Operációs Rendszerek Bsc

3.gyak.

2021.02.24.

Készítette:

Horváth Ákos Bsc

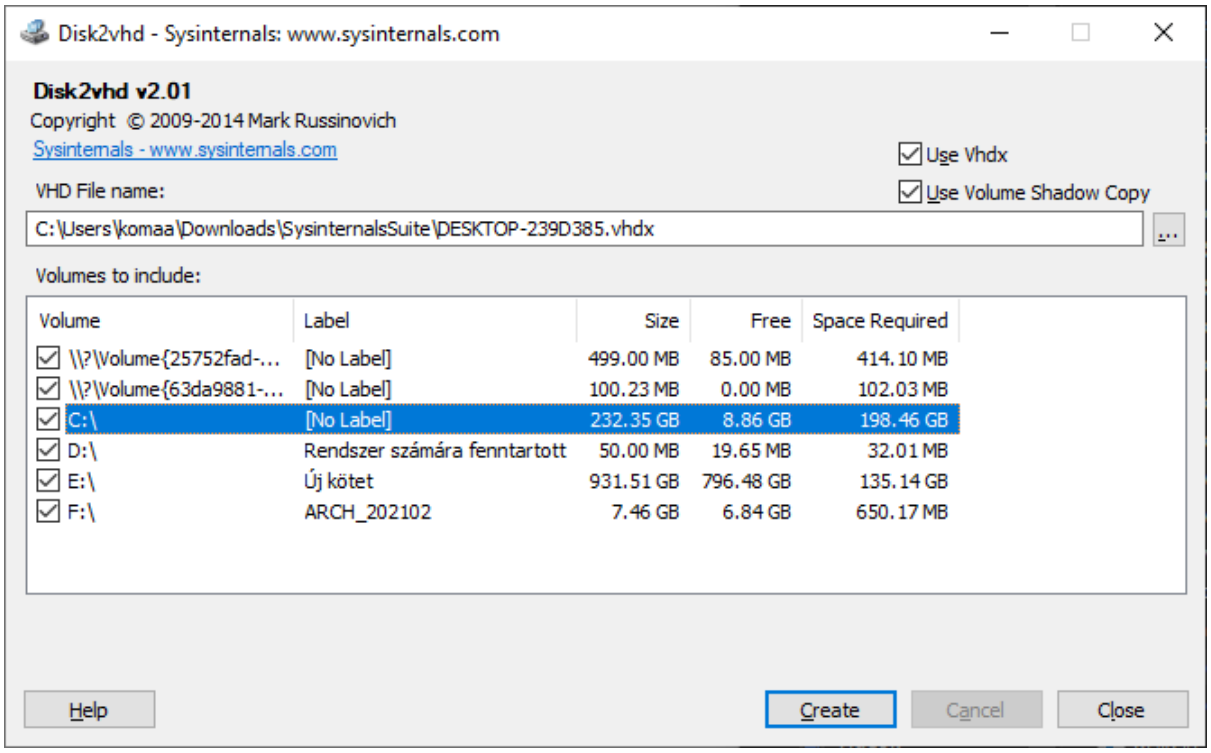
Programtervező informatikus szak

R3SZY2

Miskolc, 2021

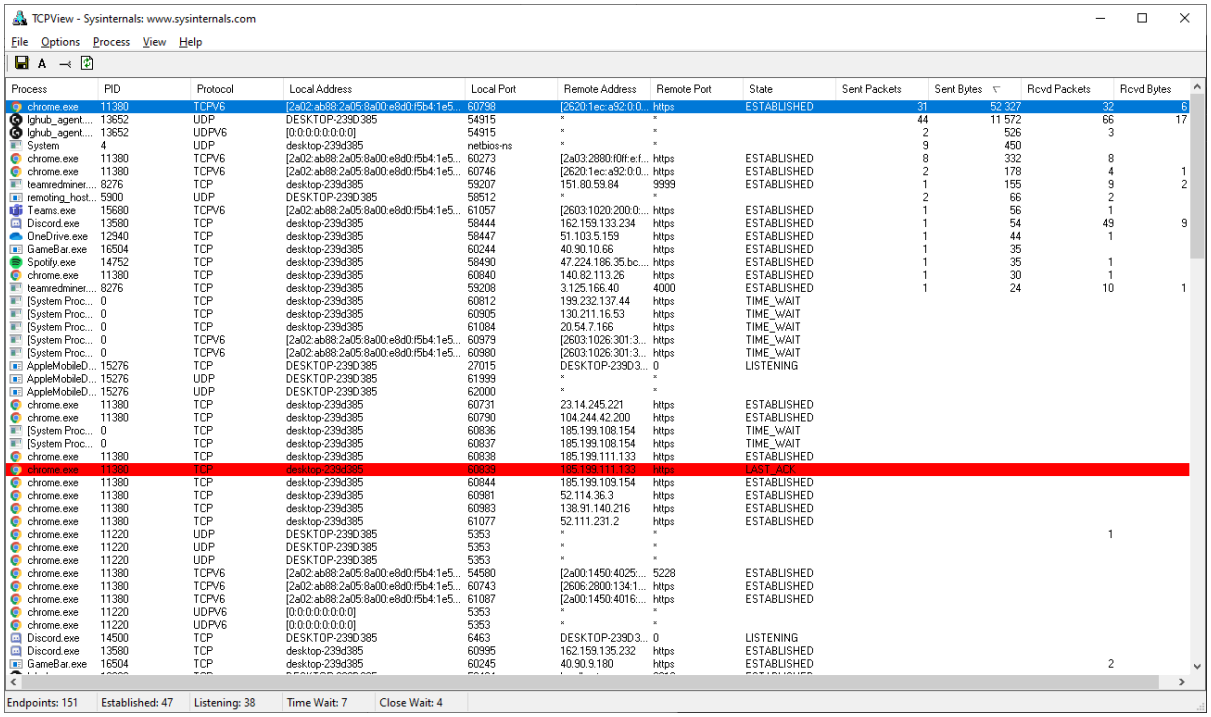
2.feladat-Sysinternals Suite segédprogramokkal vizsgálat.

