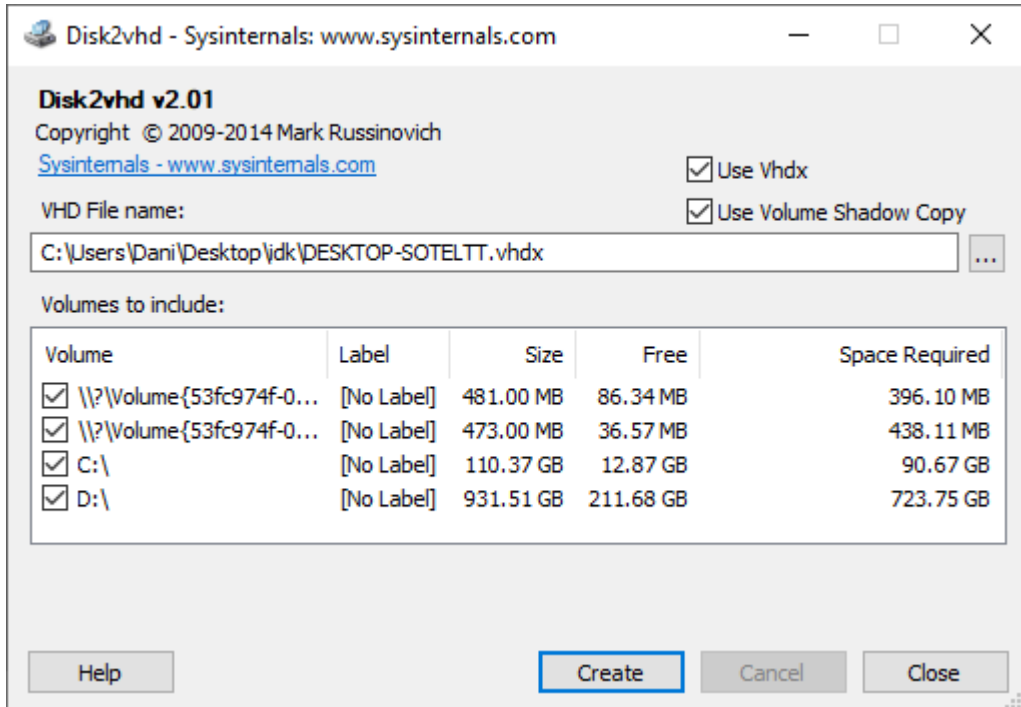


VS8KWD Gáncsos Dániel

A3 feladat:

a, a rendszeren lévő köteteket felsorolja és vhd fájlokat készít a kiválasztott kötetekről



b, részletes leírást nyújt az összes TCP és UDP végpontokról

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Proc...	0	TCP	desktop-solel...	60697	68.232.34.200	https	TIME_WAIT				
[System Proc...	0	TCP	desktop-solel...	60846	34.95.127.121	https	TIME_WAIT				
[System Proc...	0	TCP	desktop-solel...	60943	172.217.20.3	https	TIME_WAIT				
[System Proc...	0	TCP	desktop-solel...	60944	172.217.20.14	https	TIME_WAIT				
[System Proc...	0	TCP	desktop-solel...	60976	140.82.121.6	https	TIME_WAIT				
[System Proc...	0	TCP	desktop-solel...	60974	172.217.19.106	https	TIME_WAIT				
[System Proc...	0	TCP	desktop-solel...	60723	104.21.43.148	https	TIME_WAIT				
[System Proc...	0	TCP	desktop-solel...	60966	172.217.16.100	https	TIME_WAIT				
[System Proc...	0	TCP	desktop-solel...	60967	172.217.19.110	https	TIME_WAIT				
[System Proc...	0	TCP	desktop-solel...	60978	216.58.207.138	https	TIME_WAIT				
[System Proc...	0	TCP	desktop-solel...	60973	172.217.19.106	https	TIME_WAIT				
AdvancedW...	9768	TCP	desktop-solel...	58799	157.245.21.45	https	ESTABLISHED				
chrome.exe	7816	TCP	desktop-solel...	58695	142.250.102.188	5228	ESTABLISHED				
chrome.exe	7816	TCP	desktop-solel...	60969	185.199.110.154	https	ESTABLISHED				
chrome.exe	7816	TCP	desktop-solel...	60970	185.199.110.154	https	ESTABLISHED				
chrome.exe	7816	TCP	desktop-solel...	60971	185.199.108.133	https	ESTABLISHED				
chrome.exe	7816	TCP	desktop-solel...	60972	172.217.20.14	https	ESTABLISHED				
chrome.exe	7816	TCP	desktop-solel...	60979	140.82.113.26	https	ESTABLISHED				
chrome.exe	7804	UDP	DESKTOP-SOTE...	5353	*	*					
chrome.exe	7804	UDP	DESKTOP-SOTE...	5353	*	*					
chrome.exe	7804	UDP	DESKTOP-SOTE...	5353	*	*					
chrome.exe	7804	UDP	DESKTOP-SOTE...	5353	*	*					
chrome.exe	7804	UDP	DESKTOP-SOTE...	5353	*	*					
chrome.exe	7804	UDPv6	[0.0.0.0.0.0.0]	5353	*	*					
chrome.exe	7816	TCP	desktop-solel...	60990	172.217.20.3	https	ESTABLISHED	6	1315	5	1353
chrome.exe	7816	TCP	desktop-solel...	60991	216.58.207.163	https	ESTABLISHED	11	1806	8	1988
chrome.exe	7816	TCP	desktop-solel...	60992	216.58.214.238	https	ESTABLISHED	7	1153	6	2730
dashHost.exe	5652	UDP	DESKTOP-SOTE...	ws-discovery	*	*					
dashHost.exe	5652	UDP	DESKTOP-SOTE...	ws-discovery	*	*					
dashHost.exe	5652	UDP	DESKTOP-SOTE...	53162	*	*					
dashHost.exe	5652	UDPv6	[0.0.0.0.0.0.0]	3702	*	*					
dashHost.exe	5652	UDPv6	[0.0.0.0.0.0.0]	3702	*	*					
dashHost.exe	5652	UDPv6	[0.0.0.0.0.0.0]	53163	*	*					
Discord.exe	5700	TCP	DESKTOP-SOTE...	6463	DESKTOP-SOTE...	0	LISTENING				
Discord.exe	3428	TCP	desktop-solel...	59063	47.224.186.35.bc	https	ESTABLISHED	1	43	1	40
Discord.exe	3428	TCP	desktop-solel...	59252	162.159.130.235	https	ESTABLISHED	9	724	2	114
Discord.exe	3428	TCP	desktop-solel...	59958	162.159.133.234	https	ESTABLISHED	1	54	9	945
Discord.exe	3428	TCP	desktop-solel...	60629	162.159.137.232	https	ESTABLISHED				
Discord.exe	5700	UDP	DESKTOP-SOTE...	50484	*	*		146	19378	164	18260
Discord.exe	5700	UDP	DESKTOP-SOTE...	51524	*	*					
lsass.exe	728	TCP	DESKTOP-SOTE...	49664	DESKTOP-SOTE...	0	LISTENING				
lsass.exe	728	TCPv6	[0.0.0.0.0.0.0]	49664	[0.0.0.0.0.0.0]	0	LISTENING				
mredge.exe	1896	TCP	desktop-solel...	60736	185.199.108.133	https	ESTABLISHED				
mredge.exe	1896	TCP	desktop-solel...	60849	23.6.124.158	https	ESTABLISHED				
mredge.exe	1896	TCP	desktop-solel...	60857	23.6.124.158	https	ESTABLISHED				
mredge.exe	1896	TCP	desktop-solel...	60862	151.101.13.192	https	ESTABLISHED				
mredge.exe	11412	UDP	DESKTOP-SOTE...	5353	*	*					
mredge.exe	11412	UDP	DESKTOP-SOTE...	5353	*	*					
mredge.exe	11412	UDP	DESKTOP-SOTE...	5353	*	*					
mredge.exe	11412	UDP	DESKTOP-SOTE...	5353	*	*					
mredge.exe	11412	UDP	DESKTOP-SOTE...	5353	*	*					
mredge.exe	11412	UDPv6	[0.0.0.0.0.0.0]	5353	*	*					
mredge.exe	11412	UDPv6	[0.0.0.0.0.0.0]	5353	*	*					
services.exe	716	TCP	DESKTOP-SOTE...	49669	DESKTOP-SOTE...	0	LISTENING				
services.exe	716	TCPv6	[0.0.0.0.0.0.0]	49669	[0.0.0.0.0.0.0]	0	LISTENING				
Skype.exe	8244	TCP	desktop-solel...	60440	13.83.65.43	https	ESTABLISHED	1	2795	1	361
Skype.exe	8244	TCP	desktop-solel...	60442	13.83.65.43	https	ESTABLISHED				
Skype.exe	3488	TCP	desktop-solel...	60445	13.69.188.18	https	ESTABLISHED	1	57	1	46
Skype.exe	8244	TCP	desktop-solel...	60601	40.78.128.150	https	ESTABLISHED				
Skype.exe	3488	TCP	desktop-solel...	60638	52.114.104.82	https	ESTABLISHED	1	585	1	582
Skype.exe	8244	TCP	desktop-solel...	60988	13.94.251.244	https	ESTABLISHED				
Skype.exe	8244	TCP	desktop-solel...	60989	68.232.34.200	https	ESTABLISHED				
Skype.exe	3488	UDP	desktop-solel...	17622	*	*					
Skype.exe	3488	UDP	desktop-solel...	28631	*	*		39	10804	28	2109
Skype.exe	3488	UDP	desktop-solel...	40118	*	*					
Endpoints: 136 Established: 27 Listening: 24 Time Wait: 11 Close Wait: 0											

c, az operációs rendszeren futó processzeket listázza ki

Autoruns - Sysinternals: www.sysinternals.com						
File Entry Options Help						
Filter:						
<div> <div>Known DLLs</div> <div>Winlogon</div> <div>Winsock Providers</div> <div>Print Monitors</div> <div>LSA Providers</div> <div>Network Providers</div> <div>WMI</div> <div>Office</div> </div> <div> <div>Everything</div> <div>Logon</div> <div>Explorer</div> <div>Internet Explorer</div> <div>Scheduled Tasks</div> <div>Services</div> <div>Drivers</div> <div>Codecs</div> <div>Boot Execute</div> <div>Image Hijacks</div> <div>AppInit</div> </div>						
Autorun Entry	Description	Publisher	Image Path	Timestamp	Virus Total	
HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell				2021.02.23.13:00		
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	1953.12.11.3:58		
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	1953.12.11.3:58		
AdobeAAMUpdater-1.0	Adobe Updater Startup Utility	(Verified) Adobe Systems Incorporated	c:\program files (x86)\common files\adobe\adobe updater\adobeupdater.exe	2015.05.17.15:36		
Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2021.01.28.14:18		
Kraken USB APO Helper	Kraken USB APO Helper	(Verified) Razer USA Ltd.	c:\program files (x86)\vazer\razer_kra...	2017.06.30.7:15		
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		
USB Gamepad	WYunpeng MFC Application	(Verified) Shen Zhen Dragon Rise Ma...	c:\windows\usb vibration\7906\usb...	2008.12.09.4:27		
VMonitor\VMUNC	Monitor SnapShot Button	(Not verified) Vmicio Corporation	c:\program files (x86)\vmicio corpora...	2008.08.29.10:27		
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021.01.31.13:38		
com.squirrel.Teams.Teams	Microsoft Teams	(Verified) Microsoft 3rd Party Applicati...	c:\users\dani\appdata\local\microso...	2020.10.02.13:48		
Discord	Update	(Verified) Discord Inc.	c:\users\dani\appdata\local\discord...	2020.06.01.21:58		
EpicGamesLauncher	EpicGamesLauncher	(Verified) Epic Games Inc.	d:\epic games\epic games\launch...	2021.01.26.18:48		
Extension_game			File not found: C:\Users\Dani\AppData\Local\Microsoft\Windows\CurrentVersion\Run			
OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	c:\users\dani\appdata\local\microso...	1958.02.05.12:59		
Overwolf	Overwolf Launcher	(Verified) Overwolf Ltd	c:\program files (x86)\overwolf\over...	2020.12.03.7:37		
Skype for Desktop	Skype	(Verified) Skype Software Sarl	c:\program files (x86)\microsoft\skyp...	2018.10.12.17:32		
Spotify	Spotify	(Verified) Spotify AB	c:\users\dani\appdata\roaming\spoti...	2018.05.04.10:55		
Spotify Web Helper	Spotify WebHelper	(Verified) Spotify AB	c:\users\dani\appdata\roaming\spoti...	2018.05.04.10:53		
uTorrent	uTorrent	(Verified) BitTorrent Inc.	c:\users\dani\appdata\roaming\utor...	2020.12.09.1:05		
Wargaming.net Game C...	Wargaming.net Game Center	(Verified) Wargaming.net Limited	d:\wot\wargaming.net\gamecenter\...	2021.02.02.16:40		
Web Companion			File not found: C:\Program Files (x86)...			
C:\Users\Dani\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				2020.11.29.16:08		
hide.me VPNLink	hide.me VPN	(Verified) eVenture Limited	c:\program files (x86)\hide.me\vpn\h...	2019.12.02.9:57		
IMVULink			File not found: File			
mathpix-snipping-tool-link	Mathpix snipping tool	(Verified) Mathpix, Inc.	c:\users\dani\appdata\local\mathpix...	2020.10.08.10:53		
Tintaszint-felvezetetes			c:\users\dani\appdata\roaming\micr...	2021.02.15.7:33		
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2020.12.12.23:40		
Google Chrome	Google Chrome Installer	(Verified) Google LLC	c:\program files\google\chrome\appli...	2021.02.13.0:08		

d, figyelni hogy az aktivitást amikor egy felhasználó ki és bejelentkezik a rendszerbe

Kijelölés C:\Users\Dani\Desktop\jdk\logonsessions.exe

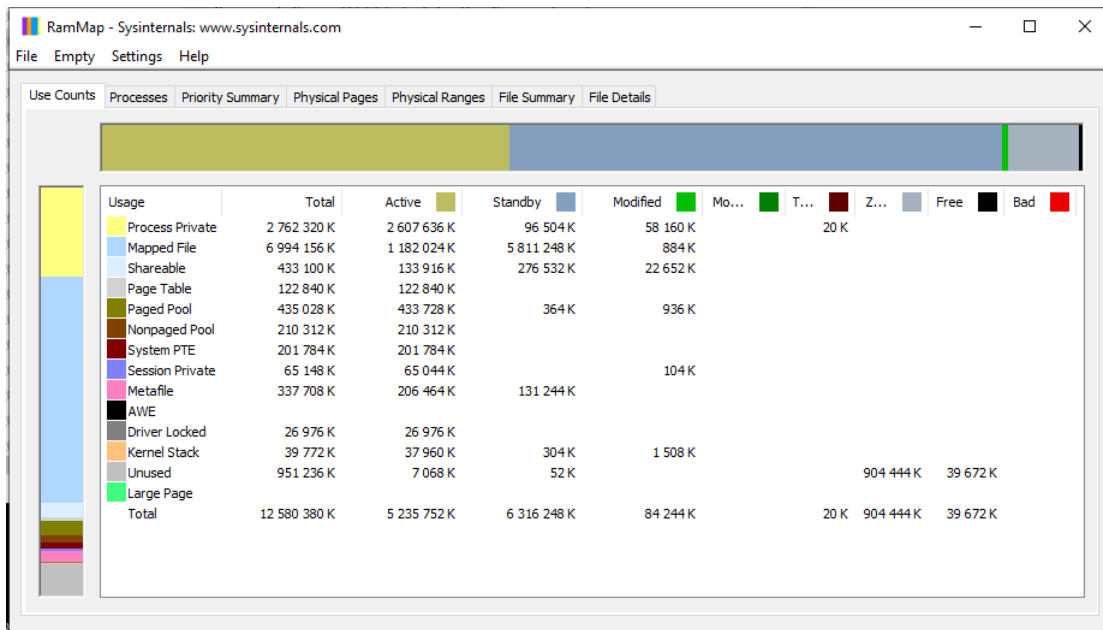
LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
User name: WORKGROUP\DESKTOP-SOTELTT\$
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: S-1-5-18
Logon time: 2021. 02. 23. 11:09:24
Logon server:
DNS Domain:
UPN:

[1] Logon session 00000000:0000c337:
User name:
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: (none)
Logon time: 2021. 02. 23. 11:09:24
Logon server:
DNS Domain:
UPN:

[2] Logon session 00000000:0000c7b2:
User name: Font Driver Host\UMFD-0
Auth package: Negotiate
Logon type: Interactive
Session: 0
Sid: S-1-5-96-0-0
Logon time: 2021. 02. 23. 11:09:24
Logon server:

e, figyelj a memóriahasználatot és a merevlemezre való írást



f, választott program: procmon. Feladata a processzek kimutatása

Time	Process Name	PID	Operation	Path	Result	Detail
14:29:...	MsMpEng.exe	3700	ReadFile	C:\Users\Dani\Desktop\ldk\Procmon6...	SUCCESS	Offset: 917 504, Le...
14:29:...	MsMpEng.exe	3700	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 073 856...
14:29:...	MsMpEng.exe	3700	ReadFile	C:\Users\Dani\Desktop\ldk\Procmon6...	SUCCESS	Offset: 983 040, Le...
14:29:...	MsMpEng.exe	3700	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 032 896...
14:29:...	MsMpEng.exe	3700	ReadFile	C:\Users\Dani\Desktop\ldk\Procmon6...	SUCCESS	Offset: 1 048 576, ...
14:29:...	MsMpEng.exe	3700	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 159 872...
14:29:...	MsMpEng.exe	3700	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 14 446 592...
14:29:...	MsMpEng.exe	3700	ReadFile	C:\Users\Dani\Desktop\ldk\Procmon6...	SUCCESS	Offset: 1 114 112, ...
14:29:...	explorer.exe	5672	ReadFile	C:\Windows\System32\UIAnimation.dll	SUCCESS	Offset: 212 480, Le...
14:29:...	svchost.exe	1920	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 690 688, Le...
14:29:...	ctfmon.exe	848	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS	Offset: 4 088 320, ...
14:29:...	MsMpEng.exe	3700	LockFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Exclusive: False, O...
14:29:...	MsMpEng.exe	3700	ReadFile	C:\Users\Dani\Desktop\ldk\Procmon6...	SUCCESS	Offset: 1 179 648, ...
14:29:...	explorer.exe	5672	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
14:29:...	MsMpEng.exe	3700	CloseFile	C:\Users\Dani\Desktop\ldk\Procmon6...	SUCCESS	
14:29:...	explorer.exe	5672	RegCloseKey	HKCU	SUCCESS	
14:29:...	MsMpEng.exe	3700	CloseFile	C:\Users\Dani\Desktop\ldk\Procmon6...	SUCCESS	
14:29:...	ctfmon.exe	848	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
14:29:...	ctfmon.exe	848	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
14:29:...	ctfmon.exe	848	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
14:29:...	ctfmon.exe	848	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
14:29:...	ctfmon.exe	848	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
14:29:...	ctfmon.exe	848	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...

Showing 223 619 of 627 799 events (35%) Backed by virtual memory

3, feladat

AIDA64: komoly diagnosztikai információkat készít a különböző hardwarekről ilyen pl a memória és a gyorsítótár felmérés, vagy a GPU / CPU teszt

AIDA64 Cache & Memory Benchmark

	Read	Write	Copy	Latency
Memory	9691 MB/s	TRIAL VERSION	TRIAL VERSION	82.6 ns
L1 Cache	TRIAL VERSION	63872 MB/s	129.97 GB/s	1.1 ns
L2 Cache	217.21 GB/s	55054 MB/s	102.58 GB/s	TRIAL VERSION
L3 Cache	96096 MB/s	21894 MB/s	42767 MB/s	TRIAL VERSION

CPU Type

HexaCore AMD FX-6300 (Vishera, Socket AM3+)

CPU Stepping

OR-C0

CPU Clock

3800.2 MHz (original: [TRIAL VERSION] MHz, overclock: 8%)

CPU FSB

200.0 MHz (original: 200 MHz)

CPU Multiplier

19x

North Bridge Clock

2000.1 MHz

Memory Bus

666.7 MHz

DRAM:FSB Ratio

20:6

Memory Type

Single Channel DDR3-1333 SDRAM (9-9-9-24 CR2)

Chipset

AMD 760G, AMD K15

Motherboard

[TRIAL VERSION]

BIOS Version

F2

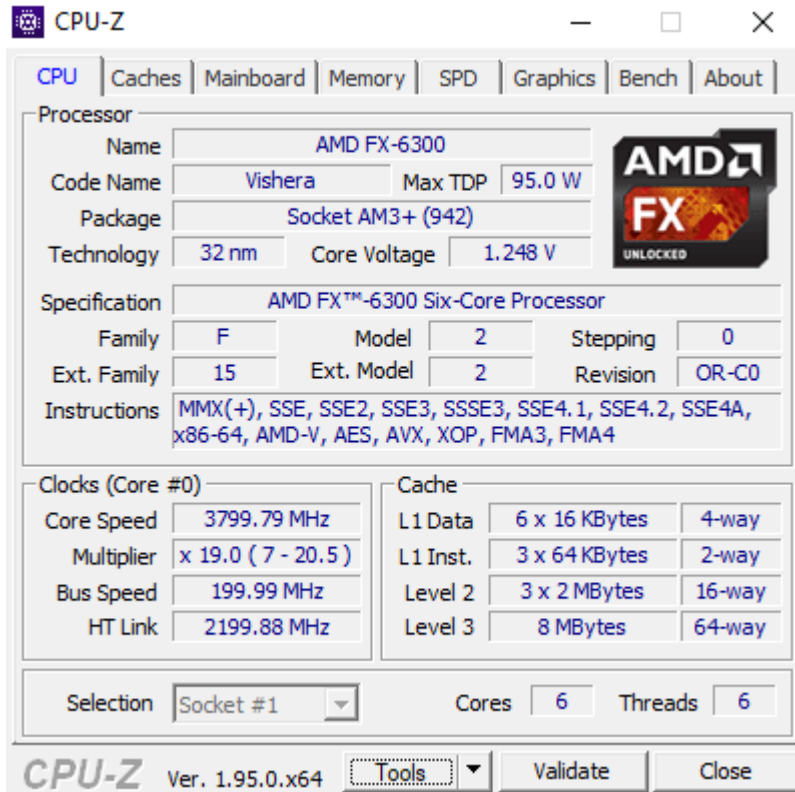
AIDA64 v6.32.5600 / BenchDLL 4.5.841.8-x64 (c) 1995-2020 FinalWire Ltd.

Save

Start Benchmark

Close

CPU-Z: Pontos információkat mutat a számítógép hardwares részéről, pl: CPU, Gyorsítótár, Alaplap, Memória, GPU stb.



GPU-Z: Információkat biztosít a számítógép videokártyáiról és azoknak a működéséről

TechPowerUp GPU-Z 2.37.0

Graphics CardSensorsAdvancedValidation

NameRadeon(TM) RX 460 GraphicsLookup

GPUBaffinRevisionCF

AMDRADEON GRAPHICS

Technology14 nmDie Size123 mm²

Release DateAug 8, 2016Transistors3000M

BIOS Version015.050.000.000.000000UEFI

SubvendorSapphire/PCPartnerDevice ID1002 67EF - 174B E348

ROPs/TMUs16 / 56Bus InterfacePCIe x8 3.0 @ x8 2.0?

Shaders896 UnifiedDirectX Support12 (12_0)

Pixel Fillrate19.4 GPixel/sTexture Fillrate67.8 GTexel/s

Memory TypeGDDR5 (Hynix)Bus Width128 bit

Memory Size2048 MBBandwidth112.0 GB/s

Driver Version27.20.1034.6 (Adrenalin 20.10.35.02) / Win10 64

Driver DateAug 21, 2020Digital SignatureWHQL

GPU Clock1210 MHzMemory1750 MHzShaderN/A

Default Clock1210 MHzMemory1750 MHzShaderN/A

AMD CrossFireDisabled

Computing☒ OpenCL☐ CUDA☒ DirectCompute☒ DirectML

Technologies☒ Vulkan☐ Ray Tracing☐ PhysX☒ OpenGL 4.6

Radeon(TM) RX 460 GraphicsClose