

Disk2vhd: virtuális merevlemez hoz létre ami a microsoft virtuális gépeknél használható.

TCPView: megmutatja mi folyik éppen a hálózaton.

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
System Proc...	0	TCP	LAPTOP-KIEM...	53534	localhost	53535	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53539	localhost	53538	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53542	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53544	localhost	53543	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53547	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53549	localhost	53548	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53552	ecs-159-138-206...	https	TIME_WAIT	1		5	3 766
System Proc...	0	TCP	LAPTOP-KIEM...	53554	localhost	53553	TIME_WAIT	4		894	
System Proc...	0	TCP	laptop-kitem...	53557	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53559	localhost	53558	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53562	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53564	localhost	53563	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53567	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53569	localhost	53568	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53572	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53574	localhost	53573	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53577	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53579	localhost	53578	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53582	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53584	localhost	53583	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53587	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53589	localhost	53588	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53592	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53594	localhost	53593	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53597	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53599	localhost	53598	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53602	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53604	localhost	53603	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53607	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53609	localhost	53608	TIME_WAIT	1		11	
System Proc...	0	TCP	laptop-kitem...	53612	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53614	localhost	53613	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53617	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53619	localhost	53618	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53622	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53624	localhost	53623	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53627	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53629	localhost	53628	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53632	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53634	localhost	53633	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53637	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53639	localhost	53638	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53642	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53644	localhost	53643	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53647	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53649	localhost	53648	TIME_WAIT				
System Proc...	0	TCP	laptop-kitem...	53652	ecs-159-138-206...	https	TIME_WAIT				
System Proc...	0	TCP	LAPTOP-KIEM...	53654	localhost	53653	TIME_WAIT				
chrome.exe	13740	TCP	localhost	51203	13.107.42.12	https	ESTABLISHED	18	45 636	11	3 572

Endpoints: 147 Established: 25 Listening: 22 Time Wait: 49 Close Wait: 0

Process Explorer: a számítógép erőforrásairól és futó processzekről ad információt.

