

Szeszák Ádám

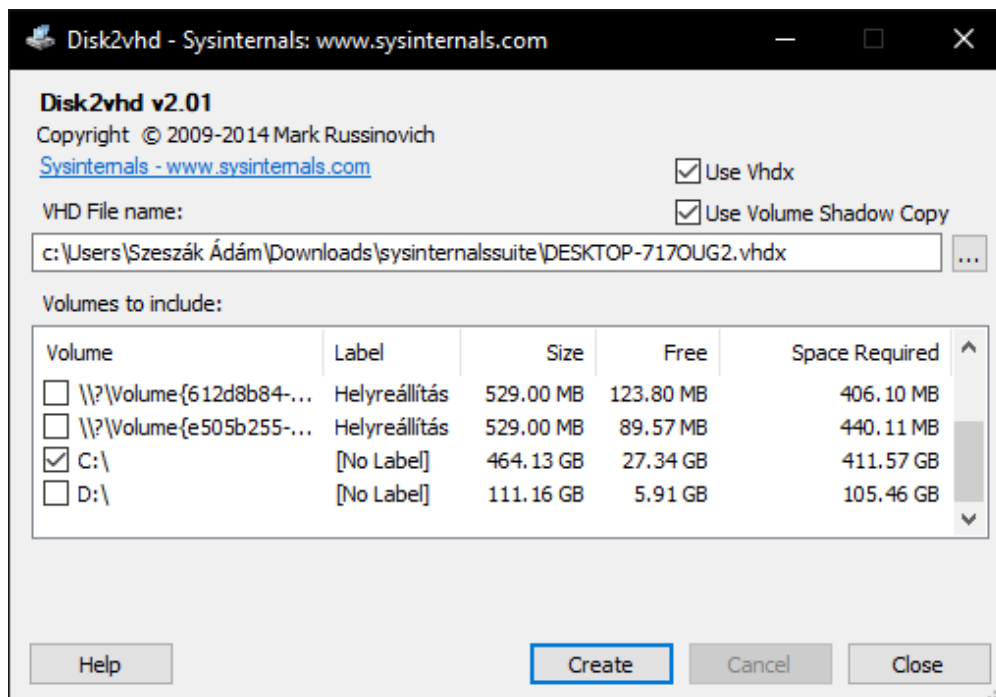
AZCTJJ

Operációs rendszerek gyakorlat 02.23

1. Feladat

a, Disk2vhd

Ez a program a kiválasztott merevlemezről készít vhd-t (Virtual Hard Disk), melyet virtuális gépen lehet használni. Nekem sajnos nem volt elegendő tárhelyem, így nem tudtam elkészíteni.



b, TCPView

Ez egy olyan program, mely listázza az összes TCP és UDP végpontot a rendszerünkön, local és remote címeit és státuszát a TCP kapcsolatoknak. Nekem elég sok volt, nem fért ki screenshotra az összes.

