

Filemon

Copyright 1996-1997 Mark Russinovich and Bryce Cogswell
<http://www.ntinternals.com>

Introduction

Filemon is a GUI/device driver combination that together monitor 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 Windows 95 works, seeing how applications use files and DLLs, or tracking down problems in system or application configurations.

Starting Filemon

Simply run the *Filemon* GUI (*Filemon.exe*) from the same directory that the driver (*filemon.vxd*) resides. Menus, hot-keys, or toolbar buttons can be used to clear the window, select and deselect monitored drives, 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.

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

Filtering Output

Use the Filter dialog 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 path include filter, but that are not excluded with the path exclude filter, are displayed. The process filter also accepts the wildcard character.

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

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.

Limiting Output

The History Depth entry in the Filter dialog 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.

Reporting Bugs and Feedback

If you encounter a problem while running *Filemon*, please record all the information you can about your system configuration and the software you are running. Determine if the problem is reproducible, and if so, how, and send this information to:

mark@ntinternals.com and
cogswell@winternals.com

