

# ACCESSDATA SUPPLEMENTAL APPENDIX

## Using Filters in FTK 2

One of the most powerful features of AccessData® Forensic Toolkit® 2 (FTK®2) is the Oracle\* database upon which it is built. When FTK 2 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 2 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+ files. If a case contains 10 to 20 hard drives, you might have to sort and organize millions of files and email. 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.

After 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. Creating and using filters is a perfect solution.

This appendix reviews the following concepts:

- *Rule-Based Filtering – The Concept* on page 1
- *Global and Tab Filters* on page 2
- *Defining or Editing a Filter* on page 4
- *Adding and Removing Rules* on page 8
- *Live Preview* on page 10
- *Nesting Filters* on page 10
- *Exporting Filters* on page 12
- *Importing Filters* on page 12

### RULE-BASED FILTERING – THE CONCEPT

In contrast to the graphical filtering utility in FTK 1.x, filters in FTK 2 are “rule based.” This means that you define a filter by specifying any number of rules. Each rule consists of three parts: the Property, the Operator, and the Criteria. A filter consists of any number of rules, and they are applied to the dataset cumulatively or independently (Match Any or Match All).

## Properties

Properties are the fields stored in the Oracle database. Some examples of properties are Created Date, Modified Date, Accessed Date, Logical Size, Name (File Name), Path, Owner SID, various file system flags, File Type, File Category, and even fields from email such as To, From, Date, Subject, etc. Anything that FTK 2 stores in the Oracle database about an object could conceivably be a property to filter on.

## Operators

Operators are conditions set after choosing a property. The available operators will vary depending on the property chosen. For example, if File Type is chosen as a property, then the available operators are Is, Is Not, Attribute Exists, and Attribute Does Not Exist. If Logical Size is selected as a property, then the available operators are Is, Is Not, Is Less Than, Is Not Less Than, Is Greater Than, Is Not Greater Than, etc.

---

**Note:** Some operators exist out of necessity but are rarely used. For example, the Attribute Exists and Attribute Does Not Exist operators are asking whether the database stores this property regardless of what is in that property.

---

## Criteria

Criteria are values used to further define an operator. For example, if Logical Size is chosen for the Property and Is Greater Than is chosen for the operator, the criteria might be something like 10 MB. Some criteria are chosen from FTK 2 generated lists such as File Type. Others are user text fields such as Owner SID or a specific filename.

Once defined, filters are saved and then applied as needed in one of two ways—global filters or tab filters.

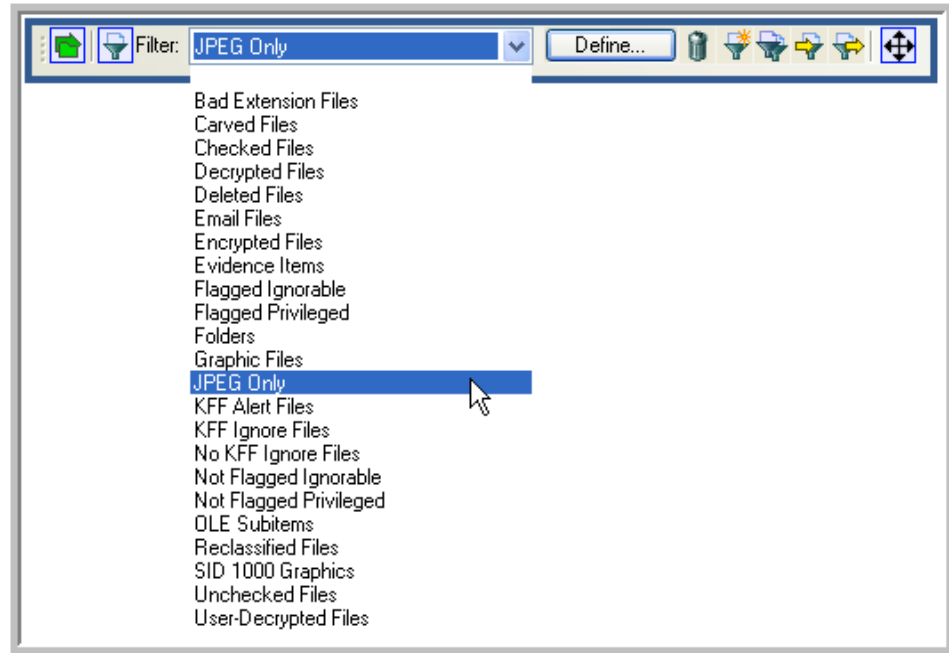
## GLOBAL AND TAB FILTERS

Filters in the FTK 2 interface can be applied globally or as tab filters. Global filters are in effect across all tabs in the FTK 2 interface, while Tab filters apply only to a specific tab. For example, a user might want to apply a global filter across all tabs which is designed to exclude any KFF Ignorable files. In contrast, a user might want to apply a tab filter to a specific tab limiting the view to files with a specific Owner SID.

