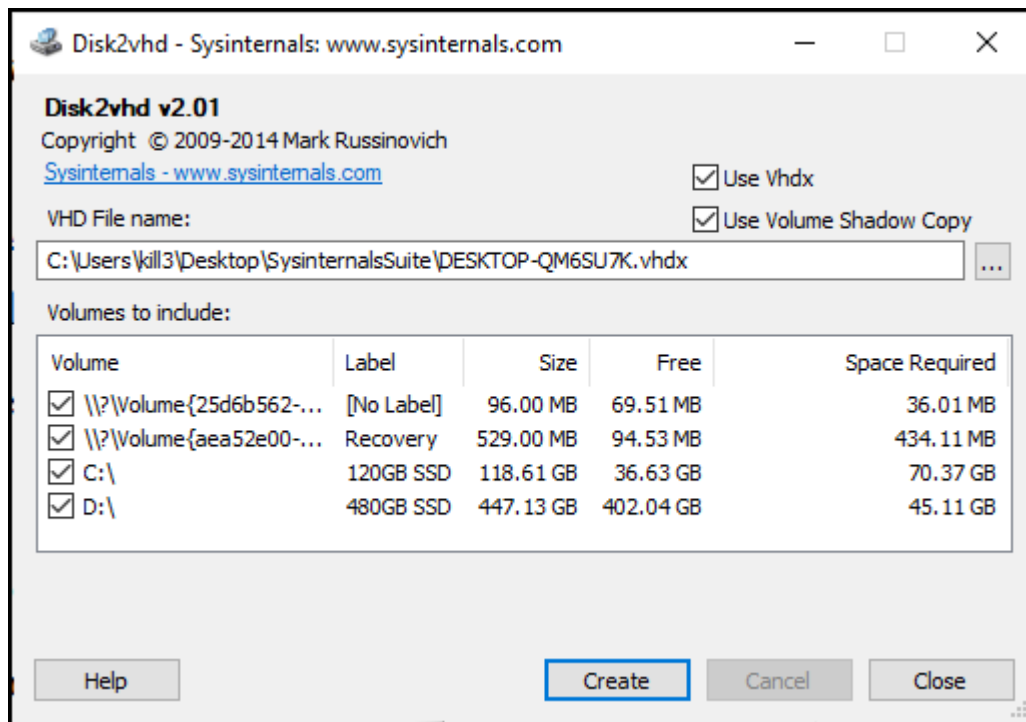


Név: Nagy Róbert

Neptunkód: JMDRGG

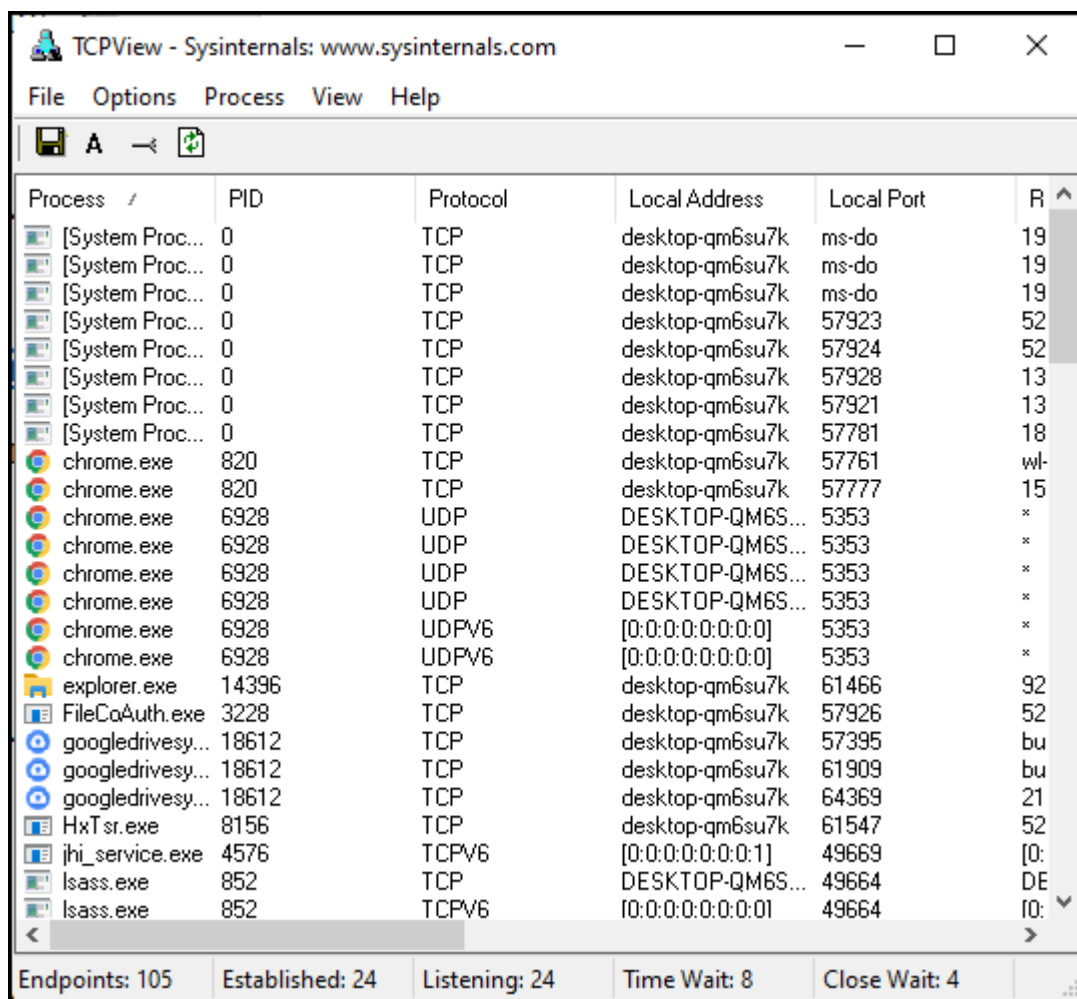
2.) feladat:

1. Disk2vhd



A Disk2vhd program a fizikai diskről vhd disket konvertál. A VHD – Virtual Hard Disk a Microsoft virtuális gép disk formátuma, amelyeket virtuális gépekkel lehet használni. Pl: Microsoft Hyper-V

## 2. TCPView



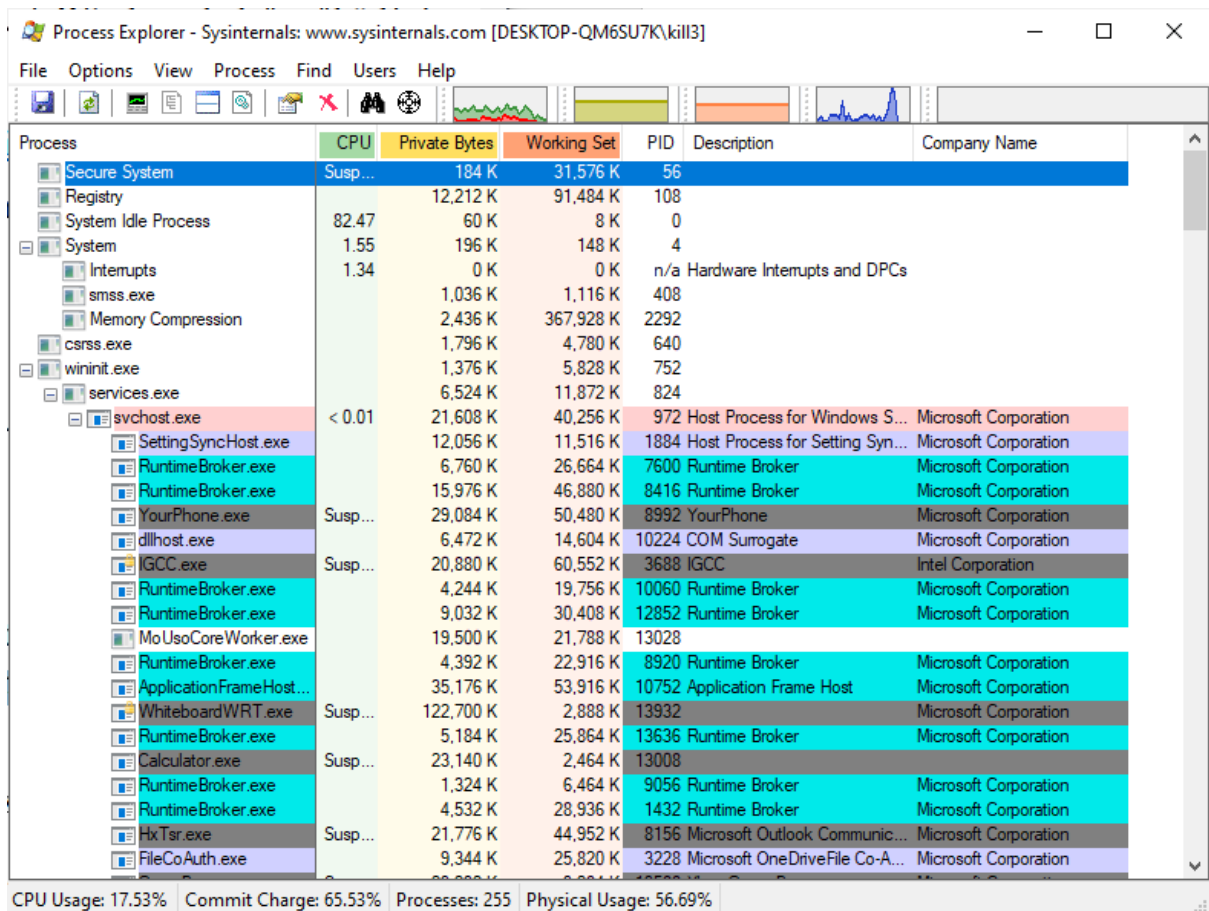
The screenshot shows the TCPView application window with the title bar 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Options', 'Process', 'View', and 'Help'. The toolbar contains icons for saving, printing, and refreshing. The main table displays network connections with columns for Process, PID, Protocol, Local Address, Local Port, and R (Status). The status bar at the bottom shows statistics: Endpoints: 105, Established: 24, Listening: 24, Time Wait: 8, and Close Wait: 4.

