

Disk2vhd v2.01

Copyright © 2009-2014 Mark Russinovich

[Sysinternals - www.sysinternals.com](http://www.sysinternals.com)☒ Use Vhdx☒ Use Volume Shadow Copy

VHD File name:

C:\Users\simon\Desktop\SysinternalsSuite\DESKTOP-IHQ09DL.vhdx

Volumes to include:

| Volume | Label | Size | Free | Space Required |
|---|------------|-----------|-----------|----------------|
| <input checked="" type="checkbox"/> \\?\Volume{66f4976a-... | [No Label] | 1.18 GB | 676.37 MB | 530.13 MB |
| <input checked="" type="checkbox"/> \\?\Volume{ed726225-... | Image | 11.12 GB | 141.98 MB | 10.97 GB |
| <input checked="" type="checkbox"/> \\?\Volume{f2b64ba9-... | WINRETOOLS | 498.00 MB | 96.92 MB | 400.10 MB |
| <input checked="" type="checkbox"/> C:\ | [No Label] | 225.07 GB | 97.07 GB | 112.49 GB |

Help

Create

Cancel

Close

2.a)

Disk2vhd

Copyright © 2009-2013 Mark Russinovich

Sysinternals - www.sysinternals.com

Disk2vhd is a utility that creates VHD (Virtual Hard Disk) or VHDX (usable on Windows 8 and higher and Windows Server 2012 and higher) versions of physical disks for use in Microsoft Virtual PC or Microsoft Hyper-V virtual machines (VMs). The difference between Disk2vhd and other physical-to-virtual tools is that you can run Disk2vhd on a system that's online. Disk2vhd uses Windows' Volume Snapshot capability, introduced in Windows XP, to create consistent point-in-time snapshots of the volumes you want to include in a conversion. You can even have Disk2vhd create the VHDs on local volumes, even ones being converted (though performance is better when the VHD is on a disk different than ones being converted).

Disk2vhd runs Windows XP SP2, Windows Server 2003 SP1, and higher, including x64 systems.

A Program leírása szerint virtuális merevlemez képes létrehozni a kívánt számítógépen, mely online formában is használható. Hely szűkében a merevlemezen nem hoztam létre virtuális merevlemez.

File Edit Options Help

| # | Time | Duration (s) | Disk | Request | Sector | Length |
|-----|-----------|--------------|------|---------|-----------|--------|
| 275 | 20.782663 | 0.00000000 | 0 | Write | 17948904 | 8 |
| 276 | 20.989523 | 0.00000000 | 0 | Write | 148111920 | 16 |
| 277 | 21.017199 | 0.00000000 | 0 | Write | 165934080 | 256 |
| 278 | 21.018833 | 0.00000000 | 0 | Write | 165934336 | 256 |
| 279 | 21.983375 | 0.00000000 | 0 | Write | 7434304 | 16 |
| 280 | 21.983759 | 0.00000000 | 0 | Write | 238159496 | 120 |
| 281 | 21.984007 | 0.00000000 | 0 | Write | 7434184 | 8 |
| 282 | 21.989522 | 0.00000000 | 0 | Write | 7434184 | 8 |
| 283 | 21.990737 | 0.00000000 | 0 | Read | 98994496 | 8 |
| 284 | 22.145971 | 0.00000000 | 0 | Write | 17948904 | 8 |
| 285 | 22.146273 | 0.00000000 | 0 | Write | 98855688 | 8 |

2.b)