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-717oug2...	59194	162.159.136.232	https	TIME_WAIT				
[System Proc...	0	TCP	desktop-717oug2...	59195	162.159.136.232	https	TIME_WAIT				
[System Proc...	0	TCP	desktop-717oug2...	59459	52.109.88.174	https	TIME_WAIT				
[System Proc...	0	TCP	desktop-717oug2...	59460	52.109.88.174	https	TIME_WAIT				
[System Proc...	0	TCP	desktop-717oug2...	59461	52.109.88.174	https	TIME_WAIT				
[System Proc...	0	TCPV6	[2001:4c4d:1443...	59359	[2606:2800:133:f1...	https	TIME_WAIT				
[System Proc...	0	TCPV6	[2001:4c4d:1443...	59443	[2a00:1450:400d...	https	TIME_WAIT				
[System Proc...	0	TCPV6	[2001:4c4d:1443...	59415	[2a03:2880:f1#63...	https	TIME_WAIT				
ABService.exe	4416	TCP	DESKTOP-7170U...	2008	DESKTOP-7170U...	0	LISTENING				
ABService.exe	4416	TCP	DESKTOP-7170U...	6045	DESKTOP-7170U...	0	LISTENING				
ABService.exe	4416	UDP	DESKTOP-7170U...	2015	*	*					
AppleMobileD...	12300	TCP	DESKTOP-7170U...	27015	localhost	51098	ESTABLISHED				
AppleMobileD...	12300	TCP	DESKTOP-7170U...	27015	DESKTOP-7170U...	0	LISTENING				
AppleMobileD...	12300	TCP	DESKTOP-7170U...	59324	localhost	5354	ESTABLISHED				
AppleMobileD...	12300	TCP	DESKTOP-7170U...	59325	localhost	5354	ESTABLISHED				
AppleMobileD...	12300	UDP	DESKTOP-7170U...	49278	*	*					
AppleMobileD...	12300	UDP	DESKTOP-7170U...	49279	*	*					
brave.exe	22340	TCP	desktop-717oug2...	58573	ec2-52-43-181-58...	https	ESTABLISHED	3		408	297
brave.exe	22340	TCP	desktop-717oug2...	58971	185.193.110.133	https	ESTABLISHED				
brave.exe	22340	TCP	desktop-717oug2...	58990	140.82.114.26	https	ESTABLISHED	1	30		26
brave.exe	10560	UDP	DESKTOP-7170U...	5353	*	*				8	312
brave.exe	10560	UDP	DESKTOP-7170U...	5353	*	*					
brave.exe	10560	UDP	DESKTOP-7170U...	5353	*	*					
brave.exe	22340	TCPV6	[2001:4c4d:1443...	52592	[2606:4700:0:0:0...	https	ESTABLISHED	2	3770		7930
brave.exe	22340	TCPV6	[2001:4c4d:1443...	54055	[2606:4700:0:0:0...	https	ESTABLISHED	1	61		59
brave.exe	22340	TCPV6	[2001:4c4d:1443...	59113	[2a04:4e42:1b:0:0...	https	ESTABLISHED				
brave.exe	22340	TCPV6	[2001:4c4d:1443...	59328	[2a04:4e42:3:0:0...	https	ESTABLISHED				
brave.exe	22340	TCPV6	[2001:4c4d:1443...	59329	[2a04:4e42:3:0:0...	https	ESTABLISHED				
brave.exe	10560	UDPV6	[0:0:0:0:0:0:0:0]	5353	[2a03:2880:f0f1:e1...	https	ESTABLISHED	5	253		146
brave.exe	10560	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*					
