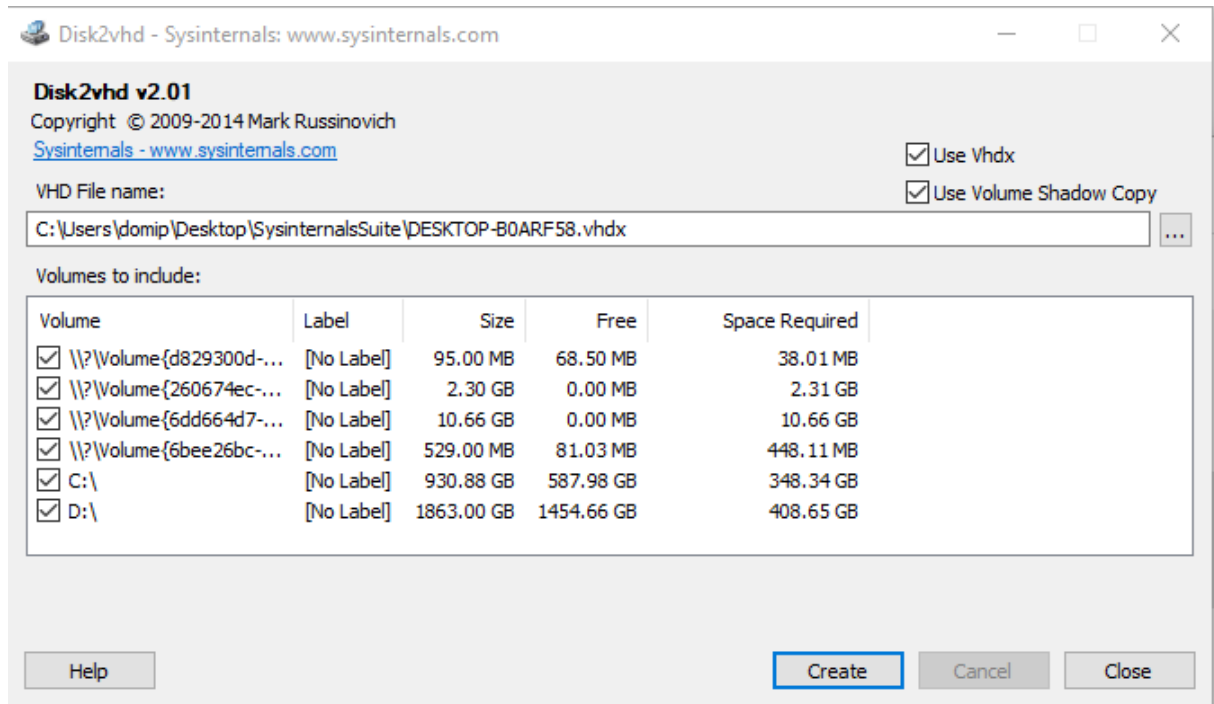


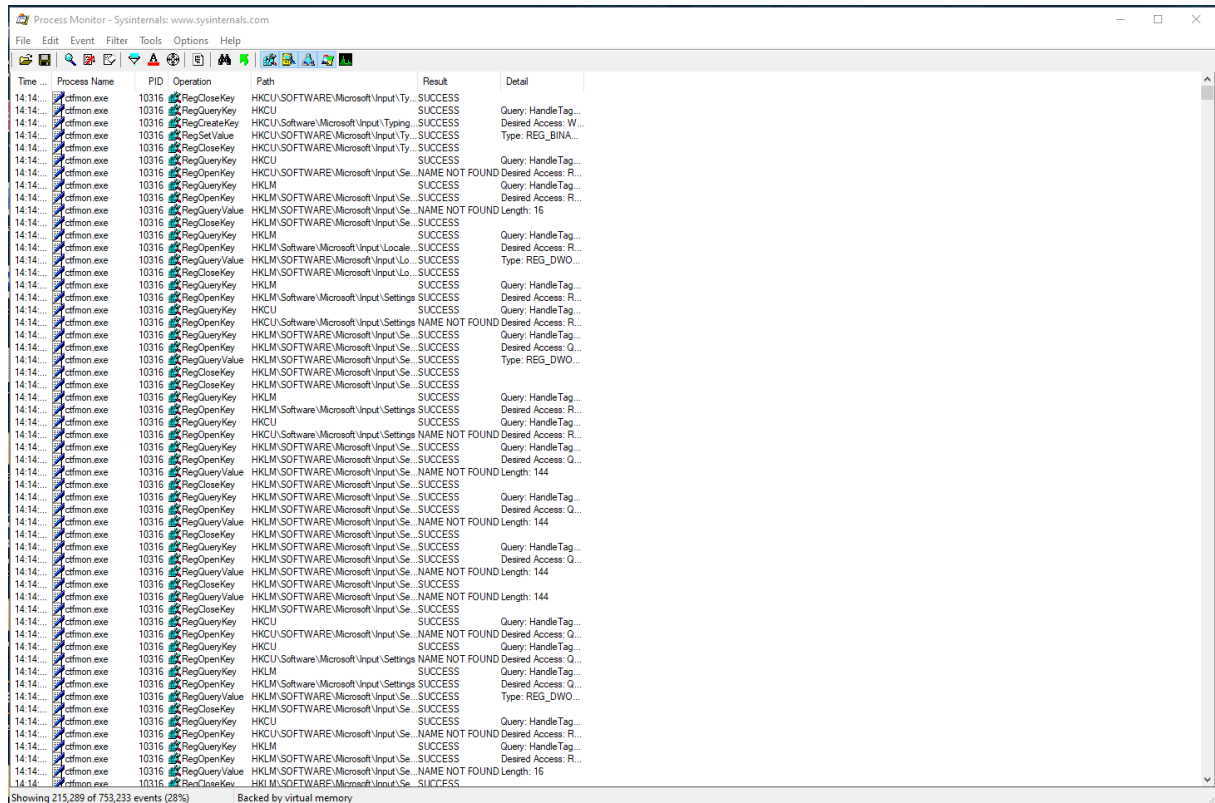
Disk2vhd

A Disk2vhd-vel lehet készíteni egy Virtual Hard Disk-et ami egy virtuális gép lemez formátuma.



Process Monitor

A Process Monitor egy speciális megfigyelő eszköz Windows számára, amely valós idejű fájlrendszert, nyilvántartást és folyamat / szál tevékenységet mutat