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

| 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-ihq09dl | 54415 | prg03s06-in-f31e1... | https | TIME_WAIT | | | | |
| System Proc... | 0 | TCP | desktop-ihq09dl | 54424 | 35.186.224.25 | https | TIME_WAIT | 3 | 458 | 4 | 4,942 |
| System Proc... | 0 | TCP | desktop-ihq09dl | 54425 | 104.123.111.225 | http | TIME_WAIT | 1 | 213 | 2 | 4,563 |
| System Proc... | 0 | TCP | desktop-ihq09dl | 54416 | prg03s06-in-f14.1e... | https | TIME_WAIT | 11 | 13,106 | 8 | 1,529 |
| atmgr.exe | 15604 | TCP | DESKTOP-IHQ09... | 64232 | localhost | 64233 | ESTABLISHED | | | | |
| atmgr.exe | 15604 | TCP | DESKTOP-IHQ09... | 64233 | localhost | 64232 | ESTABLISHED | | | | |
| atmgr.exe | 15604 | TCP | DESKTOP-IHQ09... | 64234 | localhost | 64235 | ESTABLISHED | | | | |
| atmgr.exe | 15604 | TCP | DESKTOP-IHQ09... | 64235 | localhost | 64234 | ESTABLISHED | | | | |
| atmgr.exe | 15604 | TCP | DESKTOP-IHQ09... | 64236 | localhost | 64237 | ESTABLISHED | | | | |
| atmgr.exe | 15604 | TCP | DESKTOP-IHQ09... | 64237 | localhost | 64236 | ESTABLISHED | | | | |
| atmgr.exe | 15604 | TCP | DESKTOP-IHQ09... | 64238 | localhost | 64239 | ESTABLISHED | | | | |
| atmgr.exe | 15604 | TCP | DESKTOP-IHQ09... | 64239 | localhost | 64238 | ESTABLISHED | | | | |
| chrome.exe | 10316 | TCP | desktop-ihq09dl | 51996 | 142.250.27.188 | 5228 | ESTABLISHED | 1 | 26 | 1 | 24 |
| chrome.exe | 10316 | TCP | desktop-ihq09dl | 52009 | edge-star-shv-01-v... | https | ESTABLISHED | 106 | 4,924 | 109 | 3,319 |
| chrome.exe | 3752 | UDP | DESKTOP-IHQ09... | 5353 | * | * | | | | 16 | 448 |
| chrome.exe | 10316 | UDP | DESKTOP-IHQ09... | 5353 | * | * | | | | 16 | 448 |
| chrome.exe | 3752 | UDP | DESKTOP-IHQ09... | 5353 | * | * | | | | | |
| chrome.exe | 10316 | UDP | DESKTOP-IHQ09... | 5353 | * | * | | | | | |
| chrome.exe | 3752 | UDP | DESKTOP-IHQ09... | 5353 | * | * | | | | | |
| chrome.exe | 3752 | UDP | DESKTOP-IHQ09... | 5353 | * | * | | | | | |
| chrome.exe | 10316 | UDP | DESKTOP-IHQ09... | 5353 | * | * | | | | | |
| chrome.exe | 10316 | UDP | DESKTOP-IHQ09... | 5353 | * | * | | | | | |
| chrome.exe | 3752 | UDPv6 | [0:0:0:0:0:0:0:0] | 5353 | * | * | | | | | |
| chrome.exe | 3752 | UDPv6 | [0:0:0:0:0:0:0:0] | 5353 | * | * | | | | | |
| chrome.exe | 10316 | UDPv6 | [0:0:0:0:0:0:0:0] | 5353 | * | * | | | | | |
| chrome.exe | 10316 | UDPv6 | [0:0:0:0:0:0:0:0] | 5353 | * | * | | | | | |
| chrome.exe | 10316 | TCP | desktop-ihq09dl | 54428 | prg03s06-in-f31e1... | https | ESTABLISHED | 6 | 1,351 | 7 | 1,353 |
| dashHost.exe | 4752 | UDP | DESKTOP-IHQ09... | ws-discovery | * | * | | | | | |
| dashHost.exe | 4752 | UDP | DESKTOP-IHQ09... | ws-discovery | * | * | | | | | |
| dashHost.exe | 4752 | UDP | DESKTOP-IHQ09... | 61952 | * | * | | | | | |
| dashHost.exe | 4752 | UDPv6 | [0:0:0:0:0:0:0:0] | 3702 | * | * | | | | | |
| dashHost.exe | 4752 | UDPv6 | [0:0:0:0:0:0:0:0] | 3702 | * | * | | | | | |
| dashHost.exe | 4752 | UDPv6 | [0:0:0:0:0:0:0:0] | 61953 | * | * | | | | | |
| DiscSoftBus... | 10992 | TCP | DESKTOP-IHQ09... | 45769 | DESKTOP-IHQ09... | 0 | LISTENING | | | | |
| DiscSoftBus... | 10992 | UDP | DESKTOP-IHQ09... | 45769 | * | * | | | | | |
| fhj_service.exe | 4688 | TCPv6 | [0:0:0:0:0:0:0:1] | 49669 | [0:0:0:0:0:0:0:0] | 0 | LISTENING | | | | |
| lsass.exe | 872 | TCP | DESKTOP-IHQ09... | 49664 | DESKTOP-IHQ09... | 0 | LISTENING | | | | |
| lsass.exe | 872 | TCPv6 | [0:0:0:0:0:0:0:0] | 49664 | [0:0:0:0:0:0:0:0] | 0 | LISTENING | | | | |
| invcontainer.exe | 7780 | UDP | DESKTOP-IHQ09... | 62103 | * | * | | | | | |
| NVIDIA Web... | 9928 | TCP | DESKTOP-IHQ09... | 49768 | DESKTOP-IHQ09... | 0 | LISTENING | | | | |
| NVIDIA Web... | 9928 | UDP | DESKTOP-IHQ09... | 10010 | * | * | | | | | |
| services.exe | 864 | TCP | DESKTOP-IHQ09... | 49670 | DESKTOP-IHQ09... | 0 | LISTENING | | | | |
| services.exe | 864 | TCPv6 | [0:0:0:0:0:0:0:0] | 49670 | [0:0:0:0:0:0:0:0] | 0 | LISTENING | | | | |
| Skype.exe | 17244 | TCP | desktop-ihq09dl | 52424 | 40.74.219.49 | https | ESTABLISHED | 7 | 19,138 | 7 | 3,621 |
| Skype.exe | 17244 | TCP | desktop-ihq09dl | 54101 | 40.74.219.49 | https | ESTABLISHED | 12 | 19,864 | 7 | 2,889 |
| Skype.exe | 14072 | TCP | desktop-ihq09dl | 54111 | 52.114.104.80 | https | ESTABLISHED | 23 | 13,455 | 23 | 13,386 |
| Skype.exe | 14072 | TCP | desktop-ihq09dl | 54144 | 13.69.158.96 | https | ESTABLISHED | 16 | 4,924 | 16 | 50,796 |
| Skype.exe | 17244 | TCP | desktop-ihq09dl | 54423 | 68.232.34.200 | https | ESTABLISHED | 6 | 1,847 | 11 | 8,545 |
| Skype.exe | 14072 | UDP | desktop-ihq09dl | 9410 | * | * | | 2,370 | 395,034 | 21,714 | 4,232,895 |
| Skype.exe | 14072 | UDP | desktop-ihq09dl | 18198 | * | * | | | | | |
| Skype.exe | 14072 | UDP | desktop-ihq09dl | 58203 | * | * | | | | | |
| Skype.exe | 14072 | UDP | desktop-ihq09dl | 53021 | * | * | | | | | |
| Skype.exe | 14072 | UDP | DESKTOP-IHQ09... | 65258 | * | * | | 14 | 5,464 | 40 | 4,236 |
| Skype.exe | 14072 | UDPv6 | [0:0:0:0:0:0:0:0] | 65258 | * | * | | | | | |
| spoolsv.exe | 3332 | TCP | DESKTOP-IHQ09... | 49668 | DESKTOP-IHQ09... | 0 | LISTENING | | | | |
| spoolsv.exe | 3332 | TCPv6 | [0:0:0:0:0:0:0:0] | 49668 | [0:0:0:0:0:0:0:0] | 0 | LISTENING | | | | |
| svchost.exe | 904 | TCP | DESKTOP-IHQ09... | epmap | DESKTOP-IHQ09... | 0 | LISTENING | | | | |
| svchost.exe | 9332 | TCP | DESKTOP-IHQ09... | 5040 | DESKTOP-IHQ09... | 0 | LISTENING | | | | |
| svchost.exe | 1600 | TCP | DESKTOP-IHQ09... | 49666 | DESKTOP-IHQ09... | 0 | LISTENING | | | | |
| svchost.exe | 788 | TCP | DESKTOP-IHQ09... | 49667 | DESKTOP-IHQ09... | 0 | LISTENING | | | | |
| svchost.exe | 4564 | TCP | desktop-ihq09dl | 51958 | 51.103.5.159 | https | ESTABLISHED | | | | |
| svchost.exe | 5656 | TCP | DESKTOP-IHQ09... | 57627 | DESKTOP-IHQ09... | 0 | LISTENING | | | | |
| svchost.exe | 14000 | TCP | DESKTOP-IHQ09... | ms-do | DESKTOP-IHQ09... | 0 | LISTENING | | | | |
| svchost.exe | 4160 | UDP | DESKTOP-IHQ09... | isakmp | * | * | | | | | |
| svchost.exe | 5492 | UDP | DESKTOP-IHQ09... | ssdp | * | * | | | | 148 | 62,722 |
| svchost.exe | 5492 | UDP | desktop-ihq09dl | ssdp | * | * | | | | | |

Endpoints: 120 Established: 17 Listening: 31 Time Wait: 4 Close Wait: 1

TCPView

Copyright 1997-2010 Mark Russinovich and Bryce Cogswell

Sysinternals - www.sysinternals.com


Introduction

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the owning process name, remote address and state of TCP connections. TCPView provides a conveniently presented subset of the Netstat program that ships with Windows NT/2000/XP.

