F-Check User Manual

What is F-Check ?

F-Check is an integrity checker program – it allows you to specify a set of objects (directories, files and boot sectors) which may be checked for any changes in content at a later date. Information about these objects are stored in a special F-Check database. F-Check is an "on-demand" program, meaning it must be started manually and does not operate in the background. F-Check is a tool intended for advanced users and works best when combined with the user's knowledge of the data contents of his system.

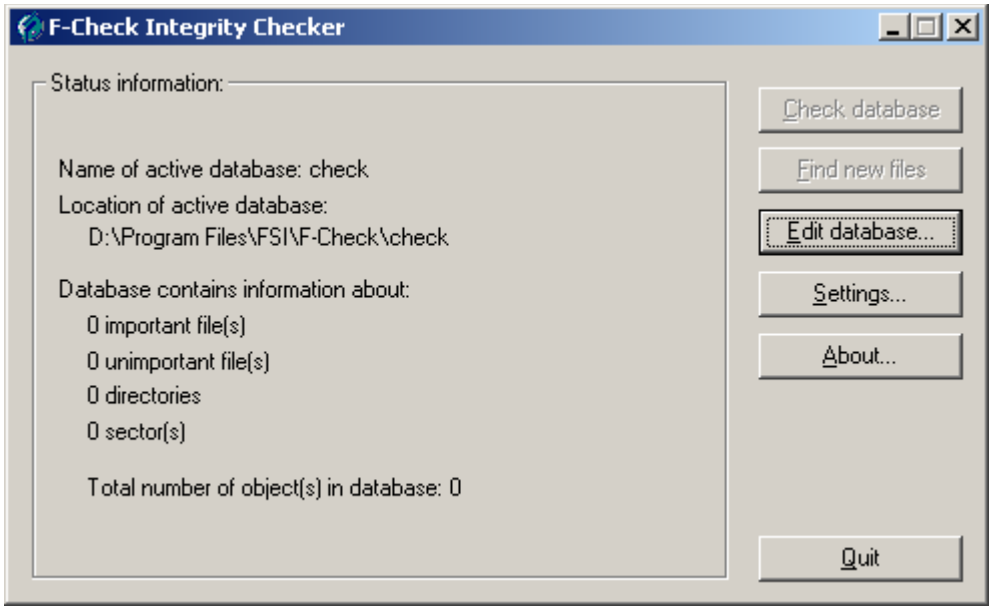
How is F-Check useful ?

Tracking changes in certain objects (directories, files or boot sectors) can be useful if a user encounters a virus that is unknown to the current anti-virus software installed on the machine. F-Check will give a warning when any of the objects specified in it's database have changed. This does not always mean that the object has been infected by a virus but nevertheless changes in certain files are suspicious. If F-Check finds an object which has changed it can try to fix (i.e. restore it to it's original state) it – thus indirectly disinfecting the file if it was indeed infected by a virus. However F-Check can not determine if a file is infected with a virus or not, only that it has changed. If there are any directories specified in the database then F-Check can also look for any new files in those directories - in some cases it is suspicious if new files appear in certain directories.

What to be careful of...

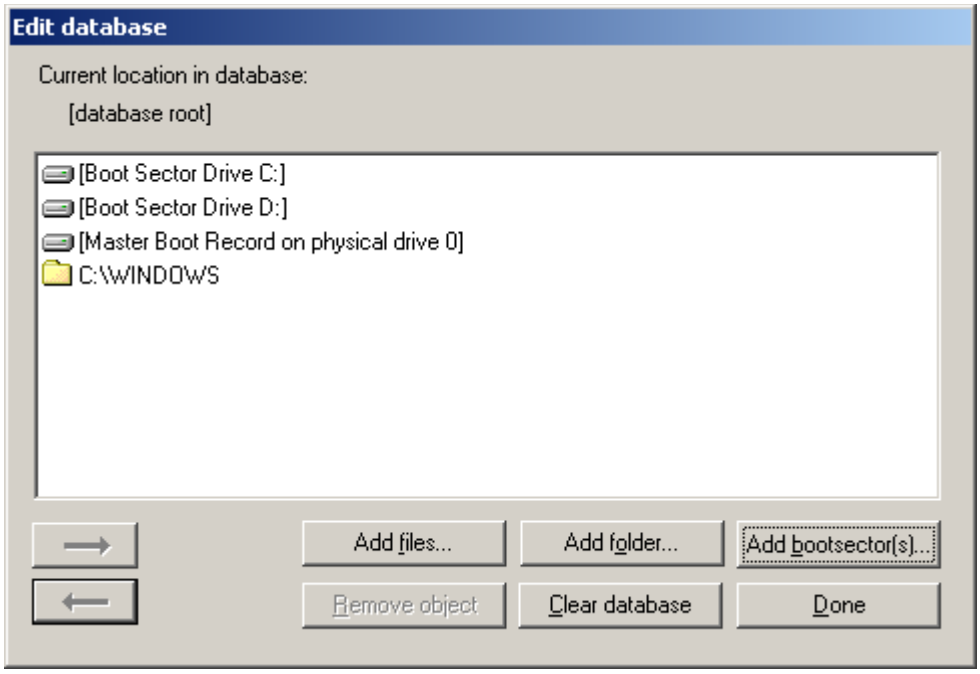
It is important to keep in mind that not all warnings F-Check reports because of changed objects are because of viruses or other security threats and with a poorly defined set of objects (files, directories or boot sectors) F-Check can generate many such warnings. In those cases F-Check should not be told to try to fix the object in question. Special care should be taken when dealing with boot sectors or MBRs that have changed, although F-Check includes tools which will let the user undo any damage in most cases. When a new operating system is installed or the hard drive is repartioned it is normal for these objects to change and asking F-Check to fix them might result in the system not rebooting normally.

