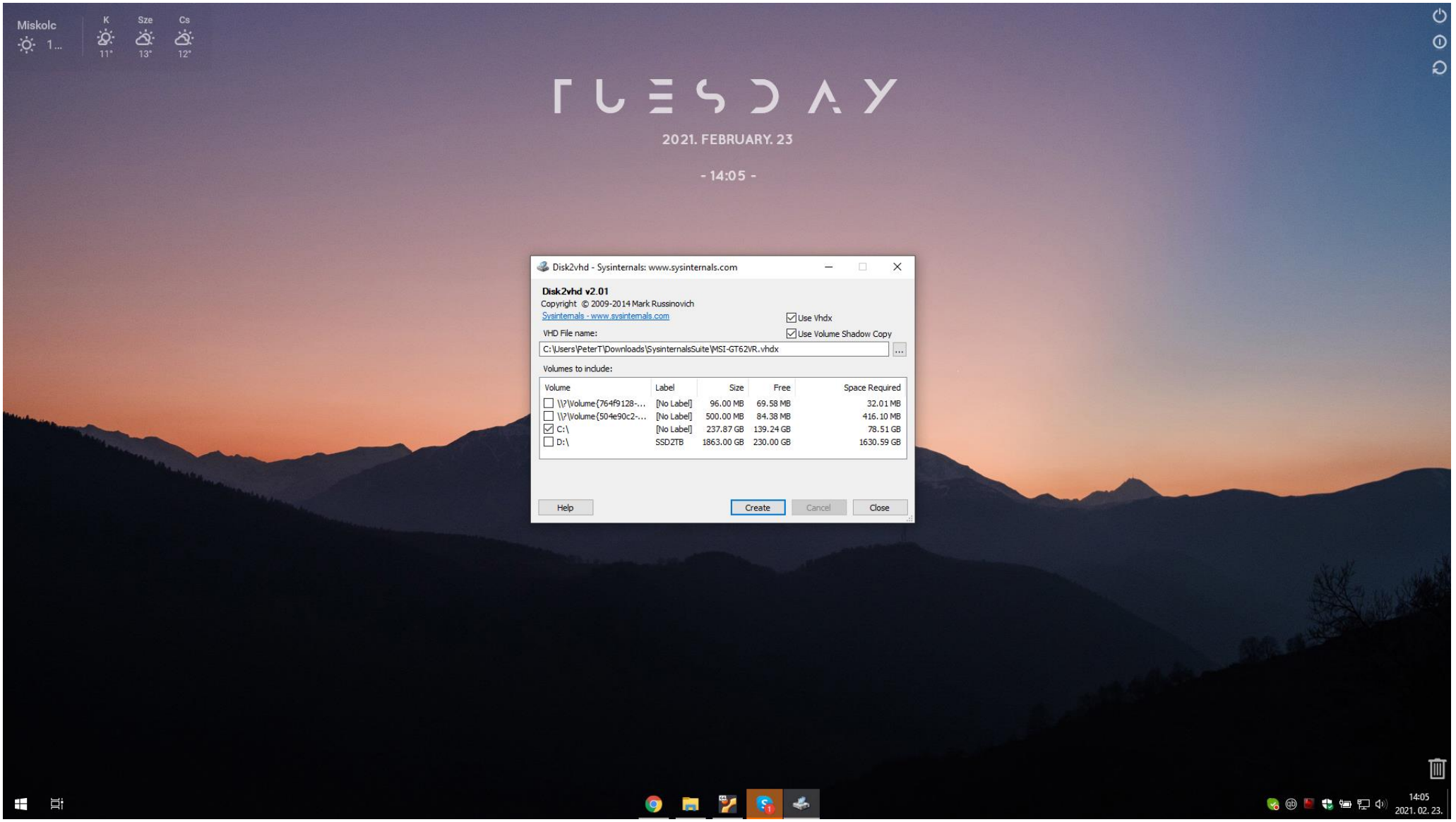
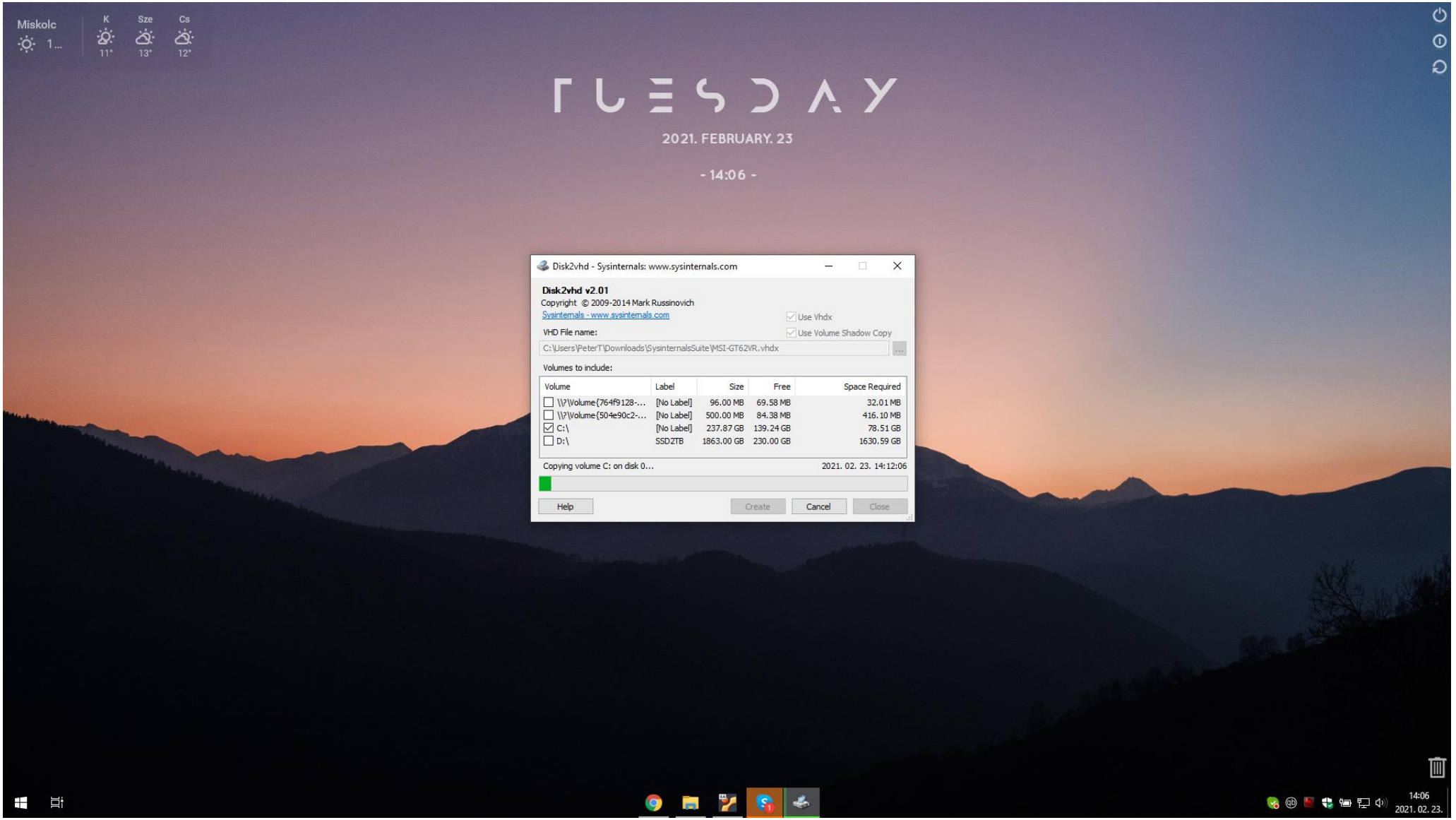
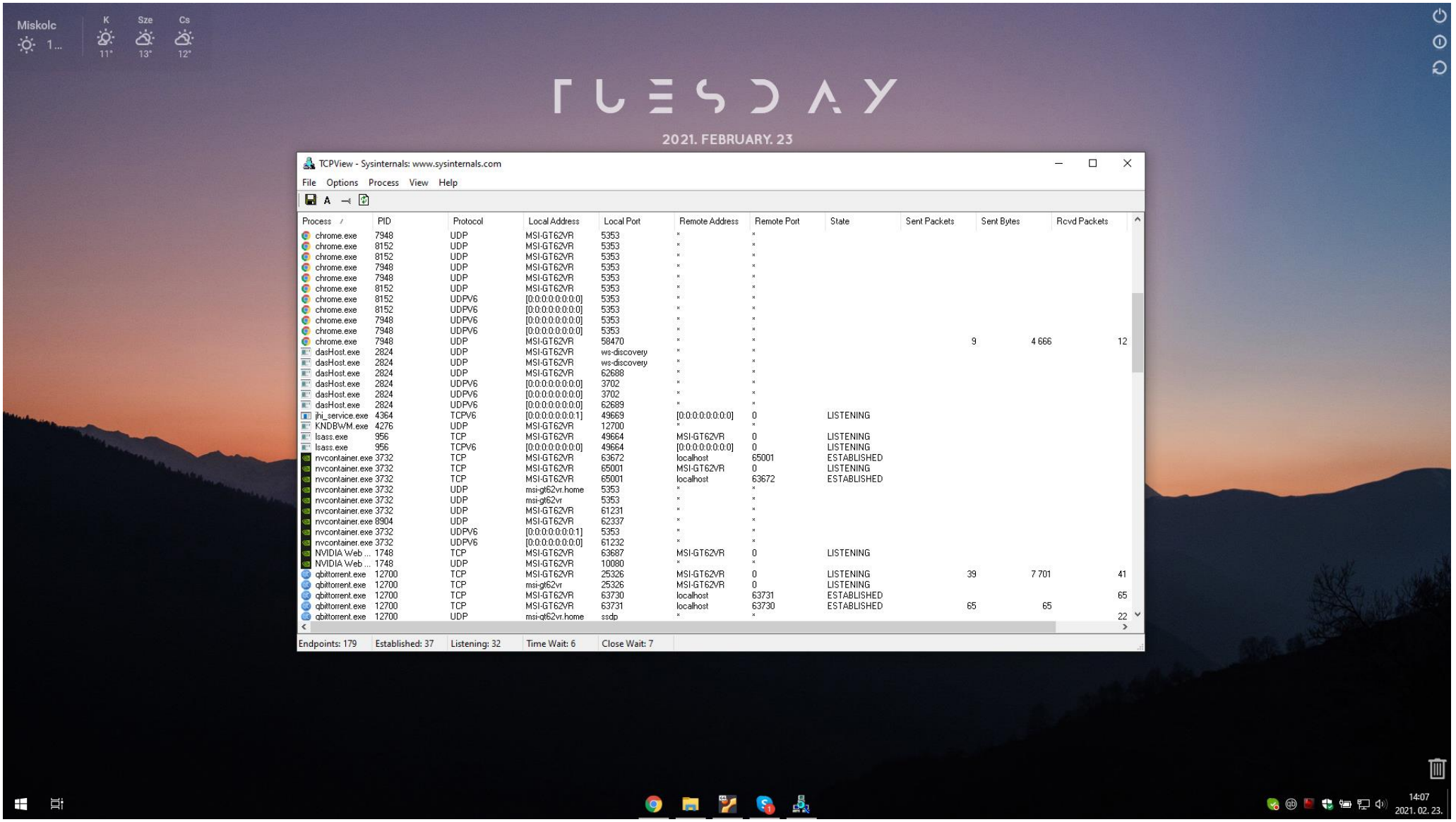
Disk2vhd: Lemezekről, partíciókról lehet a program segítségével virrtuális lemezképfájlt készíteni.

