

Operációs rendszerek BSc

3. gyakorlat

2021.02.25.

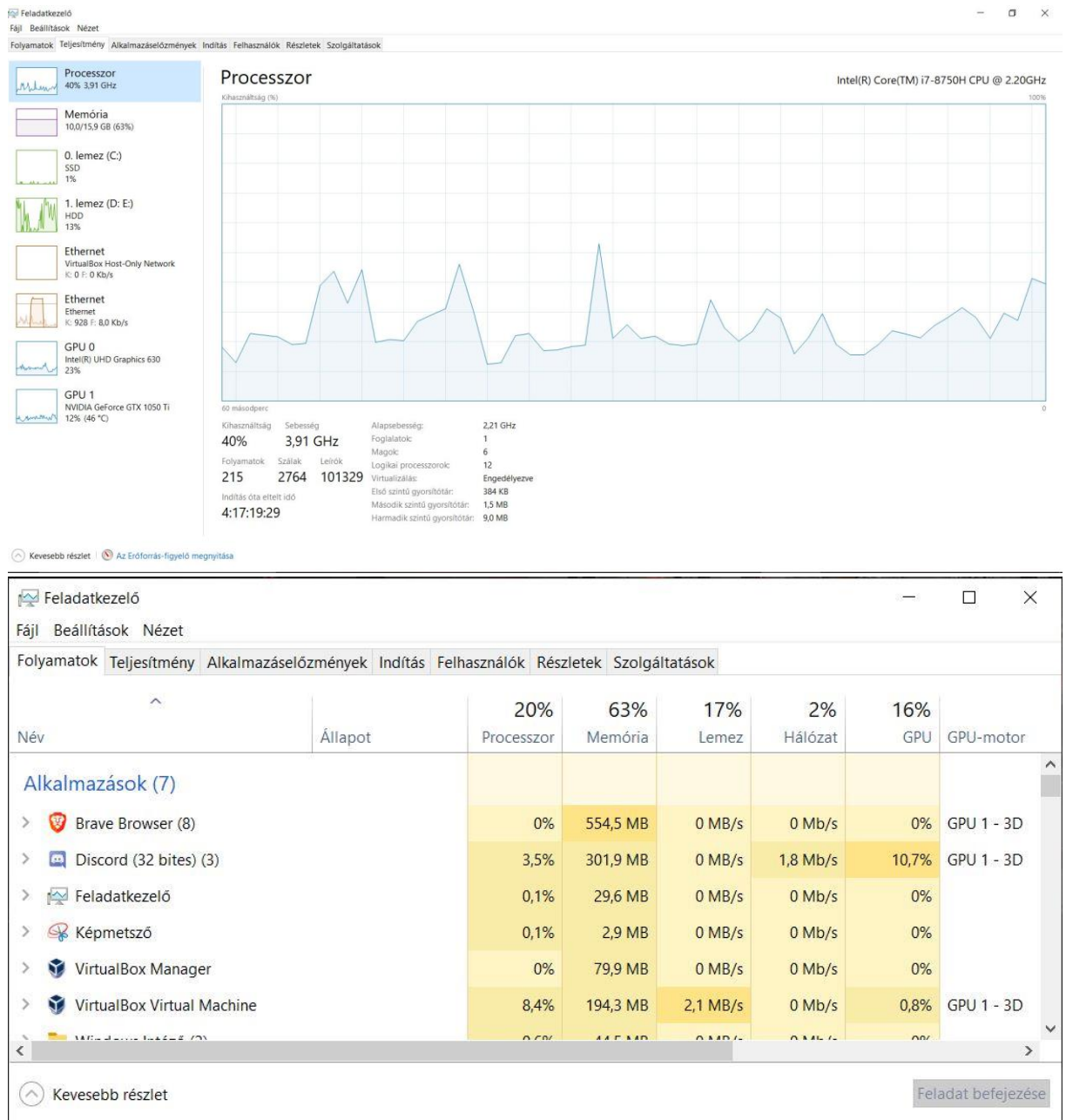
Készítette:

Csősz Péter BSc

Programtervező informatikus

NORS38

1. feladat: Windows belső működésének tanulmányozása



2.Feladat: A Sysinternals Suite programcsomag tanulmányozása.

a, File and Disk Utilities (Disk2vhd)

Nem indul el.

b, Networking Utilities (TCPView)

TCPView - Sysinternals: www.sysinternals.com

FileOptionsProcessViewHelp

Process / PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
System Proc... 0	TCP	desktop-j90kbf.t	58276	51.195.68.172	http	TIME_W
System Proc... 0	TCP	desktop-j90kbf.t	58272	140.82.121.5	http	TIME_W
brave.exe 9636	TCP	desktop-j90kbf.t	58285	140.82.121.25	ESTABL	ESTABL
brave.exe 9636	TCP	desktop-j90kbf.t	58271	172.217.18.69	https	ESTABL
brave.exe 9636	UDP	DESKTOP-JE90K	5353	*	*	*
brave.exe 9636	UDP	DESKTOP-JE90K	5353	*	*	*
brave.exe 9252	UDP	DESKTOP-JE90K	5353	*	*	*
brave.exe 9252	UDP	DESKTOP-JE90K	5353	*	*	*
brave.exe 9636	UDP	DESKTOP-JE90K	5353	*	*	*
brave.exe 9636	UDP	DESKTOP-JE90K	55727	*	*	*
brave.exe 9636	UDP	DESKTOP-JE90K	57241	*	*	*
brave.exe 9636	UDP	DESKTOP-JE90K	5353	*	*	*
brave.exe 9252	UDP	DESKTOP-JE90K	5353	*	*	*
brave.exe 9252	UDPV6	[0.0.0.0.0.0.0]	5353	*	*	*
brave.exe 9636	UDPV6	[0.0.0.0.0.0.0]	5353	*	*	*
brave.exe 9636	UDP	DESKTOP-JE90K	51272	[0.0.0.0.0.0.0]	LISTEN	LISTEN
PL-service.exe 4656	TCFV6	[0.0.0.0.0.0.1]	49669	DESKTOP-JE90K	0	LISTEN
lsass.exe 964	TCPV6	DESKTOP-JE90K	49664	[0.0.0.0.0.0.0]	0	LISTEN
lsass.exe 964	TCFV6	[0.0.0.0.0.0.0]	49664	[0.0.0.0.0.0.0]	0	LISTEN
nvcontainer.exe 4804	TCP	DESKTOP-JE90K	56879	localhost	65001	ESTABL
nvcontainer.exe 4804	TCP	DESKTOP-JE90K	65001	DESKTOP-JE90K	0	LISTEN
nvcontainer.exe 4804	TCP	DESKTOP-JE90K	65001	localhost	56879	ESTABL
nvcontainer.exe 4804	UDP	desktop-j90kbf.t	5353	*	*	*
