

FlashStats 2006

User Guide



Table of Contents

Chapter 1: Quick Start Guide	4
Introduction.....	4
Installation	4
Starting FlashStats.....	4
Defining your web site	4
Running your first report	6
Next steps	8
Uninstalling FlashStats 2006	8
System Requirements	9
Chapter 2: Search engines	10
Introduction.....	10
Updating	10
How to define a new search engine.....	10
Ordering search engine definitions	13
Using the alternate method	13
Defining human-organized directories	15
How to define a new search provider.....	15
Filtering search engine activity.....	17
Recognizing new search engines	17
Chapter 3: Filters.....	18
Introduction.....	18
Using multiple filters.....	19
Overview of filters	19
A sample filter.....	19
Using multiple filters.....	21
Unintended effects of filters	21
Defining filters via drag and drop.....	22
Using the Filter Library	22
Chapter 4: Using DNS.....	24
Introduction.....	24
Using DNS lookup	24
Setting DNS options.....	25
Understanding DNS	26
Chapter 5: Log files.....	27
Introduction.....	27
Log Files view.....	27
Defining your web site's log folder	29
Downloading log files	29
Support for zipped logs	30
Management of zipped logs.....	30
Organizing zipped logs.....	30
Additional notes on log files.....	32
Chapter 6: BitKinex	33
Introduction.....	33
Installing BitKinex	33
Data sources.....	33

Managing data sources	34
Disabling BitKinex.....	35
How to get more information.....	36
Chapter 7: Spam referrers.....	37
Introduction.....	37
Managing the master list of spam referrers	37
Importing spam referrers from a report set.....	39
Adding spam referrers using drag and drop	42
Chapter 8: Updating FlashStats	43
Introduction.....	43
Checking for and downloading new configuration files	43
Updating chart templates	47
Updating XSL templates	48
Updating the FlashStats 2006 Program.....	49
Advanced settings for the Update FlashStats Program wizard.....	50
Configuring the Update FlashStats Program wizard.....	51

Chapter 1: Quick Start Guide

Introduction

FlashStats 2006 is a web analytics program which will analyze your web site's log files and create reports telling you information such as the number of page views each page received, the paths that visitors took through your site, and so on.

There are two editions of FlashStats 2006 available:

- FlashStats 2006 Standard Edition — This edition can analyze one web site.
- FlashStats 2006 Professional Edition — This edition can analyze any number of web sites. Each web site is defined and worked with separately.

This chapter shows you how to install and begin using FlashStats 2006.

Installation

To install FlashStats, simply open the FlashStats2006.msi file and follow the prompts.

You will be asked if you wish to install FlashStats 2006 for use by anyone who uses the computer or by the current user only. Choose the option to install for use by the current user only.

Note

FlashStats includes an FTP (File Transfer Protocol) utility called BitKinex. FlashStats uses BitKinex to download the log files from your web server. You can have FlashStats use BitKinex to download log files, or you can use another FTP program if desired. If you choose to use a different FTP client, then you will need to manually download your web site's log files. If your log files are already available locally then you do not need to use BitKinex.

If you want to use BitKinex, then be sure to install it at the end of the FlashStats installation routine.

Starting FlashStats

To run the FlashStats program, click on the Windows *Start* button, choose *All Programs*, choose *Maximized Software*, and then choose *FlashStats 2006*.

Defining your web site

You need to define your web site within FlashStats so that it knows the name of the web site, the home page URL, the location of the log files, and other defining characteristics.

To define your web site, open the FlashStats *Web Site* menu and choose *New*. This will start the New Web Site wizard. In each step, the wizard will display information and ask for details about your web site. Read all instructions and provide the requested information in the main part of the wizard window, then click the *Next* button at the bottom of the wizard window to proceed to the next step of the wizard.

Tip

FlashStats provides an advanced way to enter URLs. You can click the *Pick with IE* button to have FlashStats display an Internet Explorer window which you can then use to navigate to the desired page. See Figure 1-1 below. (You can use all of IE's features, such as bookmarks, to select the desired page.) Once you have navigated IE to the desired page, you can either close the IE window or click the *OK* button in the FlashStats URL Browser. FlashStats will insert the URL of the current page into the appropriate field.

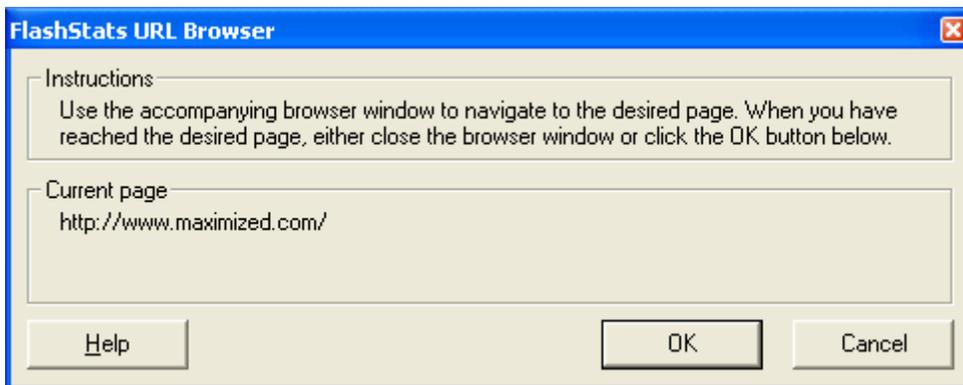


Figure 1-1: *FlashStats URL Browser* window

After you have finished the New Web Site wizard, FlashStats will automatically select the *Log Files* view. (Look along the left-hand side of the FlashStats window as shown in Figure 1-2 and you'll see a button bar where you can select among the different views available within FlashStats.) This view where is you manage the log files for your web site.

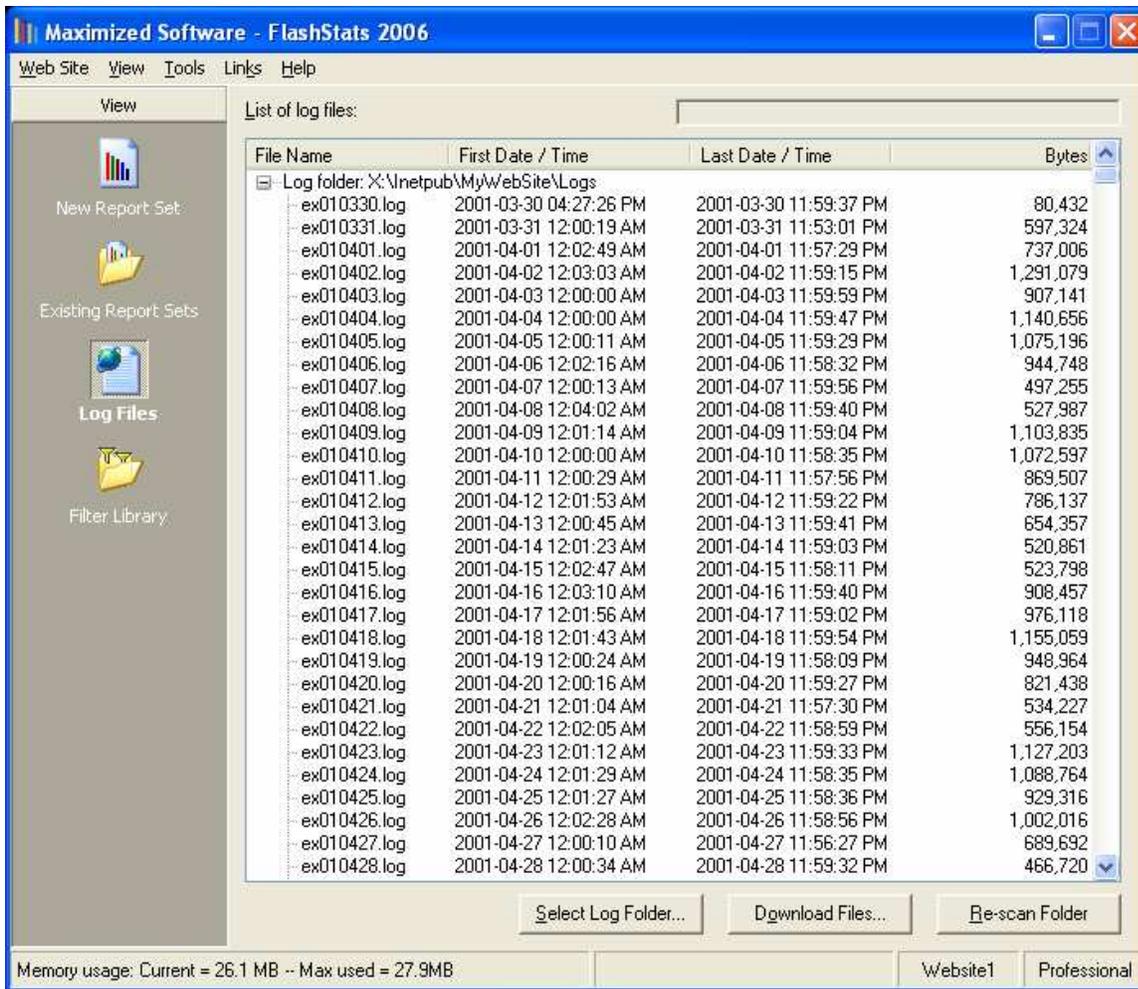


Figure 1-2: FlashStats 2006 Log Files view

FlashStats will prompt you to click the *Re-scan Folder* button. Click it to have FlashStats scan the log files in the log folder that you entered in the New Web Site wizard. (You may need to manually copy log files into that folder, or use the *Download Files* button to use BitKinex to download your log files.)

After FlashStats has scanned your log files, you are ready to run your first reports.

Running your first report

Click the *New Report Set* view in the *View* bar at the left of the FlashStats window; the window will now look something like Figure 1-3. The *New Report Set* view has two tabs where you can specify the desired report options. For the first set of reports (called a *report set*) you'll just select the desired date range and a few options.

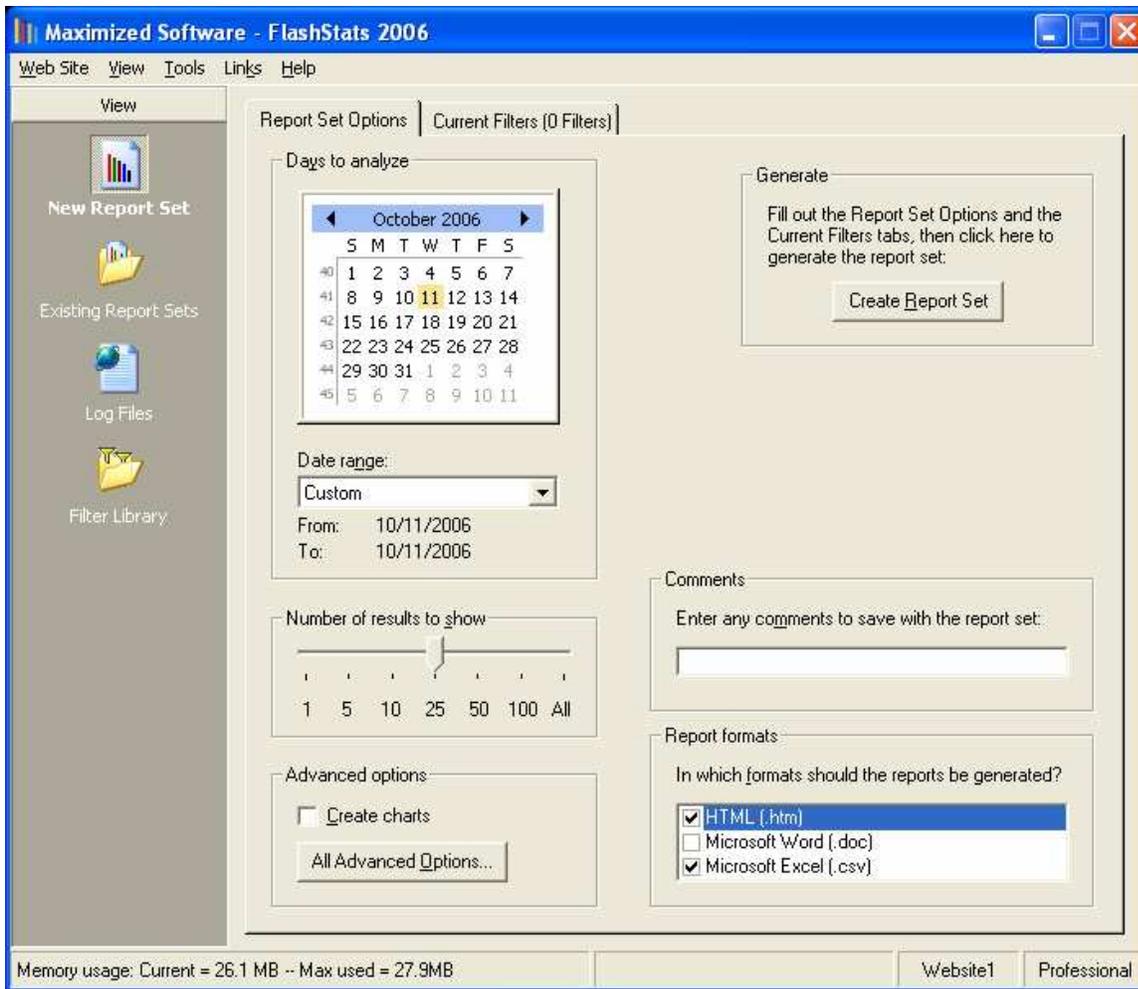


Figure 1-3: FlashStats 2006 New Report Set view

Select the range of dates that you would like to include in your first report set. You can click and drag across a range of dates in the calendar, or use the *Date range* list to choose a pre-defined starting and ending date.

In the *Advanced options* group, make sure that *Create charts* is checked. Then click the *All Advanced Options* button. In the resulting window (see Figure 1-4) make sure that *Perform DNS lookups* and *Show query strings* are cleared, then click *OK*.

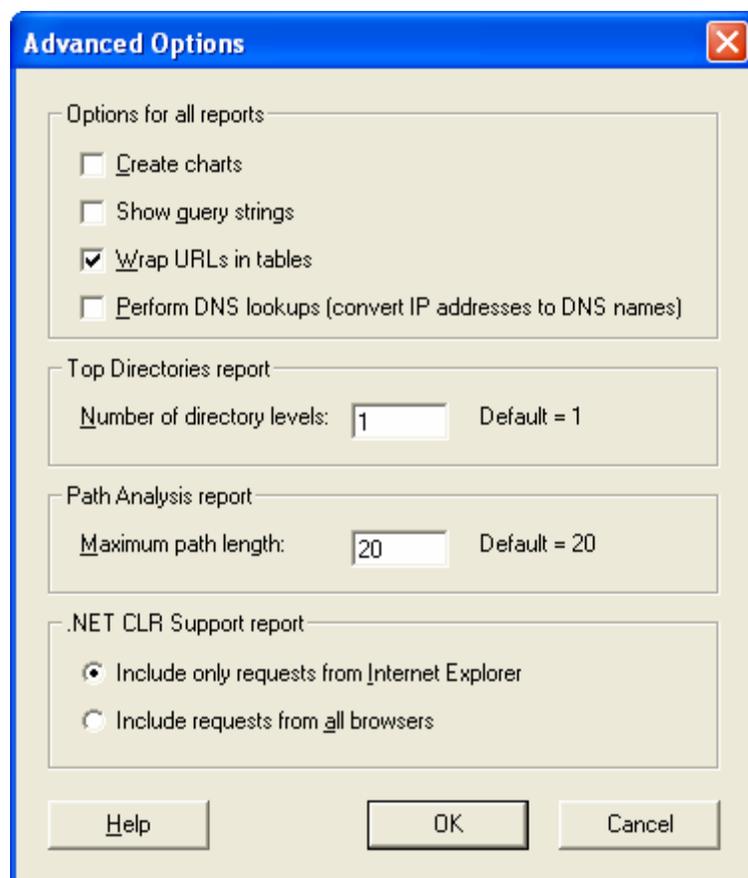


Figure 1-4: Advanced options for reports

That's all you need to do! Finally, click on the *Create Report Set* button and FlashStats will analyze your logs and create your first reports. After the reports have been created, FlashStats will automatically launch a browser window to display the Summary Data report. You can use the drop-down menus within each report to view different reports.

Next steps

Now that you have successfully run your first reports, feel free to explore all the features of FlashStats. In particular, be sure to check out the advanced filtering features, described in Chapter 3: Filters. You can also press F1 or click any *Help* button to get help for the current window.

Uninstalling FlashStats 2006

If for any reason you would like to remove FlashStats 2006 from your system, you should first uninstall BitKinex (if it was installed originally). You can do this by open the Windows Control Panel, then choosing *Add or Remove Programs*. Scroll down to BitKinex, then click the *Remove* button.