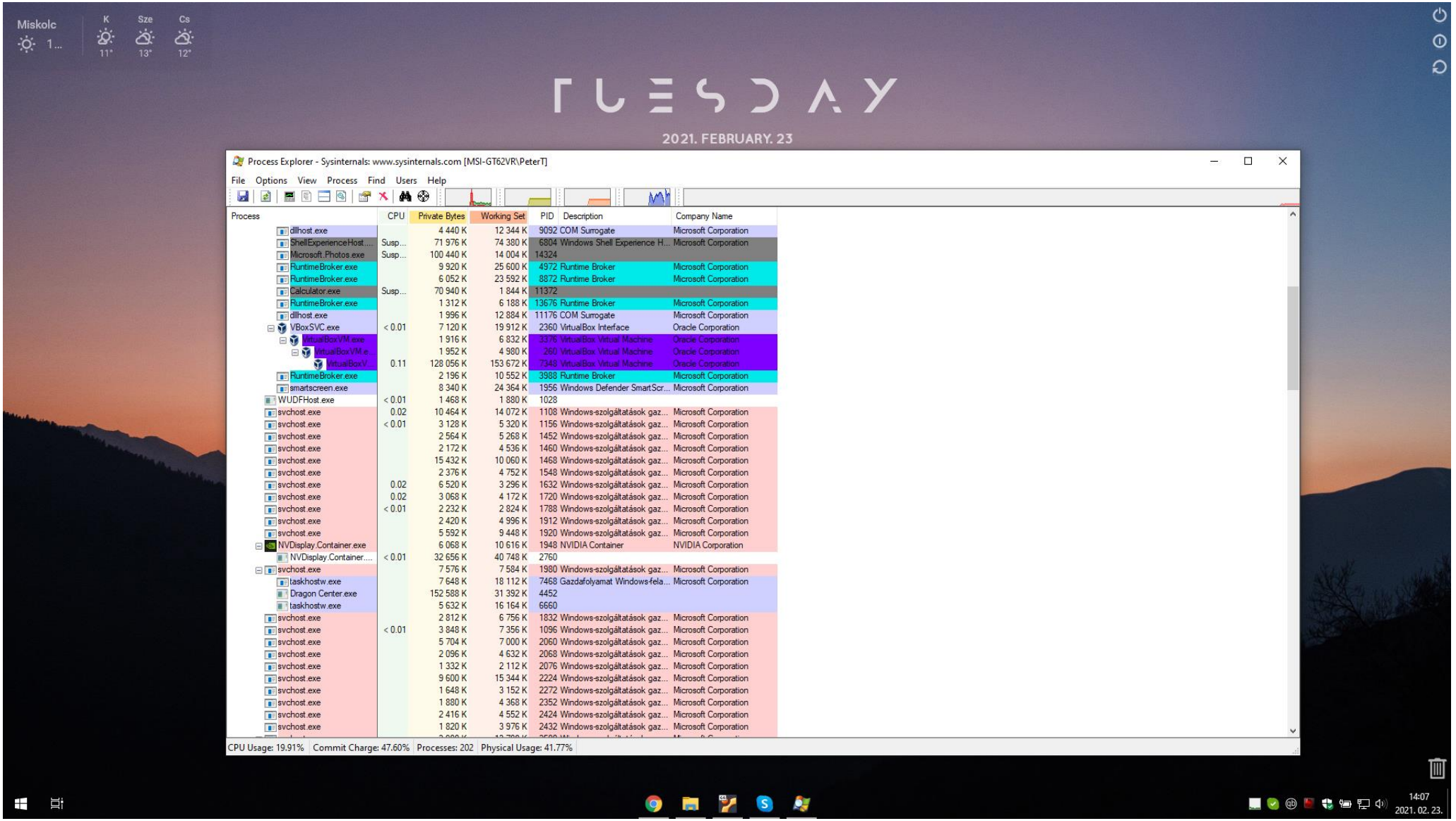


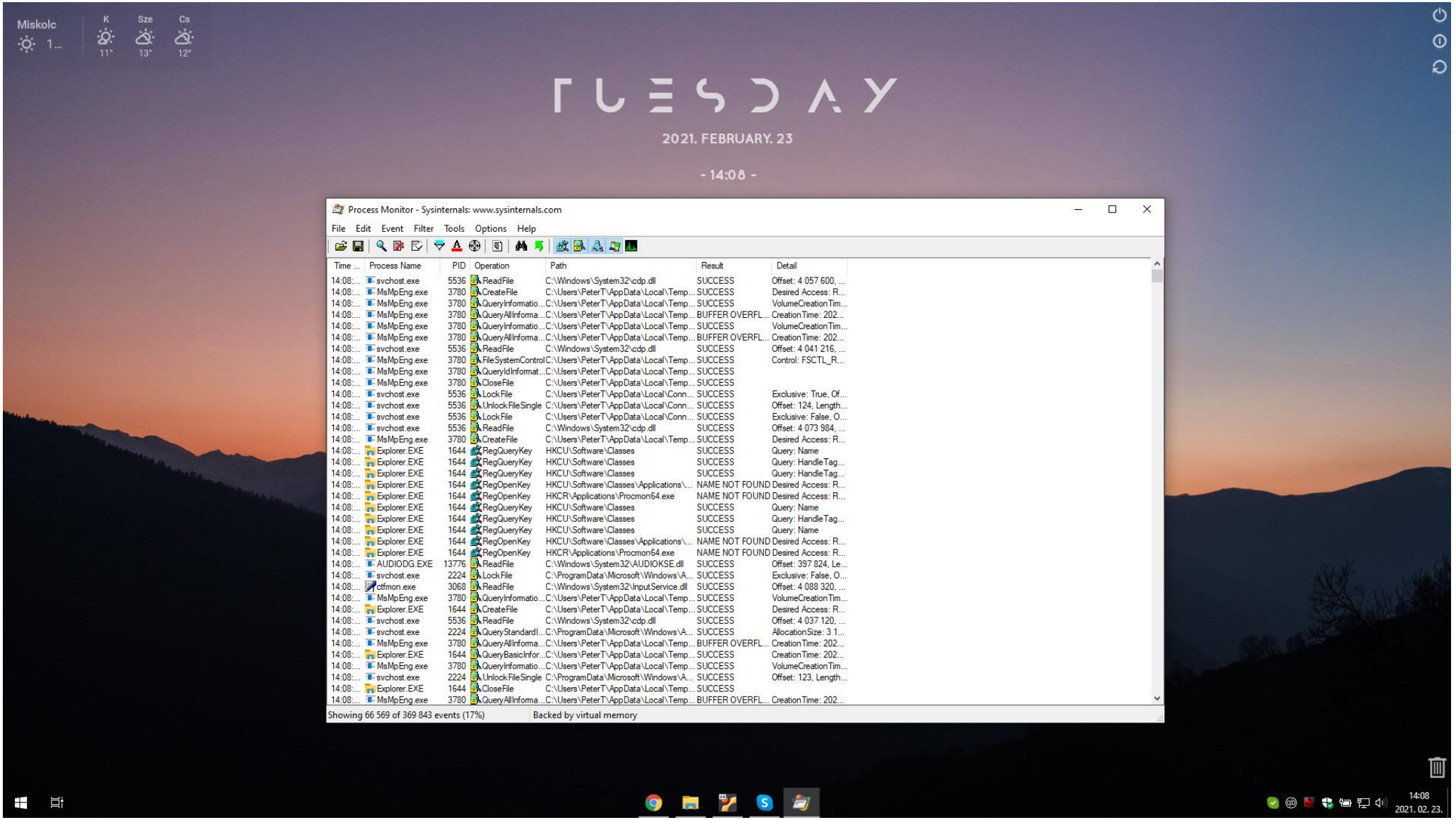

Miskolc
K
Sze
Cs
11°
13°
12°
TUESDAY
2021. FEBRUARY. 23
- 14:06 -
Disk2vhd - Sysinternals: www.sysinternals.com
Disk2vhd v2.01
Copyright © 2009-2014 Mark Russinovich
Sysinternals - www.sysinternals.com
Use Vhdx
VHD File name:
Use Volume Shadow Copy
C:\Users\PeterT\Downloads\SysinternalsSuite\MSI-GT62VR.vhdx
Volumes to include:
Volume
Label
Size
Free
Space Required
\\?\Volume{764f9128-...
[No Label]
96.00 MB
69.58 MB
32.01 MB
\\?\Volume{504e90c2-...
[No Label]
500.00 MB
84.38 MB
416.10 MB
C:\
[No Label]
237.87 GB
139.24 GB
78.51 GB
D:\
SSDZTB
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.

