GLSOF-QUERIES

Glsof (http://glsof.sourceforge.net) is two separate utilities (Queries and FileMonitor) to the command line utility **Lsof** (http://people.freebsd.org/~abe/) by Vic Abell. Glsof is released under GPL 3 license (http://www.gnu.org/licenses/gpl.html).

You can contact me at: danielef@users.sourceforge.net

Donations

If you use and appreciate my open source project, please consider making a donation. All donations are handled by PayPal. Any amount is greatly appreciated.

Thank you for supporting the project.

Link to donate

Introduction

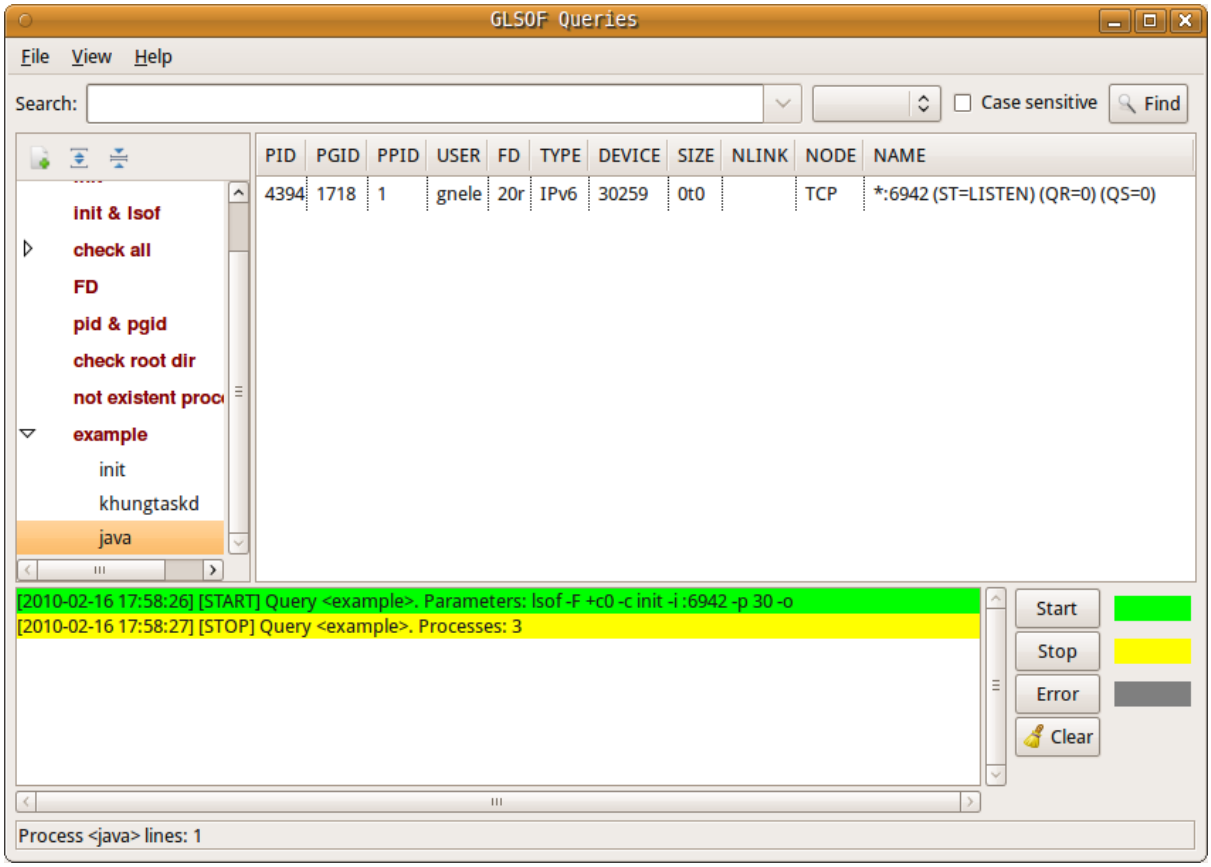
Queries manages multiple queries for Lsof, returning output in different tables. To launch it just use:

```
$> java -jar path/queries.jar
```

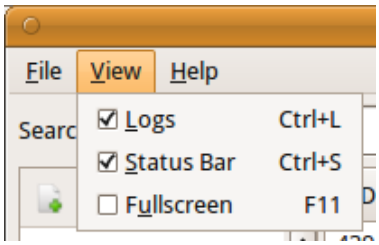
Queries permits the user to manage Lsof's options (though not all yet - this gap will be filled with next releases) as a **query**. A query is the unit of work for Queries. For example you can express:

```
$> lsof -c init -i :6942 -p 30
```

like a query and run it. The application will return something similar to:



Menu



Queries has a main menu at the top, composed of:

- **File->Exit (Ctrl+Q):** close application and save main window coordinates and internal widgets dispositions.
- **View->Logs (Ctrl+L):** show/hide the logger.
- **View->Status Bar (Ctrl+S):** show/hide the status bar.
- **View->Fullscreen (F11):** enable/disable fullscreen mode.
- **Help->About:** show dialog with logo, author info and license.

Search bar

Search bar enables you to search a specific test around executed queries. If one or more queries are running, the search bar will be disabled and reset.