TCPView requires Windows XP or higher.

A program értelmezésem szerint részletes leírást ad az eszközünkön futó azon programokról melyek használják internetkapcsolatunkat jelen pillanatban vagy arra várnak hogy sorra kerüljenek esetleg válaszra várákoznak.

2.c)

 Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-IHQ09DL\simon]

File Options View Process Find Users Help

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name |
|-------------------------|---------|---------------|-------------|-------|---------------------------------|-----------------------|
| Registry | | 9,392 K | 67,040 K | 100 | | |
| System Idle Process | 76.38 | 60 K | 8 K | 0 | | |
| System | 0.47 | 208 K | 3,064 K | 4 | | |
| Interrupts | 0.81 | 0 K | 0 K | n/a | Hardware Interrupts and DPCs | |
| smss.exe | | 1,080 K | 1,076 K | 484 | | |
| Memory Compression | < 0.01 | 2,536 K | 279,248 K | 2260 | | |
| csrss.exe | | 1,992 K | 5,472 K | 692 | | |
| wininit.exe | | 1,400 K | 5,972 K | 792 | | |
| services.exe | 1.71 | 7,788 K | 9,836 K | 864 | | |
| svchost.exe | < 0.01 | 30,408 K | 35,616 K | 1000 | Host Process for Windows S... | Microsoft Corporation |
| dllhost.exe | | 3,424 K | 10,588 K | 6916 | | |
| StartMenuExperience... | | 42,428 K | 60,684 K | 10428 | | |
| RuntimeBroker.exe | | 11,640 K | 19,288 K | 10684 | Runtime Broker | Microsoft Corporation |
| SearchApp.exe | Susp... | 150,996 K | 42,764 K | 11048 | Search application | Microsoft Corporation |
| RuntimeBroker.exe | | 24,712 K | 28,080 K | 11196 | Runtime Broker | Microsoft Corporation |
| dllhost.exe | | 5,468 K | 14,212 K | 11388 | COM Surrogate | Microsoft Corporation |
| SettingSyncHost.exe | | 15,652 K | 6,100 K | 12320 | Host Process for Setting Syn... | Microsoft Corporation |
| LockApp.exe | Susp... | 17,600 K | 7,412 K | 12372 | LockApp.exe | Microsoft Corporation |
| RuntimeBroker.exe | | 10,948 K | 8,708 K | 12548 | Runtime Broker | Microsoft Corporation |
| RuntimeBroker.exe | | 7,372 K | 22,500 K | 11844 | Runtime Broker | Microsoft Corporation |
| ShellExperienceHost.... | Susp... | 60,576 K | 39,620 K | 13680 | Windows Shell Experience H... | Microsoft Corporation |
| RuntimeBroker.exe | | 9,680 K | 16,172 K | 14224 | Runtime Broker | Microsoft Corporation |
| TextInputHost.exe | < 0.01 | 25,024 K | 66,740 K | 12044 | | Microsoft Corporation |
| ApplicationFrameHost... | | 36,552 K | 14,636 K | 14692 | Application Frame Host | Microsoft Corporation |
| UserOOBEBroker.exe | | 2,152 K | 9,060 K | 14608 | User OOBE Broker | Microsoft Corporation |
| CompPkgSrv.exe | | 2,316 K | 9,016 K | 14628 | Component Package Suppor... | Microsoft Corporation |
| WinStore.App.exe | Susp... | 50,592 K | 2,512 K | 8656 | Store | Microsoft Corporation |
| RuntimeBroker.exe | < 0.01 | 7,604 K | 10,116 K | 1192 | Runtime Broker | Microsoft Corporation |
| Time.exe | Susp... | 21,060 K | 2,072 K | 10640 | Time | |
| RuntimeBroker.exe | | 2,980 K | 8,680 K | 4832 | Runtime Broker | Microsoft Corporation |
| SystemSettingsBroker... | | 23,156 K | 12,372 K | 11068 | System Settings Broker | Microsoft Corporation |
| Video.UI.exe | Susp... | 20,768 K | 10,732 K | 16888 | | |
| RuntimeBroker.exe | | 1,580 K | 2,684 K | 18356 | Runtime Broker | Microsoft Corporation |
| Maps.exe | Susp... | 96,532 K | 2,148 K | 16792 | Maps | |
| RuntimeBroker.exe | | 3,060 K | 13,664 K | 12524 | Runtime Broker | Microsoft Corporation |
| RuntimeBroker.exe | | 4,744 K | 16,956 K | 15100 | Runtime Broker | Microsoft Corporation |
| dllhost.exe | | 7,836 K | 18,332 K | 16100 | COM Surrogate | Microsoft Corporation |
| MoUsCoreWorker.exe | | 181,240 K | 9,236 K | 14688 | | |
| Microsoft.Photos.exe | Susp... | 54,760 K | 1,120 K | 13228 | | |
| RuntimeBroker.exe | | 13,200 K | 19,940 K | 18096 | Runtime Broker | Microsoft Corporation |
| YourPhone.exe | Susp... | 28,708 K | 1,696 K | 10764 | YourPhone | Microsoft Corporation |
| RuntimeBroker.exe | | 7,020 K | 18,020 K | 12900 | Runtime Broker | Microsoft Corporation |
| SpeechRuntime.exe | | 26,724 K | 8,080 K | 17972 | Speech Runtime Executable | Microsoft Corporation |
| SystemSettings.exe | Susp... | 28,628 K | 1,700 K | 15680 | Settings | Microsoft Corporation |
| GameBar.exe | Susp... | 17,636 K | 1,860 K | 19444 | Xbox Game Bar | Microsoft Corporation |
| GameBarFTServer.exe | | 2,844 K | 12,932 K | 14100 | Xbox Game Bar Full Trust C... | Microsoft Corporation |
| RuntimeBroker.exe | | 2,712 K | 11,720 K | 19028 | Runtime Broker | Microsoft Corporation |
| RuntimeBroker.exe | | 2,132 K | 9,540 K | 19304 | Runtime Broker | Microsoft Corporation |
| VBxSVC.exe | < 0.01 | 8,144 K | 18,868 K | 12620 | VirtualBox Interface | Oracle Corporation |
| WmiPrvSE.exe | | 2,256 K | 9,916 K | 20276 | | |
| smartscreen.exe | | 7,924 K | 23,724 K | 13032 | Windows Defender SmartScr... | Microsoft Corporation |
| WUDFHost.exe | | 4,896 K | 10,360 K | 364 | | |
| svchost.exe | 0.01 | 25,104 K | 23,244 K | 904 | Host Process for Windows S... | Microsoft Corporation |
| WUDFHost.exe | < 0.01 | 14,168 K | 12,724 K | 1044 | | |
| svchost.exe | | 3,196 K | 7,584 K | 1120 | Host Process for Windows S... | Microsoft Corporation |
| svchost.exe | | 2,920 K | 9,532 K | 1412 | Host Process for Windows S... | Microsoft Corporation |
| svchost.exe | | 2,336 K | 11,584 K | 1420 | Host Process for Windows S... | Microsoft Corporation |
| svchost.exe | | 2,460 K | 8,988 K | 1508 | Host Process for Windows S... | Microsoft Corporation |