Process Explorer - Sysinternals: www.sysinternals.com [LAPTOP-KIEMIMO\uljiz]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	89.23	60 K	8 K	0		
System	0.83	196 K	20 K	4		
smss.exe	0.58	OK	OK	n/a	Hardware Interrupts and DPCs	
svchost.exe	1.152 K	172 K	428			
Memory Compression	< 0.01	824 K	223 480 K	2204		
csrss.exe	< 0.01	1 860 K	1 952 K	800		
svchost.exe	1.420 K	600 K	500			
services.exe	< 0.01	5 512 K	5 736 K	396		
svchost.exe	920 K	964 K	1040	1040	Windows-szolgáltatások gaz.	Microsoft Corporation
svchost.exe	< 0.01	14 300 K	25 648 K	1112	Windows-szolgáltatások gaz.	Microsoft Corporation
WsmPrvSE.exe	0.03	7 656 K	8 760 K	1712		
dhcpcd.exe		3 436 K	3 756 K	2748		
unsecapp.exe		1 816 K	3 344 K	7052		
unsecapp.exe		1 836 K	3 236 K	7516		
StartMenuExperienceHo...		42 216 K	51 284 K	7872		
RuntimeBroker.exe		6 772 K	19 960 K	7882	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		18 272 K	29 428 K	8372	Runtime Broker	Microsoft Corporation
SettingSyncHost.exe		16 080 K	6 428 K	9188	Host Process for Setting Syn...	Microsoft Corporation
LockApp.exe	Susp...	26 836 K	28 568 K	9172	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		9 128 K	17 940 K	9256	Runtime Broker	Microsoft Corporation
VisualHost.exe	Susp...	39 160 K	1 600 K	9612	VisualHost	Microsoft Corporation
RuntimeBroker.exe		2 732 K	4 584 K	10140	Runtime Broker	Microsoft Corporation
SearchUI.exe	Susp...	151 608 K	68 248 K	10564	Search and Cortana applicat...	Microsoft Corporation
RuntimeBroker.exe		2 224 K	2 860 K	11400	Runtime Broker	Microsoft Corporation
ApplicationFrameHost.e...	< 0.01	10 728 K	30 700 K	2216	Application Frame Host	Microsoft Corporation
Windows App.exe	Susp...	43 912 K	1 056 K	2452	Store	Microsoft Corporation
RuntimeBroker.exe		2 332 K	3 032 K	3624	Runtime Broker	Microsoft Corporation
SystemSettings.exe	Susp...	37 896 K	608 K	14192	Gépkész	Microsoft Corporation
UserOOBEBroker.exe		1 976 K	1 624 K	1772	User OOBE Broker	Microsoft Corporation
dhcpcd.exe		2 832 K	7 324 K	6212	COM Surrogate	Microsoft Corporation
SecurityHealthHost.exe		2 528 K	6 184 K	4476	Windows Security Health Host	Microsoft Corporation
ShellExperienceHost.exe	Susp...	48 652 K	50 776 K	8668	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		8 116 K	23 636 K	3140	Runtime Broker	Microsoft Corporation
SystemSettingsBroker.e...		7 916 K	19 196 K	10396	System Settings Broker	Microsoft Corporation
RuntimeBroker.exe		5 848 K	10 980 K	3276	Runtime Broker	Microsoft Corporation
Microsoft Photos.exe	Susp...	63 940 K	21 212 K	5940		
RuntimeBroker.exe		12 444 K	28 468 K	2756	Runtime Broker	Microsoft Corporation
dhcpcd.exe		9 100 K	16 328 K	6744	COM Surrogate	Microsoft Corporation
lsocoreworker.exe		9 248 K	16 784 K	11976		
smartscreen.exe		13 032 K	30 588 K	9924	Windows Defender SmartScr...	Microsoft Corporation
WWANHost.exe	Susp...	225 684 K	73 560 K	13300	Windows webalkalmazás ga...	Microsoft Corporation
RuntimeBroker.exe		5 180 K	29 712 K	1056	Runtime Broker	Microsoft Corporation
BackgroundTaskHost.exe	Susp...	15 672 K	22 648 K	9572	Background Task Host	Microsoft Corporation
BackgroundTaskHost.exe	Susp...	15 372 K	21 728 K	9296	Background Task Host	Microsoft Corporation
WUDFHost.exe		2 752 K	608 K	1120		

CPU Usage: 10.77% Commit Charge: 80.55% Processes: 206

Process monitor: megmutatja a futó folyamatok operációit, ösvényeit és eredményüket.

Autoruns: megmutatja a windows alkotóelemeit amelyek a bootoláskor indulnak el.

