3A Feladatok

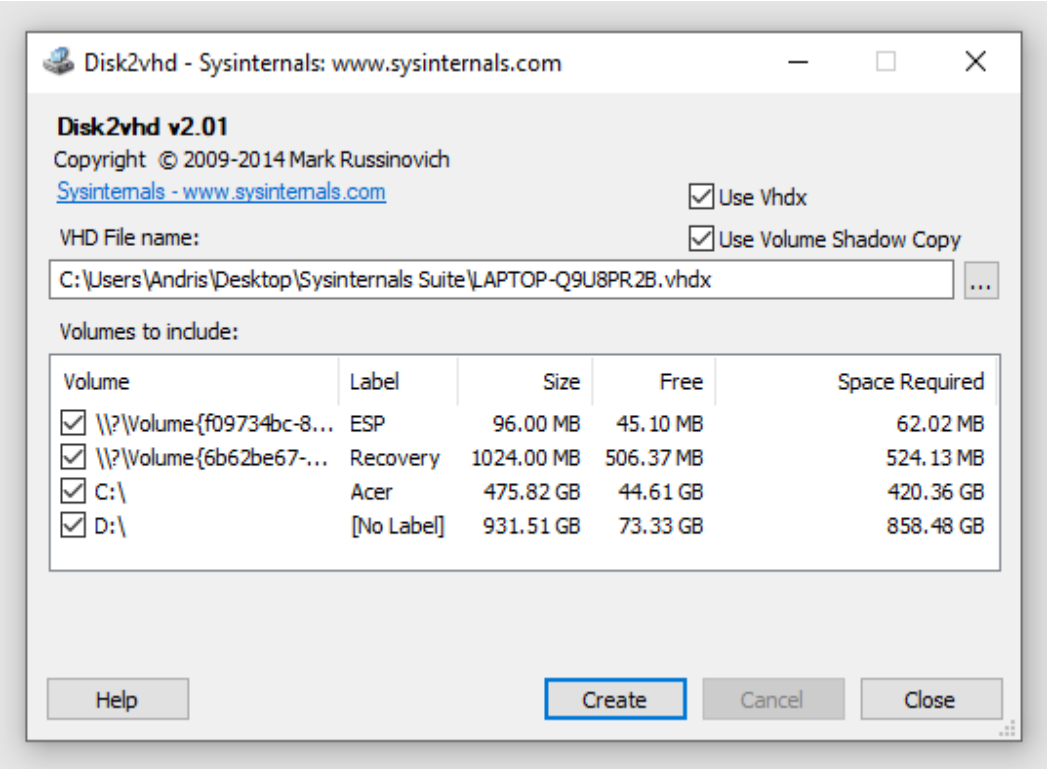
1. Feladat

Sysinternals Suite letöltve.

