

# Segédprogramok

- a) Disk2vhd: Felsorolja a jelenlévő köteteket a rendszerben. Megőrzi a partíciós információkat de csak az adat tartalmát másolja át a köteteknek. Egy virtuális merevlemez lehetne létrehozni a kötetekből.

**Disk2vhd v2.01**  
Copyright © 2009-2014 Mark Russinovich  
[Sysinternals - www.sysinternals.com](http://www.sysinternals.com)

☒ Use Vhdx  
☒ Use Volume Shadow Copy

VHD File name:  
F:\WIN-KCUGJTGPH75.vhdx

Volumes to include:

Volume	Label	Size	Free	Space Required
<input checked="" type="checkbox"/> \\?\Volume{355b4de5-...	[No Label]	96.00 MB	69.58 MB	32.01 MB
<input type="checkbox"/> C:\	[No Label]	232.77 GB	73.17 GB	144.16 GB
<input type="checkbox"/> D:\	game	200.00 GB	74.32 GB	125.75 GB
<input type="checkbox"/> E:\	adat	731.51 GB	274.77 GB	454.33 GB
<input type="checkbox"/> F:\	13	298.09 GB	233.00 GB	62.50 GB

Disk export to VHD completed successfully.

[Help](#) [Create](#) [Cancel](#) [Close](#)

b) TCPView: Listázza a jelenlegi TCP és UDP végpontokat beleértve a folyamatok nevét címét és a csatlakozás állapotát.