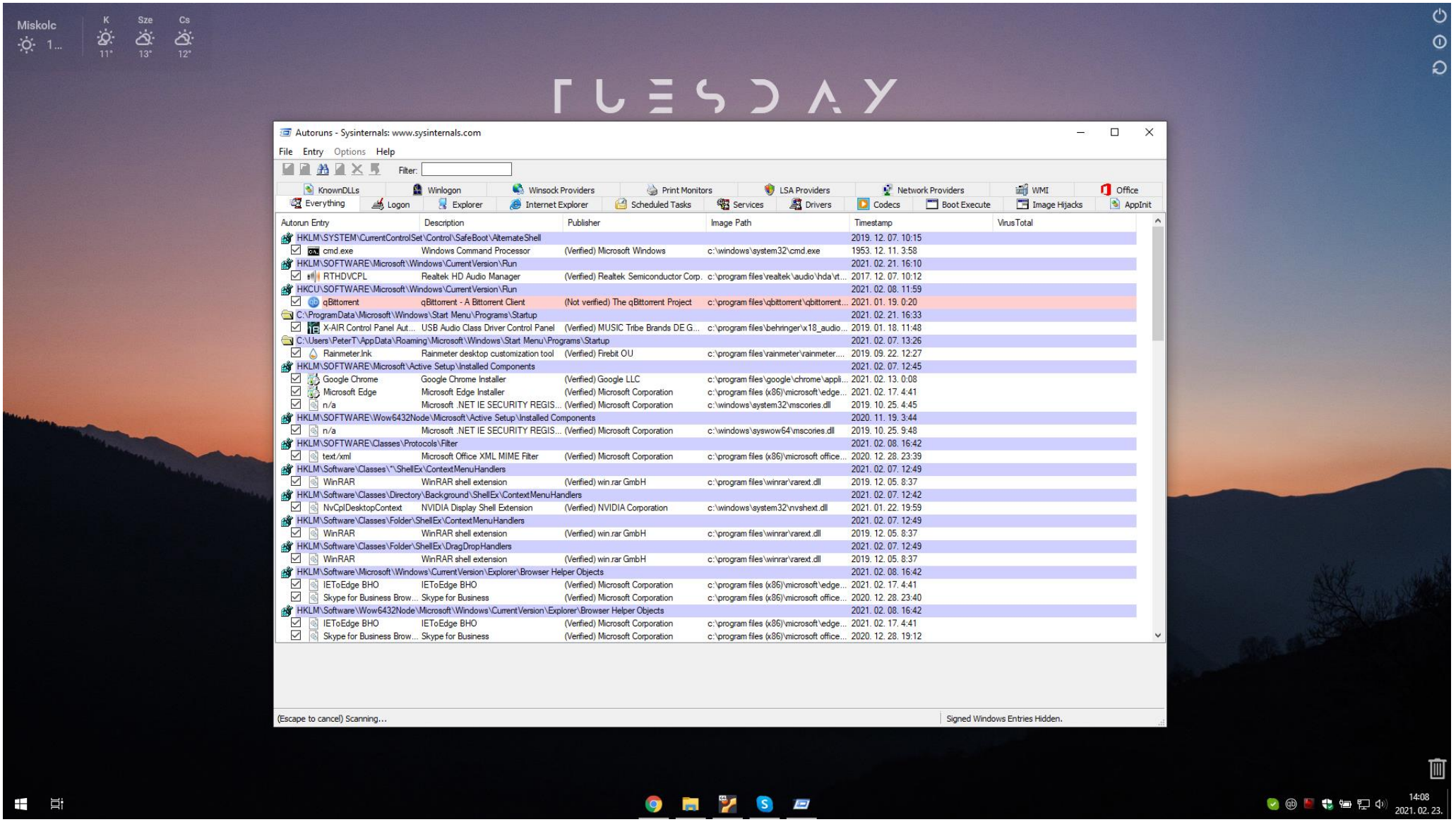


Process Explorer / Process Monitor: A gépen futó processzeket lehet monitorozni, megfigyelni.

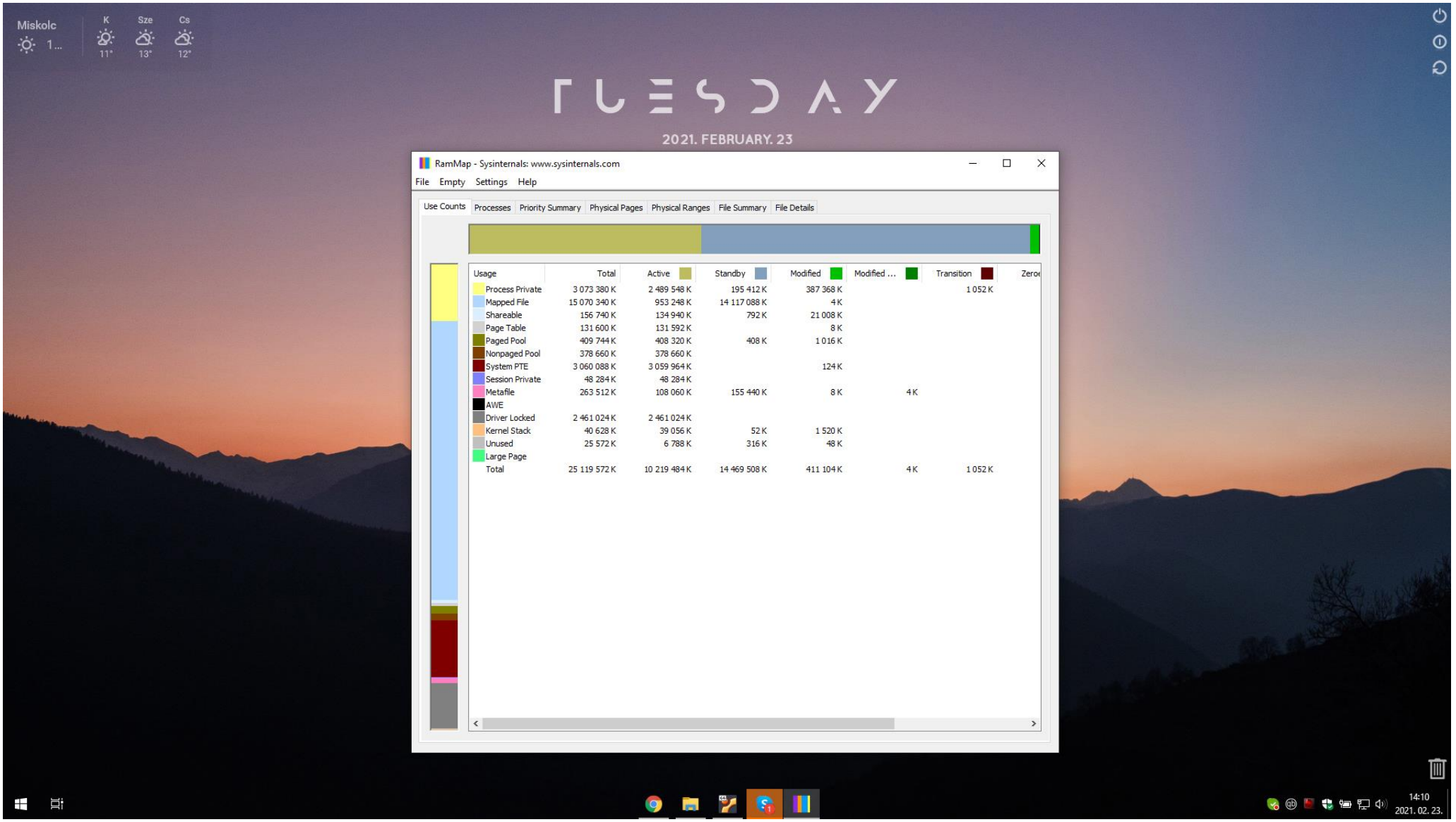



Miskolc
K
Sze
Cs
11°
13°
12°
TUESDAY
2021. FEBRUARY. 23
- 14:08 -
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
14:08:... svchost.exe 5536 ReadFile C:\Windows\System32\cdp.dll SUCCESS Offset: 4 057 600, ...
