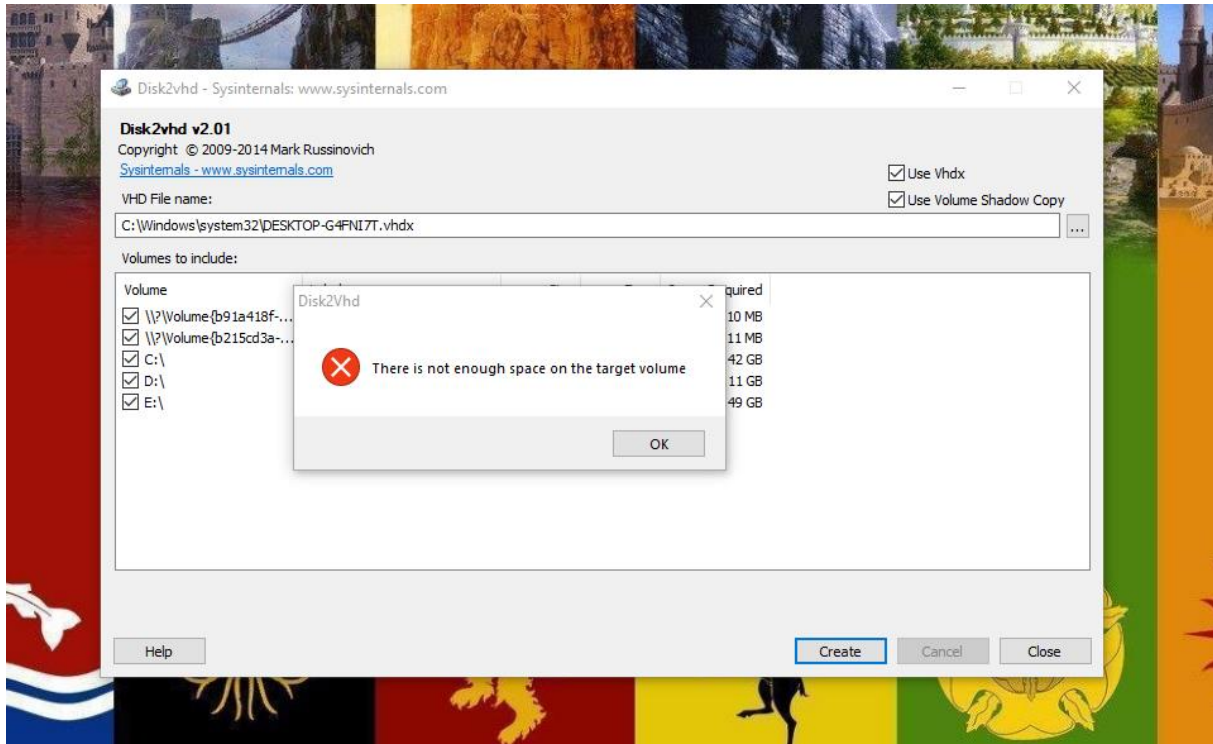


## 2, Feladat

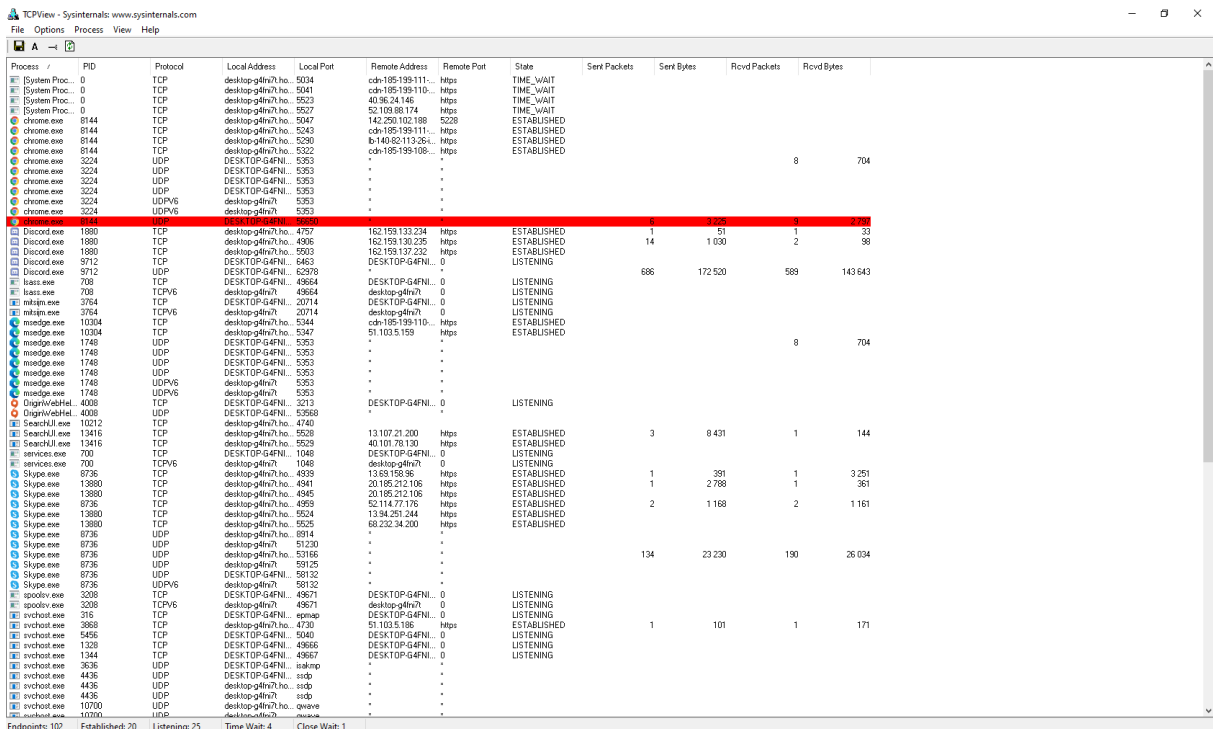
a,(Disk2vhd)

Létrehozz a kijelölt meghajtókon egy fájlt, de nincs rá elég hely.



b,(TCPView)

A programon belül látható a process-nek az adott process-nek a PID-je és a Protocol típusa.



c,(Process Explorer, Process Monitor, AutoRuns)

AutoRuns: Észlel minden programot, ami a számítógép bekapcsolásakor automatikusan elkezd futni a rendszer mellett. Ezeket a program segítségével ki lehet törölni vagy szerkeszteni.