Process	PID	Protocol	Local Address	Local Port	R
[System Proc...	0	TCP	desktop-qm6su7k	ms-do	19
[System Proc...	0	TCP	desktop-qm6su7k	ms-do	19
[System Proc...	0	TCP	desktop-qm6su7k	ms-do	19
[System Proc...	0	TCP	desktop-qm6su7k	57923	52
[System Proc...	0	TCP	desktop-qm6su7k	57924	52
[System Proc...	0	TCP	desktop-qm6su7k	57928	13
[System Proc...	0	TCP	desktop-qm6su7k	57921	13
[System Proc...	0	TCP	desktop-qm6su7k	57781	18
chrome.exe	820	TCP	desktop-qm6su7k	57761	wl-
chrome.exe	820	TCP	desktop-qm6su7k	57777	15
chrome.exe	6928	UDP	DESKTOP-QM6S...	5353	*
chrome.exe	6928	UDP	DESKTOP-QM6S...	5353	*
chrome.exe	6928	UDP	DESKTOP-QM6S...	5353	*
chrome.exe	6928	UDP	DESKTOP-QM6S...	5353	*
chrome.exe	6928	UDPV6	[0:0:0:0:0:0:0:0]	5353	*
chrome.exe	6928	UDPV6	[0:0:0:0:0:0:0:0]	5353	*
explorer.exe	14396	TCP	desktop-qm6su7k	61466	92
FileCoAuth.exe	3228	TCP	desktop-qm6su7k	57926	52
googledrivesy...	18612	TCP	desktop-qm6su7k	57395	bu
googledrivesy...	18612	TCP	desktop-qm6su7k	61909	bu
googledrivesy...	18612	TCP	desktop-qm6su7k	64369	21
HxTsr.exe	8156	TCP	desktop-qm6su7k	61547	52
jhi_service.exe	4576	TCPV6	[0:0:0:0:0:0:0:1]	49669	[0:
lsass.exe	852	TCP	DESKTOP-QM6S...	49664	DE
lsass.exe	852	TCPV6	[0:0:0:0:0:0:0:0]	49664	[0:

Endpoints: 105   Established: 24   Listening: 24   Time Wait: 8   Close Wait: 4

A TCPView egy olyan Windows program, amely részletesen megmutatja az összes TCP és UDP végpontokat a rendszeren, beleértve a lokális és távoli címeket és a TCP kapcsolatok státuszát.