By default, a tab filter is applied to the Graphics and Email tabs limiting the view to graphics and email items, respectively.

## Applying a Predefined Filter As a Global Filter

FTK 2 has a number of predefined filters. To apply any of these filters or a filter you have created, select it from the pull-down menu on the Filter toolbar.



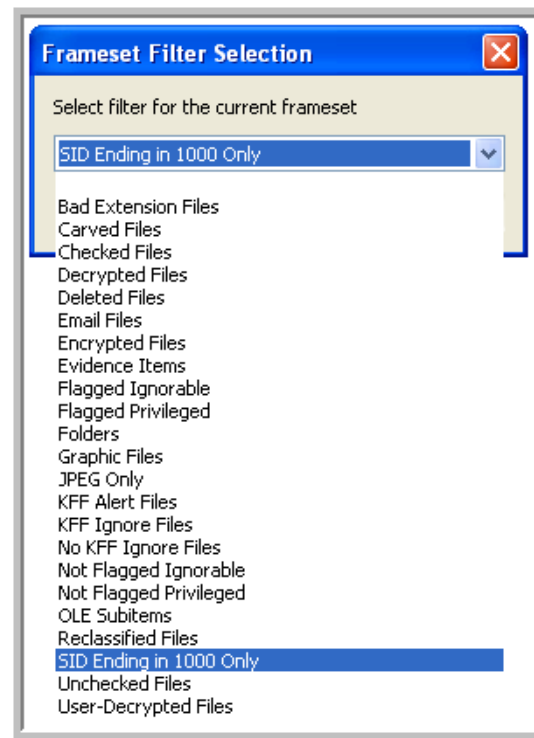
When selected, this filter is on and will be used on every tab (Global). Selecting the  icon toggle this filter on and off.

## Applying a Predefined filter As a Tab Filter

To apply a defined filter as a tab filter:

- 1 Navigate to the tab you want to filter.
- 2 Click **Filter > Tab Filter**.

- 3 Select a filter from the drop-down list.




- 4 Click **OK**.


The selected filter is now applied to the active tab. The active tab filter is indicated in the bottom center of the FTK 2 Interface.

## DEFINING OR EDITING A FILTER

There are a number of ways to define and edit filters:

- To create a new filter, click the **Create New Filter** icon  on the Filter toolbar or click **Filter > New**. This opens a temporary window to design your new filter in.
- To create a new filter, click **Define** on the Filter toolbar with no filter selected.
- To edit an existing filter, apply that filter from the Filter toolbar, then click **Define**.