Disk2vhd: Lemezképfájlt lehet készíteni



TCPView:

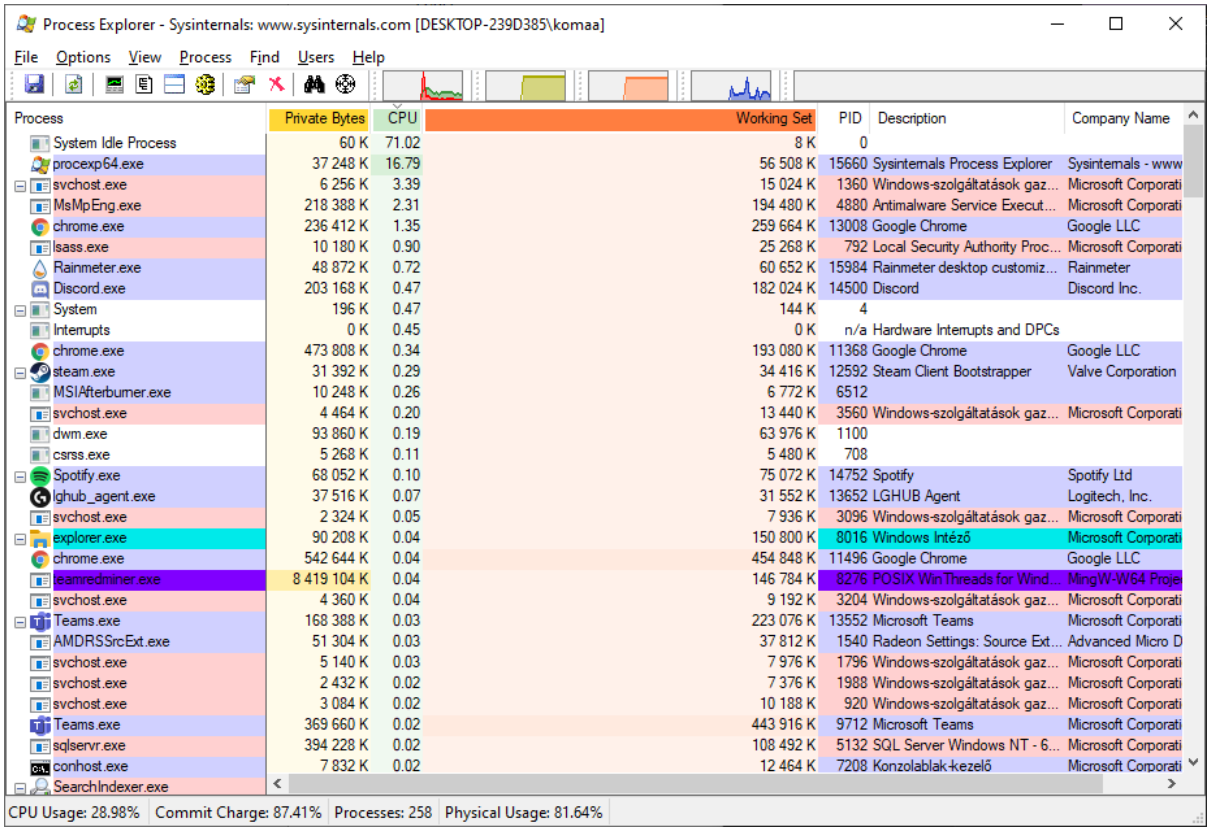
Hálózati tevékenységet lehet vizsgálni, küldött byteok szerint rendeztem a listát.



Miskolc, 2021

Process Explorer:

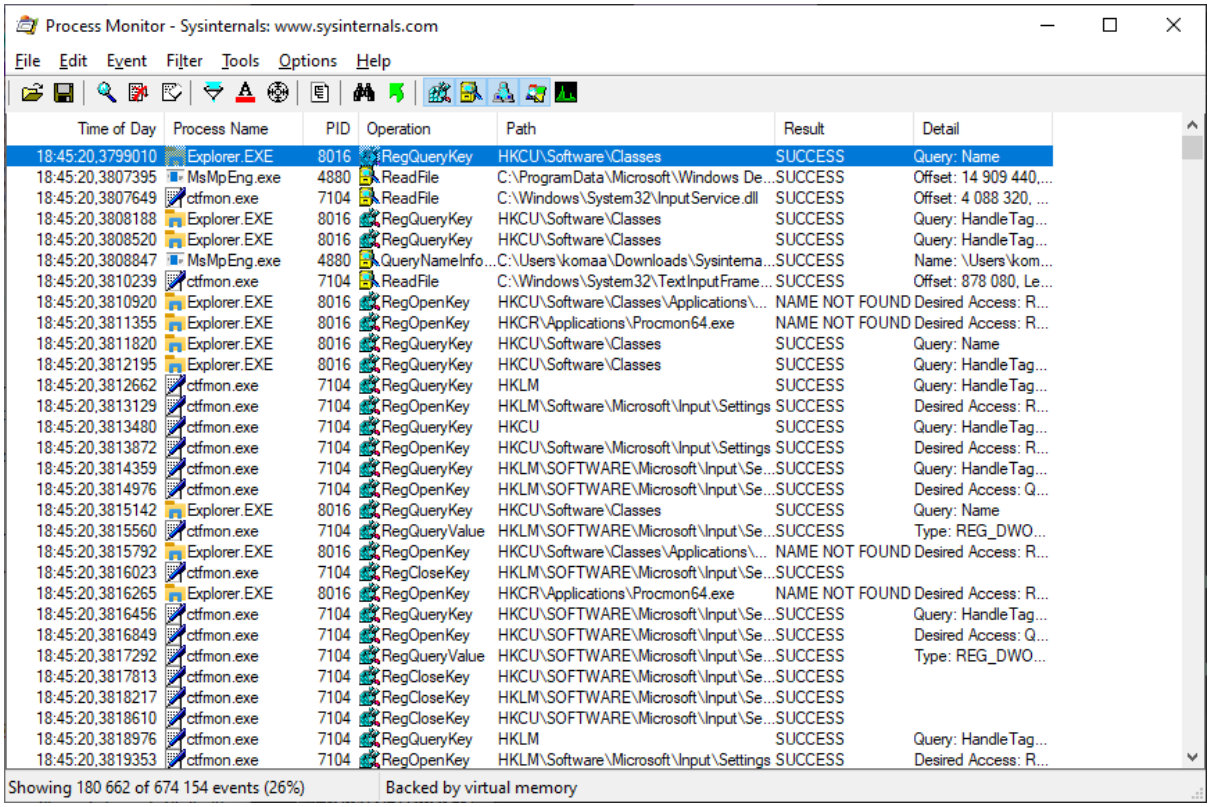
Futó processzek listája, CPU használat szerint rendeztem.



