

# G-Lock SpamCombat



---

# Table of Contents

## Introduction

Features and Benefits .....	5
Minimum Requirements to use SpamCombat .....	8
How to Install and Uninstall SpamCombat.....	9
How to Backup and Restore Profile .....	10
SpamCombat Overview .....	11
Quick Startup.....	19

## Account Settings

General Settings.....	24
Advanced Settings .....	32
Importing Accounts .....	34

## SpamCombat Settings

General Settings.....	37
Automation Settings.....	39
Hot Keys Configuration .....	41
Internal Mail Server .....	42
Color Theme and Font Size.....	45
Customizing Menus and Toolbars .....	47
Customizing Message Preview Screen .....	51

## Complex Filters

Adding Complex Filter.....	55
Creating Script .....	59

## **Whitelist**

Adding Emails to Whitelist .....	79
Working with Whitelist .....	84

## **Blacklist**

Adding Emails to Blacklist .....	87
Working with Blacklist.....	92
Blocking Spam by Country of Origin.....	95

## **HTML Validator**

Working with HTML Validator .....	104
-----------------------------------	-----

## **Bayesian Filter**

Working with Bayesian Filter .....	106
Bayesian Filter Settings .....	108
Ignore List.....	111

## **DNSBL Filter**

Working with DNSBL Filter.....	112
DNSBL Filter Settings .....	115

## **Working with Emails**

Sorting and Filtering Emails .....	117
Managing Deleted Emails .....	124
Recovering Deleted Emails .....	128
Working with SpamCombat in System Tray .....	130
Test Regular Expressions.....	132
About Regular Expressions .....	133
SpamCombat Command-Line Switches .....	142

## Viewing SpamCombat Statistics

General Table .....	143
Assembled Diagram.....	147
Filters Rating .....	148
Bayesian Efficiency .....	149
SpamCombat Efficiency .....	150
Email Traffic .....	151

## Features and Benefits

Spam emails have become an ever increasing problem, and nowadays it is practically impossible to use email without receiving spam in large amounts. G-Lock SpamCombat is your powerful solution for clearing your Inbox from spam, virus, and junk emails.

SpamCombat benefits:

- Catches and deletes spam BEFORE it reaches your inbox
- Self learns based on your spam and good email and adapts to new types of spam
- Detects spam with great precision and accuracy
- Stops viruses and malicious code
- Safe email preview - no pictures are downloaded, no hidden scripts or codes are executed
- Cuts down unproductive email traffic and saves bandwidth
- Filters email from multiple email accounts
- Can work in a fully automatic mode
- Provides an easy way of recovering deleted emails
- Allows you quickly save and restore your profile (accounts and filters settings)
- Has a very customizable user interface
- Provides comprehensive statistics graphs
- Helps save your money and valuable time

SpamCombat uses a powerful set of filters to prevent spam from entering your Inbox: Complex Filter, Whitelist, Blacklist, HTML Validator, DNSBL filter, and the Bayesian filter.

**Complex Filter** lets you write a script containing different functions, procedures, or operators to compare any header fields to the specified value and classify the email as spam or good depending on the result.

For your convenience and saving time, SpamCombat lets you '**whitelist**' emails you receive from known senders: primarily newsletters you subscribed to, messages from newsgroups, and other informative letters. Opposite to the whitelist there is the '**blacklist**' to which you can add suspicious, unknown or unwanted emails or their senders. The messages can be whitelisted or blacklisted based on any words from the message header and/or body, and on the sender's IP address. SpamCombat is provided with a solid Blacklist, which allows catching the most known kinds of spam and virus emails.

**HTML Validator** is a filter that parses the HTML part of the incoming email and checks the HTML tags for validity. If xx dubious HTML tags are found, the message is considered spam.

**DNSBL filter** consists in comparing the senders' IP addresses against a list of known spam databases using Public Blacklists (also called DNSBL lists). These databases are maintained and updated daily.

The **Bayesian filter** is the most powerful anti-spam filter based on the analysis of the message content and mathematical calculation of spam. The advantage of the Bayesian filter is that it can be trained by each individual user by categorizing each received email as either spam or good; after you categorized a few emails the filter begins classifying the emails by itself. If the filter makes a mistake, you re-categorize the email.

The filter learns from its mistakes. The accuracy of the Bayesian filter increases with time. "Well trained" filter can determine up to 99.5% of spam emails coming into your inbox.

SpamCombat lets you preview incoming emails in the following formats: HTML, Message Source, and Message body (decoded message). HTML preview is absolutely safe. No pictures are actually downloaded, no hidden scripts, or codes are executed. When you preview the emails retrieved by SpamCombat, no notice to the email senders is sent letting them know that the email was opened or read. Thus, nobody will know whether your email address is valid or not if you don't want it.

SpamCombat ensures the efficient and easy control under incoming emails!

## Munimum Requirements to Use SpamCombat

No Apple Macintosh or Linux version of SpamCombat is available.

The minimum requirements to run SpamCombat are:

Computer:	Pentium III or higher *
Operating System:	Windows 98, NT, 2000, XP, Vista, 7
Memory:	128 megabytes
Disk Space:	5 megabytes
Video:	256 colors **
Internet Connection:	The faster, the better ***

\* Performance of SpamCombat is relative to the speed of your computer and the amount of memory (RAM) you have in your PC. These requirements are considered minimum, not ideal.

\*\* Note that SpamCombat is designed to look and perform best with 16-bit color and normal fonts. If you are running at 256 colors, SpamCombat will run considerably slower because your computer spends a great deal of resources adjusting the colors to a 256 color palette. If you are running your computer with 'LARGE FONTS' enabled, SpamCombat may not display correctly.

\*\*\* The speed and quality of your Internet connection will determine how fast processing incoming messages is performed.

## How to Install and Uninstall SpamCombat

To install SpamCombat:

1. Create a temp directory on your hard drive.
2. Unzip spamcombat.zip to this directory.
3. Run the spamcombat\_setup.exe file.
4. Follow the steps of the setup guide.

To uninstall SpamCombat:

Choose **Uninstall** from the SpamCombat program group. Or:

1. Open the Control Panel (under the Start menu choose Settings -> Control Panel).
2. Double-click on **Add/Remove Programs** icon.
3. Search in the list for G-Lock SpamCombat and double-click on it.

💡 **Tip:** If the above procedures do not uninstall SpamCombat, do this: click Start -> Run, type 'regedit' and click OK. You will see the Registry Editor. Search for SpamCombat registry and delete it (HKEY\_CURRENT\_USER\Software\G-Lock Software\SpamCombat). Then delete manually the directory, to which the SpamCombat was installed. This will remove the SpamCombat from your PC completely.

## How to Backup and Restore Profile

G-Lock SpamCombat provides you with a quick and easy way to backup and restore your profile (accounts and filters settings). It is very useful option if you would like to move the program on another computer or simply re-install it. You can save a backup of all your data and restore it in the new program installation at any time.

To backup the profile:

1. Click on **File** menu.
2. Select **Backup Profile**.
3. Specify the file on the disk to save a backup.
4. Click **Backup**.
5. Click **Close** when finished.















To restore the profile:

1. Click on **File** menu.
2. Select **Restore Profile**.
3. Specify the file on the disk with the data backup.
4. Click **Restore**.
5. Click **Close** when finished.

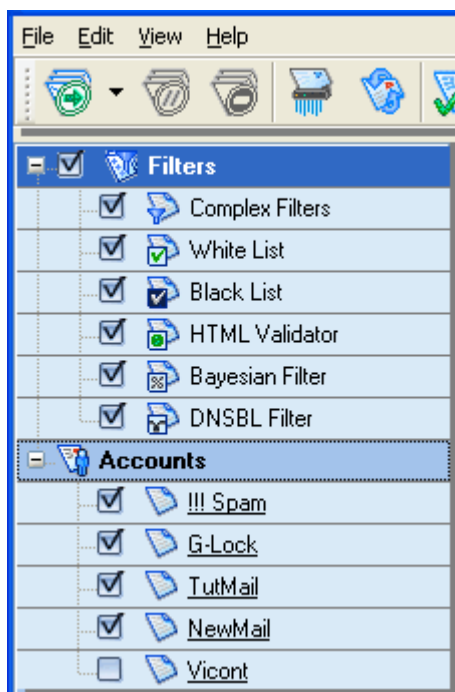
💡 **Important!** The **Restore** operation has no Undo option. If you use the Restore operation, your current workplace in G-Lock SpamCombat will be overwritten by the data from backup.


# SpamCombat Overview

Program toolbar:

	<b>Start</b> - start retrieving emails from the mail server
	<b>Pause</b> - pause the program. When SpamCombat is paused, you can edit the filters as you like. When you re-start the program, it will continue processing emails using the updated filters.
	<b>Stop</b> - stop retrieving emails from the mail server
	<b>Delete</b> - delete selected emails from the mail server
	<b>Settings</b> - configure SpamCombat settings
	<b>Launch Email Client</b> - open your email client
	<b>Clear MessageID Cache</b> - remove the messages ID from the program's cache. To avoid processing the same email twice, the program saves the ID of processed messages to its internal cache. To reprocess the same emails, clear the message cache before you click <b>Start</b> button
	<b>View/Hide Left Pane</b> - view/hide the program's left pane
	<b>View/Hide Top Accounts Pane</b> - view/hide the accounts statistics
	<b>Toggle Sound On/Off</b> - switch on/off a sound notification when new good or unknown messages arrive
	<b>Filters</b> - add and edit the filters: Complex Filters, Whitelist, Blacklist, HTML Validator, DNSBL and Bayesian filter
	<b>Statistics</b> - view the SpamCombat statistics
	<b>Deleted Items</b> - show deleted messages
	<b>Help</b> - bring up the SpamCombat guide

The program main window is separated into two panes. At the left pane are the SpamCombat's filters: Complex Filter, White List, Black List, HTML Validator, Bayesian Filter, and DNSBL Filter. There is the Accounts section too.



You can hide the left pane if you want more space for viewing the emails. To hide the program's left pane, click  **View/hide Left Pane** button on the Toolbar.

## Filters

SpamCombat is provided with a set of powerful filters to block spam emails from slipping into your Inbox.

**Complex Filter** lets you write a script using a wide range of functions, procedures, and operators to filter your incoming emails and classify them as spam and clean.

**Whitelist** allows the SpamCombat to automatically classify the emails as good.

**Blacklist** stands opposite the Whitelist. All the emails that come under any of the Blacklist conditions are automatically marked as spam.

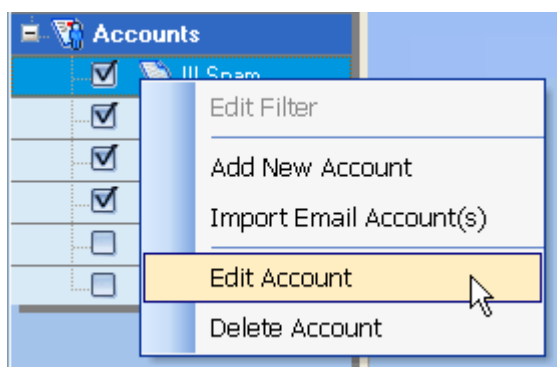
**HTML Validator** parses the HTML part of the incoming email and checks the HTML tags for validity. If a number of dubious HTML tags are found, the message is considered spam.

**Bayesian filter** is the most powerful filter that allows catching up to 99.5% of spam emails basing on the analysis of the message content and mathematical calculation of spam.

**DNSBL filter** consists in comparing the sender's IP address against Public Blacklists. If the IP address is listed within a spam database, the email is flagged as spam.

## Accounts

In the Accounts section you can manage your accounts. Click the right mouse button and select the appropriate option from the popup menu to add, import, edit, or delete an account.



To change the order of the accounts, select an account, then hold down Ctrl button on the keyboard and use the buttons with up and down arrows to move the account up or down.

The right pane is separated into 3 screens.

The top screen shows the accounts statistics. The arrow at the left of the Accounts pane indicates the account that is currently in focus. If you click the right mouse button, you can choose the option to either edit or delete the appropriate account:

Account	Total	Marked	Retrieved	Status	Total Size	Last Checked	Found Spam
G-Lock	0		0	No messages	0.00 Kb	1/16/2004 2:17:00 PM	0
!!! Spam	0	0	0	No messages	0.00 Kb	5/26/2004 11:11:11 AM	0
TutMail	2	1	2	OK	12.34 Kb	1/16/2004 11:11:11 AM	1
NewMail	5		5	OK	82.36 Kb	1/16/2004 11:11:11 AM	0

**Account** - account name

**Total # of Messages** - total of emails on the account

**Marked** - number of emails flagged as spam


**Retrieved Headers** - number of message headers retrieved from the mail server

**Status** - current account status

**Total Size** - total size of all the emails from the account

**Last Checked** - date and time when the account was last checked

**Found Spam** - number of emails SpamCombat classified as spam

To hide the top screen, click  **View/Hide Accounts Pane** button on the program's Toolbar. Or, select View/Hide Accounts Pane option under View menu.

The grid shows you incoming emails and their details. The arrow at the left of the pane indicates the message that is currently in focus:

Status	Country	Account	Size	From	Subject	Date
<input type="checkbox"/> U: Bayesian: 50	United States	TutMail	7.65 Kb	"TUT.B...	Mobile Offi...	12/30/1899
<input checked="" type="checkbox"/> S: Dubious HTM...	United States	TutMail	4.69 Kb	"RASM...	14.11.2003	11/13/2003 ...
<input type="checkbox"/> N: Bayesian: 0	Canada	NewMail	19.08 Kb	"ACD S...	IZone Web...	11/13/2003 ...