2. Feladat

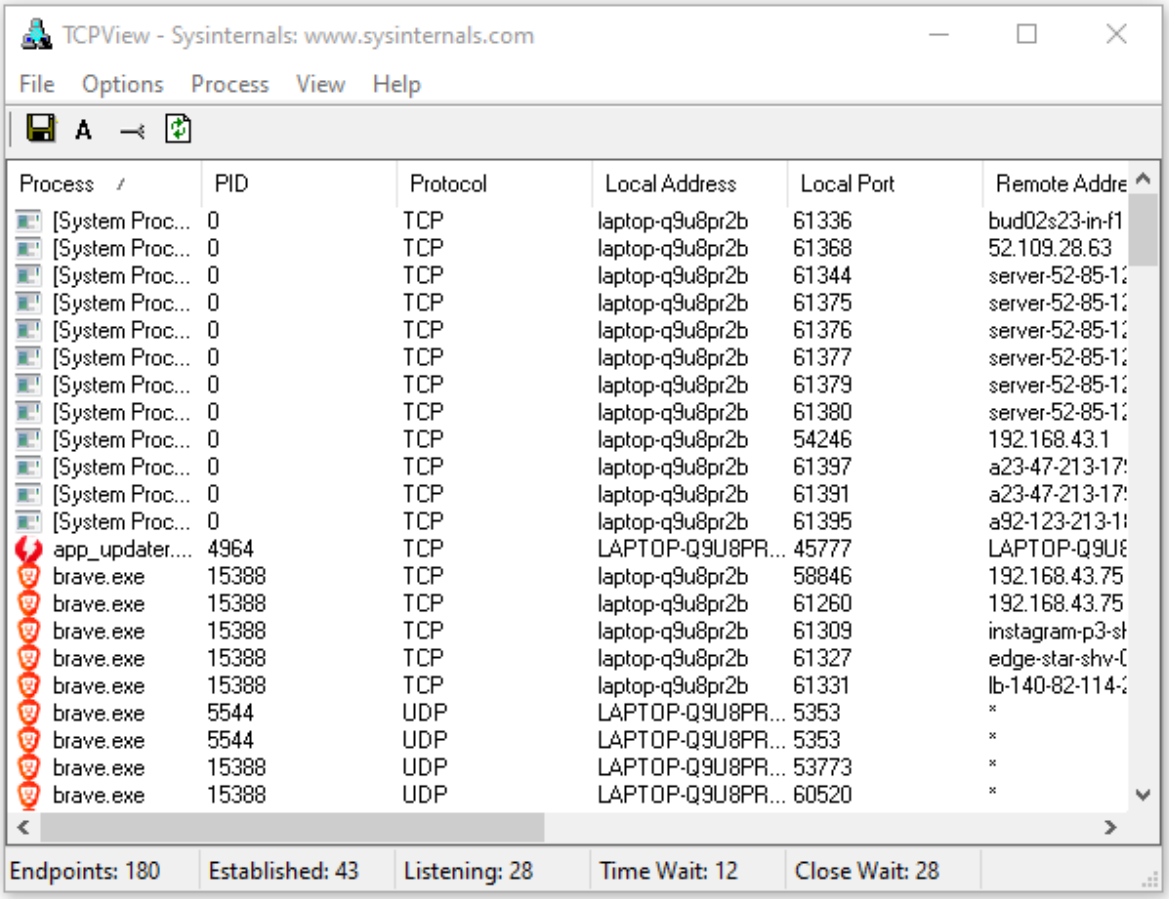
a. *Disk2vhd*

A program egy fizikai lemezből képes virtuális merevlemezt (VHD) készíteni, melyet lehet virtuális gépen (VM) hasznosítani.
A program így néz ki futás közben:



b. *TCPView*

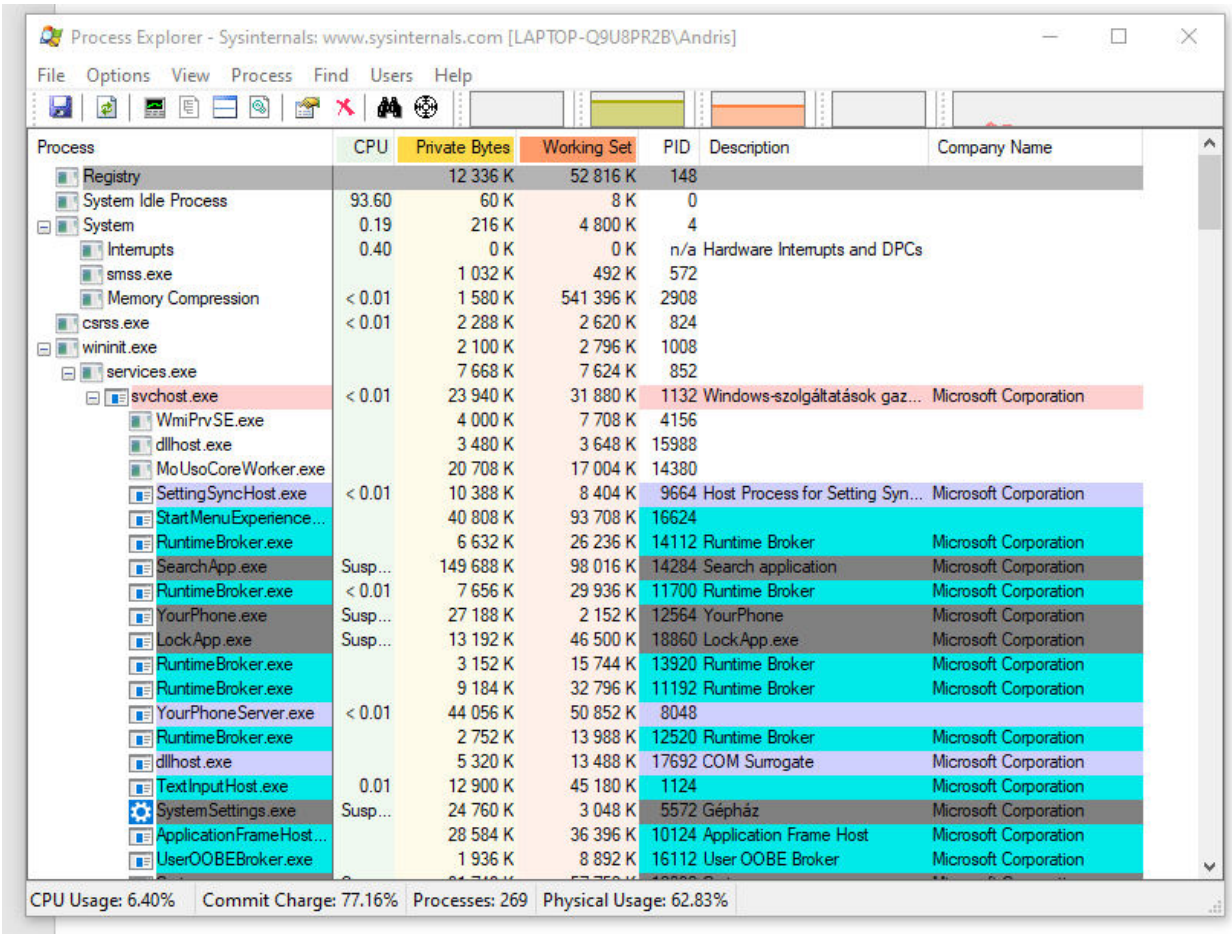
Egy grafikus program, melyben megtekinthetjük az éppen futó folyamatok nevét, protokollját, valamint portot is.
A program így néz ki futás közben:

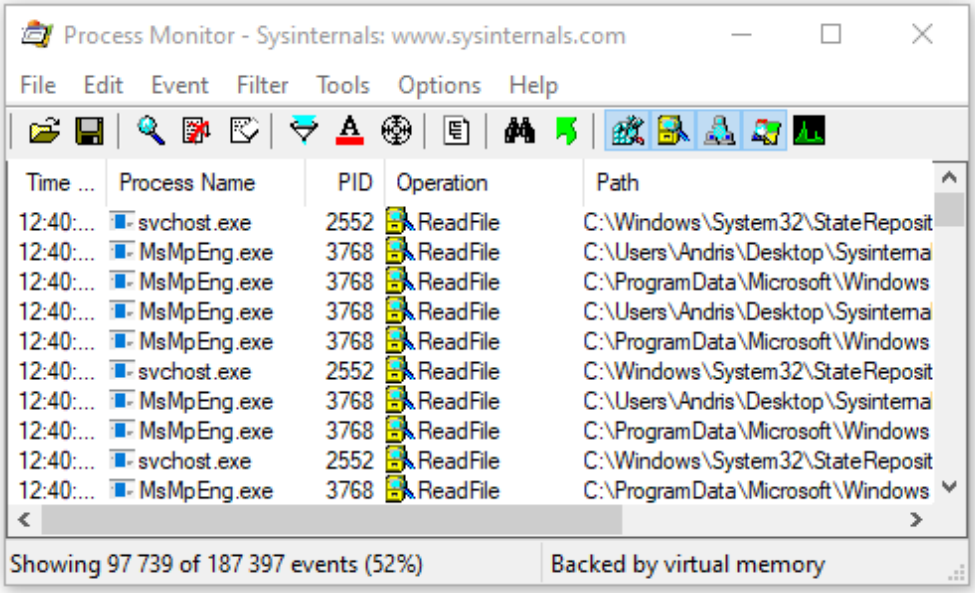


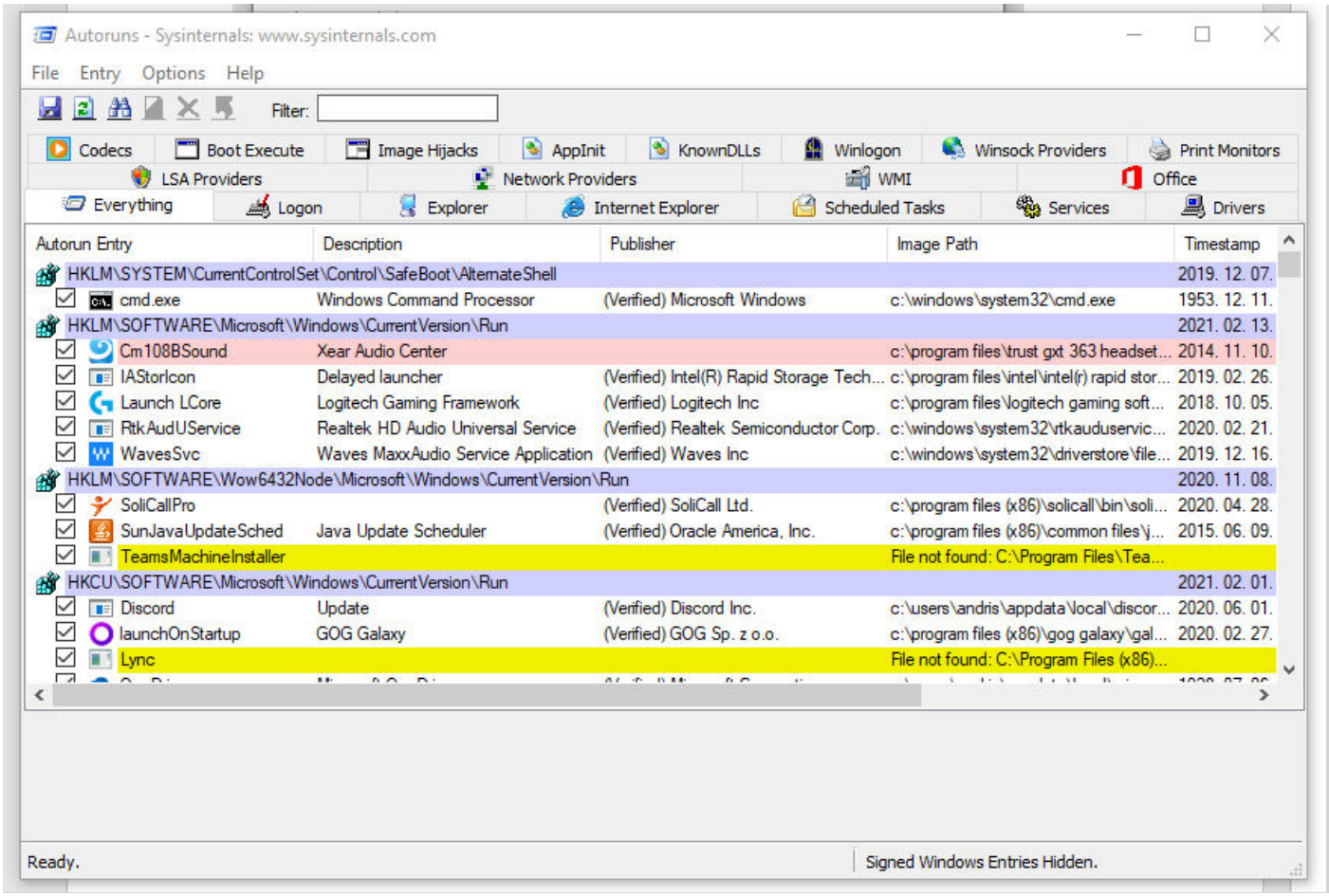
c. *Process Explorer, Process Monitor, AutoRuns*

A számítógépen futó aktuális folyamatokról kaphatunk egy részletes betekintőt ezen alkalmazások használatával.