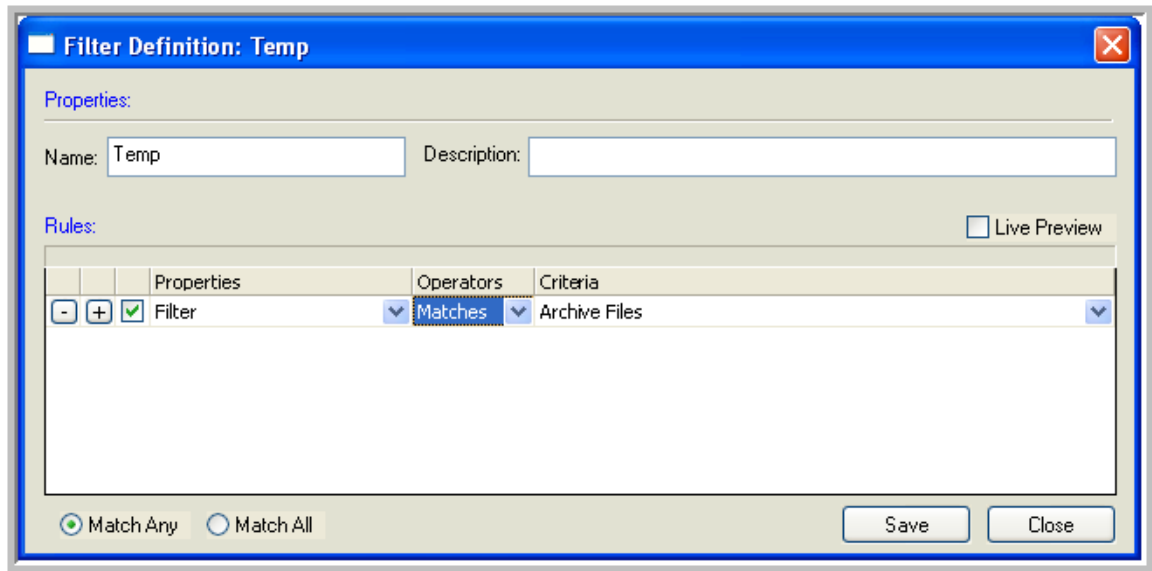
---

**Note:** Some default filters are read-only. You cannot edit a read-only filter. Instead, you can apply that filter, then click the Copy Filter  icon or click **Filter > Duplicate** to duplicate that filter as a non-read-only filter.

---

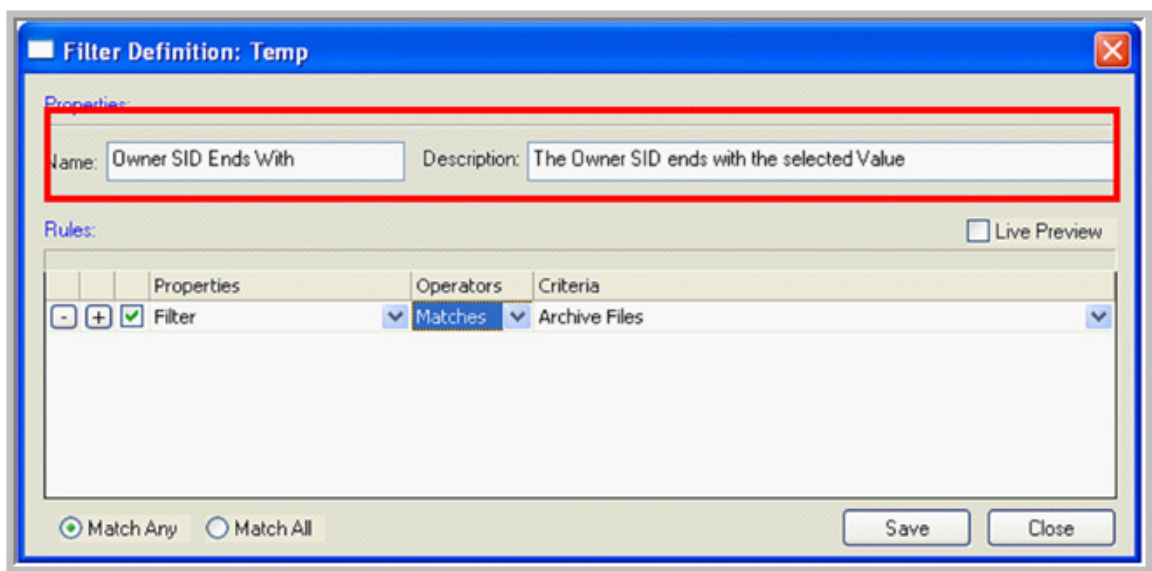
The following example illustrates a simple filter template with a single rule.