The icons legend:

✓ email is resolved as normal (N)

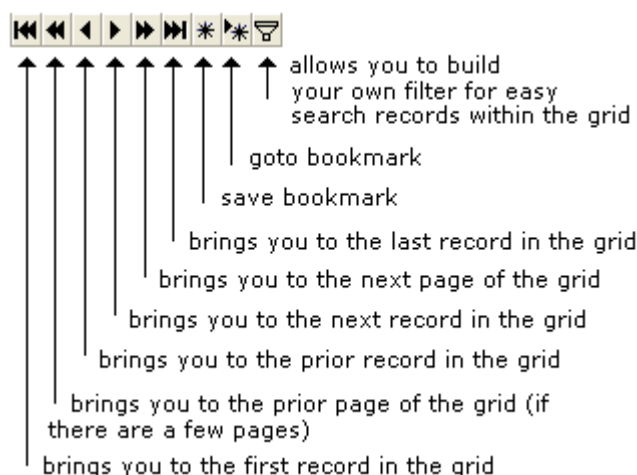
✗ email is resolved as Spam (S)

! email is flagged as unknown (U). Though it passed through the filters, the email was not resolved because the Bayesian filter is not trained. Click either Mark as Spam or Mark as Good button to categorize the email

? email is not resolved because of a bad Internet connection (message header is empty). Such emails should be re-scanned

~ email has not enough significant words to be processed by the Bayesian filter. Such emails should be either whitelisted, or blacklisted

At the bottom of the grid there is a range of useful buttons:








You can also use the Message Control toolbar to work with incoming messages:

✓ Mark Message as Clean

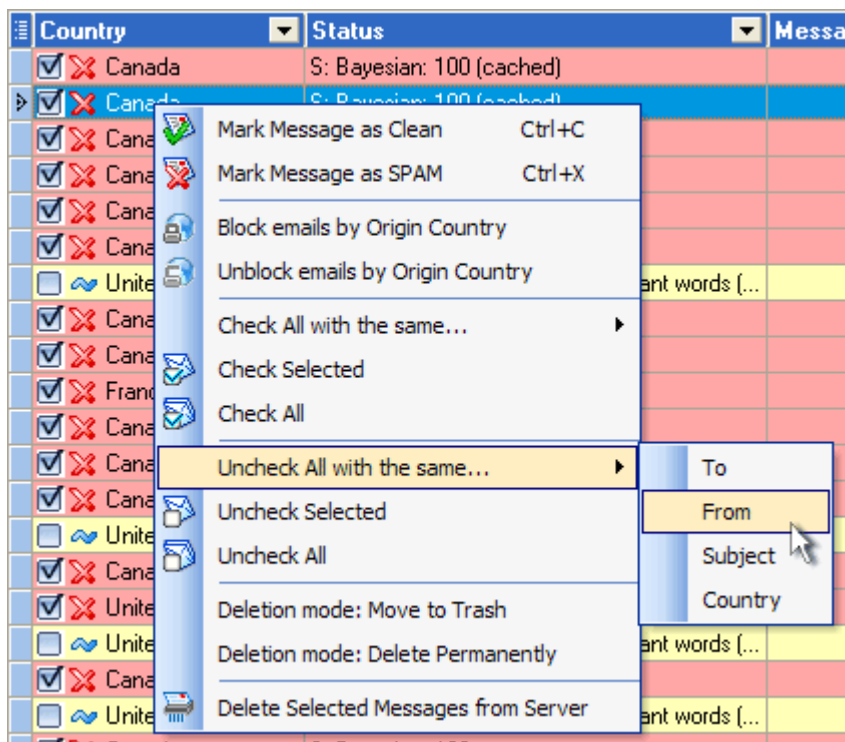
✗ Mark Message as SPAM

➕ Add to White List

➖ Add to Black List

-  Block emails by Origin Country
-  Unblock emails by Origin Country
-  View HTML/Message Source/Decoded Message
-  View/Hide Message Header
-  View/Hide Interesting Words (used by the Bayesian filter)

Most of the above options are also available from the popup menu if you click the right mouse button on the selected record within the grid:

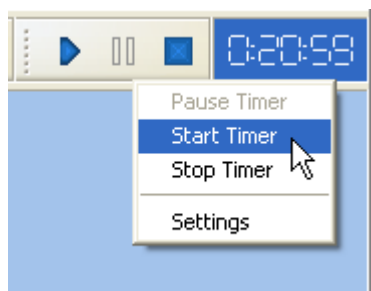


From the SpamCombat main window you can easily switch on the accounts auto-check mode. Just click Start Timer button next to the clock. The countdown starts and SpamCombat will retrieve your incoming emails every period of time specified in the Automation Settings. If you delete emails from the server while the timer goes, the countdown is not restarted but continued till the next accounts auto-check.


To pause the timer, click **Pause Timer**.

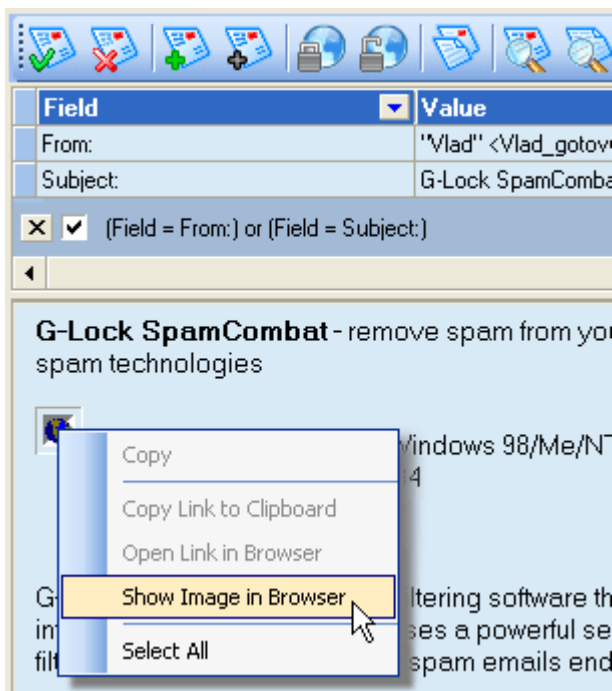
To resume, click **Start Timer** button.


To disable the accounts auto-check mode, click **Stop Timer**.

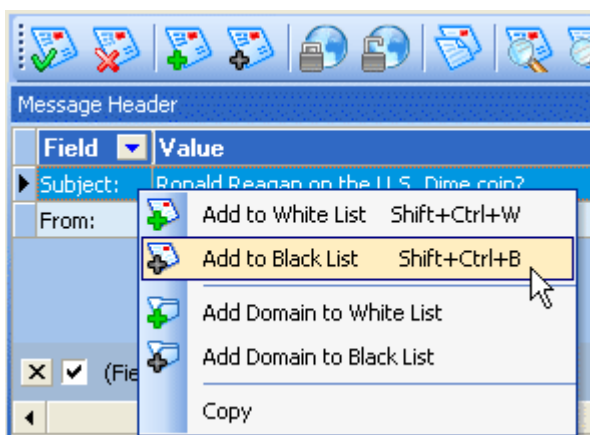


At the bottom screen you can preview your incoming emails. The following message preview formats are available: HTML, message source (RAW message code), and decoded message (message body).

To switch between the message preview formats, click  **View HTML/Message Source/Decoded Message** button. The HTML preview is absolutely safe. No pictures are actually downloaded; no hidden scripts or codes are executed. You can see only a picture frames in the preview screen. If you put the cursor to the picture frame, at the bottom of the SpamCombat main screen you will see the URL of this picture and the URL the picture includes (if there is any URL). If you click the right mouse button on the picture frame, you can either open the picture with your browser, or copy the URL the picture includes to the clipboard, or open this URL with your Internet browser.



To show/hide the message header, click  **View/Hide Message Header** button. You can select any field from the message header to whitelist or blacklist the email by this field. Select the appropriate string, click the right mouse button and select Add to White List or Add to Black List option.

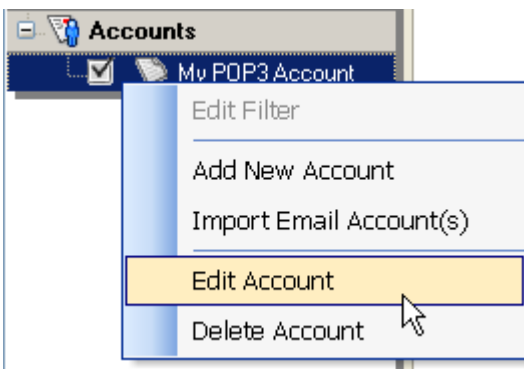


## Quick Startup

**Important!** Run SpamCombat before you receive the emails with your email client. After SpamCombat deletes all unwanted emails from the server, you can safely run your email client to receive only good emails.

### Creating Account

To get SpamCombat working, you need to setup an account, from which you will retrieve incoming emails. This account is already created in the SpamCombat Accounts section. You only need to fill in the required fields. To do this, click the right mouse button on the default account in the **Accounts** section and select **Edit Account**:



On **Edit Account** screen enter a display name for your account (any name you want), server name, port number, your account name, and password. You can pick up the server name, account name and password from the settings in your regular email client. Look for something like Incoming Mail Server. If you are not able to find this information then you'll need to ask your Internet Server Provider (ISP).

If you work with an IMAP account, check IMAP Account checkbox and fill the required fields in. If you have an account that uses SSL, check **Use secure connection (SSL)** checkbox and fill the required fields in.

It is a good idea to test your account before you save it. To do this, click

**Test** button. If the test is OK, click OK to save the account settings.

**Edit Account**

General | Advanced

Display Name:  
My Account

☐ IMAP Account ☒ Use secure connection (SSL)

☒ Process Seen messages ☒ Process Flagged messages

☐ Process messages received within the last 1 day(s)

Incoming Mail Server (POP3 or IMAP): Your server Port: 110

Account Name: Your account name Password: \*


☐ Log on using Secure Password Authentication

☐ Use safe deletion mode

Test

OK Cancel Help

## Retrieving Emails

Make sure that the checkbox next to your account in the **Accounts** section is checked and click  **Start** button on the Toolbar to start retrieving messages. You will see your incoming emails and their details on the screen.

Status	Country	Account	Size	From	Subject	Date
<input type="checkbox"/> ! U: Bayesian: 50	United States	TutMail	7.65 Kb	"TUT.B...	Mobile Offi...	12/30/1899
<input checked="" type="checkbox"/> ✗ S: Dubious HTM...	United States	TutMail	4.69 Kb	"RASM...	14.11.2003	11/13/2003 ...
<input type="checkbox"/> ✓ N: Bayesian: 0	Canada	NewMail	19.08 Kb	"ACD S...	IZone Web...	11/13/2003 ...

The icons legend:


- ✓ email is resolved as OK
- ✗ email is resolved as Spam
- ! email is flagged as unknown. Click either **Mark as Spam** or **Mark as Good** button to categorize the email
- ? email is not resolved because of a bad Internet connection (message header is empty). Click **Start** button to reprocess such emails
- ≈ email has not enough significant words to be processed by the Bayesian filter. Add such emails either to Whitelist, or Blacklist

## Training SpamCombat

To get the best performance of the program, you should train SpamCombat to classify your emails to spam and good. When the emails are retrieved, check whether they are properly categorized, i.e. whether ✗ emails are really spam and ✓ emails are really clean. If not, you should re-classify them by yourself. To do this, use ✗ **Mark Message as Spam** and ✓ **Mark Message as Clean** buttons on the Message Control Toolbar under the grid. The program learns from its mistakes and the next time the emails will be marked properly. Also categorize by yourself the emails with ! icon. The Bayesian filter learns from these emails as well.

**Attention!** Training applies to the Bayesian filter only. If an email was wrongly classified as spam or good by any other filter such as Complex Filter, Blacklist, Whitelist, HTML Validator, or DNSBL, there is no sense to re-classify this email. In this case, just edit or de-activate the appropriate filter.

The emails flagged by ≈ icon should be either whitelisted, or blacklisted. A green question mark ? means that the email could not be resolved as good or spam because of a glitch with the Internet connection. You should just re-process such messages some time later.

SpamCombat deletes from the server only those emails, which have the checkbox in the **Status** checked. Make sure the checkboxes are checked for all spam messages. Then click  **Delete** on the Toolbar to delete spam emails from the server.

Now you can safely run your email client to pull down the messages you really want to read. However, if it happens that a good email was deleted and moved to the SpamCombat trash, the program provides you with the ability to recover this email. See **Recovering Deleted Emails**.

Most users will be happy with the default settings. But SpamCombat is very configurable and you can customize it as you like.

You may want to examine a graphical scheme that shows how SpamCombat works. This scheme was gratefully provided by the SpamCombat user Dilson Cardoso.

Legend:

Complex - Complex Filter

WL - Whitelist

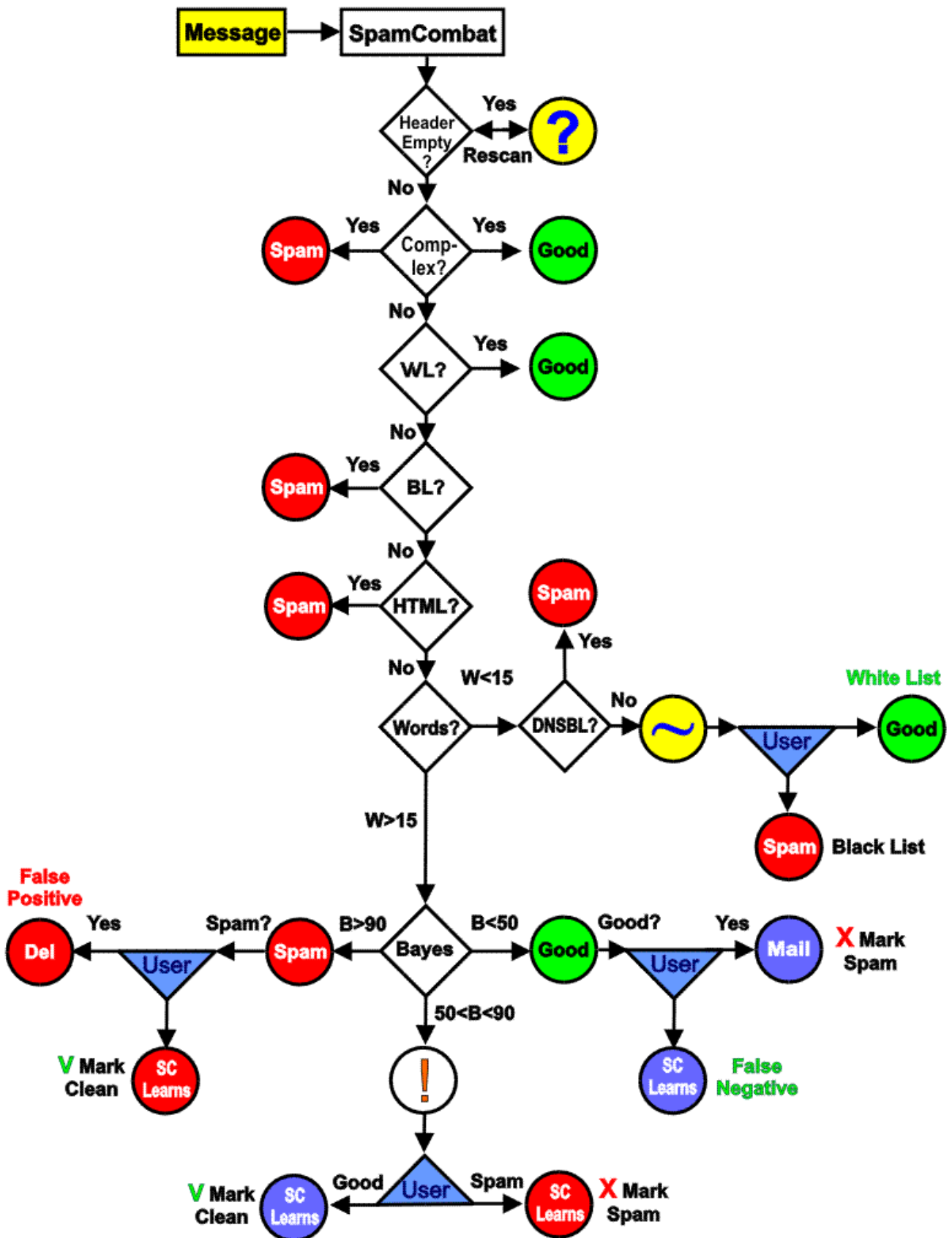
BL - Blacklist

HTML - HTML Validator

DNSBL - DNSBL filter

Words - number of significant words in the email

Bayes – Bayesian Filter



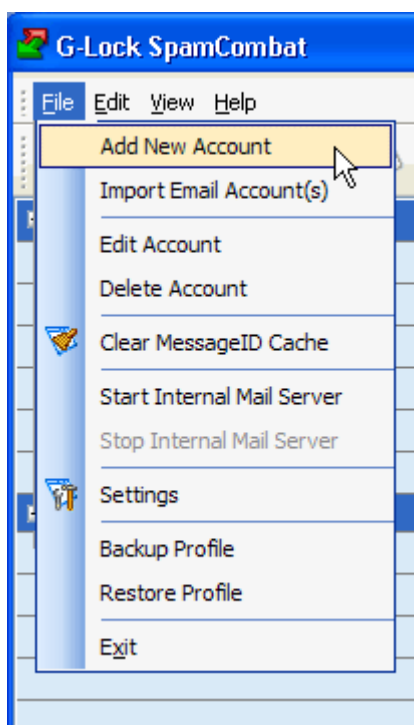
---

# Account Settings

## General Settings

You can add more accounts only in the registered version of SpamCombat!