A programok így néznek ki futás közben:







d. LogonSession

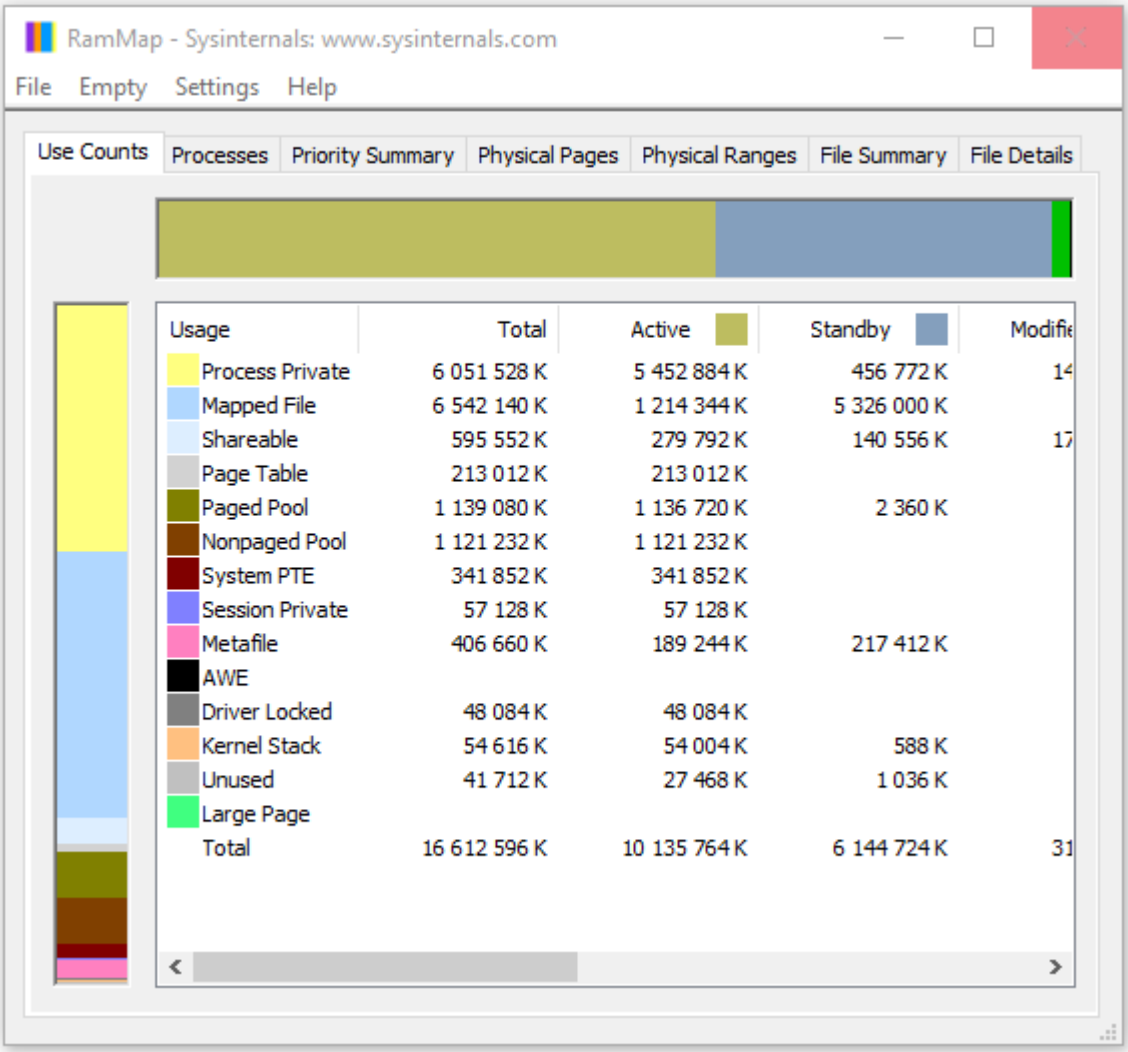
A program kilistázza a bejelentkezési sessionöket. A parancssorban futtattam, rendszergazdai jogosultsággal.