AutoRuns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

AutoRun Entry	Description	Publisher	Image Path	Timestamp	VeriaTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				2019. 03. 19. 5:53	
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	1909. 05. 14. 1:57	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021. 02. 18. 9:12	
Vanguard	Vanguard tray notification	(Verified) Riot Games, Inc.	c:\program files\riot\vanguard\vgtray	2021. 01. 22. 21:31	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2020. 06. 16. 14:00	
Autodesk Desktop App	Autodesk Desktop App	(Verified) Autodesk, Inc.	c:\program files (x86)\autodesk\auto	2020. 03. 04. 5:35	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021. 02. 23. 14:28	
CCPProcess	CCPProcess	(Verified) Adobe Inc.	c:\program files (x86)\adobe\adobe	2019. 11. 27. 0:11	
com.squirrel.Teams Teams	Microsoft Teams	(Verified) Microsoft 3rd Party Applic...	c:\users\Aron\AppData\local\micro...	2020. 10. 02. 13:40	
Discord	Update	(Verified) Discord Inc.	c:\users\Aron\AppData\local\discord	2020. 06. 01. 21:58	
EADN	Origin	(Verified) Electronic Arts, Inc.	c:\program files (x86)\origin\origin.exe	2021. 02. 10. 19:35	
EpicGamesLauncher	EpicGamesLauncher	(Verified) Epic Games Inc.	c:\program files (x86)\epic\games\la...	2021. 02. 16. 14:42	
OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	c:\users\Aron\AppData\local\micro...	1956. 02. 05. 12:59	
Parsec App 0	Parsec	(Verified) Parsec Cloud, Inc.	c:\program files\parsec\parsec.exe	2020. 09. 10. 14:18	
Update Notifier	Update Notifier	(Verified) MAGIX Software GmbH	c:\program files\common files\magi...	2019. 08. 13. 15:32	
Steam Client Bootstrapper	Steam Client Bootstrapper	(Verified) Valve	c:\program files (x86)\steam\steam.exe	2021. 02. 13. 0:23	
uTorrent	uTorrent	(Verified) BitTorrent Inc.	c:\users\Aron\AppData\local\utor...	2020. 12. 09. 1:05	
Wargaming.net Game C...	Wargaming.net Game Center	(Verified) Wargaming.net Limited	c:\programdata\wargaming.net\gam...	2021. 02. 02. 16:40	
Web Companion	Web Companion	(Verified) LAVASOFT SOFTWARE C...	c:\program files (x86)\lavasoft\web.c...	2020. 05. 21. 14:32	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2020. 11. 23. 17:15	
Google Chrome	Google Chrome Installer	(Verified) Google LLC	c:\program files (x86)\google\chrome	2021. 02. 18. 22:08	
Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge	2021. 02. 17. 4:41	
n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\system32\mscores.dll	2019. 03. 04. 13:54	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				2020. 06. 09. 9:29	
n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\assembly\mscores.dll	2019. 03. 04. 13:12	
HKLM\SOFTWARE\Classes\Protocols\Filer				2021. 02. 03. 10:52	
test.xml	Microsoft Office XML MIME Filter	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\office	2020. 12. 28. 23:39	
HKLM\Software\Classes\ShellEx\ContextMenuHandlers				2020. 12. 10. 11:34	
AcroExt	Core Sync	(Verified) Adobe Systems Incorporated	c:\program files (x86)\common files\...	2018. 03. 05. 16:02	
AcShellExtension.Acro...	AutoCAD Dwg common shell extensi...	(Verified) Autodesk, Inc.	c:\program files\common files\autode...	2016. 02. 07. 3:36	
Notepad++64	ShellHandler for Notepad++ (64 bit)	(Verified) Notepad++	c:\program files (x86)\notepad++\inp...	2014. 05. 12. 10:49	
WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	c:\program files\winrar\winrar.dll	2020. 06. 25. 11:38	
HKLM\Software\Classes\WinFt\SystemObject\ShellEx\ContextMenuHandlers				2021. 02. 18. 9:12	
MBAMSHExt	Malwarebytes	(Verified) Malwarebytes Corporation	c:\program files\malwarebytes\anti-m...	2019. 06. 13. 23:40	
HKLM\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers				2020. 06. 08. 20:46	
NvCplDesktopContent	NVIDIA Display Shell Extension	(Verified) NVIDIA Corporation	c:\windows\system32\driverstore\file...	2020. 10. 22. 17:26	
HKLM\Software\Classes\Folder\Shell\ColumnsHandlers				2020. 06. 16. 19:54	
AcColumnHandler	AutoCAD Dwg common shell extensi...	(Verified) Autodesk, Inc.	c:\program files\common files\autode...	2016. 02. 07. 3:36	
AdpShellExt Class	Autodesk Workflow Shell Extension	(Verified) Autodesk, Inc.	c:\program files\common files\autode...	2010. 02. 05. 14:51	
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers				2021. 02. 18. 9:12	
AcroExt	Core Sync	(Verified) Adobe Systems Incorporated	c:\program files (x86)\common files\...	2018. 03. 05. 16:02	
MBAMSHExt	Malwarebytes	(Verified) Malwarebytes Corporation	c:\program files\malwarebytes\anti-m...	2019. 06. 13. 23:40	
WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	c:\program files\winrar\winrar.dll	2020. 06. 25. 11:38	
HKLM\Software\Classes\Folder\ShellEx\DropDropHandlers				2020. 11. 22. 15:16	
WinRAR	WinRAR shell extension	(Verified) win.rar GmbH	c:\program files\winrar\winrar.dll	2020. 06. 25. 11:38	

Process Explorer:

Látja a processzor terheltségét, az adott exe fájlok byte-os lefoglaltságát láthatjuk a PID és az adott alkalmazás Company nevét is.

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-G4FNI7T\Aron]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
chrome.exe		121 888 K	89 320 K	14148	Google Chrome	Google LLC
chrome.exe		112 552 K	186 732 K	3224	Google Chrome	Google LLC
explorer.exe	0.07	108 708 K	167 312 K	7732	Windows Intéző	Microsoft Corporation
WINWORD.EXE	1.97	102 556 K	163 548 K	1564	Microsoft Word	Microsoft Corporation
msedge.exe		100 808 K	79 624 K	10384	Microsoft Edge	Microsoft Corporation
dwm.exe	1.87	97 740 K	69 152 K	13620		
svchost.exe		75 008 K	33 020 K	3700	Windows-szolgáltatások gaz...	Microsoft Corporation
Skype.exe	0.08	64 624 K	70 116 K	9440	Skype	Skype Technologies S.A.
msedge.exe		59 600 K	98 096 K	504	Microsoft Edge	Microsoft Corporation
RdrCEF.exe	0.04	57 584 K	85 112 K	9004	Adobe RdrCEF	Adobe Systems Incorporated
chrome.exe		56 172 K	96 212 K	904	Google Chrome	Google LLC
RdrCEF.exe	0.03	55 720 K	78 448 K	10020	Adobe RdrCEF	Adobe Systems Incorporated
RdrCEF.exe	< 0.01	54 352 K	78 604 K	1736	Adobe RdrCEF	Adobe Systems Incorporated
RdrCEF.exe		53 744 K	77 556 K	1672	Adobe RdrCEF	Adobe Systems Incorporated
msedge.exe	< 0.01	53 296 K	142 924 K	1748	Microsoft Edge	Microsoft Corporation
RdrCEF.exe		52 504 K	76 316 K	8232	Adobe RdrCEF	Adobe Systems Incorporated
chrome.exe		48 564 K	78 876 K	936	Google Chrome	Google LLC
msedge.exe		47 412 K	84 132 K	480	Microsoft Edge	Microsoft Corporation
YourPhone.exe	Susp...	47 048 K	1 728 K	1732	YourPhone	Microsoft Corporation
OfficeClickToRun.exe	< 0.01	45 060 K	36 576 K	1012	Microsoft Office Click-to-Run...	Microsoft Corporation
Calculator.exe	Susp...	43 280 K	648 K	13700		
SearchIndexer.exe	0.06	41 816 K	48 380 K	13956	A Microsoft Windows Search...	Microsoft Corporation
Video.UI.exe	Susp...	40 152 K	584 K	11960		
Skype.exe	0.02	39 812 K	84 320 K	11504	Skype	Skype Technologies S.A.
Lavasoft.WCAssistant.WinServi...	< 0.01	37 284 K	7 008 K	3836	SPWindowsService	
AcroRd32.exe		35 352 K	32 676 K	10692	Adobe Acrobat Reader DC	Adobe Systems Incorporated
ShellExperienceHost.exe	Susp...	35 096 K	61 556 K	6844	Windows Shell Experience H...	Microsoft Corporation

d,(LogonSession)

Környezeti változókat látja, rendszer adminisztrátorként futtatjuk.

