

3A Feladatok

1. Feladat

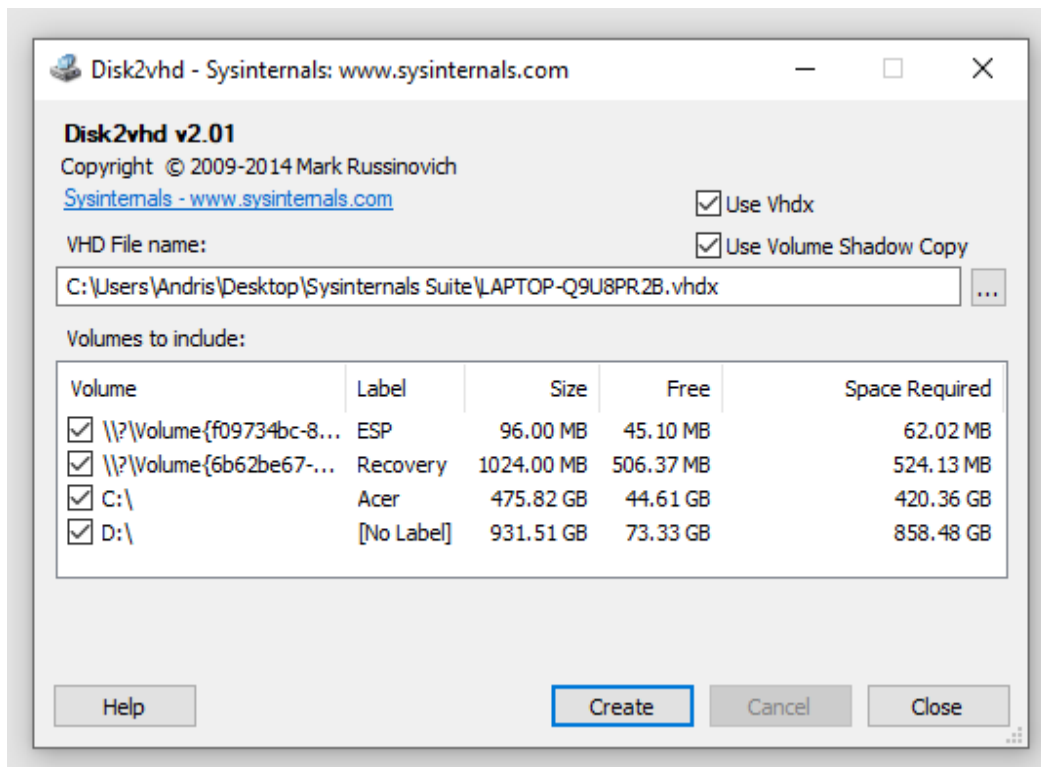
Sysinternals Suite letöltve.

2. Feladat

a. Disk2vhd

A program egy fizikai lemezből képes virtuális merevlemez (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:

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address
[System Proc...	0	TCP	laptop-q9u8pr2b	61336	bud02s23-in-f1
[System Proc...	0	TCP	laptop-q9u8pr2b	61368	52.109.28.63
[System Proc...	0	TCP	laptop-q9u8pr2b	61344	server-52-85-1:
[System Proc...	0	TCP	laptop-q9u8pr2b	61375	server-52-85-1:
[System Proc...	0	TCP	laptop-q9u8pr2b	61376	server-52-85-1:
[System Proc...	0	TCP	laptop-q9u8pr2b	61377	server-52-85-1:
[System Proc...	0	TCP	laptop-q9u8pr2b	61379	server-52-85-1:
[System Proc...	0	TCP	laptop-q9u8pr2b	61380	server-52-85-1:
[System Proc...	0	TCP	laptop-q9u8pr2b	54246	192.168.43.1
[System Proc...	0	TCP	laptop-q9u8pr2b	61397	a23-47-213-17:
[System Proc...	0	TCP	laptop-q9u8pr2b	61391	a23-47-213-17:
[System Proc...	0	TCP	laptop-q9u8pr2b	61395	a92-123-213-1:
app_updater...	4964	TCP	LAPTOP-Q9U8PR...	45777	LAPTOP-Q9U8PR...
brave.exe	15388	TCP	laptop-q9u8pr2b	58846	192.168.43.75
brave.exe	15388	TCP	laptop-q9u8pr2b	61260	192.168.43.75
brave.exe	15388	TCP	laptop-q9u8pr2b	61309	instagram-p3-s:
brave.exe	15388	TCP	laptop-q9u8pr2b	61327	edge-star-shv-
brave.exe	15388	TCP	laptop-q9u8pr2b	61331	lb-140-82-114-
brave.exe	5544	UDP	LAPTOP-Q9U8PR...	5353	*
brave.exe	5544	UDP	LAPTOP-Q9U8PR...	5353	*
brave.exe	15388	UDP	LAPTOP-Q9U8PR...	53773	*
brave.exe	15388	UDP	LAPTOP-Q9U8PR...	60520	*