CPU Usage: 23.62% Commit Charge: 57.69% Processes: 258 Physical Usage: 63.48%

Process Explorer

Copyright © 1996-2012 Mark Russinovich
Sysinternals - www.sysinternals.com

Process Explorer is an advanced process management utility that picks up where Task Manager leaves off. It will show you detailed information about a process including its icon, command-line, full image path, memory statistics, user account, security attributes, and more. When you zoom in on a particular process you can list the DLLs it has loaded or the operating system resource handles it has open. A search capability enables you to track down a process that has a resource opened, such as a file, directory or Registry key, or to view the list of processes that have a DLL loaded.

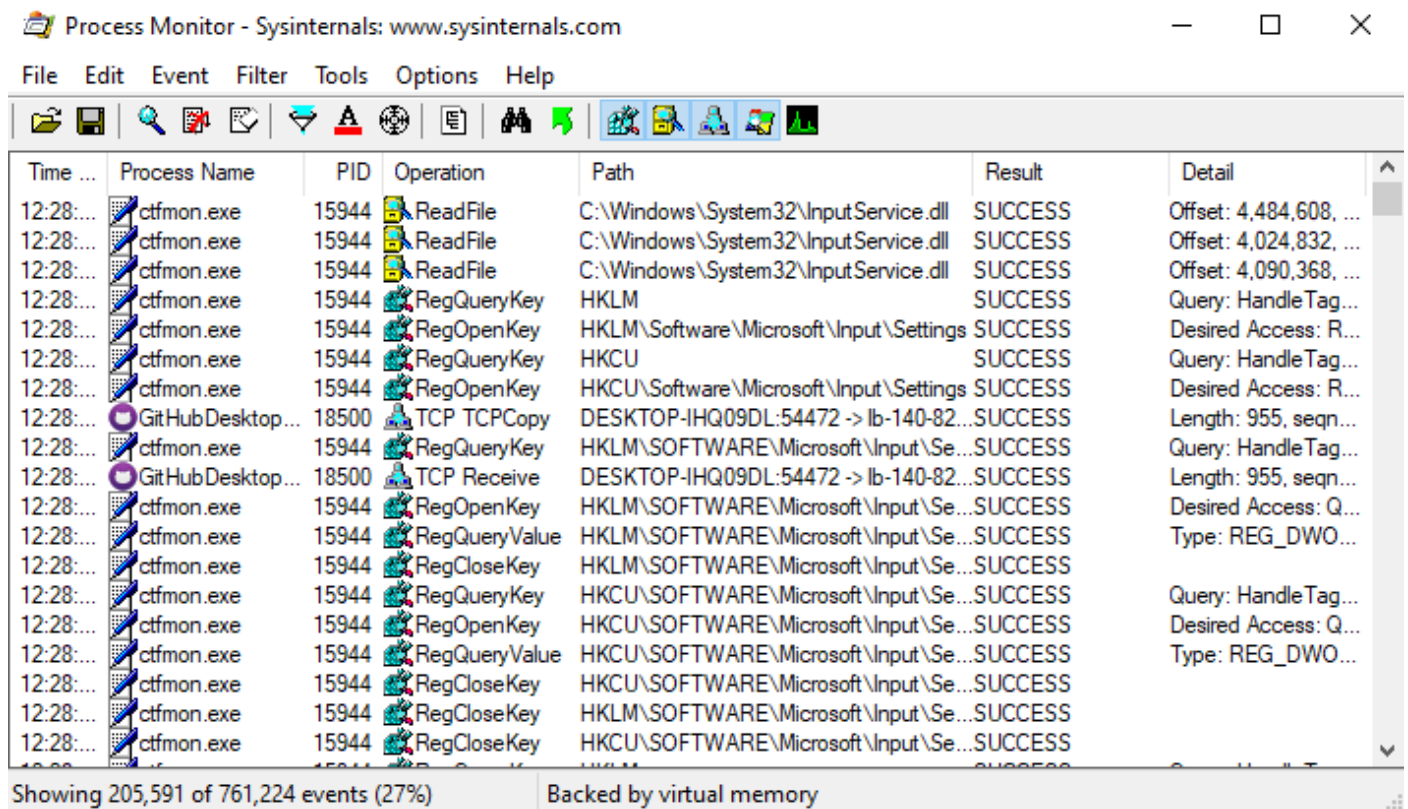
The Process Explorer display consists of two sub-windows. The top always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window, which you can close, depends on the mode that Process Explorer is in: if it is in handle mode you will see the handles that the process selected in the top window has opened; if Process Explorer is in DLL mode you will see the DLLs and memory-mapped files that the process has loaded.

Process Explorer also has a powerful search capability that will quickly show you which processes have particular handles opened or DLLs loaded. The unique capabilities of Process Explorer make it useful for tracking down DLL-version problems or handle leaks, and provide insight into the way Windows and applications work.