TCPView - Sysinternals: www.sysinternals.com							
File Options Process View Help							
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
[System Proc...	0	TCP	win-kcugitgph75.L...	62328	server-52-85-121-...	https	TIME_WAIT
[System Proc...	0	TCP	WIN-KCUGJTGP...	62588	localhost	1120	TIME_WAIT
[System Proc...	0	TCP	WIN-KCUGJTGP...	1120	localhost	62696	TIME_WAIT
[System Proc...	0	TCP	WIN-KCUGJTGP...	62613	localhost	1120	TIME_WAIT
[System Proc...	0	TCP	WIN-KCUGJTGP...	1120	localhost	62631	TIME_WAIT
[System Proc...	0	TCP	win-kcugitgph75.L...	62565	ec2-18-158-45-21...	https	TIME_WAIT
[System Proc...	0	TCP	WIN-KCUGJTGP...	62629	localhost	1120	TIME_WAIT
[System Proc...	0	TCP	WIN-KCUGJTGP...	1120	localhost	1120	TIME_WAIT
[System Proc...	0	TCP	win-kcugitgph75.L...	62393	muc11s01-in-f10.1...	https	TIME_WAIT
[System Proc...	0	TCP	win-kcugitgph75.L...	62402	bud02s27-in-f3.1e...	https	TIME_WAIT
[System Proc...	0	TCP	WIN-KCUGJTGP...	1120	localhost	62657	TIME_WAIT
[System Proc...	0	TCP	WIN-KCUGJTGP...	62691	localhost	1120	TIME_WAIT
[System Proc...	0	TCP	win-kcugitgph75.L...	62675	111-243-155-205...	25392	TIME_WAIT
Agent.exe	10984	TCP	WIN-KCUGJTGP...	1120	WIN-KCUGJTGP...	0	LISTENING
Agent.exe	10984	TCP	win-kcugitgph75.L...	62455	24.105.29.76	https	CLOSE_WAIT
Avira Service...	4816	UDP	WIN-KCUGJTGP...	62852	*	*	
Avira Softwar...	4916	TCP	win-kcugitgph75.L...	62592	ec2-35-156-163-2...	https	CLOSE_WAIT
Avira Systray...	10844	UDP	WIN-KCUGJTGP...	59489	*	*	
Battle.net.exe	3108	TCP	WIN-KCUGJTGP...	22885	WIN-KCUGJTGP...	0	LISTENING
Battle.net.exe	3108	TCP	WIN-KCUGJTGP...	55714	localhost	55715	ESTABLISHED
Battle.net.exe	3108	TCP	WIN-KCUGJTGP...	55715	localhost	55714	ESTABLISHED
Battle.net.exe	3108	TCP	win-kcugitgph75.L...	62400	s3-us-west-2-r-w.a...	https	CLOSE_WAIT
Battle.net.exe	3108	TCP	win-kcugitgph75.L...	63491	37.244.54.10	1119	ESTABLISHED
Battle.net.exe	3108	TCP	win-kcugitgph75.L...	65198	cds133.fra.llnwd.net	1119	CLOSE_WAIT
chatterino.exe	12324	TCP	win-kcugitgph75.L...	52824	ec2-44-226-36-14...	https	ESTABLISHED
chatterino.exe	12324	TCP	win-kcugitgph75.L...	52825	ec2-44-226-36-14...	https	ESTABLISHED
chatterino.exe	12324	TCP	win-kcugitgph75.L...	55543	199.232.138.214	https	ESTABLISHED
chatterino.exe	12324	TCP	win-kcugitgph75.L...	62664	ec2-54-184-232-1...	https	ESTABLISHED
chrome.exe	9528	TCP	win-kcugitgph75.L...	52121	ec2-18-157-118-5...	https	ESTABLISHED
chrome.exe	9528	TCP	WIN-KCUGJTGP...	52575	localhost	49678	ESTABLISHED
chrome.exe	9528	TCP	win-kcugitgph75.L...	52637	142.250.102.188	5228	ESTABLISHED
chrome.exe	9528	TCP	win-kcugitgph75.L...	57158	edge-star-shv-01-o...	https	ESTABLISHED
chrome.exe	9528	TCP	win-kcugitgph75.L...	60354	bud02s28-in-f14.1...	https	ESTABLISHED
chrome.exe	9528	TCP	win-kcugitgph75.L...	61768	151.101.1.140	https	ESTABLISHED
chrome.exe	9528	TCP	win-kcugitgph75.L...	62235	ec2-54-235-160-2...	https	ESTABLISHED
chrome.exe	9528	TCP	win-kcugitgph75.L...	62236	ec2-54-235-160-2...	https	ESTABLISHED
chrome.exe	9528	TCP	win-kcugitgph75.L...	62464	11.224.186.35.bc...	https	ESTABLISHED
chrome.exe	9528	TCP	win-kcugitgph75.L...	62799	45.224.186.35.bc...	https	ESTABLISHED
chrome.exe	9528	TCP	win-kcugitgph75.L...	64717	ec2-35-157-231-4...	https	ESTABLISHED
chrome.exe	16904	UDP	WIN-KCUGJTGP...	5353	*	*	
chrome.exe	16904	UDP	WIN-KCUGJTGP...	5353	*	*	
chrome.exe	16904	UDP	WIN-KCUGJTGP...	5353	*	*	
chrome.exe	16904	UDP	WIN-KCUGJTGP...	5353	*	*	
Endpoints: 229		Established: 59	Listening: 30	Time Wait: 55	Close Wait: 10		

c) Autoruns: Futó folyamatokat lehet vele ellenőrizni

Autoruns [WIN-KCUGJTGPH79]Gabe - Sysinternals: www.sysinternals.com

File Entry Options User Help

KnownDLLs Logon Explorer Internet Explorer Scheduled Tasks Services LSA Providers Network Providers WMI Office

