

ACCESSDATA SUPPLEMENTAL APPENDIX

Using File Filter Manager in FTK 1

One of the most powerful features of AccessData® Forensic Toolkit® (FTK®) is the database upon which it is built. When FTK analyzes a hard drive, it creates a database entry for every item it finds (files, directories, OLE objects, email, boot records, file slack, deleted files, etc.). After FTK has entered the file data into the database, you can easily sort and organize the information.

As a computer forensics examiner, you often have to wade through enormous amounts of data to find small fragments of evidence. It is not uncommon for a single hard drive to contain 250,000-plus files. If a case contains 10-20 hard drives, you might have to sort and organize millions of files and emails. A database is perfectly designed to store, sort, and filter huge volumes of information and is, therefore, ideal as a base for computer forensics investigations.

Once file data has been loaded into the database, you must have a method of sorting and filtering the database to retrieve only the information needed. The File Filter Manager is designed specifically for this purpose.

This appendix introduces the File Filter Manager and provides information to help you manage filters in FTK 1.

- “Overview” on page 2
- “Single Criteria Filters” on page 3
- “Multiple Criteria Filters” on page 5
- “Creating a Default Filter” on page 7
- “Choosing a Filter” on page 7
- “Ignoring Data” on page 8
- “Applying Filters in the Overview Tab” on page 8
- “Applying Filters in the Search Tab” on page 8

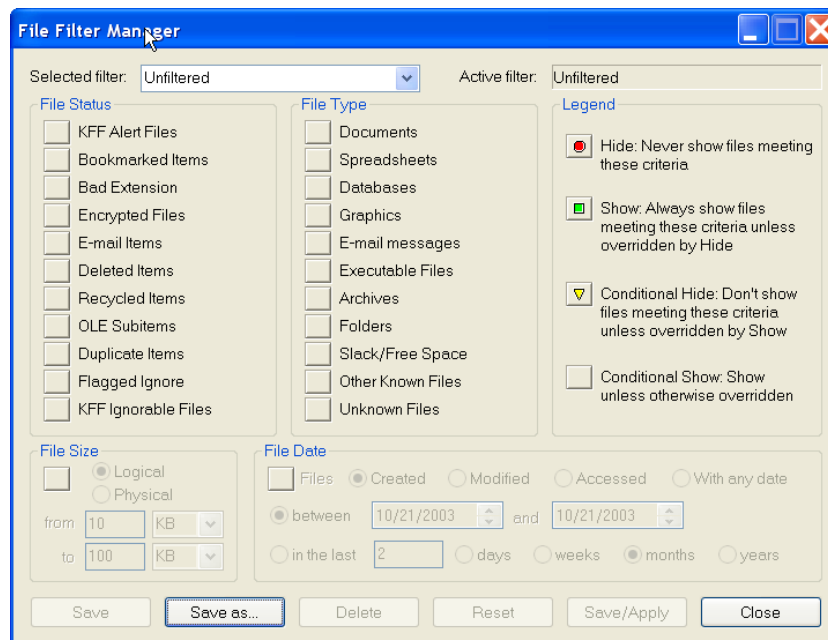
OVERVIEW

You can open the File Filter Manager by clicking **View > File Filter Manager**.

You can also click the File Filter Manager button on the toolbar  .

The File Filter Manager filters information based upon four primary criteria:

- File Status
- File Type
- File Size
- File Date



The File Filter Manager allows you to either Hide or Show various file items based upon the file data criteria information. The File Filter Manager has four settings (listed in order of priority):

Setting	Function
Hide	Never show files meeting these criteria.
Show	Always show files meeting these criteria unless overridden by Hide.
Conditional Hide	Don't show files meeting these criteria unless overridden by Show.
Conditional Show	Show unless otherwise overridden.