Process	Private Bytes	CPU	Working Set	PID	Description	Company Name
System Idle Process	60 K	71.02	8 K	0		
procexp64.exe	37 248 K	16.79	56 508 K	15660	Sysinternals Process Explorer	Sysinternals - www
svchost.exe	6 256 K	3.39	15 024 K	1360	Windows-szolgáltatások gaz...	Microsoft Corporati
MsMpEng.exe	218 388 K	2.31	194 480 K	4880	Antimalware Service Execut...	Microsoft Corporati
chrome.exe	236 412 K	1.35	259 664 K	13008	Google Chrome	Google LLC
lsass.exe	10 180 K	0.90	25 268 K	792	Local Security Authority Proc...	Microsoft Corporati
Rainmeter.exe	48 872 K	0.72	60 652 K	15984	Rainmeter desktop customiz...	Rainmeter
Discord.exe	203 168 K	0.47	182 024 K	14500	Discord	Discord Inc.
System	196 K	0.47	144 K	4		
Interrupts	0 K	0.45	0 K	n/a	Hardware Interrupts and DPCs	
chrome.exe	473 808 K	0.34	193 080 K	11368	Google Chrome	Google LLC
steam.exe	31 392 K	0.29	34 416 K	12592	Steam Client Bootstrapper	Valve Corporation
MSIAfterburner.exe	10 248 K	0.26	6 772 K	6512		
svchost.exe	4 464 K	0.20	13 440 K	3560	Windows-szolgáltatások gaz...	Microsoft Corporati
dwm.exe	93 860 K	0.19	63 976 K	1100		
csrss.exe	5 268 K	0.11	5 480 K	708		
Spotify.exe	68 052 K	0.10	75 072 K	14752	Spotify	Spotify Ltd
lghub_agent.exe	37 516 K	0.07	31 552 K	13652	LGHUB Agent	Logitech, Inc.
svchost.exe	2 324 K	0.05	7 936 K	3096	Windows-szolgáltatások gaz...	Microsoft Corporati
explorer.exe	90 208 K	0.04	150 800 K	8016	Windows Intéző	Microsoft Corporati
chrome.exe	542 644 K	0.04	454 848 K	11496	Google Chrome	Google LLC
teamredminer.exe	8 419 104 K	0.04	146 784 K	8276	POSIX WinThreads for Wind...	MingW-W64 Proje
svchost.exe	4 360 K	0.04	9 192 K	3204	Windows-szolgáltatások gaz...	Microsoft Corporati
Teams.exe	168 388 K	0.03	223 076 K	13552	Microsoft Teams	Microsoft Corporati
AMDRSSrcExt.exe	51 304 K	0.03	37 812 K	1540	Radeon Settings: Source Ext...	Advanced Micro D
svchost.exe	5 140 K	0.03	7 976 K	1796	Windows-szolgáltatások gaz...	Microsoft Corporati
svchost.exe	2 432 K	0.02	7 376 K	1988	Windows-szolgáltatások gaz...	Microsoft Corporati
svchost.exe	3 084 K	0.02	10 188 K	920	Windows-szolgáltatások gaz...	Microsoft Corporati
Teams.exe	369 660 K	0.02	443 916 K	9712	Microsoft Teams	Microsoft Corporati
sqlservr.exe	394 228 K	0.02	108 492 K	5132	SQL Server Windows NT - 6...	Microsoft Corporati
conhost.exe	7 832 K	0.02	12 464 K	7208	Konzolablak-kezelő	Microsoft Corporati
SearchIndexer.exe						

Process Monitor:

Processzek által végrehajtott operációkat listázza.



Process Monitor - Sysinternals: www.sysinternals.com

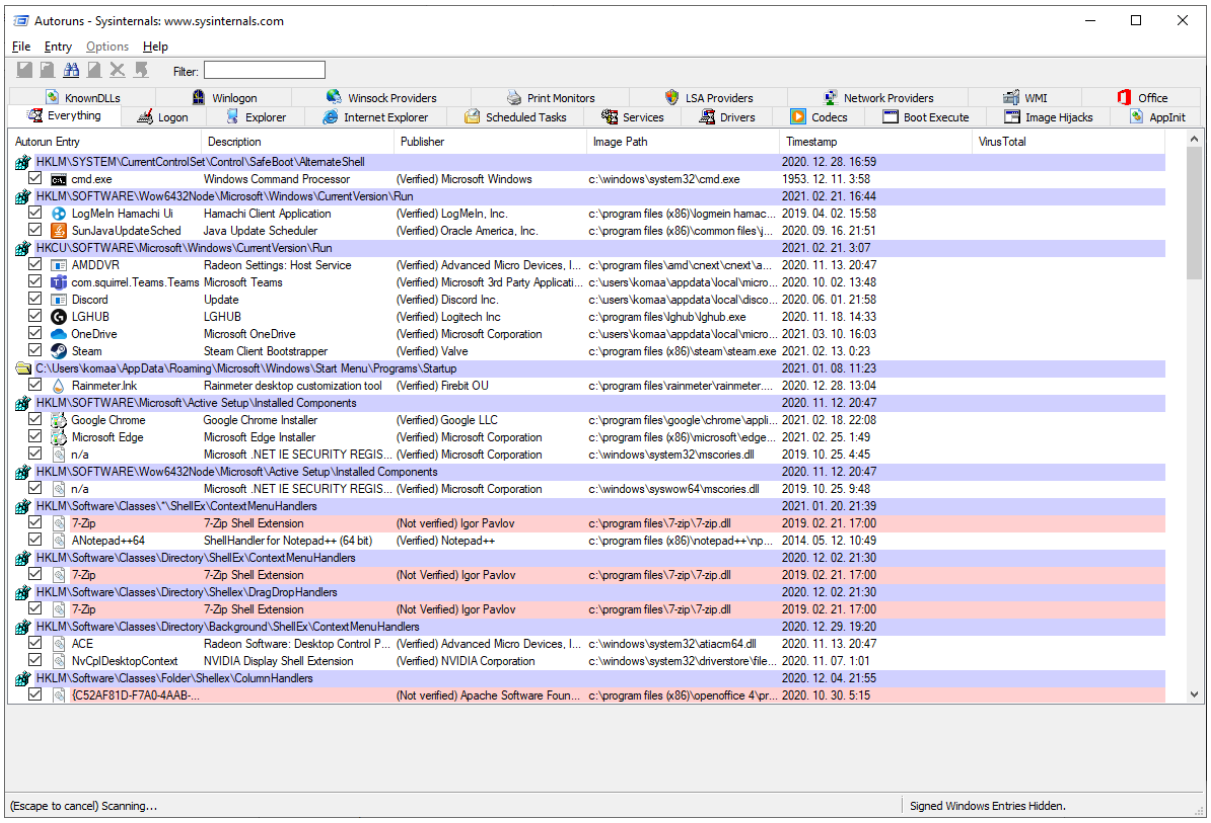
File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result	Detail
18:45:20,3799010	Explorer.EXE	8016	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
18:45:20,3807395	MsMpEng.exe	4880	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 909 440,...
18:45:20,3807649	ctfmon.exe	7104	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS	Offset: 4 088 320, ...
18:45:20,3808188	Explorer.EXE	8016	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
18:45:20,3808520	Explorer.EXE	8016	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
18:45:20,3808847	MsMpEng.exe	4880	QueryNameInfo...	C:\Users\komaa\Downloads\Sysinterna...	SUCCESS	Name: \Users\kom...
18:45:20,3810239	ctfmon.exe	7104	ReadFile	C:\Windows\System32\TextInputFrame...	SUCCESS	Offset: 878 080, Le...
18:45:20,3810920	Explorer.EXE	8016	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
18:45:20,3811355	Explorer.EXE	8016	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
18:45:20,3811820	Explorer.EXE	8016	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
18:45:20,3812195	Explorer.EXE	8016	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
18:45:20,3812662	ctfmon.exe	7104	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
18:45:20,3813129	ctfmon.exe	7104	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
18:45:20,3813480	ctfmon.exe	7104	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
18:45:20,3813872	ctfmon.exe	7104	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
18:45:20,3814359	ctfmon.exe	7104	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
18:45:20,3814976	ctfmon.exe	7104	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
18:45:20,3815142	Explorer.EXE	8016	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
18:45:20,3815560	ctfmon.exe	7104	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Type: REG_DWO...
18:45:20,3815792	Explorer.EXE	8016	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
18:45:20,3816023	ctfmon.exe	7104	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
18:45:20,3816265	Explorer.EXE	8016	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
18:45:20,3816456	ctfmon.exe	7104	RegQueryKey	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
18:45:20,3816849	ctfmon.exe	7104	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
18:45:20,3817292	ctfmon.exe	7104	RegQueryValue	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Type: REG_DWO...
18:45:20,3817813	ctfmon.exe	7104	RegCloseKey	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
18:45:20,3818217	ctfmon.exe	7104	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
18:45:20,3818610	ctfmon.exe	7104	RegCloseKey	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
18:45:20,3818976	ctfmon.exe	7104	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
18:45:20,3819353	ctfmon.exe	7104	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...