A search has the following parameters:

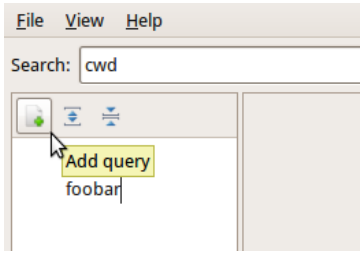
1. **Input field** represents text to search.
2. **Column** is the query's column to search in. *Process* enables search on the process column (Queries tree). The remaining columns enable search in the processes' tables for the chosen column. If no column is specified, the search will be executed for every column.
3. **Case sensitive** enables case sensitive for text to search.

To execute a search press the **Find** button. If input text and/or column and/or case-sensitive change before executing the next search, it will be restarted from the top row of the top process of the top query. When a search reaches the last table's row of the last process of the last query, a dialog comes up with the choice to restart the search from the beginning or not.

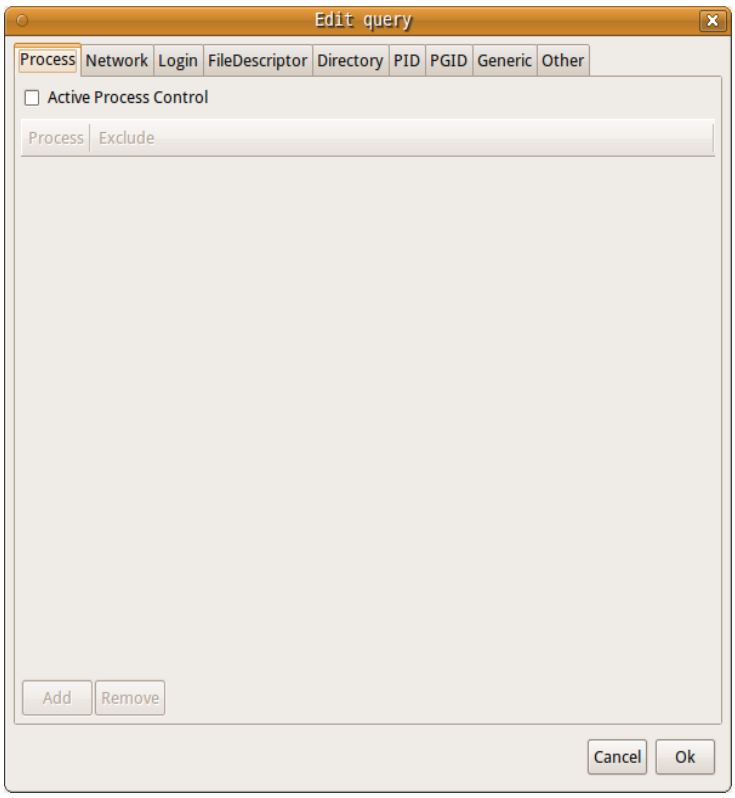
Queries

As stated before, a **query** is the unit of work for Queries. It consists of a set of lists and checkable options that will be converted in parameters for Lsof. The area representing queries is divided in a left tree that collects queries' names and relative processes, and a right part showing returned information for every single process in a table. The left and right side are separated by a split panel that enable you to resize them.

Create a new query



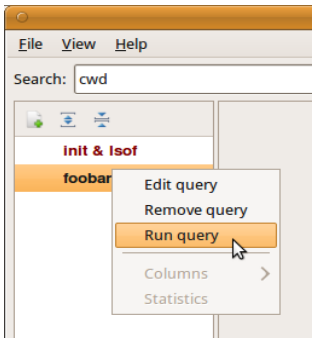
To create a new query just click on the 'Add query' button (next to it there are 'Expand all the queries' and 'Collapse all the queries' buttons to expand or collapse the processes list for executed queries), type the name (e.g. foobar) and press 'Enter'. Afterwards a dialog will open to set the options for your query. More details about 'query dialog' will be given in later chapters.



Once you have set your options, just press 'OK' and automatically the dialog will be closed and the query saved. Otherwise, if you press 'Cancel' the dialog will be closed but the query will be not saved.

You can create as many queries as you like but you cannot create two queries with the same name.

Run a query



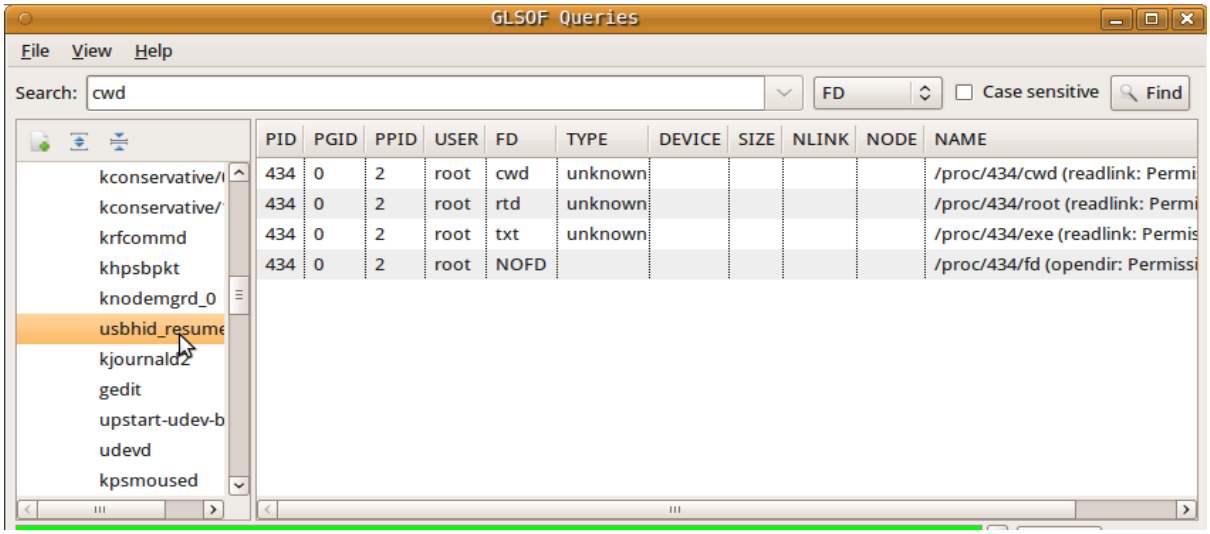
To run a query you have to click with the right mouse button on the query name that you want to execute and choose the 'Run query' option from the popup menu that will come up.