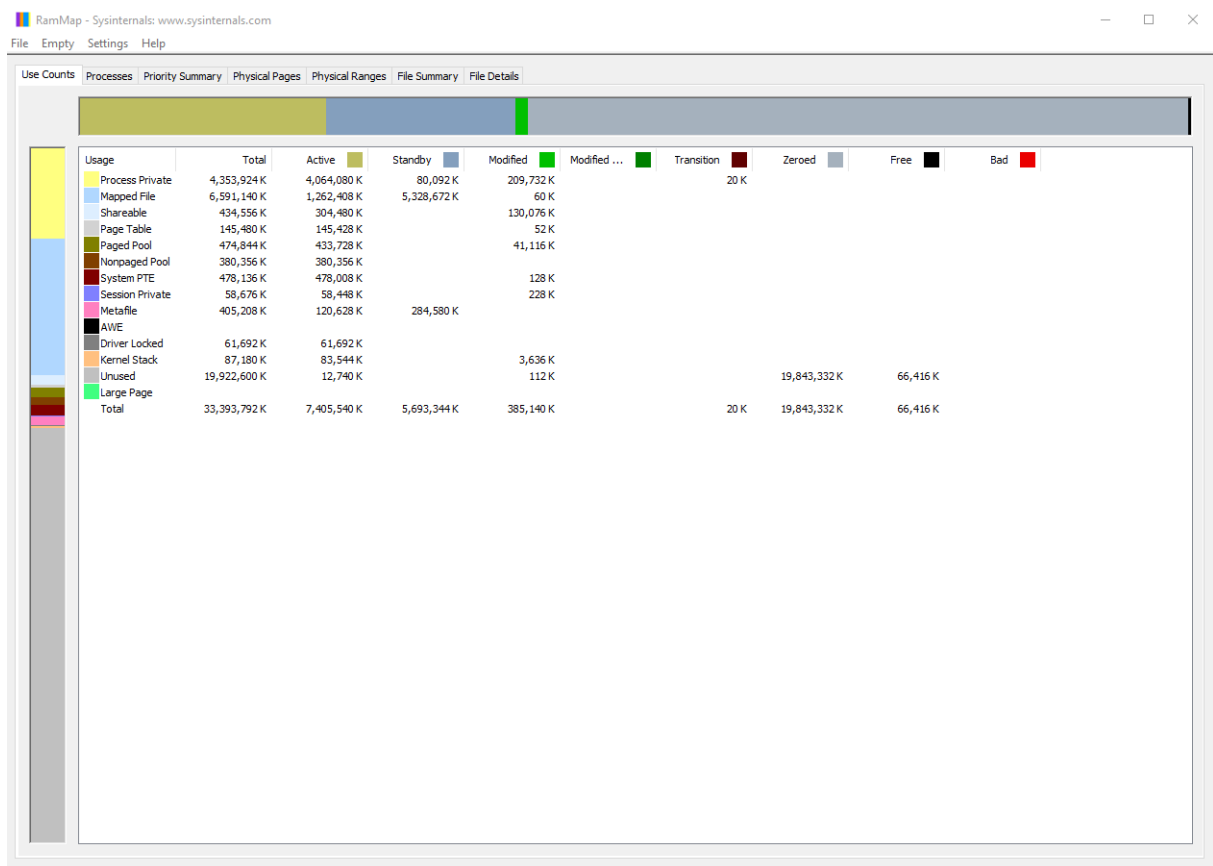
The screenshot shows the Process Monitor application window with the following columns: Time, Process Name, PID, Operation, Path, Result, and Detail. The events listed are primarily registry operations performed by 'ctfmon.exe' with PID 10316. The operations include RegCloseKey, RegOpenKey, RegCreateKey, RegSetValue, RegQueryValue, and RegCloseKey. The paths involved are mostly under 'HKCU\Software\Microsoft\Input\Settings' and 'HKLM\Software\Microsoft\Input\Settings'. The results are mostly 'SUCCESS', with some 'NAME NOT FOUND' errors. The details provide further information about the operations, such as 'Query: HandleTag...', 'Desired Access: R...', and 'Type: REG_DWORD'.

Time	Process Name	PID	Operation	Path	Result	Detail
14:14	ctfmon.exe	10316	RegCloseKey	HKCU\SOFTWARE\Microsoft\Input\Ty...	SUCCESS	
14:14	ctfmon.exe	10316	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegCreateKey	HKCU\Software\Microsoft\Input\Typing...	SUCCESS	Desired Access: W...
14:14	ctfmon.exe	10316	RegSetValue	HKCU\SOFTWARE\Microsoft\Input\Ty...	SUCCESS	Type: REG_BINA...
14:14	ctfmon.exe	10316	RegCloseKey	HKCU\SOFTWARE\Microsoft\Input\Ty...	SUCCESS	
14:14	ctfmon.exe	10316	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Desired Access: R...
14:14	ctfmon.exe	10316	RegOpenKey	HKLM	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: R...
14:14	ctfmon.exe	10316	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 16
14:14	ctfmon.exe	10316	RegOpenKey	HKLM	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegOpenKey	HKLM\Software\Microsoft\Input\Locale...	SUCCESS	Desired Access: R...
14:14	ctfmon.exe	10316	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	Type: REG_DWO...
14:14	ctfmon.exe	10316	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	
14:14	ctfmon.exe	10316	RegOpenKey	HKLM	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