Showing 180 662 of 674 154 events (26%) | Backed by virtual memory

AutoRuns:

Azokat a programokat listázza, amelyek a gép elindításakor automatikusan lefutnak



Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

KnownDLLs | Winlogon | Winsock Providers | Print Monitors | LSA Providers | Network Providers | WMI | Office

Everything | Logon | Explorer | Internet Explorer | Scheduled Tasks | Services | Drivers | Codecs | Boot Execute | Image Hijacks | AppInit

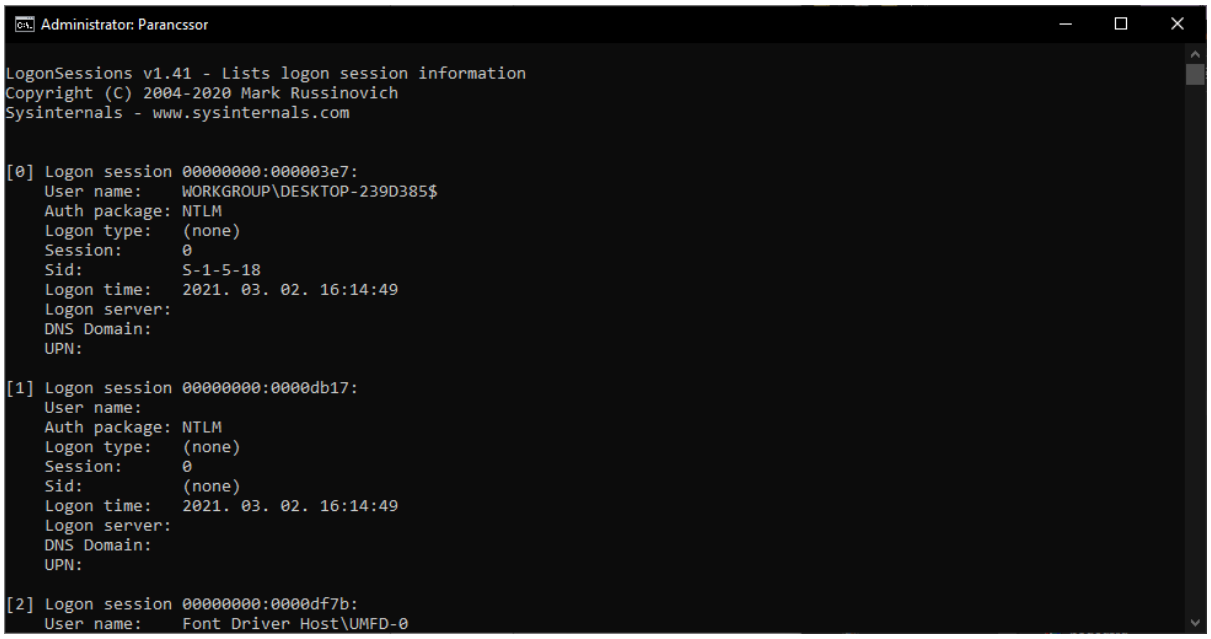
Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				2020. 12. 28. 16:59	
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	1953. 12. 11. 3:58	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2021. 02. 21. 16:44	
LogMeIn Hamachi UI	Hamachi Client Application	(Verified) LogMeIn, Inc.	c:\program files (x86)\logmein hamac...	2019. 04. 02. 15:58	
SunJavaUpdateSched	Java Update Scheduler	(Verified) Oracle America, Inc.	c:\program files (x86)\common files\j...	2020. 09. 16. 21:51	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021. 02. 21. 3:07	
AMDDVR	Radeon Settings: Host Service	(Verified) Advanced Micro Devices, I...	c:\program files\amd\cnext\cnext\a...	2020. 11. 13. 20:47	
com.squirrel.Teams.Teams	Microsoft Teams	(Verified) Microsoft 3rd Party Applicati...	c:\users\komaa\appdata\local\micro...	2020. 10. 02. 13:48	
Discord	Update	(Verified) Discord Inc.	c:\users\komaa\appdata\local\disco...	2020. 06. 01. 21:58	
LGHUB	LGHUB	(Verified) Logitech Inc	c:\program files\lghub\lghub.exe	2020. 11. 18. 14:33	
OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	c:\users\komaa\appdata\local\micro...	2021. 03. 10. 16:03	
Steam	Steam Client Bootstrapper	(Verified) Valve	c:\program files (x86)\steam\steam.exe	2021. 02. 13. 0:23	
C:\Users\komaa\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				2021. 01. 08. 11:23	
Rainmeter.lnk	Rainmeter desktop customization tool	(Verified) Firebit OU	c:\program files\rainmeter\rainmeter....	2020. 12. 28. 13:04	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2020. 11. 12. 20:47	
Google Chrome	Google Chrome Installer	(Verified) Google LLC	c:\program files\google\chrome\appli...	2021. 02. 18. 22:08	
Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge...	2021. 02. 25. 1:49	
n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	2019. 10. 25. 4:45	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				2020. 11. 12. 20:47	
n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\syswow64\mscories.dll	2019. 10. 25. 9:48	
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers				2021. 01. 20. 21:39	
7-Zip	7-Zip Shell Extension	(Not verified) Igor Pavlov	c:\program files\7-zip\7-zip.dll	2019. 02. 21. 17:00	
ANotepad++64	ShellHandler for Notepad++ (64 bit)	(Verified) Notepad++	c:\program files (x86)\notepad++\np...	2014. 05. 12. 10:49	
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers				2020. 12. 02. 21:30	
7-Zip	7-Zip Shell Extension	(Not Verified) Igor Pavlov	c:\program files\7-zip\7-zip.dll	2019. 02. 21. 17:00	
HKLM\Software\Classes\Directory\Shellex\DragDropHandlers				2020. 12. 02. 21:30	
7-Zip	7-Zip Shell Extension	(Not Verified) Igor Pavlov	c:\program files\7-zip\7-zip.dll	2019. 02. 21. 17:00	
HKLM\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers				2020. 12. 29. 19:20	
ACE	Radeon Software: Desktop Control P...	(Verified) Advanced Micro Devices, I...	c:\windows\system32\atiacm64.dll	2020. 11. 13. 20:47	
NvCplDesktopContext	NVIDIA Display Shell Extension	(Verified) NVIDIA Corporation	c:\windows\system32\driverstore\file...	2020. 11. 07. 1:01	
HKLM\Software\Classes\Folder\Shellex\ColumnHandlers				2020. 12. 04. 21:55	
{C52AF81D-F7A0-4AAB-...		(Not verified) Apache Software Foun...	c:\program files (x86)\openoffice 4\pr...	2020. 10. 30. 5:15	

