

Operációs rendszerek Bsc

02.26

Készítette:

Butella Bence Kristóf

NK:IVLJQO

Miskolc 2021

1. Tölts le a *Sysinternals Suite* csomagot, majd csomagolja ki. A Windows belső működését lehet tanulmányozni, vagy a hibakeresésben segít.

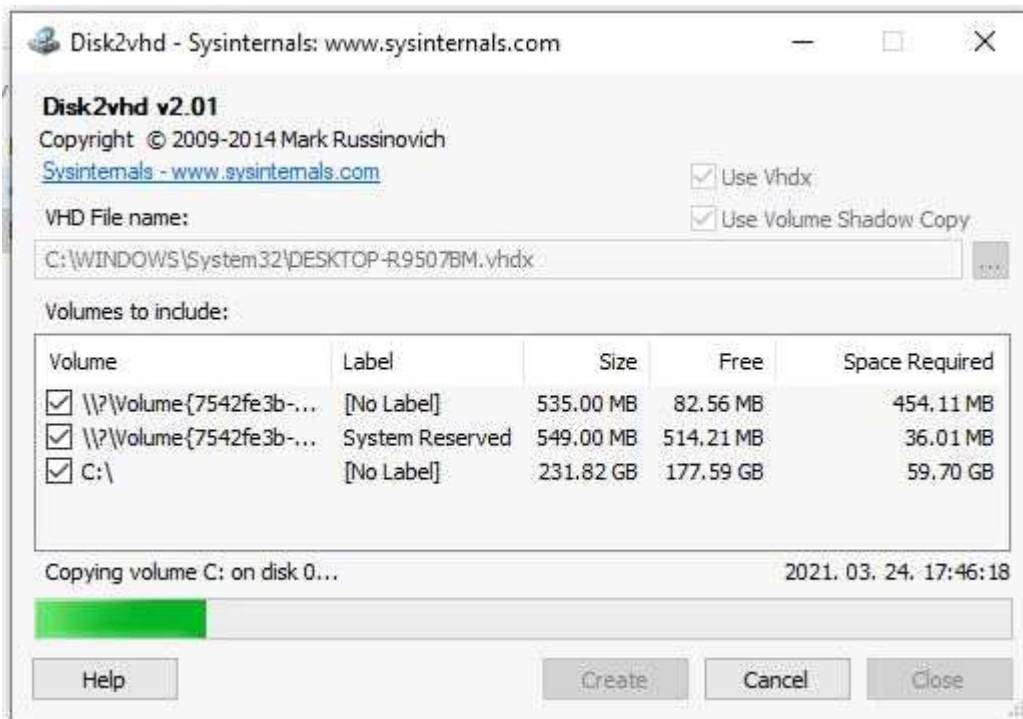
<https://docs.microsoft.com/hu-hu/sysinternals/downloads/sysinternals-suite>

2. A Sysinternals weboldalán kategóriákba sorolva hasznos programok érhetők el:

- a) File and Disk Utilities (Disk2vhd)
- b) Networking Utilities (TCPView)
- c) Process Utilities (Process Explorer, Process Monitor, AutoRuns)
- d) Security Utilities (LogonSession)
- e) Information Utilities (RAMMap)

A felsorolt eszközök közül minden eszköz esetén tölts le, futtassa - és írja le a program szolgáltatásait és a futtatás eredményét egy-egy mondattal - majd mentse el a megadott dokumentumba (képernyőkép).

Megj: a zárójelben lévő eszközön felül válasszon még egy eszközt is.



A Disk2vhd egy nagyszerű kis program, mely segítségével könnyedén készíthetünk merevlemezeinken tárolt fájlokról biztonsági mentést virtuális meghajtóként, tehát amelyet VHD-ként ment. Ezeket virtualbox-hoz és egyéb virtualizációs szoftverhez kapcsolhatunk.

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	996	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2021.02.17.9:54:57	RpcSs
System	4	TCP	Listen	172.19.48.1	139	0.0.0.0	0	2021.03.24.16:23:04	System
System	4	TCP	Listen	192.168.0.109	139	0.0.0.0	0	2021.03.24.14:09:06	System
EEEventManager.exe	1468	TCP	Listen	0.0.0.0	2968	0.0.0.0	0	2021.03.24.14:14:45	EEEventManager.exe
svchost.exe	1216	TCP	Listen	0.0.0.0	3389	0.0.0.0	0	2021.02.17.9:54:58	TermService
svchost.exe	6136	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2021.03.24.16:23:02	CDPSvc
lsass.exe	784	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2021.02.17.9:54:57	lsass.exe
wininit.exe	680	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2021.02.17.9:54:57	wininit.exe
svchost.exe	1604	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2021.02.17.9:54:58	EventLog
svchost.exe	1360	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2021.02.17.9:54:58	Schedule
svchost.exe	2652	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	2021.02.17.9:54:58	SessionEnv
spoolsv.exe	3732	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	2021.02.17.9:54:59	Spooler
services.exe	752	TCP	Listen	0.0.0.0	49675	0.0.0.0	0	2021.02.17.9:55:45	services.exe
OneDrive.exe	12768	TCP	Established	192.168.0.109	55510	51.103.5.159	443	2021.03.24.16:24:02	OneDrive.exe
SearchApp.exe	14836	TCP	Close Wait	192.168.0.109	55929	152.199.19.161	443	2021.03.24.16:47:06	SearchApp.exe
SearchApp.exe	14836	TCP	Close Wait	192.168.0.109	55935	152.199.19.161	443	2021.03.24.16:47:23	SearchApp.exe
svchost.exe	900	TCP	Established	192.168.0.109	55951	52.142.114.176	443	2021.03.24.17:05:19	BITS
svchost.exe	900	TCP	Established	192.168.0.109	55952	184.30.21.38	443	2021.03.24.17:05:19	BITS
svchost.exe	4056	TCP	Established	192.168.0.109	59464	51.103.5.159	443	2021.03.24.16:23:04	WpnService
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	2021.02.17.9:55:00	System
svchost.exe	4656	TCP	Listen	0.0.0.0	7680	0.0.0.0	0	2021.03.23.18:38:19	DoSvc
svchost.exe	996	TCPv6	Listen	::	135	::	0	2021.02.17.9:54:57	RpcSs
System	4	TCPv6	Listen	::	445	::	0	2021.02.17.9:55:00	System
svchost.exe	1216	TCPv6	Listen	::	3389	::	0	2021.02.17.9:54:58	TermService

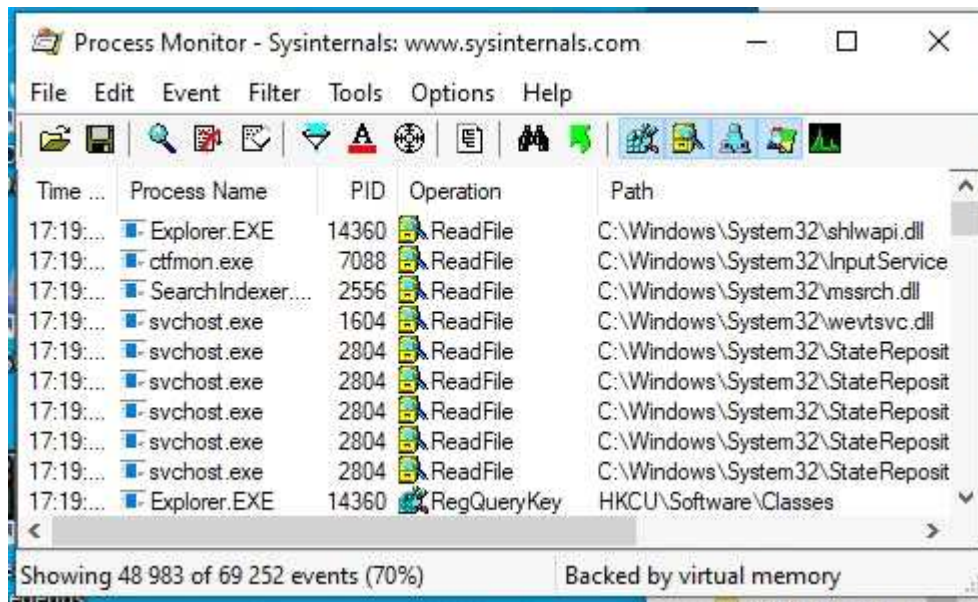
Endpoints: 65 Established: 4 Listening: 26 Time Wait: Close Wait: 2 Update: 2 sec

A Tcpview.exe nem egy Windows alapfájl. A fájl digitális aláírással rendelkezik. A Tcpview.exe képes figyelni az alkalmazásokat.

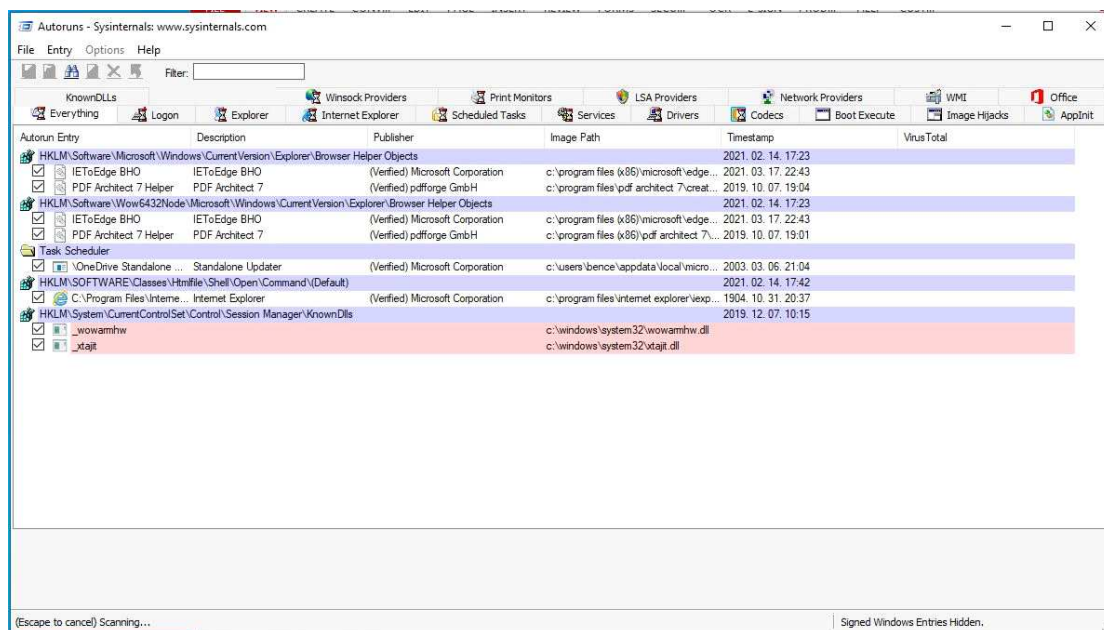
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System	Susp...	184 K	13 548 K	56		
Registry		6 660 K	55 296 K	104		
System Idle Process	81.56	60 K	8 K	0		
System	1.01	216 K	2 676 K	4		
Interrupts	1.72	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1 064 K	776 K	440		
Memory Compression	< 0.01	1 160 K	114 920 K	2388		
csrss.exe	< 0.01	1 880 K	3 736 K	584		
wininit.exe		1 804 K	3 652 K	680		
services.exe	0.06	6 588 K	6 776 K	752		
svchost.exe	0.06	28 672 K	43 204 K	908	Windows-szolgáltatások gaz...	Microsoft Corporation
MoUsocoreWorker.exe		95 496 K	36 836 K	8592		
StartMenuExperienceHost.exe		28 252 K	40 752 K	14572		
TextInputHost.exe	0.17	16 088 K	18 084 K	15596		Microsoft Corporation
RuntimeBroker.exe		3 756 K	15 428 K	13680	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe	0.01	10 620 K	33 640 K	3624	Runtime Broker	Microsoft Corporation
YourPhone.exe	< 0.01	30 956 K	40 060 K	2552	YourPhone	Microsoft Corporation
SearchApp.exe	Susp...	155 764 K	69 244 K	14836	Search application	Microsoft Corporation
Cortana.exe	Susp...	31 364 K	23 408 K	1964	Cortana	Microsoft Corporation
Video UI.exe	Susp...	22 916 K	23 276 K	14584		
RuntimeBroker.exe		4 324 K	21 824 K	9120	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	Susp...	32 428 K	18 084 K	6204	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe	0.01	4 980 K	24 528 K	13324	Runtime Broker	Microsoft Corporation
SystemSettingsBroker.exe	0.01	6 276 K	16 468 K	4464	System Settings Broker	Microsoft Corporation
RuntimeBroker.exe		1 464 K	7 116 K	11444	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		3 720 K	16 640 K	16980	Runtime Broker	Microsoft Corporation
Microsoft.Photos.exe	Susp...	51 676 K	32 896 K	8820		
RuntimeBroker.exe		9 856 K	27 280 K	17152	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		4 960 K	18 212 K	16280	Runtime Broker	Microsoft Corporation

CPU Usage: 18.44% Commit Charge: 46.86% Processes: 165 Physical Usage: 66.22%

Amikor először elindítottam a Process Explorer programot, sok vizuális adat jelent meg azonnal - a számítógépen futó folyamatokról hierarchikus fa nézet jelenik meg, beleértve a CPU és a RAM használatát az egyes folyamatok számértékeivel.



Az eszköz valós időben figyeli és megjeleníti az összes fájlrendszeri tevékenységet egy Microsoft Windows vagy Unix-szerű operációs rendszeren.



Az Autoruns képes figyelni az alkalmazásokat és csatlakozni az internethez.

```

Administrator: Command Prompt

LogonSessions v1.3
Copyright (C) 2004-2015 Mark Russinovich
Sysinternals - www.sysinternals.com

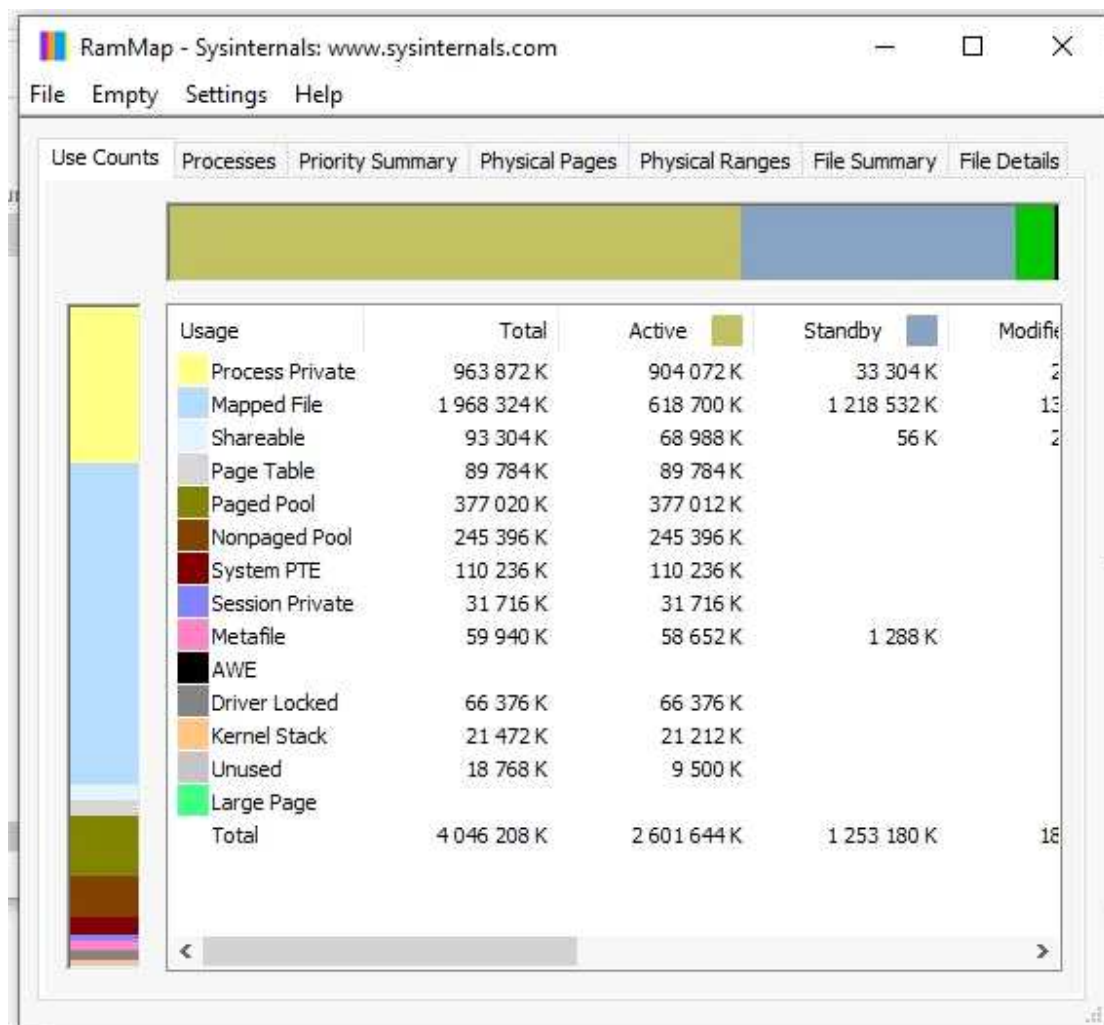
[0] Logon session 00000000:000003e7:
User name: WORKGROUP\SOFTPEDIA\PC$
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: S-1-5-18
Logon time: 1/31/2016 8:04:16 AM
Logon server:
DNS Domain:
UPN:

[1] Logon session 00000000:00000b92:
User name:
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: (none)
Logon time: 1/31/2016 8:04:16 AM
Logon server:
DNS Domain:
UPN:

[2] Logon session 00000000:000003e4:
User name: WORKGROUP\SOFTPEDIA\PC$

```

A logonsession olyan számítási munkamenet, amely akkor kezdődik, amikor a felhasználó hitelesítése sikeres, és akkor ér véget, amikor a felhasználó kijelentkezik a rendszerből.

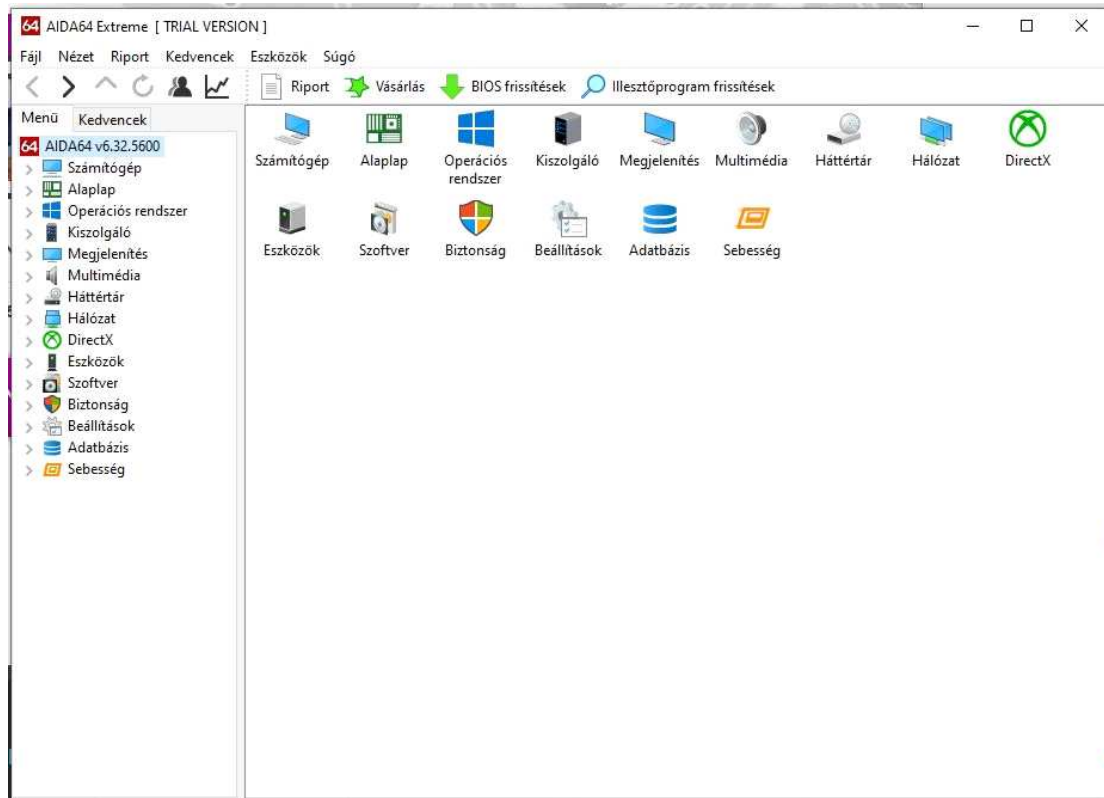


A RAMMap egy fejlett fizikai memóriahasználati elemző segédprogram.

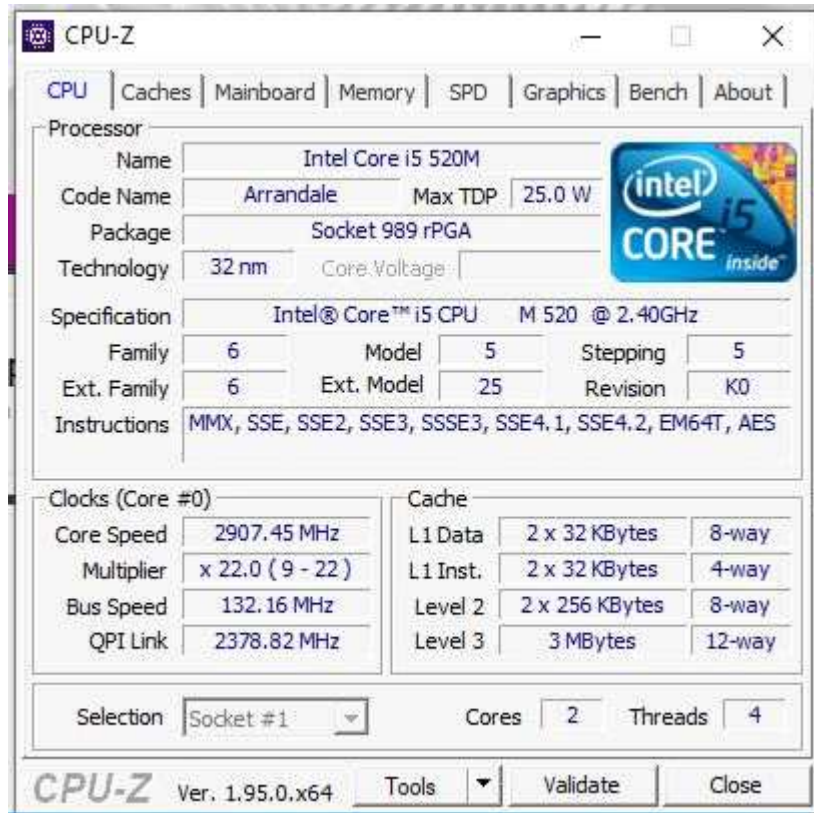
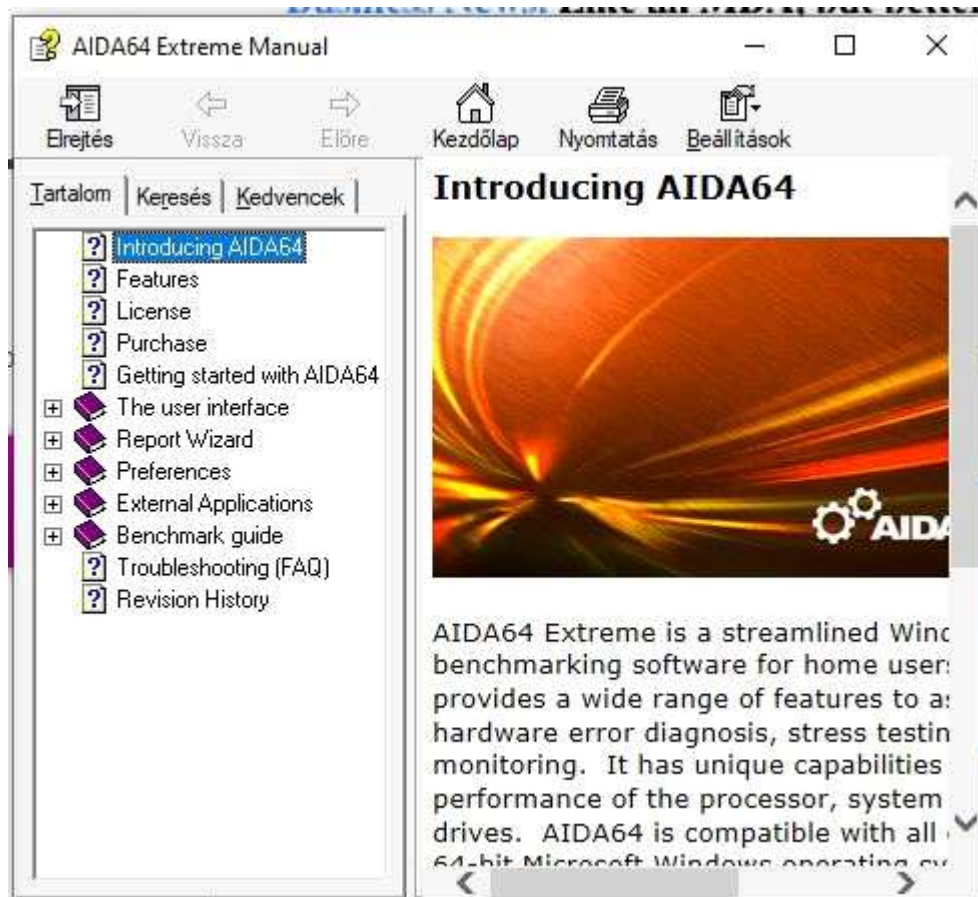
3. Töltse le és végezzen vizsgálatot az *AIDA64_Engineer_v5.98.4800_Portable*, *CPU-Z*, *GPU-Z* programokkal.

A felsorolt segédprogramoknak írja le a szolgáltatásait és a futtatás eredményét egy-egy mondattal - majd mentse el az alábbi dokumentumba (képernyőkép is).

Mentés: *neptunkod_segedprog.pdf*



Az AIDA64 Extreme egy otthoni, míg az AIDA64 Engineer egy üzleti Windows-felhasználóknak szánt rendszerinformációs, -diagnosztikai és sebességmérő alkalmazás.



CPU-Z programban magáról a cpurol kapunt részletes leírást működéséről teljesítményéről.