To remove FlashStats 2006, stay within *Add or Remove Program* in Control Panel. Choose Maximized Software FlashStats 2006 then click *Remove*. At the end of the uninstall routine for FlashStats, clear the *Run BitKinex Setup* checkbox before clicking *Finish*.

System Requirements

FlashStats 2006 has the following system requirements:

1. Windows 98, Windows ME, Windows NT 4, Windows 2000, Windows XP, or Windows Server 2003. (Current service packs recommended.)
2. 25MB disk space, plus enough space for your web site's log files. In addition, if the log files are zipped you will also need enough space to store an unzipped copy of them.
3. Enough free memory equal to approximately 70% of the total size of the log files you'd like to analyze. If you don't have enough memory, then FlashStats will use virtual memory on your hard disk, which can slow down performance considerably. FlashStats includes a display which tells you how much memory it is using.

If you only want to analyze one web site, then you can use FlashStats 2006 Standard Edition. If you want to analyze more than one web site, then you need FlashStats 2006 Professional Edition. Visit the Maximized Software web site to purchase a license. The Standard Edition can be upgraded to the Professional Edition.

Chapter 2: Search engines

Introduction

FlashStats 2006 offers comprehensive analysis of hits that your site receives from search engines.

In addition to analysis of search engines (such as Google and Yahoo!), FlashStats offers analysis of *search providers*. Search providers are those search engines which provide results to other search engines. For example, Google is a search engine as well as a search provider (Google provides results to about.com, AOL Search, and others). Tracking hits from search providers rather than search engines can help when you are trying to determine if your web site is listed in the most popular search indices.

FlashStats maintains one master list of search engines and providers. You cannot define a search engine (or provider) to be included in the results for only one web site.

In order to keep the list of search engines current, you may want to define new search engines yourself. You can also download a new list of the most current search engines (and providers) from the Maximized Software web site. Keep in mind that if you edit the search engines (or search providers) and then download an updated list of search engines from the Maximized Software web site, then you will lose the definitions of your new search engines.

Updating

Rather than manually editing them yourself, you may want to occasionally download new search engine and search provider definitions from the Maximized Software web site. Use the Update Configuration Files wizard as discussed in Chapter 8: Updating FlashStats.

How to define a new search engine

You can display the list of search engines that FlashStats uses by opening the *Tools* menu and choosing *Options*. The *Search Engines* tab shows all of the search engines defined within FlashStats, as well as a button to let you access the list of search providers.

To define a new search engine, follow these steps:

1. Open the *Tools* menu and choose *Options*. Make sure that the *Search Engines* tab is selected. You should see a window that looks like Figure 2-1:

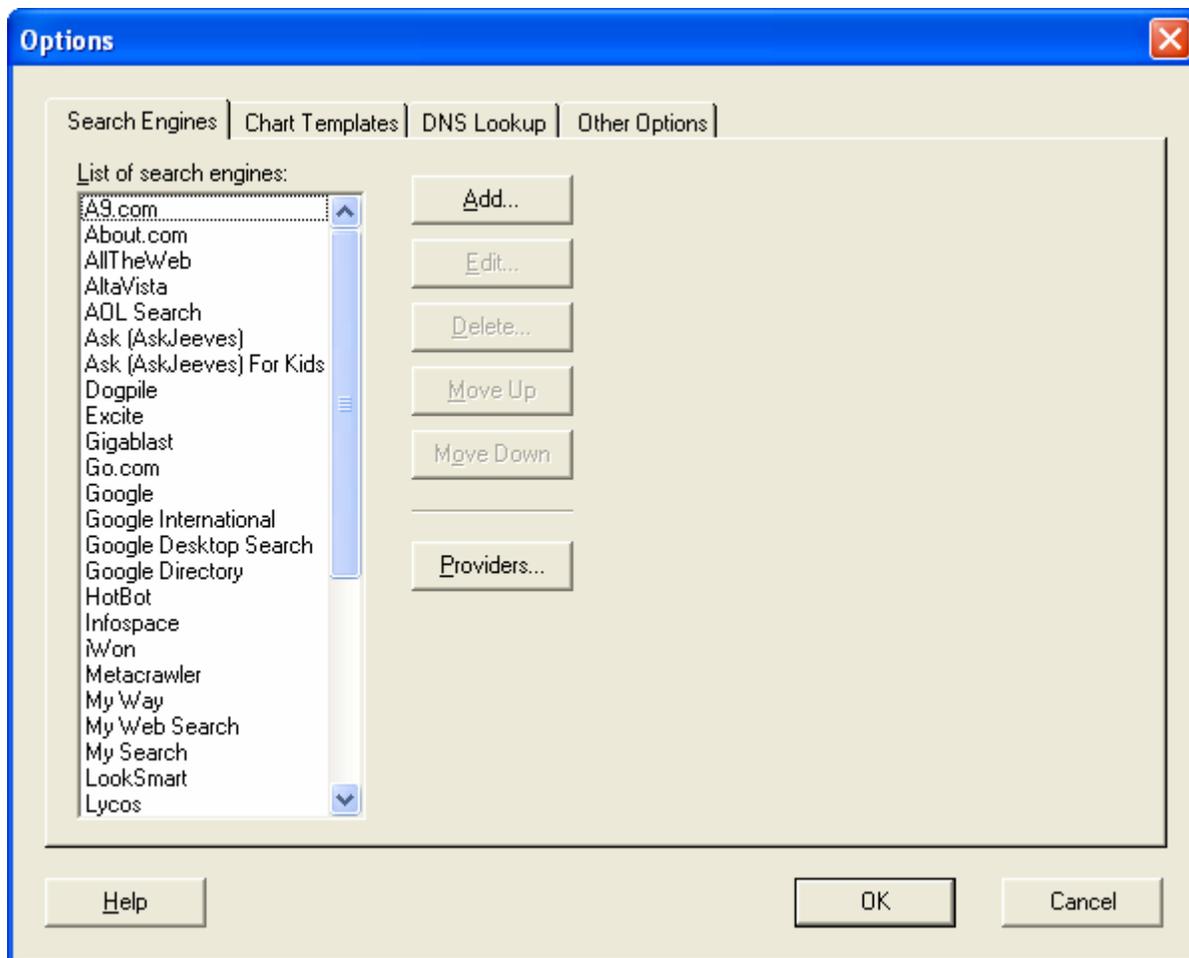


Figure 2-1 Options window, Search Engines tab

2. Click the *Add* button. The *Search Engine* window (Figure 2-2) will appear:

Search Engine

Home page URL:

Name:

Search provider
This search engine gets its results from this search provider:

Server names
List the server names used by the search engine when performing a search. Omit any leading "www."

Separate multiple names with a space or comma.
Example: ask.com askjeeves.com askforkids.com [Click Help for more information.](#)

Query string variables
List the query string variables used by the search engine when performing a search. [Click Help for more information.](#)

Separate multiple names with a space or comma.
Example: q

If this search engines passes the search phrase in the URL path instead of in a query string, click this button: Does not use alternate method

Figure 2-2 Search Engine window

3. Enter the name and home page URL for the search engine. You may want to click the *Pick with IE* button to display an Internet Explorer window which you can use to navigate to the search engine's home page. When you close the IE window, the *Home page URL* and *Name* fields will be filled in.
4. Specify the search provider used by the search engine. If the provider is not listed, then choose *Other* for now; you can come back later to change it after you have defined a new search provider.
5. Enter the search engine's web server name. You can omit any leading part of the server name, such as "www." or "search." and FlashStats will still match hits from the base part of the server name. You can enter multiple server names, separated by a comma or a space. Click

the *Pick with IE* button to display an IE window to help navigate to an appropriate page (usually a search results page), and FlashStats will extract the server name from the page's URL.

6. Specify the variable which the search engine uses to specify the phrase being searched for. If the search engine uses different query string variables in different scenarios you can list them all here, separated by a comma or a space. You can click the *Pick with IE* button to help figure out the appropriate query string variable. Click *Pick with IE*, navigate to the search engine, and run a search for any phrase (for example, "FlashStats"). When the search engine has displayed its results, close the popup IE window. FlashStats will display a list of the query string variables that were used in the URL for the search results page. Look for the "name=value" pair which contains the phrase that you searched for (for example, "q=FlashStats") and click on it; FlashStats will add it to the list of query string variables.

When you are satisfied with the settings in this window, click *OK* to save the new search engine definition and return to the *Options* window.

Ordering search engine definitions

You can move any search engine definition up or down in the list by using the *Move Up* and *Move Down* buttons. FlashStats analyzes the list of search engines in the order listed. If you have two similar search engine definitions, one very specific and one more general (usually using an asterisk to match any characters), then you should order the specific search engine definition above the more general definition. This will ensure that the specific case is matched when appropriate, rather than always matching the general definition.

For example, the definition for Google matches the server name google.com. The definition for Google International matches any name with the pattern *.google*. It is important to have the Google definition above the Google International definition, so that requests coming from www.google.com will match the Google definition, and requests coming from www.google.ca will match Google International. If the definitions were in the other order, then requests from www.google.com would match the Google International definition when tested, and the plain Google definition would never be tested.

Using the alternate method

In order to create its search reports, FlashStats analyzes the referring URL that accompanies each hit to your web site. The vast majority of search engines pass the search phrase via a query string; for example, "http://www.google.com/search?q=Phrase". However, a few search engines pass the search phrase in a different part of the URL. For example, the A9.com search engine passes the search phrase in the path, like this: "http://a9.com/Phrase". Likewise, Excite uses a URL like this: "http://msxml.excite.com/info.xcite/search/web/Phrase".

FlashStats can analyze referrals from these types of search engines. To define a search engine that passes the search phrase in the URL path instead of query string, click on the *Settings* button

at the bottom of the *Search Engine* window. This will display the *Alternate Method Settings* window (Figure 2-3):

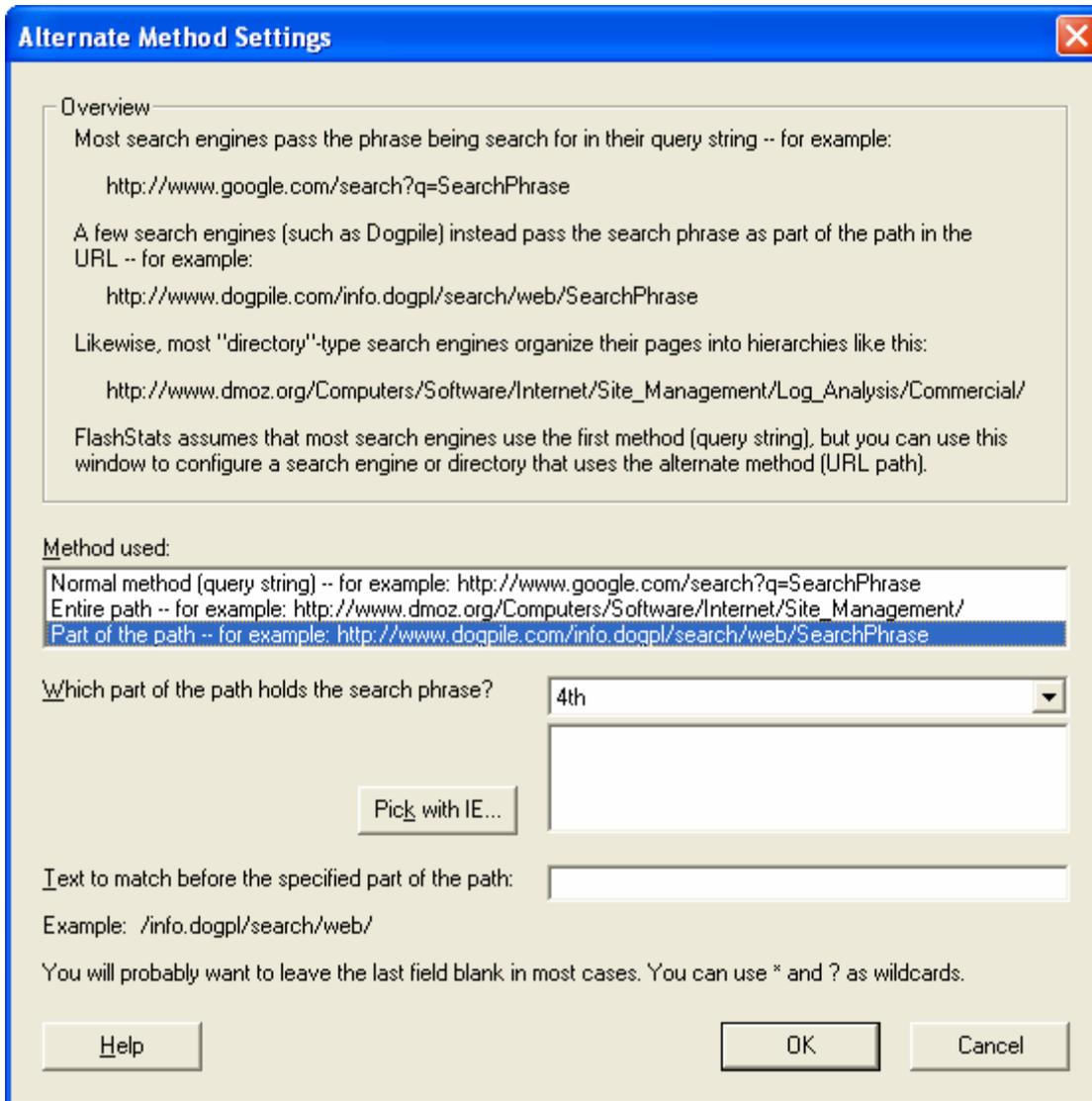


Figure 2-3 Search engine alternate method settings

In the *Method used* list, choose "Part of the path". In the *Which part of the path holds the search phrase?* list, choose the appropriate part of the path. You can click the *Pick with IE* button to open an Internet Explorer window to navigate to the search engine, run a sample query, then close the browser to return to this FlashStats configuration window and select the desired portion from the list box. Finally, if there is any leading text that you want to require in the path, you can enter it in the *Text to match before the specified part of the path* edit field. Any request which does not contain the text you specify will not match the search engine definition. (In most cases you can just leave this field blank.)

Defining human-organized directories

FlashStats also lets you report on referrals from "directories" which are organized by a human staff, such as Yahoo's directory or the DMOZ Open Directory.

To enable analysis of referrals from such a directory:

1. Create a new search engine definition and click the *Settings* button to display the *Alternate Method Settings* window as described above.
2. In the first list, choose "Entire path".
3. You can leave the other fields blank, although you might need to fill in some text in the *Text to match at the start of the path* field. Filling in this field enables FlashStats to accurately detect referrers from entries in the "directory" rather than any other links or search engine used on the site.

How to define a new search provider

Use this procedure to define a new search provider:

1. Open the *Tools* menu and choose *Options*. Make sure that the *Search Engines* tab is selected.
2. Click the *Providers* button. The *Search Providers* window (Figure 2-4) will appear:

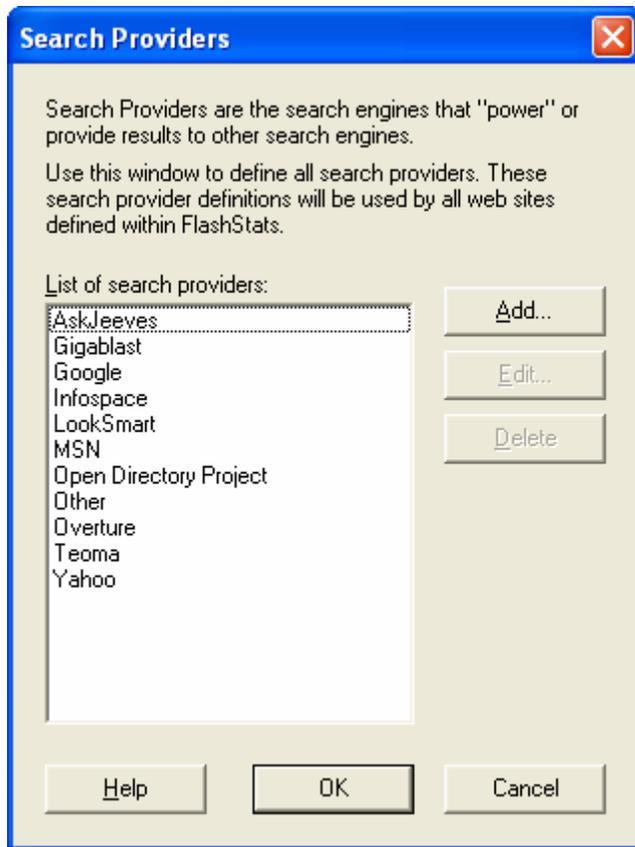


Figure 2-4 Search Providers window

3. Click the *Add* button. The *Search Provider* window (Figure 2-5) will appear:



Figure 2-5 Search Provider window

4. Enter the name of the search provider and the URL of its home page. You can click the *Pick with IE* button to display a popup Internet Explorer window to help select these two values.
5. Click *OK* when you are done.