(Escape to cancel) Scanning... | Signed Windows Entries Hidden.

Miskolc, 2021

LogonSession:

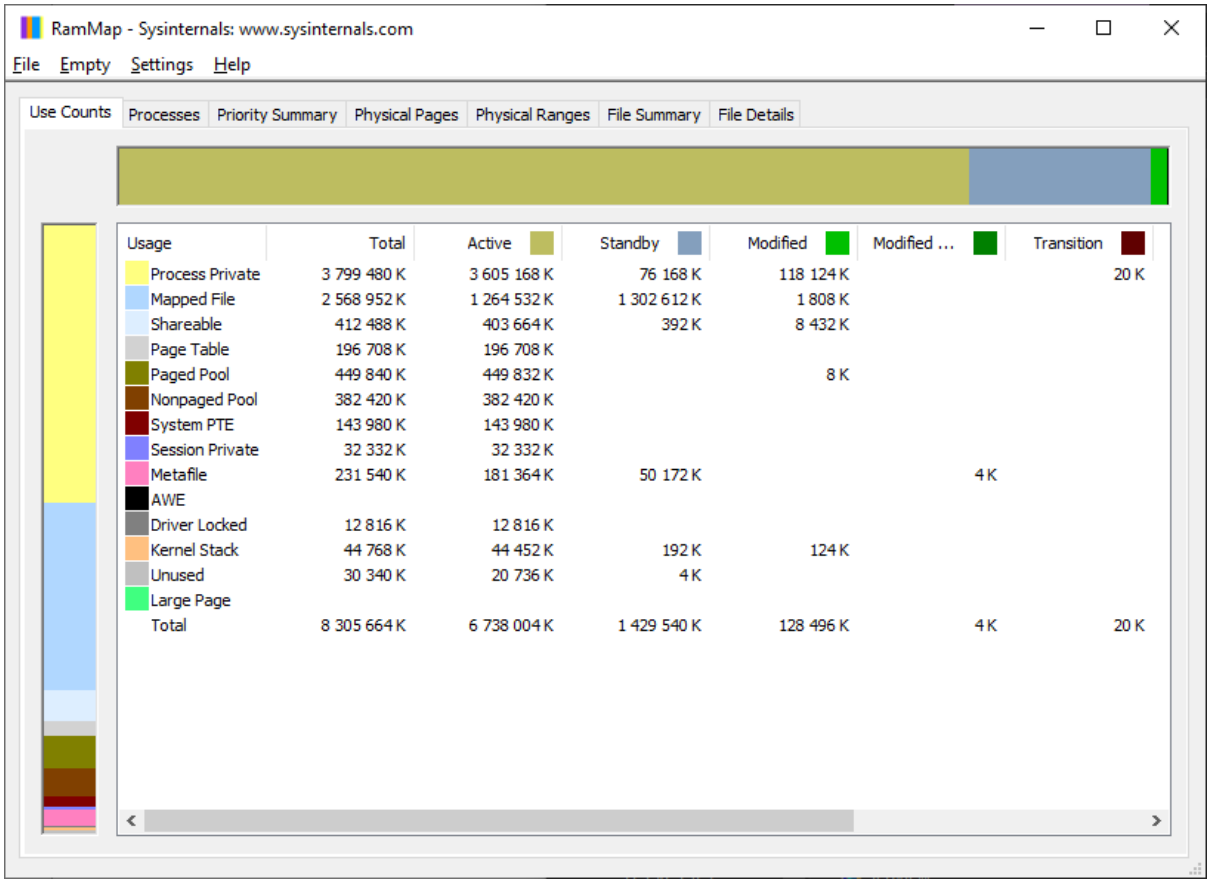
Belépett felhasználokat lehet vele vizsgálni.



```
Administrator: Parancssor

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\DESKTOP-239D385$
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          S-1-5-18
    Logon time:   2021. 03. 02. 16:14:49
    Logon server:
    DNS Domain:
    UPN:

[1] Logon session 00000000:0000db17:
    User name:
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          (none)
    Logon time:   2021. 03. 02. 16:14:49
    Logon server:
    DNS Domain:
    UPN:

[2] Logon session 00000000:0000df7b:
    User name:    Font Driver Host\UMFD-0
```

Rammap:

RAM használtságát mutatja.