14:08:... MsMpEng.exe 3780 CreateFile C:\Users\PeterT\AppData\Local\Temp... SUCCESS Desired Access: R...
14:08:... MsMpEng.exe 3780 QueryInformatio... C:\Users\PeterT\AppData\Local\Temp... SUCCESS VolumeCreationTim...
14:08:... MsMpEng.exe 3780 QueryAllInforma... C:\Users\PeterT\AppData\Local\Temp... BUFFER OVERFL... CreationTime: 202...
14:08:... MsMpEng.exe 3780 QueryInformatio... C:\Users\PeterT\AppData\Local\Temp... SUCCESS VolumeCreationTim...
14:08:... MsMpEng.exe 3780 QueryAllInforma... C:\Users\PeterT\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:... MsMpEng.exe 3780 FileSystemControl C:\Users\PeterT\AppData\Local\Temp... SUCCESS Control: FSCTL_R...
14:08:... MsMpEng.exe 3780 QueryIdInformat... C:\Users\PeterT\AppData\Local\Temp... SUCCESS
14:08:... MsMpEng.exe 3780 CloseFile C:\Users\PeterT\AppData\Local\Temp... SUCCESS
14:08:... svchost.exe 5536 LockFile C:\Users\PeterT\AppData\Local\Conn... SUCCESS Exclusive: True, Of...
14:08:... svchost.exe 5536 UnlockFileSingle C:\Users\PeterT\AppData\Local\Conn... SUCCESS Offset: 124, Length...
14:08:... svchost.exe 5536 LockFile C:\Users\PeterT\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:... MsMpEng.exe 3780 CreateFile C:\Users\PeterT\AppData\Local\Temp... SUCCESS Desired Access: R...
14:08:... Explorer.EXE 1644 RegQueryKey HKCU\Software\Classes SUCCESS Query: Name
14:08:... Explorer.EXE 1644 RegQueryKey HKCU\Software\Classes SUCCESS Query: HandleTag...
14:08:... Explorer.EXE 1644 RegQueryKey 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 RegQueryKey HKCU\Software\Classes SUCCESS Query: Name
14:08:... Explorer.EXE 1644 RegQueryKey HKCU\Software\Classes SUCCESS Query: HandleTag...
14:08:... Explorer.EXE 1644 RegQueryKey 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 LockFile 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:... MsMpEng.exe 3780 QueryInformatio... C:\Users\PeterT\AppData\Local\Temp... SUCCESS VolumeCreationTim...
14:08:... Explorer.EXE 1644 CreateFile C:\Users\PeterT\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:... MsMpEng.exe 3780 QueryAllInforma... C:\Users\PeterT\AppData\Local\Temp... BUFFER OVERFL... CreationTime: 202...
14:08:... Explorer.EXE 1644 QueryBasicInfor... C:\Users\PeterT\AppData\Local\Temp... SUCCESS CreationTime: 202...
14:08:... MsMpEng.exe 3780 QueryInformatio... C:\Users\PeterT\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\PeterT\AppData\Local\Temp... SUCCESS
14:08:... MsMpEng.exe 3780 QueryAllInforma... C:\Users\PeterT\AppData\Local\Temp... BUFFER OVERFL... CreationTime: 202...
Showing 66 569 of 369 843 events (17%)
Backed by virtual memory
14:08
2021. 02. 23.