**Note:** The default selection for a rule is the first item in each drop-down list (Properties, Operator, Criteria).



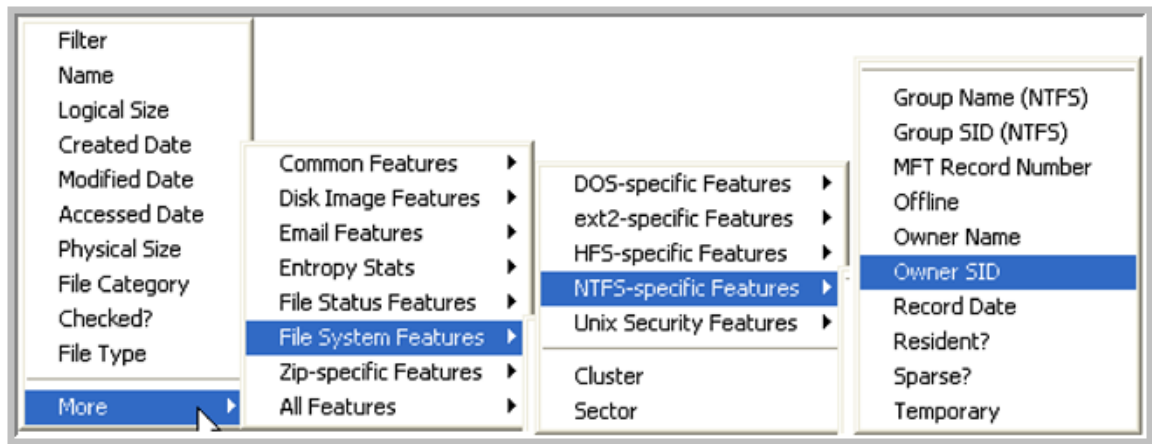
### 1 Name this filter.

This will be the name that appears in any available filter lists. In this example, a filter will be created that will allow the analyst to filter files based on a particular Owner SID (Security Identifier). The name chosen is "Owner SID Ends With" and the optional description is "The Owner SID ends with the selected Value." These two text fields can contain any string.



## 2 Select the rule properties.

The list of available properties is extensive. The most common values are listed at the top of the pull-down window. Click **More** to display the full list divided into sections by type.

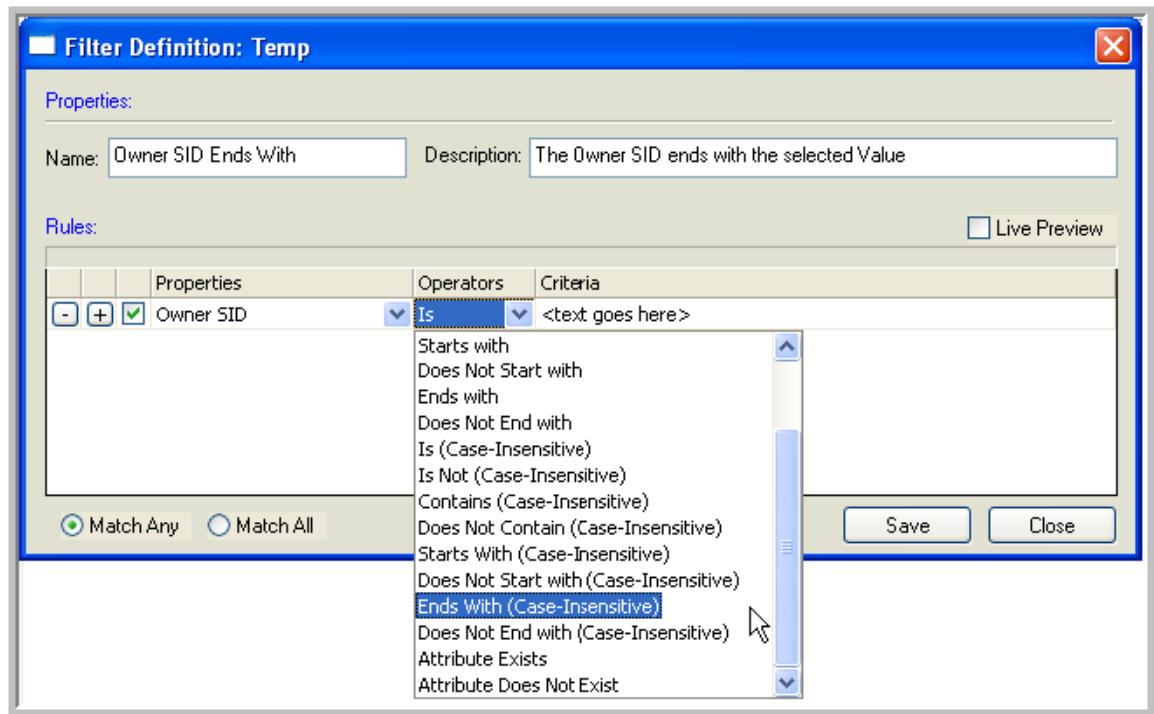


**Note:** Click **All Features** to open an alphabetical listing of every available property. Typically, only a fraction of the available properties are ever used. Nevertheless, they exist in the database and so they are available should the need arise. Users should make sure they understand the specific property before using it.