Endpoints: 180 Established: 43 Listening: 28 Time Wait: 12 Close Wait: 28

c. Process Explorer, Process Monitor, AutoRuns

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

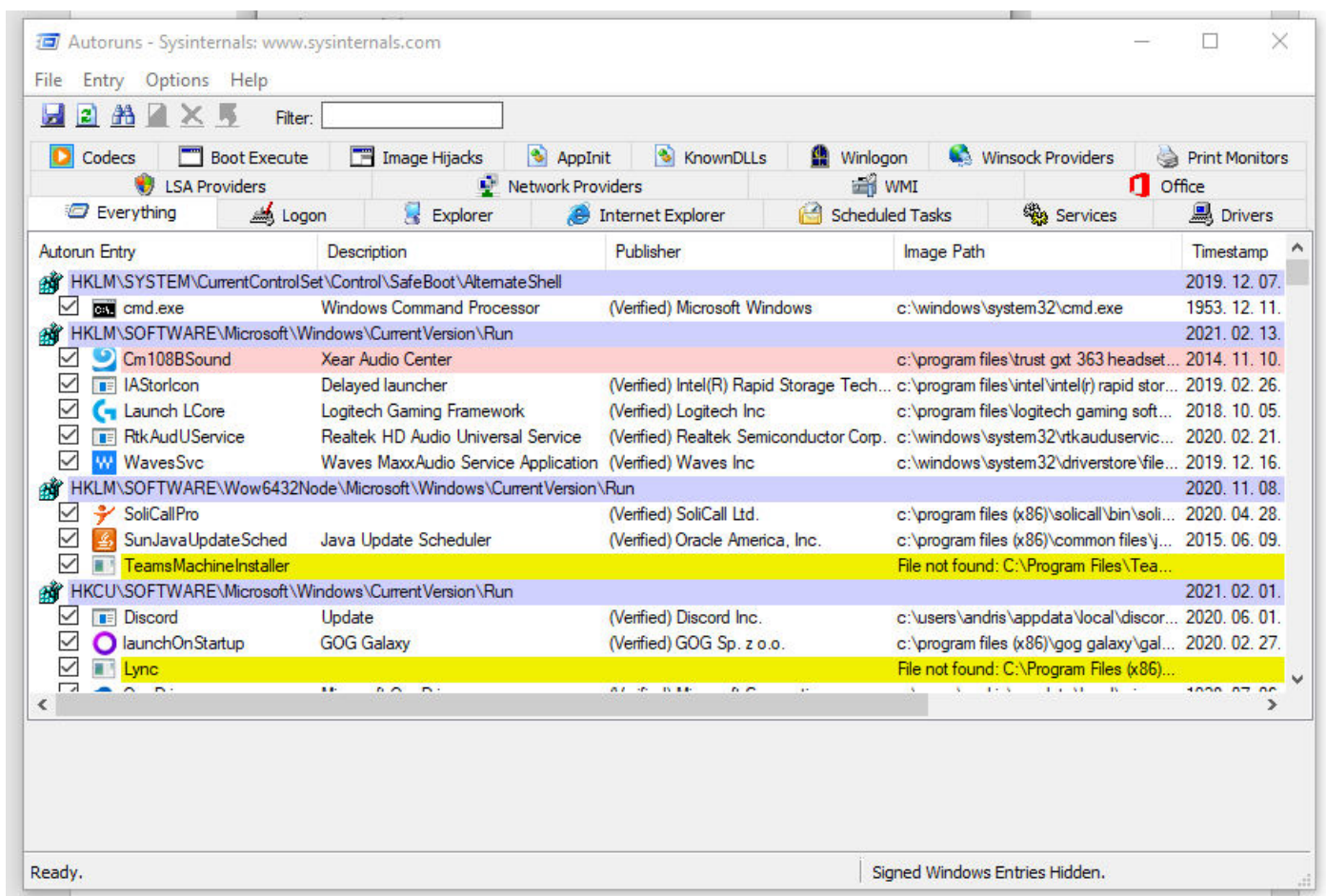
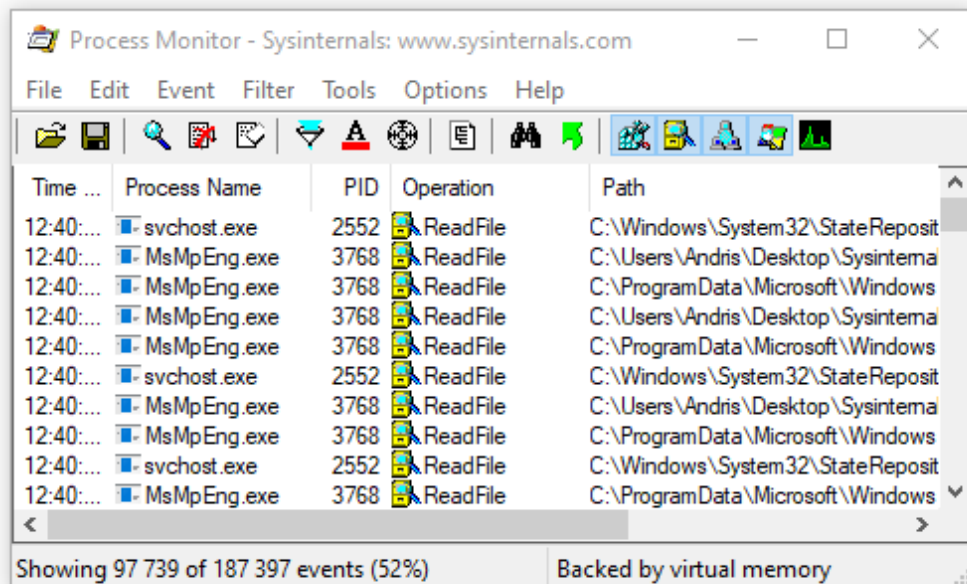
A programok így néznek ki futás közben:

Process Explorer - Sysinternals: www.sysinternals.com [LAPTOP-Q9U8PR2B\Andris]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		12 336 K	52 816 K	148		
System Idle Process	93.60	60 K	8 K	0		
System	0.19	216 K	4 800 K	4		
Interrupts	0.40	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 032 K	492 K	572		
Memory Compression	< 0.01	1 580 K	541 396 K	2908		
csrss.exe	< 0.01	2 288 K	2 620 K	824		
wininit.exe		2 100 K	2 796 K	1008		
services.exe		7 668 K	7 624 K	852		
svchost.exe	< 0.01	23 940 K	31 880 K	1132	Windows-szolgáltatások gaz...	Microsoft Corporation
WmiPrvSE.exe		4 000 K	7 708 K	4156		
dllhost.exe		3 480 K	3 648 K	15988		
MoUsCoreWorker.exe		20 708 K	17 004 K	14380		
SettingSyncHost.exe	< 0.01	10 388 K	8 404 K	9664	Host Process for Setting Syn...	Microsoft Corporation
StartMenuExperience...		40 808 K	93 708 K	16624		
RuntimeBroker.exe		6 632 K	26 236 K	14112	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	149 688 K	98 016 K	14284	Search application	Microsoft Corporation
RuntimeBroker.exe	< 0.01	7 656 K	29 936 K	11700	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	27 188 K	2 152 K	12564	YourPhone	Microsoft Corporation
LockApp.exe	Susp...	13 192 K	46 500 K	18860	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		3 152 K	15 744 K	13920	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		9 184 K	32 796 K	11192	Runtime Broker	Microsoft Corporation
YourPhoneServer.exe	< 0.01	44 056 K	50 852 K	8048		
RuntimeBroker.exe		2 752 K	13 988 K	12520	Runtime Broker	Microsoft Corporation
dllhost.exe		5 320 K	13 488 K	17692	COM Surrogate	Microsoft Corporation
TextInputHost.exe	0.01	12 900 K	45 180 K	1124		Microsoft Corporation
SystemSettings.exe	Susp...	24 760 K	3 048 K	5572	Gépház	Microsoft Corporation
ApplicationFrameHost...		28 584 K	36 396 K	10124	Application Frame Host	Microsoft Corporation
UserOOBEBroker.exe		1 936 K	8 892 K	16112	User OOBEBroker	Microsoft Corporation