To create an account, click the right mouse button on the **Accounts** area and select **Add New Account**. Or, click **File -> Add New Account**.



Fill in the required fields:

**Display Name** - name for your account.

**Incoming Mail Server (POP3 or IMAP)** - in most cases, the only time you've ever dealt with the Incoming Mail Server was when you setup your email client. So, your email client is where we'll start our search. At

the bottom of this topic we give the instructions how to retrieve the Incoming Mail Server information from the most popular email clients. If your email client is not listed then you'll need to check the settings of your email client looking for something that either says Incoming Mail Server, POP3 Mail Server, or, simply, POP3 Server. If you are not able to find this information then you'll need to ask your Internet Server Provider (ISP). Below we also included a list of popular ISPs with their Incoming Mail Servers.

**Account Name and Password** - most of the time your password is not explicitly shown in your email client. It is usually hidden under \* or similar characters. The Account Name is usually the first part of your email address. For example, if your email address is john.smith@hms.com then your account name is usually john.smith. However, if you do not know either of these values then you will need to contact your ISP to get them.

**Important!** You can leave **Password** empty when you setup an account. If there is no password provided, the program asks you for a password when it connects to the server. The password is remembered only for the current session. This option is very useful if you run the SpamCombat on a shared computer and are concerned about your privacy. Leaving the Password field blank you can be sure that no third party user can access your incoming emails. If you entered a wrong password and the program remembered it, open the Accounts settings and click OK. This will change a wrong password to "none". If you minimize the SpamCombat to the system tray, the password is saved. If you exit the program, the password is lost. If you check **Save Password** option, the password is remembered whenever you open the SpamCombat.

If you work with an IMAP account, check **IMAP Account** checkbox, enter your IMAP server name, IMAP server port (usually 143), account name and password. If you want SpamCombat to process already viewed

messages from your IMAP account, check **Process Seen Messages** option. To process flagged messages, check **Process Flagged Messages** option. If both options are disabled, the program retrieves and processes only NEW messages from your IMAP account.

To process only the emails you received within the last xx days, check **Process messages received within the last xx days** option and enter the number of days.

If you have an account that uses SSL, check **Use secure connection (SSL)** checkbox and fill the required fields in.

It is a good idea to test your account before saving it. To do this, click **Test** button. If the test is OK, click OK to save the account settings.

**Add New Account**

General | Advanced

Display Name:

☐ IMAP Account ☒ Use secure connection (SSL)

☒ Process Seen messages ☒ Process Flagged messages

☒ Process messages received within the last  day(s)

Incoming Mail Server (POP3 or IMAP):  Port:

Account Name:  Password:

☐ Log on using Secure Password Authentication

☐ Use safe deletion mode

Additional options:

**Log on using Secure Password Authentication** - specifies that you can use Secure Password Authentication to log on to this server. If you select this option, you might be prompted to log on when you connect to this server. If you are prompted for a user name and password, this account information is usually supplied by the Internet service or content provider when you sign up for their service.

**Use safe deletion mode** - check this option if SpamCombat deletes wrong emails from the server. When you use safe deletion mode, SpamCombat compares the headers of all the emails on the server to the headers of the emails you checked for deletion to ensure right messages are being deleted.

Before you save the account settings, it is a good idea to test whether they are correct. Click **Test** and check the records that appear in the empty screen. If everything is OK, click OK to save the account settings. You can create as many POP3 accounts as you want.

To edit an account, select **Edit Account** from the popup menu.

To delete an account, select **Delete Account** from the popup menu.

### **Common Email Clients**

Below is a list of common email clients and the steps within each to extract the Incoming Mail Server. If you not are using one of these applications and are not able to find the information your are looking within your email client then you can either 1) check the list of common Internet Service Providers (ISPs) provided at the bottom of this topic to see if your ISP and its settings are listed or 2) contact your ISP directly.

## **Outlook Express**

- Click on the Tools menu
- Click on the Accounts menu item
- Click on the Mail tab
- Select the desired account
- Click the Properties button
- Click the Servers tab
- Record the value next to Incoming mail (POP3)

## **Eudora**

- Click on the Tools menu
- Click on the Options menu item
- In the categories bar, click on Checking Mail
- Record the value next to Mail Server

## **Outlook 2002/XP**

- Click on the Tools menu
- Click on the E-mail Accounts menu item
- Select the View or Change existing e-mail accounts
- Click the Next button
- Select the desired account
- Click on the Change button
- Record the value next to Incoming mail server (POP3)

## **IncrediMail**

- Click on the Tools menu
- Click on the Accounts menu item
- Select the desired account
- Click on the Properties button
- Click on the Servers tab

Record the value next to Incoming mail server

## **Outlook 98/2000**

Click on the Tools menu

Click on the Accounts menu item

Click on the Mail tab

Select the desired account

Click on the Properties button

Click on the Servers tab

Record the value next to Incoming mail (POP3)

## **NetScape 4**

Click the Edit menu

Click the Preferences menu item

Expand Mail & Newsgroups by clicking the 'plus symbol'

Click Mail Servers

Select the desired Incoming Mail Server

Click Edit

Record the value next to Server Name

## **NetScape Mail 6**

Click the Tasks menu

Click Mail and Newsgroups

Click the Edit menu

Click the Mail and Newsgroups Settings menu item

Click on Server under your account name in the list on the left  
(indented)

Record the value next to Server Name for the Incoming mail server

## Common Internet Service Providers

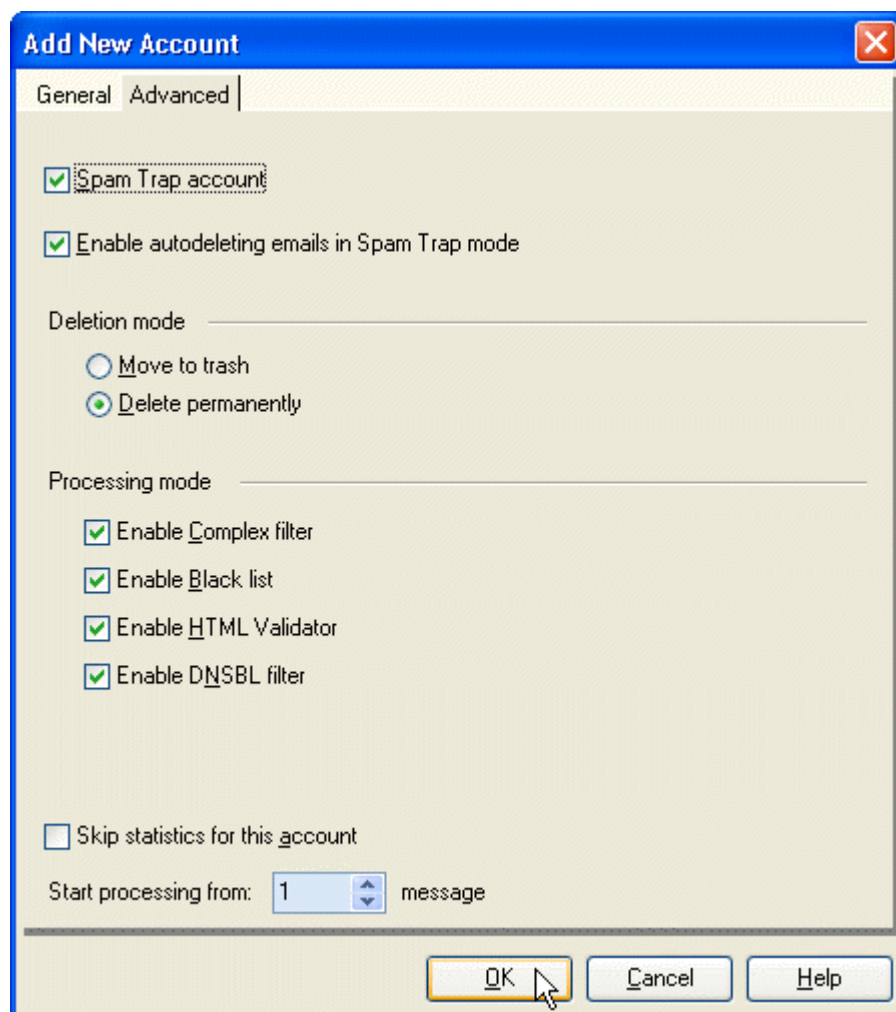
ISP	Incoming Mail Server
AT&T Broadband	mail.attbi.com
AT&T Worldnet*	ipostoffice.worldnet.att.net
Bell South	check with your Bell South
BestWeb	pop.bestweb.net
BlueLight	pop.myBlueLight.com
Cablevision	mail.optonline.net
Charter	pop.charter.net
Compuserve	pop.compuserver.com
Covad	pop3.covad.net
Cox	check with your Cox
CySpace City	mail.cyspacecity.net
EarthLink	pop.earthlink.net
GreaterBayNet	pop.greaterbaynet.com
Intra-Connect	mail.intra-connect.net
Interfold	mail.interfold.com
Leapfrog Internet	mail.leapmail.net
LocalNet	mail.localnet.com
MindSpring (EarthLink)	pop.mindspring.com
Monster ISP	mail.vcmails.com

NCCW Online	mail.nccw.net
NetZero	pop.netzero.com
PeoplePC	mail.peoplepc.com
Prodigy	pop.prodigy.net
Qwest	check with your Qwest
RCN	pop.rcn.com
RoadRunner	check with your RoadRunner
SBC	check with your SBC
SkyPoint Communications	popmail.skypoint.com
T-Online.de	securepop.t-online.de
Verizon	incoming.verizon.net
Videotron	pop.videotron.ca
Vision ISP	pop.vision-isp.com
Volaris (EarthLink)	mail.vol.com
WebConnects	mail.wcox.com
Yahoo! Mail	pop.mail.yahoo.com

\* AT&T Worldnet requires that the Incoming Mail Server Port be set to 995.

## Advanced Settings

Here you can specify advanced settings for your account:



**Spam Trap Account** - if you check this option, all the emails you receive on this account are automatically classified as spam. A **spamtrap** is an email address used to catch spammers, as nobody should be sending email to it - as it's never used. The spam trap account has a red icon in the Accounts section:



**Enable autodeleting emails in Spam Trap mode** - check this option if you want the emails that come to the SpamTrap account to be automatically

deleted.

Select a deletion mode for the emails you receive on the SpamTrap account:

**Move to trash** - spam emails are deleted from the server and moved to Deleted Items folder (saved to the disk)

**Delete permanently** - spam emails are deleted from the server without being saved to the disk

Select processing mode for the emails you receive on the SpamTrap account. There are four checkboxes:

Enable Complex filter

Enable Blacklist

Enable HTML Validator

Enable DNSBL filter

If you uncheck all the checkboxes, the Bayesian filter learns from ALL the messages you receive on the Spam Trap account while other filters are turned off. Or, you can activate any filter(s) and the Bayesian filter will learn only from the emails that were not caught by the selected filter(s).

**Skip statistics for this account** - if you check this option, the appropriate account will not be included in the SpamCombat statistics.

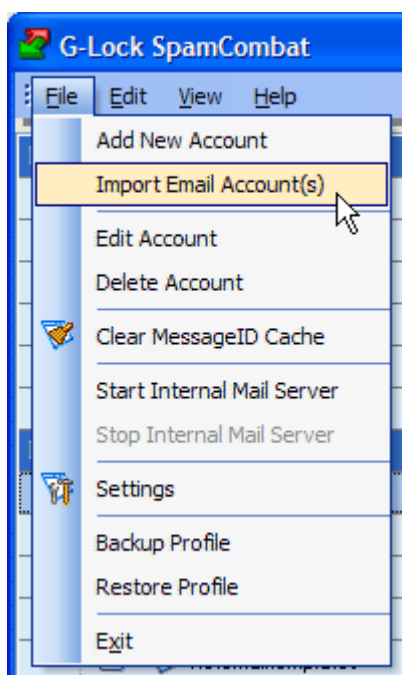
**Start processing from xx message** - here you can specify the message# from which the SpamCombat will start processing emails. This option allows skipping first xx messages and start processing from the next message. Example: you have 150 emails on your POP3 account at the moment. You know that first 100 emails are good and you need to process only the last 50 messages. To do this, you enter 101 in this box and the

SpamCombat skips the first 100 emails and starts retrieving from the 101 message. When you exit the program, the message number is remembered.