You can obtain equivalent command-line tools, Handle and ListDLLs, at the [Sysinternals](http://www.sysinternals.com) Web site.

Process Explorer does not require administrative privileges to run and works on clients running Windows XP and higher (Including IA64) and servers running Windows Server 2003 and higher (Including IA64).

A program saját leírása szerint a task manager továbbfejlesztett verziója, amely részletesebb leírást ad az operációs rendszerünkön futó process-ekről.



The screenshot shows the Process Monitor application window. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. The toolbar contains various icons for file operations, search, and system functions. The main display area is a table with the following columns: Time, Process Name, PID, Operation, Path, Result, and Detail. The table lists several events for the process ctfmon.exe, showing operations like ReadFile, RegQueryKey, RegOpenKey, and TCP operations. The status bar at the bottom indicates "Showing 205,591 of 761,224 events (27%)" and "Backed by virtual memory".

| Time | Process Name | PID | Operation | Path | Result | Detail |
|-----------|-------------------|-------|---------------|--|---------|------------------------|
| 12:28:... | ctfmon.exe | 15944 | ReadFile | C:\Windows\System32\InputService.dll | SUCCESS | Offset: 4,484,608, ... |
| 12:28:... | ctfmon.exe | 15944 | ReadFile | C:\Windows\System32\InputService.dll | SUCCESS | Offset: 4,024,832, ... |
| 12:28:... | ctfmon.exe | 15944 | ReadFile | C:\Windows\System32\InputService.dll | SUCCESS | Offset: 4,090,368, ... |
| 12:28:... | ctfmon.exe | 15944 | RegQueryKey | HKLM | SUCCESS | Query: HandleTag... |
| 12:28:... | ctfmon.exe | 15944 | RegOpenKey | HKLM\Software\Microsoft\Input\Settings | SUCCESS | Desired Access: R... |
| 12:28:... | ctfmon.exe | 15944 | RegQueryKey | HKCU | SUCCESS | Query: HandleTag... |
| 12:28:... | ctfmon.exe | 15944 | RegOpenKey | HKCU\Software\Microsoft\Input\Settings | SUCCESS | Desired Access: R... |
| 12:28:... | Git HubDesktop... | 18500 | TCP TCPCopy | DESKTOP-IHQ09DL:54472 -> lb-140-82... | SUCCESS | Length: 955, seqn... |
| 12:28:... | ctfmon.exe | 15944 | RegQueryKey | HKLM\SOFTWARE\Microsoft\Input\Se... | SUCCESS | Query: HandleTag... |
| 12:28:... | Git HubDesktop... | 18500 | TCP Receive | DESKTOP-IHQ09DL:54472 -> lb-140-82... | SUCCESS | Length: 955, seqn... |
| 12:28:... | ctfmon.exe | 15944 | RegOpenKey | HKLM\SOFTWARE\Microsoft\Input\Se... | SUCCESS | Desired Access: Q... |
| 12:28:... | ctfmon.exe | 15944 | RegQueryValue | HKLM\SOFTWARE\Microsoft\Input\Se... | SUCCESS | Type: REG_DWO... |
| 12:28:... | ctfmon.exe | 15944 | RegCloseKey | HKLM\SOFTWARE\Microsoft\Input\Se... | SUCCESS | |
| 12:28:... | ctfmon.exe | 15944 | RegQueryKey | HKCU\SOFTWARE\Microsoft\Input\Se... | SUCCESS | Query: HandleTag... |
| 12:28:... | ctfmon.exe | 15944 | RegOpenKey | HKCU\SOFTWARE\Microsoft\Input\Se... | SUCCESS | Desired Access: Q... |
| 12:28:... | ctfmon.exe | 15944 | RegQueryValue | HKCU\SOFTWARE\Microsoft\Input\Se... | SUCCESS | Type: REG_DWO... |
| 12:28:... | ctfmon.exe | 15944 | RegCloseKey | HKCU\SOFTWARE\Microsoft\Input\Se... | SUCCESS | |
| 12:28:... | ctfmon.exe | 15944 | RegCloseKey | HKLM\SOFTWARE\Microsoft\Input\Se... | SUCCESS | |
| 12:28:... | ctfmon.exe | 15944 | RegCloseKey | HKCU\SOFTWARE\Microsoft\Input\Se... | SUCCESS | |

Process Monitor

Copyright © 1996-2010 Mark Russinovich and Bryce Cogswell
Sysinternals - www.sysinternals.com

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

A program hasonló az előzőhöz abban, hogy process-eket vizsgál, viszont az előzővel ellentétben kevesebb szempontját figyeli azoknak.