Because a single record item can be affected by several filter criteria simultaneously, it is helpful to think of the four filtering conditions as an embedded “if” statement.

if(one of the file criteria = Hide), hide the file item and break; else go to next line

if(one of the file criteria = Show), show the file item and break; else go to next line

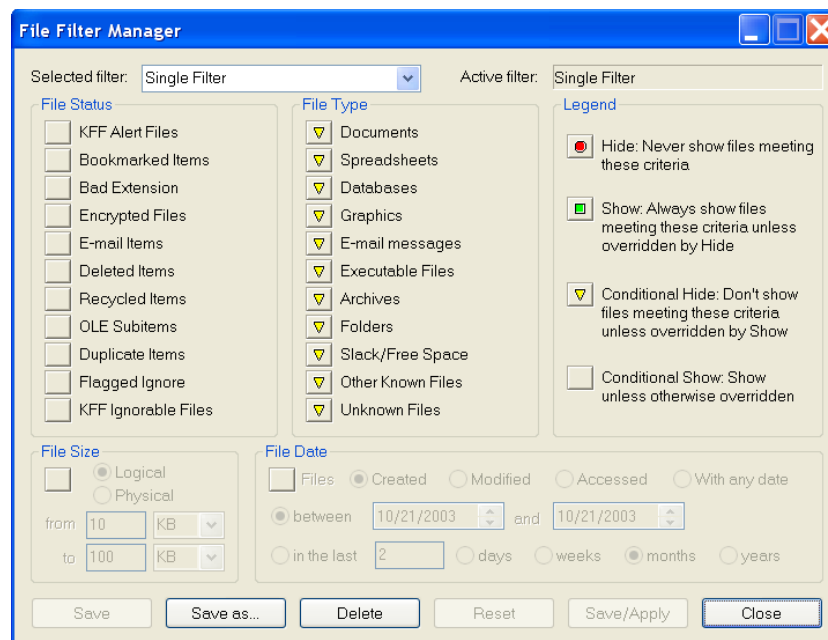
if(one of the file criteria = Conditional Hide), hide the file item and break; else

if we get to this point, show the file.

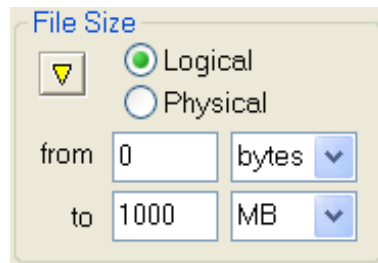
SINGLE CRITERIA FILTERS

A single criteria filter is the easiest type of filter to build. For example, you can use a single criteria filter to find all the spreadsheets in the case or perhaps all the files that had some kind of activity during a specific period of time.

The easiest way to build a single criteria filter is to start by setting every File Type option to Conditional Hide, as shown in the following graphic.

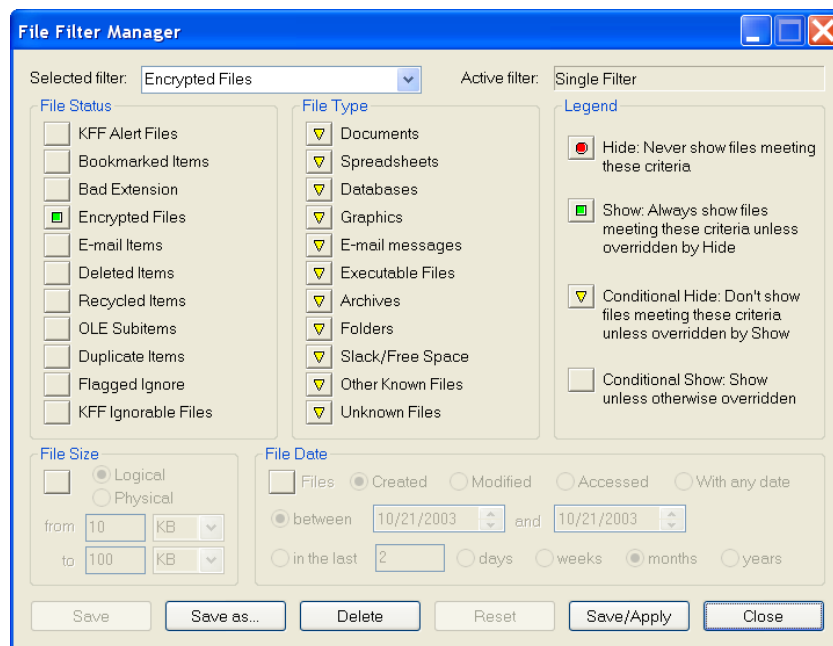


Alternatively, you can start building a single criteria filter by setting File Size to Conditional Hide. In the **from** box, enter 0 bytes and in the **to** box, enter an enormous value like 1000 MB.



Your objective is to create a filter that filters out all the files in the database.