14:14	ctfmon.exe	10316	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: R...
14:14	ctfmon.exe	10316	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
14:14	ctfmon.exe	10316	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Type: REG_DWO...
14:14	ctfmon.exe	10316	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
14:14	ctfmon.exe	10316	RegOpenKey	HKLM	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
14:14	ctfmon.exe	10316	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: R...
14:14	ctfmon.exe	10316	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
14:14	ctfmon.exe	10316	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
14:14	ctfmon.exe	10316	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
14:14	ctfmon.exe	10316	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
14:14	ctfmon.exe	10316	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
14:14	ctfmon.exe	10316	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
14:14	ctfmon.exe	10316	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Desired Access: Q...
14:14	ctfmon.exe	10316	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Q...
14:14	ctfmon.exe	10316	RegOpenKey	HKLM	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: Q...
14:14	ctfmon.exe	10316	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Type: REG_DWO...
14:14	ctfmon.exe	10316	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
14:14	ctfmon.exe	10316	RegOpenKey	HKCU	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Desired Access: R...
14:14	ctfmon.exe	10316	RegOpenKey	HKLM	SUCCESS	Query: HandleTag...
14:14	ctfmon.exe	10316	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: R...
14:14	ctfmon.exe	10316	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 16
14:14	ctfmon.exe	10316	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	