A program így néz ki futás közben:

```
C:\WINDOWS\system32>cd C:\Users\Andris\Desktop\Sysinternals Suite

C:\Users\Andris\Desktop\Sysinternals Suite>logonsessions64

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\LAPTOP-Q9U8PR2B$
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          S-1-5-18
    Logon time:   2021. 02. 12. 15:01:59
    Logon server:
    DNS Domain:
    UPN:

[1] Logon session 00000000:000142d4:
    User name:
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          (none)
    Logon time:   2021. 02. 12. 15:01:59
```

e. *RAMMap*

A program megjeleníti a Windows memóriájában tárolt fájlokat.
A program így néz ki futás közben:



f. *+1 program: Handle*

A program megjeleníti az alkalmazások által használt fájlokat, melyek nyitva vannak éppen.
A program így néz ki futás közben:

C:\Users\Andris\Desktop\Sysinternals Suite\handle64.exe

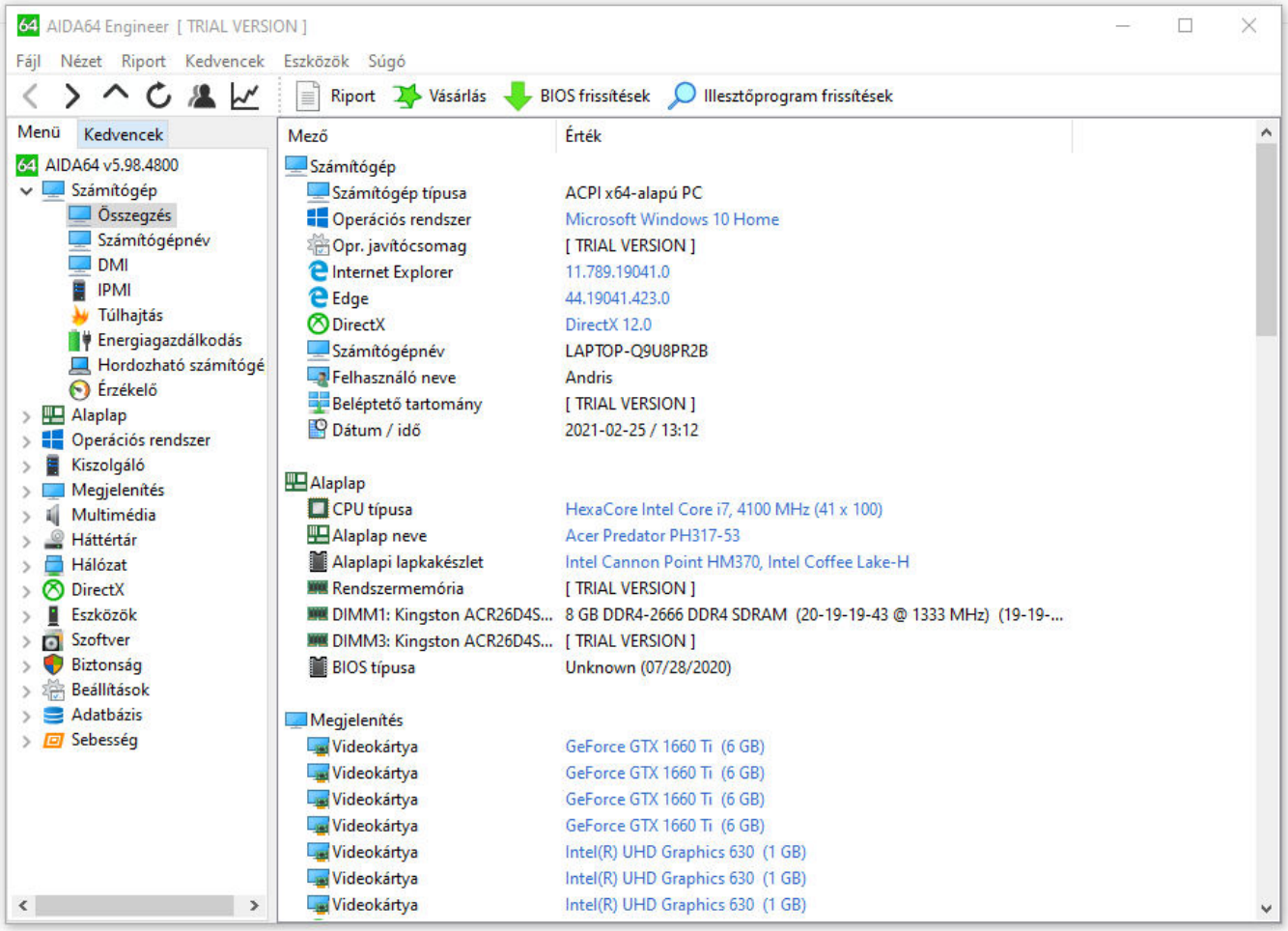
```
 267C: File          C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.746_none_ca02b
4b61b8320a4
 2684: File          C:\Users\Andris\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\IndexedDB\https_www.you
tube.com_0.indexeddb.leveldb\001420.ldb
 26EC: Section       \Sessions\15\BaseNamedObjects\15a8HWNDInterface:50272
 26F8: File          C:\Users\Andris\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\File System\Origins\LOC
K
 2718: File          C:\Users\Andris\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Shortcuts-journal