Filtering search engine activity

You can create a filter to have FlashStats include or exclude hits coming from search engines. Filter search engines by creating a filter with a test of the referrer field. Be sure to enter a test pattern which will match a referring URL from the desired search engine.

See Chapter 3: Filters for more information on creating and using filters.

Recognizing new search engines

You should periodically review the Unrecognized User Agents report. This report lists all user agent strings that FlashStats finds in your web site log files that it does not recognize. Manually reviewing these values may lead you to discover new search engines that interest you. You can then define a new search engine using the procedure given above and then run new reports.

Keep in mind that if you create new search engines (or search providers) and then download an updated list of search engines from the Maximized Software web site, you will lose the definitions of your new search engines.

Chapter 3: Filters

Introduction

Normally you will want FlashStats 2006 to analyze every request it finds in your web site's log files, providing grand totals for your web site activity.

Sometimes, however, you may want to obtain results on a subset of the hits to get information about only certain activity. For example, you may only be interested in hits on a certain web page, or requests from users using a certain brand of browser. You can restrict the data analyzed by FlashStats by defining *filters*.

A filter tells FlashStats whether it should include or exclude certain hits in its analysis. Each filter consists of a set of possible *tests*, and each test has one or more *patterns* which need to match a particular request in order to take effect.

The types of tests available are:

- Client IP address or DNS name
- Authenticated user name
- Browser brand
- User agent category
- User agent string
- URL
- File name
- Directory
- Content type
- Query string parameter
- Return code
- Referring page
- Originating referrer
- Entry page
- Exit page

Each filter must use at least one test. All of the tests in a filter must match a given hit in order for the hit to be included (or excluded).

You can specify multiple patterns to match in a given test. For example, in the return code test, you can specify several different return codes (eg, 200, 404, 501). If a hit's return code matches one of the test patterns, then the test matches. If all other tests within the filter also match, then the filter matches, and the given hit will be included in the analysis (or excluded, if the filter action is exclude).

Using multiple filters

You can define as many filters as desired. Each hit in your log files will be compared against the set of filters. A hit will be included in the analysis if it matches at least one include filter, and does not match any exclude filters.

If you are only using include filters, then each hit will only be included if it matches at least one of the include filters. If you are only using exclude filters, then each hit will only be included if it does not match any of the exclude filters.

In addition, FlashStats uses an innovative drag and drop interface to let you easily drill down into existing results with a minimum of typing.

Overview of filters

Filters must be defined before you press the *Create Report Set* button to have FlashStats analyze the log files and generate reports. Add new filters or edit or delete existing filters on the *Filters* tab of the *New Report Set* view. After you have run reports, FlashStats adds each filter to the Filter Library. You can switch to the *Filter Library* view at any time to retrieve any previously-used filter and use it when creating another report set.

A sample filter

Figure 3-1 shows an example of a filter:

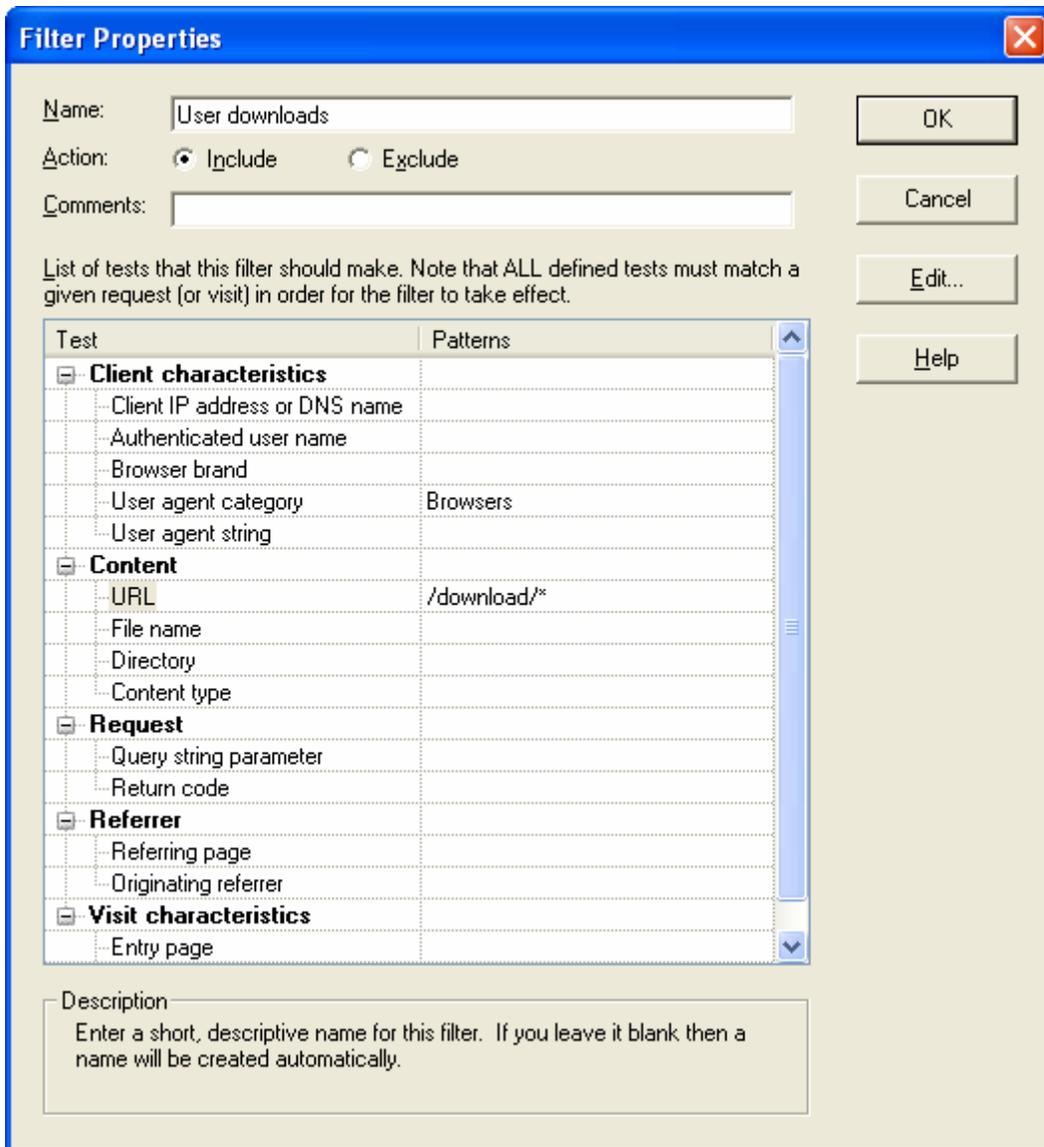


Figure 3-1 Sample filter

Here is an explanation of the important parts of this filter:

The filter has been named "User downloads". This is an easy-to-read description which is shown in other areas of FlashStats. You do not have to assign a name to each filter, but it can help you to remember what each one does. (You can also use the *Comments* field to make notes to yourself if desired.)

The filter is an include filter; when FlashStats reads the web site's log files, only requests which match this filter's tests will be included. (You can also define exclude filters; FlashStats will exclude requests which match the exclude filter's tests.)

This filter will perform two tests. Both tests must match in order for the filter to take effect.

The first test is User agent category. FlashStats will check to see if the user agent which made the request is a Browser. In other words, FlashStats will only care about requests coming from browsers rather than from other types of user agents (such as search engines or HTML validators).

The second test is URL. FlashStats will only include each request if it is for a file within the /download folder. Note that trailing asterisk, which means to match any remaining text, so this will match any file within the /download/ folder (or a subfolder).

Since both tests must match, the effect of this filter is that FlashStats will only include requests which were made a browser for a file whose URL begins with /download/.

Here are some sample requests and whether they would be included or excluded based upon this filter:

User agent	URL requested	Filter result
MSIE 6.0	/download/setup.exe	Include
MSIE 6.0	/products/index.htm	Exclude (wrong folder)
Googlebot/2.1 (<i>see note below</i>)	/download/setup.exe	Exclude (wrong user agent)

Note:

GoogleBot is the name of the "spider" used by Google to crawl the Web to index your pages.

Using multiple filters

You can use multiple filters when running FlashStats. FlashStats will apply each filter against each request in order to decide whether to include the request.

Each request will be included if it matches at least one Include filter and does not match any Exclude filters.

As you define multiple filters, FlashStats will provide a description of how the filters will interact. Look for the text in the box labeled *Combined effect of filters* on the *Filters* tab.

Unintended effects of filters

FlashStats will try to make sure that you only define useful filters, but it is possible to define a filter which has unintended effects. For example, if you create an include filter which only includes requests to a file or directory which doesn't exist on your web site, then your reports will have no data in them.

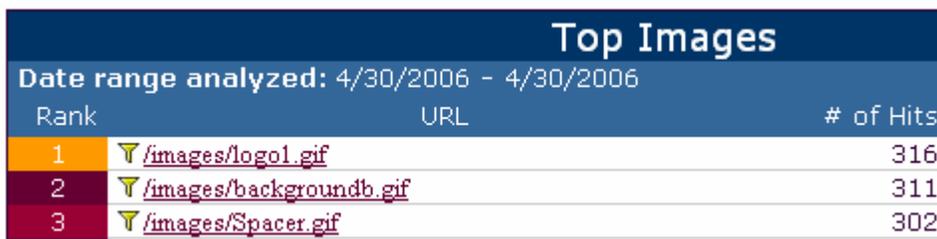
Likewise, be careful when defining multiple filters. For example, if you define an include filter which only includes requests if made by a search engine, and then also make an exclude filter

which matches requests made by a search engine, then no hits will be counted and your reports will be empty.

Defining filters via drag and drop

In addition to manually creating filters, FlashStats 2006 lets you easily define filters using drag and drop.

When FlashStats creates reports, most entries will have a small filter icon to the left of the value. For example:



Top Images		
Date range analyzed: 4/30/2006 - 4/30/2006		
Rank	URL	# of Hits
1	 /images/logo1.gif	316
2	 /images/backgroundb.gif	311
3	 /images/Spacer.gif	302

Figure 3-2 Snippet from the Top Images report

Notice the little filter icon: . You can drag and drop this icon to anywhere on the FlashStats window, and FlashStats will create a new filter using the value to the right of the filter icon. (The *New Report Set* view must be selected in order for FlashStats to accept the dropped filter icon.)

Using the sample report shown above, if you were to drag the filter icon from the first row, then FlashStats would create a filter which would test for requests to /images/logo1.gif.

When you drag and drop a filter icon onto the FlashStats window, FlashStats will create a new filter. However, if you are currently editing a filter, then FlashStats will add an appropriate test for the dropped value to the filter that you are editing.

When you use this drag and drop interface to create new filters, be sure to provide a name for the filter and choose whether you want it to be an include or exclude filter.

Using the Filter Library

You may want to use the same filter every time you analyze your logs. Or, there may be a set of filters that you want to use in different analysis scenarios. FlashStats provides the Filter Library as a place to store filters for re-use.

Each time generate reports, FlashStats saves a copy of each filter used into the Filter Library. You can see the *Filter Library* view at any point by choosing it from the *View* bar on the left hand side of the FlashStats window. See Figure 3-3.

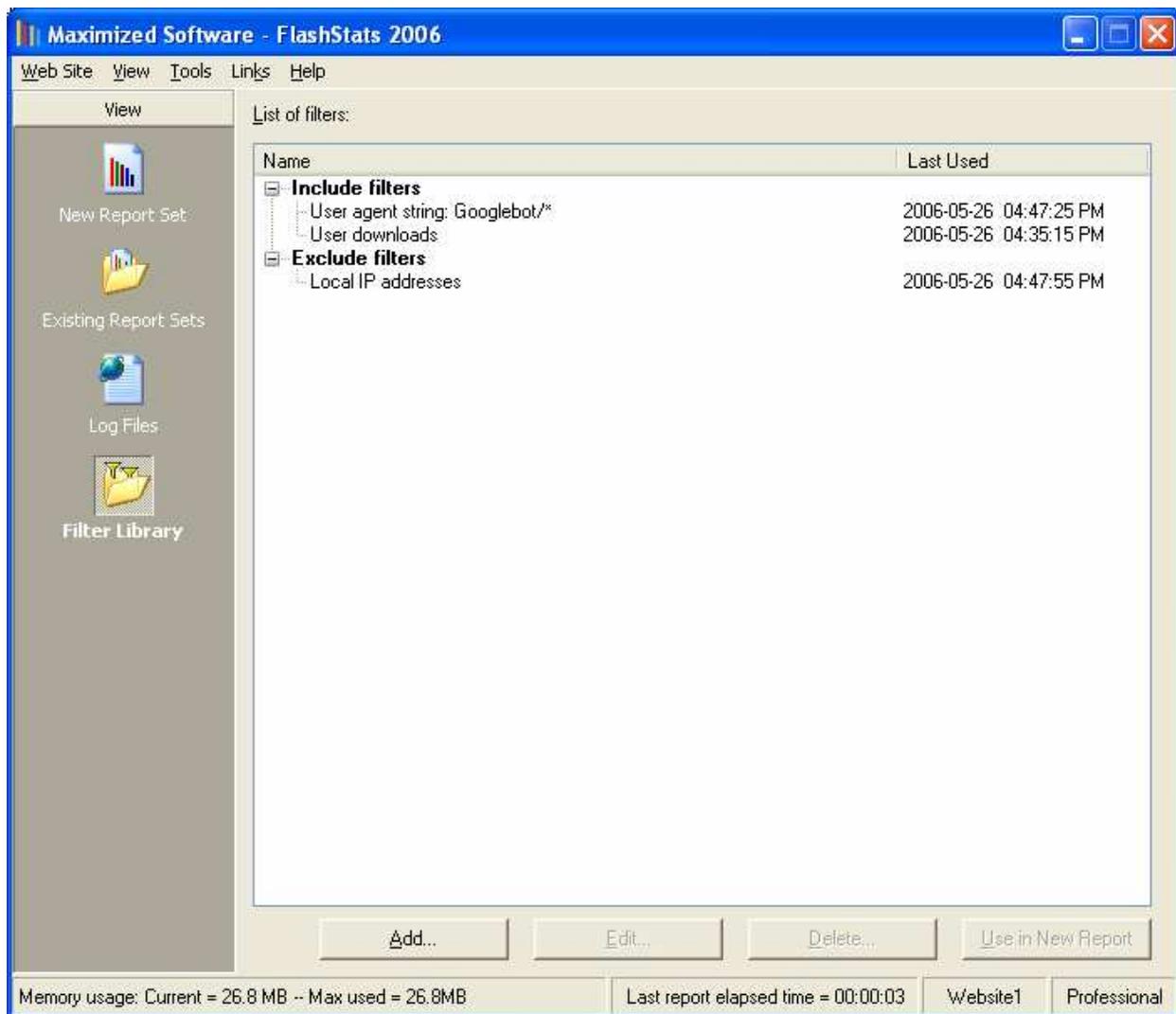


Figure 3-3 *Filter Library* view

To further information on using the Filter Library, open the *Help* menu and choose *Help on This Window*.

Chapter 4: Using DNS

Introduction

Most web servers log each visitor's *IP address*. FlashStats can convert each IP address to a *DNS name* (also called a *host name* or *fully qualified domain name*). See the *Understanding DNS* section at the end of this chapter for additional general information about DNS.

Using DNS lookup

FlashStats automatically converts each IP address to its equivalent DNS name if you have selected the check box labeled *Perform DNS lookups* (in the *All Advanced Options* section of the *New Report Set* view) when creating reports, as shown in Figure 4-1.