Showing 215,289 of 753,233 events (28%) Backed by virtual memory

Rammap

A RAMMap egy hordozható, önálló szoftvereszköz, amely lehetővé teszi, hogy pontosan lássuk, hogyan rendeli a Windows a fizikai memóriát.



Tcpview

A TCPView egy Windows program, amely megmutatja a rendszer összes TCP és UDP végpontjának részletes felsorolását.

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-B0ARF...	1120	localhost	50533	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50640	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50639	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50638	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50642	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50566	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50645	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50645	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50644	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50616	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50613	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50606	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50611	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50641	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50654	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50667	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50663	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50648	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50668	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50619	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50671	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50655	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50655	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50643	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50660	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50569	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50590	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50591	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50597	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50605	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50595	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50658	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50612	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50635	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50624	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50657	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50653	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50631	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50632	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50634	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50651	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50636	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50664	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50669	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50604	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50607	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	50584	xx-fbcdn-shv-01-a...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50521	xx-fbcdn-shv-01-a...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50571	get-dul.adobe.com	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50573	a184-51-8-147.de...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50580	a104-103-72-51.d...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50582	a104-103-72-178...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50583	a184-51-9-85.depl...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50585	a104-103-72-179...	https	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	50569	localhost	1120	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50592	a104-103-105-234...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50633	52.155.94.78	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50143	edge-star-mini-shv...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50553	muc0307-in-f931...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50602	get-dul.adobe.com	https	TIME_WAIT					
[System Proc...	0	TCP	DESKTOP-B0ARF...	1120	localhost	50655	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50662	52.137.110.235	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50370	lhr35s02-in-42.1e...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50380	bud02c25-in-f8.1e...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50381	bud02c23-in-194...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50382	23.235.196.35.bc...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50384	25.25.190.35.bc.g...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50385	wlr-in-f155.1e100.net	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50386	bud02c24-in-f2.1e...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50389	prg02a12-in-f2.1e...	https	TIME_WAIT					
[System Proc...	0	TCP	desktop-b0arf58	50310	bud02c26-in-f3.1e...	https	TIME_WAIT					
Agent.exe	11400	TCP	DESKTOP-B0ARF...	1120	DESKTOP-B0ARF...	0	LISTENING					
Agent.exe	11400	TCP	desktop-b0arf58	50474	24.105.29.76	https	CLOSE_WAIT					
ArmouryCrate...	4292	TCP	DESKTOP-B0ARF...	9487	DESKTOP-B0ARF...	0	LISTENING					
ArmouryCrate...	4292	TCP	DESKTOP-B0ARF...	9487	localhost	49720	ESTABLISHED	2		104		56
ArmouryCrate...	4292	TCP	DESKTOP-B0ARF...	13010	DESKTOP-B0ARF...	0	LISTENING					
ArmouryCrate...	1360	TCP	DESKTOP-B0ARF...	13031	DESKTOP-B0ARF...	0	LISTENING					
ArmouryCrate...	1360	TCP	DESKTOP-B0ARF...	13032	DESKTOP-B0ARF...	0	LISTENING					
ArmouryCrate...	1360	TCP	DESKTOP-B0ARF...	17945	DESKTOP-B0ARF...	0	LISTENING					
ArmouryCrate...	1360	TCP	DESKTOP-B0ARF...	49720	localhost	9487	ESTABLISHED	2		56		104
ArmouryCrate...	1360	TCP	DESKTOP-B0ARF...	49759	localhost	9012	ESTABLISHED					
Endpoints: 291 Established: 105 Listening: 48 Time Wait: 71 Close Wait: 15												

Diskview

A DiskView a lemez grafikus térképét jeleníti meg, amely lehetővé teszi, hogy meghatározza a fájl helyét, vagy egy förtre kattintva megnézze, melyik fájl foglalja el.