### 3. Process Explorer

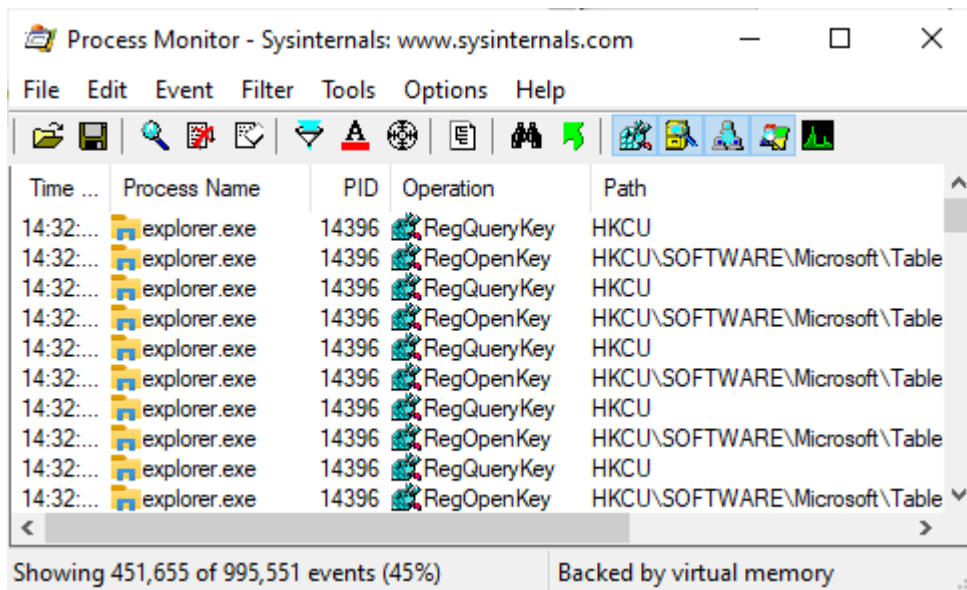


A Process Explorer megmutatja, hogy melyik processznek melyik file vagy directory van megnyitva.

Ezen túl a hardver kihasználtságot is lehet vizsgálni.

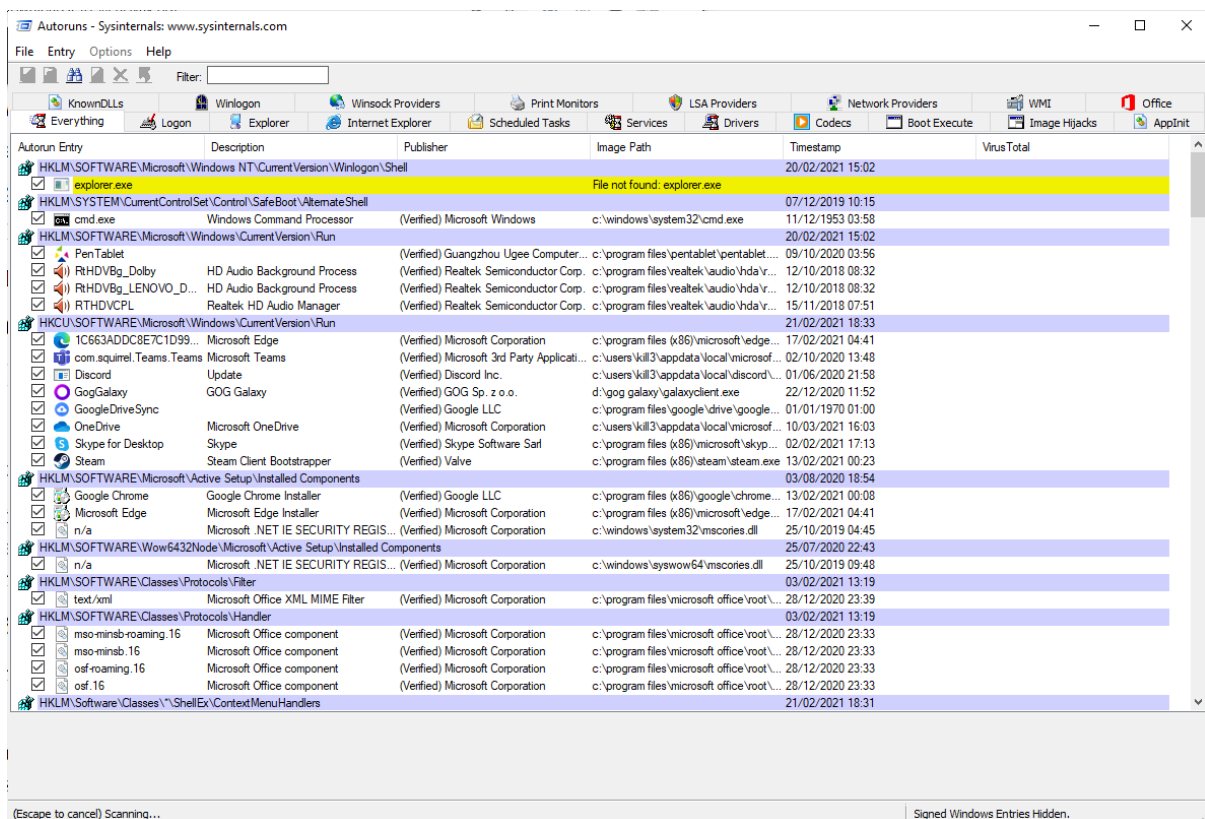


### 3. Process Monitor



A Process Monitor egy olyan eszköz, amely a fájl rendszer, windows registry és a folyamatok / szálak Aktivitását mutatja meg valós időben.

### 4. Autoruns



Az Autoruns egy olyan eszköz, amely az operációs rendszer indításakor és más programok indításakor automatikusan induló programokról mutat meg információkat.

## 5.Logonsessions

```
Administrator Command Prompt
cd SysinternalsSuite
cd ~\Users\kill3\Desktop\SysinternalsSuite
logonsessions.exe

logonsessions v1.48 - Lists Logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003c7:
User name: WORKGROUP\DESKTOP-QH6SU7K$
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: S-1-5-18
Logon time: 20/02/2021 15:02:39
Logon server:
DNS Domain:
UPN:

[1] Logon session 00000000:000003b5:
User name:
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: (none)
Logon time: 20/02/2021 15:02:39
Logon server:
DNS Domain:
UPN:

[2] Logon session 00000000:0000f2a6:
User name: Font Driver Host\UMFD-0
Auth package: Negotiate
Logon type: Interactive
Session: 0
Sid: S-1-5-96-0-0
Logon time: 20/02/2021 15:02:39
Logon server:
DNS Domain:
UPN:

[3] Logon session 00000000:000003e4:
User name: WORKGROUP\DESKTOP-QH6SU7K$
Auth package: Negotiate
Logon type: Service
Session: 0
Sid: S-1-5-20
Logon time: 20/02/2021 15:02:39
Logon server:
DNS Domain:
UPN:

[4] Logon session 00000000:00015dae:
User name: Font Driver Host\UMFD-1
Auth package: Negotiate
Logon type: Interactive
Session: 1
Sid: S-1-5-96-0-1
Logon time: 20/02/2021 15:02:40
Logon server:
DNS Domain:
UPN:
```

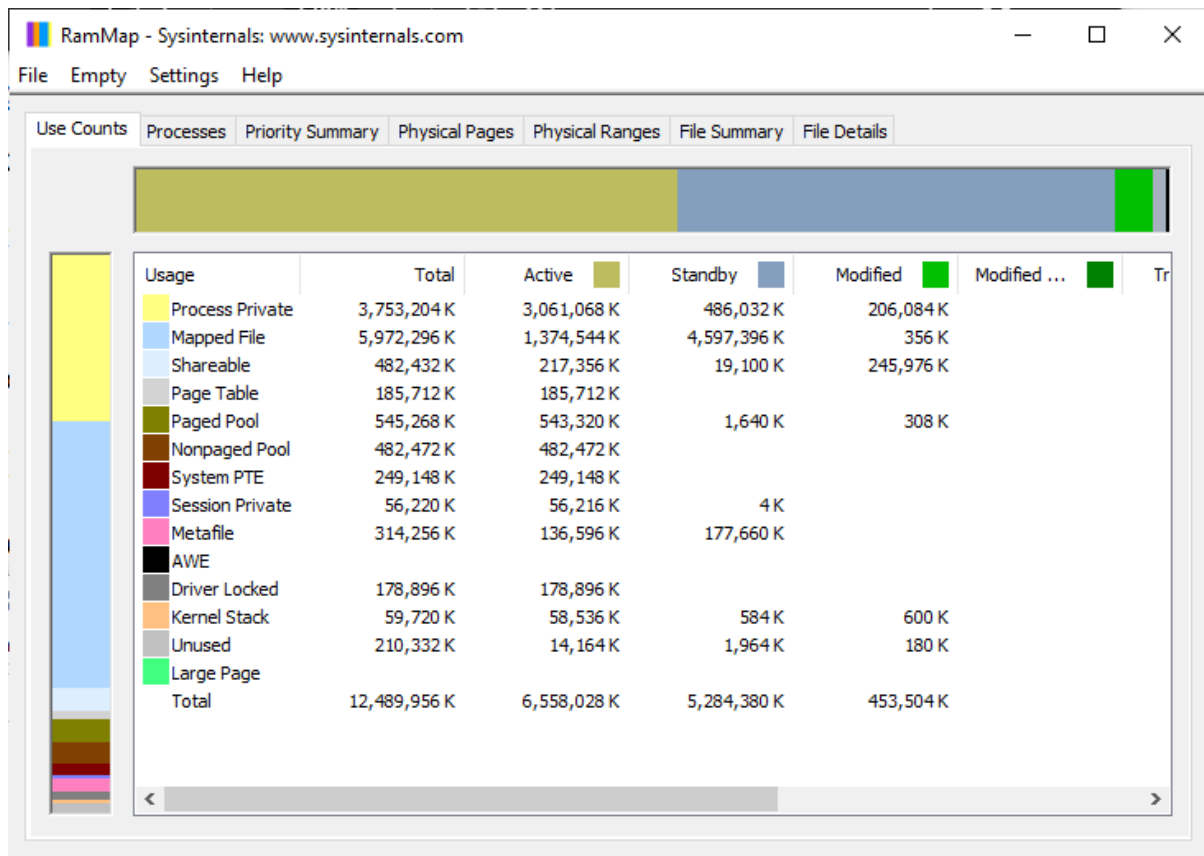
A logonsessions egy olyan program, amely megmutatja az aktív sessionokat és a -p flag használatával a különböző sessionok folyamatait kilistázza.

```
Administrator Command Prompt

Logon server:
DNS Domain:
UPN:
4988: OpenHardwareMonitor.exe
5272: taskhostw.exe
21602: cmd.exe
17568: conhost.exe
10344: logonsessions.exe

[0] Logon session 00000000:00025440:
User name: DESKTOP-QH6SU7K\kill3
Auth package: CloudAP
Logon type: Interactive
Session: 1
Sid: S-1-5-21-1331135437-2888005139-2733254555-1001
Logon time: 20/02/2021 15:02:41
Logon server:
DNS Domain:
UPN:
4556: ETDCtrl.exe
4768: slhost.exe
4864: svchost.exe
5080: svchost.exe
4752: taskhostw.exe
5344: lsass.exe
5672: ETDPouch.exe
5808: svchost.exe
6240: svchost.exe
1884: SettingSyncHost.exe
7600: RuntimeBroker.exe
8416: RuntimeBroker.exe
8992: YourPhone.exe
9080: ctfmon.exe
6928: chrome.exe
1156: chrome.exe
6596: chrome.exe
820: chrome.exe
9348: chrome.exe
9568: chrome.exe
9640: chrome.exe
9672: chrome.exe
9856: chrome.exe
10024: chrome.exe
10224: dillhost.exe
10280: chrome.exe
6424: chrome.exe
10304: chrome.exe
10360: chrome.exe
10392: chrome.exe
8612: SecurityHealthSystray.exe
8720: AVG64.exe
11296: AVG64.exe
11536: AVG64.exe
11776: OneDrive.exe
11464: EarTrumpet.exe
1460: OneDrive.exe
4072: OneDrive.exe
3688: ICCC.exe
10608: RuntimeBroker.exe
12852: RuntimeBroker.exe
8920: RuntimeBroker.exe
10752: ApplicationFramework.exe
13932: WhiteboardMT.exe
12616: RuntimeBroker.exe
```