CPU Usage: 6.40% Commit Charge: 77.16% Processes: 269 Physical Usage: 62.83%



d. LogonSession

A program kilistázza a bejelentkezési sessionöket. A parancssorban futtattam, re ndszergazdai 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:

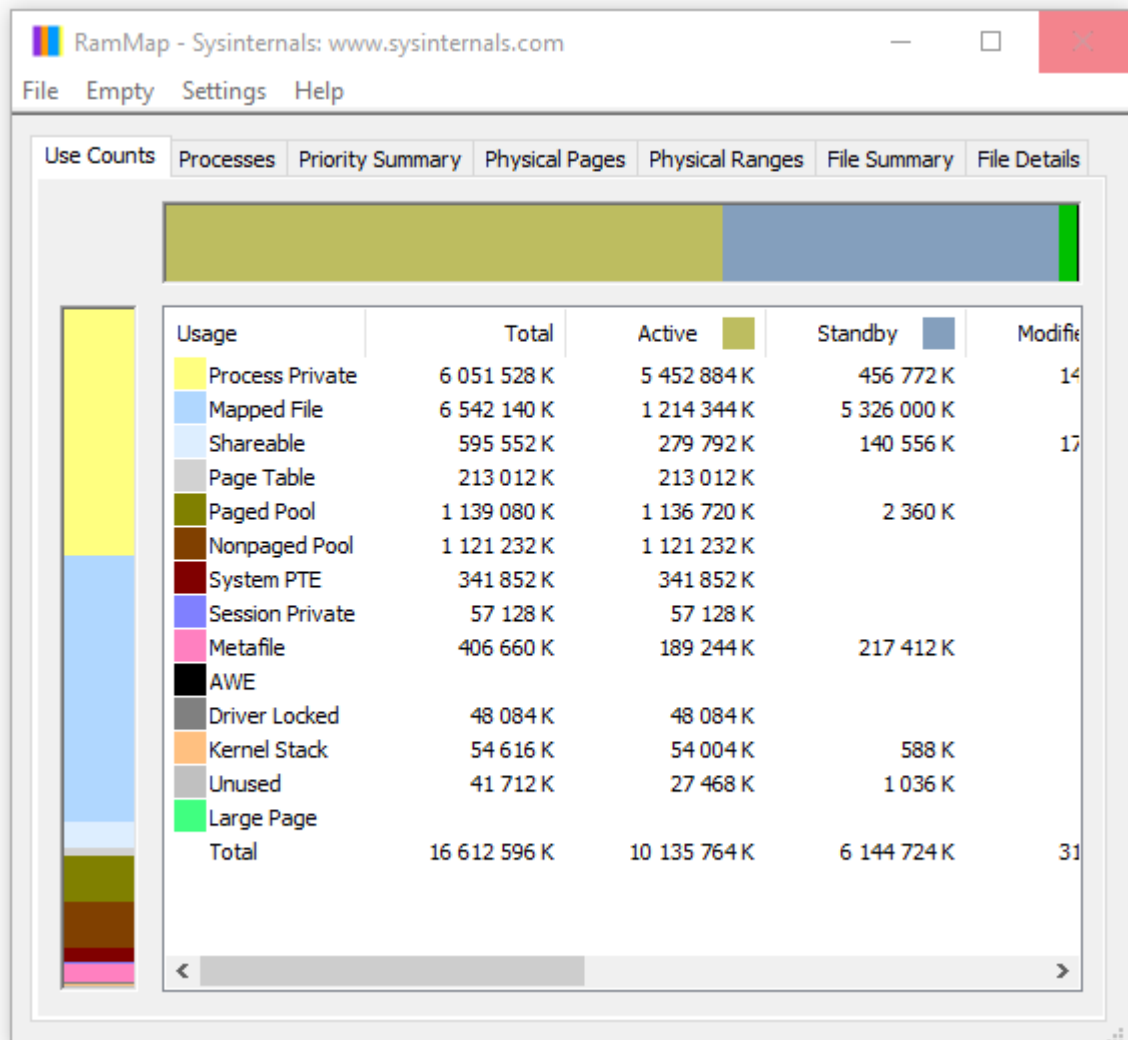
[1] Logon session 00000000:000142d4:
  User name:
  Auth package: NTLM
  Logon type: (none)
  Session: 0
  Sid: (none)
  Logon time: 2021. 02. 12. 15:01:59

```