 27CC: Section       \Sessions\15\BaseNamedObjects\windows_webcache_counters_{9B6AB5B3-91BC-4097-835C-EA2DEC95E9CC}_S-1-
5-21-1609454350-4145425502-3884221099-1001
 2A08: File          C:\Users\Andris\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\IndexedDB\https_www.ins
tagram.com_0.indexeddb.leveldb\LOG
 2A6C: File          C:\Users\Andris\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Sync Data\LevelDB\00432
0.ldb
 2AFC: Section       \Sessions\15\BaseNamedObjects\15a8HWNDInterface:20350
 2B40: File          C:\Users\Andris\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\IndexedDB\https_www.ins
tagram.com_0.indexeddb.leveldb\LOCK
 2E38: File          C:\Users\Andris\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Sync Data\LevelDB\00432
2.ldb
 38A4: File          C:\Users\Andris\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Sync Data\LevelDB\00432
1.log
---------------------------------------------------------------------------
brave.exe pid: 18668 LAPTOP-Q9U8PR2B\Andris
   40: File          C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application
   90: File          C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\88.1.20.110
   DC: File          C:\Users\Andris\AppData\Local\BraveSoftware\Brave-Browser\User Data\CrashpadMetrics.pma
  1D4: Section       \Windows\Theme3410262184
  1D8: Section       \Sessions\15\Windows\Theme3342905786
```