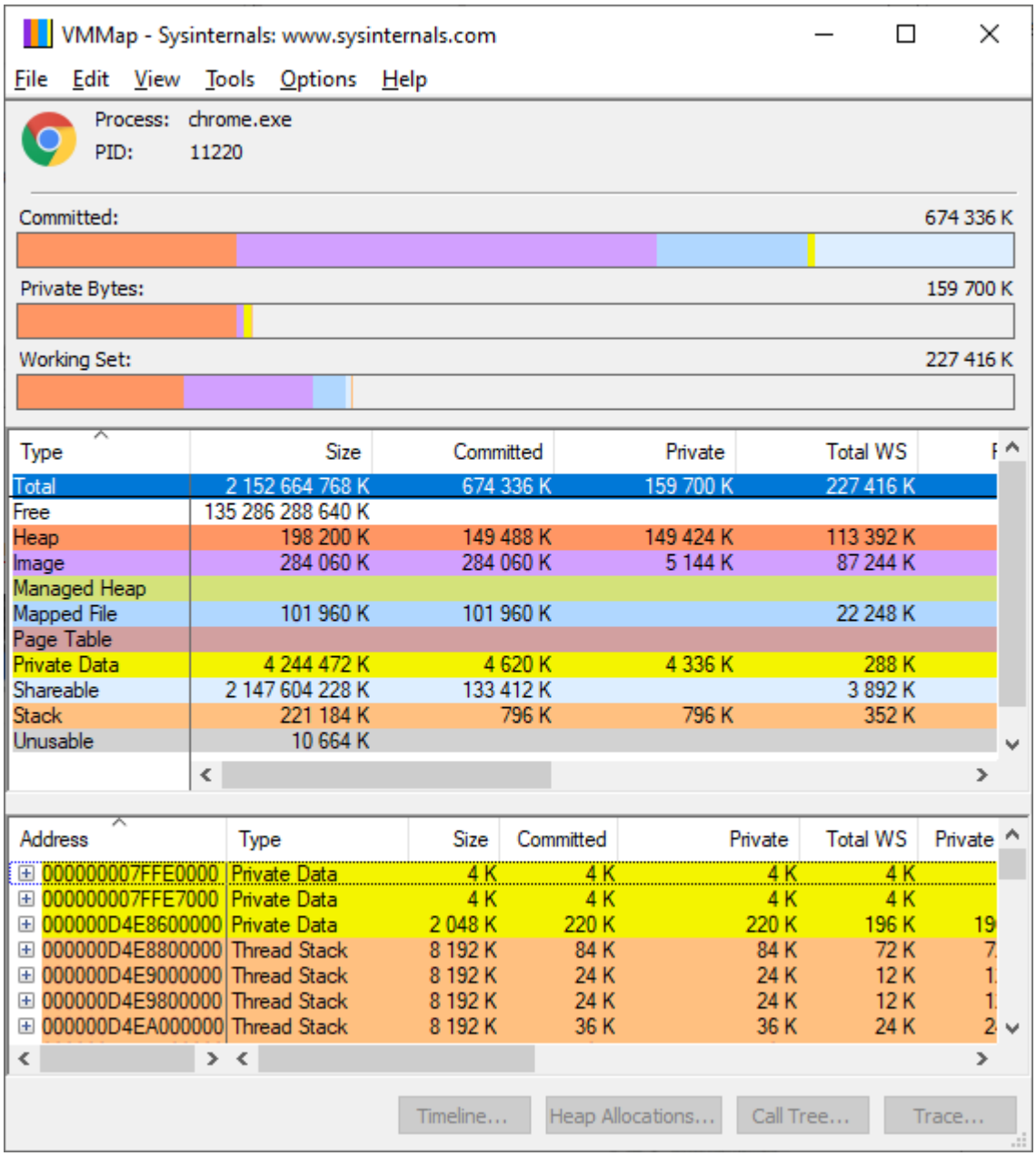
RamMap - Sysinternals: www.sysinternals.com

File Empty Settings Help

Use Counts | Processes | Priority Summary | Physical Pages | Physical Ranges | File Summary | File Details