When a query is executed, a spinning arrow beside the query's name will be run. When execution is completed, a list of processes (if any) will be shown in an automatically expanded subtree item just below the query's name. When you click one of the processes, it’s returned information will be displayed in a table on the right side.

The returned data has the following columns:

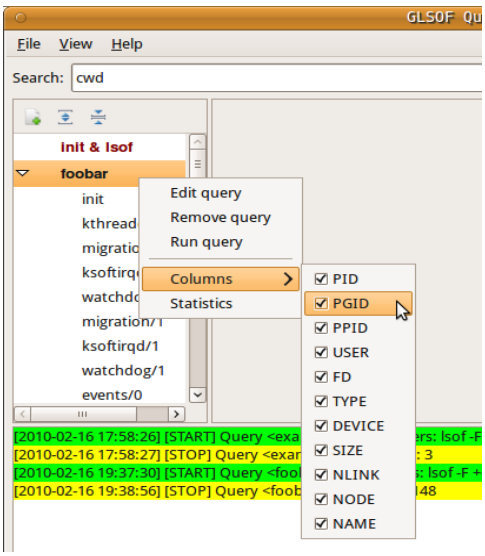
1. **PROCESS (queries tree)** contains the name of the UNIX command associated with the process.

2. **PID** is the Process IDentification number of the process.
3. **PGID** is the process group IDentification number associated with the process.
4. **PPID** is the Parent Process IDentification number of the process.
5. **USER** is the user ID number or login name of the user to whom the process belongs, usually the same as reported by ps(1). However, on Linux USER is the user ID number or login that owns the directory in /proc where lsof finds information about the process. Usually that is the same value reported by ps(1), but may differ when the process has changed its effective user ID.
6. **FD** is the File Descriptor number of the file (lsof-man for more info).
7. **TYPE** is the type of the node associated with the file (lsof-man for more info).
8. **DEVICE** contains the device numbers, separated by commas, for a character special, block special, regular, directory or NFS file (lsof-man for more info).
9. **SIZE** is the size of the file or the file offset in bytes. A value is displayed in this column only if it is available (lsof-man for more info).
10. **NLINK** contains the file link count.
11. **NODE** is the node number of a local file (lsof-man for more info).
12. **NAME** is the name of the mount point and file system on which the file resides (lsof-man for more info).



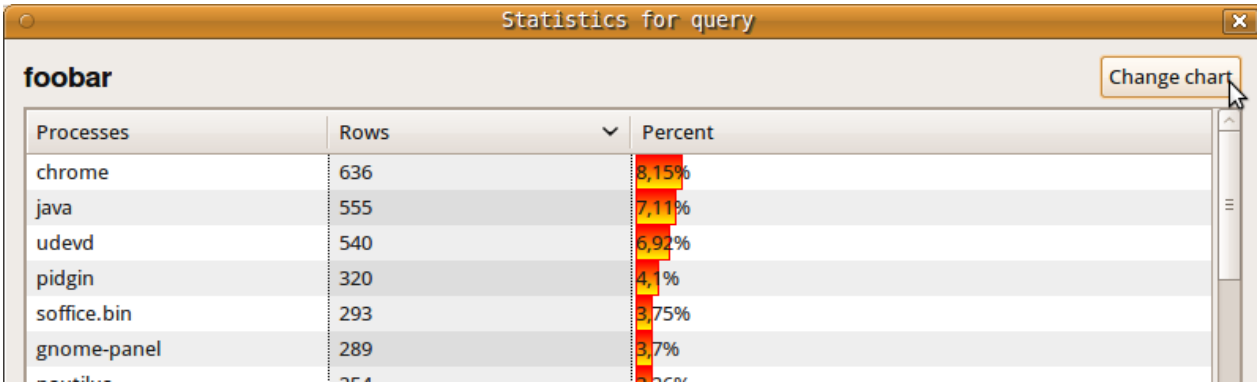
Columns

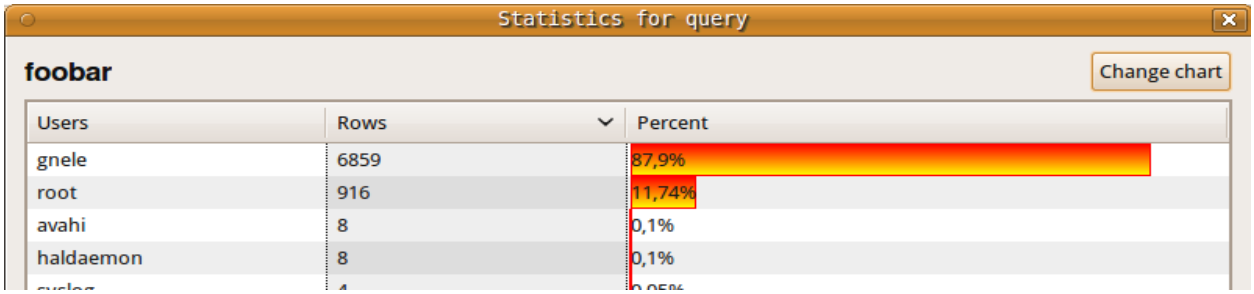
When a query is executed, it is possible to hide undesired columns. This setting will be automatically saved and will not influence other queries' settings.