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

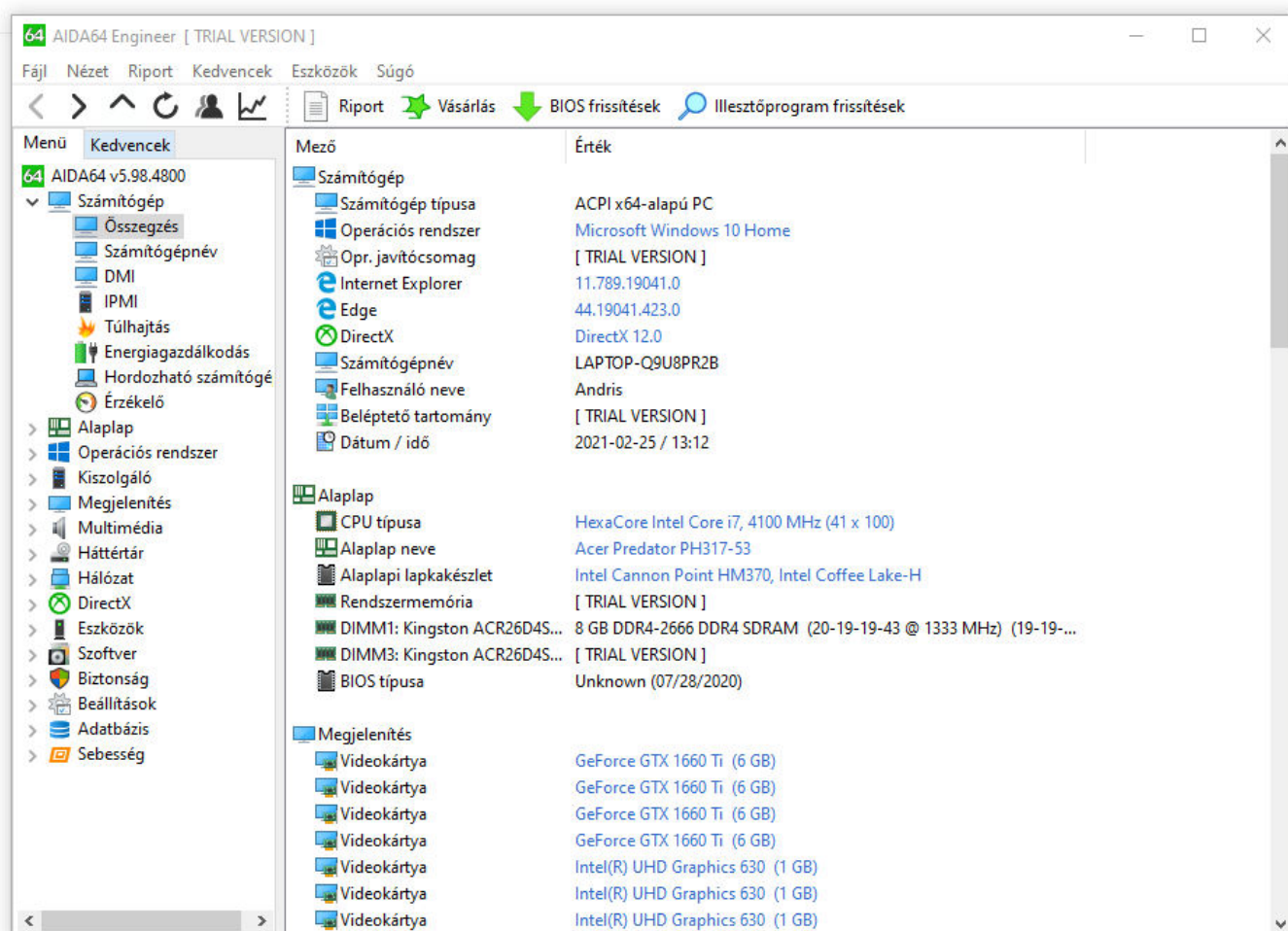
267C: File C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.746_none_ca02b
4b61b8320a4
2684: File C:\Users\Andris\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\IndexedDB\https_www.you
tube.com_0.indexeddb.leveldb\001420.ldb
26EC: Section \Sessions\15\BaseNamedObjects\15a8HwndInterface:50272
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