nvcontainer.exe 4804	UDP	192.168.56.1	5353	*	*	*
nvcontainer.exe 5824	UDP	DESKTOP-JE90K	58040	*	*	*
nvcontainer.exe 4804	UDP	DESKTOP-JE90K	58526	*	*	*
nvcontainer.exe 4804	UDPV6	[0.0.0.0.0.0.1]	5353	*	*	*
nvcontainer.exe 4804	UDPV6	[0.0.0.0.0.0.0]	58527	*	*	*
NVIDIA Share... 10008	TCP	DESKTOP-JE90K	56363	localhost	56322	ESTABL
NVIDIA Web... 6588	TCP	DESKTOP-JE90K	56322	DESKTOP-JE90K	0	LISTEN
NVIDIA Web... 6588	UDP	DESKTOP-JE90K	56322	localhost	56363	ESTABL
NVIDIA Web... 6588	TCP	DESKTOP-JE90K	10060	*	*	*
OriginWebHel... 4300	TCP	DESKTOP-JE90K	3213	DESKTOP-JE90K	0	LISTEN
OriginWebHel... 4300	UDP	DESKTOP-JE90K	54371	*	*	*
PhkBotA.exe 4848	UDP	DESKTOP-JE90K	44301	*	*	*
SearchApp.exe 4768	TCP	desktop-j90kbf.t	57793	152.199.19.161	https	LAST_AC
SearchApp.exe 4768	TCP	desktop-j90kbf.t	57824	152.199.19.161	https	LAST_AC
SearchApp.exe 4768	TCP	desktop-j90kbf.t	57835	152.199.19.161	https	LAST_AC
SearchApp.exe 4768	TCP	desktop-j90kbf.t	58289	204.79.197.200	https	ESTABL
SearchApp.exe 4768	TCP	desktop-j90kbf.t	58294	40.101.7.162	https	ESTABL
SearchApp.exe 4768	TCP	desktop-j90kbf.t	58295	13.107.6.158	https	ESTABL
SearchApp.exe 4768	TCP	desktop-j90kbf.t	58296	13.107.6.158	https	ESTABL
SearchApp.exe 4768	TCP	desktop-j90kbf.t	58297	52.114.128.75	https	ESTABL
SearchApp.exe 4768	TCP	desktop-j90kbf.t	58298	136.167.250	https	ESTABL
SearchApp.exe 4768	TCP	desktop-j90kbf.t	58299	137.128.254	https	ESTABL
services.exe 872	TCP	DESKTOP-JE90K	49677	DESKTOP-JE90K	0	LISTEN
services.exe 872	TCFV6	[0.0.0.0.0.0.0]	49677	[0.0.0.0.0.0.0]	0	LISTEN
Skype.exe 2184	TCP	desktop-j90kbf.t	57799	13.69.188.18	https	ESTABL
Skype.exe 14860	TCP	desktop-j90kbf.t	58128	40.74.213.49	https	ESTABL