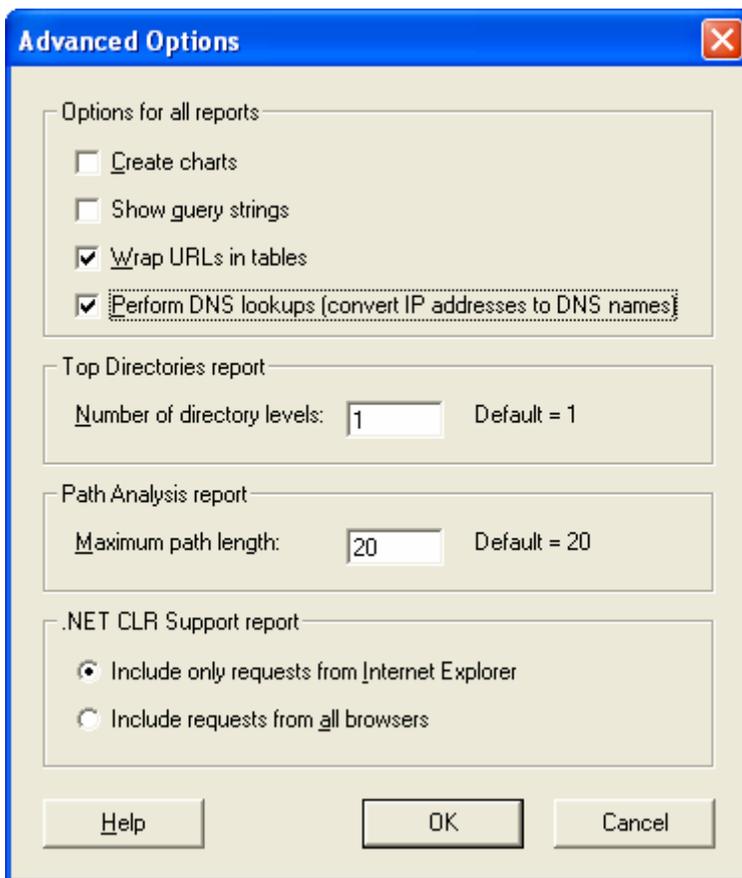


Figure 4-1: Enabling DNS lookups

When FlashStats begins analyzing your log files, it will first scan the log files and convert each IP address to a DNS name (if you have checked the *Perform DNS lookups* option as described above). FlashStats can convert up to 128 IP addresses at a time. Converting IP addresses to DNS names can add considerably to the amount of time that it takes to generate reports for the first

time. Once the conversion has been completed and cached, future reports will use the cached values and so performance will not be greatly impacted.

If you are trying to get quick results, don't care about DNS names, and have not yet converted the IP addresses to DNS names, then you should disable the DNS name lookup using the *Advanced Options* window (Figure 4-1 above).

Setting DNS options

To configure DNS options within FlashStats, open the *Tools* menu and choose *Options*. Click on the *DNS Lookup* tab; the *Options* window will look like Figure 4-2 below.

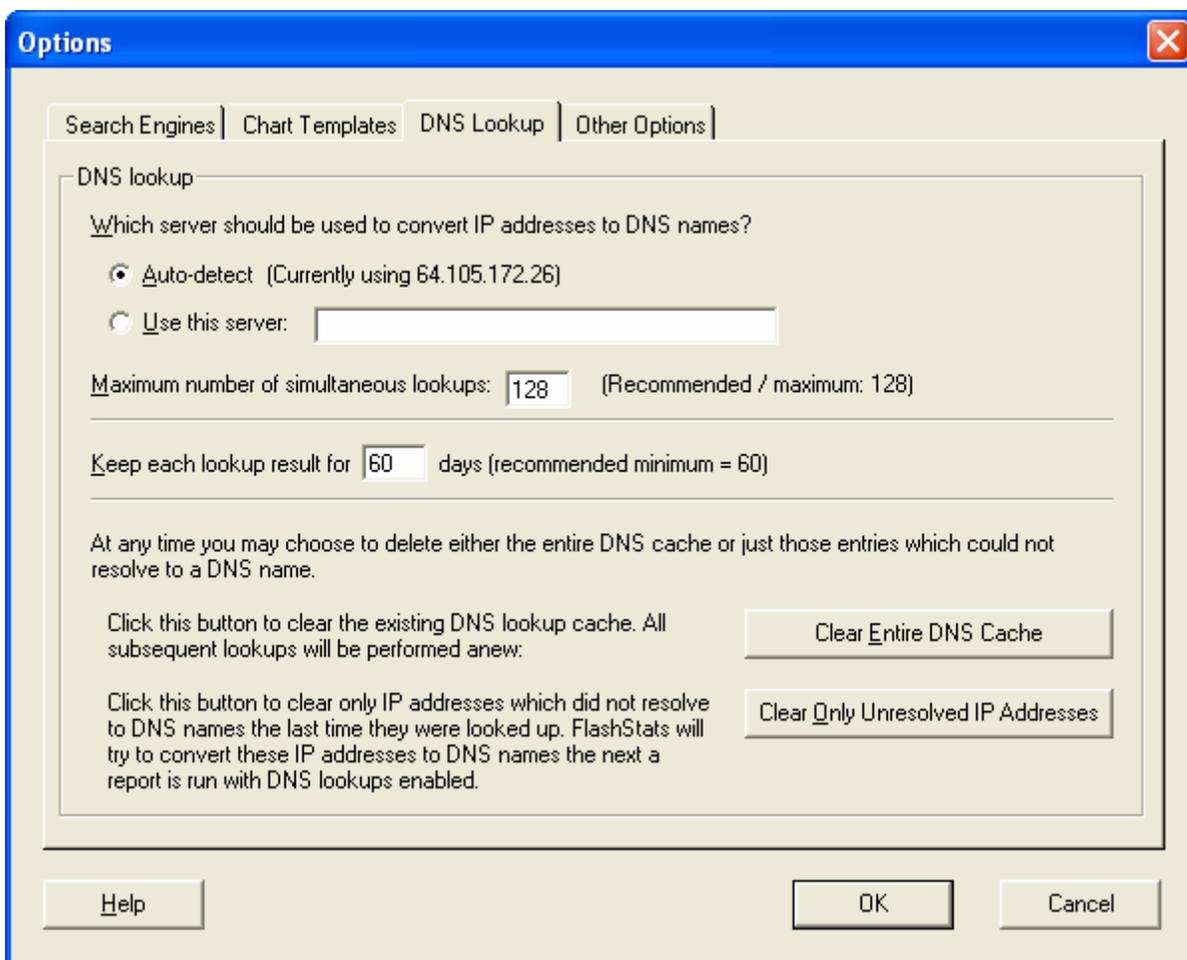


Figure 4-2 Options window, DNS Lookup tab

FlashStats caches each DNS name for up to 60 days (by default). When the DNS name has expired FlashStats will look it up again. You can change the number of days that FlashStats caches each DNS name in the *Keep each lookup result for X days* field. (See Figure 4-1 above.)

You can manually flush the entire cache at any point by clicking on the *Clear Entire DNS Cache* button. Clearing the DNS cache will cause subsequent runs of FlashStats to perform a new lookup for every IP address it finds in your web site log files.

FlashStats may not be able to convert any given IP address to its equivalent DNS name. In this case, FlashStats will remember that the DNS name for that IP address could not be looked up. You can choose to clear from the cache only those IP addresses which could not be converted to their DNS name. FlashStats will then try to convert them the next time it analyzes your log files. To do this, click the *Clear Only Unconverted IP Addresses* button.

Understanding DNS

Every computer on the Internet is assigned an *IP address*, which is a 4-part number that looks something like 123.45.67.89. These numbers can be converted to *DNS names*, which tend to look something like *port2.sanfrancisco.bigisp.com*. These DNS names will show up the following reports:

- Visitor DNS Names -- This report shows the entire DNS name (sometimes called a “fully qualified domain name”).
- Top Level Domains -- This report shows only the “top-most” domain, that is, the furthest right component, such as *.com*, *.net*, *.edu*, or *.uk*.
- Primary Domains -- This report shows the right-most part for the common domains such as *.com*, *.net*, and *.edu*, and includes an extra level for two-letter country top-level domains, such as *.co.uk*.
- Secondary Domains -- This report shows one more level than the Primary Domains report, so that you see secondary domains such as *bellsouth.net* and *demon.co.uk*.

If these reports show only “Unresolved IP address” then FlashStats is not configured to convert IP addresses to DNS names. Enable this option in the *All Advanced Options* window (Figure 4-1 above) and then create a new report set.

Chapter 5: Log files

Introduction

In order to create reports for your web site, FlashStats needs a local copy of your log files. (FlashStats can access files on a local drive or on a network hard drive.) If your web site stores its log files on a remote server, then you need to download a copy of the log files into a local (or network) folder.

If your web site already stores its log files on a drive accessible to your computer, then FlashStats can read those files directly. You will not need to make a copy of the files.

Note

FlashStats includes a File Transfer Protocol (FTP) program called BitKinex. If your log files need to be downloaded from a remote server, you can have FlashStats use BitKinex to download your web site's log files, or you can use a different FTP program of your choice.

Log Files view

The *Log Files* view (see Figure 5-1 below) is used to manage the log files for your web site.

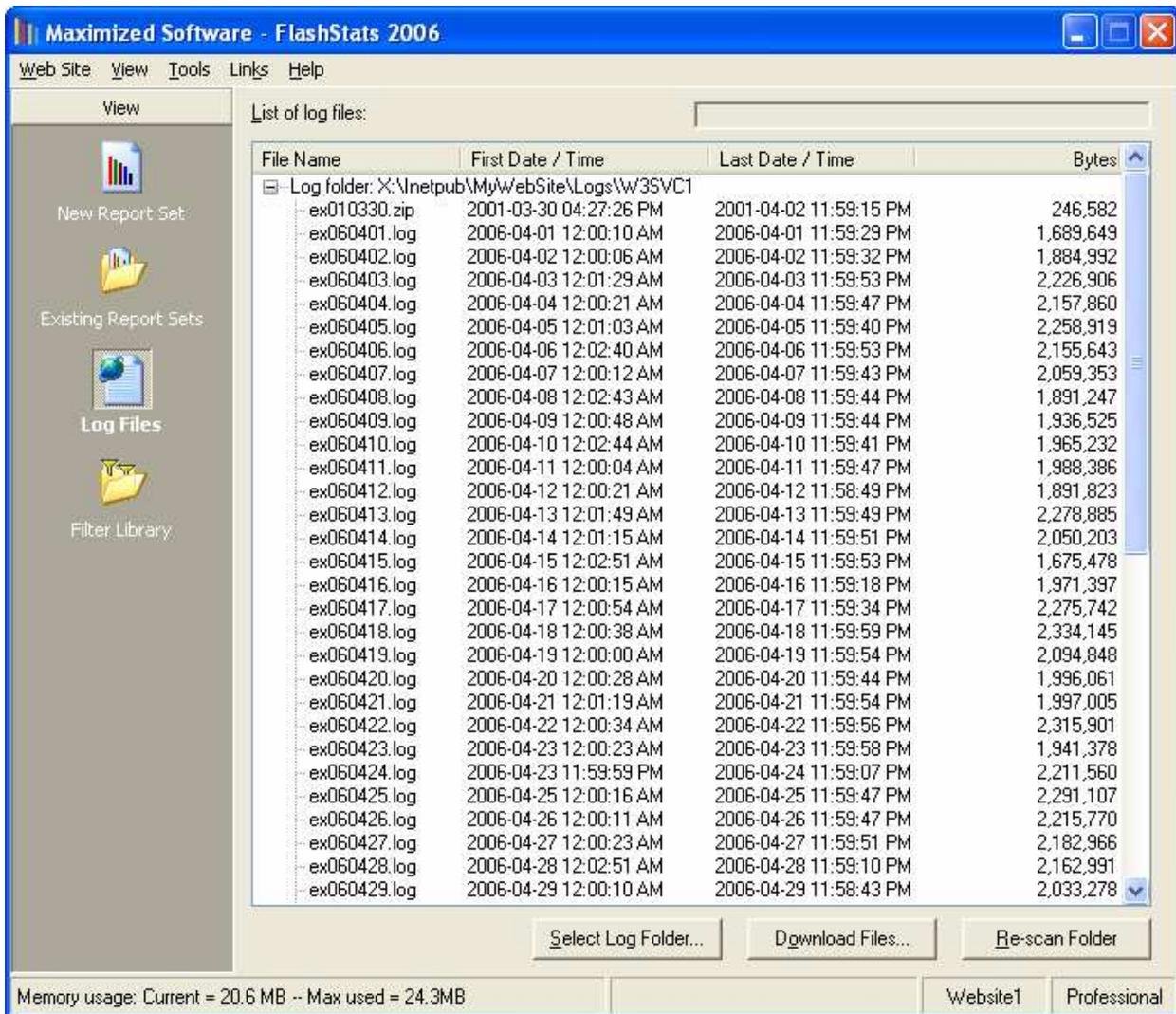


Figure 5-1 Log Files view

You can right-click on any log file to get a pop-up menu of useful commands, such as *Select Date Range for Analysis*.

The following buttons are available:

- *Select Log Folder* — Click this button to start the Log Folder wizard so that you can select the folder where your web site's log files are saved.
- *Download Files* — Click this button to display the *Download Log Files* window, which you can use to begin the download of your web site's log files. This is only useful if you have configured the web site so that FlashStats will use the included BitKinex FTP program to download log files from a remote server.

- *Re-scan Folder* — Click this button to re-scan your log folder for any changes. FlashStats will detect new files, changed files, and deleted files. You may need to click this button if you manually add, edit, or delete files in the log folder.

Defining your web site's log folder

FlashStats needs to know the location of the folder where your log files are stored. This folder is called the *log folder*. There are three scenarios for defining your log folder; review the following list to see which one applies to your setup.

1. The log files are already stored locally, so there is no need to make a copy of them. In this case, simply define the log folder where the log files are already saved. Also, you will not need to use BitKinex or any other FTP program to download the log files.
2. The log files are stored on a remote server, and you want to have FlashStats use BitKinex to download them to your computer. Define the log folder into which BitKinex should save the log files, as well as the values that BitKinex needs in order to download the log files.
3. The log files are stored on a remote server, and you want to use your own FTP program to manually download them to your computer. Define the log folder into which you will download the log files. You will need to manually download new log files when desired.

Click the *Select Log Folder* button to start the Log Folder wizard, and then follow the prompts. You can click the *Help* button at any point to get more information about the current step of the wizard.

Downloading log files

If you want to analyze the most recent data from your web site, you may need to download new log files. Follow this procedure when analyzing your web site's most recent activity:

1. If you have configured FlashStats to have BitKinex download your web site's log files from a remote server, you can click the *Download Files* button to initiate downloading new log files. If you need to manually download new log files, use your preferred FTP program instead to get any new log files.
2. Click the *Re-scan Folder* button. FlashStats will quickly examine the log folder and update the list of log files.
3. Switch to the *New Report Set* view. Select any desired options, and then click the *Create Report Set* button to analyze your web site and create a new report set.

Support for zipped logs

FlashStats can automatically extract data from zipped logs. The following compression formats are supported:

- .ARC
- .ARJ
- .ARK
- .CAB
- .DWC
- .EXE (PKZIP format)
- .GZ (GZip)
- .LBR (Novosielski)
- .LHA
- .LZH
- .PAK
- .TAR
- .Z (UNIX Compress)
- .ZIP
- .ZOO

Management of zipped logs

If you manually unzip a log compressed log file, be sure to keep only one copy of the file in the log folder defined within FlashStats; otherwise, FlashStats will analyze both copies and your results will be doubled. Therefore, if you manually unzip a compressed log file and store the unzipped copy in the FlashStats log folder, then be sure delete the original zipped copy of the file. (Or, you can move the original file to a different folder so that FlashStats will not see it.)

FlashStats performs minimal management of zipped log files. FlashStats will use BitKinex to download zipped files from your web server. FlashStats will then unzip each zipped file into a temporary folder so that it can analyze its contents. This means that you need enough disk space to hold the zipped copy of the logs as well as an unzipped copy which can be read by FlashStats.

Organizing zipped logs

If your log folder contains zipped log files, FlashStats will unzip each file as necessary. Files need to be unzipped when initially scanning them to determine the range of dates included in each file, as well as when performing full analysis on them.

Unzipped files are stored on your local hard drive (or network drive) in a different folder than your log folder. To view the unzipped logs folder, open the *Tools* menu and choose *Unzipped Logs*; the window shown in Figure 5-2 appears.

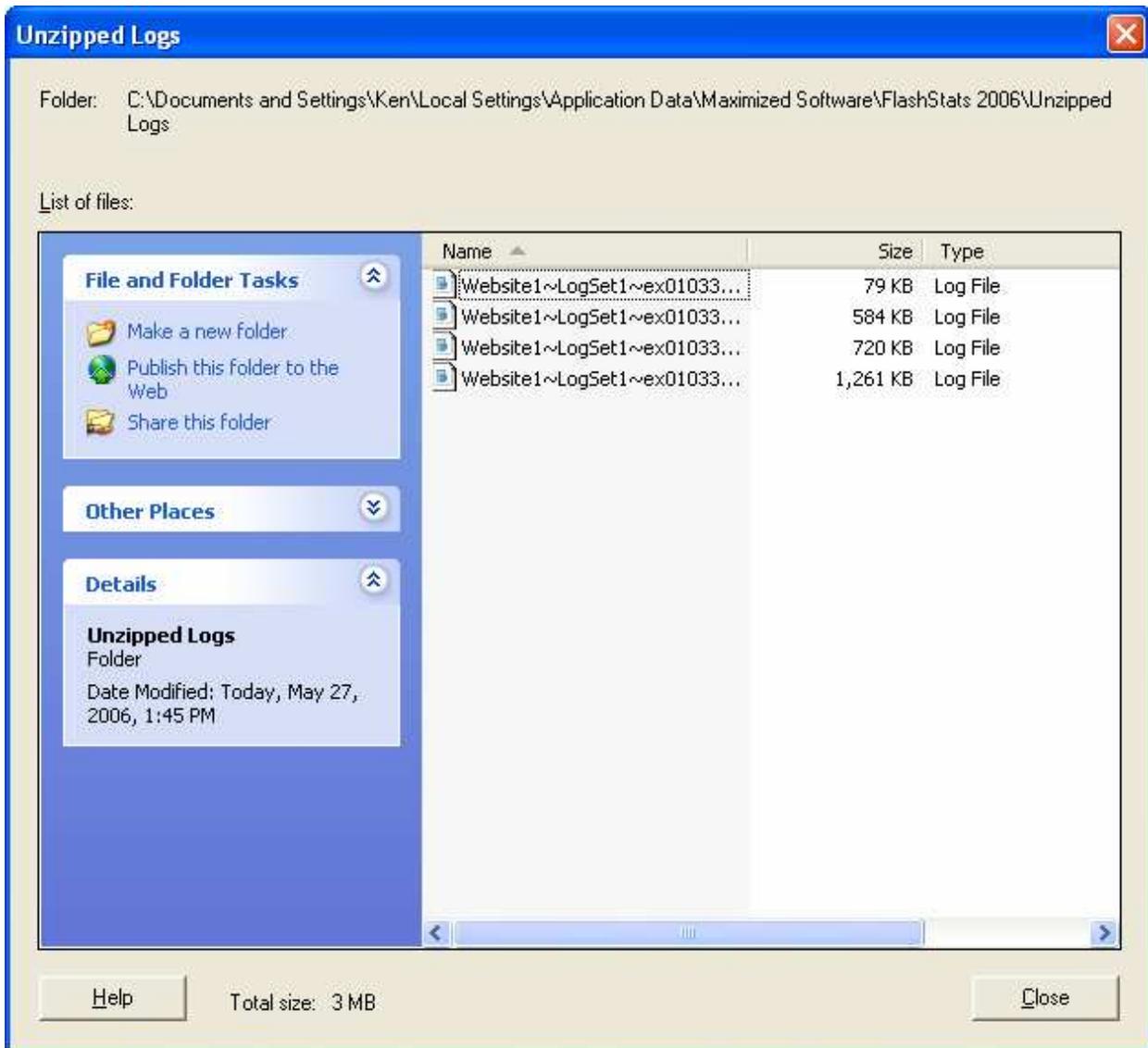


Figure 5-2 *Unzipped Logs* window

This window contains an embedded Windows Explorer pane showing the folder where unzipped log files are stored. You can manage the files in this folder just like you would in a normal Windows Explorer window. For example, you can right-click on any file to get standard commands like *Delete* or *Properties*.

You can always delete any file in the unzipped logs file folder (except while analyzing them, of course). FlashStats unzips files on demand; any file that you delete from this folder may be re-created in the future if FlashStats needs it.

When FlashStats unzips a log file, it gives it a name consisting of four parts: the ID for the web site; the text “LogSet1”; the zipped file name and extension; and the name and extension of the file contained within the zipped file.

For example, assume that you have a zipped file called logs.zip for your first web site. The web site ID will probably be Website1. If logs.zip contains a file named Jan.log, then when it gets unzipped it will be named Website1~LogSet1~logs.zip~Jan.log.

Additional notes on log files

1. If your web site hosting company automatically deletes log files after a certain amount of time, you need to be sure to download a copy of all log files before they are deleted.
2. FlashStats should still work correctly if your web site rotates its log files. FlashStats determines if a file has changed by examining the file size.
3. You should not have multiple copies of the same log file data in separate files. This might happen if you end up with one copy in a file named something like access.log and another copy in a file with a name based on the date, such as 200601.log. If this happens, FlashStats will include the data from each log file, effectively doubling your results. This will not happen for most users; simply make sure that your log files are properly named and cleaned up if they are rotated by your web site.
4. If you manually download log files using a FTP program, be sure to download them using binary mode rather than text mode. (Text mode is also called ASCII mode). This is necessary because FlashStats determines if a file has changed by examining the file size. If you download with text mode then the size of the file may change and FlashStats will think that the file has changed when in fact it hasn't.
5. FlashStats can read log files saved with any style of terminating each line, whether it is UNIX (LF character), Mac (CR), or DOS (CR+LF).
6. All of the log files for your web site must be stored in the same folder. FlashStats will not read files from any sub-folders of the defined log folder.

Chapter 6: BitKinex

Introduction

Many FlashStats users have web sites hosted on remote servers. FlashStats needs to have local access to your web site's log files to analyze them. Therefore, the log files need to be downloaded from the remote web server onto the local FlashStats computer. FlashStats includes an FTP (File Transfer Program) utility called BitKinex to help automate this task.

BitKinex allows you download files from remote servers. (It can also upload files to remote servers, although FlashStats does not take advantage of that feature.)

Note:

This chapter about BitKinex does not apply to you if you do not need to download log files, or if you want to use a different FTP utility.

Installing BitKinex

At the end of the FlashStats setup routine there is a check box which allows you to run BitKinex setup. Be sure to select this check box so that the BitKinex setup program will run.

You can also manually run BitKinex setup at any point in the future by clicking on the Windows *Start* button, choosing *All Programs*, choosing *Maximized Software*, then choosing *Run BitKinex Setup*. Follow the prompts.

Data sources

Within BitKinex, you can define each remote server from which you will download files. Each server definition is called a *data source*. In fact, your local computer is also considered to be a data source. BitKinex knows how to open any two data sources and move files between them.

FlashStats automatically creates and manages a data source for your web site. You can edit the primary data source values (for example, the server name and user name used to log on to the server) directly within FlashStats. You can also edit the data source directly within BitKinex; simply select the data source, then open the *Data Source* menu and choose *Properties*.

If you are running FlashStats Professional Edition, you can have an unlimited number of web sites defined within FlashStats. FlashStats will create a BitKinex data source for each web site which is configured to use BitKinex for downloading its log files.

Your license for FlashStats Standard Edition or FlashStats Professional Edition includes a BitKinex serial number. In addition to using it with FlashStats, you can also BitKinex for any other purpose as desired.

Managing data sources

FlashStats will normally manage the data sources that it creates within BitKinex. However, if for some reason you need to manually make changes to or delete a data source you can do so from within the main BitKinex window.

Before manually editing the data source within BitKinex, you might want to try editing it from within FlashStats. To do this:

1. Make sure you have opened the correct web site within FlashStats.
2. Select the *Log Files* view.
3. Click *Select Log Folder*.
4. In step 1 of the Log Folder wizard, you should select the answer *Yes*. Click *Next*.
5. When you get to the second step of the wizard, enter as many values as you can in the provided fields, then click the *Edit All BitKinex Settings* button. FlashStats will cause BitKinex to display a window where you can edit all of the data source's settings. Click *OK* to close that window when you are done. Then return to and complete the Log Files wizard.

If you need to manually edit the data source within BitKinex, you will find it listed under the FTP node, then under the FlashStats node. Each web site that you have defined within FlashStats will have its own sub-node, and it will contain a further sub-node for the log folder.

For example, the first web site that you define within FlashStats will have the web site ID of "Website1", and its log folder will have the ID of "LogSet1". So the BitKinex data source will be located at Ftp / FlashStats / Website1 / LogSet1.

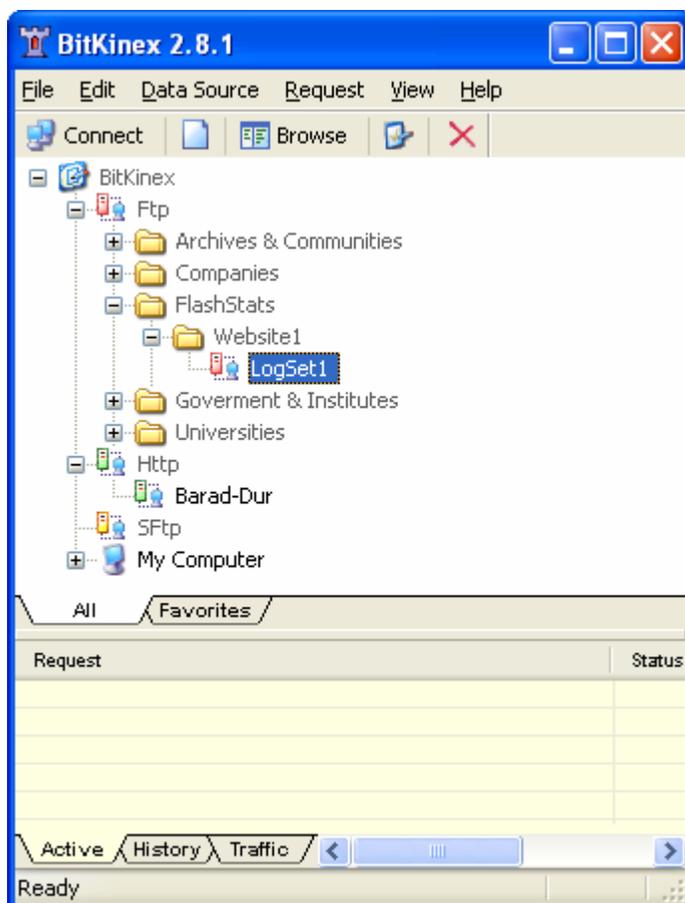


Figure 6-1 BitKinex main window

Disabling BitKinex

By default, FlashStats is able to use BitKinex to download your web site's log files if you so desire. However, you can configure FlashStats not to use BitKinex. If you disable BitKinex within FlashStats, then you will not be able to use the BitKinex-specific features of FlashStats. Please note that disabling BitKinex is a global setting, so if you are running FlashStats Professional Edition, then you will not be able to use BitKinex for *any* web site defined in FlashStats.

To disable the use of BitKinex within FlashStats, open the *Tools* menu and choose the *Options* command. Click on the *Other Options* tab, then clear the check box from the *Use BitKinex for downloading log files* option. See Figure 6-2 below. Click *OK* to close the *Options* window.

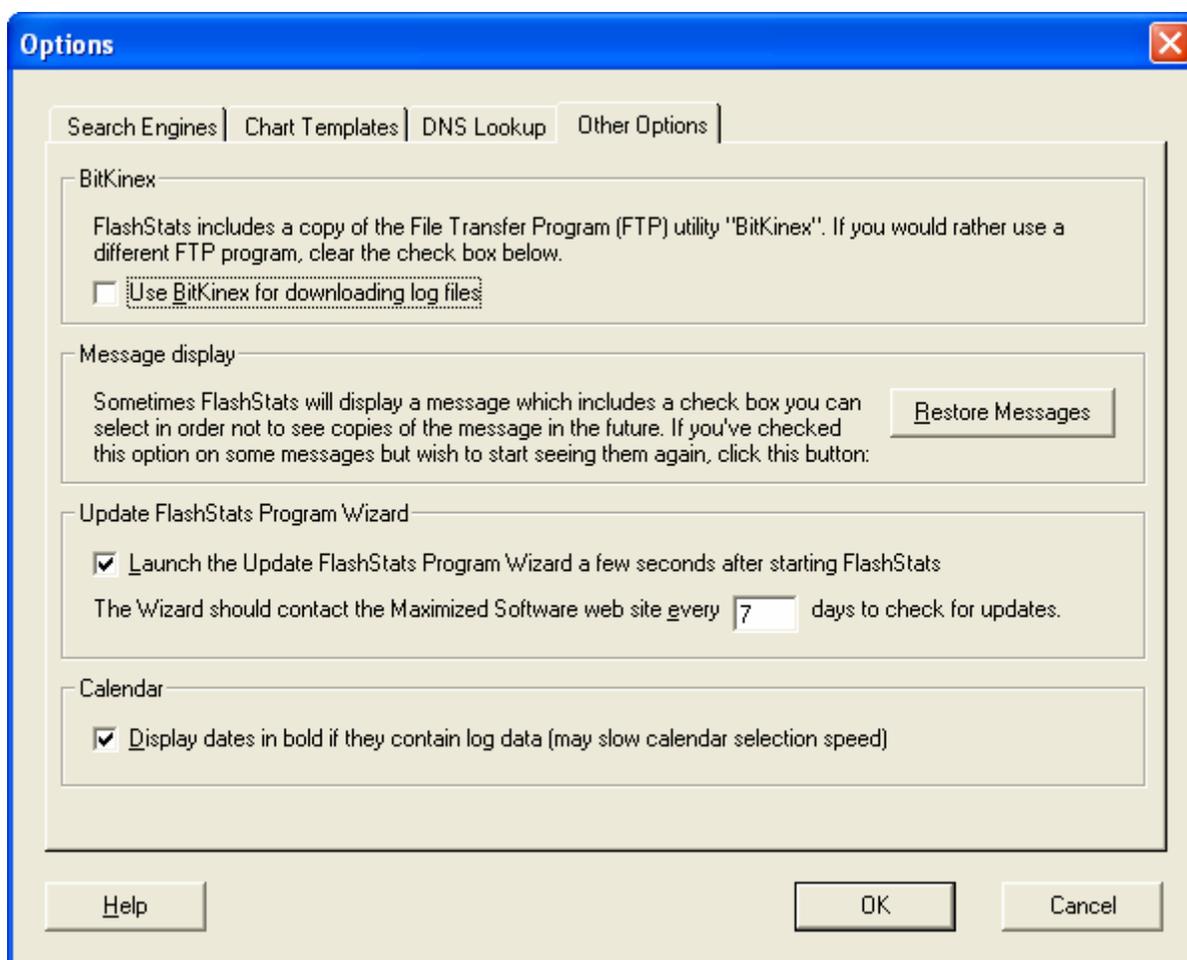


Figure 6-2 Disabling BitKinex within FlashStats

How to get more information

Full BitKinex documentation is available in three places:

1. Press F1 while in the BitKinex window. To start BitKinex you can choose *Run BitKinex* from the *Tools* menu in FlashStats.
2. Online documentation is available at the BitKinex web site. Visit <http://www.bitkinex.com> and go to the Support area.
3. Documentation is installed to your system when you install BitKinex. You can access this documentation by clicking the Windows *Start* button, choosing *All Programs*, choosing *BitKinex*, choosing the *Help* sub-menu, then choosing *BitKinex Help*.

Chapter 7: Spam referrers

Introduction

In order to drive traffic to their web sites, some owners of web sites will run programs which make requests to your web site and provide their web site as the referrer (in the HTTP header). When you run a Referrers report you will then see these "spam" referrers and you might be tempted to click on them to see what they are, thus driving up traffic to those sites.

In addition, many web sites innocently publish the reports (including referrer reports) generated by some log file analysis programs. Spammer sites try to flood these other sites with their referring URL so that it appears in those reports. The links back to the spammer make it look like more web sites are linking to the spammer, thus hopefully increasing their search engine ranking.

Due to the popularity of these techniques, spam referrers are proliferating rapidly. Many web sites get a huge amount of spam referrers every day. These spam referrers pollute your list of actual referrers, and they also inflate the hit count of the pages that they request.

Therefore, it's good to eliminate spam referrers. FlashStats provides the ability to filter out all traffic which includes spam referrers. If any hit within a visit includes a spam referrer, then the entire visit is ignored.

Note

FlashStats reports are safe to post to the Internet because they include the following tag:

```
<meta name="robots" content="nofollow">
```

This tag tells search engines not to count the links in the report as being relevant links, thus not inflating the link count of those URLs.

Managing the master list of spam referrers

FlashStats maintains a master list of spam referrers. When you create a report set, if any hit within a visit contains a referrer which is one of these spam referrers, then the entire visit is ignored.

Follow this procedure to edit the list of spam referrers:

1. Open the *Tools* menu and choose *Spam Referrers*. The *Spam Referrers* window opens; see Figure 7-1.

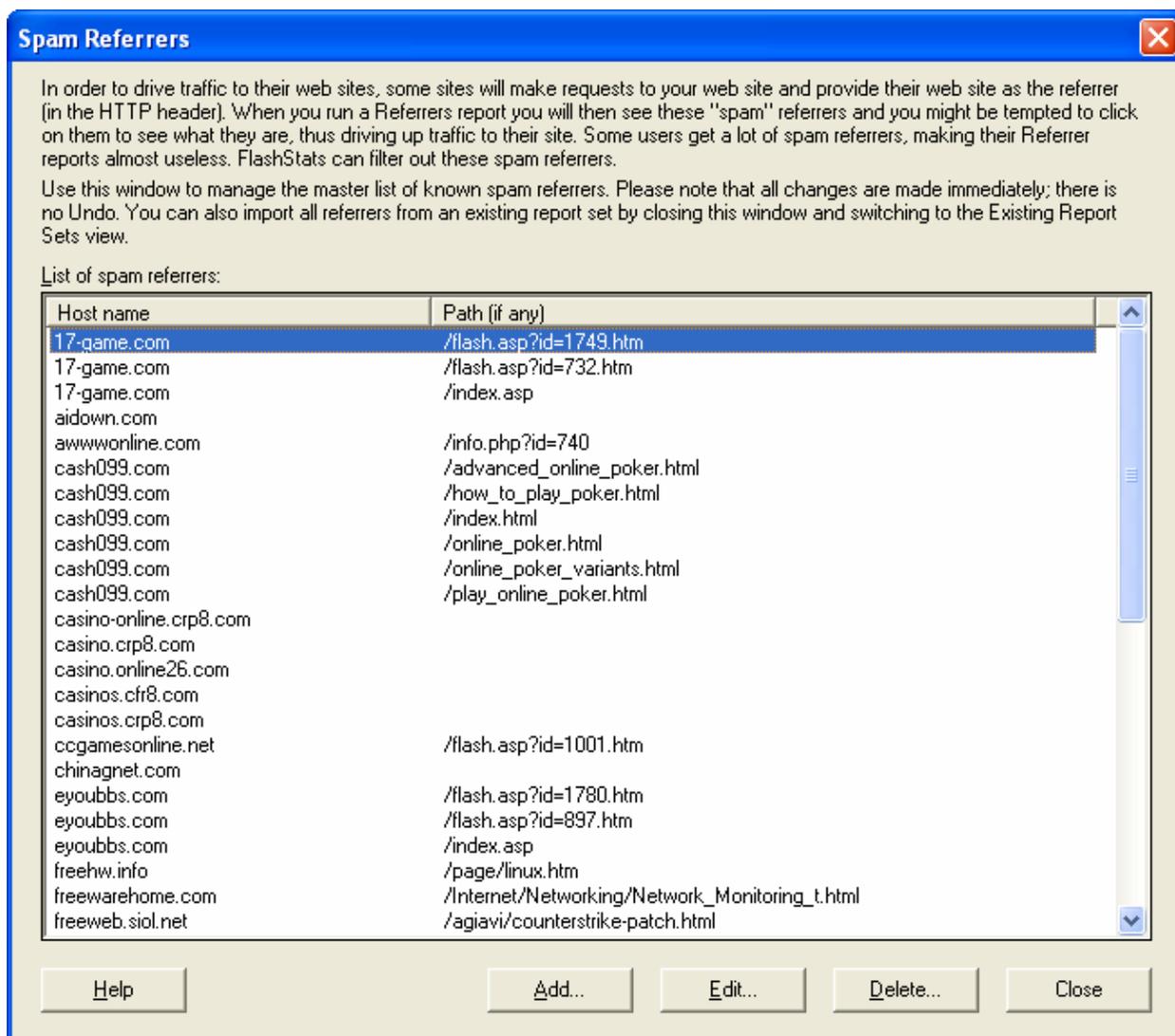


Figure 7-1 Spam Referrers window

2. The following buttons are available:

- *Add* - Click *Add* to define a new URL for inclusion in the master spam referrer list. See Figure 7-2.
- *Edit* - Select any individual entry then click *Edit* to edit it. See Figure 7-2.
- *Delete* - Select one or more entries then click *Delete* to remove them from the master spam list.



Figure 7-2 *Edit Spam Referrer* window

Figure 7-2 shows the *Edit Spam Referrer* window, which is used when adding or editing a spam referrer.

Server name - Specify the web site server name. When analyzing a referrer to see if it matches a spam referrer definition, FlashStats will try to match the referrer's host name. You can omit any leading www. or other sub-domain part.

Path pattern - Specify any path portion which follows the server name.

For example, if you define a server name of spammer.com and no path, then the following referrers would match:

```
http://www.spammer.com  
http://www2.spammer.com  
http://spammer.com  
http://spammer.com/AnyFile.ext
```

But a referrer such as http://otherspammer.com would not match since the server name did not match.

If you specify a path portion then it must exist and match for any given referrer to be considered spam. You can use pattern matching characters such as ? and * in the *Path pattern* field.

Importing spam referrers from a report set

In addition to manually defining spam referrers, you can import all referrers from a given report set and select the ones which are spam referrers. This method provides an easy way to define many spam referrers all at once.

To import spam referrers from an existing report set, first select the *Existing Report Sets* view. Select the desired report, then click *Import Spam Referrers*. The following window (Figure 7-3) appears:

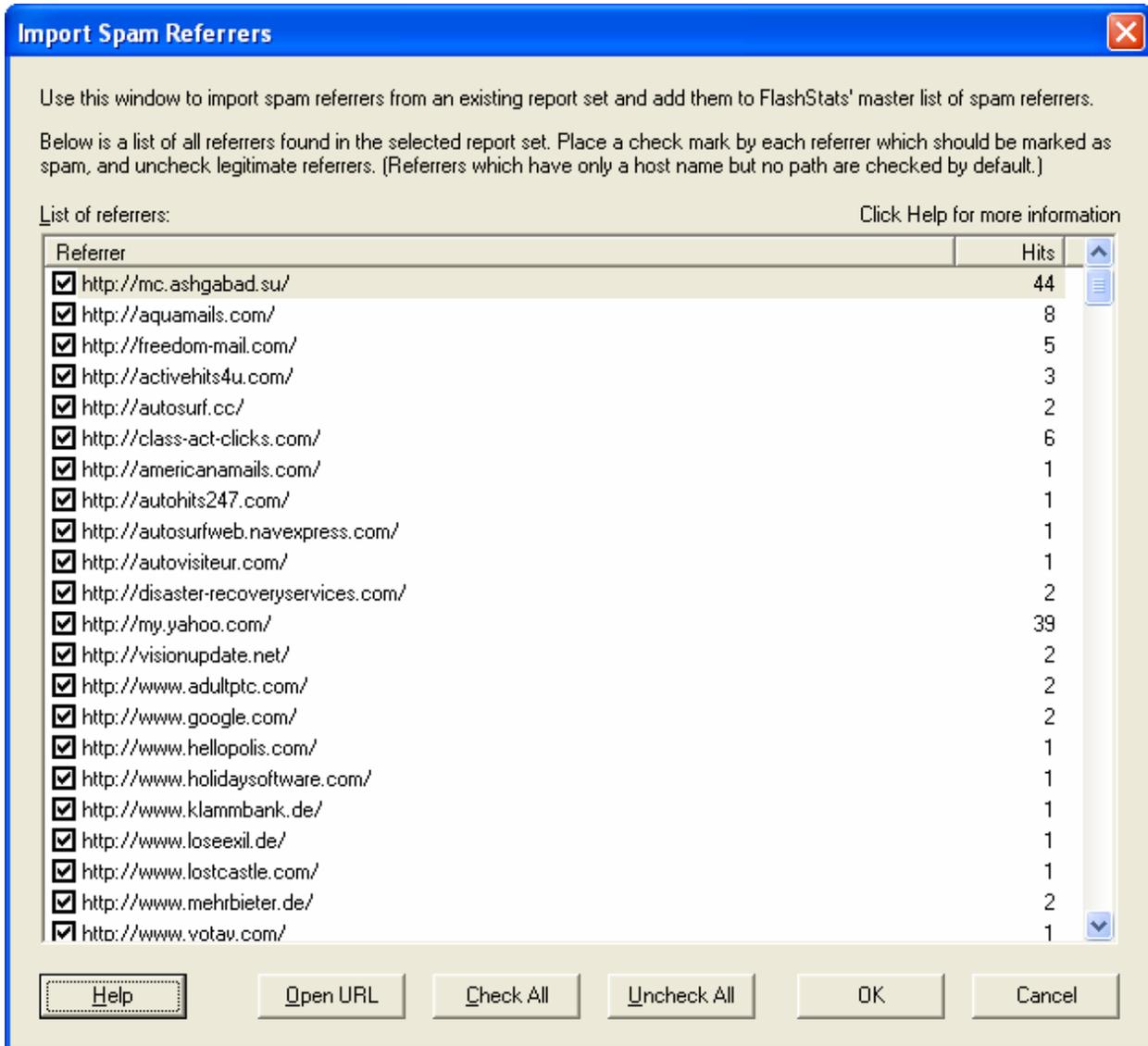


Figure 7-3 *Import Spam Referrers* window

This window lists all referrers found in the selected report(s). FlashStats will select by default any referrer which consists of just a host name but no path.

Carefully review the check mark on all URLs. You can click the *Open URL* button to view the web site of the currently selected referrer URL.

Note

Be careful when using the *Open URL* button to view a referrer URL, because the URL may point to a web site which tries to install malware on your computer.

When you are satisfied with your selections, click the *OK* button. All selected URLs will be added to the master list of spam referrers and will therefore not show up in any future reports.

The master spam list is used by all web sites analyzed by FlashStats.

You control whether spam referrers are removed for each web site defined within FlashStats. Open the *Web Site* menu and choose *Properties*. On the *Advanced* tab, select or clear the check mark in the *Ignore spam referrers* check box, as shown in Figure 7-4 below.

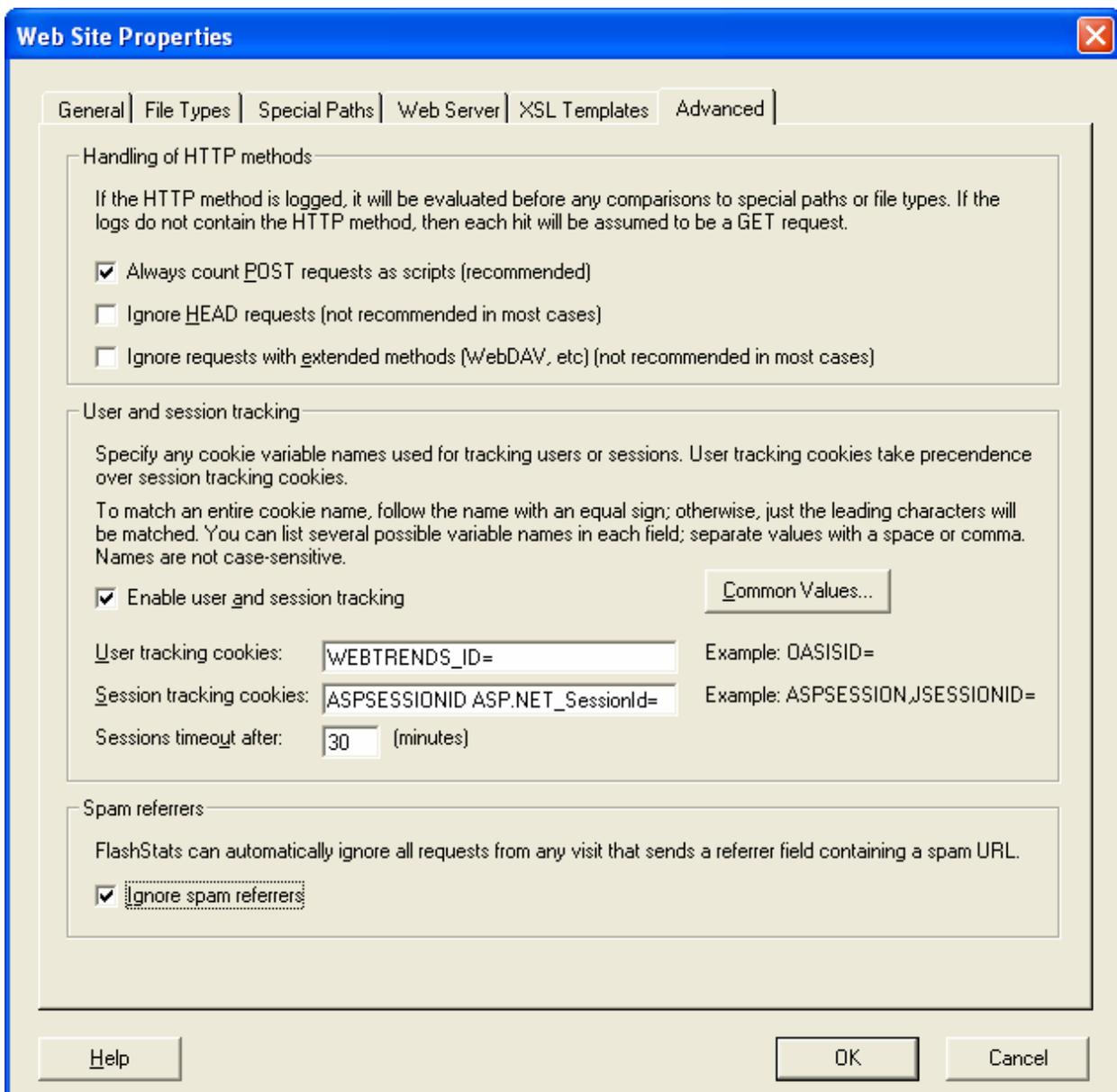


Figure 7-4 *Web Site Properties* window, *Advanced* tab

After editing the master list of spam referrers you will need to generate new reports in order to get new results which omit the spam referrers. Previously existing reports are not updated to reflect the new contents of the master spam list.

Adding spam referrers using drag and drop

If you are looking at any of the FlashStats reports which list referrers (such as the Referrers report) you will notice a small red circle icon in each row: . You can drag this icon and drop it onto the FlashStats window to automatically add the given referrer to the master spam list. (Be sure that the *New Report Set* view is selected before dropping the icon onto the FlashStats window.).

Chapter 8: Updating FlashStats

Introduction

FlashStats stores configuration information in several XML files, and includes built-in procedures for updating these files. This chapter explains how to update the FlashStats configuration files, as well as how to check for a new version of the FlashStats program file itself.

Checking for and downloading new configuration files

You should occasionally use the following procedure to see if new configuration files have been made available.

1. Open the *Tools* menu and choose the *Update Configuration Files* command. The window in Figure 8-1 appears.

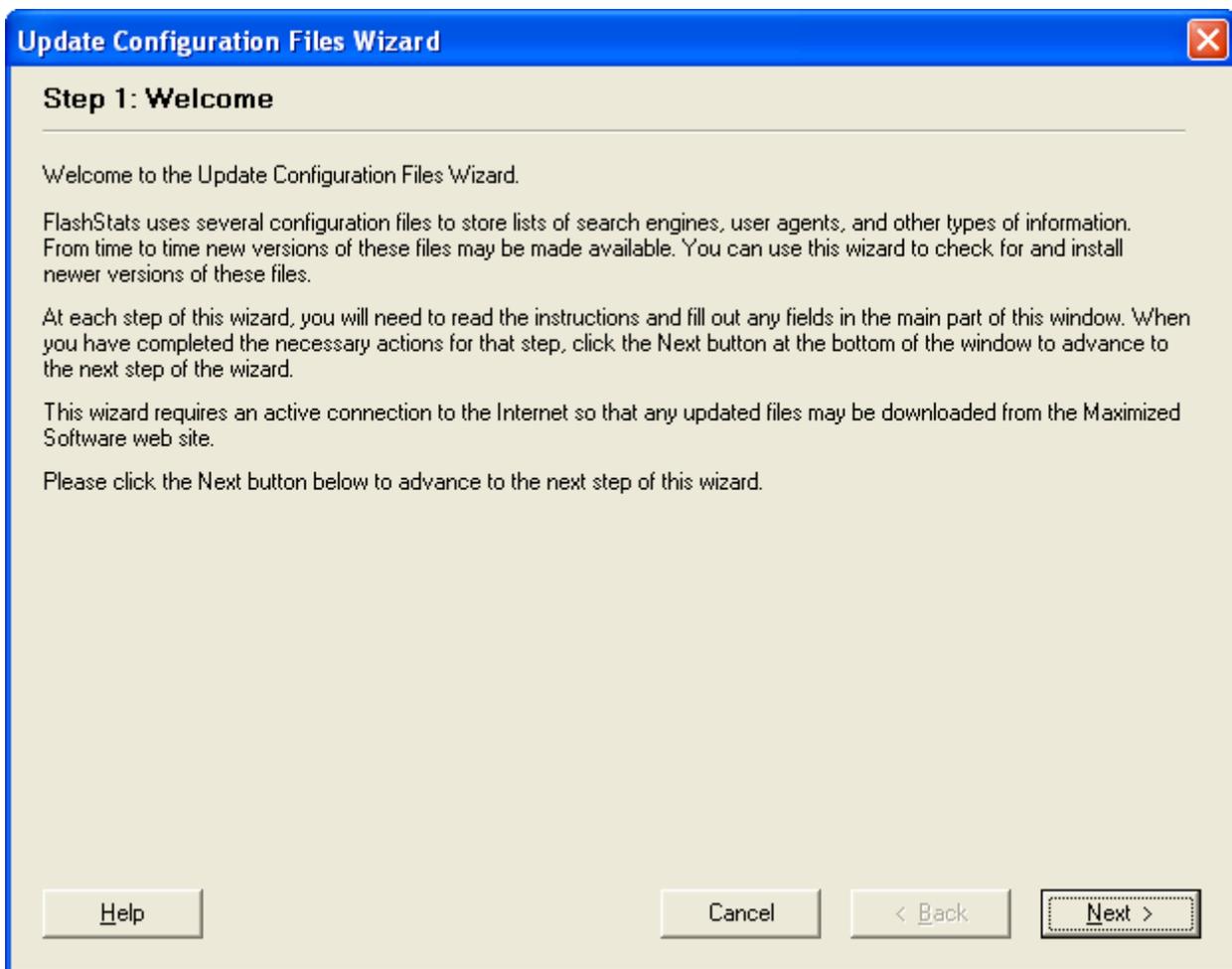


Figure 8-1 Update Configuration Files wizard, step 1

2. Read the information in this window, then click the *Next* button to continue.
3. The next step consists of downloading the list of current configuration files from the Maximized Software web site so that it can be compared to the configuration files currently used on your computer. Click the *Download List of Configuration Files* button to perform this download.
4. After the list of files has been downloaded the window will look like Figure 8-2 below. Click *Next* to continue.