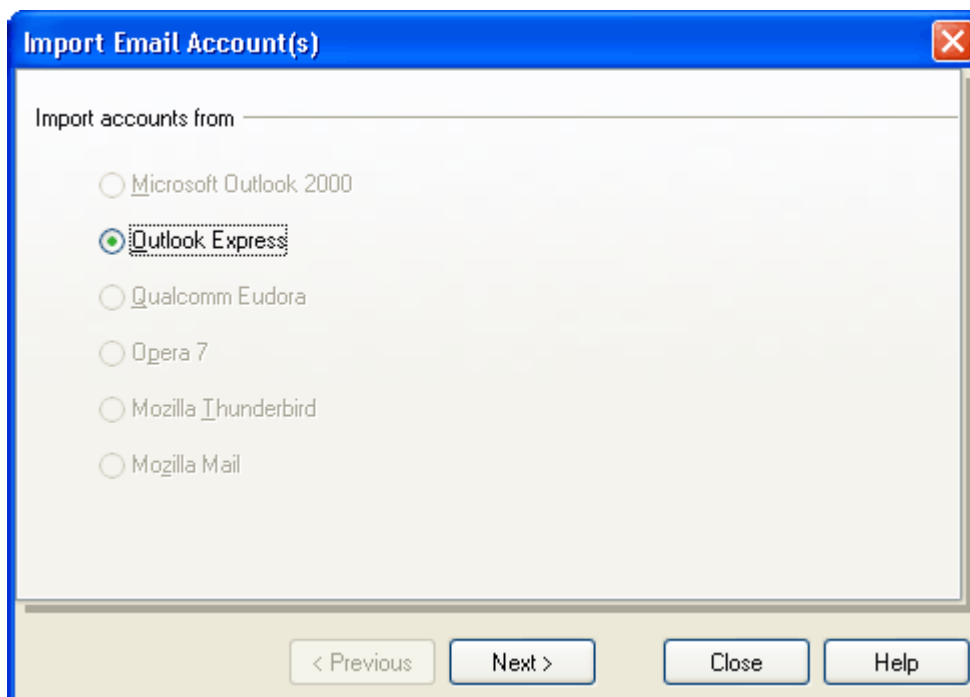
## Importing Accounts

For your convenience and saving time you can import the account information from your regular email client. SpamCombat supports import of POP3/IMAP accounts from MS Outlook 2000, Outlook Express, Qualcomm Eudora, Opera 7, Mozilla Thunderbird, and Mozilla Mail.

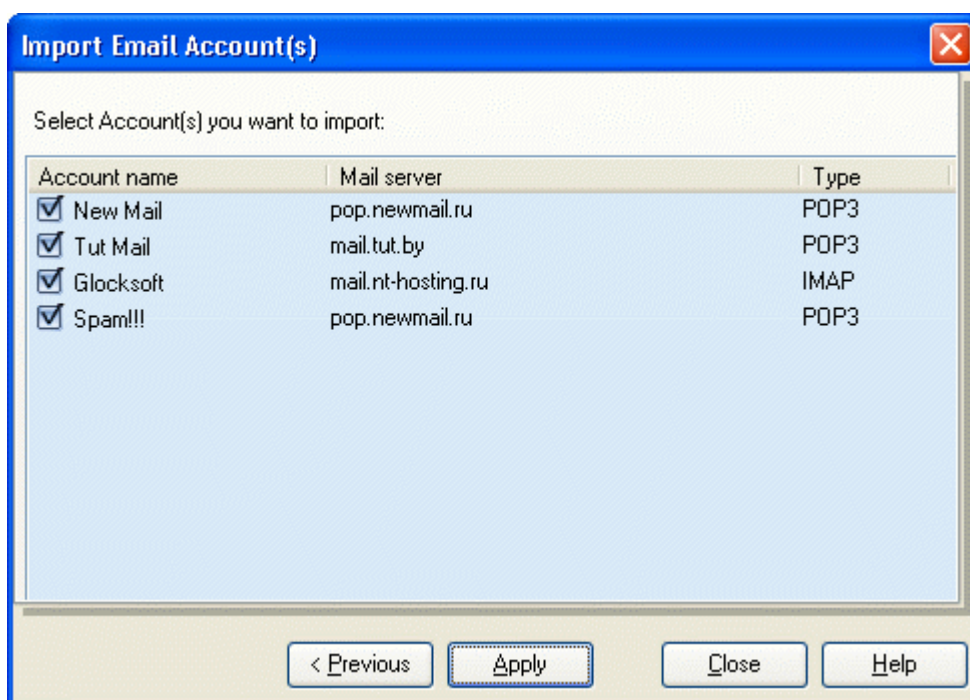
To import an account, click on **File** menu and select **Import Email Account(s)**



Select an email client to import the account from. Click **Next**.



You will see a list of POP3/IMAP accounts in your email client. All the accounts are selected by default. Just uncheck the account(s) you do not want to import into SpamCombat.




Click **Apply**.

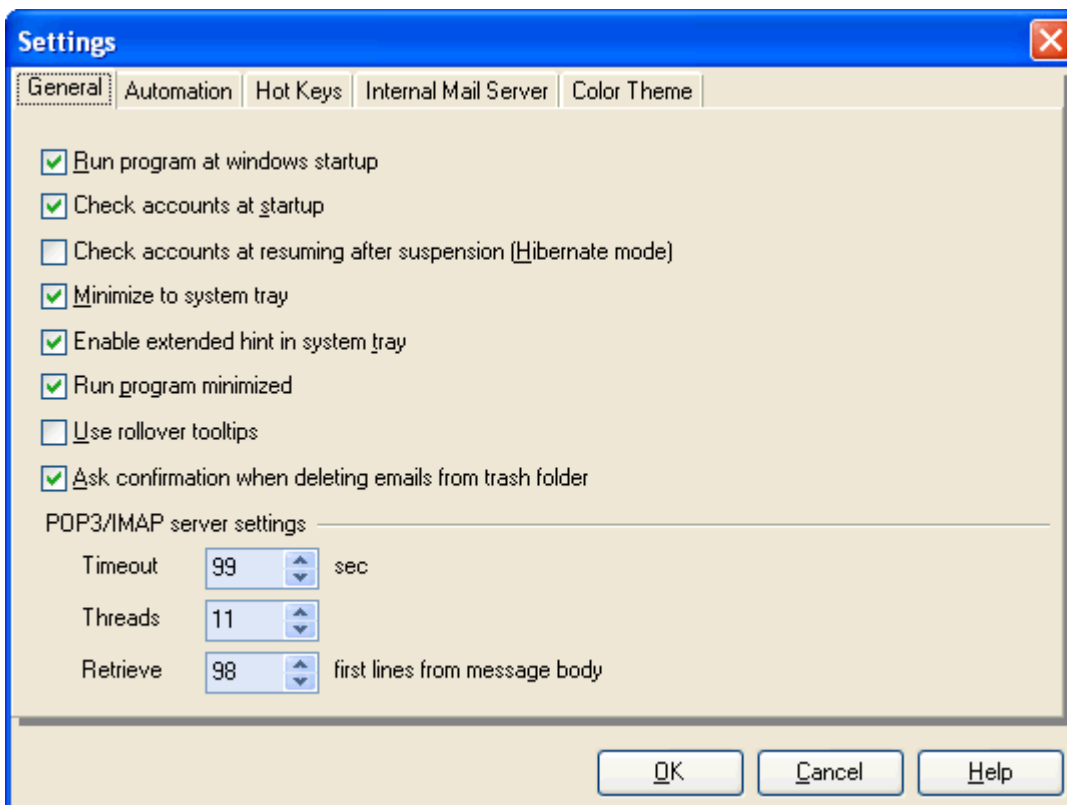
The imported account(s) appear in the Accounts section at the left pane of

the program's main screen. Double click the mouse on the account to view the account details. **Incoming Mail Server (POP3 or IMAP)**, **Port**, **Account Name**, and **User Name** are automatically filled in. You only have to type your password for the appropriate account. To test the account, click **Test**. You can also leave **Password** field empty. If no password is provided for the appropriate account, SpamCombat asks for a password when connecting to the server.

# SpamCombat Settings

## General Settings

To configure the General settings of SpamCombat, click  Settings button on the Toolbar and then click General tab.



**Run program at windows startup** - check this option if you want the program to be run just at Windows startup.

**Check accounts at startup. Startup Delay xx sec** - check this option if you want the program to start retrieving the emails just at startup. Set the delay in seconds.

**Check accounts at resuming after suspension (Hibernate mode)** - when this option is checked, the program automatically starts retrieving the

emails as soon as the computer is brought out from hibernation.

**Minimize to system tray** - when this option is checked, the program minimizes to system tray after you close it.

**Enable extended hint in system tray** - when this option is checked, the program displays the lite screen if you put the mouse in the icon in the system tray. See also **Working with SpamCombat in System Tray**

**Run Program Minimized** - when this option is checked, the program minimizes to the system tray as soon as you open it.

**Use rollover tooltips** - if this option is checked, a hint comes up when you point the mouse on the record within the grid if the record is not entirely visible.

**Ask confirmation when deleting emails from trash folder** - if you check this option, you will have to confirm that you want to permanently delete the messages from the SpamCombat trash bin.

### **POP3/IMAP Server Settings**

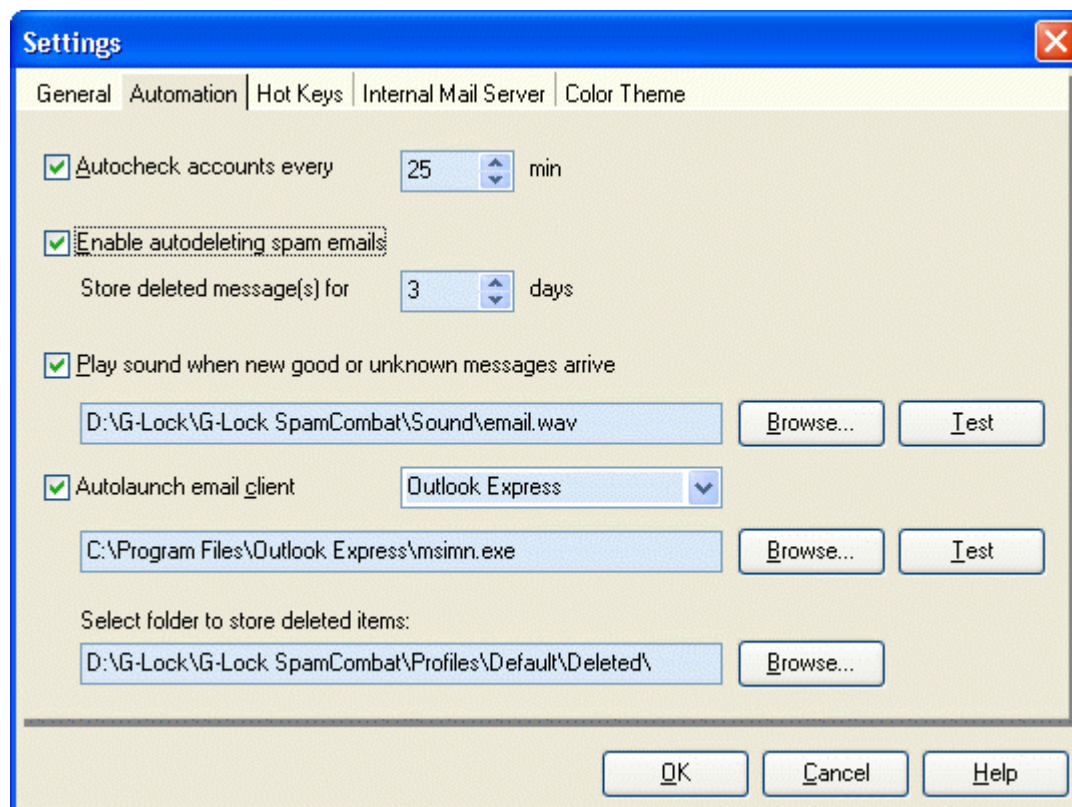
**Timeout** - time limit used by the program to connect to the POP3 server.

**Threads** - number of POP3 accounts the program connects to at the same time.

**Retrieve XX first lines from message body** - shows how many lines from the message body SpamCombat must retrieve to resolve the message as good or spam. The attachments are not shown if the message had a big size and was not entirely retrieved. The ability to show the email attachment is mostly aimed to block virus messages that usually have a small size.

## Automation Settings

You can setup SpamCombat to automatically check your accounts for incoming emails every period of time and delete spam messages. To do this, click **Settings** button on the Toolbar and then click **Automation** tab.




**Autocheck accounts every xx min** - if you check this option, the program will automatically check your accounts for incoming emails every xx min.

**Enable autodeleting spam emails** - if you check this option, spam emails are automatically deleted from the mail server and saved to **Deleted Items** folder in SpamCombat. **ATTENTION!** It is not recommended that you select this option without training SpamCombat as there is a chance that good emails will be moved to **Deleted Items** folder.

**Store deleted message(s) for xx days** - shows for how many days deleted emails will be stored on the disk. When xx days since the message had been removed from the server pass, the message is automatically deleted from the disk.

**Play sound when new good or unknown messages arrive** - check this option to receive a sound notification every time a new good or unknown message arrives. If a spam email or an email with "Cached" status is received, the sound does not play. You can either use a default sound file provided with SpamCombat, or select a different sound file on your HDD. To test how the file plays, click **Test**.

**Autolaunch Email Client** - if you check this option, your default email client will be automatically opened as soon as spam emails are deleted from the server. Select your email client from the drop down box. If you have an email program other than Hotmail, MS Outlook, or Outlook Express, select **Other** and specify a full path to it using Browse button. **IMPORTANT!** If auto-deletion mode is ON, the email client automatically opens after spam emails are deleted from the server. If auto-deletion mode is OFF, the email client is automatically launched after you manually delete spam emails. You can also open your email client if you click  **Launch Email Client** button on the Toolbar.

**Select folder to store deleted items** - here you can select a folder on your HDD to store deleted emails.

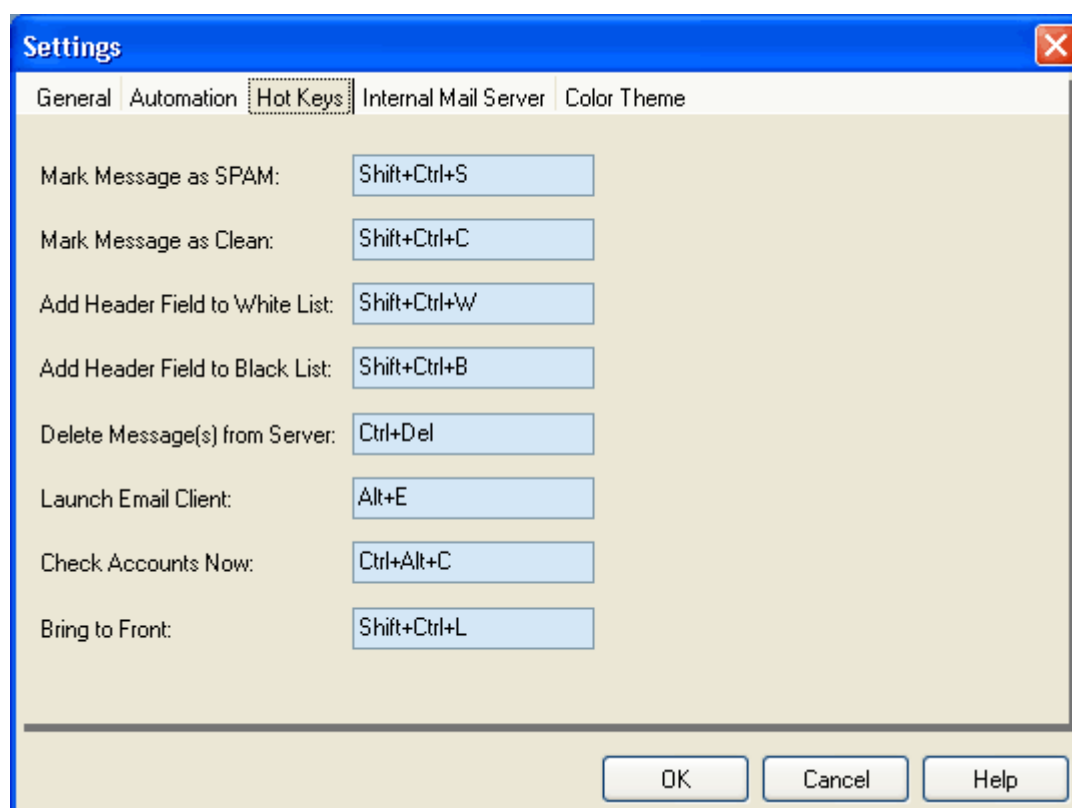
## Hot Keys Configuration

Here you can set the keys that control most important SpamCombat functions. To assign a hot key to an operation, put the cursor to the appropriate field and press the desired key on the keyboard. When you're finished, click OK to save your hot key combinations. The Hot Keys combinations function only if SpamCombat is maximized, i.e. displayed as a full screen. When the program is minimized, you can use **Bring to Front** hot key to maximize it. Using the hot key combination **ALT+any character** is not recommended as ALT is used to work with menus in the programs.