The main F-Check dialog



When F-Check is started the programs main dialog will appear. This dialog displays information about which database is currently selected and what that database contains. The dialog also displays the programs main menu which consists of the buttons on the right.

Edit database



The "Edit database..." option in the main menu leads to this dialog where you can add items (files, directories and boot sectors) to the current database. This dialog will also allow you to travel into directories which have been added to the database. To help keep track of where you are in the database your current position is displayed at the top of the dialog (see "Current location in database:"). Below is the list of objects that have been added to the database (relative to your current location in the database). You can enter a directory by selecting it and pressing the blue right-arrow button. In the same way you can exit a directory by pressing the blue left-arrow button.

"***Add files...***" : Allows you to add individual files to the database. Note that this operation can only be performed when you are located in the database root.

"***Add folder...***" : Allows you to add whole folders (directories) to the database. The "Include subfolders" option can be unchecked if you don't want to add subfolders of the selected directory to the database also. Note that this operation can be time consuming for large folders.

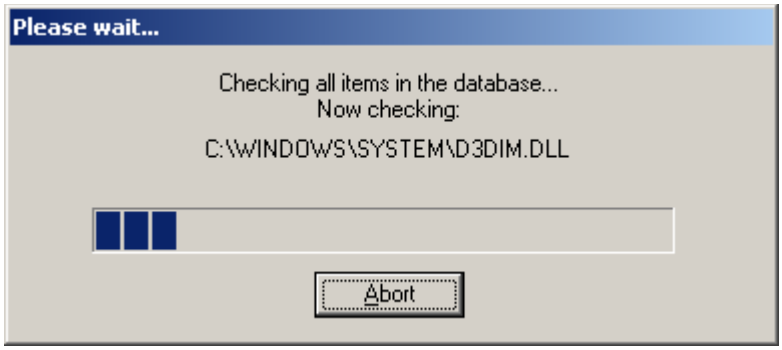
"***Add bootsector(s)...***" : Allows you to add all bootsectors and MBRs (master boot records) to the database. If you do not wish to include all these sectors in the database they can be individually removed later.

"***Remove object***" : This option removes the item which is currently selected in the list. If you have selected a directory all it's subdirectories will also be removed from the database.

"***Clear database***" : This option clears everything from the database leaving it completely empty.

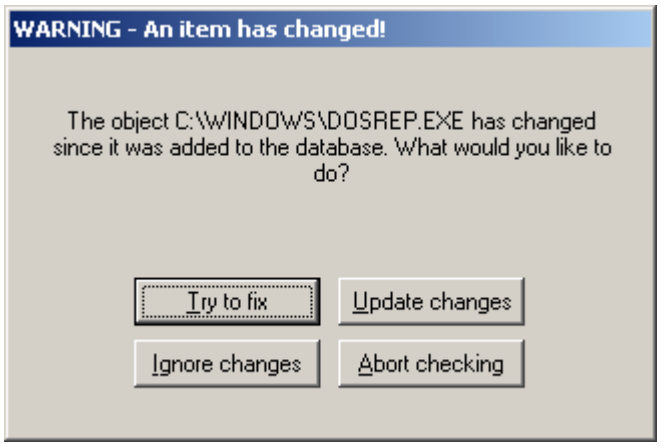
"***Done***" : Saves changes to the checklist and returns you to the main F-Check dialog.

Check database



When the "Check database" button is pressed F-Check will start checking all object in the database for changes. Meanwhile you can see which object is currently being checked and what the current progress is. When the operation completes you are shown it's results. The "***Abort***" button can be pressed at any time to cancel the operation.