Endpoints: 156Established: 44Listening: 27Time Wait: 2Close Wait: 18

TCPView v3.01 - TCP/UDP endpoint viewer

Copyright (C) 1998-2010 Mark Russinovich and Bryce Cogswell

Sysinternals - www.sysinternals.com

TCP

nvcontainer.exe

PID: 4804

State: ESTABLISHED

Local: DESKTOP-JE90KBF

Remote: localhost

svchost.exe

PID: 9068

State: ESTABLISHED

Local: desktop-j90kbf.t

Remote: 51.103.5.159

NVIDIA Web Helper.exe

PID: 6588

State: ESTABLISHED

Local: DESKTOP-JE90KBF

Remote: localhost

NVIDIA Share.exe

PID: 10008

State: EST

c, Process Explorer v16.32

Process Monitor

Process Monitor - Sysinternals: www.sysinternals.com

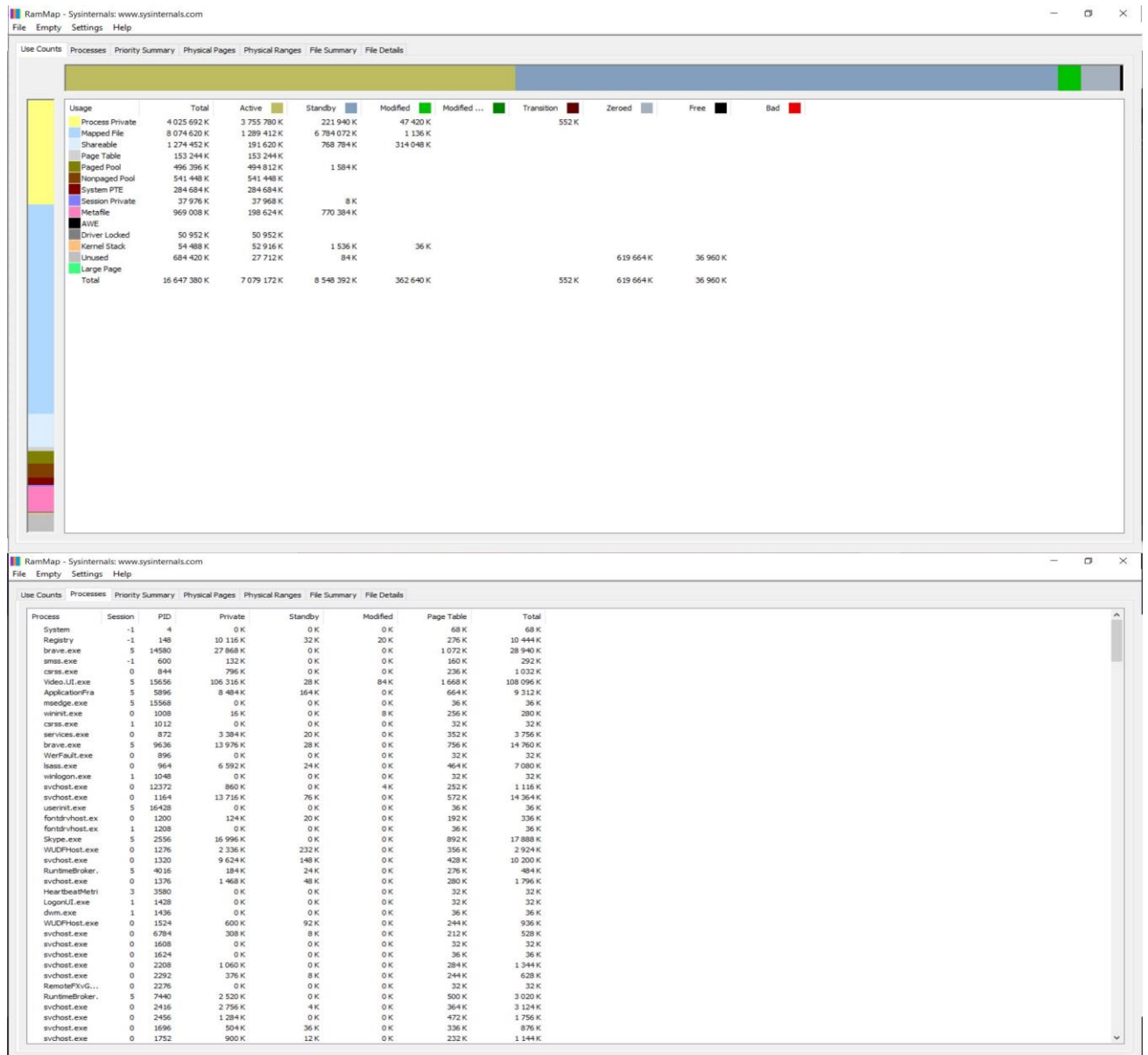
Time o...	Process Name	PID	Operation	Path	Result	Detail
17:31:38	svchost.exe	2560	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset 690 688, Len...
17:31:38	svchost.exe	2560	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset 678 400, Len...
17:31:38	svchost.exe	2560	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset 635 904, Len...
17:31:38	svchost.exe	2560	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset 623 616, Len...
17:31:38	Explorer.EXE	4940	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query Name
17:31:38	Explorer.EXE	4940	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query Handle Tag...
17:31:38	Explorer.EXE	4940	RegOpenKey	HKCU\Software\Classes\Applications\Pr...	NAME NOT FOUND	Desired Access: R...
17:31:38	Explorer.EXE	4940	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
17:31:38	svchost.exe	2560	LockFile	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Exclusive False, Of...
17:31:38	svchost.exe	2560	QueryStandardI...	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	AllocationSize: 6 29...
17:31:38	Explorer.EXE	4940	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query Handle Tag...
17:31:38	svchost.exe	2560	QueryStandardI...	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	AllocationSize: 6 29...
17:31:38	Explorer.EXE	4940	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query Name
17:31:38	svchost.exe	2560	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Offset 123, Length: 1
17:31:38	Explorer.EXE	4940	RegOpenKey	HKCU\Software\Classes\Applications\Pr...	NAME NOT FOUND	Desired Access: R...
17:31:38	Explorer.EXE	4940	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