Here are 2 examples of the hot key combinations with ALT where:

**Alt+W** is NOT working

**Shift+Alt+B** is working



## Internal Mail Server

The SpamCombat Internal Mail Server allows you to recover an email from the Deleted Items folder and receive it with your email client. SpamCombat has the Internal Mail Server settings pre-setup: Account Name - SpamCombat, password - SpamCombat, and port - 110. You can either use these default parameters to create an account in your email client, or you can change the default account name and password to your own.

### Note:

As a server name in your email client you can use either your computer name or 'localhost'. You can easily find your computer name by clicking Test in the Internal Mail Server settings. You will see the records like this if all is OK:

+OK G-Lock SpamCombat POP3 server

+OK Proceed with PASS command.

+OK Vlad44 Welcome SpamCombat, 0 messages (0 octets)

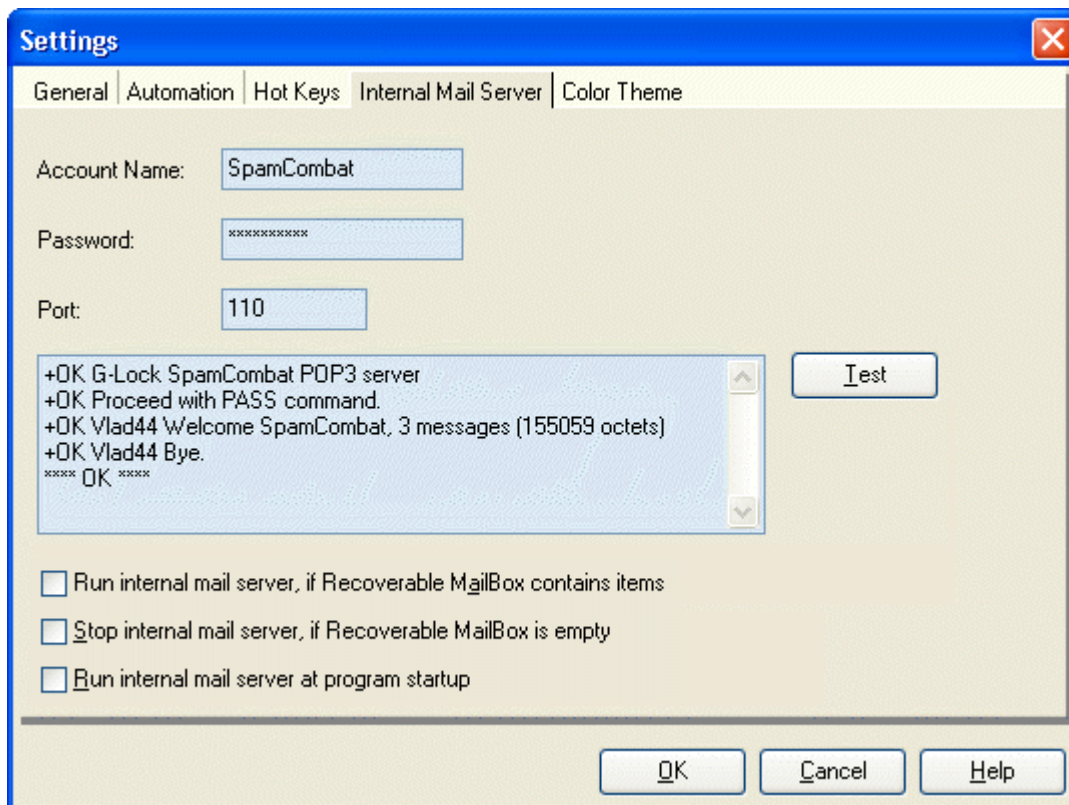
+OK Vlad44 Bye.

\*\*\*\* OK \*\*\*\*

Where Vlad44 happens to be the machine name in this case.

Don't forget that there's no SMTP server provided by SpamCombat, so you'll have to use your ISP SMTP server if it's not already configured as such.

To open the Internal Mail Server settings, click Settings button on the Toolbar and then click **Internal Mail Server** tab.



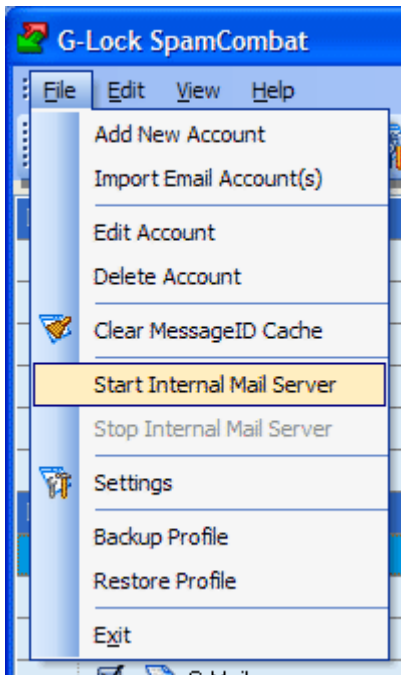
If you changed the account name and/or password, it is a good idea to test whether they are correct. Click **Test** and check the records that appear in the empty screen. If everything is OK, click **OK** to save your settings.


**Run Internal Mail Server if Recoverable mailbox contains items** - when this option is checked, the Internal Mail Server starts as soon as an email is moved to the Recoverable mailbox.

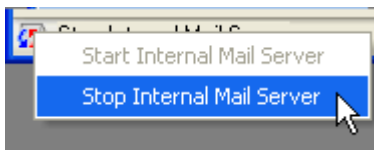
**Stop Internal Mail Server if Recoverable mailbox is empty** - when this option is checked, the Internal Mail Server stops as soon as the Recoverable mailbox empties.

**Run internal mail server at program startup** - when this option is checked, the Internal Mail Server will automatically start at the program startup.

To start the SpamCombat Internal Mail Server, click **File** and select **Start Internal Mail Server**.



When the Internal Mail Server is started, you can see the  icon at the left bottom corner of the SpamCombat screen. To stop the Internal Mail Server, click on the icon and select the appropriate menu.



## Color Theme and Font Size

For your convenience you can let the SpamCombat show the emails by different colors according to how they are classified.

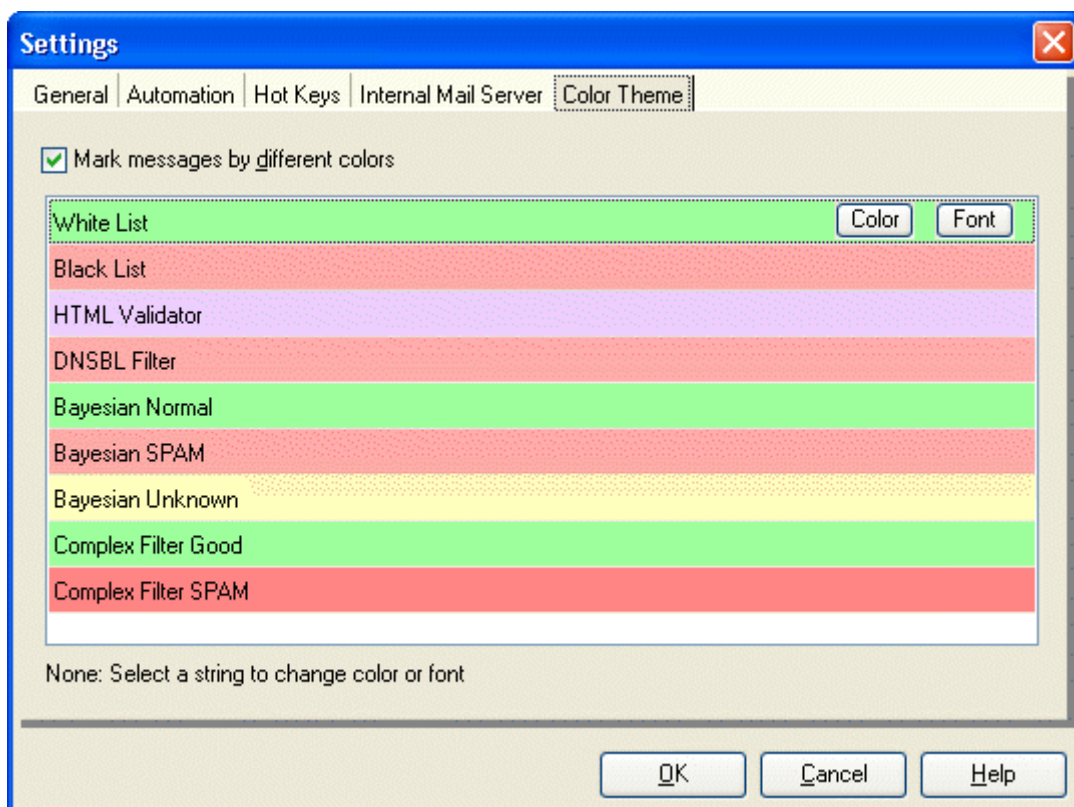
To adjust **Color Theme** settings, click **Settings** button on the Toolbar and then click **Color Theme** tab.

Check **Mark messages by different colors** option.

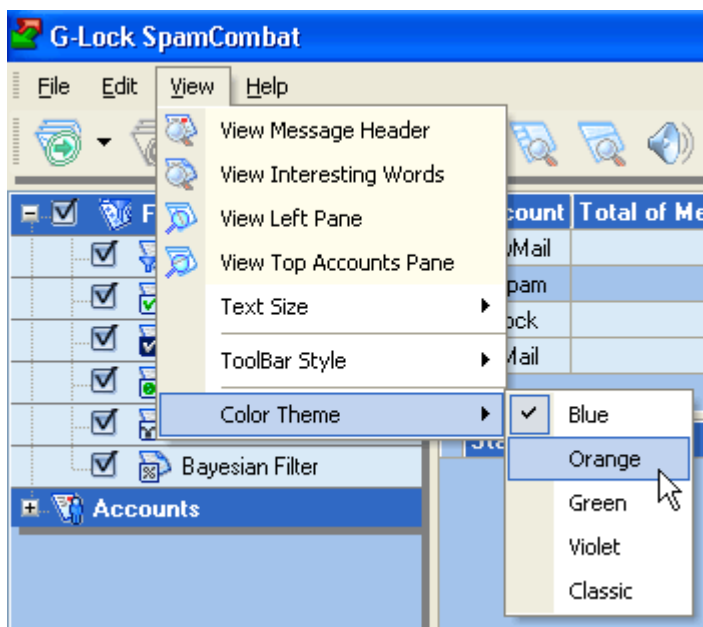
To change the color, click **Color** button.

To change the font, click **Font** button.

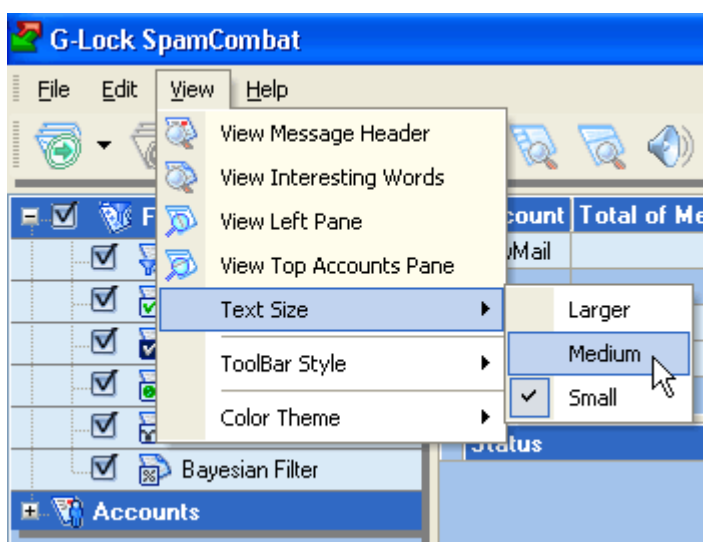
When you finished, click OK to save the settings.



You can also customize the color and appearance of the SpamCombat interface. To change the color theme of the program's main screen, click **View** menu, then click **Color Theme** and select the color.



You can also change the font of the SpamCombat interface. To change the font, click **View** and select **Text Size** -> **Larger**, **Medium**, **Small**.



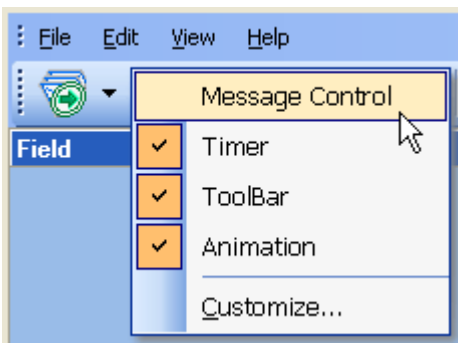
## Customizing Menus and Toolbars

You can customize the SpamCombat toolbars yourself. You can add and remove buttons on toolbars, create your own custom toolbars, hide or display toolbars, and move toolbars.

### Showing/Hiding Toolbars

You can show/hide the main program **Toolbar**, **Message Control Toolbar** and **Timer Toolbar**. But you can't hide the top menu bar.

Click the right mouse button on a toolbar and check/uncheck the checkbox next to the toolbar you want to show/hide.