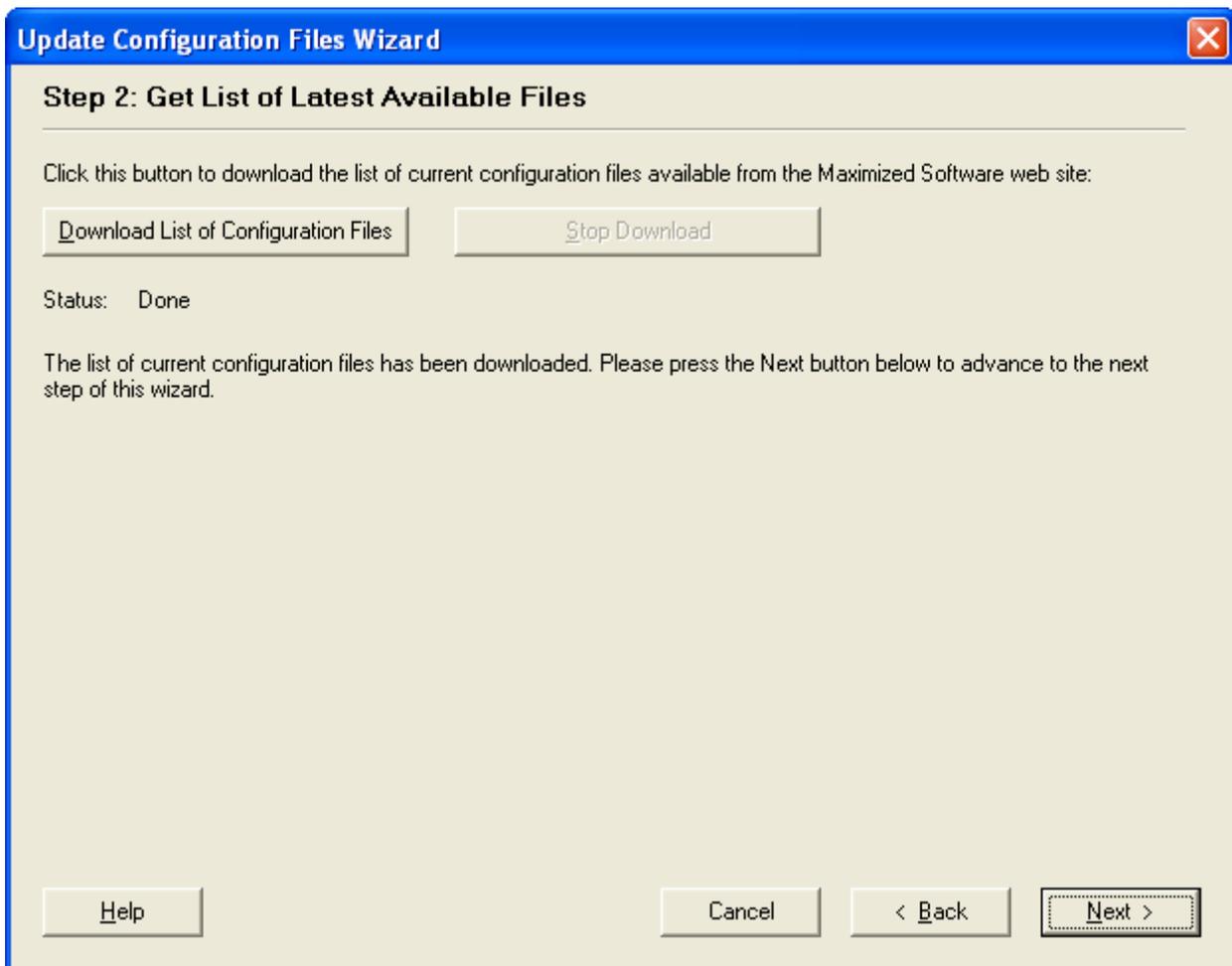


Figure 8-2 Update Configuration Files wizard, step 2

5. FlashStats will now analyze whether any of your configuration files should be updated with newer versions from the Maximized Software web site. The details and recommendations will be displayed in step 3 of the wizard as shown in Figure 8-3 below.

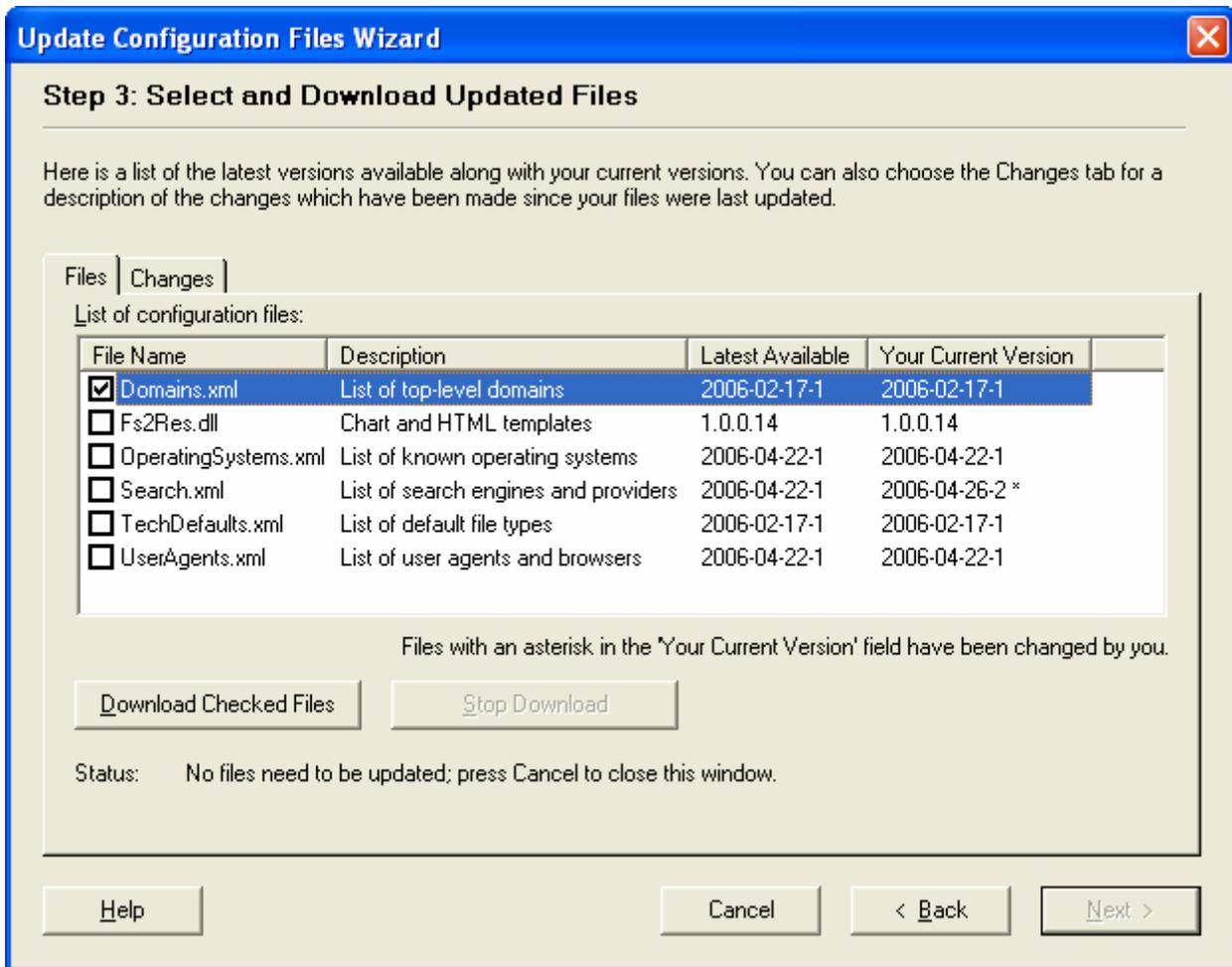


Figure 8-3 Update Configuration Files wizard, step 3

- FlashStats compares the version number of the latest version of each file to the version number of the same file currently being used on your system. If a newer version is available, then the check box next to the file will be selected by default. If no newer version is available, then the check box will be cleared.

The check box next to each file name controls whether the next step of the update wizard will download and install a new version of the file.

- Review the default check marks. Be sure to select the check box next to any file that you wish to update with a newer version from the Maximized Software web site, and to clear the check box next to any file that you do not want to update.

You can choose the *Changes* tab to view the changes made to each configuration file.

Note

If you have modified your search engine and search provider definitions, then you may not want to update your copy of Search.xml, which is the file which contains the search engine and search provider definitions. Downloading and using a newer version from the

Maximized Software web site will overwrite your existing Search.xml file, thus causing you to lose your changes. Click on the *Changes* tab to see what changes have been made to Search.xml and see if you still want to replace your copy of Search.xml. If you have made relatively simple changes then you may want to download the new version then make your changes again to the new version.

8. If you do not want to download any updated files, you can close the wizard by clicking the *Cancel* button. Otherwise, after reviewing the check boxes as discussed in step 7 above, click the *Download Checked Files* button to begin downloading the selected files. After the files have finished downloading, the wizard will look like Figure 8-4. Click *Next*.

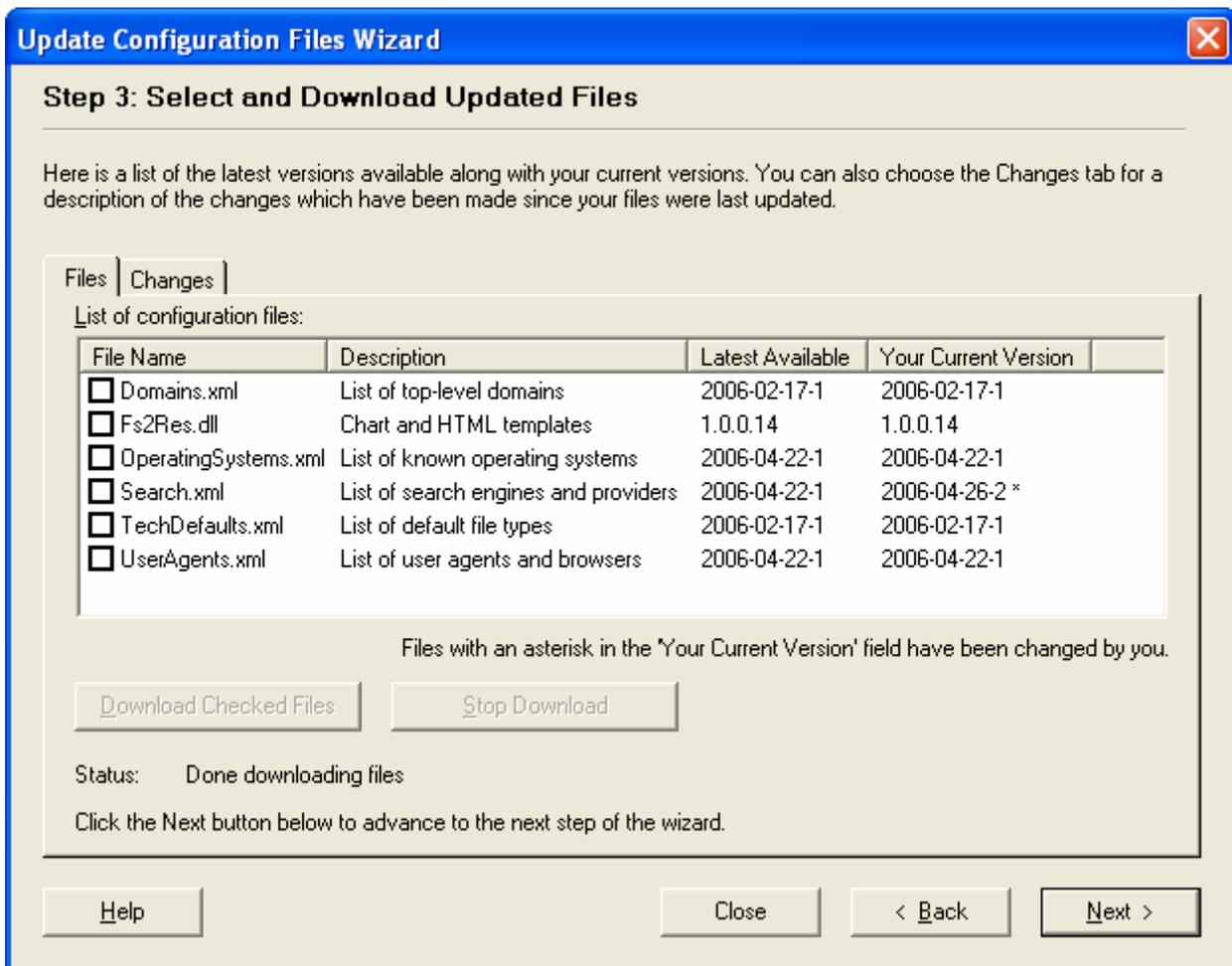


Figure 8-4 Update Configuration Files wizard, step 3 after downloading files

9. If you did not download a new version of Fs2Res.dll, then click *Finish* to exit the wizard.

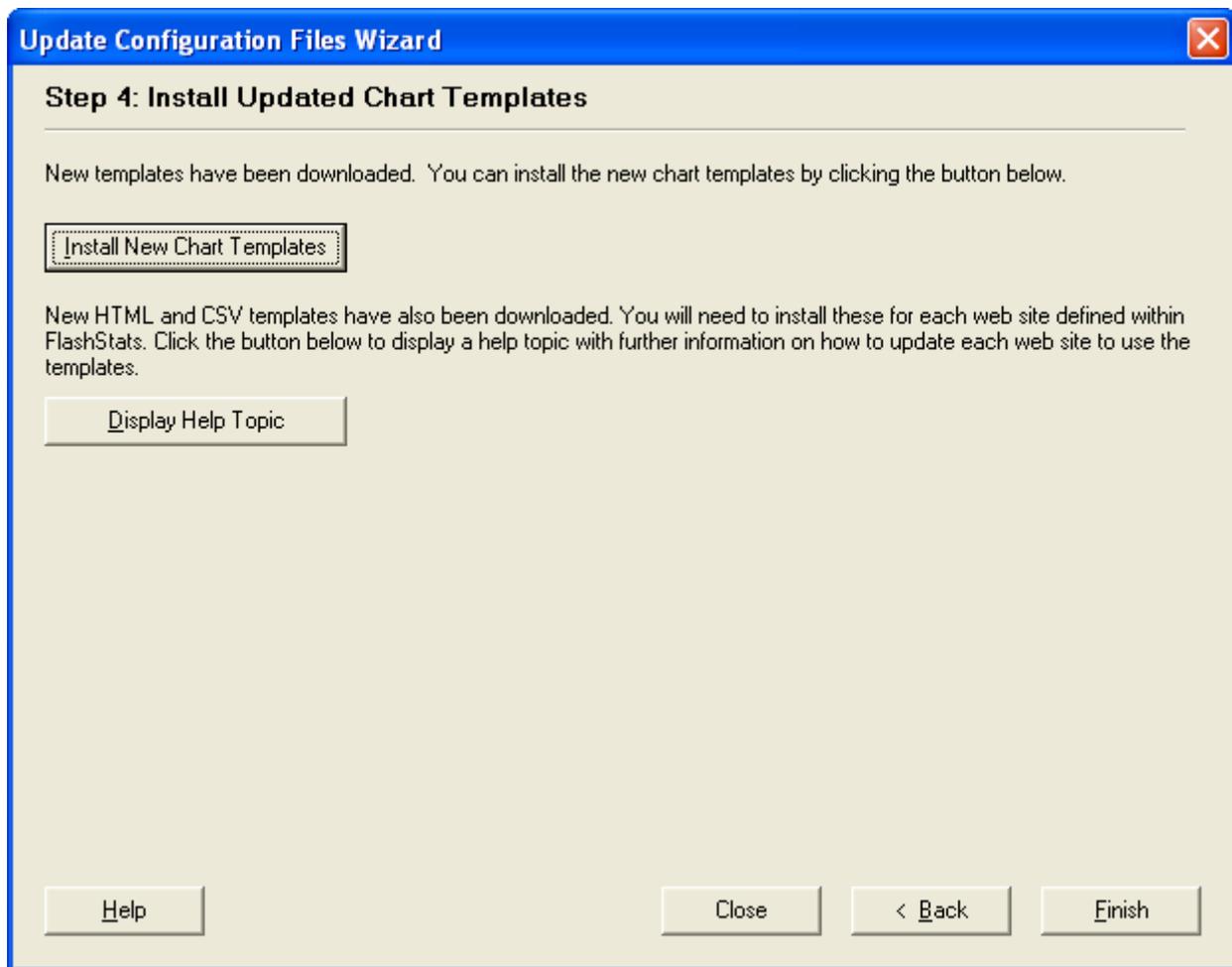


Figure 8-5 Update Configuration Files wizard, step 4 after downloading Fs2Res.dll

10. If you have downloaded an updated version of Fs2Res.dll you will have new chart templates and XSL templates, and step 4 of the wizard will look like Figure 8-5. Click the *Help* button for more information on installing the updated templates. After installing the new chart templates, click *Finish* to exit the wizard.