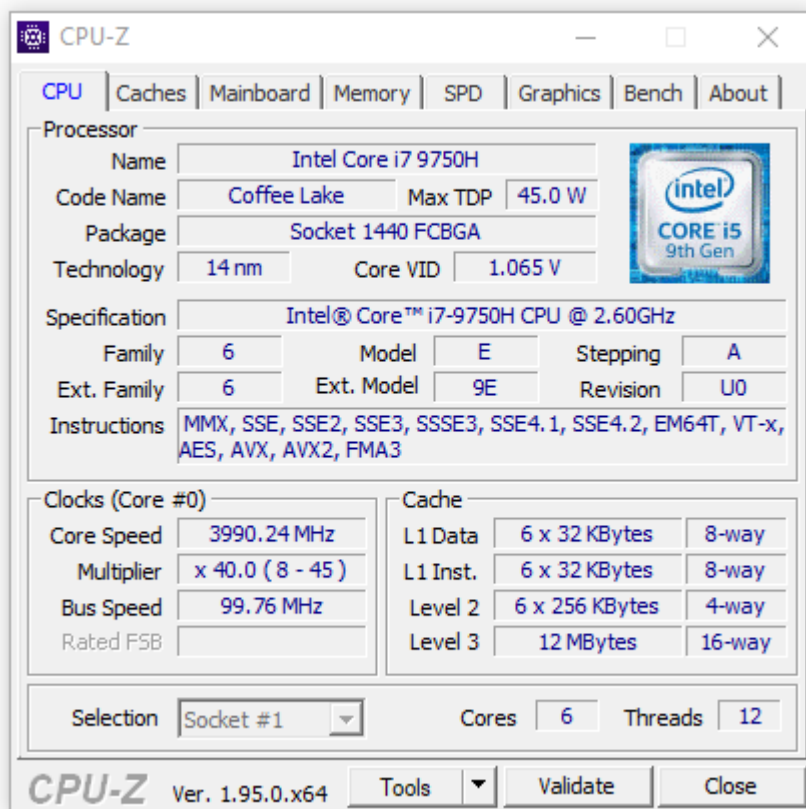
AIDA64 Engineer

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:



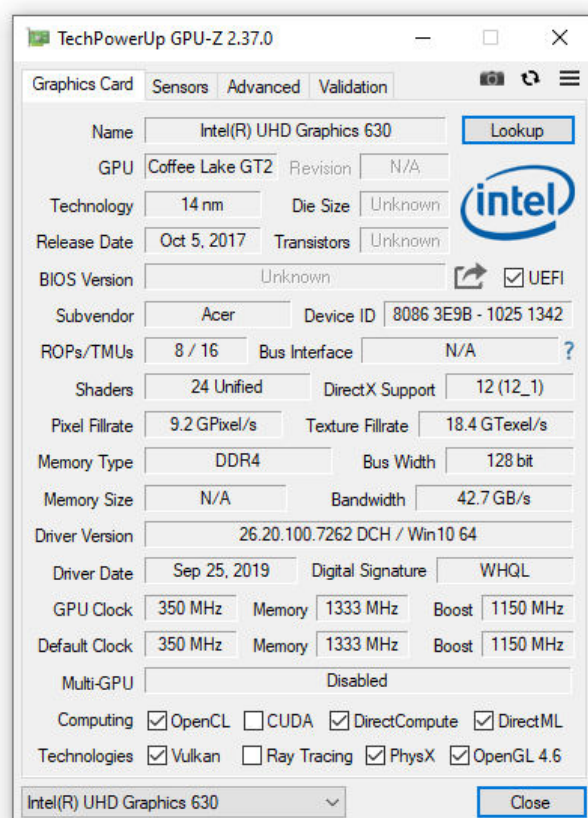
Az alkalmazás nagyon hasznos, információt jelenít meg a rendszerről, hardverről, például processzor neve, típusa, különböző folyamatok, memória típusa, mérete, valamint egyéb, hozzájuk kapcsolódó adatokról. A program így néz ki futás közben:



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