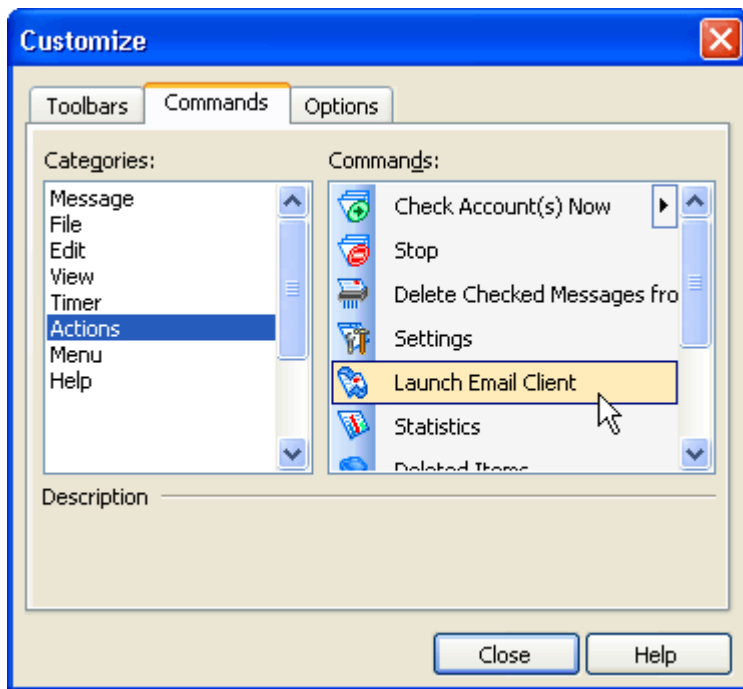


### Customizing Toolbars

You can customize the main program **Toolbar**, and the **Message Control Toolbar**.

**To add buttons to the toolbar:**

1. Open the **Customize** screen
2. Click the **Commands** tab on the **Customize** screen.
3. Select a command category in the **Categories** frame.
4. Select a command in the **Commands** frame and drag it to the toolbar where you want the button to be.

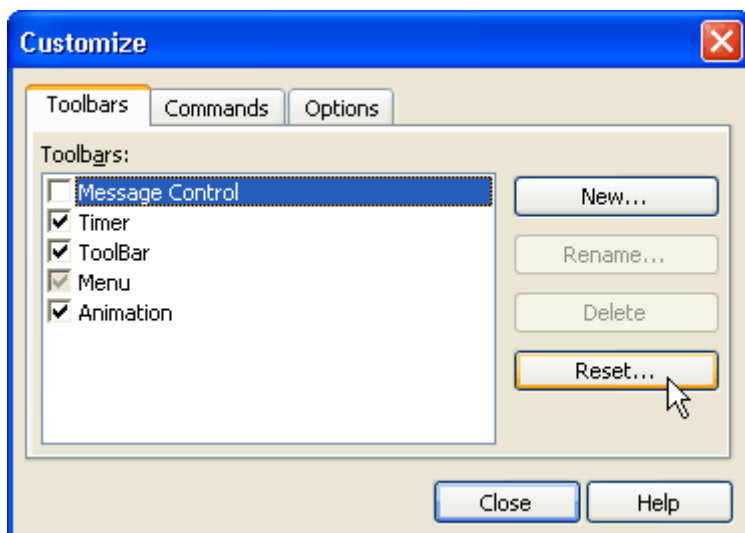


To remove buttons from the toolbar:

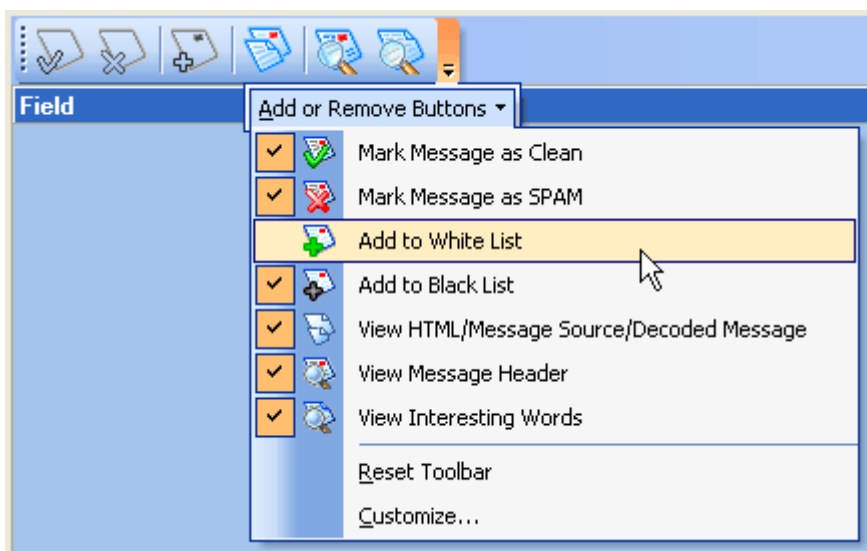
1. Open the **Customize** screen
2. Click the **Commands** tab on the **Customize** screen.
3. Select a button on the toolbar and drag it to the **Commands** frame.

To restore the toolbar:

1. Open the **Customize** screen
2. Click the **Toolbars** tab on the **Customize** screen.
3. Select a toolbar you want to restore and click **Reset** button.



To customize the **Message Control** toolbar, you can click **More Buttons** at the end of the toolbar and then click **Add or Remove Buttons**:



To hide a button from the toolbar, uncheck the checkbox next to the button.

To show a button on the toolbar, check the checkbox next to the button.

To restore the toolbar, click **Reset Toolbar**.

To add more buttons to the standard Message Control toolbar, click **Customize...**

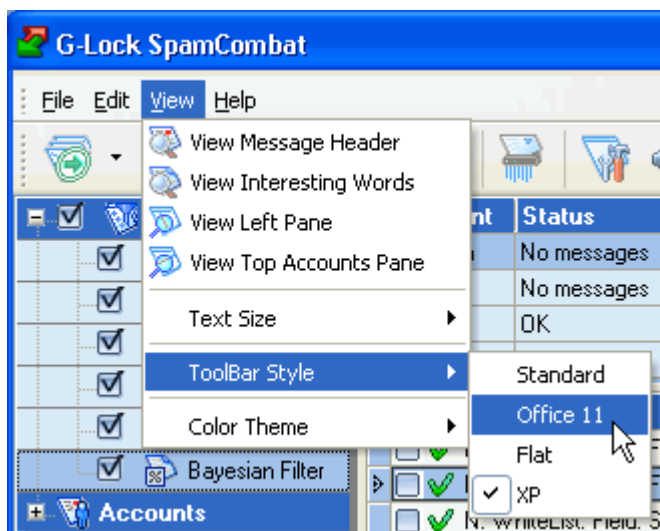
## Moving Toolbars

You can move the top menu bar as well as the main program **Toolbar**, **Message Control**, and **Timer Toolbars** to position them at the place on the SpamCombat main screen that is most convenient for you. To move a toolbar, drag and drop it where you want it to be.



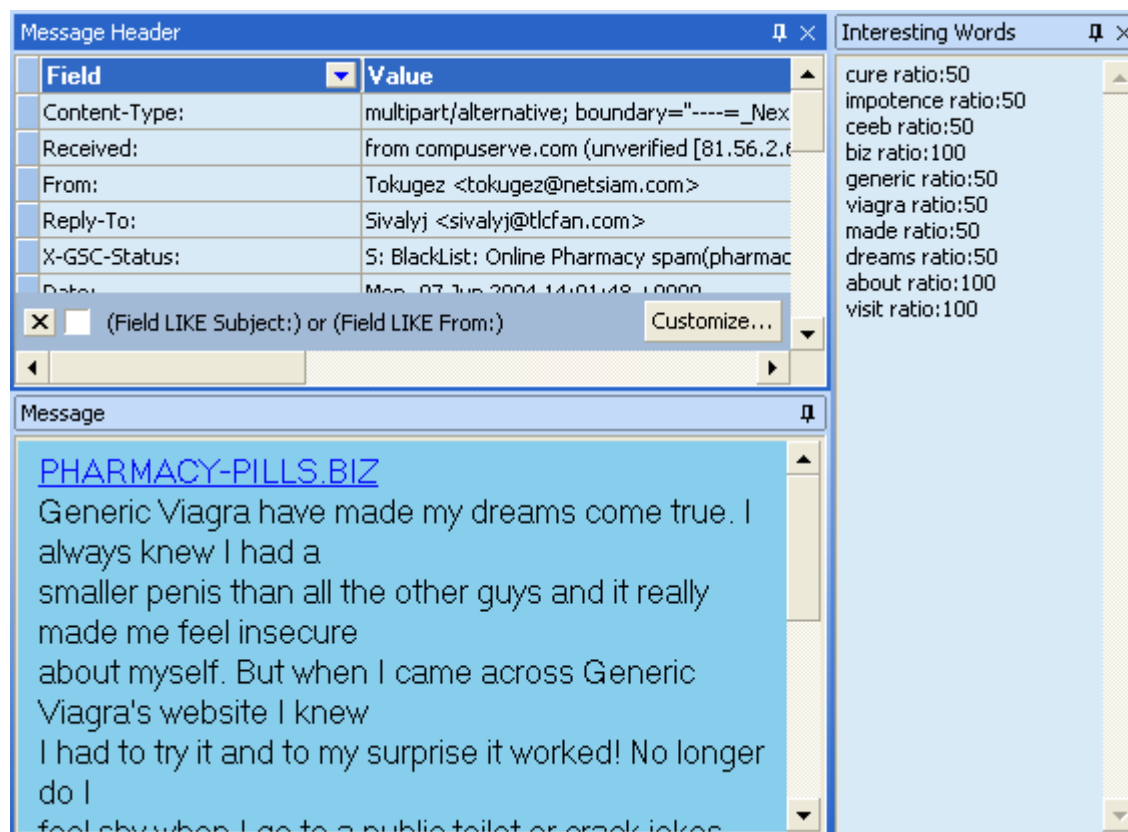
## Changing Toolbar Style

To change the style of the SpamCombat toolbars, click **View** on the menu bar and select **Toolbar Style**. Then select a style to show the toolbars: Standard, Office 11, Flat, or XP.



## Customizing Message Preview Screen

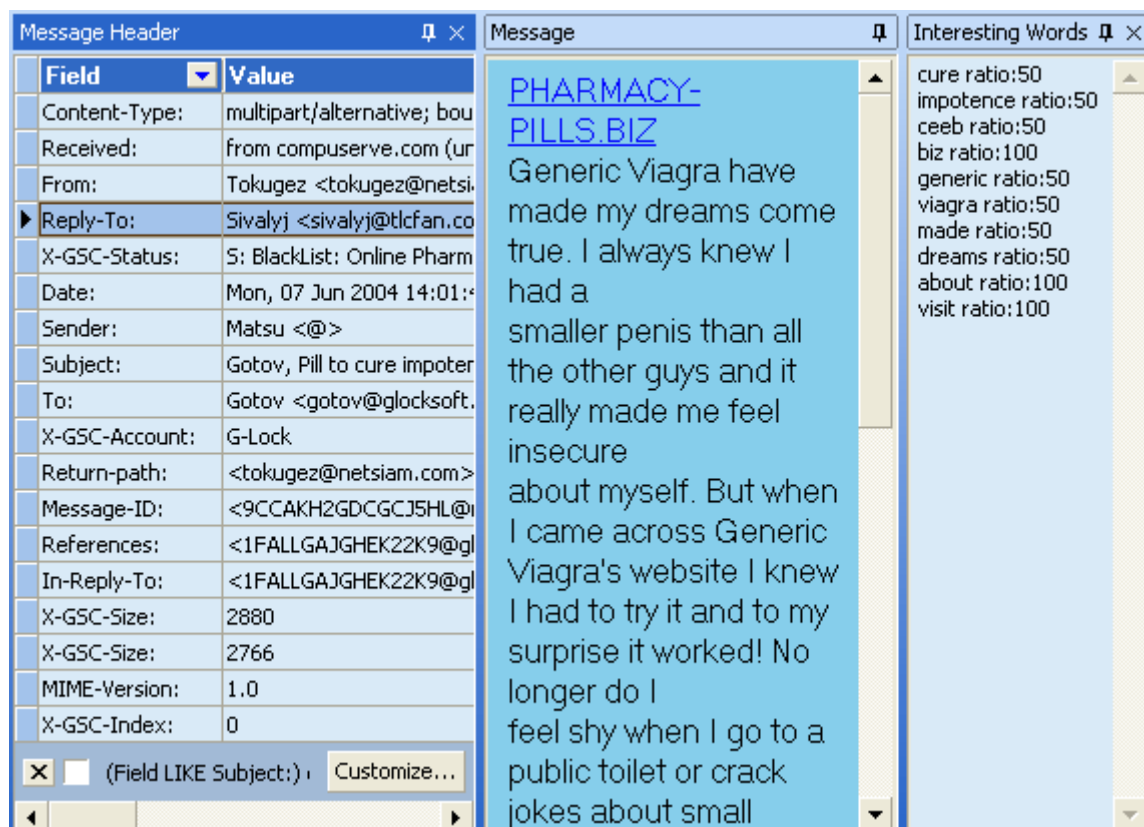
The SpamCombat Message Preview screen consists of three dock panels: Message Header, Message (or message body), and Interesting Words. The default layout of the dock panels is as follows:



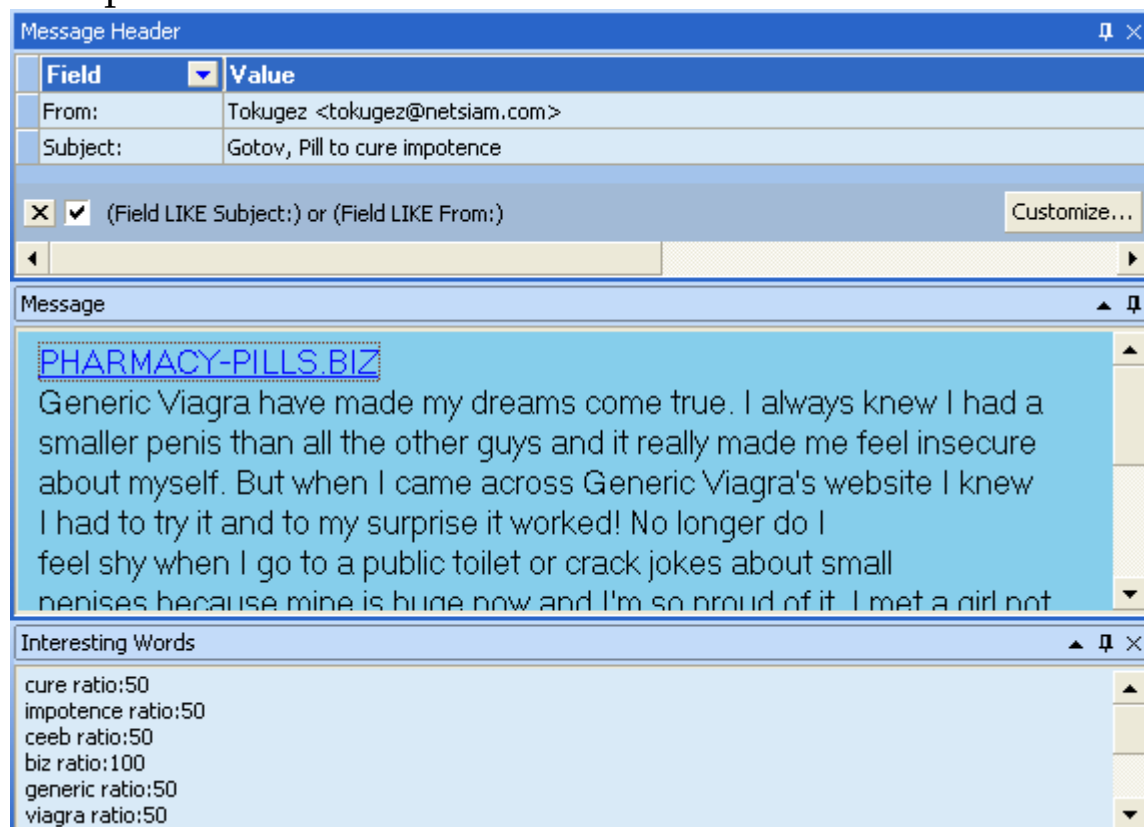
You can modify the default layout in the manner you find the most convenient for the work with inbound emails. To do this, you have the following alternatives:

1) create a vertical side container. To do this, you need to dock one panel to the top of bottom edge of an other panel. The image below shows how to create a vertical side container comprised of three dock panels.