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 | Virus Total |
|--|-------------------------------------|---|---|------------------|-------------|
| HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell | | | | 07/12/2019 10:15 | |
| <input checked="" type="checkbox"/> cmd.exe | Windows Command Processor | (Verified) Microsoft Windows | c:\windows\system32\cmd.exe | 26/01/2037 16:29 | |
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run | | | | 04/11/2020 10:20 | |
| <input checked="" type="checkbox"/> MouseDriver | | | File not found: TiltWheelMouse.exe | | |
| <input checked="" type="checkbox"/> RTHDVBg_PushButton | HD Audio Background Process | (Verified) Realtek Semiconductor Corp. | c:\program files\realtek\audio\hda\vt... | 09/10/2019 08:58 | |
| <input checked="" type="checkbox"/> RTHDVCPL | Realtek HD Audio Manager | (Verified) Realtek Semiconductor Corp. | c:\program files\realtek\audio\hda\vt... | 05/12/2019 09:21 | |
| <input checked="" type="checkbox"/> WavesSvc | Waves MaxxAudio Service Application | (Verified) Waves Inc | c:\program files\waves\maxxaudio\w... | 26/08/2019 05:33 | |
| HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run | | | | 03/11/2020 17:50 | |
| <input checked="" type="checkbox"/> LogMeIn Hamachi UI | Hamachi Client Application | (Verified) LogMeIn, Inc. | c:\program files (x86)\logmein\hamac... | 02/04/2019 15:58 | |
| <input checked="" type="checkbox"/> SunJavaUpdateSched | Java Update Scheduler | (Verified) Oracle America, Inc. | c:\program files (x86)\common files\j... | 17/09/2020 04:26 | |
| HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run | | | | 14/02/2021 11:08 | |
| <input checked="" type="checkbox"/> CiscoMeetingDaemon | Cisco Webex Meeting | (Verified) Cisco WebEx LLC | c:\users\simon\appdata\local\webe... | 05/02/2021 14:55 | |
| <input checked="" type="checkbox"/> com.squirrel.Teams.Teams | Microsoft Teams | (Verified) Microsoft 3rd Party Applicati... | c:\users\simon\appdata\local\microso... | 02/10/2020 13:48 | |
| <input checked="" type="checkbox"/> DAEMON Tools Lite Aut... | DAEMON Tools Lite | (Verified) Disc Soft Ltd | c:\program files\daemon tools lite\dta... | 15/12/2017 12:18 | |
| <input checked="" type="checkbox"/> Discord | Update | (Verified) Discord Inc. | c:\users\simon\appdata\local\discor... | 01/06/2020 21:58 | |
| <input checked="" type="checkbox"/> DriverFix | DriverFix | (Verified) Blueroad Technologies Limit... | c:\program files (x86)\driverfix\driverf... | 07/05/2020 15:39 | |
| <input checked="" type="checkbox"/> EvolveClient | EvolveClient | (Verified) Echobit, LLC | c:\program files\echobit\evolve\evol... | 10/11/2015 19:26 | |
| <input checked="" type="checkbox"/> OneDrive | Microsoft OneDrive | (Verified) Microsoft Corporation | c:\users\simon\appdata\local\microso... | 05/02/1958 12:59 | |
| <input checked="" type="checkbox"/> Overwolf | Overwolf Launcher | (Verified) Overwolf Ltd | c:\program files (x86)\overwolf\over... | 07/01/2021 13:30 | |
| <input checked="" type="checkbox"/> Wargaming.net Game C... | | | File not found: F:\EIIH\wot\Wargami... | | |
| <input checked="" type="checkbox"/> Windscribe | Windscribe client | (Verified) Windscribe Limited | c:\program files (x86)\windscribe\win... | 18/01/2019 23:29 | |
| HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce | | | | 08/02/2021 09:20 | |
| <input checked="" type="checkbox"/> Delete Cached Standalo... | | | File not found: del | | |
| <input checked="" type="checkbox"/> Delete Cached Update ... | | | File not found: del | | |
| <input checked="" type="checkbox"/> Uninstall 20.201.1005.0... | | | File not found: mdir | | |
| <input checked="" type="checkbox"/> Uninstall 20.201.1005.0... | | | File not found: mdir | | |
| C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup | | | | 20/10/2020 20:52 | |
| <input checked="" type="checkbox"/> SteelSeries Engine 3.Ink | SteelSeries Engine 3 Core | (Verified) SteelSeries ApS | c:\program files\steelseries\steelserie... | 23/04/2018 17:36 | |
| HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components | | | | 23/10/2020 18:10 | |
| <input checked="" type="checkbox"/> Google Chrome | Google Chrome Installer | (Verified) Google LLC | c:\program files (x86)\google\chrome... | 18/02/2021 22:08 | |
| <input checked="" type="checkbox"/> Microsoft Edge | Microsoft Edge Installer | (Verified) Microsoft Corporation | c:\program files (x86)\microsoft\edge... | 17/02/2021 04:41 | |
| <input checked="" type="checkbox"/> n/a | Microsoft .NET IE SECURITY REGIS... | (Verified) Microsoft Corporation | c:\windows\system32\mscores.dll | 25/10/2019 04:45 | |

Ready. Signed Windows Entries Hidden.

Autoruns

Copyright © 1996-2015 Mark Russinovich
Sysinternals - www.sysinternals.com

This utility, which has the most comprehensive knowledge of auto-starting locations of any startup monitor, shows you what programs are configured to run during system bootup or login, and what extension load into various Windows processes, including Explorer and Internet Explorer. It reports the image timestamp of executables, the last-modified timestamp of other file types, and the last-modified timestamp of the autostart locations. A "Hide Signed Microsoft Entries" option helps you to zoom in on third-party auto-starting images that have been added to your system.

Ez a program az előző kettővel ellentétben nem a jelenleg futó process-ekre koncentrál hanem a bekapcsolaskor operációs rendszer által először végrehajtott műveletekre.


Administrator: Command Prompt

Logon server:
DNS Domain:
UPN:

- [7] Logon session 00000000:0001ff1c:
User name: Window Manager\DWM-1
Auth package: Negotiate
Logon type: Interactive
Session: 1
Sid: S-1-5-90-0-1
Logon time: 20/01/2021 22:16:44
Logon server:
DNS Domain:
UPN:
- [8] Logon session 00000000:000f1276:
User name: DESKTOP-IHQ09DL\simon
Auth package: CloudAP
Logon type: Interactive
Session: 1
Sid: S-1-5-21-2522384817-1811695907-3332416438-1001
Logon time: 20/01/2021 22:17:05
Logon server:
DNS Domain:
UPN:
- [9] Logon session 00000000:000f13b9:
User name: DESKTOP-IHQ09DL\simon
Auth package: CloudAP
Logon type: Interactive
Session: 1
Sid: S-1-5-21-2522384817-1811695907-3332416438-1001
Logon time: 20/01/2021 22:17:05
Logon server:
DNS Domain:
UPN:
- [10] Logon session 00000000:010c117e:
User name: DESKTOP-IHQ09DL\defaultuser100000
Auth package: NTLM
Logon type: Interactive
Session: 2
Sid: S-1-5-21-2522384817-1811695907-3332416438-1002
Logon time: 21/01/2021 13:38:58
Logon server: DESKTOP-IHQ09DL
DNS Domain:
UPN:
- [11] Logon session 00000000:013743b2:
User name: DESKTOP-IHQ09DL\defaultuser100001
Auth package: NTLM
Logon type: Interactive
Session: 3
Sid: S-1-5-21-2522384817-1811695907-3332416438-1003
Logon time: 21/01/2021 13:44:07
Logon server: DESKTOP-IHQ09DL
DNS Domain:
UPN:

C:\Users\simon\Desktop\SysinternalsSuite>

LSA Logon Sessions

05/31/2018 • 2 minutes to read • 

A *logon session* is a computing session that begins when a user authentication is successful and ends when the user logs off of the system.

When a user is successfully authenticated, the authentication package creates a logon session and returns information to the *Local Security Authority* (LSA) that is used to create a *token* for the new user. This token includes, among other things, a *locally unique identifier* (LUID) for the logon session, called the *logon id*.