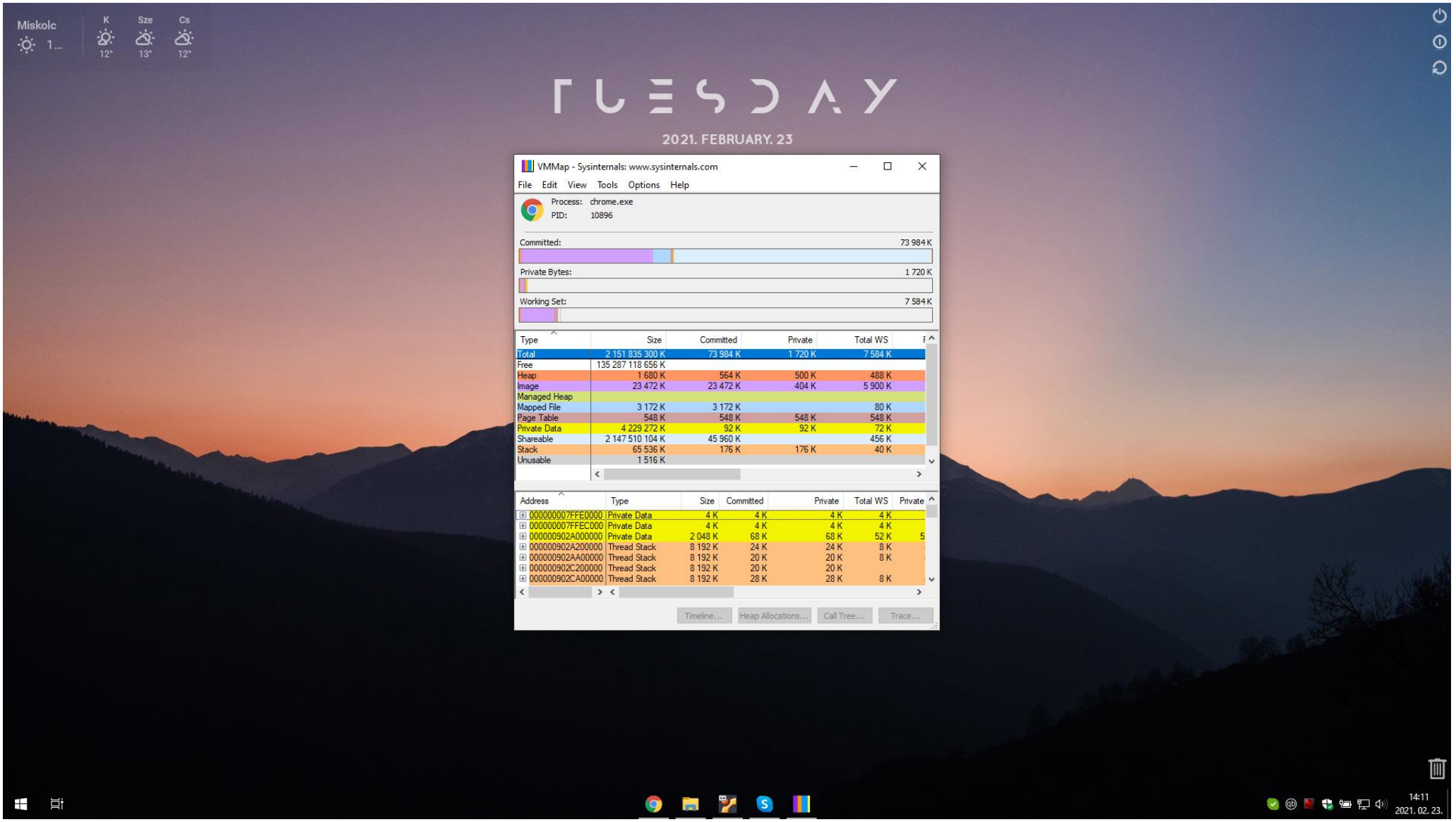
Autoruns: A gépen bekapcsolás után automatikusan induló programokat, folyamatokat mutatja meg.



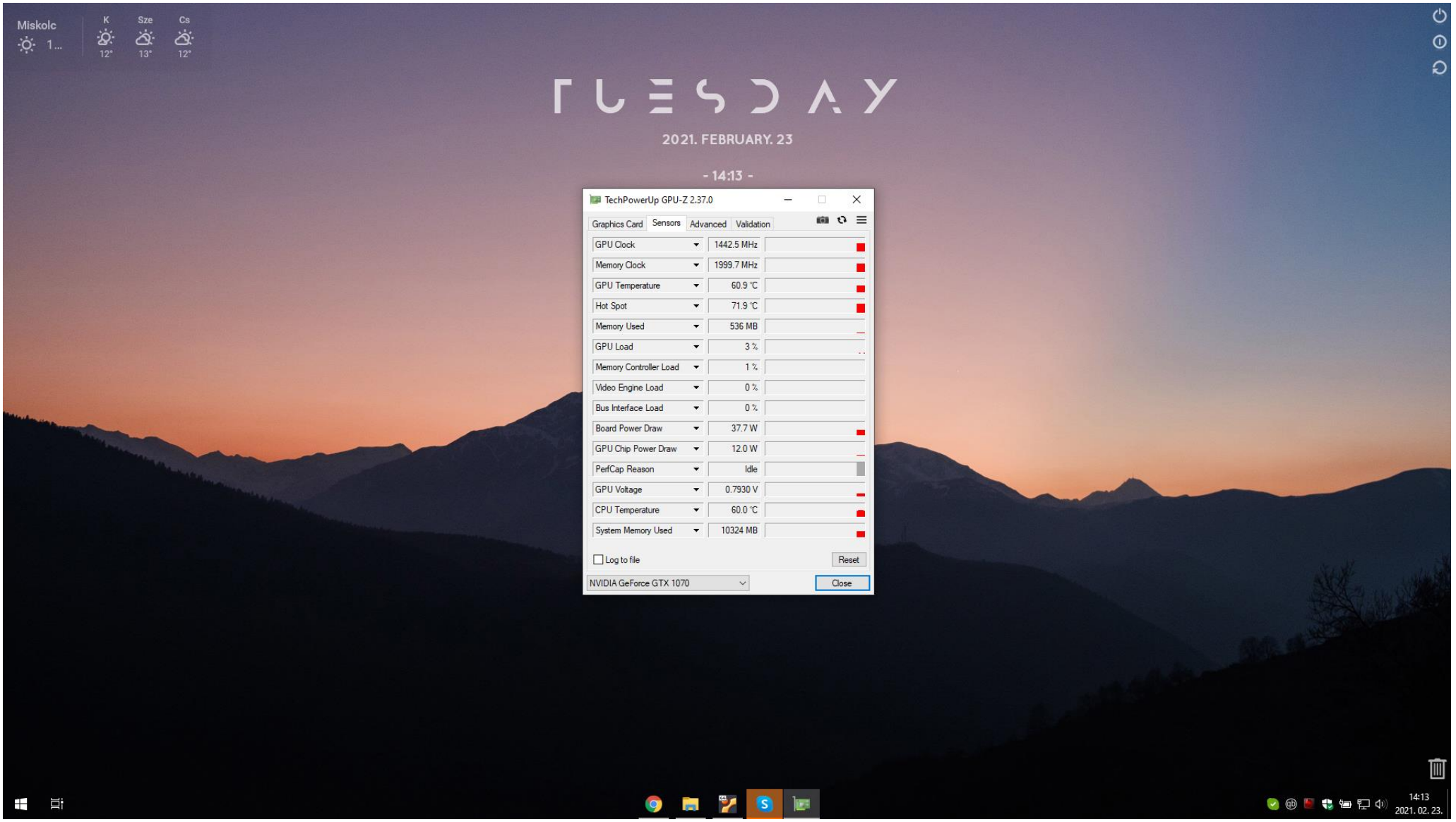
RamMap: A memória kiosztását, felhasználását mutatja meg.