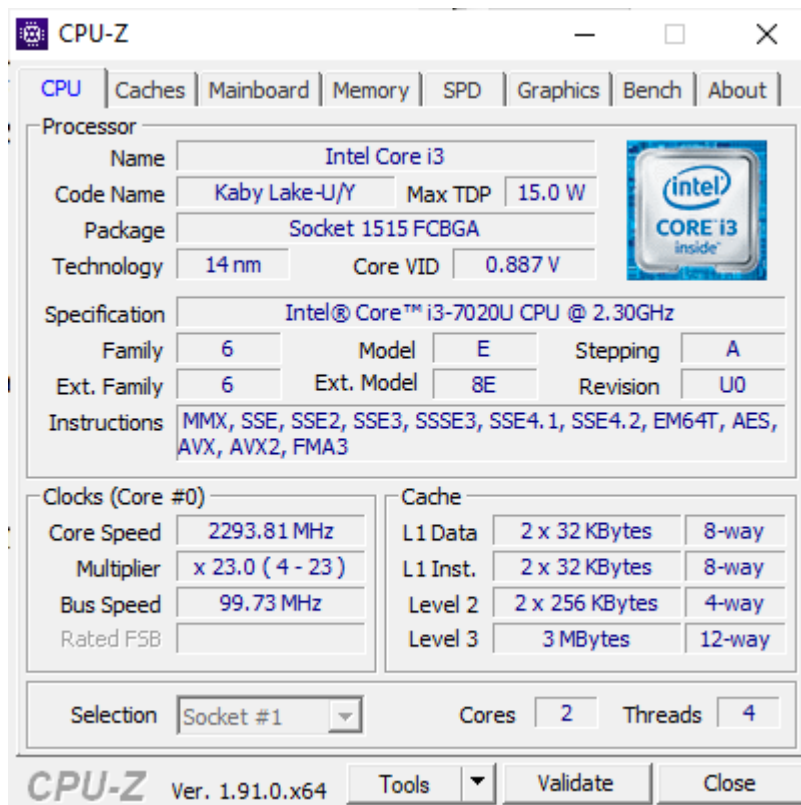
## 6. RAMMap



A RAMMap megmutatja, hogy a windows mennyi fizikai memóriát használ, mennyi adat van becacheleve a memóriába, vagy, hogy mennyi memóriát használ a kernel vagy a device driverek.

3.)

### 1. CPU-Z

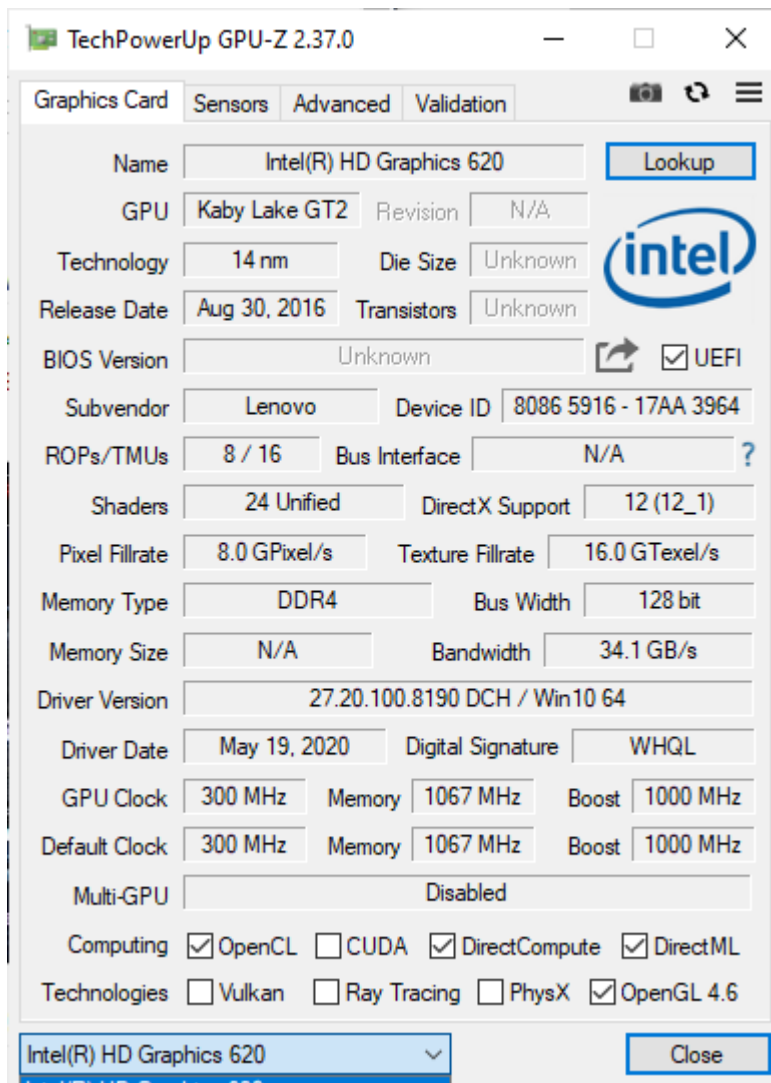


A cpu-z Információt gyűjt a rendszer legfontosabb eszközeiről mint pl: alaplapp, chipset, memória.

Valós időben lehet a processzor sebességet és frekvenciát, memória frekvenciát lekérdezni.

Stressztesztelni lehet a számítógépet.

