Regmon for Windows 95/98

http://www.sysinternals.com

Introduction

Regmon is a GUI/device driver combination that together monitor and display all Registry activity on a system. It has advanced filtering and search capabilities that make it a powerful tool for exploring the way Windows 95/98 works, seeing how applications use the Registry, or tracking down problems in system or application configurations. A Windows NT version of *Regmon* is available at Systems Internals (http://ww.sysinternals.com).

Starting Regmon

Simply run the *Regmon* GUI (Regmon.exe) from the same directory that the driver (regvxd.vxd) resides in. Menus, hot-keys, or toolbar buttons can be used to clear the window, 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 *Regmon's* internal buffers are overflowed during extremely heavy activity, this will be reflected with gaps in the sequence number. Note that if *Regmon* sees an access to a Registry key that was opened before it was started, *Regmon* won't know the key's name. In such cases it prints out the raw value of the key instead, which will show up as a hexadecimal value (e.g. 0xc0002304).

Each time you exit *Regmon* 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, filters are case-insensitive. Only matches shown in the path include filter, but that are not excluded with the path exclude filter, are displayed. Use ';' to separate multiple filter component strings (e.g. "*CurrentControl*;*Software*"). The process filter also accepts the wildcard character, and multiple process strings separated with ';'.

For example, if the path include filter is "HKLM*", and the path exclude filter is "HKLM\System*", all references to keys and values under HLM\, except to those under HKLM\System would be monitored.

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.

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.

Viewing Partially Obscured Fields

Fields within a row in *Regmon's* output may be partially hidden if the field's column is not wide enough to fully display the field's text. You can direct *Regmon* to display a tool-tip that contains the full text of the field for convenient viewing by right-clicking on the desired field. To remove the tool-tip just move the mouse over it. Also, an existing tool-tip will disappear if you right click again to make another one pop-up.

Reporting Bugs and Feedback

If you encounter a problem while running *Regmon*, please visit http://www.sysinternals.com to obtain the latest version. If you still have problems, please record all the information available on your system and the software you are running. Determine if the problem is reproducible, and if so, how, and send this information to:

mark@sysinternals.com and
cogswell@winternals.com