chrome.exe	26900	UDP	DESKTOP-7170U...	5353	*	*				8	312
chrome.exe	26900	UDP	DESKTOP-7170U...	5353	*	*					
chrome.exe	26900	UDP	DESKTOP-7170U...	5353	*	*					
chrome.exe	26900	UDP	DESKTOP-7170U...	5353	*	*					
chrome.exe	26900	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*					
chrome.exe	26900	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*					
Discord.exe	23408	TCP	DESKTOP-7170U...	6463	DESKTOP-7170U...	0	LISTENING				
Discord.exe	17496	TCP	desktop-717oug2...	60607	162.159.130.234	https	ESTABLISHED	1	54		33
EpicGamesLa...	14636	TCP	desktop-717oug2...	59344	54.80.64.179	https	ESTABLISHED				
EpicGamesLa...	14636	TCP	desktop-717oug2...	59441	3.210.121.233	https	CLOSE_WAIT				31
EpicGamesLa...	14636	TCP	desktop-717oug2...	59474	34.204.64.129	https	ESTABLISHED	1	2909		3699
EXCELE.exe	13064	UDP	DESKTOP-7170U...	57020	*	*					
IvCam.exe	9016	TCP	DESKTOP-7170U...	5895	DESKTOP-7170U...	0	LISTENING				
IvCam.exe	9016	TCP	DESKTOP-7170U...	6149	DESKTOP-7170U...	0	LISTENING				
IvCam.exe	9016	TCP	DESKTOP-7170U...	51098	localhost	27015	ESTABLISHED				
IvCam.exe	9016	TCP	DESKTOP-7170U...	51140	localhost	5354	ESTABLISHED				
IvCam.exe	9016	UDP	DESKTOP-7170U...	5895	*	*					
java.exe	5548	TCP	DESKTOP-7170U...	59518	DESKTOP-7170U...	0	LISTENING				
java.exe	5548	TCPV6	[0:0:0:0:0:0:0:0]	59518	[0:0:0:0:0:0:0:0]	0	LISTENING				
LCORE.exe	1316	UDP	DESKTOP-7170U...	54915	*	*		42	11046		11046
LCORE.exe	1316	UDPV6	[0:0:0:0:0:0:0:0]	54915	*	*					
Isass.exe	1068	TCP	DESKTOP-7170U...	49664	DESKTOP-7170U...	0	LISTENING				
Isass.exe	1068	TCPV6	[0:0:0:0:0:0:0:0]	49664	[0:0:0:0:0:0:0:0]	0	LISTENING				
mDNSRespo...	4424	TCP	DESKTOP-7170U...	5354	DESKTOP-7170U...	0	LISTENING				
mDNSRespo...	4424	TCP	DESKTOP-7170U...	5354	localhost	51140	ESTABLISHED				
mDNSRespo...	4424	TCP	DESKTOP-7170U...	5354	localhost	59324	ESTABLISHED				
mDNSRespo...	4424	TCP	DESKTOP-7170U...	5354	localhost	59325	ESTABLISHED				
mDNSRespo...	4424	UDP	desktop-717oug2...	5353	*	*				4	156
mDNSRespo...	4424	UDP	192.168.56.1	5353	*	*					
mDNSRespo...	4424	UDP	DESKTOP-7170U...	49868	*	*					
mDNSRespo...	4424	UDPV6	[0:0:0:0:0:0:0:1]	5353	*	*					
mDNSRespo...	4424	UDPV6	[0:0:0:0:0:0:0:0]	49869	*	*					
OneDrive.exe	8720	TCP	desktop-717oug2...	59179	51.103.5.186	https	ESTABLISHED	1	45		176
services.exe	1056	TCP	DESKTOP-7170U...	49621	DESKTOP-7170U...	0	LISTENING				
Endpoints: 190	Established: 40	Listening: 42	Time Wait: 8	Close Wait: 14							