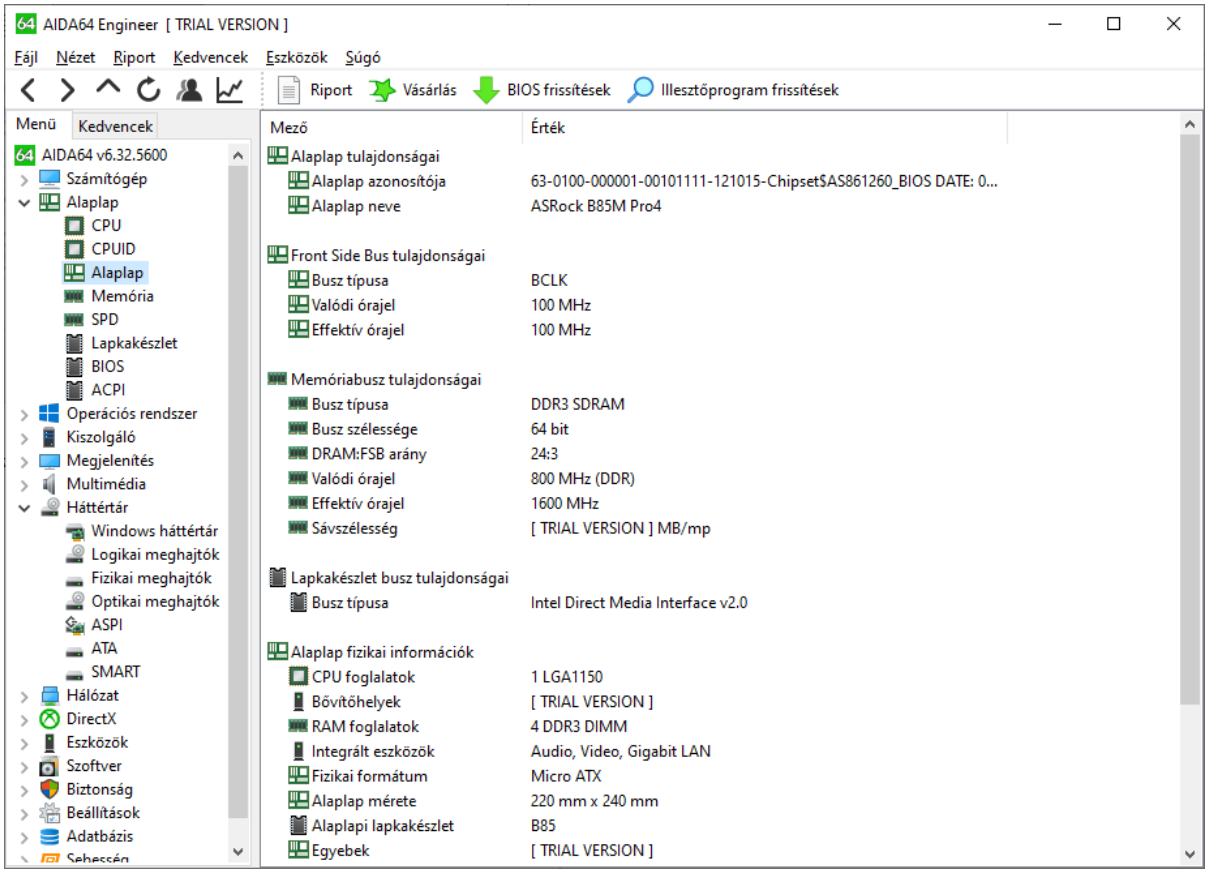
Usage	Total	Active	Standby	Modified	Modified ...	Transition
Process Private	3 799 480 K	3 605 168 K	76 168 K	118 124 K		20 K
Mapped File	2 568 952 K	1 264 532 K	1 302 612 K	1 808 K		
Shareable	412 488 K	403 664 K	392 K	8 432 K		
Page Table	196 708 K	196 708 K				
Paged Pool	449 840 K	449 832 K		8 K		
Nonpaged Pool	382 420 K	382 420 K				
System PTE	143 980 K	143 980 K				
Session Private	32 332 K	32 332 K				
Metafile	231 540 K	181 364 K	50 172 K		4 K	
AWE						
Driver Locked	12 816 K	12 816 K				
Kernel Stack	44 768 K	44 452 K	192 K	124 K		
Unused	30 340 K	20 736 K	4 K			
Large Page						
Total	8 305 664 K	6 738 004 K	1 429 540 K	128 496 K	4 K	20 K

Vmmap: Egy kiválasztott processz memóriatevékenységét lehet vizsgálni.

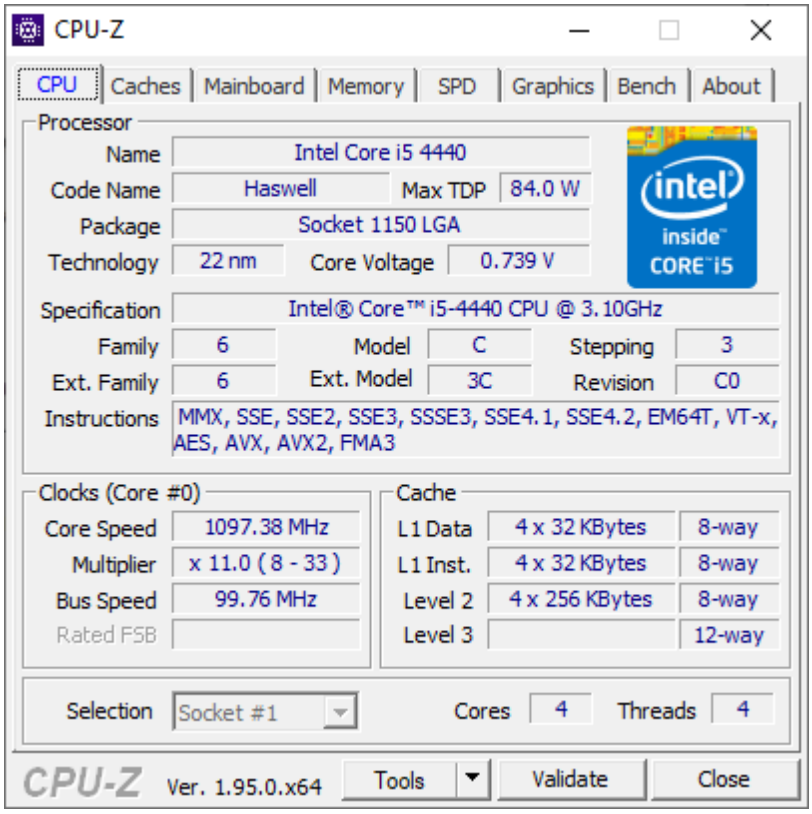


3.feladat-Rendszervizsgálat AIDA64, CPU-Z és GPU-Z szoftverekkel.

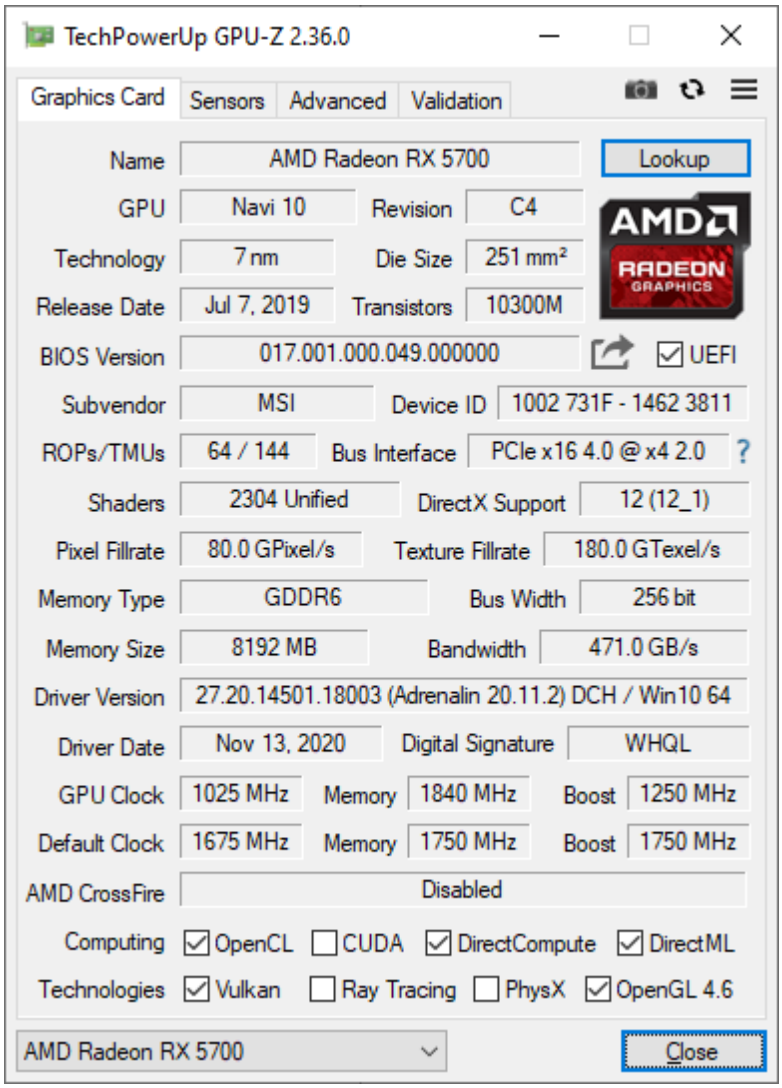
AIDA64-el megvizsgáltam az alaplap információit:

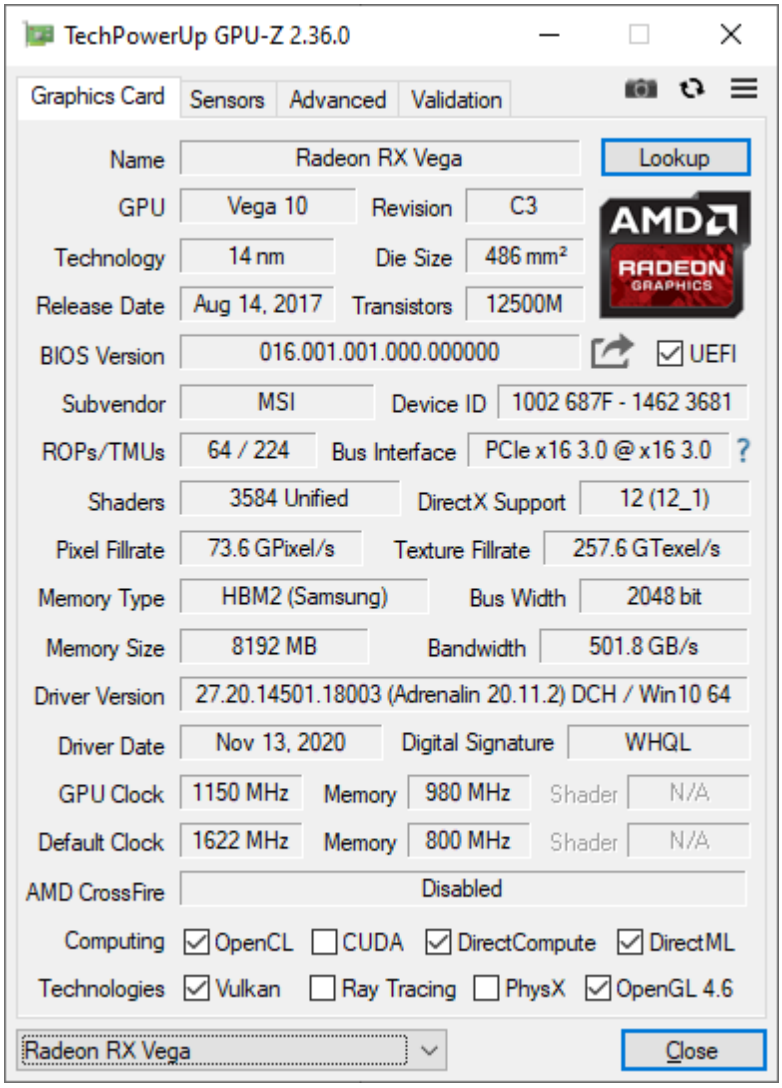


CPU-Z a processzor, memória stb. információt mutatja meg:



A GPU-Z-vel pedig a videókártyát lehet vizsgálni.

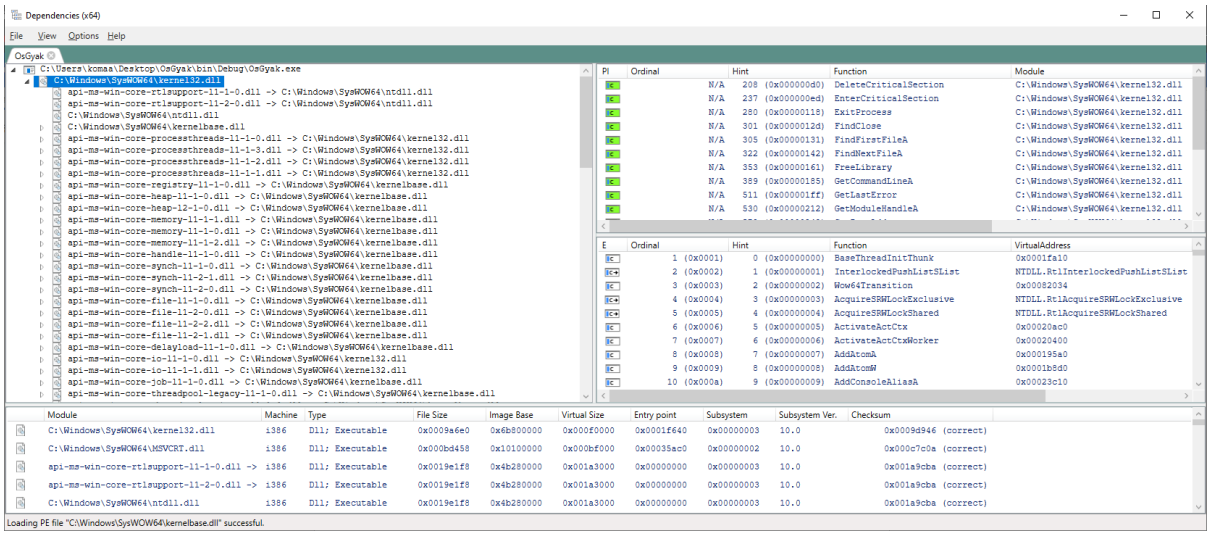




4.feladat-Dependency Walkerrel megvizsgálni, hogy egy egyszerű C program milyen API hívásokat tesz.

R3szy2.c forráskód:

```
#include <stdio.h>
#include <stdlib.h>

int main()
{
   FILE* fptr;

   fptr = fopen("vezeteknev.txt", "w");
```

```
    fprintf(fptr, "Nev: Horvath Akos\nSzak: Programtervezo Informatikus\nNeptun kod: R3SZY2\n");
    fclose(fptr);
    return 0;
}
```

Mivel a Dependecy Walker nem működött a számítógépemen, más programot használtam: