Introduction

Filemon is an application that monitors and displays all file system activity on a system. It has advanced filtering and search capabilities that make it a powerful tool for exploring the way Windows works, seeing how applications use the files and DLLs, or tracking down problems in system or application configurations.

Filemon works on NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Windows 95, Windows 98 and Windows ME.

Starting Filemon

Simply run *Filemon* (filemon.exe). You must have administrator privilege to run Filemon. When *Filemon* is started for the first time it will monitor all local hard drives. Menus, hot-keys, or toolbar buttons can be used to clear the window, select and deselect monitored volumes including network volumes (Windows NT/2K/XP), save the monitored data to a file, and to filter and search output.

If you’ve specified filters then Filemon will ask you to confirm filters used from the last session each time you start it. To start Filemon without it prompting you specify the **/q** switch on the command line.

When Filemon starts it automatically captures file system activity. To start it with capture disabled use the **/o** switch on the command-line.

As events are printed to the output, they are tagged with a sequence number. If *Filemon’s* internal buffers are overflowed during extremely heavy activity, this will be reflected with gaps in the sequence number.

Each time you exit *Filemon* it remembers the position of the window and the widths of the output columns.

Default Mode vs Advanced Mode

Filemon’s default viewing mode now has a filtering mechanism to remove the activity that is useless in most troubleshooting scenarios and that presents intuitive names for all I/O operations. FASTIO_CHECK_IF_POSSIBLE is filtered out, FASTIO_READ failures aren't shown, and FASTIO_READ's that succeed are reported as "READ" operations. In addition, the default view omits file system activity in the System process, which is the process from which the Memory and Cache Manager's perform background activity, and all Memory Manager paging activity, including that to the system's paging file. The **Options|Advanced** menu item will satisfy users, such as file system filter driver developers, that want the "raw" view of file system activity shown by previous Filemon versions.

Selecting Volumes (Windows NT/2K)

The Volumes menu can be used to select and deselect monitored volumes. Select the Network menu item to monitor accesses to any network resources, including remote shares and UNC path name accesses to remote volumes.

Formatting Drives (Windows NT)

You can watch drives being formatted using *Filemon*, however, after a format is complete you must deselect and reselect the drive in order to continue monitoring it.

Filtering Output

Use the **Filter** dialog, which is accessed with a toolbar button or the **Options|Filter/Highlight** menu selection, to select what data will be shown in the list view. The '*' wildcard matches arbitrary strings, and the filters are case-insensitive. Only matches shown in the include filter, but that are not excluded with the exclude filter, are displayed. Use ';' to separate multiple strings in a filter (e.g. "*filemon*;*temp*"). Because of the asynchronous nature of most file I/O, filtering on the result field is not possible.

For example, if the include filter is "c:\temp", and the exclude filter is "c:\temp\subdir", all references to files and directories under c:\temp, except to those under c:\temp\subdir will be monitored.

Wildcards allow for complex pattern matching, making it possible to match specific file accesses by specific applications, for example. The include filter "Winword*Windows" would have *Filemon* only show accesses by Microsoft Word to files and directories that include the word "Windows".

Use the highlight filter specify output that you want to have highlighted in the listview output. Select highlighting colors with **Options |Highlight Colors**.

Limiting Output

The **History Depth** dialog, accessed via toolbar button or the **Options |History** menu item, allows you to specify the maximum number of lines that will be remembered in the output window. A depth of 0 is used to signify no limit.

Searching the Output

You can search the output window for strings using the Find menu item (or the find toolbar button). You can repeat the search in the forward direction with the F3 key and in reverse with Shift+F3.

To start a search at a particular line in the output, select the desired line by clicking on the far left column (the index number). If no line is selected a new search starts at the first entry in searching down, and at the last entry for searching up.

Options

Filemon can either timestamp events or show their duration. The Options menu and the clock toolbar button let you toggle between the two modes. The button on the toolbar shows the current mode with a clock or a stopwatch. When showing duration the Time field in the output shows the number of seconds it took for the underlying file system to service particular requests. The **Options|Show Milliseconds** menu entry lets you add millisecond resolution to times presented when *Filemon* shows clock times.

You can toggle *Filemon* to always remain a top window with the Options|Always On Top menu item. In addition, you can toggle *Filemon* not to scroll the listview via the Options|Auto Scroll menu item or corresponding toolbar button.

Font Selection

Use the **Edit|Font** menu item to change the font used in the listview.

Jumping to a Directory in *Explorer*

If you come across a file or directory name in the output that you want to modify or view in *Filemon*, you can jump the directory by double-clicking on the output line. *Fielmon* will launch *Explorer* and navigate directly to the directory or file in which the directory resides.

Reporting Bugs and Feedback

If you encounter a problem while running *Filemon*, please visit www.sysinternals.com to obtain the latest version. If you still have problems, please record all the information in the top few lines of a Blue Screen (if you encounter one), as well as the section of addresses and driver names just above the administrative message. Determine if the problem is reproducible, and if so, how, and send this information to:

mark@sysinternals.com

Licensing

If you want to license *Filemon* for redistribution, or license *Filemon* source code, please contact licensing@sysinternals.com.