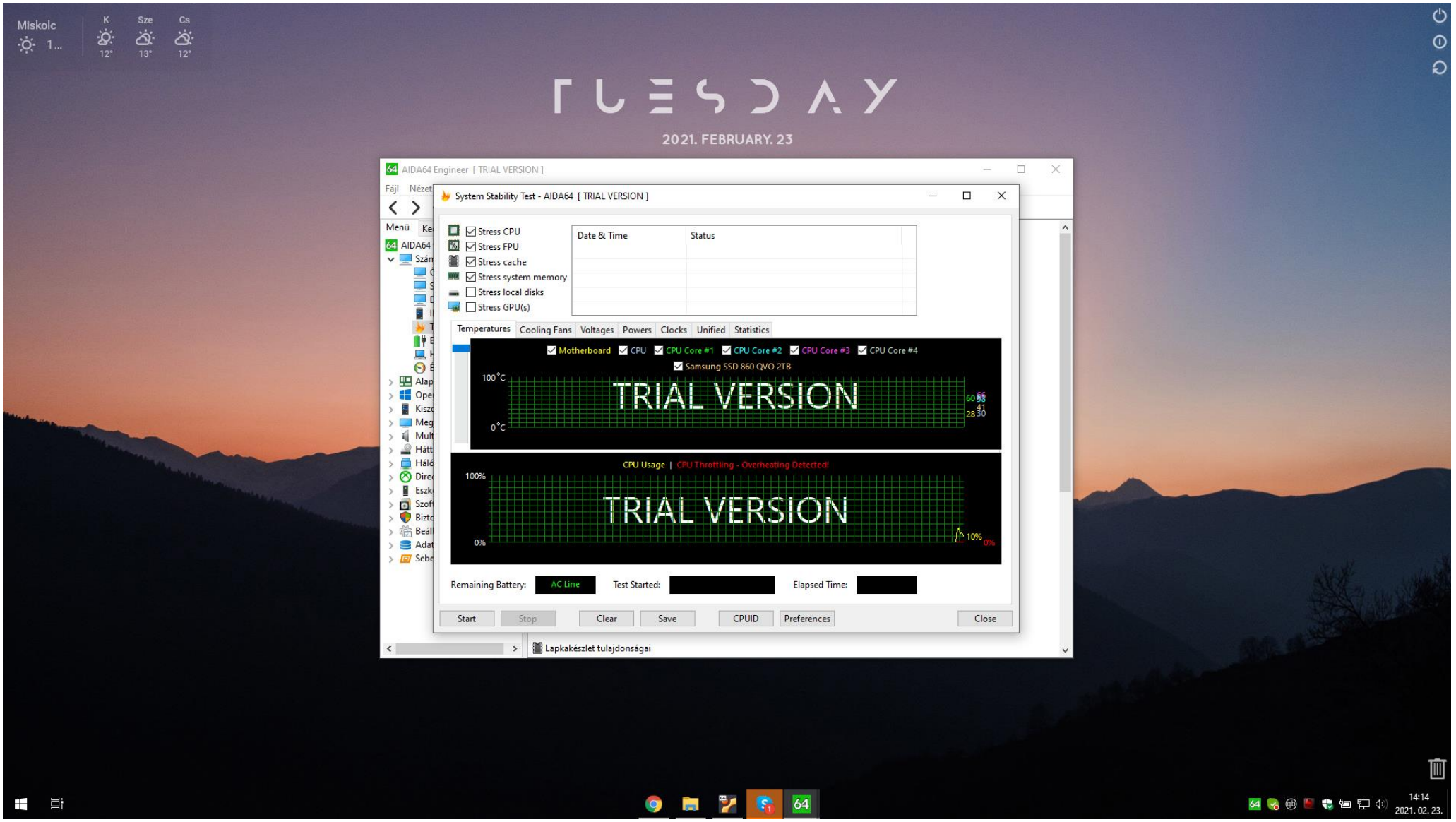
VMMap: A fizikai és virtuális memória kihasználtságát, felhasználását mutatja.



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



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 kártyaillesztő verziója.