Logonsessions: megmutatja a nemrég bejelentkezett felhasználókat

```
Administrator: Parancssor
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
User name: WORKGROUP\LAPTOP-KIEMLIH05
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: S-1-5-18
Logon time: 2021. 02. 18. 8:54:10
Logon server:
DNS Domain:
UPN:

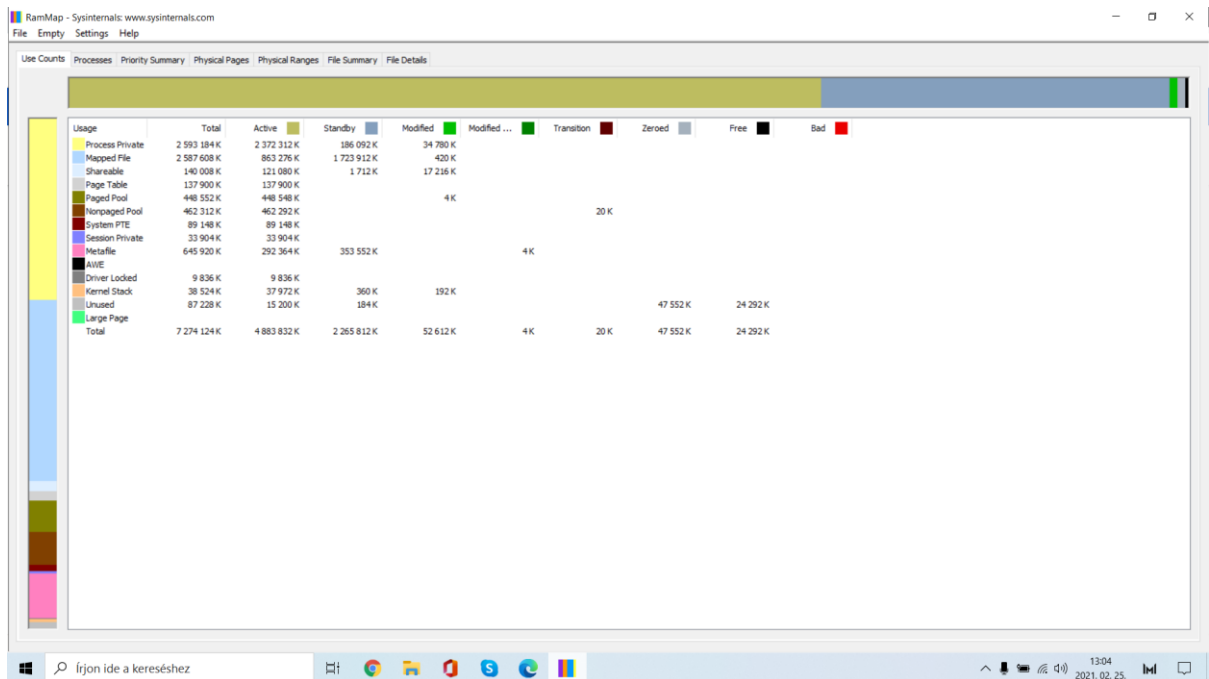
[1] Logon session 00000000:0000d113:
User name:
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: (none)
Logon time: 2021. 02. 18. 8:54:10
Logon server:
DNS Domain:
UPN:

[2] Logon session 00000000:0000d53f:
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. 18. 8:54:10
Logon server:
DNS Domain:
UPN:

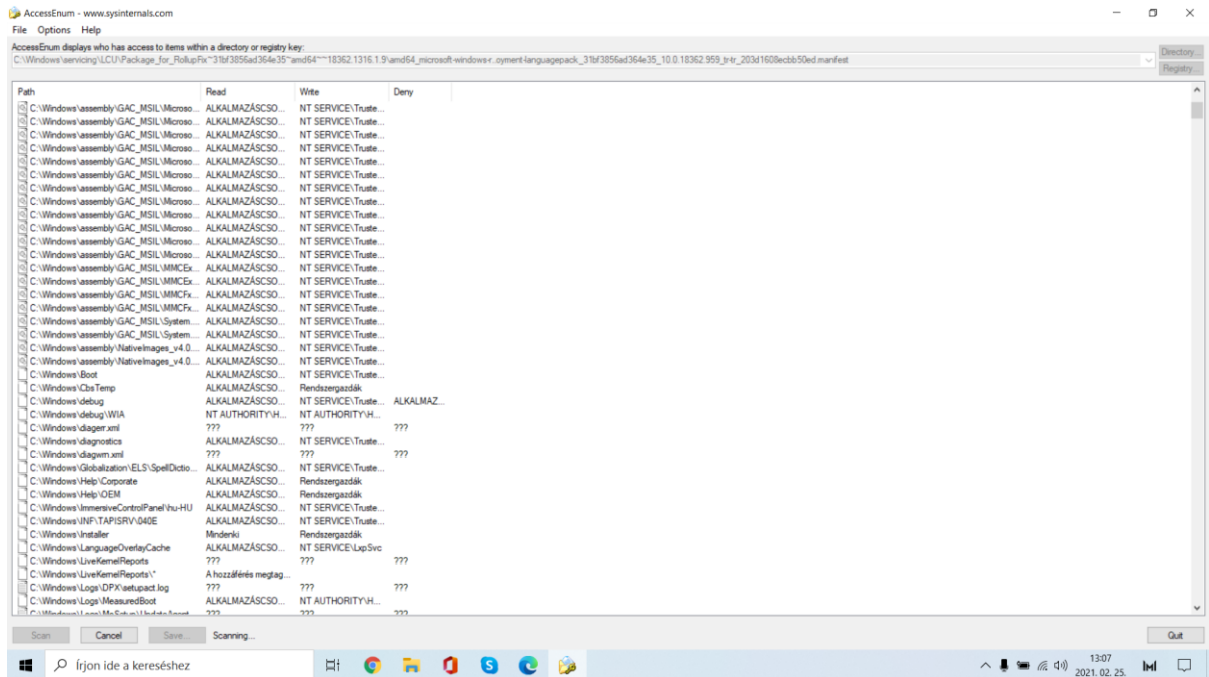
[3] Logon session 00000000:0000d55e:
User name: Font Driver Host\UMFD-1
Auth package: Negotiate
Logon type: Interactive
Session: 1
Sid: S-1-5-96-0-1
Logon time: 2021. 02. 18. 8:54:10
Logon server:
DNS Domain:
UPN:

[4] Logon session 00000000:000003e5:
User name: NT AUTHORITY\SYSTEM SZOLGALTATAS
```