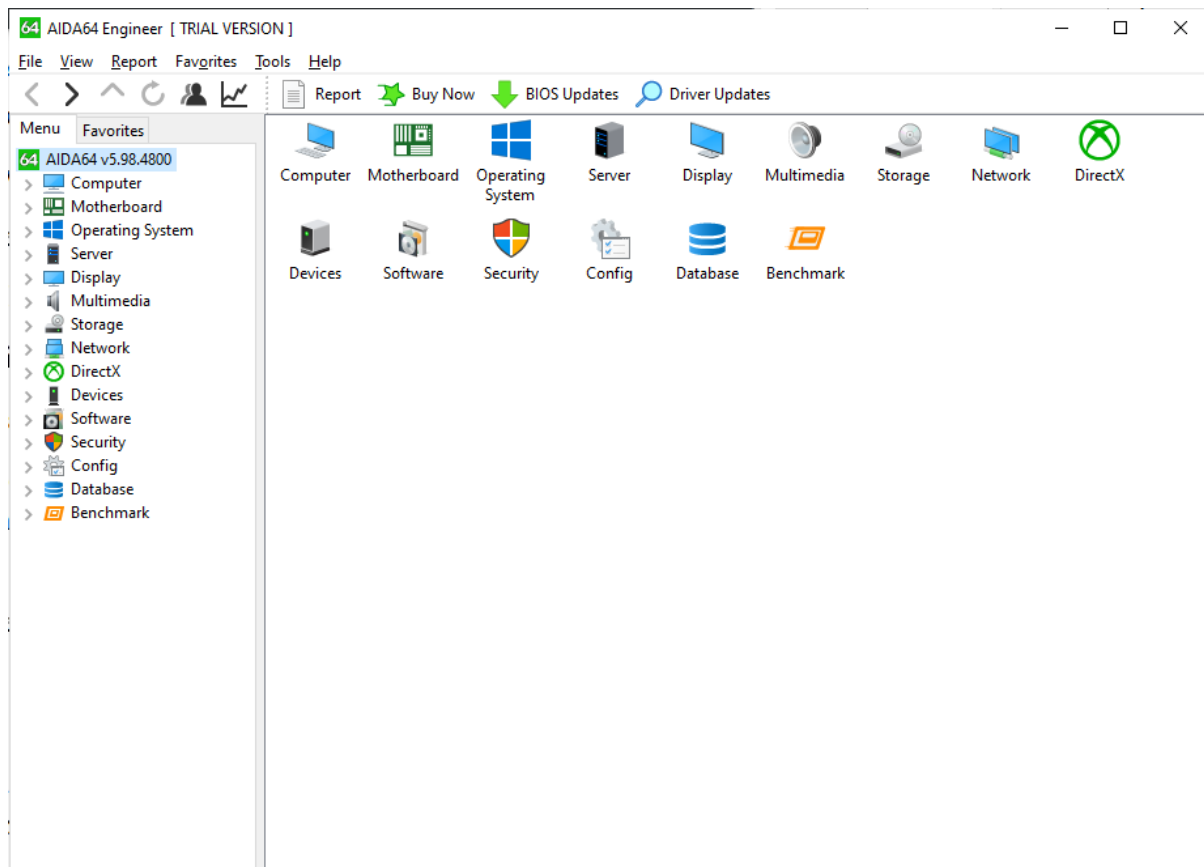
## 2. GPU-Z



A gpu-z megmutatja a számítógép videokártyájának a tulajdonságait és a videokártya szenzorok értékeit.



### 3. AIDA64 Engineer



Részletes információt tartalmaz a rendszerről és diagnosztikai funkciókkal rendelkezik

Vizsgálat eredménye:

#### AIDA64 Engineer

Navigation

Version: AIDA64 v5.98.4800  
Benchmark Module: 4.3.784-x64  
Homepage: <http://www.aida64.com/>  
Report Type: Report Wizard [ TRIAL VERSION ]  
Computer: DESKTOP-QM6SU7K  
Generator: kill3  
Operating System: Microsoft Windows 10 Home 10.0.19042.804  
Date: 2021-02-23  
Time: 15:14

#### Summary

**Computer:**  
Computer Type: ACPI x64-based PC (Mobile)  
Operating System: [Microsoft Windows 10 Home](#)  
OS Service Pack: [ TRIAL VERSION ]  
Internet Explorer: [11.789.19041.0](#)  
Edge: [44.19041.423.0](#)  
DirectX: [DirectX 12.0](#)  
Computer Name: DESKTOP-QM6SU7K  
User Name: kill3  
Logon Domain: [ TRIAL VERSION ]  
Date / Time: 2021-02-23 / 15:14

**Motherboard:**  
CPU Type: [DualCore Intel Core i3-7020U, 2300 MHz \(23 x 100\)](#)  
Motherboard Name: [Lenovo Ideapad 330-15IKB](#)  
Motherboard Chipset: [Intel Sunrise Point-LP, Intel Kaby Lake-U](#)  
System Memory: [ TRIAL VERSION ]  
DIMM3: [ TRIAL VERSION ]  
BIOS Type: Unknown (10/16/2018)

**Display:**