### 3 Select an operator from the available list.

In this case, the Ends With (Case-Insensitive) operator is selected. This means that the criteria is not case sensitive.

**Note:** Some operators are “negative” filters. Examples are **Is Not**, **Does Not Start With**, **Does Not Exist**, etc. This feature can be very powerful when used correctly.

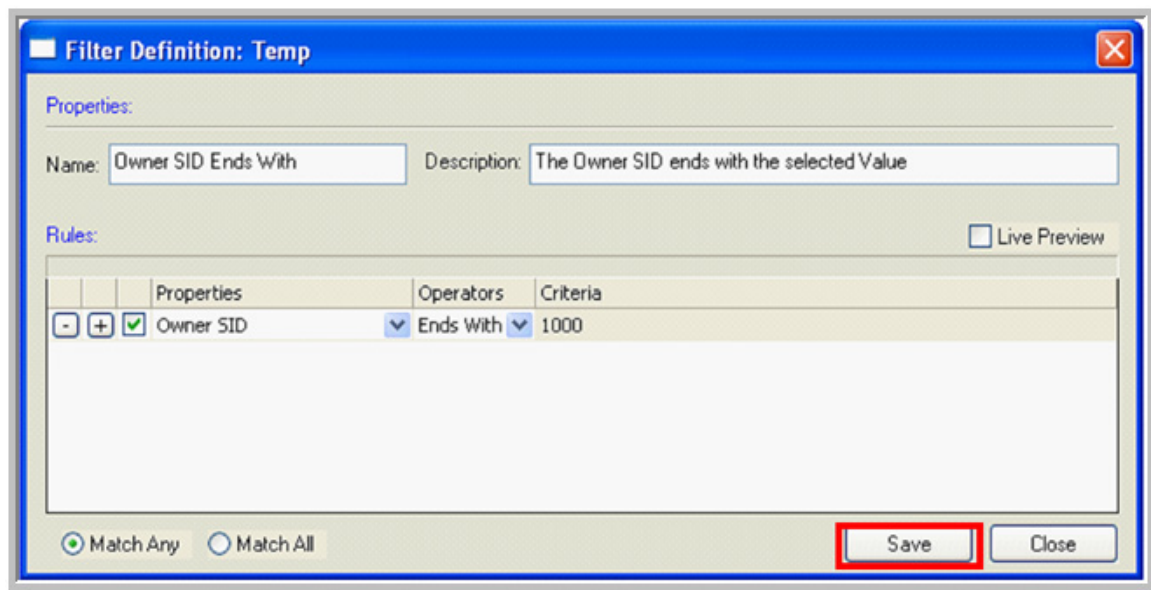


### 4 Define the criteria.

This will be in one of three forms:

- User-definable text field, such as in this example
- Pull-down list, such as file types
- Nothing, when it is not necessary to complete the rule