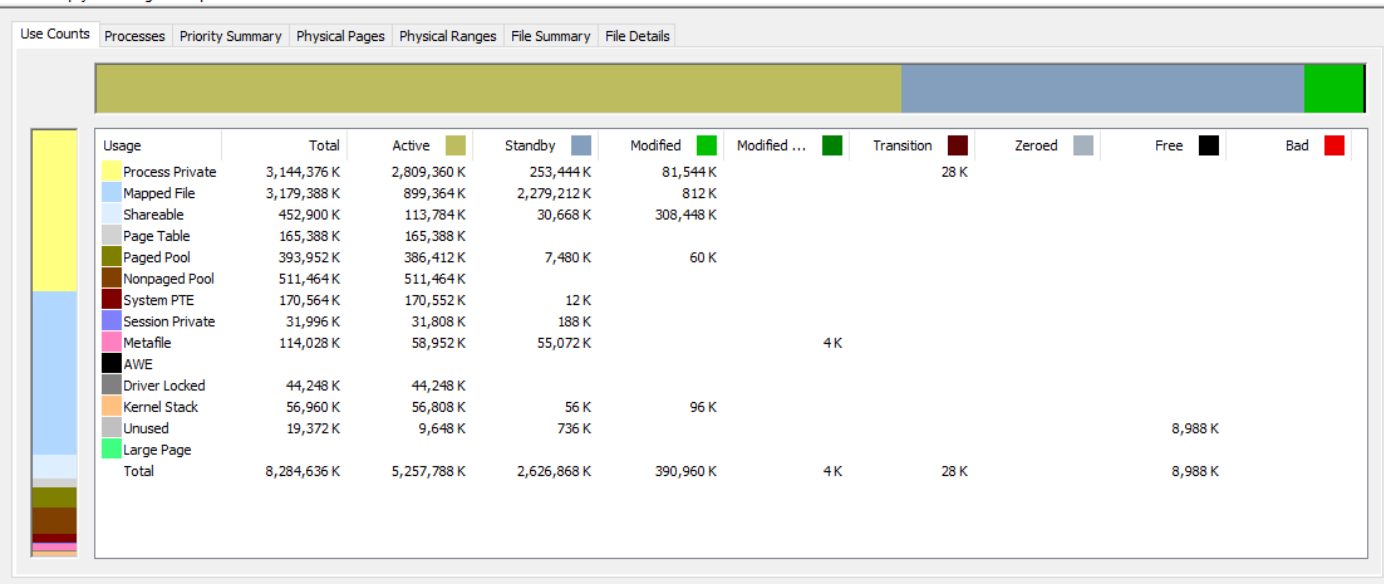
When a token is created, the *reference count* for the logon session is incremented. The reference count is also incremented whenever copies of the token are created for process creation, impersonation, or other uses. As token uses are completed and copies of the token are deleted, the reference count for the logon session is decremented. When the reference count reaches zero, the logon session is deleted.

Ez a program a felhasználói fiókok valamelyikébe sikeres bejelentkezésnél a fut le az eszközünkön.

2.e)

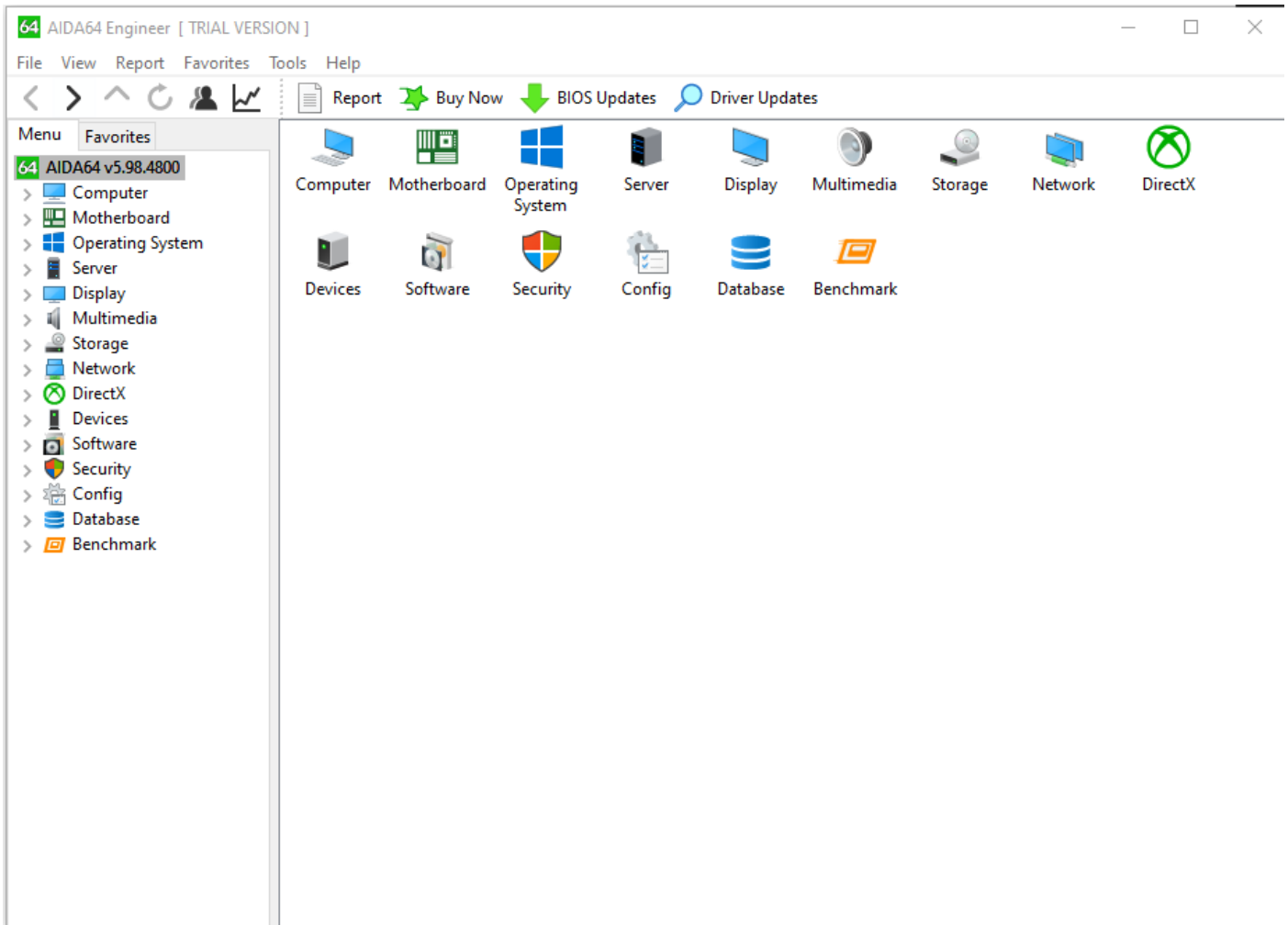
RamMap - Sysinternals: www.sysinternals.com

File Empty Settings Help



Ez a program a memóriahasználatot vizsgálja eszközünkön.

