

Process Monitor - Sysinternals: www.sysinternals.com					
File Edit Event Filter Tools Options Help					
Time o...	Process Name	PID	Operation	Path	Result
18:06:58...	MsMpEng.exe	4356	ReadFile	C:\Users\arvaidora\Desktop\OS\Sysinte...	SUCCESS
18:06:58...	svchost.exe	2964	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS
18:06:58...	svchost.exe	2964	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS
18:06:58...	MsMpEng.exe	4356	ReadFile	C:\ProgramData\Microsoft\Windows Def...	SUCCESS
18:06:58...	MsMpEng.exe	4356	ReadFile	C:\Users\arvaidora\Desktop\OS\Sysinte...	SUCCESS
18:06:58...	svchost.exe	2156	RegOpenKey	HKLM\Software\Microsoft\SecurityMana...	SUCCESS
18:06:58...	svchost.exe	2156	RegQueryValue	HKLM\SOFTWARE\Microsoft\SecurityM...	NAME NOT FOUND
18:06:58...	svchost.exe	2156	RegCloseKey	HKLM\SOFTWARE\Microsoft\SecurityM...	SUCCESS
18:06:58...	svchost.exe	2156	RegOpenKey	HKLM\Software\Microsoft\SecurityMana...	SUCCESS
18:06:58...	svchost.exe	2156	RegQueryValue	HKLM\SOFTWARE\Microsoft\SecurityM...	NAME NOT FOUND
18:06:58...	svchost.exe	2156	RegCloseKey	HKLM\SOFTWARE\Microsoft\SecurityM...	SUCCESS
18:06:58...	svchost.exe	2964	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS
18:06:58...	svchost.exe	2156	RegOpenKey	HKLM\Software\Microsoft\SecurityMana...	SUCCESS
18:06:58...	svchost.exe	2156	RegQueryValue	HKLM\SOFTWARE\Microsoft\SecurityM...	NAME NOT FOUND
18:06:58...	svchost.exe	2156	RegCloseKey	HKLM\SOFTWARE\Microsoft\SecurityM...	SUCCESS
18:06:58...	MsMpEng.exe	4356	ReadFile	C:\ProgramData\Microsoft\Windows Def...	SUCCESS
18:06:58...	MsMpEng.exe	4356	ReadFile	C:\Users\arvaidora\Desktop\OS\Sysinte...	SUCCESS
18:06:58...	svchost.exe	2964	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS
18:06:58...	MsMpEng.exe	4356	ReadFile	C:\ProgramData\Microsoft\Windows Def...	SUCCESS
18:06:58...	svchost.exe	5660	RegQueryKey	HKCU\Software\Classes	SUCCESS
18:06:58...	MsMpEng.exe	4356	ReadFile	C:\Users\arvaidora\Desktop\OS\Sysinte...	SUCCESS
18:06:58...	svchost.exe	2964	LockFile	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS
18:06:58...	svchost.exe	5660	RegQueryKey	HKCU\Software\Classes	SUCCESS
18:06:58...	svchost.exe	5660	RegQueryKey	HKCU\Software\Classes	SUCCESS
18:06:58...	svchost.exe	5660	RegOpenKey	HKCU\Software\Classes\CLSID\{37987...	NAME NOT FOUND
<div> <div>Showing 55 088 of 386 183 events (14%)</div> <div>Backed by virtual memory</div> </div>					

A Process Monitor egy olyan program, ami megmutatja a valós idejű fájlrendszer, registry, és folyamat tevékenységeket. Például fájlból való olvasás, fájlzárolás, registry kulcsok megnyitása, stb.