5 Click the **Save** button to save the filter.



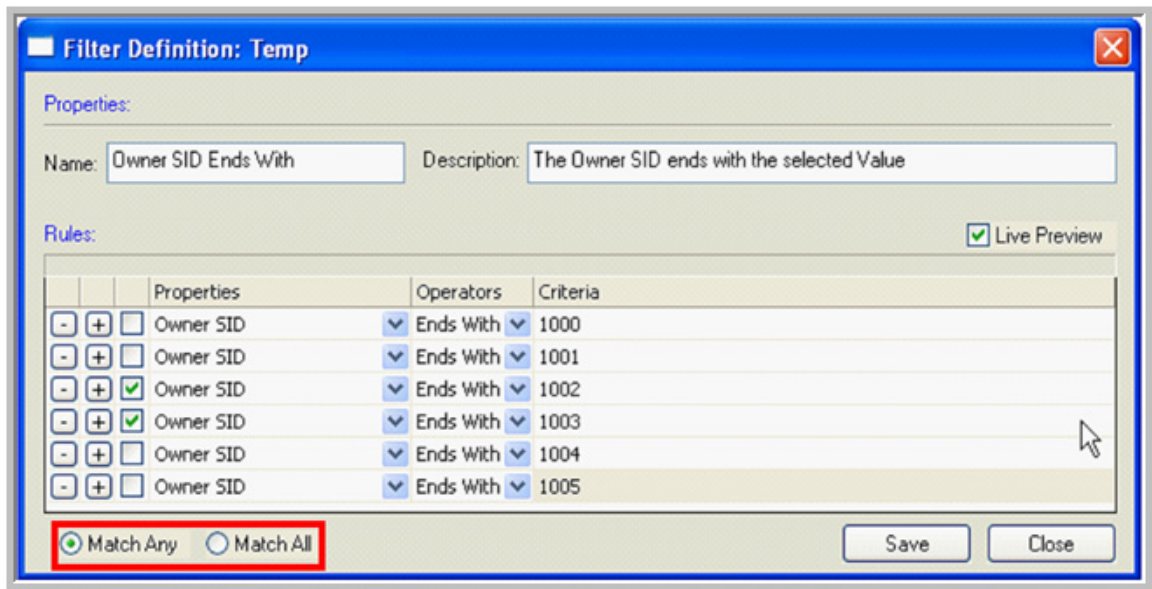
## ADDING AND REMOVING RULES

Additional rules can be added to a filter simply by clicking the Plus icon (+) next to any rule. This will insert a rule below that existing rule. There is no limit to the number of rules that can be applied; however, each rule requires additional processing time to query the results.

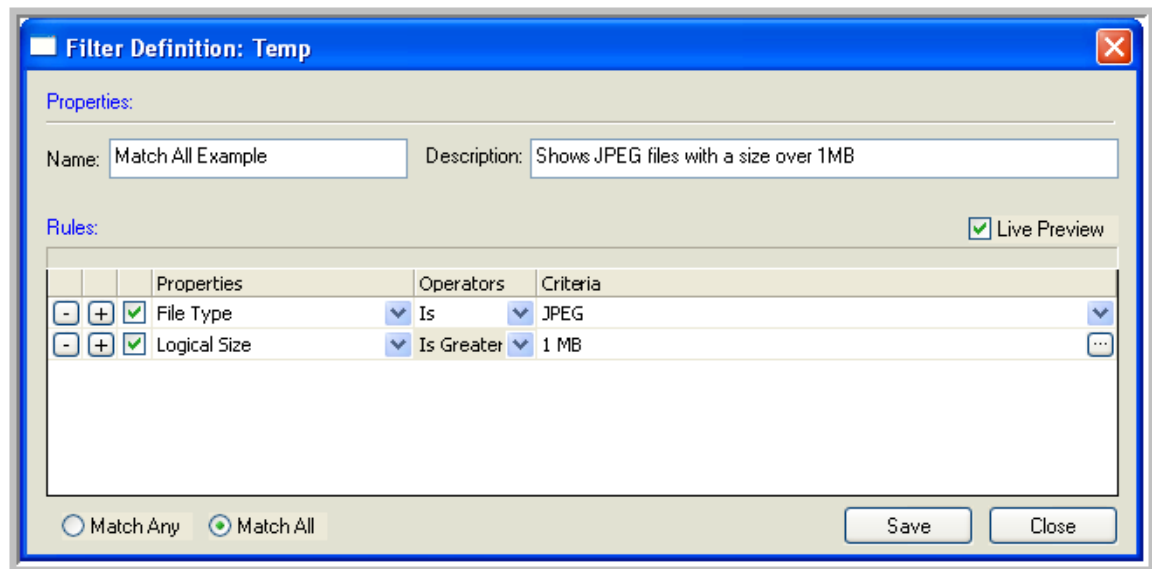
Rules can be deleted by clicking the Minus icon (-) next to a rule.

Each rule can be suspended or made active simply by selecting the check box next to the rule.

In this example, several rules have been defined. Each is asking for files with a specific Owner SID. Out of the five rules defined, only two are active. Additionally, the Match Any option at the bottom is selected, allowing objects that meet *any* of these rules to remain. Alternately, if the Match All option were used, then no files would remain as a file can't end with two different strings.



In this example, a filter has been created that requires the Match All option. This filter requires that the file type be JPEG only and that the Logical Size be greater than 1 MB. Selecting the Match Any option would allow both JPEG files as well as any other file with a logical size greater than 1 MB to remain.