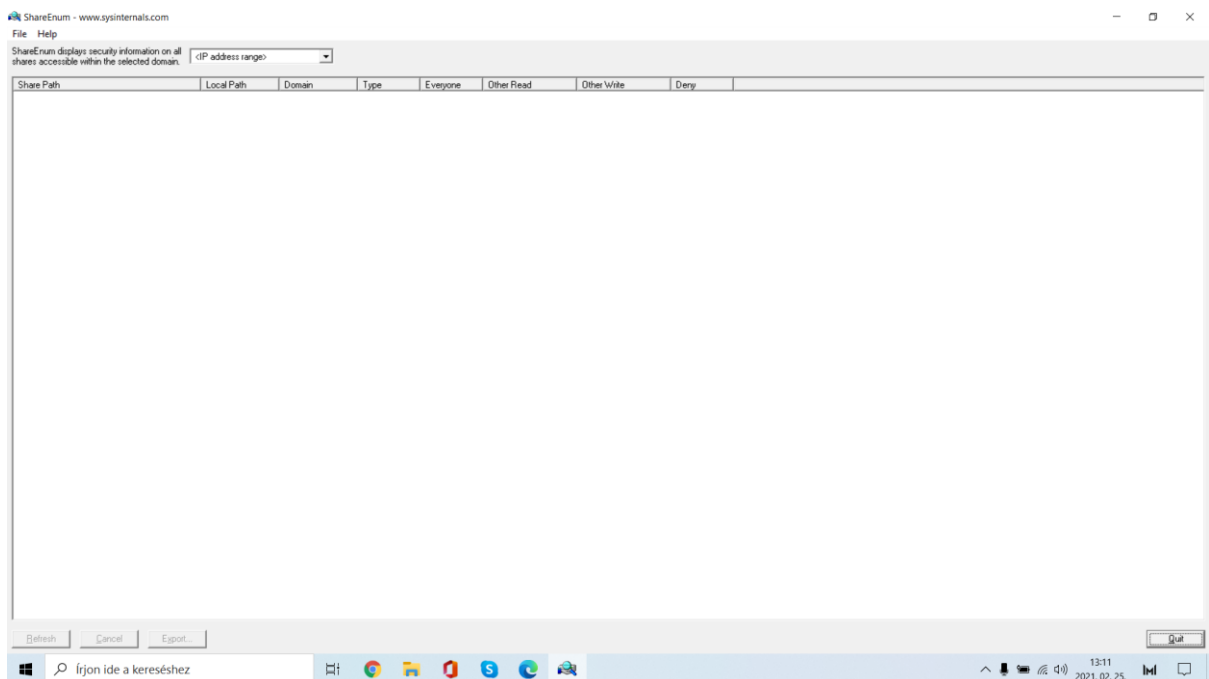
RamMap: részletesen megmutatja a ramhasználatot.