17:31:38	cdmon.exe	17360	ReadFile	C:\Windows\System32\inputService.dll	SUCCESS	Offset 4 088 320, Le...
17:31:38	Explorer.EXE	4940	CreateFile	C:\Users\Peter\AppData\Local\Temp\Pi...	SUCCESS	Desired Access: R...
17:31:38	Explorer.EXE	4940	QueryBasicInfor...	C:\Users\Peter\AppData\Local\Temp\Pi...	SUCCESS	CreationTime: 2021...
17:31:38	Explorer.EXE	4940	CreateFile	C:\Users\Peter\AppData\Local\Temp\Pi...	SUCCESS	Desired Access: R...
17:31:38	cdmon.exe	17360	RegOpenKey	HKCU	SUCCESS	Query Handle Tag...
17:31:38	Explorer.EXE	4940	CloseFile	C:\Users\Peter\AppData\Local\Temp\Pi...	SUCCESS	
17:31:38	cdmon.exe	17360	RegOpenKey	HKCU\Software\Microsoft\InputSettings	SUCCESS	Desired Access: R...
17:31:38	cdmon.exe	17360	RegOpenKey	HKLM	SUCCESS	Query Handle Tag...
17:31:38	cdmon.exe	17360	RegOpenKey	HKLM\SOFTWARE\Microsoft\InputSett...	SUCCESS	Desired Access: Q...
17:31:38	cdmon.exe	17360	RegOpenKey	HKLM\SOFTWARE\Microsoft\InputSett...	SUCCESS	Desired Access: R...
17:31:38	svchost.exe	2560	QueryStandardI...	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	AllocationSize: 6 29...
17:31:38	cdmon.exe	17360	RegQueryValue	HKLM\SOFTWARE\Microsoft\InputSett...	SUCCESS	Type: REG_DWORD...
17:31:38	svchost.exe	2560	ReadFile	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Offset 3 137 536, Le...
17:31:38	MsMpEng.exe	4924	FileSystemCont...	C:\Windows\System32\wbem\wbemprox...	OPLOCK HANDLE	Control FSCTL_RE...
17:31:38	MsMpEng.exe	4924	CreateFile	C:\Windows\System32\wbem\wbemprox...	SUCCESS	Control 0x0020b (D...
17:31:38	cdmon.exe	17360	RegOpenKey	HKCU\SOFTWARE\Microsoft\InputSett...	SUCCESS	Query Handle Tag...
17:31:38	svchost.exe	2560	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Offset 123, Length: 1
17:31:38	cdmon.exe	17360	RegOpenKey	HKCU\SOFTWARE\Microsoft\InputSett...	SUCCESS	Desired Access: Q...
17:31:38	Explorer.EXE	4940	CreateFile	C:\Users\Peter\AppData\Local\Temp\Pi...	SUCCESS	Desired Access: R...
17:31:38	cdmon.exe	17360	RegQueryValue	HKCU\SOFTWARE\Microsoft\InputSett...	SUCCESS	Type: REG_DWORD...
17:31:38	Explorer.EXE	4940	QueryBasicInfor...	C:\Users\Peter\AppData\Local\Temp\Pi...	SUCCESS	CreationTime: 2021...
17:31:38	Explorer.EXE	4940	CloseFile	C:\Users\Peter\AppData\Local\Temp\Pi...	SUCCESS	
17:31:38	cdmon.exe	17360	RegCloseKey	HKCU\SOFTWARE\Microsoft\InputSett...	SUCCESS	