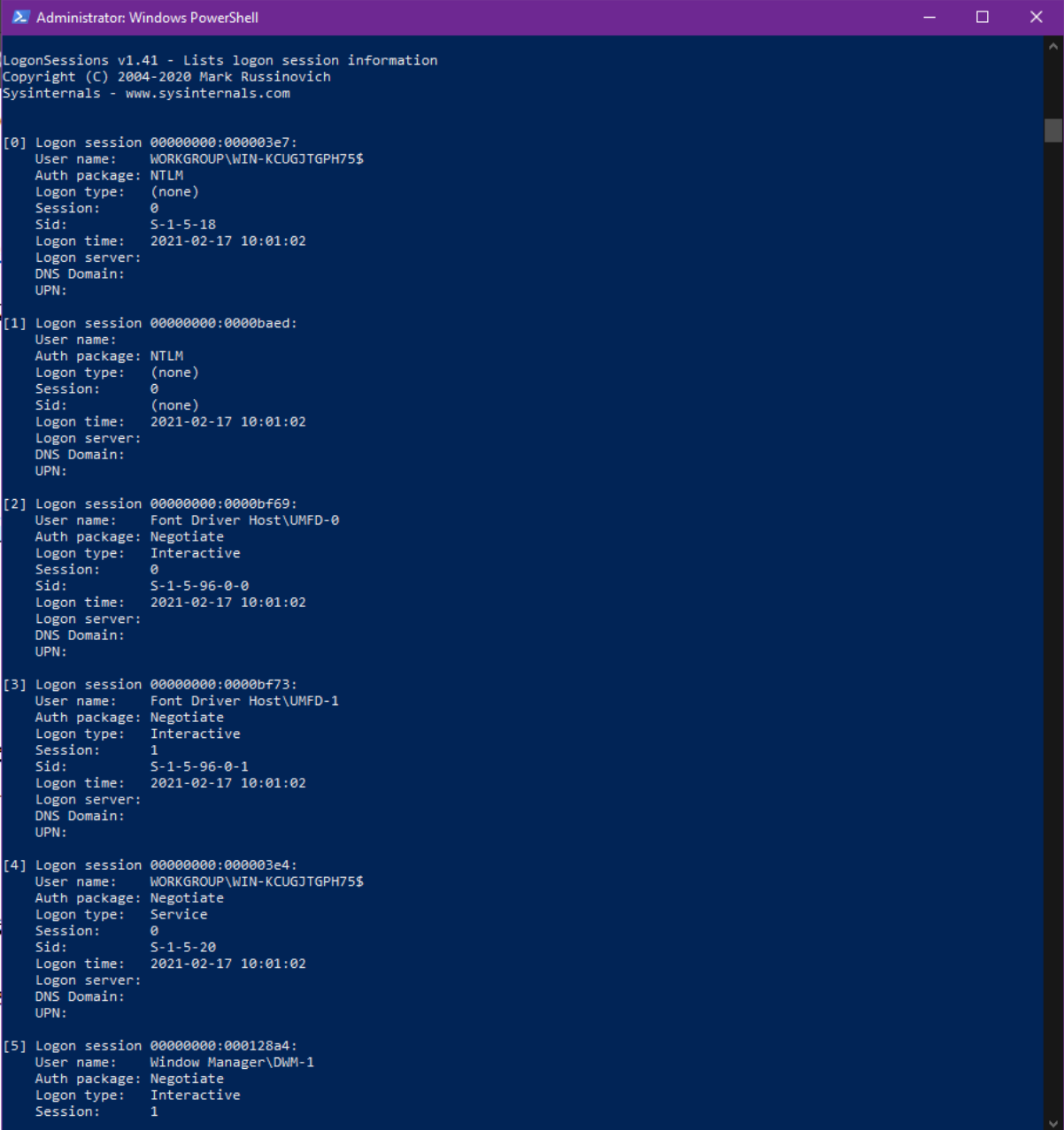
Everything Explorer Internet Explorer Scheduled Tasks Services Drivers Codex Boot Execute Image Hijacks AppInit