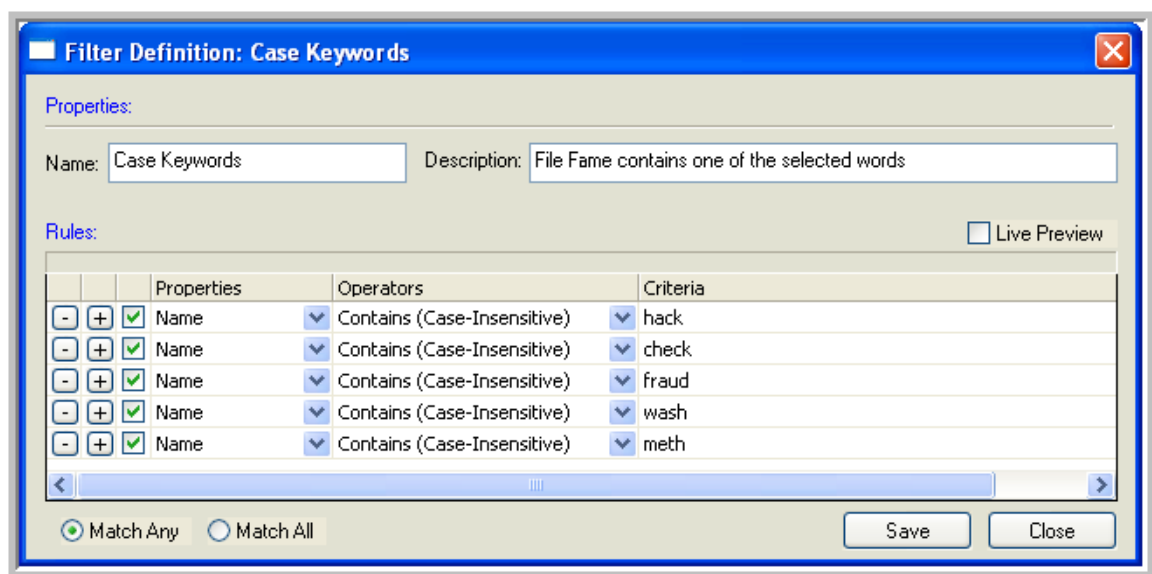
## LIVE PREVIEW

The live preview option enables your filter results to dynamically update. This can be useful when creating or testing filters. When used on large datasets, each change made to the filter can take time to populate the file list. For this reason, it is suggested that you limit your file list first, through the use of the tree view and Quick Picks, before using the live preview option. Once created, the filter can be applied across the required data.

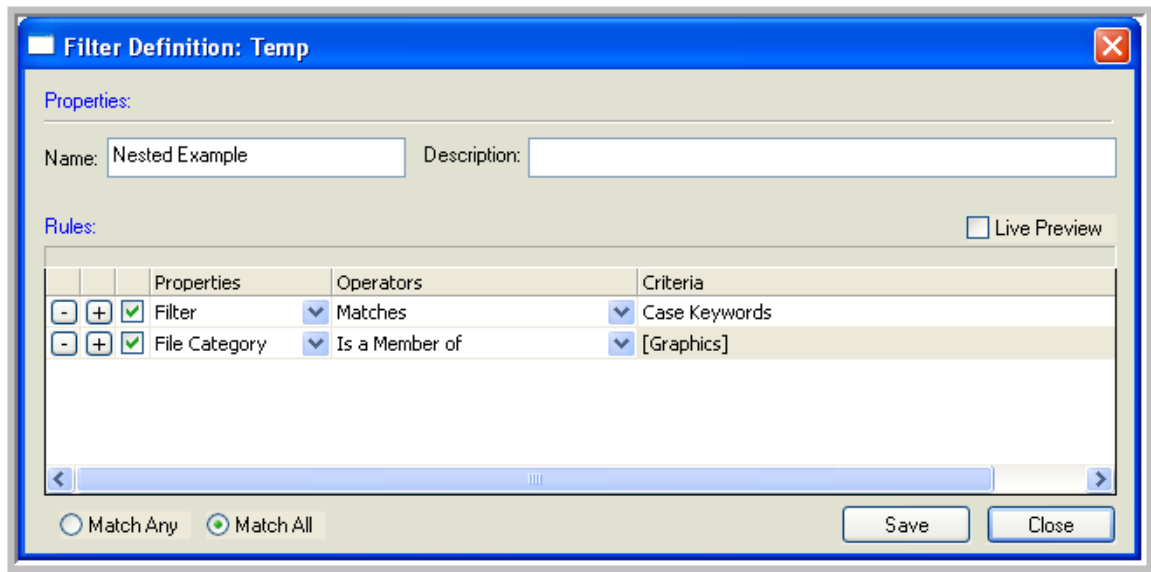
## NESTING FILTERS

One of the advantages of rule-based filtering is that previously defined filters can be used within other filters. This is called *nesting a filter*.