C:\Users\Áron\Desktop\Egyetem\2 felev\os\sysinternals Suite\cmd.exe

```
Sid: S-1-5-20
Logon time: 2021. 02. 18. 9:12:19
Logon server:
DNS Domain:
UPN:

[4] Logon session 00000000:000003e5:
User name: NT AUTHORITY\SYSTEM
Auth package: Negotiate
Logon type: Service
Session: 0
Sid: S-1-5-19
Logon time: 2021. 02. 18. 9:12:19
Logon server:
DNS Domain:
UPN:

[5] Logon session 00000000:00033a0e:
User name: DESKTOP-G4FNI7T\Áron
Auth package: NTLM
Logon type: Interactive
Session: 1
Sid: S-1-5-21-411059976-2539346685-4044709691-1001
Logon time: 2021. 02. 18. 9:12:21
Logon server: DESKTOP-G4FNI7T
DNS Domain:
UPN:

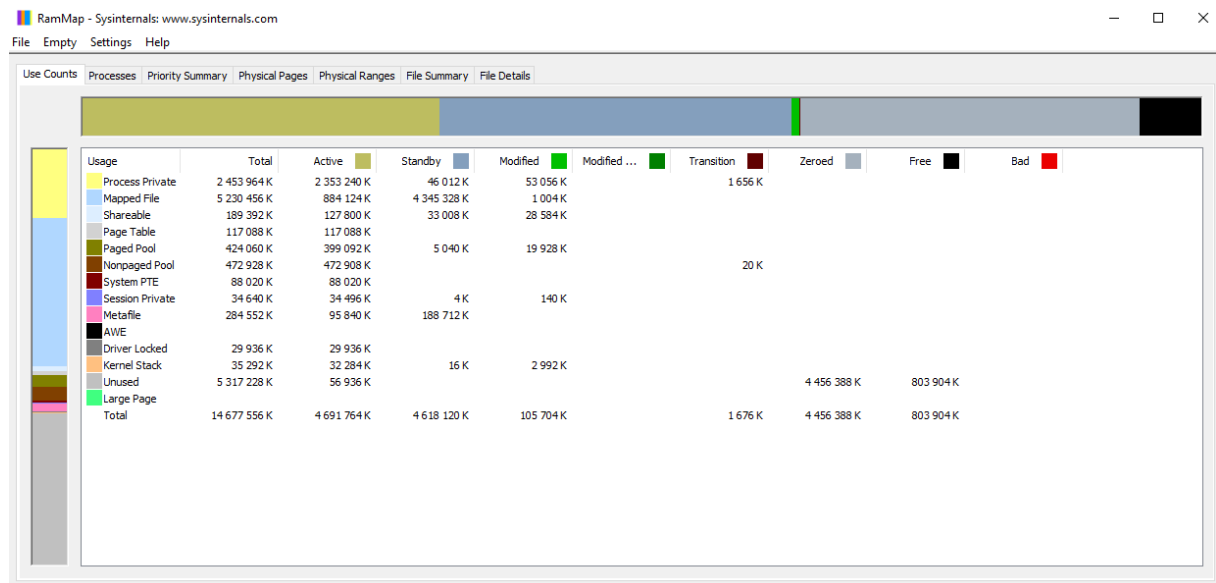
[6] Logon session 00000000:00033a61:
User name: DESKTOP-G4FNI7T\Áron
Auth package: NTLM
Logon type: Interactive
Session: 1
Sid: S-1-5-21-411059976-2539346685-4044709691-1001
Logon time: 2021. 02. 18. 9:12:21
Logon server: DESKTOP-G4FNI7T
DNS Domain:
UPN:

[7] Logon session 00000000:04d78c9c:
User name: DESKTOP-G4FNI7T\Áron
Auth package: NTLM
Logon type: Interactive
Session: 2
Sid: S-1-5-21-411059976-2539346685-4044709691-1001
Logon time: 2021. 02. 19. 9:17:42
Logon server: DESKTOP-G4FNI7T
DNS Domain:
UPN:
```

e,(RAMMAP)

Az alkalmazás fizikai memóriahasználat elemző segéd program amely különböző módon jeleníti meg a RAM használatának az információit.