Autorun Entry	Description	Publisher	Image Path	Timestamp	Virus Total
<input checked="" type="checkbox"/> HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				2019-12-07 10:15	
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	2037-01-26 16:29	
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2021-02-23 11:30	
<input checked="" type="checkbox"/> Avira SystrayStartTrigger	Avira	(Verified) Avira Operations GmbH & C...	c:\program files (x86)\avira\launcher...	2020-11-20 16:16	
<input checked="" type="checkbox"/> Sound Blaster Z-Series ...	Sound Blaster Control Panel	(Not Verified) Creative Technology Ltd	c:\program files (x86)\creative\sound...	2014-11-24 10:53	
<input checked="" type="checkbox"/> TeamsMachineInstaller	Microsoft Teams	(Verified) Microsoft Corporation	c:\program files (x86)\Teams installer\...	2020-08-28 19:30	
<input checked="" type="checkbox"/> UpdReg	Creative UpdReg	(Not Verified) Creative Technology Ltd.	c:\windows\updreg.exe	2000-05-11 03:01	
<input checked="" type="checkbox"/> HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021-02-23 11:30	
<input checked="" type="checkbox"/> com.squirrel.Teams.Teams	Microsoft Teams	(Verified) Microsoft 3rd Party Applicati...	c:\users\administrator\appdata\local...	2020-10-02 13:48	
<input checked="" type="checkbox"/> Discord	Update	(Verified) Discord Inc.	c:\users\administrator\appdata\local...	2020-06-01 21:58	
<input checked="" type="checkbox"/> IDMMan	Internet Download Manager (IDM)	(Not Verified) Tonec Inc.	c:\program files (x86)\internet downlo...	2020-10-23 17:10	
<input checked="" type="checkbox"/> Skype for Desktop	Skype	(Verified) Skype Software Sarl	c:\program files (x86)\microsoft\skyp...	2020-04-01 23:51	
<input checked="" type="checkbox"/> Steam	Steam Client Bootstrapper	(Verified) Valve	c:\program files (x86)\steam\steam.exe	2021-02-13 00:23	
<input checked="" type="checkbox"/> TSMApplication			c:\program files (x86)\tradeskillmaster...	2014-12-27 00:08	
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2020-12-26 10:30	
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	(Verified) Google LLC	c:\program files\google\chrome\appli...	2021-02-13 00:08	
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	2019-10-25 04:45	
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				2019-12-07 10:54	
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\syswow64\mscories.dll	2019-10-25 09:48	
<input checked="" type="checkbox"/> HKLM\Software\Classes\Protocols\Filter				2021-02-03 00:03	
<input checked="" type="checkbox"/> text/xml	Microsoft Office XML MIME Filter	(Verified) Microsoft Corporation	c:\program files\microsoft office\root\...	2020-12-28 23:39	
<input checked="" type="checkbox"/> HKLM\Software\Classes\Protocols\Handler				2021-02-03 00:03	
<input checked="" type="checkbox"/> mso-minsb-roaming.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft office\root\...	2020-12-28 23:33	
<input checked="" type="checkbox"/> mso-minsb.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft office\root\...	2020-12-28 23:33	
<input checked="" type="checkbox"/> oaf-roaming.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft office\root\...	2020-12-28 23:33	
<input checked="" type="checkbox"/> oaf.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft office\root\...	2020-12-28 23:33	
<input checked="" type="checkbox"/> HKLM\Software\Classes\ShellEx\ContextMenuHandlers				2021-02-03 22:14	
<input checked="" type="checkbox"/> 7-Zip	7-Zip Shell Extension	(Not Verified) Igor Pavlov	c:\program files\7-zip\7-zip.dll	2019-02-21 17:00	
<input checked="" type="checkbox"/> EPP			File not found: C:\Program Files\Win...		
<input checked="" type="checkbox"/> Shell Extension for Malw...	AntiVirus context menu	(Verified) Avira Operations GmbH & C...	c:\program files (x86)\avira\antivirus\...	2020-09-23 13:37	
<input checked="" type="checkbox"/> SystemSpeedupFilesMenu	Avira SystemSpeedup.UI.ShellExtens...	(Verified) Avira Operations GmbH & C...	c:\program files (x86)\avira\system s...	2021-02-03 08:32	
<input checked="" type="checkbox"/> HKLM\Software\Classes\Drive\ShellEx\ContextMenuHandlers				2019-12-07 10:54	

skype.exe Size: 88,883 K  
 Skype Time: 2020-04-01 23:51  
 Skype Technologies S.A. Version: 8.68.0.96  
 C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe

Ready. Signed Windows Entries Hidden.

d) Logon sessions:

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window has a dark blue background with white text. It displays the output of the "LogonSessions" command, which lists logon session information. The output includes the session ID, user name, authentication package, logon type, session number, SID, logon time, logon server, DNS domain, and UPN for six different sessions. The sessions are indexed from [0] to [5].

```
LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
    User name: WORKGROUP\WIN-KCUGJTGPH75$
    Auth package: NTLM
    Logon type: (none)
    Session: 0
    Sid: S-1-5-18
    Logon time: 2021-02-17 10:01:02
    Logon server:
    DNS Domain:
    UPN:

[1] Logon session 00000000:0000baed:
    User name:
    Auth package: NTLM
    Logon type: (none)
    Session: 0
    Sid: (none)
    Logon time: 2021-02-17 10:01:02
    Logon server:
    DNS Domain:
    UPN:

[2] Logon session 00000000:0000bf69:
    User name: Font Driver Host\UMFD-0
    Auth package: Negotiate
    Logon type: Interactive
    Session: 0
    Sid: S-1-5-96-0-0
    Logon time: 2021-02-17 10:01:02
    Logon server:
    DNS Domain:
    UPN:

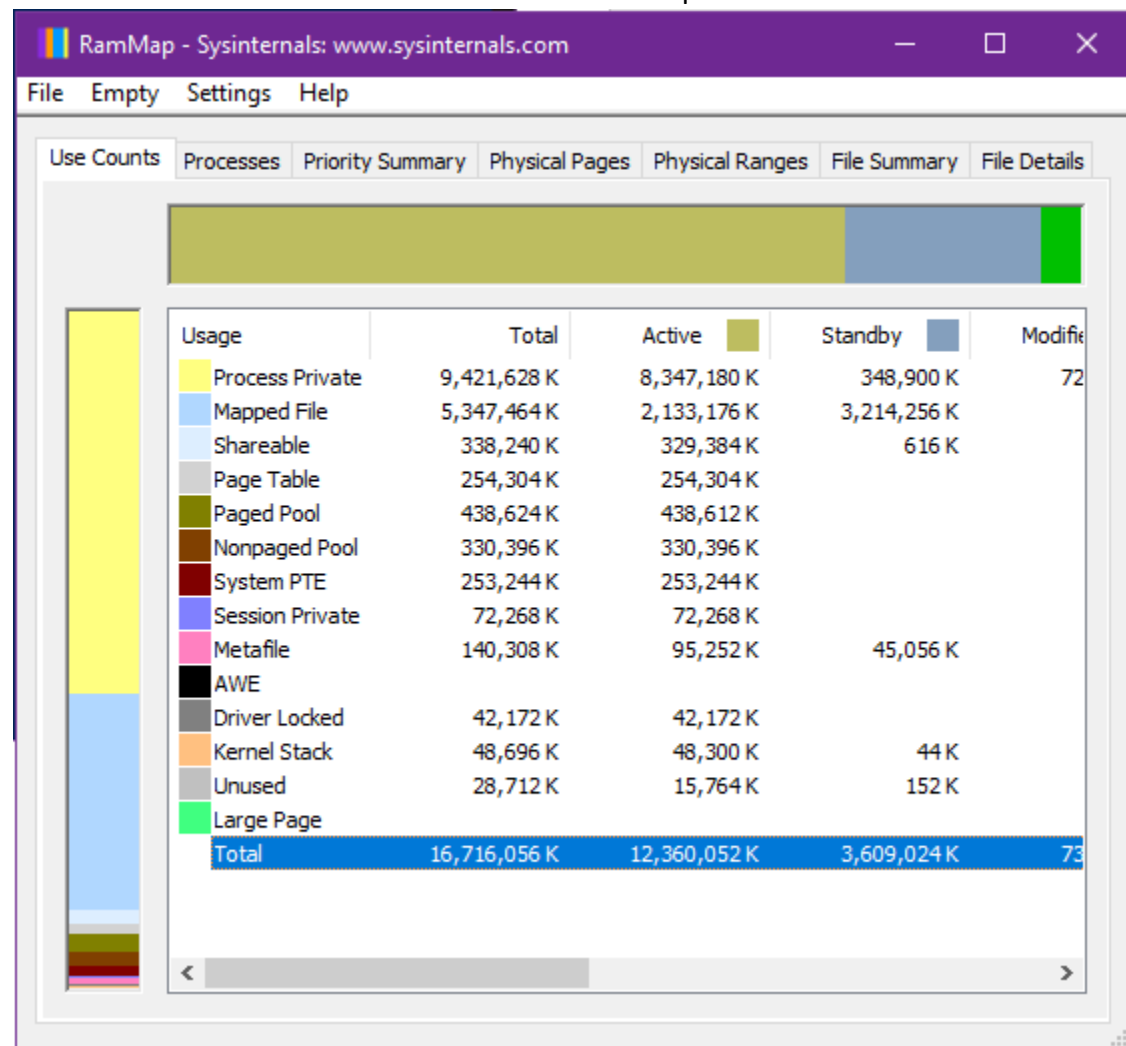
[3] Logon session 00000000:0000bf73:
    User name: Font Driver Host\UMFD-1
    Auth package: Negotiate
    Logon type: Interactive
    Session: 1
    Sid: S-1-5-96-0-1
    Logon time: 2021-02-17 10:01:02
    Logon server:
    DNS Domain:
    UPN:

[4] Logon session 00000000:000003e4:
    User name: WORKGROUP\WIN-KCUGJTGPH75$
    Auth package: Negotiate
    Logon type: Service
    Session: 0
    Sid: S-1-5-20
    Logon time: 2021-02-17 10:01:02
    Logon server:
    DNS Domain:
    UPN:

[5] Logon session 00000000:000128a4:
    User name: Window Manager\DWM-1
    Auth package: Negotiate
    Logon type: Interactive
    Session: 1
```