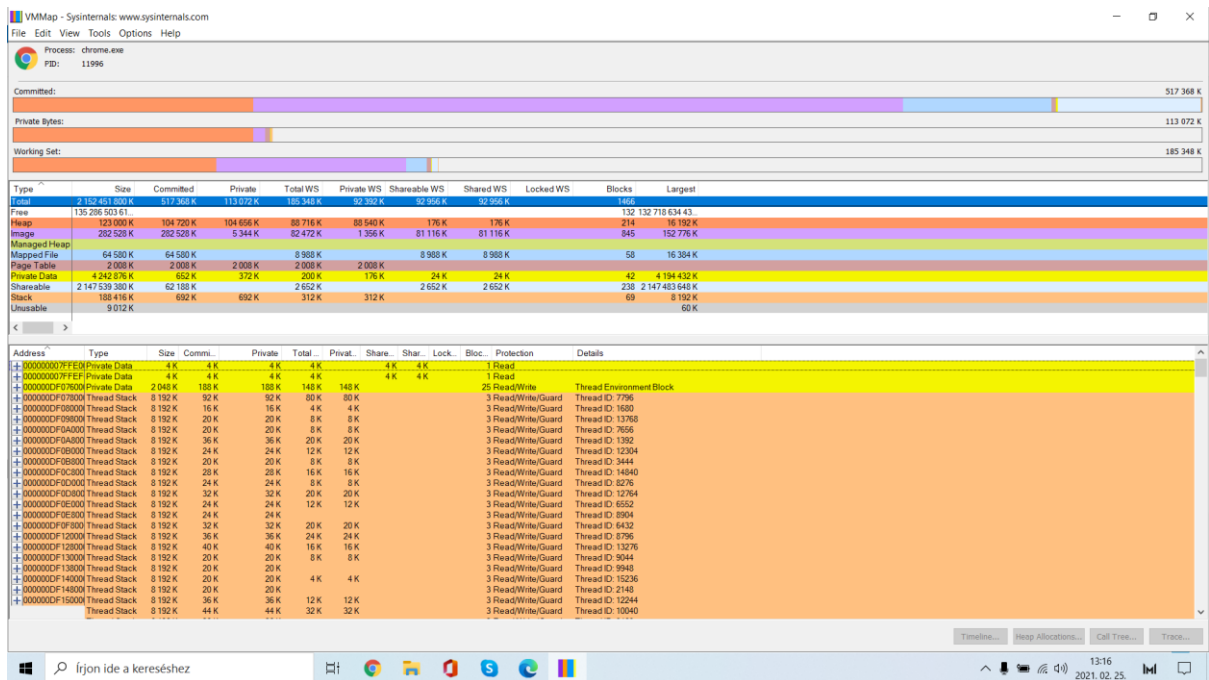
AccesEnum: megmutatja kinek van hozzáférése az adott mappákhoz, fájlokhoz, regiszter kulcsokhoz.



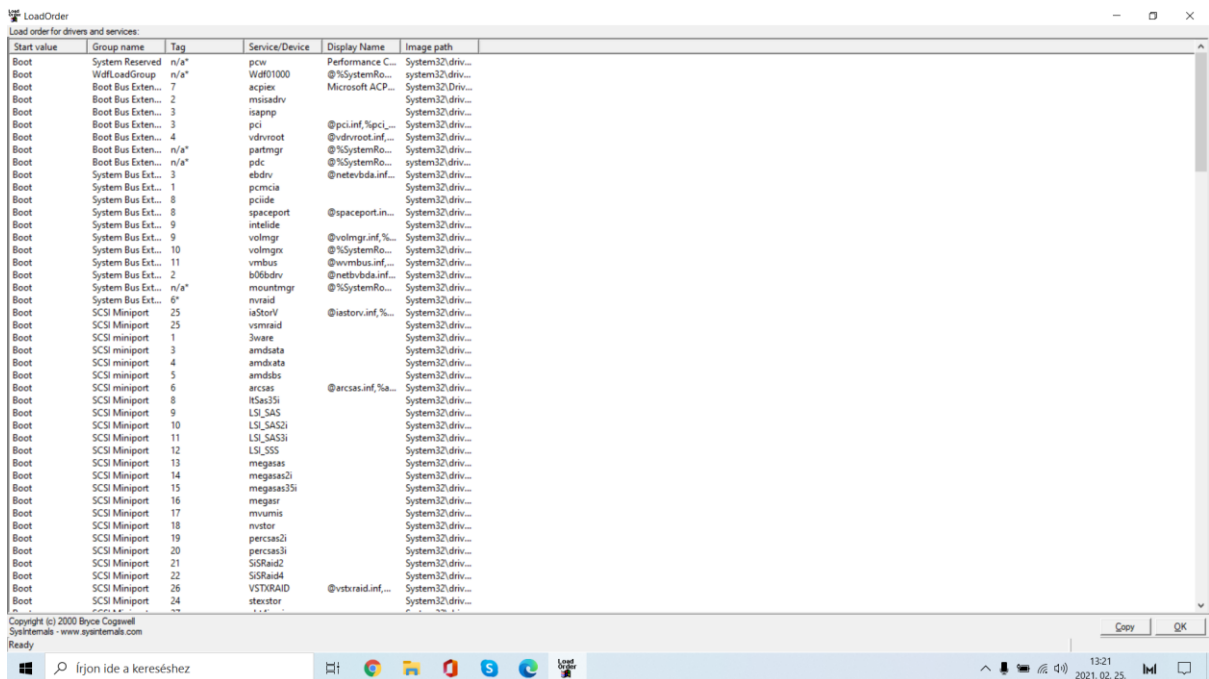
ShareEnum: megmutatja a fájlmegosztásokat a hálózaton és megmutatja azok biztonsági beállításait.