3. Feladat

AIDA64 Engineer

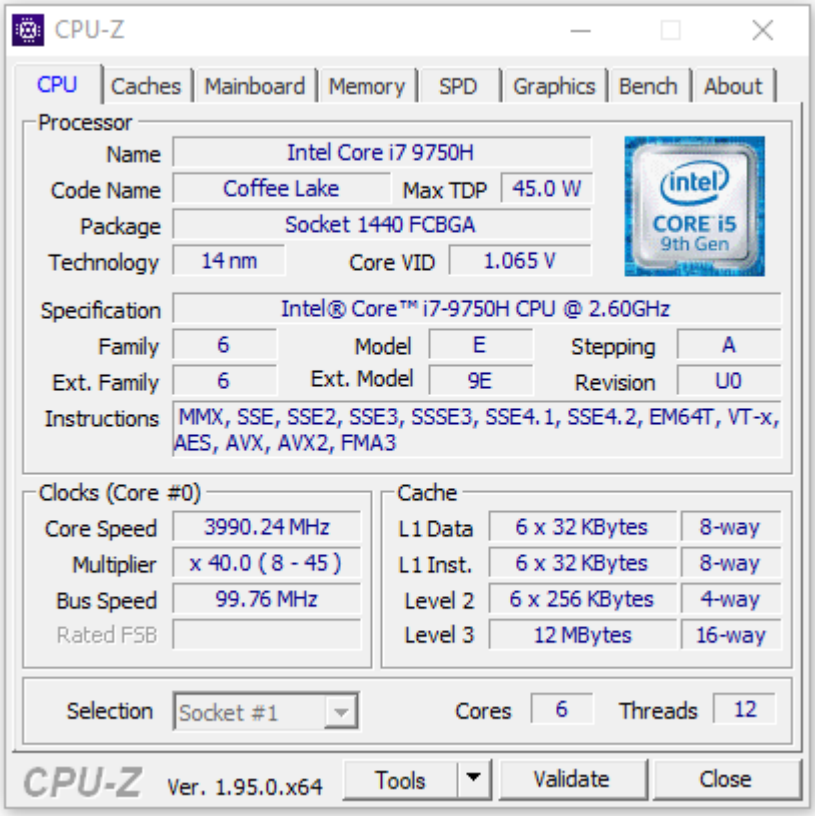
A program részletes információt jelenít meg a telepített programokról, hardverkomponensekről, tudja mérni a gép teljesítményét, segíthet a hibák felderítésében.

A program így néz ki futás közben:



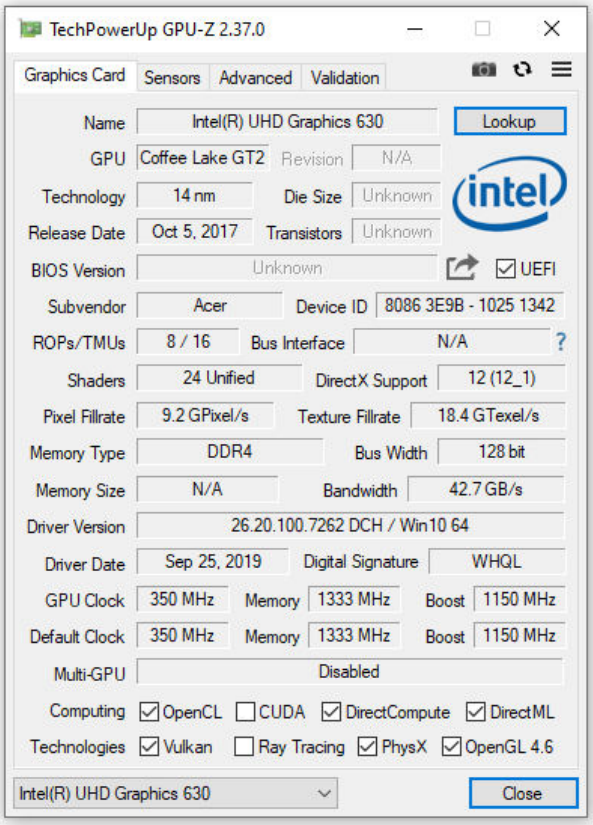
CPU-Z

Az alkalmazás nagyon hasznos, információt jelenít meg a rendszerről, hardverről, például processzor neve, típusa, különböző folyamatok, memória típusa, mérete, valamint egyéb, hozzájuk kapcsolódó adatokról.
A program így néz ki futás közben:



GPU-Z

Egy egyszer, ám praktikus program, mely futtatásakor hasznos információhoz juthatunk a videokártyánkkal kapcsolatban.
A program így néz ki futás közben:



4. Feladat

a. j
b. j
c. j