Statistics

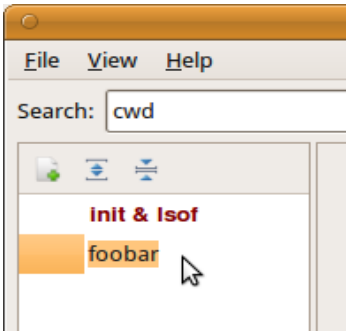
After a query execution it is possible to get some statistics (same popup menu) like number and percentage of files open for processes and users.





Rename a query

You can rename a query by just double clicking (left mouse button) on its name and typing the new name. Of course you cannot use the name of an existing query.



Remove a query

To remove a query, you have to click with the right mouse button on the query name that you want to remove. Afterwards a popup menu will come up and let you choose the 'Remove query' option.

Edit a query

To change settings in a query, you have to click on the query name that you want to edit choosing the 'edit' option on the menu that will come up. Similarly to create a new query, a dialog is opened.

Tabs inside the dialog are useful to compose parameters for Lsof. They are:

1. Process
2. Network
3. Login
4. File Descriptor
5. Directory
6. PID
7. PGID
8. Generic
9. Other

Excluding 'Other' all tabs have the same structure:

“Active XXXX Control” enables current option whose parameters are added to the table below, by the input dialog that comes up when the 'Add' button is clicked. 'Remove' is enabled when a line on the parameters' table is selected. Clicking on it, the selected parameter will be removed from the table.

It's not possible to enable an option leaving the parameters table empty. In this case a warning message will be displayed. 'Network' represents an exception to this. You will find more information later.

Note: Some parts of the following descriptions are extracted from Lsof's man-page.

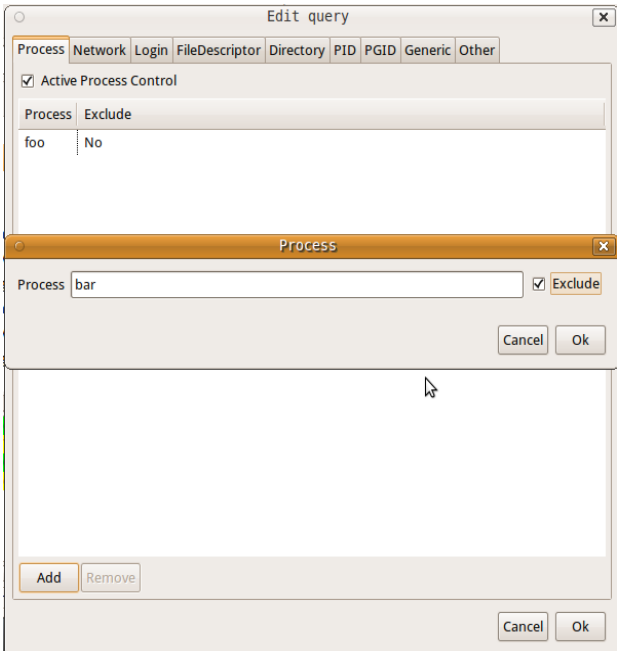
1) Process (-c)

This option selects the listing of files for processes executing the commands that begin with the characters of strings listed in the table.

If the parameter begins and ends with a slash ('/'), the characters between the slashes are interpreted

as a regular expression. The closing slash may be followed by these modifiers:

- b the regular expression is a basic one.
- i ignore the case of letters.
- x the regular expression is an extended one (default).



2) Network (-i)

This option selects the listing of files whose Internet address matches the addresses specified in the table. If no address is specified, this option selects the listing of all Internet and x.25 (HP-UX) network files.

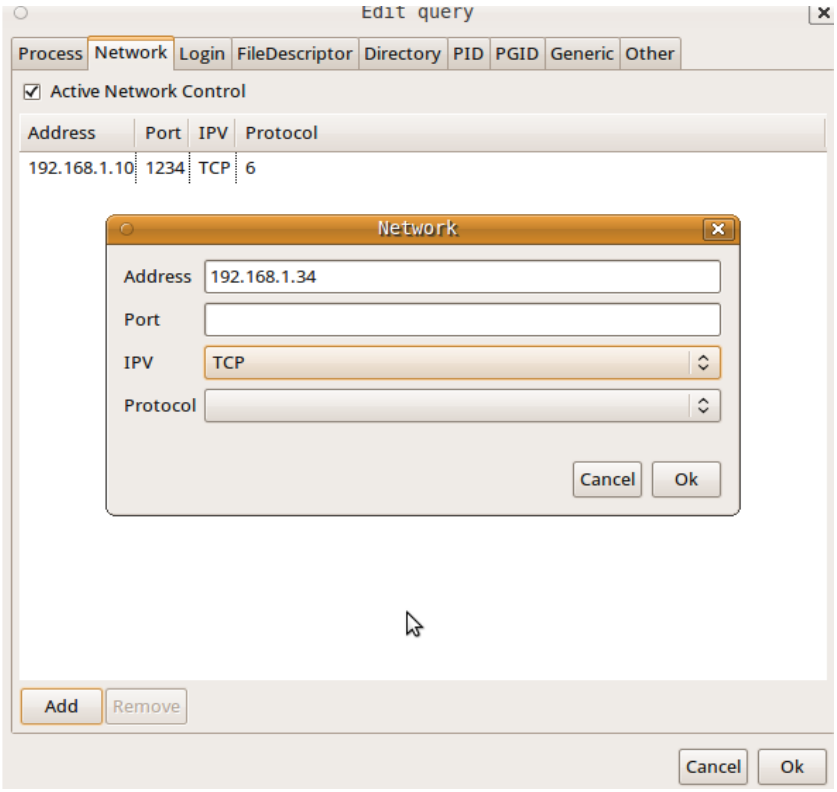
The Input dialog permits adding in the network's table an Internet address composed by Address, Port, IPV, Protocol. All these fields are optional.

An Internet address is specified in the form

[IPV][Protocol][Address][Port]

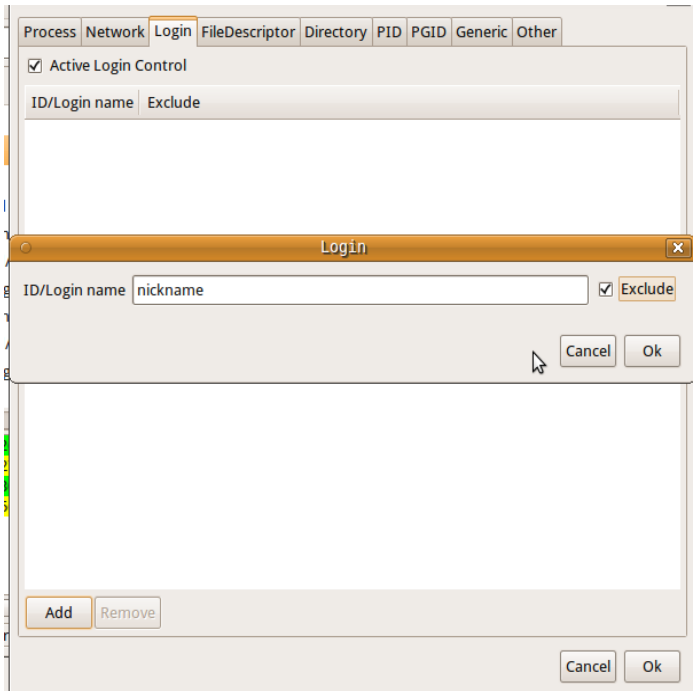
where:

- **IPV** specifies the IP version, IPv4 or Ipv6 that applies to the following address. '6' may be be specified only if the UNIX dialect supports IPv6. If neither '4' nor '6' is specified, the following address applies to all IP versions.
- **Protocol** is a protocol name - TCP, UDP
- **Address** could be an Internet host name. Unless a specific IP version is specified, open network files associated with host names of all versions will be selected. Or, a numeric Internet IPv4 address in dot form; or an IPv6 numeric address in colon form, enclosed in brackets, if the UNIX dialect supports IPv6. When an IP version is selected, only its numeric addresses may be specified.
- **Port** could be an /etc/services name - e.g., smtp - or a list of them. Otherwise it could be a port number, or a list of them.



3) Login (-u)

This option selects the listing of files for the user whose login names or user ID numbers are in the table. Multiple login names or user ID numbers are joined in a single ORed set before participating in AND option selection. If a login name or user ID is excluded, it becomes a negation - i.e., files of processes owned by the login name or user ID will never be listed. A negated login name or user ID selection is neither ANDed nor ORed with other selections; it is applied before all other selections and absolutely excludes the listing of the files of the process.



4) File Descriptor (-u)

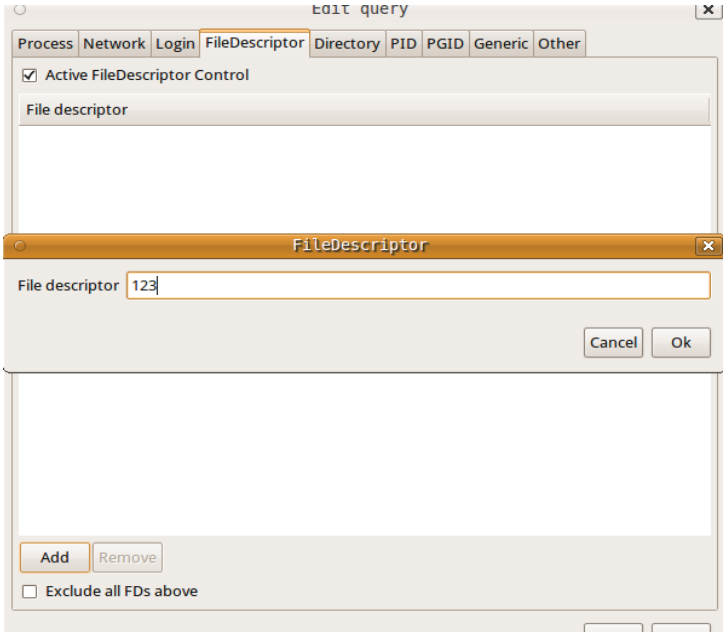
This option specifies a list of file descriptors (FDs) to exclude from or include in the output listing. The list is an exclusion list if the check button on the bottom is set (“Exclude all the FDs above”), otherwise it is an inclusion list. Mixed lists are not permitted.

A file descriptor number range may be in the set as long as neither member is empty, both members are numbers, and the ending member is larger than the starting one - e.g., ``0-7" or ``3-10". Ranges may be specified for exclusion, e.g., ``0-7" excludes all file descriptors 0 through 7 if the check button on the bottom is set.

Multiple file descriptor numbers are joined in a single ORed set before participating in AND option selection.

When there are exclusion and inclusion members in the set, lsof reports them as errors and exits with a non-zero return code.

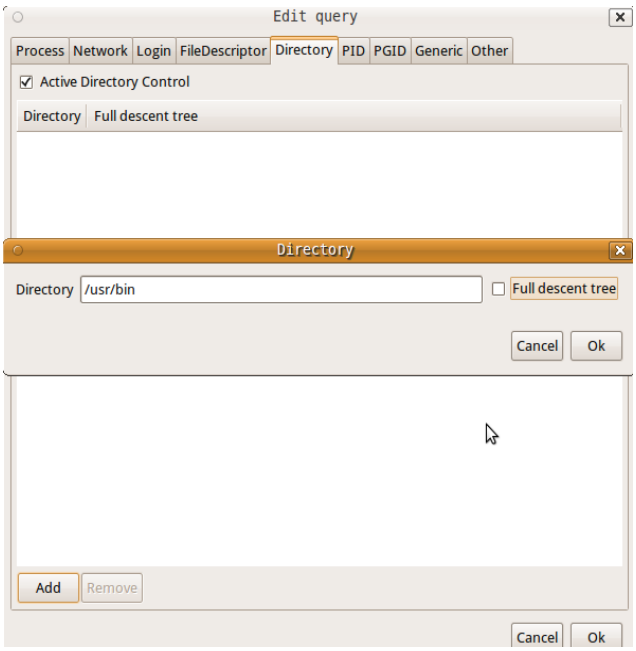
See the description of File Descriptor (FD) output values in the OUTPUT section for more information on file descriptor names on the lsof man page.



5) Directory (+d/+D)

This option causes lsof to search for all open instances of directories in the table and the files and directories they contain at their top level. If 'full-descent-tree' is enabled, this option descends the directory tree, rooted at directory.

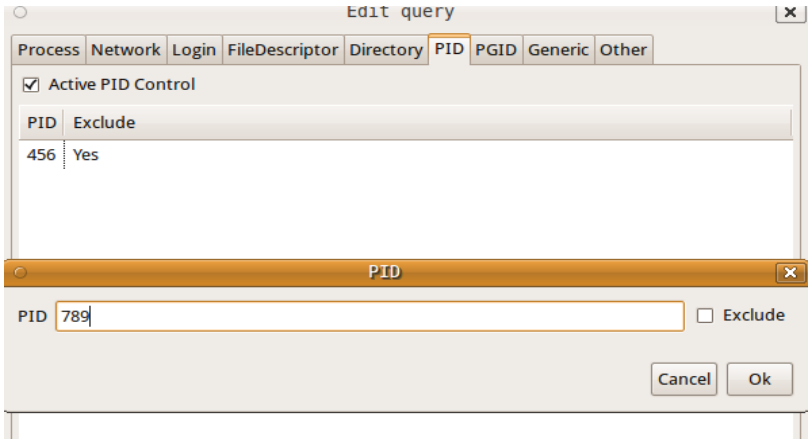
Note: the authority of the user of this option limits it to searching for files that the user has permission to examine with the system stat(2) function.



6) PID (-p)

This option excludes or selects the listing of files for the processes whose optional process IDentification (PID) numbers are in the table. Multiple process ID numbers are joined in a single ORed set before participating in AND option selection. However, PID exclusions are applied without ORing or ANDing and take effect before other selection criteria are applied.

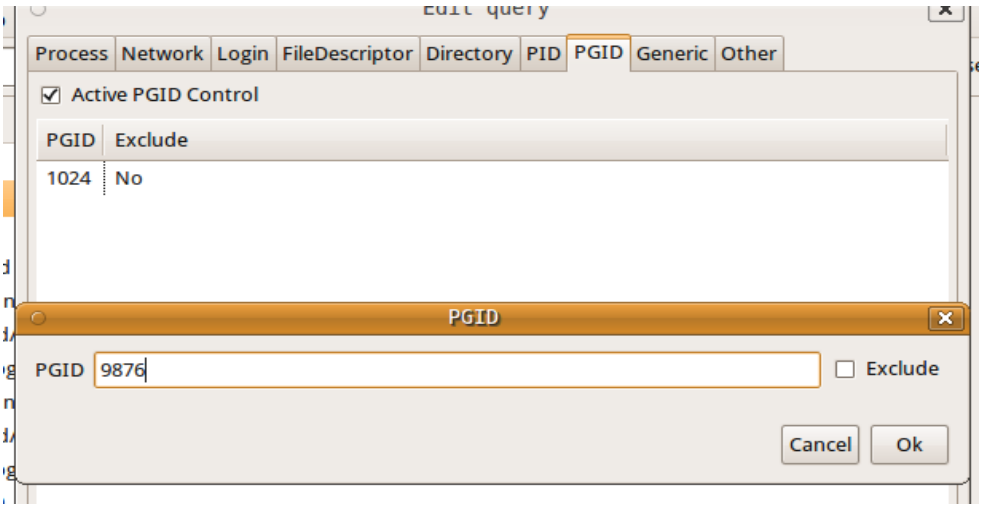
Input dialog accepts only numeric values.