Showing 90 536 of 511 626 events (17%) Backed by virtual memory

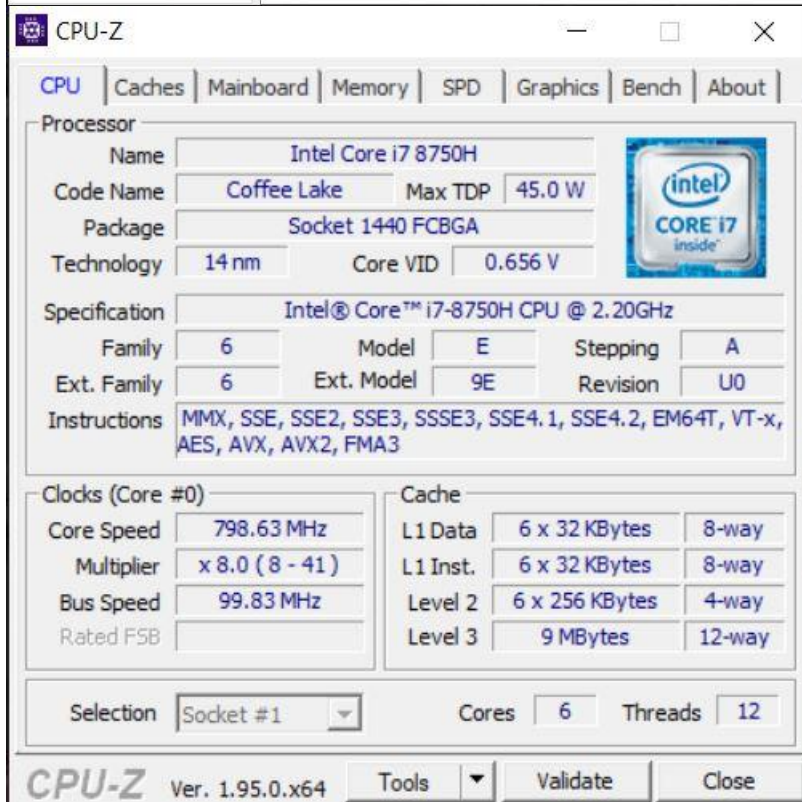
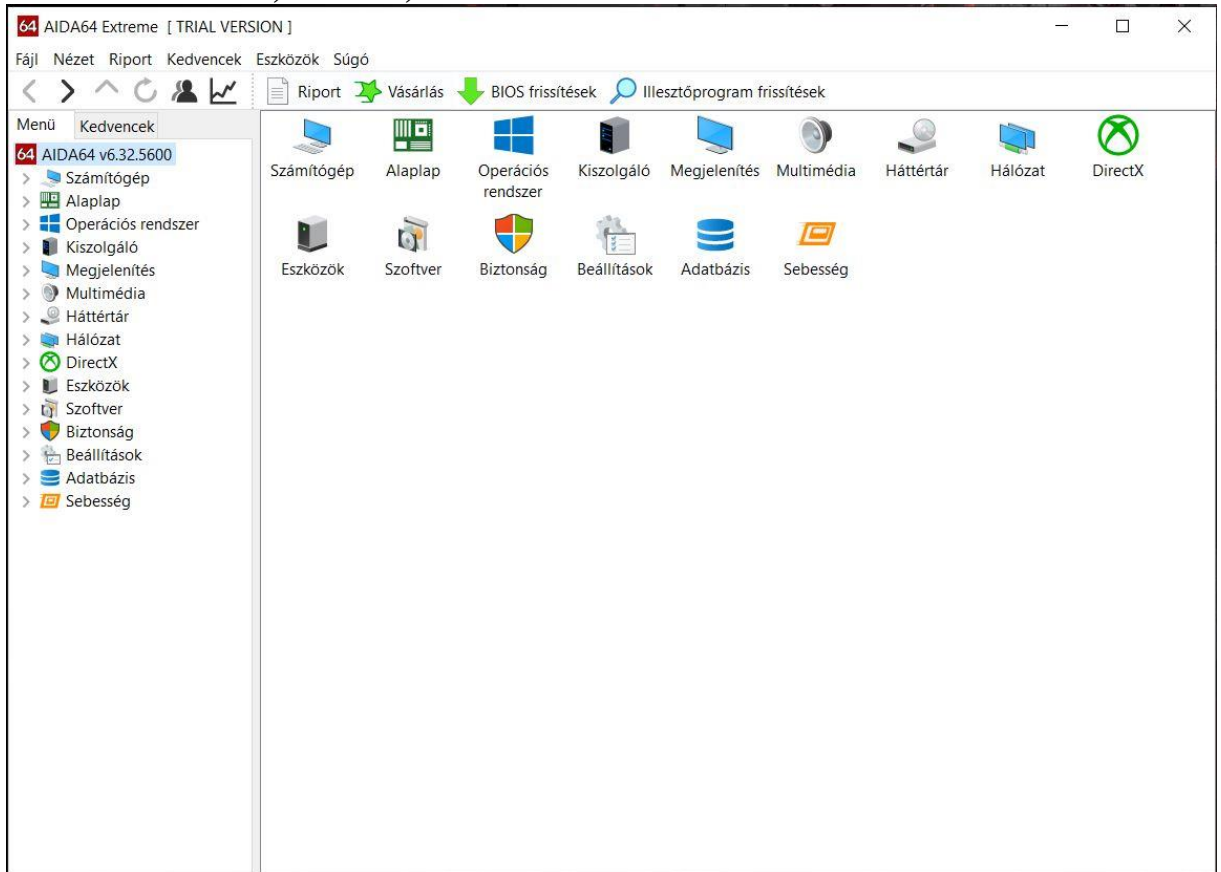
d, Security Utilities (LogonSession)