After you have accomplished this, you are ready to set the items you want viewed to Show. For example, if you want to see all the encrypted files in a given directory, set Encrypted Files to Show and set all the File Type options to Conditional Hide, as shown below:

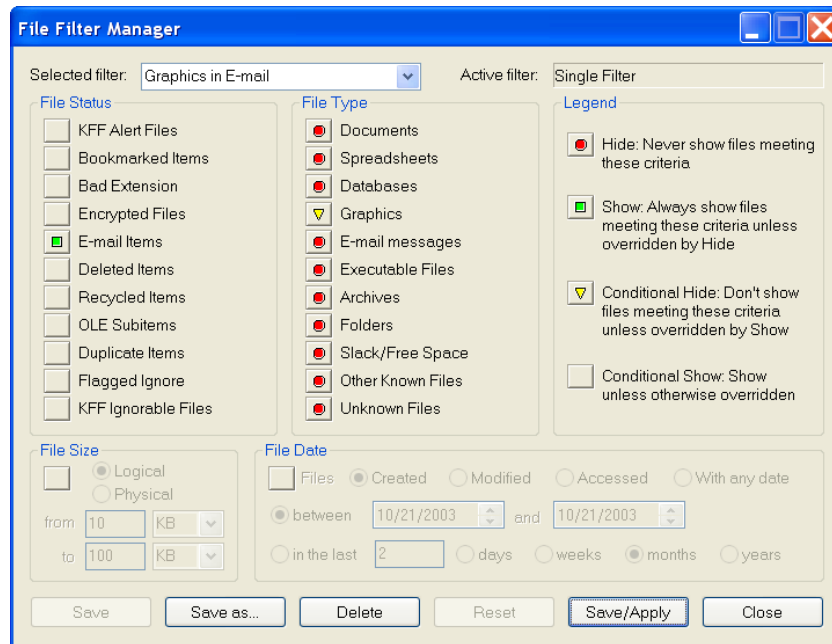


Then you can go to the directory and apply the filter.

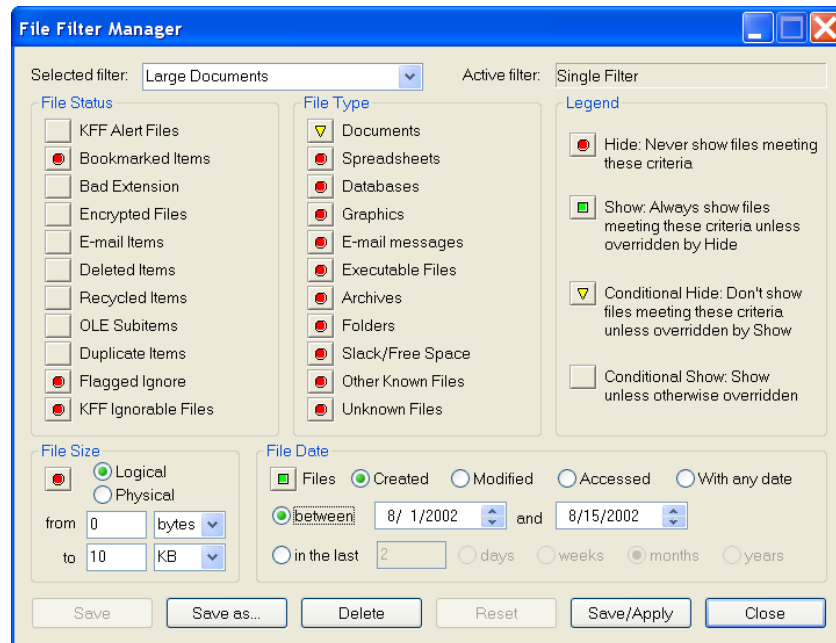
MULTIPLE CRITERIA FILTERS

Multiple criteria filters are more complicated because they require the use of all three conditions: Hide, Show, and Conditional Hide.

The following graphic shows how to create a filter that displays all graphics files that are in email.