VMMap: részletes jellemzést ad egy processz memóriahasználatáról.



LoadOrder: megmutatja milyen sorrendben töltenek be az eszközök.



Accesschk: megmutatja az egyes felhasználók vagy csoportok hozzáférési jogosultságait

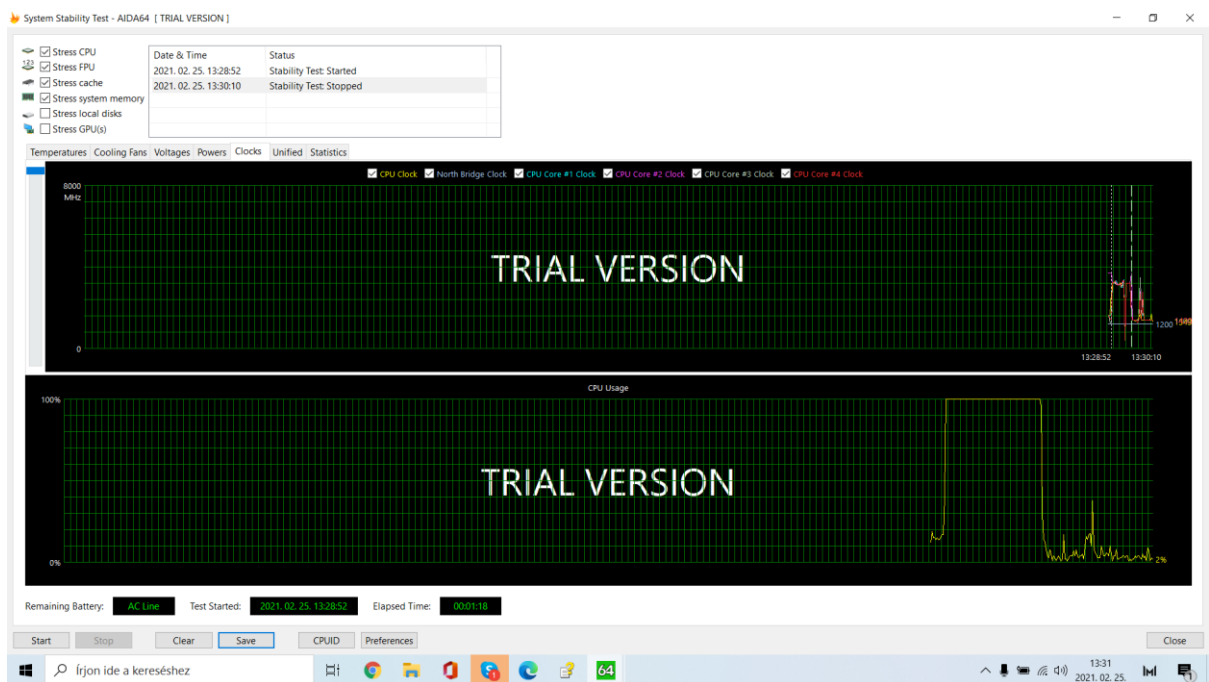

```
Administrator: Parancssor

Accesschk v6.13 - Reports effective permissions for securable objects
Copyright © 2006-2020 Mark Russinovich
sysinternals - www.sysinternals.com

usage: accesschk [-s][-e][-u][-r][-w][-n][-v][-f <accounts>,...][[-a][[-k][[-m][[-p [-f] [-t]]][[-h][-o [-t <object type>]][-c][[-d]] [[[-l[-L] [-i]]][username]]] <file, directory, event log, registry key, process,
service, object>]
-a Name is a Windows account right. Specify '*' as the name to show all
  rights assigned to a user. Note that when you specify a specific
  right, only groups and accounts directly assigned the right are
  displayed.
-c Name is a Windows Service e.g. sdparm. Specify '*' as the
  name to show all services and 'scmanager' to check the security
  of the Service Control Manager.
-d Only process directories or top level key.
-e Only show explicitly set Integrity Levels (Windows Vista and
  higher only).
-f If following -p, shows full process token information including
  groups and privileges. Otherwise is a list of comma-separated
  accounts to filter from the output.
-h Name is a file or printer share. Specify '*' as the name to show
  all shares.
-i Ignore objects with only inherited ACEs when dumping full access
  control lists.
-k Name is a Registry key e.g. hklm\software
-l Show full security descriptor. Add -i to ignore inherited ACEs.
  Specify upper-case l to have the output format as SDOL.
-m Name is an event log (specify '*' as the name to show all event logs.
-n Show only objects that have no access.
-o Name is an object in the Object Manager namespace (default is root).
  To view the contents of a directory, specify the name with a trailing
  backslash or add -s. Add -t and an object type (e.g. section) to
  see only objects of a specific type.
-p Name is a process name or PID e.g. cmd.exe (specify '*' as the
  name to show all processes). Add -f to show full process
  token information including groups and privileges. Add -t to show
  threads.
-nobanner Do not display the startup banner and copyright message.
-r Show only objects that have read access.
-s Recurse.
-t Object type filter e.g. "section"
-u Suppress errors.
-v Verbose (includes Windows Vista Integrity Level).
-w Show only objects that have write access.

If you specify a user or group name and path Accesschk will report the
effective permissions for that account; otherwise it will show the effective
access for accounts referenced in the security descriptor.
```