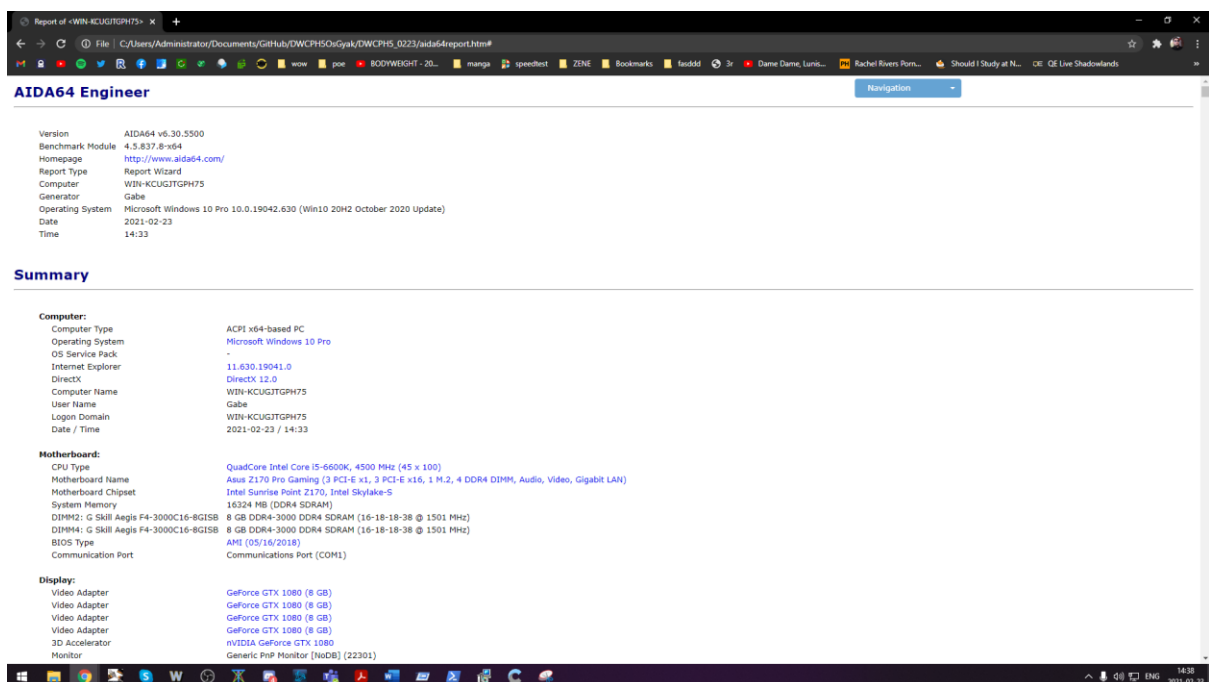
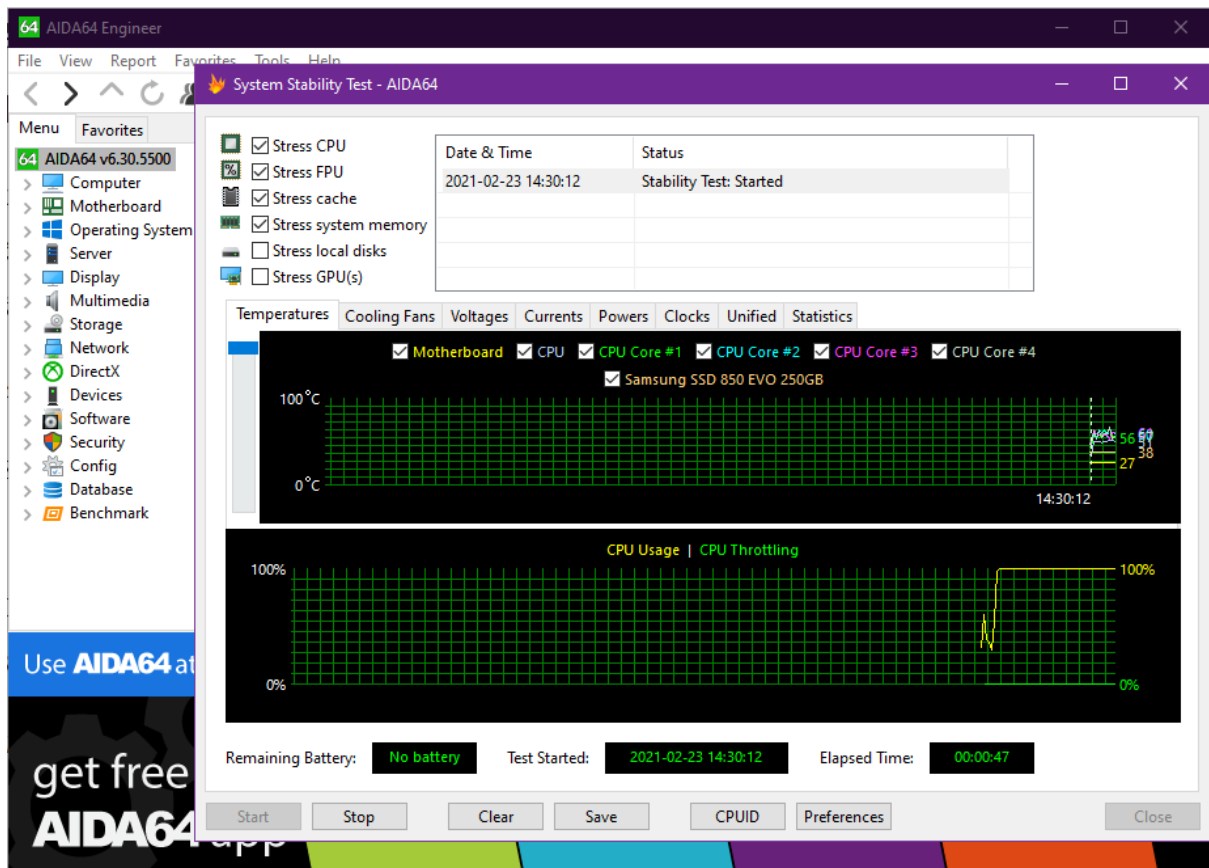
e) RAMMap