Látjuk a fájlok elérési útvonalukat

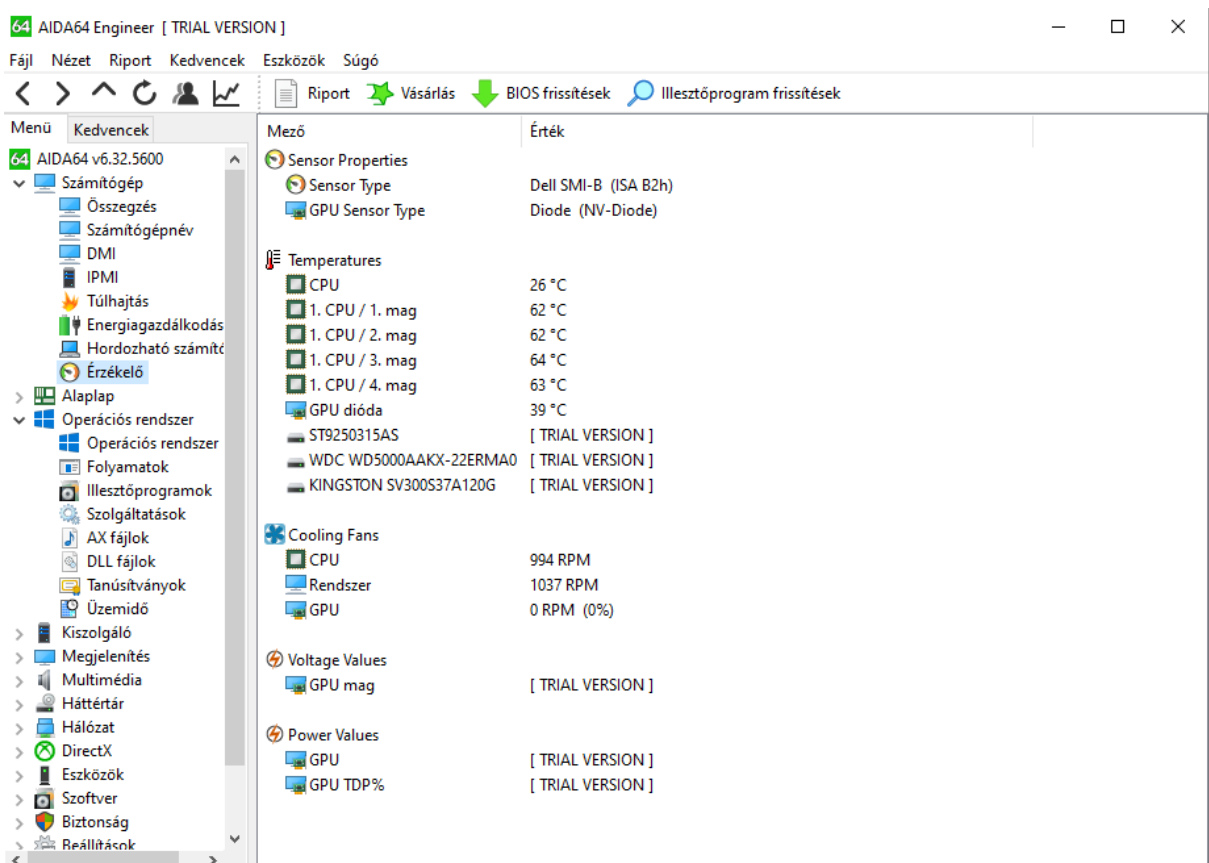