AIDA64:



CPU-Z:

The screenshot shows a Windows 10 desktop environment. On the left is the File Explorer window showing the 'Képek' (Pictures) folder. In the center is the CPU-Z application window, displaying the 'CPU' tab. The CPU is identified as an AMD Ryzen 5 Mobile 3500U. To the right, a web browser window is open, displaying a document titled '3A. Gyak.pdf'. The document contains instructions for using Sysinternals Suite and CPU-Z. A small window with a blue circle and the letters 'SL' is also visible in the background.

CPU-Z Ver. 1.95.0.x64

CPU	
Name	AMD Ryzen 5 Mobile 3500U
Code Name	Picasso
Package	Socket FFS
Technology	12 nm
Core VID	0.800 V
Specification	
Family	F
Model	8
Stepping	1
Ext. Family	17
Ext. Model	18
Revision	B1
Instructions	MMX(+), SSE, SSE2, SSE3, SSE4.1, SSE4.2, SSE4A, x86-64, AMD-V, AES, AVX, AVX2, FMA3, SHA
Clocks (Core #0)	
Core Speed	1334.79 MHz
Multiplier	x 13.38
Bus Speed	99.80 MHz
Cache	
L1 Data	4 x 32 KiBytes 8-way
L1 Inst.	4 x 64 KiBytes 4-way
Level 2	4 x 512 KiBytes 8-way
Level 3	4 MiBytes 16-way
Selection	
Socket #1	Cores 4 Threads 8