When F-Check find an object that has changed you will see a dialog like this one:



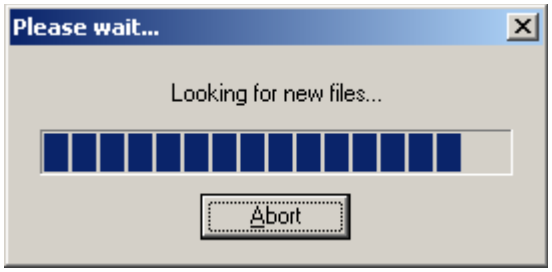
"***Try to fix"*** : Tries to restore the object to it's original state (the state it was in when it was added to the database). If the object has been infected by a virus it will in many cases disinfect it. However avoid this option if you do not find it suspicious that the object has changed (for example if you have upgraded the software this object is a part of since you added it to the database).

"***Update changes"*** : Updates the information about the object in the database with it's current state. Use this option if you find nothing suspicious about the object having changed – you will not receive more warnings about this object until it changes again.

"***Ignore changes"*** : Ignore the changes to the object. If the object is still different from it's original state the next time you run the "Check database" operation you will get the same warning again.

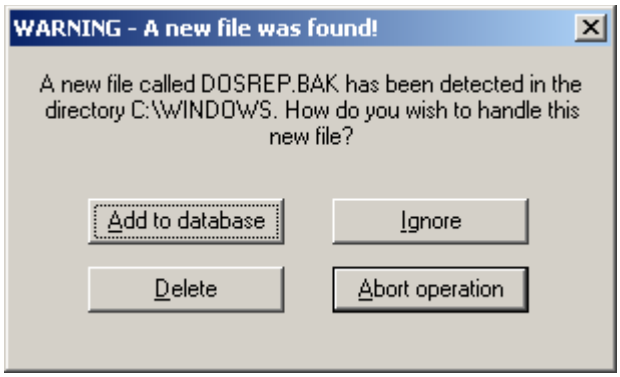
"***Abort checking***" : Aborts the checking operation. May be desireable if you are getting an excessive number of warnings and would rather output the results to a logfile.

Find new files



This operation searches for new files in all folders (directories) that are in the current database. You can abort the operation at any time by pressing the "***Abort***" button. Once the operation fininishes you will be shown it's results.

If a new file is found you will see the following dialog:



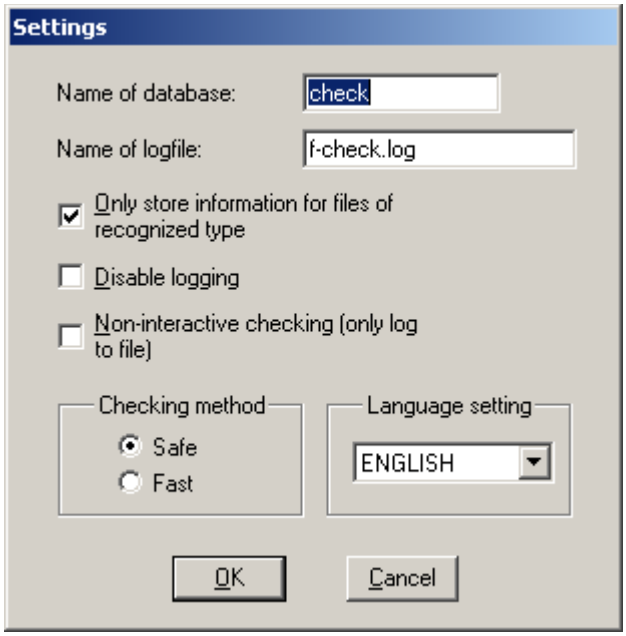
"***Add to database"*** : Adds the new file to the database. You will not see this warning again for this file the next time you run "Find new files" as it will no longer be regarded as new. Use this option if you do not find this new file suspicious.

"***Ignore***" : Ignores this new file. You will see this warning again for this file the next time you run "Find new files" as the it will still be regarded as new.

"***Delete***" : Deletes this new file permanently. Before selecting this option please be sure this is an unwanted file.

"***Abort operation"*** : Aborts the "Find new files" operation. May be desireable if you are getting an excessive number of warnings and would rather output the results to a logfile.

Settings



This dialog allows you to change the current F-Check settings.

"***Name of database***" : Name of the current database. Should ideally be one word without any special characters.

"***Name of logfile***" : Name of the logfile, relative to the main F-Check directory.

"***Only store information for files of recognized type***" :
If this option is checked F-Check will only check for changes in files that are of a known type, otherwise it will check for changes in all files in the database.

Known file types in F-Check currently consist of 16-bit and 32-bit executables.

"***Disable logging***" : If this option is checked then no results will be written to the logfile.

"***Non-interactive checking***" : If this option is checked then the "Check database" and "Find new files" operations will not display individual warnings for every change they encounter – instead they will only write them to the logfile. May be desireable if you are getting an excessive number of warnings and would rather output the results to a logfile rather then handle each warning individually.

"***Checking method*** " : The "***Fast***" method only checks the parts of individual objects that are most likely to have been changed if a virus has infected them while "***Safe***" checks the whole object.

"***Language settings***" : Let's you select the language of your choice provided you have the appropriate language files.