Updating chart templates

FlashStats uses chart templates when generating charts. These chart templates are shared by all web sites defined within FlashStats. Normally you will only replace your existing templates when you download a newer version of Fs2Res.dll as part of the Update Configuration Files wizard, as described above.

However, you can always manually re-install the current chart templates from your copy of Fs2Res.dll. To do so:

1. Open the *Tools* menu and choose the *Options* command.

2. Click the *Chart Templates* tab.
3. Click the *Install Chart Templates* button.

Updating XSL templates

FlashStats uses XSL templates when generating HTML, Word, and CSV output. Each web site defined within FlashStats has its own set of XSL templates. Advanced users can edit their XSL templates if desired.

Normally you will only replace your existing templates when you download a newer version of Fs2Res.dll as part of the Update Configuration Files wizard.

However, you can always manually re-install the current XSL templates from your copy of Fs2Res.dll. To do so:

1. Make sure that you have opened the desired web site. Open the *Web Site* menu and choose the *Open* command. Select the desired web site then click the *Open* button.
2. Open the *Web Site* menu and choose the *Properties* command.
3. Click the *XSL Templates* tab. See Figure 8-9 below.

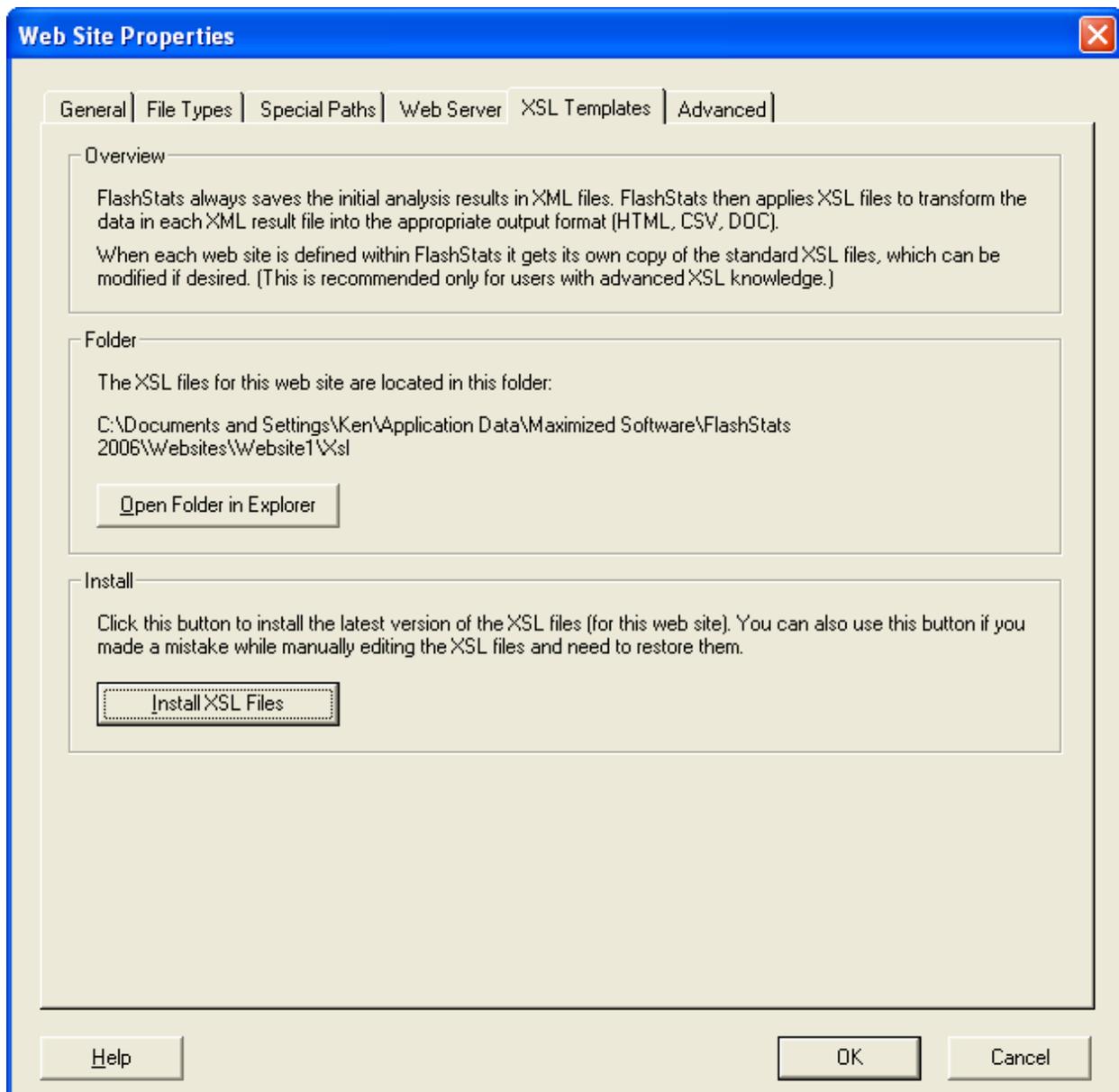


Figure 8-6 Web Site Properties window, XSL Templates tab

4. Click the *Install XSL Files* button.

If you are using FlashStats 2006 Professional Edition and have multiple web site defined, repeat this procedure for each web site whose XSL templates you wish to re-install.

Updating the FlashStats 2006 Program

From time to time, a new version of FlashStats 2006 may be released. You can have FlashStats automatically check the Maximized Software web site to see if any updates are available, and you can also manually perform this check at any time.

To manually check for a new version of FlashStats 2006:

1. Open the *Tools* menu. Choose the *Update FlashStats Program* command. The following window will appear:

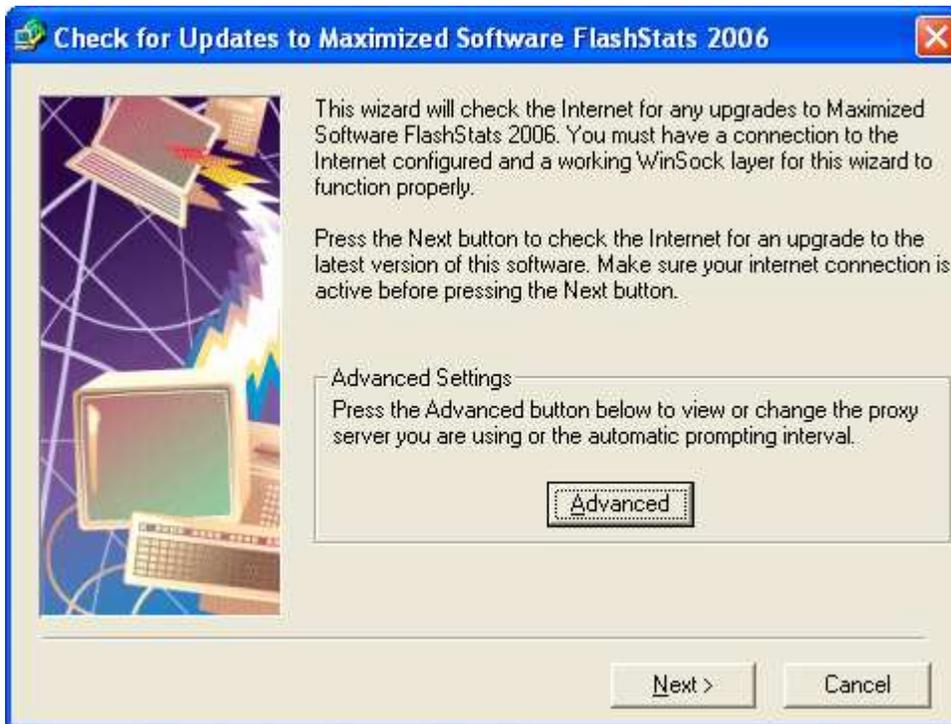


Figure 8-7 Update FlashStats Program wizard window

2. Click the *Next* button. The Maximized Software web site will be contacted to see if there is a new version of FlashStats available. (No information will be sent which identifies you or your system.)
3. You will be told whether or not a new version of FlashStats is available. If so, you can easily download and install the new version.

Advanced settings for the Update FlashStats Program wizard

If the Update FlashStats Program wizard cannot connect to the Maximized Software web site, you should press the *Advanced* button. The following window (Figure 8-8) will allow you to configure whether the wizard uses a proxy server. Contact your network administrator for information on how to complete this window.

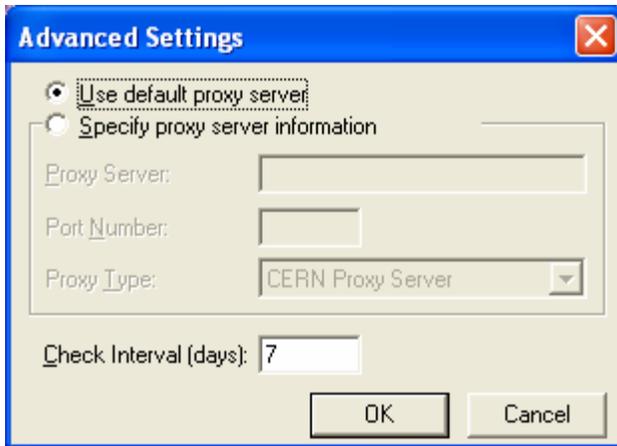


Figure 8-8 Update FlashStats Program wizard *Advanced Settings* window

Configuring the Update FlashStats Program wizard

You can configure the Update FlashStats Program wizard in the main *Options* window. Open the *Tools* menu, then choose the *Options* command. Click the *Other Options* tab, and the window will look like Figure 8-9.

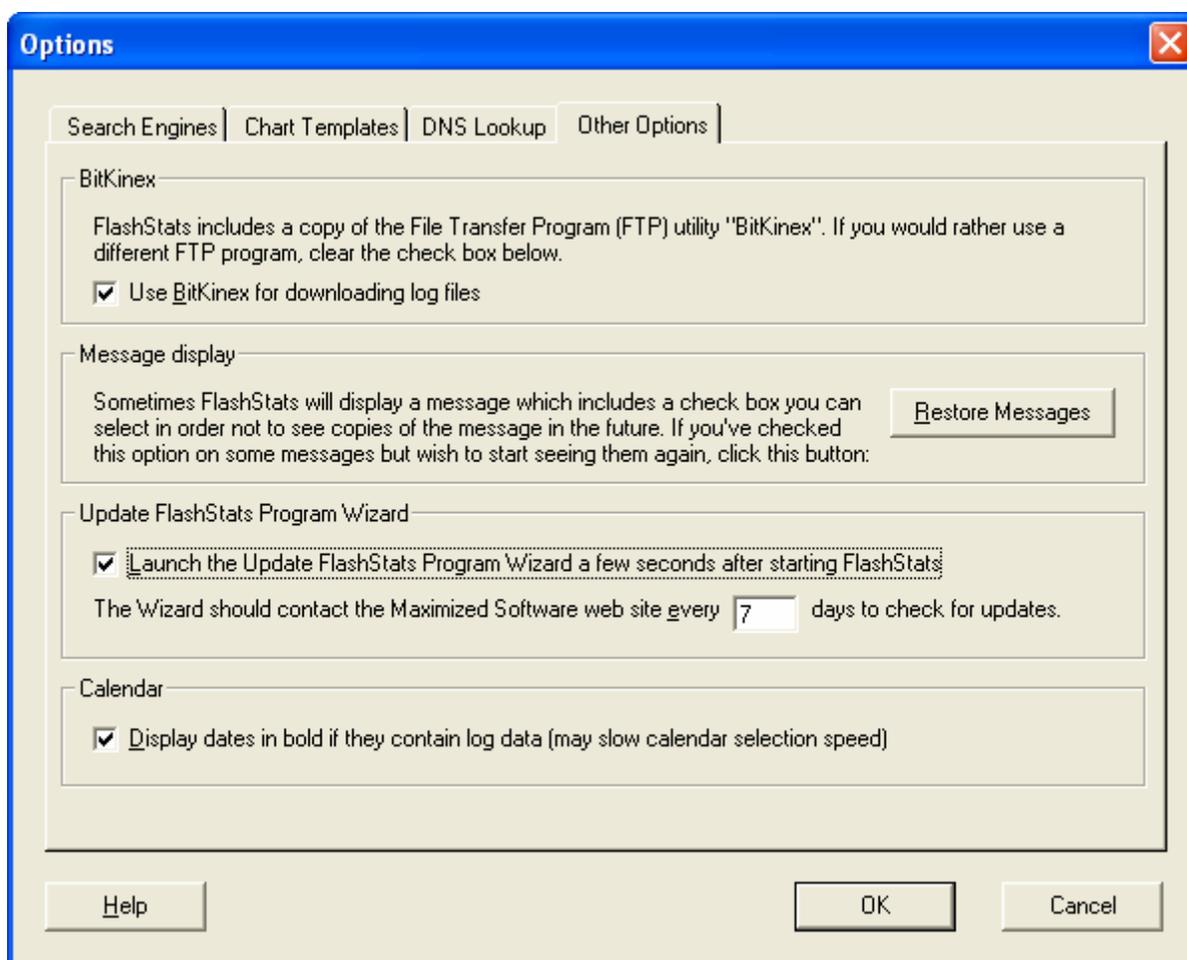


Figure 8-9 Options window, Other Options tab

In the *Update FlashStats Program Wizard* box, choose your settings:

- If the *Launch update checker a few seconds after starting FlashStats* check box is selected, then the update checker will automatically be launched each time you start FlashStats. If the check box is cleared, then the update checker will never be automatically started and you will be responsible for manually checking for program updates as described above.
- In field labeled *The wizard should contact the Maximized Software web site every X days to check for updates*, enter the number of days for how often the update checker will contact the Maximized Software web site to see if a new version of FlashStats is available. (However, if the wizard is never launched then this value has no effect.)

Keep in mind that these two values work separately. If the check box is selected then the wizard will run every time that you start FlashStats. When the wizard runs, the main FlashStats window will appear to lose focus for a moment. During this moment, the wizard determines the last time that it contacted the Maximized Software web site and whether enough days have passed that it should contact it again. If so, the window in Figure 8-7 above is displayed. Otherwise, the wizard silently finishes, without ever having displayed anything on your screen. At this point the

FlashStats window will regain the focus. If this momentary loss of focus is disconcerting, then you can prevent the wizard from launching by clearing the check box as described above. If you do so, please remember to occasionally perform a manual check for updates.