3A. Gyak.pdf

1. Tölts le a Sysinternals Suite csomagot, ha, vagy a hibakeresés...
<https://docs.microsoft.com/hu-hu/sysinternals>
...weboldalon kategóriák...
...k Utilities (Disk2vhd)
...Utilities (TCPView)
...ties (Process Explorer,
...ities (LogonSession)
...Utilities (RAMMap)
...ők közül minden eszköz esetén tölts le, futtassa - és írja le a program
...futtatás eredményét egy-egy mondatl - majd mentse el a megadott
...épennykép).
...lévő eszközön felül válasszon még egy eszközt is.
...ezzen vizsgálatot az *AIDA64 Engineer v5.98.4800 Portable*, CPU-Z,
...kal.
...rogramoknak írja le a szolgáltatásait és a futtatás eredményét egy-egy
...mentse el az alábbi dokumentumba (képernyőkép is).
...*if_segedprog.pdf*
4. Tölts le a következő programot: Dependency Walker
URL: <http://www.dependencywalker.com/>
Feladata: a segédprogram megvizsgálja milyen könyvtárakra, és azon belül milyen
függvényekre hivatkozik egy elindított program.

GPU-Z:

The screenshot shows a Windows 10 desktop environment. On the left is the File Explorer window showing the 'Képek' (Pictures) folder. In the center is the GPU-Z application window, displaying the 'Graphics Card' tab. The GPU is identified as an AMD Radeon(TM) Vega 8 Graphics. To the right, a web browser window is open, displaying a document titled '3A. Gyak.pdf'. The document contains instructions for using Sysinternals Suite and GPU-Z. A small window with a blue circle and the letters 'SL' is also visible in the background.

TechPowerUp GPU-Z 2.37.0

Graphics Card	
Name	AMD Radeon(TM) Vega 8 Graphics
GPU	Picasso
Revision	C2
Technology	12 nm
Die Size	210 mm²
Release Date	Jan 6, 2019
Transistors	4940M
BIOS Version	Unknown
Subvendor	Huawei
Device ID	1002 15D8 - 19E5 3E18
ROPs/TMUs	16 / 32
Bus Interface	PCIe x16.3.0 @ x16.3.0
Shaders	512 Unified
DirectX Support	12 (12_1)
Pixel Fillrate	19.2 GFPixel/s
Texture Fillrate	38.4 GTexel/s
Memory Type	DDR4
Memory Size	1024 MB
Bandwidth	38.4 GB/s
Driver Version	26.20.11030.22001 (Adrenalin 19.10.30.22) DCH / Win10 64
Driver Date	Apr 22, 2020
Digital Signature	WHQL
GPU Clock	1200 MHz
Memory	1200 MHz
Shader	N/A
Default Clock	1200 MHz
Memory	1200 MHz
Shader	N/A
AMD CrossFire	
Computing	<input checked="" type="checkbox"/> OpenCL <input type="checkbox"/> CUDA <input checked="" type="checkbox"/> DirectCompute <input checked="" type="checkbox"/> DirectML
Technologies	<input checked="" type="checkbox"/> Vulkan <input type="checkbox"/> Ray Tracing <input type="checkbox"/> PhysX <input checked="" type="checkbox"/> OpenGL 4.6

3A. Gyak.pdf

1. Tölts le a Sysinternals Suite csomagot, ha, vagy a hibakeresés...
<https://docs.microsoft.com/hu-hu/sysinternals>
...weboldalon kategóriák...
...k Utilities (Disk2vhd)
...Utilities (TCPView)
...ties (Process Explorer,
...ities (LogonSession)
...Utilities (RAMMap)
...ők közül minden eszköz esetén tölts le, futtassa - és írja le a program
...futtatás eredményét egy-egy mondatl - majd mentse el a megadott
...épennykép).
...lévő eszközön felül válasszon még egy eszközt is.
...ezzen vizsgálatot az *AIDA64 Engineer v5.98.4800 Portable*, CPU-Z,
...kal.
...rogramoknak írja le a szolgáltatásait és a futtatás eredményét egy-egy
...mentse el az alábbi dokumentumba (képernyőkép is).
...*if_segedprog.pdf*
4. Tölts le a következő programot: Dependency Walker
URL: <http://www.dependencywalker.com/>
Feladata: a segédprogram megvizsgálja milyen könyvtárakra, és azon belül milyen
függvényekre hivatkozik egy elindított program.