7) PGID (-g)

This option excludes or selects the listing of files for the processes whose optional process group IDentification (PGID) numbers are in the table. Multiple PGID numbers are joined in a single ORed set before participating in AND option selection. However, PGID exclusions are applied without ORing or ANDing and take effect before other selection criteria are applied. This option also enables the output display of PGID numbers. When specified without a PGID set that's all it does.

Input dialog accepts only numeric values.



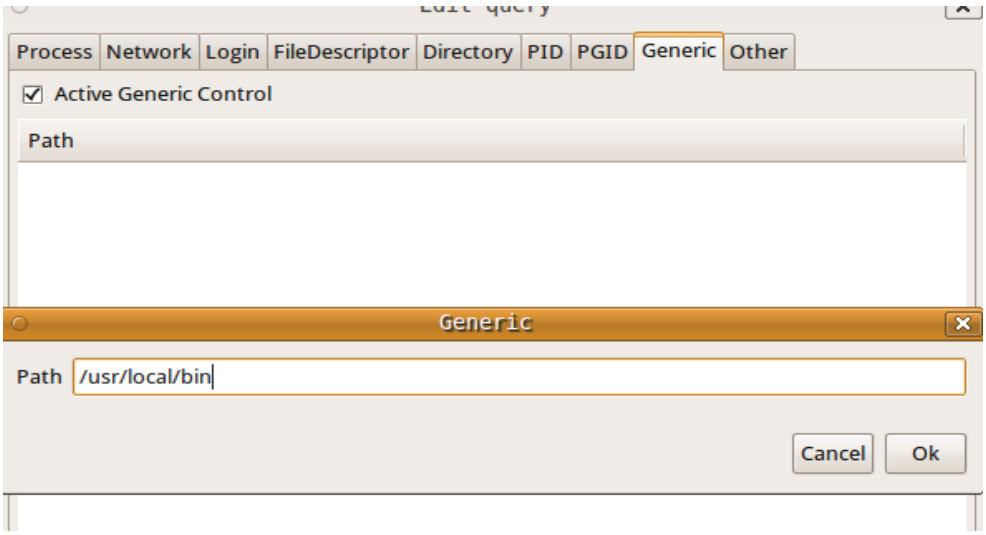
*8) Generic (*names*)*

These are path names of specific files to list. Symbolic links are resolved before use. The returned list depends on the choice of the list names:

- If a name is the mounted-on directory of a file system or the device of the file system, lsof will list all the files open on the file system. To be considered a file system, the name must match a mounted-on directory name in mount(8) output, or match the name of a block device associated with a mounted-on directory name.
- If a name is a path to a directory that is not the mounted-on directory name of a file system, it is treated just as a regular file is treated - i.e., it's listing is restricted to processes that have it open as a file or as a process-specific directory, such as the root or current working directory. To request that lsof look for open files inside a directory name, use the **Directory** options.
- If a name is the base name of a family of multiplexed files - e. g, AIX's /dev/pt[cs] - lsof will list all the associated multiplexed files on the device that are open - e.g., /dev/pt[cs]/1, /dev/pt[cs]/2, etc.
- If a name is a UNIX domain socket name, lsof will usually search for it by the characters of the name alone - exactly as it is specified and is recorded in the kernel socket structure. (See the next paragraph for an exception to that rule for Linux.) Specifying a relative path - e.g., ./file - in place of the file's absolute path - e.g., /tmp/file - won't work because lsof must match the characters you specify with what it finds in the kernel UNIX domain socket structures.
- If a name is a Linux UNIX domain socket name, in one case lsof is able to search for it by its device and inode number, allowing the name to be a relative path. The case requires that the absolute path -- i.e., one beginning with a slash ('/') be used by the process that created the socket, and hence be stored in the /proc/net/unix file; and it requires that lsof be able to obtain the device and node numbers of both the absolute path in /proc/net/unix and name via successful stat(2) system calls. When those conditions are met, lsof will be able to search for the UNIX domain socket when some path to it is is specified in name. Thus, for example, if the path is /dev/log, and an lsof search is initiated when the working directory is /dev, then name could be ./log.
- If a name is none of the above, lsof will list any open files whose device and inode match that of the specified path name.

- If you have also specified the -b option, the only names you may safely specify are file systems for which your mount table supplies alternate device numbers. See the AVOIDING KERNEL BLOCKS and ALTERNATE DEVICE NUMBERS sections for more information.

Multiple file names are joined in a single ORed set before participating in AND option selection.



9) Other

This tab has many options not including lists. They are:

- **Id or Login (-l):**

  Id number inhibits the conversion of user ID numbers to login names. It is also useful when login name lookup is working improperly or slowly.

- **Offset or size (-o/-s):**

  Offset option directs lsof to display file offset at all times. Note: on some UNIX dialects lsof can't obtain accurate or consistent file offset information from its kernel data sources, sometimes just for particular kinds of files (e.g., socket files.) Consult the lsof FAQ (The FAQ section gives its location.) for more information.

  Size directs lsof to display file size at all times. If the file does not have a size, nothing is displayed.

- **Dangerous kernel's functions (-S/-b):**

  Timeout specifies an optional time-out seconds value for kernel functions - lstat(2), readlink(2), and stat(2) - that might otherwise deadlock. The minimum is two; the default, fifteen; when no value is specified, the default is used.

  Avoid causes lsof to avoid kernel functions that might block - lstat(2), readlink(2), and stat(2).

- **Network control (-n/-N/-P/-U):**

  Show addresses in IP-format inhibits the conversion of network numbers to host names for network files. Inhibiting conversion may make lsof run faster. It is also useful when host name lookup is not working properly.