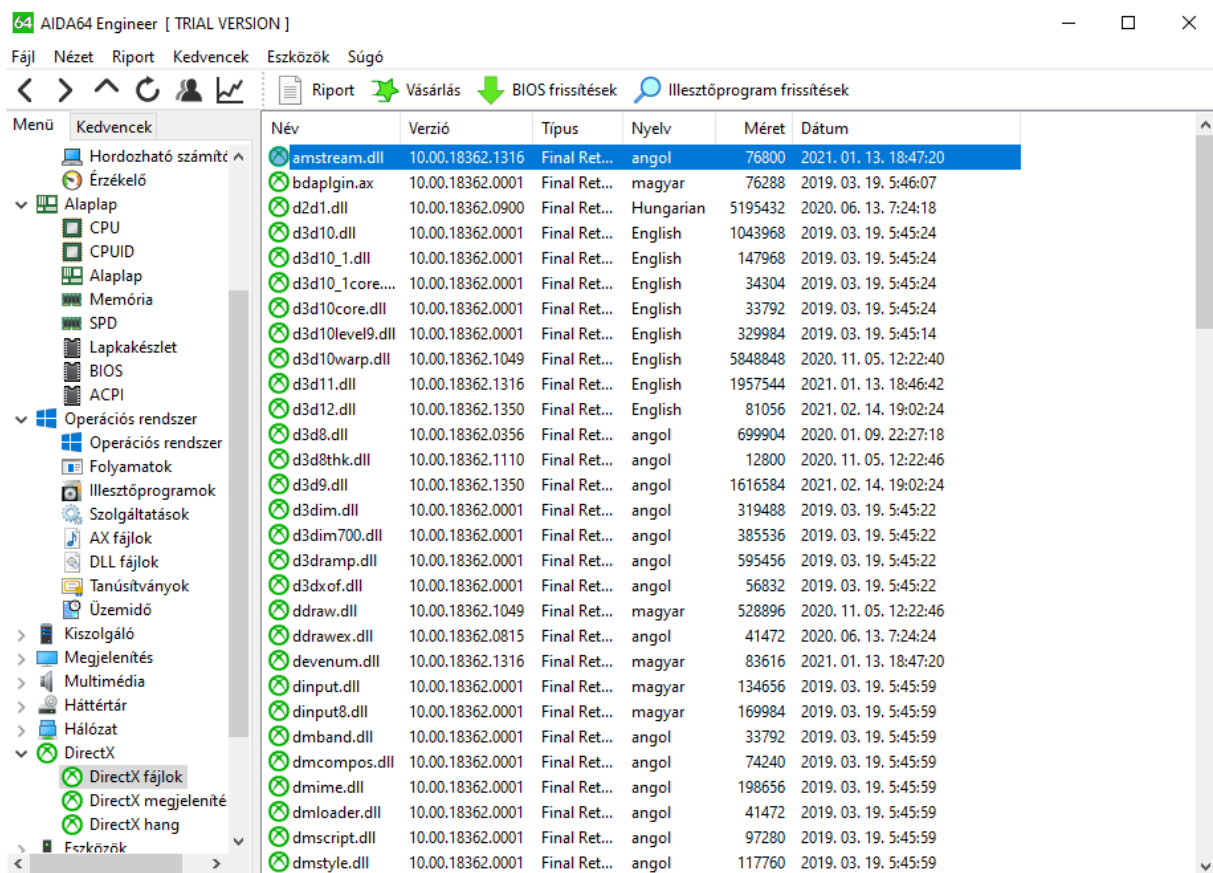
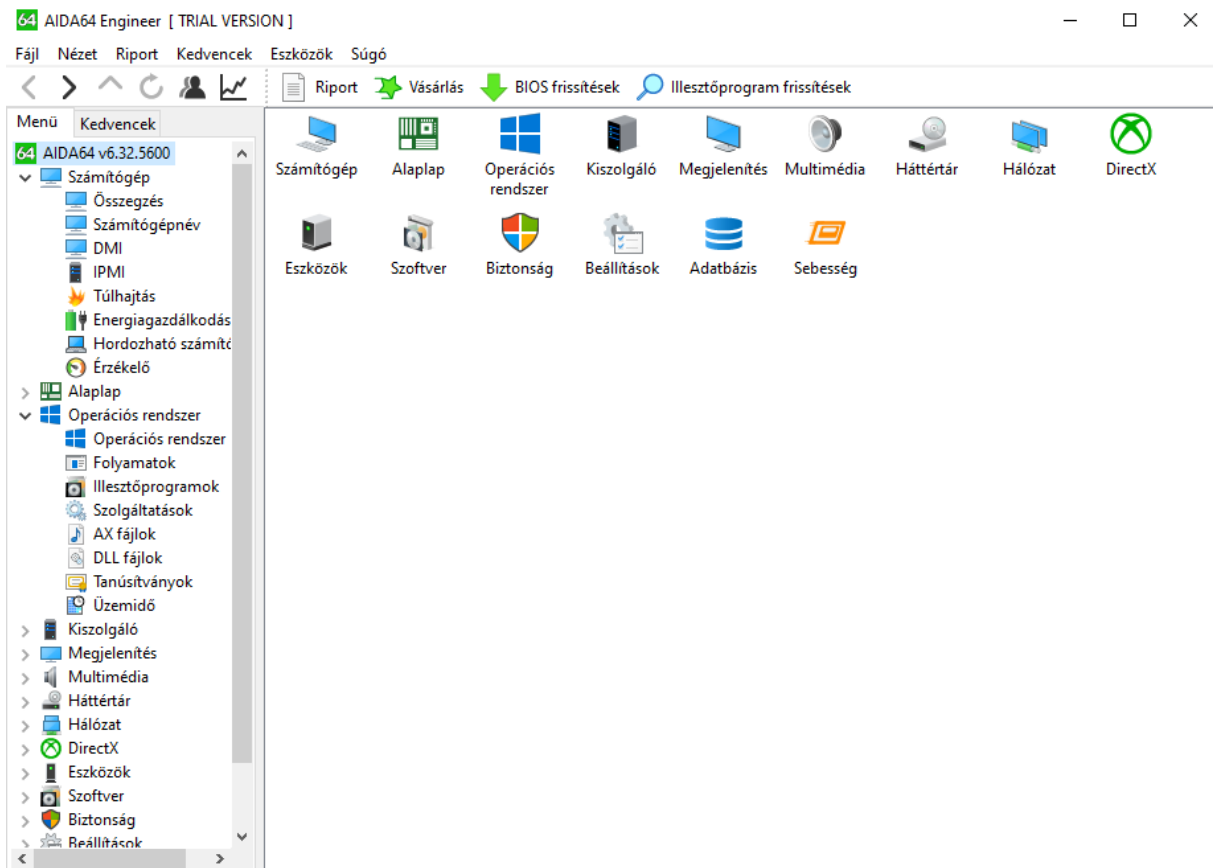
### 3. Feladat