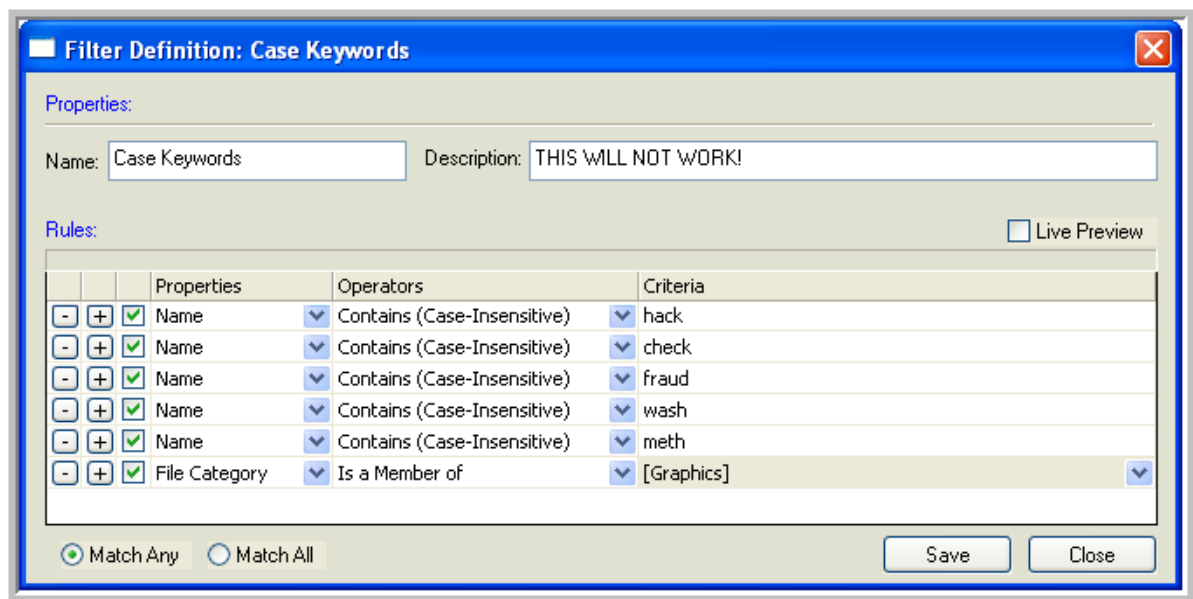
In the following example, a filter has been created that requires the Name to contain one of several strings. This is a Match Any filter.



Next, a new filter is created that uses this filter but adds the rule that the File Category must be a member of Graphics. Since the Match All option is used, this filter will allow only graphics with names that contain one of the specified strings to remain.




As an alternative, the existing filter of Case Keywords could be modified with the additional rule of File Category, as shown below.



This filter would *not* provide the correct results. If the option of Match Any is used, this filter would allow both files with names containing a specified string as well as any file that is a graphic to remain. Using the Match All would likely result in no remaining files since every qualifying file would have to contain every specified string and also be a graphic file. Nesting overcomes this problem as it allows the rules to be applied per filter.

## EXPORTING FILTERS

Once created, filters can be exported from your case for use on other cases or with other installations of FTK 2. Filters are contained in the database for that case and, as such, must be imported for each case. Filters are exported to XML files.

To export a filter, apply that filter and then select the Export Filter icon  or click **Filter > Export** to export the selected filter to an XML file. You will be provided with a Windows browse window to locate the destination.

---

**Important:** If the filter you are exporting contains a nested filter, make sure you export that filter also.

---

## IMPORTING FILTERS

To import a filter, select the Import Filter icon  or click **Filter > Import** and browse to a previously exported filter and select it. Click **Open** and you will see a success message.

---

**Important:** If you import a filter that contains a nested filter, ensure you also have that filter in your case. If it was user created, then it must be imported also.

---