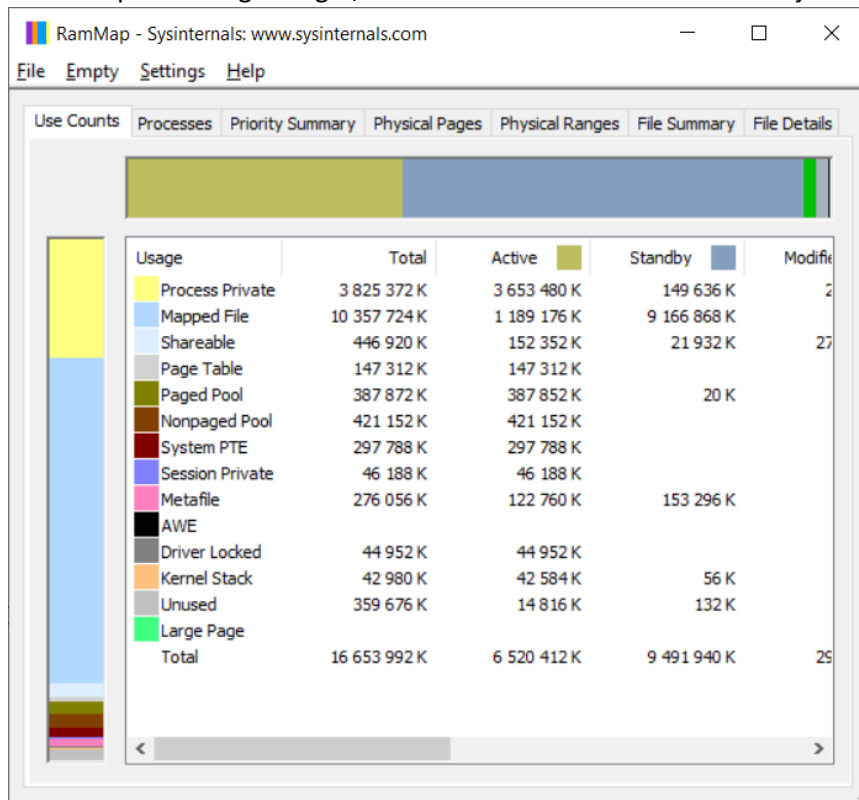
[7] Logon session 00000000:0001cde9:
User name: Window Manager\DMH-1
Auth package: Negotiate
Logon type: Interactive
Session: 1
Sid: S-1-5-90-0-1
Logon time: 2021. 02. 22. 12:11:35
Logon server:
DMS Domain:
UPN:

[8] Logon session 00000000:0003903c:
User name: ZBOOK\Levente
Auth package: NTLM
Logon type: Interactive
Session: 1
Sid: S-1-5-21-2455828862-1336757110-277662428-1001
Logon time: 2021. 02. 22. 12:11:36
Logon server: ZBOOK
DMS Domain:
UPN:

[9] Logon session 00000000:000390ff:
User name: ZBOOK\Levente
Auth package: NTLM
Logon type: Interactive
Session: 1
Sid: S-1-5-21-2455828862-1336757110-277662428-1001
Logon time: 2021. 02. 22. 12:11:36
Logon server: ZBOOK
DMS Domain:
UPN:

C:\Users\Levente\Downloads\SysinternalsSuite>
```

e) A rammap a ram foglaltságát, és az ahhoz tartozó felosztást mutatja



3) Itt a számítógépről/laptopról láthatunk részletes információkat. A cpu-z speciálisan a cpu-ról, a gpu-z speciálisan a gpu-ról ad meg extra információkat.

