Introduction

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

Filemon works on NT 3.51, NT 4.0, Windows 2000 (NT 5.0), Windows 95 and Windows 98.

Starting Filemon

Simply run the *Filemon* GUI (filemon.exe) from the same directory that the drivers (filemon.sys and filemon.vxd) reside in. *Windows NT: Note that it must be located on a non-network drive and that you must have administrative 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 drives (Windows NT/2K), save the monitored data to a file, and to filter and search output.

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.

On Windows NT/2K there is a special file name, DASD (Direct Access Storage Device), that is used to indicate file I/O that is bypassing file system structures and directly effecting data on the logical partition, or I/O that is targeted at file system-internal unnamed data streams. Unnamed data streams are used to represent file system metadata files such as the File Allocation Table in the FAT file system, or the Master File Table (MFT) in NTFS. Also on Windows NT/2K, an asterisk ('*') following an IRP_MJ_READ or IRP_MJ_WRITE indicates paging I/O.

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

Selecting Drives (Windows NT/2K)

The Drives menu can be used to select and deselect monitored drives. Note that if you deselect a network drive that is under the control as the same driver (network redirector) controlling other network drives, all drives will be deselected. The same applies for selecting a network drive for monitoring.

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 Edit|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*").

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.

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

Limiting Output

The History Depth dialog, accessed via toolbar button or the Edit|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). Once you have opened a Find dialog and hit the FindNext button, you can repeat the search without changing the focus back to the Find dialog by hitting the F3 key.

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.

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.

Reporting Bugs and Feedback

If you encounter a problem while running *Filemon*, please visit http://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 one is generated), 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 and
cogswell@winternals.com