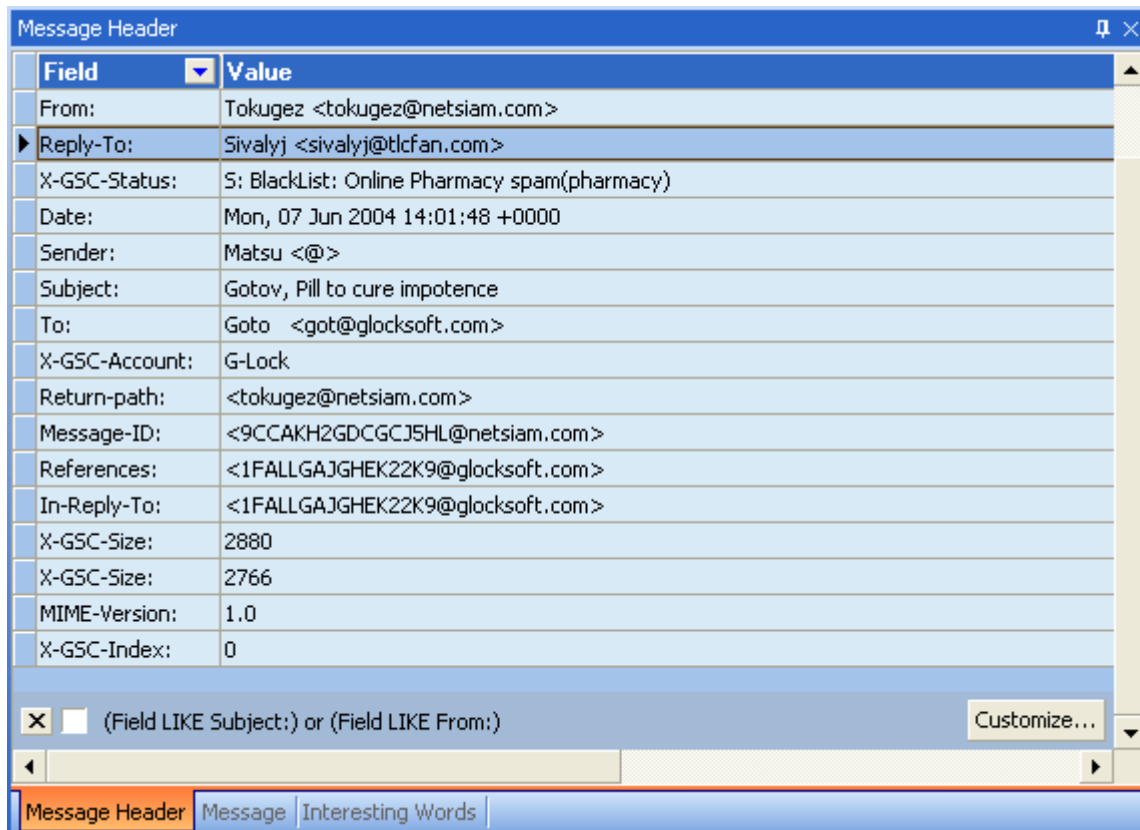
Message panel is docked to the bottom edge of Message Header panel, and Interesting Words panel is docked to the bottom edge of Message panel:



2) create a horizontal side container. A dock panel must be docked to the left or right edge of an other control. The image below shows an example:



3) create a tab container that includes three panels. To do so, you have to dock a panel to another panel so that the target control is filled entirely. This implies that the mouse cursor should point in the middle of the target dock panel when dropping. To switch between the panels, click the appropriate tab. The image below shows an example of a tab container.



If you need to drag a panel away from the tab container, drag the corresponding tab.

4) enable the auto hide feature in the tab container. To do this, click the auto hide button at the top right bottom of the panel. If the auto hide feature is enabled for a tab container, only individual panel can be displayed at a single time. To display a hidden panel, put the cursor to the corresponding tab. The panel will be automatically moved out.

Message Header

Field	Value
Content-Type:	multipart/alternative; bounde
Received:	from compuserve.com (unver
From:	Tokugez <tokugez@netsiam.
Reply-To:	Sivalyj <sivalyj@tlcfan.com>
X-GSC-Status:	S: BlackList: Online Pharmacy
Date:	Mon, 07 Jun 2004 14:01:48 -
Sender:	Matsu <@>
Subject:	Gotov, Pill to cure impotence
To:	Gotov <gotov@glocksoft.com>
X-GSC-Account:	G-Lock
Return-path:	<tokugez@netsiam.com>
Message-ID:	<9CCAKH2GDCGCJ5HL@net:
References:	<1FALLGAJGHEK22K9@glock
In-Reply-To:	<1FALLGAJGHEK22K9@glock
X-GSC-Size:	2880
X-GSC-Size:	2766
MIME-Version:	1.0
X-GSC-Index:	0

☒ (Field LIKE Subject:) or (
 ☐ Customize...

Interesting Words

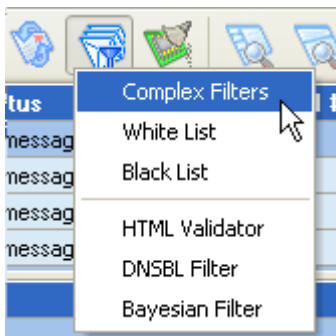
cure ratio:50  
 impotence ratio:50  
 ceeb ratio:50  
 biz ratio:100  
 generic ratio:50  
 viagra ratio:50  
 made ratio:50  
 dreams ratio:50  
 about ratio:100  
 visit ratio:100

...ams come true. I  
 ...ys and it really  
 ...ross Generic  
 ...worked! No longer  
 ...t or crack jokes  
 ...w and I'm so  
 ...had the best sex  
 ...! It was great!  
 ...MACY-PILLS.BIZ

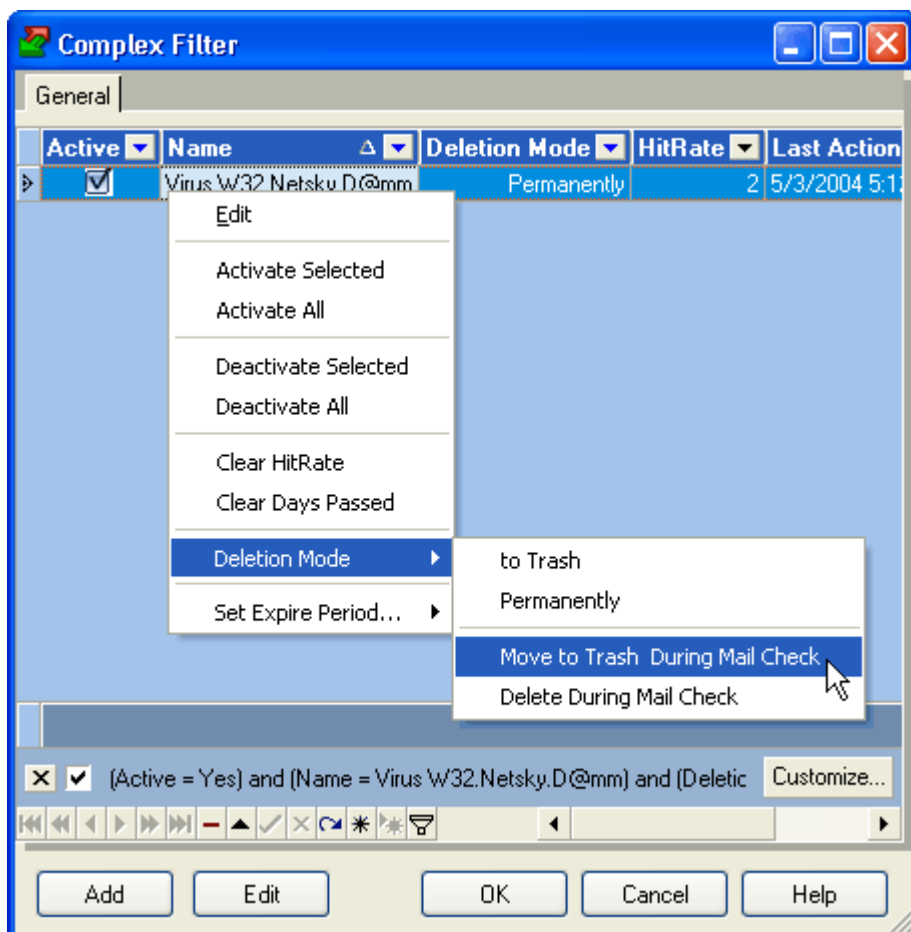
### Adding Complex Filter

**Complex Filter** lets you write a script to categorize incoming emails as spam and good depending on the defined conditions. Here you can use various functions, procedures, and operators to compare one or several fields from the message header to the specified values and classify the message as spam or good according to the result.

To open the Complex Filter settings, double click the mouse on the **Complex Filters** at the program's left pane, or click **Filters** button and select **Complex Filters**:



To add a complex filter, click **Add** button at the bottom of the screen. You will see **Script Editor** where you can write your script to filter the emails. When the script is ready, click OK on the **Script Editor** screen and the filter will be added to the grid.



The grid columns denote:

**Active** - status: enabled or disabled. Click the mouse on the checkbox to change the filter status.

**Name** - short description of the filter


**Deletion Mode** - deletion mode for spam emails detected by the Complex filter:

**to Trash** - emails are moved to **Deleted Items** folder after you click **Delete** button

**Permanently** - emails are deleted permanently and not saved to the disk after you click **Delete** button

**Move to Trash During Mail Check** - emails are moved to **Deleted Items** folder during the accounts check

**Delete During Mail Check** - emails are deleted permanently during the accounts check

 **Note:** If auto-deleting spam emails in the Automation settings is enabled, **Delete Permanently** and **Delete During Mail Check** modes work similarly: the emails are permanently deleted during mail check. The filters with **Delete During Mail Check** deletion mode are executed the first.

**HitRate** - shows how many times this filter worked since you have begun working with SpamCombat

**Last Action** - date and time when the filter last worked

**Expire** - expire period for the filter. When it is over, the filter is automatically deactivated.

**Day Passed** - progressive bar showing how many days of the expire period passed

If you click the right mouse button on the selected filter within the grid, you'll see the following menu:

**Edit** - allows you to edit the selected filter

**Activate Selected** - allows you to activate the selected filter

**Activate All** - allows you to activate all the filters

**Deactivate Selected** - allows you to deactivate the selected filters

**Deactivate All** - allows you to deactivate all the filters

**Clear HitRate** - allows you to set the HitRate statistics in the selected

string to 0. Although the HitRate is cleared, you should click OK to save the changes.

**Clear Days Passed** - clears the progressing bar so that the expire period for the selected filter restarts

**Deletion Mode** - allows you to set a deletion mode for spam emails detected by the selected filter: Move to Trash, Delete Permanently, Move to Trash During Mail Check, or Delete During Mail Check.

**Set Expire Period** - allows you set the expiration period for the filter: 30, 60, 90, 120 days, or never. Or you can enter any quantity of days by yourself.

At the bottom of the grid there is also a range of buttons you can use to work with the complex filters. Put the cursor to the button to know its function.

For your convenience you can sort and filter the records within the grid as you want.

## Creating Script

**Script Editor** allows you to write a script to filter your incoming emails. Enter a short description of the filter into **Name** field. Write your script in the Script screen. Here is a list of internal variables you can use in your script:

Account Name

Cc

Content-Transfer-Encoding

Entire Header

Content-Type

From

Mailing-List

In-Reply-To

List-Unsubscribe

Message Body

Message Source

Received

Organization

Origin-Country

Return-Path

Recipient Email

Reply-To

Subject

To

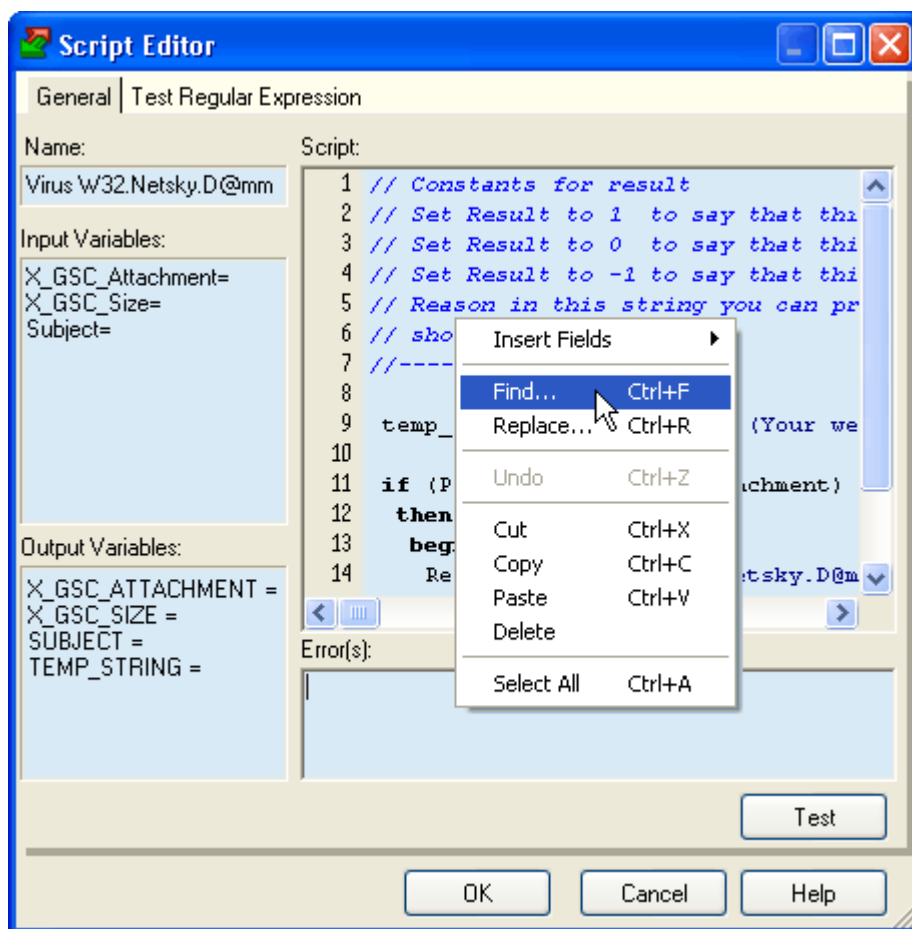
X-GSC-Attachment

X-GSC-Size

X-Mailer

To insert a variable, click the right mouse button at the place where you want to insert it, select Insert Fields and then select a variable name from the menu. You can also use regular expressions when writing a script. It is a good idea to test your regular expression to ensure it works properly. To

do this, click **Test Regular Expression** tab.