c, Process Utilities

Autoruns: Ez a program megmutatja, melyek azok az alkalmazások, amelyek a rendszer bootolása alatt vagy bejelentkezéskor indulnak és mikor indítunk windows alkalmazásokat, pl Explorer. Hasznos alkalmazás, ki lehet benne kapcsolni a rendszerindításkor nem kívánatos programokat a baloldali pipa kiszedésével.

Autoruns - Sysinternals: www.sysinternals.com

FileEntryOptionsHelp

Filter:

KnownDLLs

Logon

Explorer

Internet Explorer

Scheduled Tasks

Services

Drivers

Codecs

Boot Execute

Image Hijacks

Applint

Winlogon

Winsock Providers

Print Monitors

LSA Providers

Network Providers

WMI

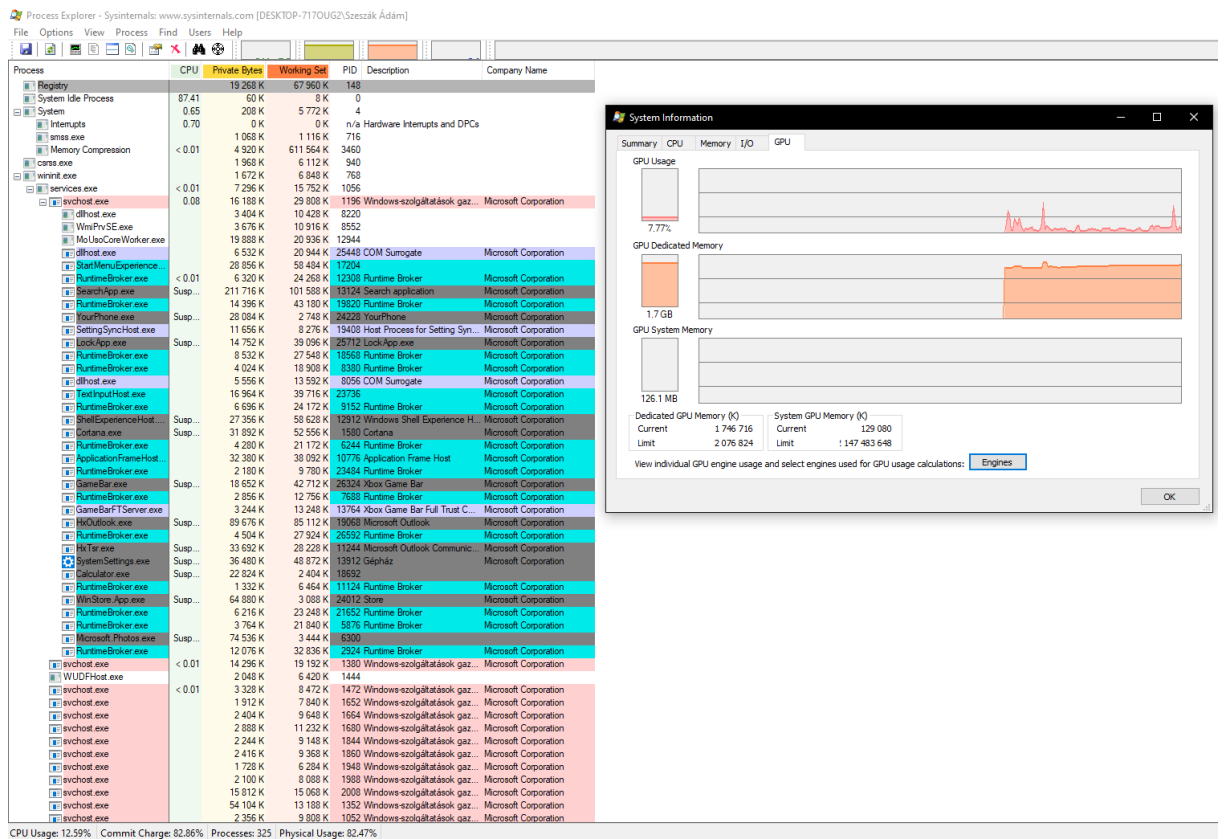
Office

Autorun Entry	Description	Publisher	Image Path	Timestamp	Virus Total
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				2019. 12. 07. 10:15	
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	1953. 12. 11. 3:58	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021. 02. 19. 22:31	
<input checked="" type="checkbox"/> hpdfe	HP Slate Message Application	(Verified) Hewlett-Packard	c:\program files\hp\shared\hpdfe.exe	2015. 08. 21. 17:52	
<input checked="" type="checkbox"/> Launch LCore	Logitech Gaming Framework	(Verified) Logitech Inc.	c:\program files\logitech\gaming soft...	2018. 10. 05. 9:27	
<input checked="" type="checkbox"/> Riot Vanguard	Vanguard tray notification.	(Verified) Riot Games, Inc.	c:\program files\riot_vanguard\vgtray...	2021. 01. 22. 21:31	
<input checked="" type="checkbox"/> RtkAudUService	Realtek HD Audio Universal Service	(Verified) Realtek Semiconductor Corp.	c:\windows\system32\rtkaudservic...	2019. 06. 13. 7:58	
<input checked="" type="checkbox"/> Screen+	AOC grid screen executable file	(Verified) AOC International (Europe) ...	c:\program files\screen+\screenlm64...	2014. 08. 06. 12:20	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2021. 02. 19. 22:31	
<input checked="" type="checkbox"/> BrStaMon00	Status Monitor Application	(Not verified) Brother Industries, Ltd.	c:\program files (x86)\brozny02\bro...	2014. 05. 22. 5:50	
<input checked="" type="checkbox"/> StartCCC	Catalyst® Control Center Launcher	(Verified) Advanced Micro Devices, L...	c:\program files (x86)\ati technologie...	2014. 08. 12. 3:55	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021. 02. 11. 15:44	
<input checked="" type="checkbox"/> com.squirrel.Teams.Teams	Microsoft Teams	(Verified) Microsoft 3rd Party Applicati...	c:\users\szeszak Adam\appdata\loc...	2020. 10. 02. 13:48	
<input checked="" type="checkbox"/> Discord	Update	(Verified) Discord Inc.	c:\users\szeszak Adam\appdata\loc...	2020. 06. 01. 21:58	
<input checked="" type="checkbox"/> EpicGamesLauncher	EpicGamesLauncher	(Verified) Epic Games Inc.	c:\program files (x86)\epic games\lau...	2021. 02. 16. 14:42	
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	c:\users\szeszak Adam\appdata\loc...	2021. 03. 10. 16:03	
<input checked="" type="checkbox"/> Overwolf	Overwolf Launcher	(Verified) Overwolf Ltd	c:\program files (x86)\overwolf\over...	2020. 12. 03. 7:37	
<input checked="" type="checkbox"/> qBittorrent	qBittorrent - A BitTorrent Client	(Not verified) The qBittorrent Project	c:\program files (x86)\qbittorrent\qbitt...	2020. 11. 24. 23:20	
<input checked="" type="checkbox"/> Screenpresso	Screenpresso	(Verified) Leampulse	c:\users\szeszak Adam\appdata\loc...	2021. 02. 16. 16:03	
<input checked="" type="checkbox"/> Spotify	Spotify	(Verified) Spotify AB	c:\users\szeszak Adam\appdata\voa...	2021. 02. 18. 17:19	
<input checked="" type="checkbox"/> Steam	Steam Client Bootstrapper	(Verified) Valve	c:\program files (x86)\steam\steam.exe	2021. 02. 13. 0:23	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce				2021. 02. 19. 22:31	
<input checked="" type="checkbox"/> Application Restart #0	Brave Browser	(Verified) Brave Software, Inc.	c:\program files\bravesoftware\brave...	2021. 02. 13. 0:08	
C:\Users\Szeszak Adam\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				2021. 02. 10. 9:21	
<input checked="" type="checkbox"/> Xilinx Information Center...		(Verified) Xilinx Inc	d:\xilinx\vic\vic.exe	2017. 07. 08. 7:59	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2020. 12. 07. 17:13	
<input checked="" type="checkbox"/> Brave	Brave Installer	(Verified) Brave Software, Inc.	c:\program files\bravesoftware\brave...	2021. 02. 13. 0:08	
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	(Verified) Google LLC	c:\program files\google\chrome\appli...	2021. 02. 13. 0:08	
<input checked="" type="checkbox"/> Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge...	2021. 02. 17. 4:41	
<input checked="" type="checkbox"/> n/a	Microsoft .NET IIE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\system32\mscorlib.dll	2019. 10. 25. 4:45	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				2020. 12. 01. 19:02	
<input checked="" type="checkbox"/> n/a	Microsoft .NET IIE SECURITY REGIS...	(Verified) Microsoft Corporation	c:\windows\syswow64\mscorlib.dll	2019. 10. 25. 9:48	
HKLM\SOFTWARE\Classes\Protocols\Filter				2021. 02. 03. 0:23	
<input checked="" type="checkbox"/> text/xml	Microsoft Office XML MIME Filter	(Verified) Microsoft Corporation	c:\program files\microsoft office\root\...	2020. 12. 28. 23:39	
HKLM\SOFTWARE\Classes\Protocols\Handler				2021. 02. 03. 0:23	
<input checked="" type="checkbox"/> mso-minsb-roaming.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft office\root\...	2020. 12. 28. 23:33	
<input checked="" type="checkbox"/> mso-minsb.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft office\root\...	2020. 12. 28. 23:33	
<input checked="" type="checkbox"/> osf-roaming.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft office\root\...	2020. 12. 28. 23:33	
<input checked="" type="checkbox"/> osf.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft office\root\...	2020. 12. 28. 23:33	
HKLM\Software\Classes\ShellEx\ContextMenuHandlers				2020. 11. 28. 11:12	
<input checked="" type="checkbox"/> ANotepad++64	ShellHandler for Notepad++ (64 bit)	(Verified) Notepad++	c:\program files\notepad++\nppshell...	2014. 05. 12. 10:49	
<input checked="" type="checkbox"/> PowerISO	PowerISO Shell DLL	(Verified) Power Software Limited	c:\program files\poweriso\pwisosh.dll	2020. 11. 05. 0:26	
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers				2020. 11. 28. 11:12	

Ready.

Signed Windows Entries Hidden.

Process Explorer: Megmutatja, mely kezelők és DLL processzek vannak megnyitva, használatban. A bal oldalon láthatóak az aktív processzek, jobb oldalon pedig a módtól függ: handle módban a kiválasztott kezelők láthatóak, DLL módban pedig a memóriahasználatot mutatja.



Process Monitor: Valós idejű fájlrendszer, registry, process/thread aktivitást monitorozó program.

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
14:29:...	Skype.exe	12792	UDP Receive	DESKTOP-7170UG21.hu:2581 -> 13.6...	SUCCESS	Length: 201, seqn...
14:29:...	ctfmon.exe	19396	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS	Offset: 4 088 320, ...
14:29:...	Explorer.EXE	1412	ReadFile	C:\Windows\System32\UIAnimation.dll	SUCCESS	Offset: 212 480, Le...
14:29:...	Explorer.EXE	1412	ReadFile	C:\Windows\System32\UIAnimation.dll	SUCCESS	Offset: 193 536, Le...
14:29:...	Explorer.EXE	1412	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
14:29:...	ctfmon.exe	19396	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
14:29:...	ctfmon.exe	19396	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
14:29:...	Explorer.EXE	1412	RegCloseKey	HKCU	SUCCESS	
14:29:...	ctfmon.exe	19396	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
14:29:...	ctfmon.exe	19396	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
14:29:...	ctfmon.exe	19396	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
14:29:...	ctfmon.exe	19396	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
14:29:...	ctfmon.exe	19396	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Type: REG_DWO...
14:29:...	ctfmon.exe	19396	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
14:29:...	ctfmon.exe	19396	RegQueryKey	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
14:29:...	ctfmon.exe	19396	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
14:29:...	ctfmon.exe	19396	RegQueryValue	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Type: REG_DWO...
14:29:...	Explorer.EXE	1412	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
14:29:...	ctfmon.exe	19396	RegCloseKey	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
14:29:...	Explorer.EXE	1412	RegCloseKey	HKCU	SUCCESS	
14:29:...	ctfmon.exe	19396	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
14:29:...	ctfmon.exe	19396	RegCloseKey	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
14:29:...	ctfmon.exe	19396	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
14:29:...	ctfmon.exe	19396	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
14:29:...	ctfmon.exe	19396	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
14:29:...	ctfmon.exe	19396	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
14:29:...	ctfmon.exe	19396	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
14:29:...	ctfmon.exe	19396	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
14:29:...	ctfmon.exe	19396	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
14:29:...	ctfmon.exe	19396	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
14:29:...	ctfmon.exe	19396	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
14:29:...	ctfmon.exe	19396	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
14:29:...	Explorer.EXE	1412	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
14:29:...	ctfmon.exe	19396	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
14:29:...	ctfmon.exe	19396	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
14:29:...	Explorer.EXE	1412	RegCloseKey	HKCU	SUCCESS	
14:29:...	ctfmon.exe	19396	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
14:29:...	ctfmon.exe	19396	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
14:29:...	ctfmon.exe	19396	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
14:29:...	ctfmon.exe	19396	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
14:29:...	ctfmon.exe	19396	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
14:29:...	ctfmon.exe	19396	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
14:29:...	ctfmon.exe	19396	RegCloseKey	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
14:29:...	ctfmon.exe	19396	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
14:29:...	ctfmon.exe	19396	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
14:29:...	Explorer.EXE	1412	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
14:29:...	ctfmon.exe	19396	RegQueryValue	HKCU\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 16
14:29:...	ctfmon.exe	19396	RegCloseKey	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
14:29:...	Explorer.EXE	1412	RegCloseKey	HKCU	SUCCESS	
14:29:...	ctfmon.exe	19396	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
14:29:...	ctfmon.exe	19396	RegOpenKey	HKLM\Software\Microsoft\Input\Locale...	SUCCESS	Desired Access: R...
14:29:...	ctfmon.exe	19396	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	Type: REG_DWO...
14:29:...	ctfmon.exe	19396	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	
14:29:...	Explorer.EXE	1412	RegOpenKey	HKCU	SUCCESS	Desired Access: Q...
14:29:...	ctfmon.exe	19396	QueryNameInfo...	C:\Users\Szeszák Ádám\Downloads\sy...	SUCCESS	Name: \Users\Sze...
14:29:...	Explorer.EXE	1412	RegCloseKey	HKCU	SUCCESS	
14:29:...	ctfmon.exe	19396	ReadFile	C:\Windows\System32\CoreUICompon...	SUCCESS	Offset: 2 686 464, ...
14:29:...	Explorer.EXE	1412	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
14:29:...	Explorer.EXE	1412	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
14:29:...	Explorer.EXE	1412	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
14:29:...	Explorer.EXE	1412	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...	NAME NOT FOUND	Desired Access: R...
14:29:...	Explorer.EXE	1412	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...	NAME NOT FOUND	Desired Access: R...

Showing 140 829 of 410 313 events (34%)

Backed by virtual memory

d, Security Utilities
LogonSession

Listázza az aktív logon sessionöket, -p opció hozzáadásával a processzeket amik futnak egyes részek alatt.

C:\> Administrator: Parancssor

C:\Users\Szeszák Ádám\Downloads\sysinternalsuite>logonsessions64

LogonSessions v1.41 - Lists logon session information

Copyright (C) 2004-2020 Mark Russinovich

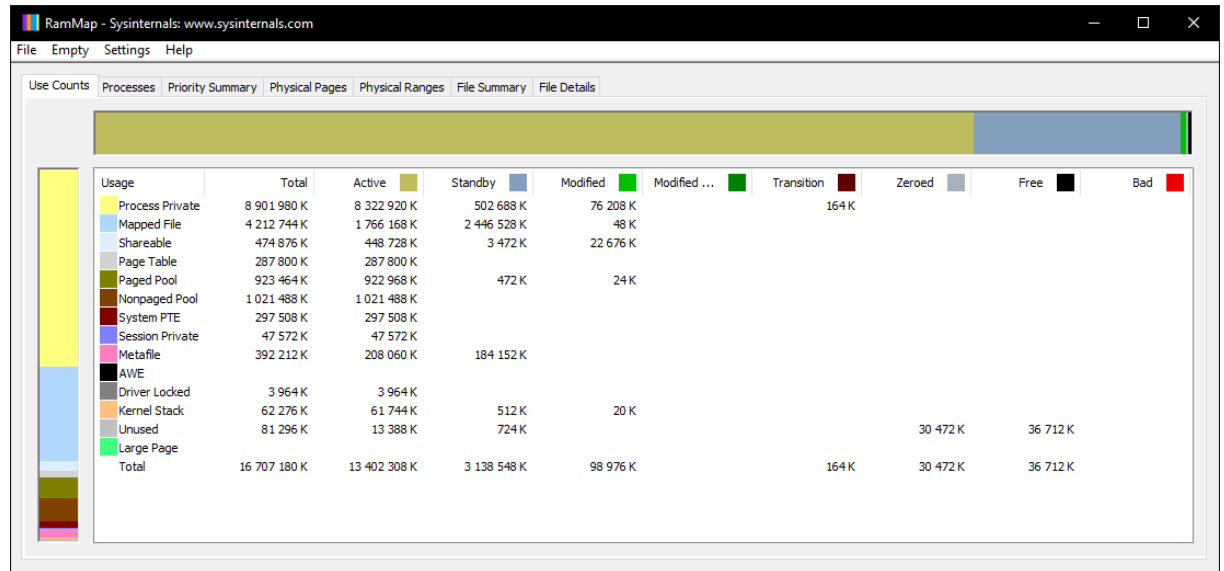
Sysinternals - www.sysinternals.com

- [0] Logon session 00000000:000003e7:
User name: WORKGROUP\DESKTOP-717OUG2\$
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: S-1-5-18
Logon time: 2021. 02. 19. 22:30:57
Logon server:
DNS Domain:
UPN:
- [1] Logon session 00000000:000115c5:
User name:
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: (none)
Logon time: 2021. 02. 19. 22:30:57
Logon server:
DNS Domain:
UPN:
- [2] Logon session 00000000:00011a5c:
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. 19. 22:30:57
Logon server:
DNS Domain:
UPN:
- [3] Logon session 00000000:000003e4:
User name: WORKGROUP\DESKTOP-717OUG2\$
Auth package: Negotiate
Logon type: Service
Session: 0
Sid: S-1-5-20
Logon time: 2021. 02. 19. 22:30:58
Logon server:
DNS Domain:
UPN:
- [4] Logon session 00000000:000003e5:
User name: NT AUTHORITY\HELYI SZOLG^LLTAT^LS
Auth package: Negotiate
Logon type: Service
Session: 0
Sid: S-1-5-19
Logon time: 2021. 02. 19. 22:30:58
Logon server:
DNS Domain:
UPN:

e, Information Utilities

RAMMap

Ez a program a memóriahasználatot analizálja, mely segítségével megnézhetjük, hogy a Windows hogyan címezi a fizikai memóriát, mennyit cachel a RAM-ban, mennyi RAM van felhasználva a kernel és a driverek által.



3, Aida64_Engineer

Rendszerinformációs szoftver, részletes információkat szolgáltat a hardverkomponensekről, telepített programokról, képes a számítógép teljesítményének mérésére, hibák felderítésében segít. Szolgáltatásai:

- Hardverfelismerés
- Teljesítménymérés
- Hardverdiagnosztika, stabilitástesz
- Érzékelőfigyelés
- Érzékelőadatok kijelzése, riasztás
- Szoftveranalitika
- Automatizálható riportkészítés

Én egy HTML sebesség riportot készítettem, ahol a processzorom sebességét méri össze a piacon lévő többi processzorral, hogy a listában hol szerepel illetve a számítógépemben lévő hardvereket listázza.

64 Riport - AIDA64

Fájl
 Mentés fájlba Küldés e-mailben Küldés a FinalWire-nak Nyomtatási kép Nyomtatás Bezárás

Összegzés

Számítógép:

Számítógép típusa	ACPI x64-alapú PC
Operációs rendszer	Microsoft Windows 10 Enterprise
Opr. javítócsomag	[TRIAL VERSION]
Internet Explorer	11.789.19041.0
Edge	88.0.705.74
DirectX	DirectX 12.0
Számítógépnév	DESKTOP-717OUG2
Felhasználó neve	Szeszák Ádám
Beléptető tartomány	[TRIAL VERSION]
Dátum / idő	2021-02-23 / 14:43

Alaplap:

CPU típusa	HexaCore AMD Ryzen 5 2600X, 4041 MHz (40.5 x 100)
Alaplap neve	ASRock B450 Pro4 (4 PCI-E x1, 2 PCI-E x16, 2 M.2, 4 DDR4 DIMM, Audio, Video, Gigabit LAN)
Alaplap lapkakészlet	AMD B450, AMD Talshan, AMD K17 IMC
Rendszermemória	[TRIAL VERSION]
DIMM2: Kingston HyperX KHX3200C16D4/8GX	[TRIAL VERSION]
DIMM4: Kingston HyperX KHX3200C16D4/8GX	[TRIAL VERSION]
BIOS típusa	AMI (12/12/2019)
Kommunikációs port	Communications Port (COM1)

Megjelenítés:

Videokártya	AMD Radeon R7 200 Series (2 GB)
Videokártya	AMD Radeon R7 200 Series (2 GB)
Videokártya	AMD Radeon R7 200 Series (2 GB)
Videokártya	AMD Radeon R7 200 Series (2 GB)
3D gyorsító	AMD Radeon R7 250 (Oland)
Képernyő	Általános PnP képernyő [NoDB] (PWPLBJA000958)
Képernyő	AOC 27G2G3 [NoDB] (LYDEE0028500)

Multimédia:

Hangkártya	ATI Radeon HDMI @ AMD Cape Verde/Pitcairn/Curacao/Heathrow/Chelsea/Venus - High Definition Audio Controller
Hangkártya	Realtek ALC892 @ AMD K17 - High Definition Audio Controller

Háttértár:

IDE vezérlő	AMD SATA Controller
IDE vezérlő	Szabványos SATA AHCI-vezérlő
Háttértár vezérlő	Asmedia 106x SATA Controller
Háttértár vezérlő	Microsoft tárolóhely-vezérlő
Háttértár vezérlő	Microsoft VHD visszacsatoló adapter
Háttértár vezérlő	Samsung NVMe Controller
Háttértár vezérlő	Xvdd SCSI Miniport
Lemez meghajtó	KINGSTON SA400S37120G (120 GB, SATA-III)
Lemez meghajtó	NVMe Samsung SSD 870 EVO SCSI Disk Device (465 GB)

Kész 381 KB

CPU-Z

A fő hardvereket és paramétereiket listázza ki a számítógépről.

CPU-Z

CPU | Caches | Mainboard | Memory | SPD | Graphics | Bench | About

Processor

Name	AMD Ryzen 5 2600X		
Code Name	Pinnacle Ridge	Max TDP	95.0 W
Package	Socket AM4 (1331)		
Technology	12 nm	Core Voltage	1.376 V

Specification

AMD Ryzen 5 2600X Six-Core Processor

Family	F	Model	8	Stepping	2
Ext. Family	17	Ext. Model	8	Revision	PIR-B2

Instructions: MMX(+), SSE, SSE2, SSE3, SSSE3, SSE4.1, SSE4.2, SSE4A, x86-64, AMD-V, AES, AVX, AVX2, FMA3, SHA

Clocks (Core #0)

Core Speed	3991.61 MHz
Multiplier	x 40.0
Bus Speed	99.79 MHz
Rated FSB	

Cache

L1 Data	6 x 32 KBytes	8-way
L1 Inst.	6 x 64 KBytes	4-way
Level 2	6 x 512 KBytes	8-way
Level 3	2 x 8 MBytes	16-way

Selection: Socket #1 Cores: 6 Threads: 12

CPU-Z Ver. 1.95.0.x64 Tools Validate Close

GPU-Z

Ez is egy rendszerdiagnosztika program mely a videokártyáról, grafikus processzorról mutat adatokat.

