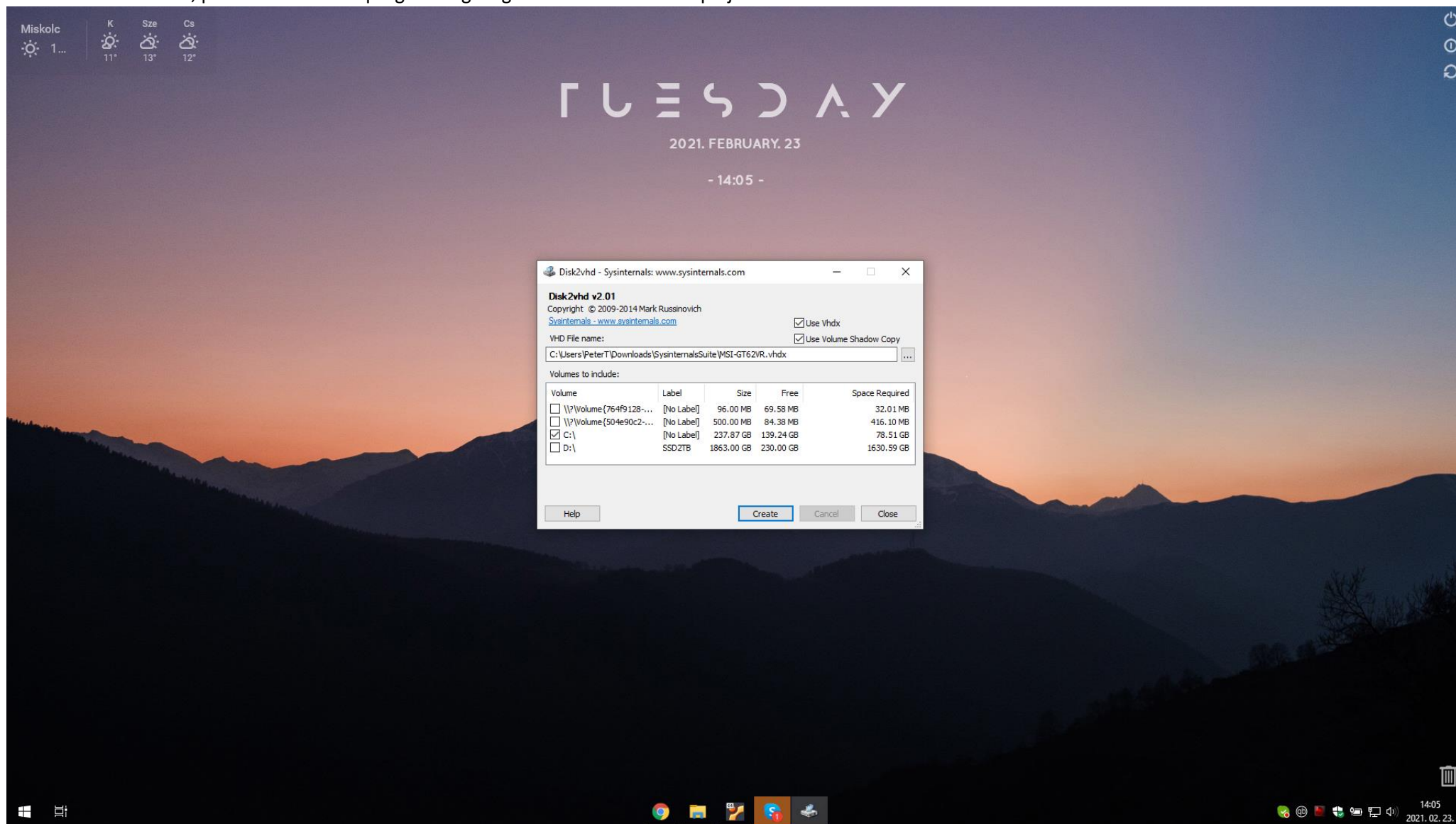


Disk2vhd: Lemezekről, partíciókról lehet a program segítségével virtuális lemezképfájlt készíteni.



Miskolc
☀️ 1 ...
K
☀️ 11°
Size
☁️ 13°
Cs
☁️ 12°

T U E S D A Y

2021. FEBRUARY. 23

- 14:06 -

Disk2vhd - Sysinternals: www.sysinternals.com

Disk2vhd v2.01
Copyright © 2009-2014 Mark Russinovich
www.sysinternals.com

☒ Use Vhdx
☒ Use Volume Shadow Copy

VHD File name:
C:\Users\PeterT\Downloads\SysinternalsSuite\MSI-GT62VR.vhdx

Volumes to include:

Volume	Label	Size	Free	Space Required
<input type="checkbox"/> \\?\Volume{764f9128-...	[No Label]	96.00 MB	69.58 MB	32.01 MB
<input type="checkbox"/> \\?\Volume{504e90c2-...	[No Label]	500.00 MB	84.38 MB	416.10 MB
<input checked="" type="checkbox"/> C:\	[No Label]	237.87 GB	139.24 GB	78.51 GB
<input type="checkbox"/> D:\	SSD2TB	1863.00 GB	230.00 GB	1630.59 GB

Copying volume C: on disk 0... 2021. 02. 23. 14:12:06

Help Create Cancel Close



14:06
2021. 02. 23.

TCPView: TCP és UDP adatcsomagokat lehet monitorozni vele.

Miskolc K Size Cs
11° 13° 12°

TUESDAY
2021. FEBRUARY. 23

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
chrome.exe	7948	UDP	MSI-GT62VR	5353	*	*				
chrome.exe	8152	UDP	MSI-GT62VR	5353	*	*				
chrome.exe	8152	UDP	MSI-GT62VR	5353	*	*				
chrome.exe	7948	UDP	MSI-GT62VR	5353	*	*				
chrome.exe	7948	UDP	MSI-GT62VR	5353	*	*				
chrome.exe	8152	UDP	MSI-GT62VR	5353	*	*				
chrome.exe	8152	UDPv6	[0.0.0.0.0.0.0]	5353	*	*				
chrome.exe	8152	UDPv6	[0.0.0.0.0.0.0]	5353	*	*				
chrome.exe	7948	UDPv6	[0.0.0.0.0.0.0]	5353	*	*				
chrome.exe	7948	UDPv6	[0.0.0.0.0.0.0]	5353	*	*				
chrome.exe	7948	UDP	MSI-GT62VR	58470	*	*				
dashHost.exe	2824	UDP	MSI-GT62VR	ws-discovery	*	*		9	4 666	12
dashHost.exe	2824	UDP	MSI-GT62VR	ws-discovery	*	*				
dashHost.exe	2824	UDP	MSI-GT62VR	62688	*	*				
dashHost.exe	2824	UDPv6	[0.0.0.0.0.0.0]	3702	*	*				
dashHost.exe	2824	UDPv6	[0.0.0.0.0.0.0]	3702	*	*				
dashHost.exe	2824	UDPv6	[0.0.0.0.0.0.0]	62689	*	*				
jhi_service.exe	4364	TCPv6	[0.0.0.0.0.0.1]	49669	[0.0.0.0.0.0.0]	0	LISTENING			
KNDBWM.exe	4276	UDP	MSI-GT62VR	12700	*	*				
lsass.exe	956	TCP	MSI-GT62VR	49664	MSI-GT62VR	0	LISTENING			
lsass.exe	956	TCPv6	[0.0.0.0.0.0.0]	49664	[0.0.0.0.0.0.0]	0	LISTENING			
nvcontainer.exe	3732	TCP	MSI-GT62VR	63672	localhost	65001	ESTABLISHED			
nvcontainer.exe	3732	TCP	MSI-GT62VR	65001	MSI-GT62VR	0	LISTENING			
nvcontainer.exe	3732	TCP	MSI-GT62VR	65001	localhost	63672	ESTABLISHED			
nvcontainer.exe	3732	UDP	msi-gt62vr.home	5353	*	*				
nvcontainer.exe	3732	UDP	msi-gt62vr	5353	*	*				
nvcontainer.exe	3732	UDP	MSI-GT62VR	61231	*	*				
nvcontainer.exe	8904	UDP	MSI-GT62VR	62337	*	*				
nvcontainer.exe	3732	UDPv6	[0.0.0.0.0.0.1]	5353	*	*				
nvcontainer.exe	3732	UDPv6	[0.0.0.0.0.0.0]	61232	*	*				
NVIDIA Web ...	1748	TCP	MSI-GT62VR	63687	MSI-GT62VR	0	LISTENING			
NVIDIA Web ...	1748	UDP	MSI-GT62VR	10080	*	*				
qbitorrent.exe	12700	TCP	MSI-GT62VR	25326	MSI-GT62VR	0	LISTENING	39	7 701	41
qbitorrent.exe	12700	TCP	msi-gt62vr	25326	MSI-GT62VR	0	LISTENING			
qbitorrent.exe	12700	TCP	MSI-GT62VR	63730	localhost	63731	ESTABLISHED			
qbitorrent.exe	12700	TCP	MSI-GT62VR	63731	localhost	63730	ESTABLISHED	65	65	65
qbitorrent.exe	12700	UDP	msi-gt62vr.home	ssdp	*	*				22

Endpoints: 179 Established: 37 Listening: 32 Time Wait: 6 Close Wait: 7

14:07
2021. 02. 23.

Process Explorer / Process Monitor: A gépen futó processzeket lehet monitorozni, megfigyelni.

Process Explorer - Sysinternals: www.sysinternals.com [MSI-GT62VR\PeterT]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
dlhost.exe		4 440 K	12 344 K	9092	COM Surrogate	Microsoft Corporation
ShellExperienceHost.exe	Susp...	71 976 K	74 380 K	6804	Windows Shell Experience Host	Microsoft Corporation
Microsoft.Photos.exe	Susp...	100 440 K	14 004 K	14324		
RuntimeBroker.exe		9 920 K	25 600 K	4972	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		6 052 K	23 592 K	8872	Runtime Broker	Microsoft Corporation
Calculator.exe	Susp...	70 940 K	1 844 K	11372		
RuntimeBroker.exe		1 312 K	6 188 K	13676	Runtime Broker	Microsoft Corporation
dlhost.exe		1 996 K	12 884 K	11176	COM Surrogate	Microsoft Corporation
VBoxSVC.exe	< 0.01	7 120 K	19 912 K	2360	VirtualBox Interface	Oracle Corporation
VirtualBoxVM.exe		1 916 K	6 832 K	3376	VirtualBox Virtual Machine	Oracle Corporation
VirtualBoxVM.exe		1 952 K	4 980 K	260	VirtualBox Virtual Machine	Oracle Corporation
VirtualBoxVM.exe	0.11	128 056 K	153 672 K	7348	VirtualBox Virtual Machine	Oracle Corporation
RuntimeBroker.exe		2 196 K	10 552 K	3988	Runtime Broker	Microsoft Corporation
smartscreen.exe		8 340 K	24 364 K	1956	Windows Defender SmartScreen	Microsoft Corporation
WUDFHost.exe	< 0.01	1 468 K	1 880 K	1028		
svchost.exe	0.02	10 464 K	14 072 K	1108	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe	< 0.01	3 128 K	5 320 K	1156	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe		2 564 K	5 268 K	1452	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe		2 172 K	4 536 K	1460	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe		15 432 K	10 060 K	1468	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe		2 376 K	4 752 K	1548	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe	0.02	6 520 K	3 296 K	1632	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe	0.02	3 068 K	4 172 K	1720	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe	< 0.01	2 232 K	2 824 K	1788	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe		2 420 K	4 996 K	1912	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe		5 592 K	9 448 K	1920	Windows-szolgáltatások gazd...	Microsoft Corporation
NVDisplay.Container.exe		6 068 K	10 616 K	1948	NVIDIA Container	NVIDIA Corporation
NVDisplay.Container.exe	< 0.01	32 656 K	40 748 K	2760		
svchost.exe		7 576 K	7 584 K	1980	Windows-szolgáltatások gazd...	Microsoft Corporation
taskhostw.exe		7 648 K	18 112 K	7468	Gazdafolyamat Windows-fela...	Microsoft Corporation
Dragon Center.exe		152 588 K	31 392 K	4452		
taskhostw.exe		5 632 K	16 164 K	6660		
svchost.exe		2 812 K	6 756 K	1832	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe	< 0.01	3 848 K	7 356 K	1096	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe		5 704 K	7 000 K	2060	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe		2 096 K	4 632 K	2068	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe		1 332 K	2 112 K	2076	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe		9 600 K	15 344 K	2224	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe		1 648 K	3 152 K	2272	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe		1 880 K	4 368 K	2352	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe		2 416 K	4 552 K	2424	Windows-szolgáltatások gazd...	Microsoft Corporation
svchost.exe		1 820 K	3 976 K	2432	Windows-szolgáltatások gazd...	Microsoft Corporation

CPU Usage: 19.91% | Commit Charge: 47.60% | Processes: 202 | Physical Usage: 41.77%

T U E S D A Y

2021. FEBRUARY. 23

- 14:08 -

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
14:08:...	svchost.exe	5536	ReadFile	C:\Windows\System32\cdp.dll	SUCCESS	Offset: 4 057 600, ...
14:08:...	MaMpEng.exe	3780	CreateFile	C:\Users\Peter\AppData\Local\Temp...	SUCCESS	Desired Access: R...
14:08:...	MaMpEng.exe	3780	QueryAllInforma...	C:\Users\Peter\AppData\Local\Temp...	SUCCESS	VolumeCreationTim...
14:08:...	MaMpEng.exe	3780	QueryAllInforma...	C:\Users\Peter\AppData\Local\Temp...	BUFFER OVERFL...	CreationTime: 202...
14:08:...	MaMpEng.exe	3780	QueryAllInforma...	C:\Users\Peter\AppData\Local\Temp...	SUCCESS	VolumeCreationTim...
14:08:...	MaMpEng.exe	3780	QueryAllInforma...	C:\Users\Peter\AppData\Local\Temp...	BUFFER OVERFL...	CreationTime: 202...
14:08:...	svchost.exe	5536	ReadFile	C:\Windows\System32\cdp.dll	SUCCESS	Offset: 4 041 216, ...
14:08:...	MaMpEng.exe	3780	FileSystemControl	C:\Users\Peter\AppData\Local\Temp...	SUCCESS	Control: FSCTL_R...
14:08:...	MaMpEng.exe	3780	QueryIdInformat...	C:\Users\Peter\AppData\Local\Temp...	SUCCESS	
14:08:...	MaMpEng.exe	3780	CloseFile	C:\Users\Peter\AppData\Local\Temp...	SUCCESS	
14:08:...	svchost.exe	5536	Lock File	C:\Users\Peter\AppData\Local\Conn...	SUCCESS	Exclusive: True, Of...
14:08:...	svchost.exe	5536	UnlockFileSingle	C:\Users\Peter\AppData\Local\Conn...	SUCCESS	Offset: 124, Length...
14:08:...	svchost.exe	5536	Lock File	C:\Users\Peter\AppData\Local\Conn...	SUCCESS	Exclusive: False, O...
14:08:...	svchost.exe	5536	ReadFile	C:\Windows\System32\cdp.dll	SUCCESS	Offset: 4 073 984, ...
14:08:...	MaMpEng.exe	3780	CreateFile	C:\Users\Peter\AppData\Local\Temp...	SUCCESS	Desired Access: R...
14:08:...	Explorer.EXE	1644	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query: Name
14:08:...	Explorer.EXE	1644	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
14:08:...	Explorer.EXE	1644	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
14:08:...	Explorer.EXE	1644	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
14:08:...	Explorer.EXE	1644	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
14:08:...	Explorer.EXE	1644	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query: Name
14:08:...	Explorer.EXE	1644	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
14:08:...	Explorer.EXE	1644	RegQueryValue	HKCU\Software\Classes	SUCCESS	Query: Name
14:08:...	Explorer.EXE	1644	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
14:08:...	Explorer.EXE	1644	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
14:08:...	AUDIODG.EXE	13776	ReadFile	C:\Windows\System32\AUDIOKSE.dll	SUCCESS	Offset: 397 824, Le...
14:08:...	svchost.exe	2224	Lock File	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
14:08:...	ctfmon.exe	3068	ReadFile	C:\Windows\System32\inputService.dll	SUCCESS	Offset: 4 088 320, ...
14:08:...	MaMpEng.exe	3780	QueryAllInforma...	C:\Users\Peter\AppData\Local\Temp...	SUCCESS	VolumeCreationTim...
14:08:...	Explorer.EXE	1644	CreateFile	C:\Users\Peter\AppData\Local\Temp...	SUCCESS	Desired Access: R...
14:08:...	svchost.exe	5536	ReadFile	C:\Windows\System32\cdp.dll	SUCCESS	Offset: 4 037 120, ...
14:08:...	svchost.exe	2224	QueryStandardI...	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	AllocationSize: 3 1...
14:08:...	MaMpEng.exe	3780	QueryAllInforma...	C:\Users\Peter\AppData\Local\Temp...	BUFFER OVERFL...	CreationTime: 202...
14:08:...	Explorer.EXE	1644	QueryBasicInfor...	C:\Users\Peter\AppData\Local\Temp...	SUCCESS	CreationTime: 202...
14:08:...	MaMpEng.exe	3780	QueryAllInforma...	C:\Users\Peter\AppData\Local\Temp...	SUCCESS	VolumeCreationTim...
14:08:...	svchost.exe	2224	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Offset: 123, Length...
14:08:...	Explorer.EXE	1644	CloseFile	C:\Users\Peter\AppData\Local\Temp...	SUCCESS	
14:08:...	MaMpEng.exe	3780	QueryAllInforma...	C:\Users\Peter\AppData\Local\Temp...	BUFFER OVERFL...	CreationTime: 202...

Showing 66 569 of 369 843 events (17%) Backed by virtual memory

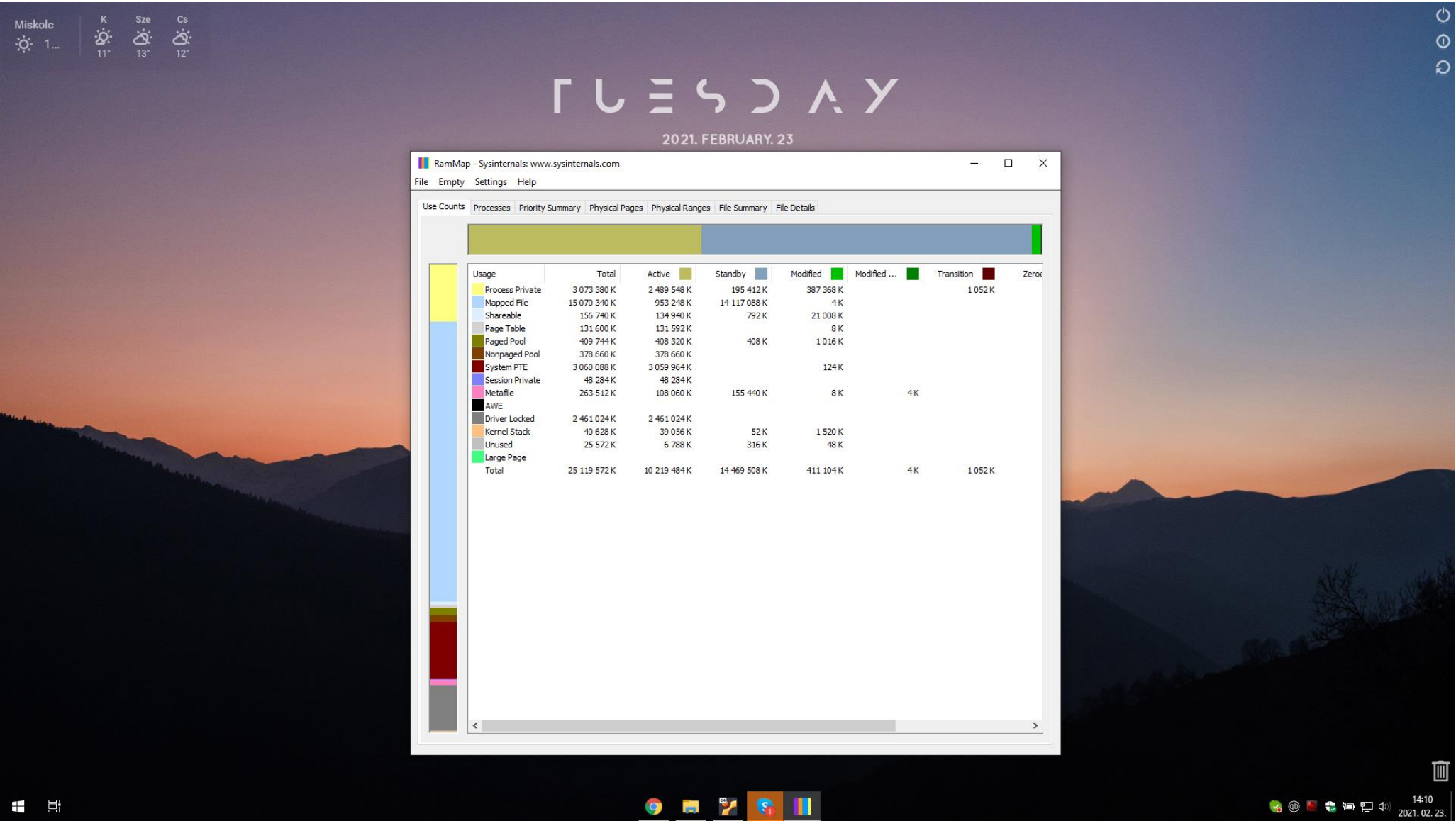
Autoruns: A gépen bekapcsolás után automatikusan induló programokat, folyamatokat mutatja meg.

The screenshot displays the Autoruns utility window, which is used to manage programs and services that start automatically with the Windows operating system. The window is titled "Autoruns - Sysinternals: www.sysinternals.com" and has a menu bar with "File", "Entry", "Options", and "Help". Below the menu bar is a toolbar with icons for "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", and "AppInit".

The main window displays a list of entries in a table with the following columns: "Autorun Entry", "Description", "Publisher", "Image Path", "Timestamp", and "VirusTotal". The entries are listed in alphabetical order by path. The "Autorun Entry" column shows the path of the entry, such as "HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell" and "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup". The "Description" column provides a brief description of the entry, such as "Windows Command Processor" and "Rainmeter desktop customization tool". The "Publisher" column shows the publisher of the entry, such as "Microsoft Windows" and "Frebit OU". The "Image Path" column shows the path to the executable file, such as "c:\windows\system32\cmd.exe" and "c:\program files\rainmeter\rainmeter.exe". The "Timestamp" column shows the date and time when the entry was created or modified, such as "2019. 12. 07. 10:15" and "2019. 09. 22. 12:27". The "VirusTotal" column shows the status of the entry, such as "Verified" and "Not verified".

At the bottom of the window, there is a status bar that says "(Escape to cancel) Scanning..." and "Signed Windows Entries Hidden."

RamMap: A memória kiosztását, felhasználását mutatja meg.



Miskolc 1 ... K Size Cs

12° 13° 12°

TUESDAY

2021. FEBRUARY. 23

VMMMap - Sysinternals: www.sysinternals.com

Process: chrome.exe
PID: 10896

Committed: 73 984 K

Private Bytes: 1 720 K

Working Set: 7 584 K

Type	Size	Committed	Private	Total WS
Total	2 151 835 300 K	73 984 K	1 720 K	7 584 K
Free	135 287 118 656 K			
Heap	1 680 K	564 K	500 K	488 K
Image	23 472 K	23 472 K	404 K	5 900 K
Managed Heap				
Mapped File	3 172 K	3 172 K		80 K
Page Table	548 K	548 K	548 K	548 K
Private Data	4 229 272 K	92 K	92 K	72 K
Shareable	2 147 510 104 K	45 960 K		456 K
Stack	65 536 K	176 K	176 K	40 K
Unusable	1 516 K			

Address	Type	Size	Committed	Private	Total WS	Private
000000007FFE0000	Private Data	4 K	4 K	4 K	4 K	4 K
000000007FFEC000	Private Data	4 K	4 K	4 K	4 K	4 K
00000000902A000000	Private Data	2 048 K	68 K	68 K	52 K	5
00000000902A200000	Thread Stack	8 192 K	24 K	24 K	8 K	8 K
00000000902A400000	Thread Stack	8 192 K	20 K	20 K	8 K	8 K
00000000902A600000	Thread Stack	8 192 K	20 K	20 K	8 K	8 K
00000000902A800000	Thread Stack	8 192 K	28 K	28 K	8 K	8 K

Timeline... Heap Allocations... Call Tree... Trace...

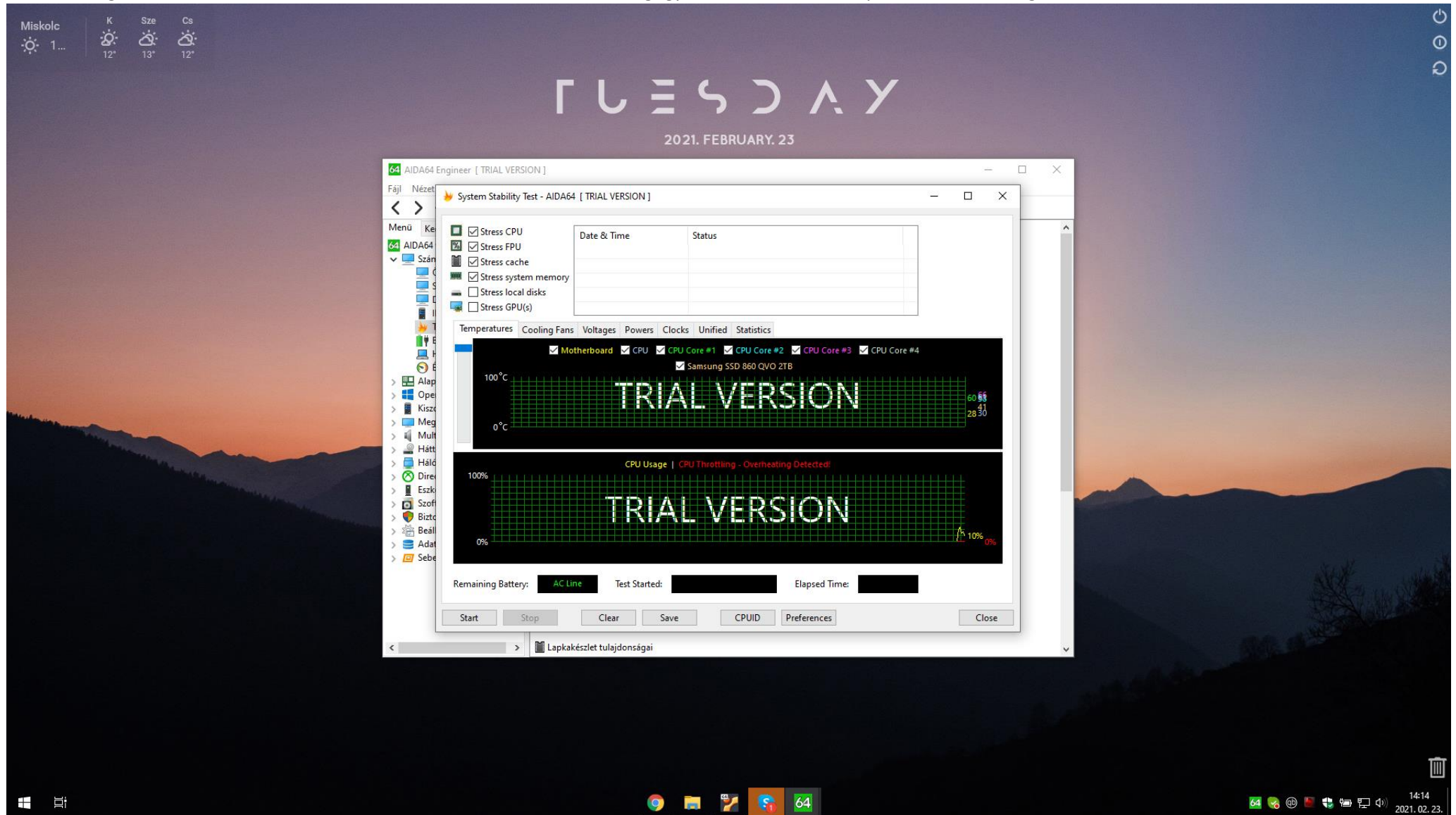
14:11
2021. 02. 23

A gépben lévő grafikus kártyáról mutat információkat, remek diagnosztikai eszköz, a hőmérsékletmérés, memória és grafikus processzor sebesség mérés miatt.

The screenshot shows a Windows 10 desktop with a sunset wallpaper. In the top-left corner, there is a weather widget for Miskolc showing a temperature of 12°C. The desktop background features the word 'TUESDAY' and the date '2021. FEBRUARY. 23' in a stylized font. The time is displayed as '- 14:13 -'. A TechPowerUp GPU-Z 2.37.0 window is open in the center, displaying various GPU metrics for an NVIDIA GeForce GTX 1070. The window has tabs for 'Graphics Card', 'Sensors', 'Advanced', and 'Validation'. The 'Sensors' tab is active, showing a list of metrics with their current values and status indicators (red bars for high values, green for normal). At the bottom of the window, there is a 'Log to file' checkbox, a 'Reset' button, and a 'Close' button. The taskbar at the bottom shows the Start button, a search icon, and several application icons including Chrome, File Explorer, and the Task Manager. The system tray in the bottom-right corner shows the date and time as '14:13 2021. 02. 23.'.

Metric	Value	Status
GPU Clock	1442.5 MHz	Normal
Memory Clock	1999.7 MHz	Normal
GPU Temperature	60.9 °C	Normal
Hot Spot	71.9 °C	Normal
Memory Used	536 MB	Normal
GPU Load	3 %	Normal
Memory Controller Load	1 %	Normal
Video Engine Load	0 %	Normal
Bus Interface Load	0 %	Normal
Board Power Draw	37.7 W	Normal
GPU Chip Power Draw	12.0 W	Normal
PerfCap Reason	Idle	Normal
GPU Voltage	0.7930 V	Normal
CPU Temperature	60.0 °C	Normal
System Memory Used	10324 MB	Normal

AIDA64: Diagnosztikai eszköz, többek közt a CPU-t lehet vele terhelni, és megfigyelni a hőmérsékletet, processzor sebességet.



CPU-Z: A processzorról és a gépről nyújt információkat, mint például memória sebesség, grafikus kártyailllesztő verziója.

Miskolc 1... K 12° Sze 13° Cs 12°

TUESDAY

2021. FEBRUARY. 23

- 14:14 -

CPU-Z

CPU | Caches | Mainboard | Memory | SPD | Graphics | Bench | About

Processor

Name: Intel Core i7 6700HQ
Code Name: Skylake Max TDP: 45.0 W
Package: Socket 1440 FCBGA
Technology: 14 nm Core VID: 1.120 V

Specification

Intel® Core™ i7-6700HQ CPU @ 2.60GHz

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

Clocks (Core #0)

Core Speed	3192.96 MHz
Multiplier	x 32.0 (8 - 35)
Bus Speed	99.78 MHz
Rated FSB	

Cache

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: 8

CPU-Z Ver. 1.95.0.x64 Tools Validate Close

14:14
2021. 02. 23.