A fizikai memória használatát listázza használati alapon.



3)

AIDA64: Információkat szolgáltat a számítógép komponenseiről, tesztelhetjük vele a főbb alkatrészek stabilitását és működését.



CPUZ: A processzor adatait leírja.

The screenshot shows the CPU-Z application window with the following data:

CPU			
<b>Processor</b>			
Name	Intel Core i5 6600K		
Code Name	Skylake	Max TDP	95.0 W
Package	Socket 1151 LGA		
Technology	14 nm	Core Voltage	1.360 V
Specification: Intel® Core™ i5-6600K CPU @ 3.50GHz			
Family	6	Model	E Stepping 3
Ext. Family	6	Ext. Model	5E Revision R0
Instructions	MMX, SSE, SSE2, SSE3, SSSE3, SSE4.1, SSE4.2, EM64T, VT-x, AES, AVX, AVX2, FMA3, TSX		
<b>Clocks (Core #0)</b>			
Core Speed	1800.00 MHz		
Multiplier	x 18.0 ( 8 - 45 )		
Bus Speed	100.00 MHz		
Rated FSB			
<b>Cache</b>			
L1 Data	4 x 32 KBytes	8-way	
L1 Inst.	4 x 32 KBytes	8-way	
Level 2	4 x 256 KBytes	4-way	
Level 3	6 MBytes	12-way	
Selection: Socket #1 Cores: 4 Threads: 4			
CPU-Z Ver. 1.95.0.x64 [Tools] [Validate] [Close]			

The screenshot shows the CPUID website displaying a detailed CPU-Z report. The report includes the following sections:

- Binaries**: CPU-Z version 1.95.0.x64
- Processors**: CPU Groups (1), CPU Group 0 (4 CPUs, mask=0xf), Number of sockets (1), Number of threads (4)
- APICS**: Socket 0, Core 0 (ID 0) Thread 0 (0), Core 1 (ID 2) Thread 1 (2), Core 2 (ID 4) Thread 2 (4), Core 3 (ID 6) Thread 3 (6)
- Timers**: ACPI timer (3.580 MHz), Perf timer (10.000 MHz), Sys timer (1.000 KHz)
- Processors Information**: Socket 1, ID = 0, Number of cores (4 (max 4)), Number of threads (4 (max 4)), Manufacturer (GenuineIntel), Name (Intel Core i5 6600K), Codename (Skylake), Specification (Intel(R) Core(TM) i5-6600K CPU @ 3.50GHz), Package (platform ID) (Socket 1151 LGA (0x1))

GPUZ grafikus kártya tulajdonságait írja le

TechPowerUp GPU-Z 2.37.0


Graphics Card | Sensors | Advanced | Validation

Name: NVIDIA GeForce GTX 1080 [Lookup](#)

GPU: GP104 Revision: A1

Technology: 16 nm Die Size: 314 mm<sup>2</sup>

Release Date: May 17, 2016 Transistors: 7200M

BIOS Version: 86.04.17.00.1C  ☒ UEFI

Subvendor: ASUS Device ID: 10DE 1B80 - 1043 8592

ROPs/TMUs: 64 / 160 Bus Interface: PCIe x16 3.0 @ x16 1.1 ?

Shaders: 2560 Unified DirectX Support: 12 (12\_1)

Pixel Fillrate: 111.0 GPixel/s Texture Fillrate: 277.4 GTexel/s

Memory Type: GDDR5X (Micron) Bus Width: 256 bit

Memory Size: 8192 MB Bandwidth: 320.3 GB/s

Driver Version: 27.21.14.6089 (NVIDIA 460.89) DCH / Win10 64

Driver Date: Dec 11, 2020 Digital Signature: WHQL


GPU Clock: 1607 MHz Memory: 1251 MHz Boost: 1734 MHz

Default Clock: 1607 MHz Memory: 1251 MHz Boost: 1734 MHz

NVIDIA SLI: Disabled

Computing: ☒ OpenCL ☒ CUDA ☒ DirectCompute ☒ DirectML

Technologies: ☒ Vulkan ☒ Ray Tracing ☒ PhysX ☒ OpenGL 4.6

NVIDIA GeForce GTX 1080  [Close](#)