3.



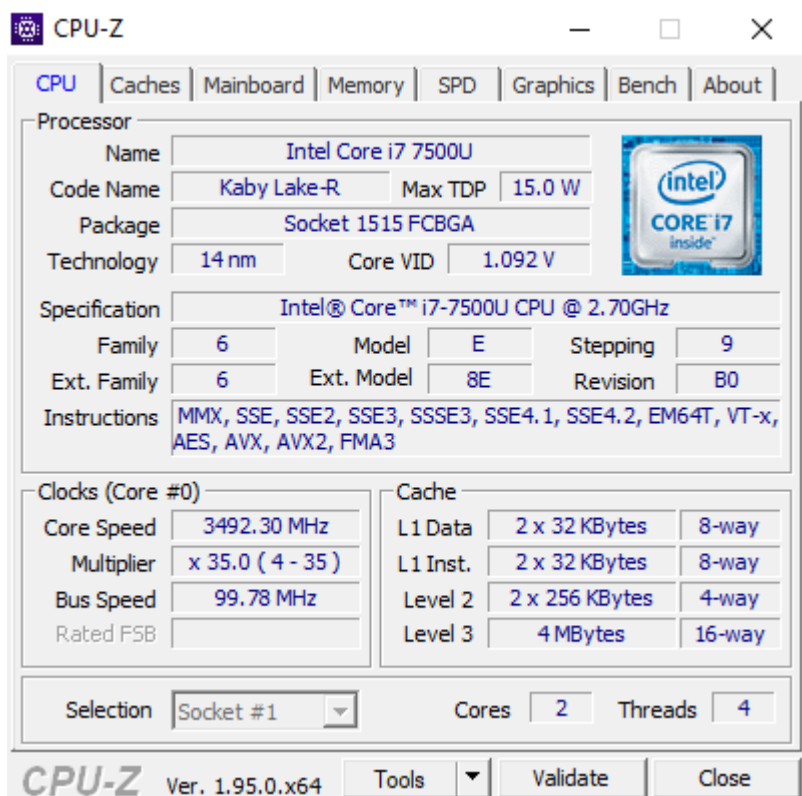
Introducing AIDA64



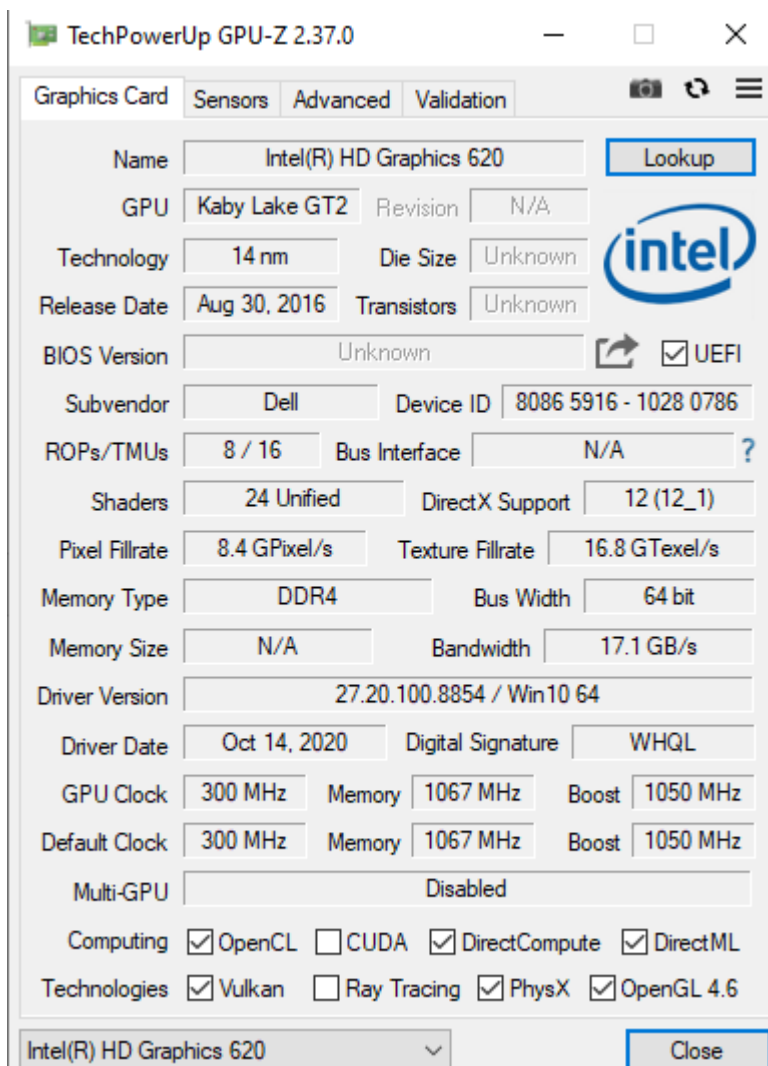
AIDA64 Engineer is a streamlined Windows diagnostic and benchmarking software for home users.

AIDA64 Engineer provides a wide range of features to assist in overclocking, hardware error diagnosis, stress testing, and sensor monitoring. It has unique capabilities to assess the performance of the processor, system memory, and disk drives. AIDA64 is compatible with all current 32-bit and 64-bit Microsoft Windows operating systems, including Windows 10 and Windows Server 2016.

A program széleskörű szolgáltatásokat biztosít a felhasználó számára mintpéldául a merevlemez hiba diagnosztika vagy tesztelés esetleg szenzor értékek listázása.



Ez a program információkat biztosít a számítógép komponenseiről.



Ez a program részletesebb leírást ad eszközünk grafikus kártyájáról.