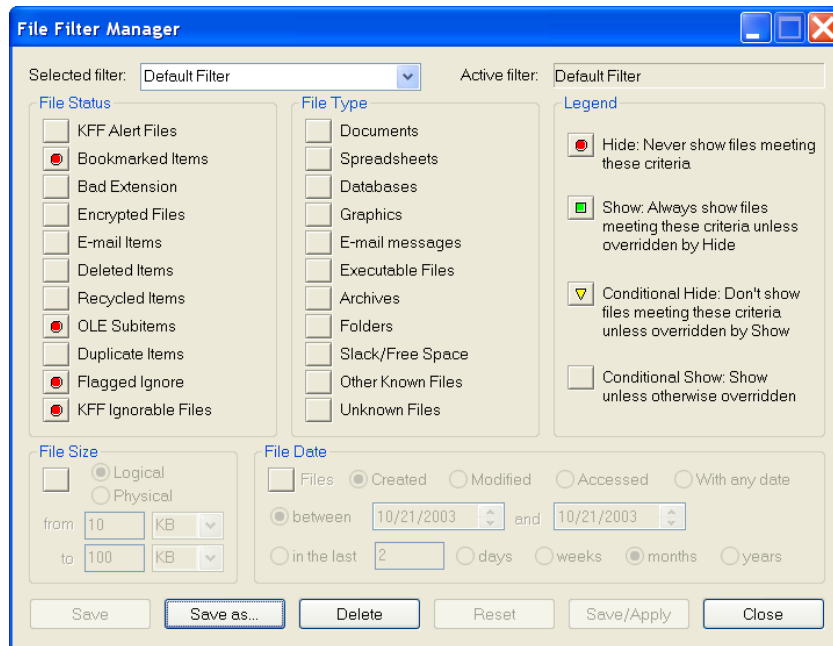


Multiple criteria filters can be as easy or as complicated as you need. For example, a complex filter could be one that displays all documents with a creation date between 8/1/02 and 8/15/02, are larger than 10 KB, and have not already been flagged as ignored, bookmarked, or part of the KFF database. The following graphic shows what this filter would look like.



CREATING A DEFAULT FILTER

During everyday operation, many investigators create a default filter that is usually set. This filter automatically filters out files that have already been bookmarked or flagged as ignored, are OLE streams, or are part of the KFF database. Many times this filter is called (for lack of a better name) Default Filter. The following graphic shows a default filter.

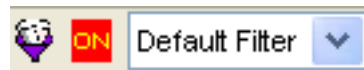


CHOOSING A FILTER

FTK includes several basic filters, but you can quickly expand this list by creating your own filters.

Filters are global. In other words, after a filter is created, it is available for use in all the cases that run on that computer.

The active filter is displayed in the text box next to the File Filter Manager button, as shown below.



The red ON sign indicates that a filter is active. The ON sign changes to OFF when Unfiltered is chosen.

IGNORING DATA

The ability to ignore data is one of FTK's most helpful features. After a file has been reviewed and determined not to contain evidence, you need to be able to flag the file Ignore so that you don't accidentally encounter the file again. The File Filter Manager allows FTK to filter out files that have been flagged Ignore.

To ignore a file, highlight or checkmark the file. Then select either **Tools > Ignore Highlighted Items** or **Tools > Ignore Checked Items**. Ignore Item is also available from the quick menu when you right-click a selected file.

Hidden items are then removed from the case for further analysis by enacting a filter that includes the setting to hide Flagged Ignore files.

APPLYING FILTERS IN THE OVERVIEW TAB

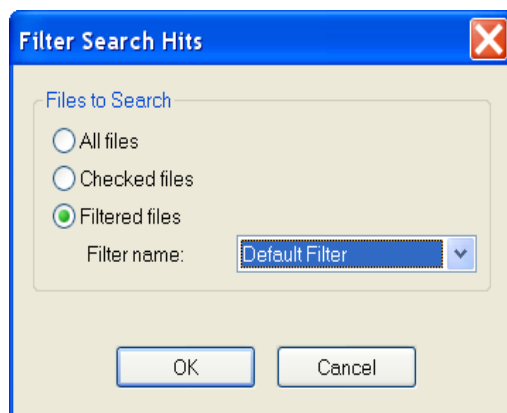
In the Overview tab, the summary results can be filtered by selecting the Filtered button, as shown below.



Unfiltered and Filtered reflect only in the Overview tab.

APPLYING FILTERS IN THE SEARCH TAB

In the Search tab, filters are applied to the search results during the searching process. After entering your search terms, FTK displays the following menu:



By selecting **Filtered files** and choosing a filter, your search results pass through the filter before they are reported.