Az AID Engineer segédprogrammal le ellenőrizhetjük a számítógépünk fizikai tulajdonságait és állapotát.

Megnézhetjük milyen DirectX fájlaink vannak ezen kívül a perifériák tulajdonságai is lekérdezhetők.

Képernyők típusát és méreteit és láthatjuk.





64 AIDA64 Engineer [ TRIAL VERSION ]

Fájl Nézet Riport Kedvencek Eszközök Súgó

< > ^ ↺ 🧑 📈 📄 Riport 🌱 Vásárlás 📉 BIOS frissítések 🔍 Illesztőprogram frissítések

Menü Kedvencek

- Alaplap
- Memória
- SPD
- Lapkakészlet
- BIOS
- ACPI
- Operációs rendszer
  - Operációs rendszer
  - Folyamatok
  - Illesztőprogramok
  - Szolgáltatások
  - AX fájlok
  - DLL fájlok
  - Tanúsítványok
  - Üzemidő
- Kiszolgáló
- Megjelenítés
  - Windows videó
  - PCI / AGP videó
  - GPU
  - Képernyő
  - Asztal
  - Multi-Monitor
  - Videomódok
  - OpenGL
  - GPGPU
  - Mantle
  - Vulkan
  - Betűkészletek
- Multimédia
- Háttértár
- Hálózat
  - Windows hálózat
  - PCI / PnP hálózat

Képernyő neve

- Általános PnP képernyő [NoDB]
- Általános PnP képernyő [NoDB]

Mező	Érték
Képernyő tulajdonságai	
Képernyő neve	Általános PnP képernyő [NoDB]
Képernyő azonosítója	AAA0001
Modell	P7229WDG
Gyártás ideje	33. hét / 2008
Sorozatszám	100583990001
Maximális látható kijelző mé...	474 mm x 296 mm (22.0")
Képarány	16:10
Vízszintes frekvencia	31 - 81 kHz
Függőleges frekvencia	56 - 75 Hz
Maximális pixel órajel	150 MHz
Gamma	2.20
DPMS mód támogatás	Standby, Suspend, Active-Off
Támogatott megjelenítési módok	
640 x 480	60 Hz
640 x 480	67 Hz
640 x 480	72 Hz
640 x 480	75 Hz
720 x 400	70 Hz
800 x 600	56 Hz
800 x 600	60 Hz
800 x 600	72 Hz
800 x 600	75 Hz
832 x 624	75 Hz
1024 x 768	60 Hz
1024 x 768	72 Hz
1024 x 768	75 Hz

#### 4. feladat

a segédprogram *megvizsgálja* milyen könyvtárakra, és azon belül milyen függvényekre hivatkozik egy elindított program.

Dependency Walker - [diskext64]

File Edit View Options Profile Window Help

DISKEXT64.EXE

- KERNEL32.DLL
  - API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
  - NTDLL.DLL
  - KERNELBASE.DLL
  - NTDLL.DLL
    - API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
    - API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL
    - API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL
    - EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL
    - EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL
    - EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL
    - EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL
    - EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL
    - EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL
    - EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL
    - EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-1.DLL

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	F
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).									
API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).									
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).									
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).									
API-MS-WIN-CORE-APPINIT-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).									
API-MS-WIN-CORE-ATOMS-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).									
API-MS-WIN-CORE-COM-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).									

Error: At least one required implicit or forwarded dependency was not found.  
 Error: At least one module has an unresolved import due to a missing export function in an implicitly dependent module.  
 Warning: At least one delay-load dependency module was not found.  
 Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

For Help, press F1