Elindulás után leáll.

e, Information Utilities (RAMMap)



3. feladat: AIDA64, CPU-Z, GPU-Z



TechPowerUp GPU-Z 2.37.0

Graphics Card

Sensors

Advanced

Validation

Name

Intel(R) UHD Graphics 630

Lookup

GPU

Coffee Lake GT2

Revision

N/A

Technology

14 nm

Die Size

Unknown

Release Date

Oct 5, 2017

Transistors

Unknown

BIOS Version

1014 PC 14.34 06/11/2018 01:51:15

UEFI

Subvendor

Lenovo

Device ID

8086 3E9B - 17AA 39FD

ROPs/TMUs

8 / 16

Bus Interface

N/A

Shaders

24 Unified

DirectX Support

12 (12_1)

Pixel Fillrate

8.8 GPixel/s

Texture Fillrate

17.6 GTexel/s

Memory Type

DDR4

Bus Width

128 bit

Memory Size

N/A

Bandwidth

42.7 GB/s

Driver Version

26.20.100.7637 DCH / Win10 64

Driver Date

Jan 16, 2020

Digital Signature

WHQL

GPU Clock

350 MHz

Memory

1333 MHz

Boost

1100 MHz

Default Clock

350 MHz

Memory

1333 MHz

Boost

1100 MHz

Multi-GPU

Disabled

Computing

☒ OpenCL

☐ CUDA

☒ DirectCompute

☒ DirectML

Technologies

☐ Vulkan

☐ Ray Tracing

☒ PhysX

☒ OpenGL 4.6

Intel(R) UHD Graphics 630

Close

TechPowerUp GPU-Z 2.37.0

Graphics Card

Sensors

Advanced

Validation

Name

NVIDIA GeForce GTX 1050 Ti

Lookup

GPU

GP107

Revision

A1

Technology

14 nm

Die Size

132 mm²

Release Date

Jan 4, 2017

Transistors

3300M

BIOS Version

86.07.66.00.09

☐ UEFI

Subvendor

Lenovo

Device ID

10DE 1C8C - 17AA 39FD

ROPs/TMUs

32 / 48

Bus Interface

PCIe x16 3.0 @ x16 1.1

?

Shaders

768 Unified

DirectX Support

12 (12_1)

Pixel Fillrate

51.8 GPixel/s

Texture Fillrate

77.8 GTexel/s

Memory Type

GDDR5 (Micron)

Bus Width

128 bit

Memory Size

4096 MB

Bandwidth

112.1 GB/s

Driver Version

26.21.14.4575 (NVIDIA 445.75) DCH / Win10 64

Driver Date

Mar 17, 2020

Digital Signature

WHQL

GPU Clock

1493 MHz

Memory

1752 MHz

Boost

1620 MHz

Default Clock

1493 MHz

Memory

1752 MHz

Boost

1620 MHz

NVIDIA SLI

Disabled

Computing

☒ OpenCL

☒ CUDA

☒ DirectCompute

☒ DirectML

Technologies

☒ Vulkan

☐ Ray Tracing

☒ PhysX

☒ OpenGL 4.6

NVIDIA GeForce GTX 1050 Ti

Close