  NFS files selects the listing of NFS files.

  Show port-numbers inhibits the conversion of port numbers to port names for network files.

Inhibiting the conversion may make lsof run a little faster. It is also useful when port name lookup is not working properly.

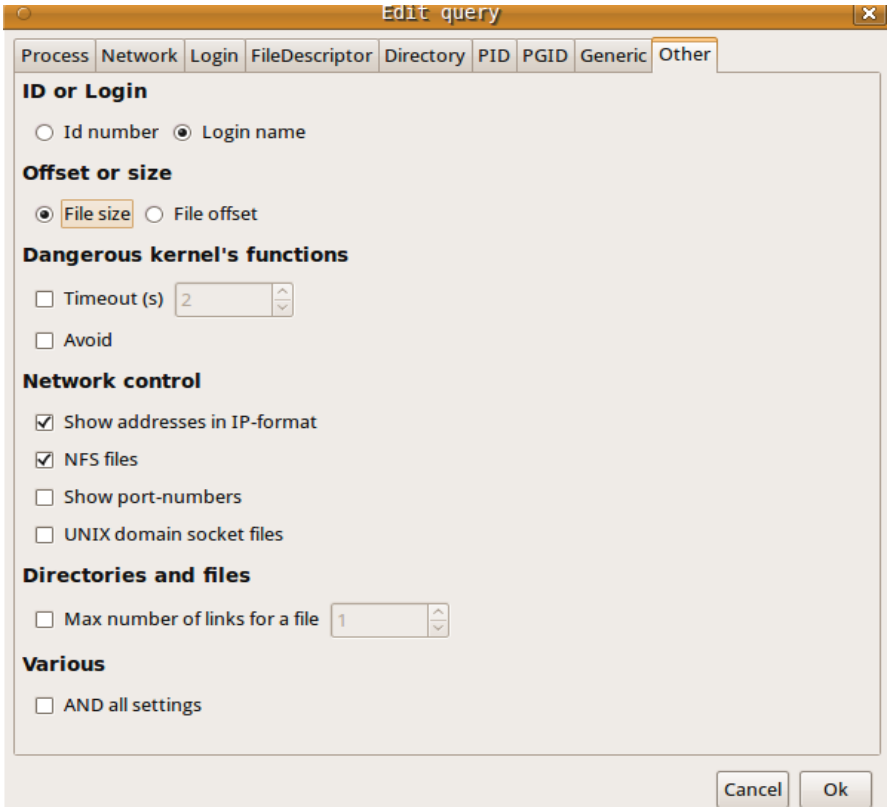
UNIX domain socket files selects the listing of UNIX domain socket files.

- **Directories and files (+L):**

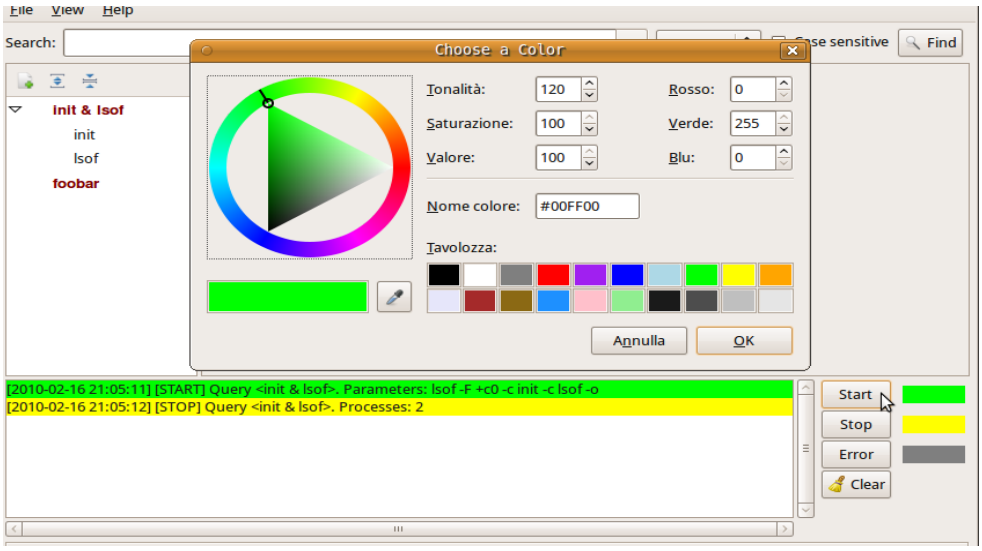
  Max number of links for a file enables the listing of file link counts, where they are available - e.g., they aren't available for sockets, or most FIFOs and pipes. Only files having a link count less than that number will be listed. With ``1" will select open files that have been unlinked.

- **Various (-a):**

  And causes list selection options to be ANDed. For example, specifying this option, *Unix domain socket files* and in the **File Descriptor** tab foo produces a listing of only UNIX socket files that belong to processes owned by user ``foo".



Logger



Autoscrolling logger displays:

1. The time the query is started, name of the query, lsof's parameters used for the execution. The start-log's color can be chosen by clicking on the **Start** button.
2. The time query is terminated, number of processes returned. The stop-log's color can be chosen by clicking on the **Stop** button.
3. The error returned by lsof. The error-log's color can be chosen by clicking on the **Error** button.

When the **Clear** button is clicked, the log text will be cancelled.

Status bar

When a query's name on the queries' tree is clicked, **status bar** displays the number of processes returned by the query's execution. When a process's name associated with a query's execution is clicked, **status bar** displays the number of rows of the process's table.