

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
16:34:...	ctfmon.exe	10912	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
16:34:...	ctfmon.exe	10912	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
16:34:...	ctfmon.exe	10912	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
16:34:...	ctfmon.exe	10912	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
16:34:...	ctfmon.exe	10912	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
16:34:...	ctfmon.exe	10912	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
16:34:...	ctfmon.exe	10912	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
16:34:...	ctfmon.exe	10912	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
16:34:...	ctfmon.exe	10912	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
16:34:...	ctfmon.exe	10912	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
16:34:...	ctfmon.exe	10912	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
16:34:...	ctfmon.exe	10912	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
16:34:...	ctfmon.exe	10912	RegCloseKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	
16:34:...	ctfmon.exe	10912	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
16:34:...	ctfmon.exe	10912	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
16:34:...	ctfmon.exe	10912	RegQueryValue	HKCU\Software\Microsoft\Input\Settin...	NAME NOT FOUND	Length: 16
16:34:...	ctfmon.exe	10912	RegCloseKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	
16:34:...	ctfmon.exe	10912	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
16:34:...	ctfmon.exe	10912	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: Q...
16:34:...	ctfmon.exe	10912	RegQueryValue	HKCU\Software\Microsoft\Input\Settin...	NAME NOT FOUND	Length: 16
16:34:...	ctfmon.exe	10912	RegCloseKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	
16:34:...	ctfmon.exe	10912	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
16:34:...	ctfmon.exe	10912	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: Q...
16:34:...	ctfmon.exe	10912	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Type: REG_DWO...
16:34:...	ctfmon.exe	10912	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
16:34:...	ctfmon.exe	10912	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
16:34:...	ctfmon.exe	10912	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
16:34:...	ctfmon.exe	10912	RegOpenKey	HKLM\Software\Microsoft\Input\Locale...	SUCCESS	Desired Access: R...
16:34:...	ctfmon.exe	10912	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
16:34:...	ctfmon.exe	10912	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	Type: REG_DWO...
16:34:...	ctfmon.exe	10912	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
16:34:...	ctfmon.exe	10912	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
16:34:...	ctfmon.exe	10912	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	
16:34:...	ctfmon.exe	10912	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
16:34:...	ctfmon.exe	10912	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Desired Access: Q...
16:34:...	ctfmon.exe	10912	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
16:34:...	ctfmon.exe	10912	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
16:34:...	ctfmon.exe	10912	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
16:34:...	ctfmon.exe	10912	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
16:34:...	ctfmon.exe	10912	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Type: REG_DWO...
16:34:...	ctfmon.exe	10912	RegQueryValue	HKCU\Software\Microsoft\Input\Settin...	NAME NOT FOUND	Length: 144
16:34:...	ctfmon.exe	10912	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
16:34:...	ctfmon.exe	10912	RegCloseKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	
16:34:...	ctfmon.exe	10912	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
16:34:...	ctfmon.exe	10912	RegOpenKey	HKCU\Software\Microsoft\Input\Locale...	NAME NOT FOUND	Desired Access: Q...
16:34:...	ctfmon.exe	10912	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
16:34:...	ctfmon.exe	10912	RegOpenKey	HKLM\Software\Microsoft\Input\Locale...	SUCCESS	Desired Access: Q...
16:34:...	ctfmon.exe	10912	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Lo...	NAME NOT FOUND	Length: 16
16:34:...	ctfmon.exe	10912	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	
16:34:...	ctfmon.exe	10912	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
16:34:...	ctfmon.exe	10912	RegOpenKey	HKLM\Software\Microsoft\Input\Locale...	SUCCESS	Desired Access: Q...
16:34:...	ctfmon.exe	10912	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	Type: REG_SZ, Le...
16:34:...	ctfmon.exe	10912	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	
16:34:...	ctfmon.exe	10912	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
16:34:...	ctfmon.exe	10912	RegOpenKey	HKLM\Software\Microsoft\Input\Locale...	SUCCESS	Desired Access: Q...
16:34:...	ctfmon.exe	10912	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Lo...	NAME NOT FOUND	Length: 16
16:34:...	ctfmon.exe	10912	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	
16:34:...	ctfmon.exe	10912	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
16:34:...	ctfmon.exe	10912	RegOpenKey	HKLM\Software\Microsoft\Input\Locale...	SUCCESS	Desired Access: Q...
16:34:...	ctfmon.exe	10912	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Lo...	NAME NOT FOUND	Length: 16
16:34:...	ctfmon.exe	10912	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	
16:34:...	ctfmon.exe	10912	RegQueryKey	C:\Windows\System32\user32.dll	SUCCESS	Offset: 4 011 000

Showing 93 953 of 126 914 events (74%) Backed by virtual memory

A Process Monitor egy speciális megfigyelő eszköz a Windows számára, amely valós idejű fájlrendszert, nyilvántartást és folyamat/szál tevékenységet mutat. Ötvözi a régi Sysinternals két segédprogram, a Filemon és a Regmon szolgáltatásait, és kiterjedt listát ad a fejlesztésekről, beleértve a gazdag és roncsolásmentes szűrést, az átfogó eseménytulajdonságokat, például a munkamenet-azonosítókat és a felhasználói neveket, a megbízható folyamatinformációkat, a teljes szálhalmokat integrált szimbólummal minden

művelet támogatása, egyidejű naplózás egy fájlba és még sok más. Egyedülálló funkciói révén a Process Monitor a rendszer hibaelhárítási és rosszindulatú program-vadász eszközkészletének alapvető segédprogramja lesz.