When the script is ready you can test whether it works properly. Enter your source data into the **Input Variables** window and click **Test**. Look at the results in the **Output Variables** window. If there are any errors, you will see them in the **Errors** screen. After you ensure the script works as expected, click **OK** to save it. The script will be added to the grid.

The Complex Filter works as a Pascal-like language interpreter. The basic differences from the standard Pascal are:

- all variables stored as variants;
- no need to declare variables, labels and functions. The Complex Filter creates variables dynamically on first assignment. Variable type depends on the last value assigned; type checking is not carried out.

You can use the following functions, procedures, and operators to write the script:

### Expressions syntax:

Arithmetic operators:	+, -, *, /, ^ (power), SHL, SHR
Bitwise operators:	BITOR,BITAND,BITXOR,BITNOT
Logical operators:	>, <, >=, <=, =, <>, AND, OR, NOT, constants TRUE and FALSE.
Operators precedence standard:	BEGIN... END IF... THEN... ELSE CASE FOR... TO/DOWNTO... DO WHILE... DO REPEAT... UNTIL BREAK CONTINUE GOTO EXIT USES INCLUDE

### String functions/procedures:

Val	Val converts the string value S to its numeric representation, as if it were read from a text file with Read. procedure Val(S; var V; var Code: Integer);
IntToStr	IntToStr converts an integer into a string containing the decimal representation of that number. function IntToStr(Value: Integer): string;

StrToInt	StrToInt converts the string S, which represents an integer-type number in either decimal or hexadecimal notation, into a number. function StrToInt(const S: string): Integer;
StrToIntDef	StrToIntDef converts the string S, which represents an integer-type number in either decimal or hexadecimal notation, into a number. function StrToIntDef(const S: string; Default: Integer): Integer;
FloatToStr	FloatToStr converts the floating-point value given by Value to its string representation. The conversion uses general number format with 15 significant digits. function FloatToStr(Value: Extended): string;
StrToFloat	Use StrToFloat to convert a string, S, to a floating-point value. S must consist of an optional sign (+ or -), a string of digits with an optional decimal point, and an optional mantissa. The mantissa consists of 'E' or 'e' followed by an optional sign (+ or -) and a whole number. Leading and trailing blanks are ignored. function StrToFloat(const S: string): Extended;
Copy	Copy returns a substring or sub array containing Count characters or elements starting at S[Index]. function Copy(S; Index, Count: Integer): string;
Pos	Pos searches for a substring, Substr, in a string, S. function Pos(Substr: string; S: string): Integer;
Length	Length returns the number of characters actually used in the string or the number of elements in the array. function Length(S): Integer;

Insert	<p>Insert merges Source into S at the position S[Index].</p> <pre>procedure Insert(Source: string; var S: string; Index: Integer);</pre>
Delete	<p>Delete removes a substring of Count characters from string S starting with S[Index].</p> <pre>procedure Delete(var S: string; Index, Count:Integer);</pre>
Trim	<p>Trim removes leading and trailing spaces and control characters from the given string S.</p> <pre>function Trim(const S: string): string;</pre>
TrimLeft	<p>TrimLeft returns a copy of the string S with leading spaces and control characters removed.</p> <pre>function TrimLeft(const S: string): string;</pre>
TrimRight	<p>TrimRight returns a copy of the string S with trailing spaces and control characters removed.</p> <pre>function TrimRight(const S: string): string;</pre>
UpperCase	<p>UpperCase returns a copy of the string S, with the same text but with all 7-bit ASCII characters between 'a' and 'z' converted to uppercase.</p> <pre>function UpperCase(const S: string): string;</pre>
LowerCase	<p>LowerCase returns a string with the same text as the string passed in S, but with all letters converted to lowercase. The conversion affects only 7-bit ASCII characters between 'A' and 'Z'.</p> <pre>function LowerCase(const S: string): string;</pre>
Format	<p>This function formats the series of arguments in the open array Args.</p> <pre>function Format(const Format: string; const Args: array of const): string;</pre>

StrReplace	<p>StrReplace replaces occurrences of the substring specified by OldPattern with the substring specified by NewPattern. StrReplace assumes that the source string, specified by S, may contain Multibyte characters.</p> <p>function StrReplace(const S, OldPattern, NewPattern: string; [[0/1],[0/1]]): string;  Square brackets enclose optional parameters.</p> <p>function StrReplace(const S, OldPattern, NewPattern: string; 0): string; -StrReplace only replaces the first occurrence of OldPattern in S.</p> <p>function StrReplace(const S, OldPattern, NewPattern: string; 1): string; - all instances of OldPattern are replaced by NewPattern.</p> <p>function StrReplace(const S, OldPattern, NewPattern: string; 0/1,1): string; - the comparison operation is case insensitive.</p> <p>Examples:</p> <p>A := StrReplace(b,'old','new');</p> <p>A := StrReplace(b,'old','new',1);</p> <p>A := StrReplace(b,'old','new',0,1);</p>
Chr	<p>Chr returns the character with the ordinal value (ASCII value) of the byte-type expression, X.</p> <p>function Chr(X: Byte): Char;</p>

### **DateTime functions:**

Now	<p>Returns the current date and time, corresponding to Date + Time.</p> <p>function Now: TDateTime;</p>
Date	<p>Use Date to obtain the current local date as a TDateTime value.</p> <p>function Date: TDateTime;</p>

Time	Time returns the current time as a TDateTime value. function Time: TDateTime;
DateToStr	Use DateToStr to obtain a string representation of a date value that can be used for display purposes. function DateToStr(Date: TDateTime): string;
StrToDate	Call StrToDate to parse a string that specifies a date. function StrToDate(const S: string): TDateTime;
TimeToStr	TimeToStr converts the Time parameter, a TDateTime value, to a string. function TimeToStr(Time: TDateTime): string;
StrToTime	Call StrToTime to parse a string that specifies a time value. function StrToTime(const S: string): TDateTime;
FormatDateTime	FormatDateTime formats the TDateTime value given by DateTime using the format given by Format. function FormatDateTime(const Format: string; DateTime: TDateTime): string;
DayOfWeek	DayOfWeek returns the day of the week of the specified date as an integer between 1 and 7, where Sunday is the first day of the week and Saturday is the seventh. function DayOfWeek(Date: TDateTime): Integer;
IncMonth	IncMonth returns the value of the Date parameter, incremented by NumberOfMonths months. function IncMonth(const Date: TDateTime; NumberOfMonths: Integer = 1): TDateTime;

DecodeDate	<p>The DecodeDate procedure breaks the value specified as the Date parameter into Year, Month, and Day values.</p> <pre>procedure DecodeDate(Date: TDateTime; var Year, Month, Day: Word);</pre>
DecodeTime	<p>DecodeTime breaks the object specified as the Time parameter into hours, minutes, seconds, and milliseconds.</p> <pre>procedure DecodeTime(Time: TDateTime; var Hour, Min, Sec, MSec: Word);</pre>
EncodeDate	<p>EncodeDate returns a TDateTime value from the values specified as the Year, Month, and Day parameters.</p> <pre>function EncodeDate(Year, Month, Day: Word): TDateTime;</pre>
EncodeTime	<p>EncodeTime encodes the given hour, minute, second, and millisecond into a TDateTime value.</p> <pre>function EncodeTime(Hour, Min, Sec, MSec: Word): TDateTime;</pre>
<b>Math functions:</b>	
Abs	<p>Abs returns the absolute value of the argument, X.</p> <pre>function Abs(X);</pre>
Int	<p>Int returns the integer part of X; that is, X rounded toward zero.</p> <pre>function Int(X: Extended): Extended;</pre>
Frac	<p>The Frac function returns the fractional part of the argument X.</p> <pre>function Frac(X: Extended): Extended;</pre>
Round	<p>The Round function rounds a real-type value to an integer-type value.</p> <pre>function Round(X: Extended): Int64;</pre>

Ceil	<p>Call Ceil to obtain the lowest integer greater than or equal to X. The absolute value of X must be less than MaxInt.</p> <pre>function Ceil(const X: Extended): Integer;</pre>
Floor	<p>Call Floor to obtain the highest integer less than or equal to X.</p> <pre>function Floor(const X: Extended): Integer;</pre>
Trunc	<p>The Trunc function truncates a real-type value to an integer-type value.</p> <pre>function Trunc(X: Extended): Int64;</pre>
Sin	<p>The Sin function returns the sine of the argument.</p> <pre>function Sin(X: Extended): Extended;</pre>
Cos	<p>Cos returns the cosine of the angle X, in radians.</p> <pre>function Cos(X: Extended): Extended;</pre>
Tan	<p>Tan returns the tangent of X.</p> <pre>function Tan(const X: Extended): Extended;</pre>
ArcSin	<p>ArcSin returns the inverse sine of X.</p> <pre>function ArcSin(const X: Extended): Extended;</pre>
ArcCos	<p>ArcCos returns the inverse cosine of X.</p> <pre>function ArcCos(const X: Extended): Extended;</pre>
ArcTan	<p>ArcTan returns the arctangent of X.</p> <pre>function ArcTan(X: Extended): Extended;</pre>
Exp	<p>Exp returns the value of e raised to the power of X, where e is the base of the natural logarithms.</p> <pre>function Exp(X: Real): Real;</pre>
Ln	<p>Ln returns the natural logarithm (<math>\text{Ln}(e) = 1</math>) of the real-type expression X.</p> <pre>function Ln(X: Real): Real;</pre>
IntPower	<p>IntPower raises Base to the Power specified by Exponent.</p> <pre>function IntPower(Base: Extended; Exponent: Integer): Extended;</pre>

Sqr	The Sqr function returns the square of the argument. function Sqr(X: Extended): Extended;
Sqrt	Returns the square root of X. function Sqrt(X: Extended): Extended;
Inc	Inc adds one or N to the variable X. procedure Inc(var X [ ; N: Longint ] );
Dec	The Dec procedure subtracts one or N from a variable. procedure Dec(var X[ ; N: Longint]);
<b>Other functions:</b>	
Beep	Beep calls the Windows API MessageBeep. procedure Beep;
ShowMessage	Call ShowMessage to display a simple message box with an OK button. procedure ShowMessage(const Msg: string);
Min	Call Min to compare multiple numeric or string values. Min returns the smaller value of all. function Min(A,B,[C,]: Integer): Integer; function Min('A','B',['C',]): String): String;
Max	Call Max to compare multiple numeric or string values. Max returns the greater value of all. function Max(A,B,[C,]: Integer): Integer; function Max('A','B',['C',]): String): String;

On the simplest level, a program is a sequence of tokens delimited by separators. A token is the smallest meaningful unit of text in a program. A separator is either a blank or a comment. Strictly speaking, it is not always necessary to place a separator between two tokens; for example, the code fragment

```
Size:=20;Price:=10;
```

is perfectly legal. Convention and readability, however, dictate that we

write this as

```
Size := 20;  
Price := 10;
```

Tokens are categorized as special symbols, identifiers, reserved words, numerals, labels, and character strings. A separator can be part of a token only if the token is a character string. Adjacent identifiers, reserved words, numerals, and labels must have one or more separators between them.

Since Fields Processor script language is case-insensitive, an identifier like CalculateValue could be written in any of these ways:

```
CalculateValue  
calculateValue  
calculatevalue  
CALCULATEVALUE
```

## Comments

Comments are ignored by the script, except when they function as separators.

There are several ways to construct comments:

```
{ Text between a left brace and a right brace constitutes a comment. }  
// Any text between a double-slash and the end of the line constitutes a  
comment.
```

## Assignment Statements

An assignment statement has the form

variable := expression;

where variable is any variable reference—including a variable, variable typecast, dereferenced pointer, or component of a structured variable—and expression is any assignment-compatible expression.

The := symbol is sometimes called the assignment operator.

An assignment statement replaces the current value of variable with the value of expression. For example,

I := 3;

assigns the value 3 to the variable I. The variable reference on the left side of the assignment can appear in the expression on the right. For example,

I := I + 1;

increments the value of I.

## Compound Statements

A compound statement is a sequence of other (simple or structured) statements to be executed in the order in which they are written. The compound statement is bracketed by the reserved words begin and end, and its constituent statements are separated by semicolons. For example:

Begin

  Z := X;

  X := Y;

  Y := Z;

end;

Compound statements are essential in contexts where Fields Processor script syntax requires a single statement. In addition to program, function, and procedure blocks, they occur within other structured statements, such as conditionals or loops. For example:

```
begin
  I := SomeConstant;
  while I > 0 do
    begin
      ...
      I := I - 1;
    end;
  end;
```

## Control Loops

Loops allow you to execute a sequence of statements repeatedly, using a control condition or variable to determine when the execution stops. Fields Processor Language has three kinds of control loop: repeat statements, while statements, and for statements.

You can use the standard Break and Continue procedures to control the flow of a repeat, while, or for statement. Break terminates the statement in which it occurs, while Continue begins executing the next iteration of the sequence.

## Repeat Statements

The syntax of a repeat statement is

```
repeat statement1; ...; statement; until expression
```

where expression returns a Boolean value. (The last semicolon before

until is optional.) The repeat statement executes its sequence of constituent statements continually, testing expression after each iteration. When expression returns True, the repeat statement terminates. The sequence is always executed at least once because expression is not evaluated until after the first iteration.

Examples of repeat statements include

repeat

    K := I mod J;

    I := J;

    J := K;

until J = 0;

## While Statements

A while statement is similar to a repeat statement, except that the control condition is evaluated before the first execution of the statement sequence. Hence, if the condition is false, the statement sequence is never executed.

The syntax of a while statement is  
while expression do statement

where expression returns a Boolean value and statement can be a compound statement. The while statement executes its constituent statement repeatedly, testing expression before each iteration. As long as expression returns True, execution continues.

Examples of while statements include

while Length(S) > 0 do

begin

    N := N + Copy(S,Length(S),1);

```
Delete(S,Length(S),1)
end;
```

## For Statements

A for statement, unlike a repeat or while statement, requires you to specify explicitly the number of iterations you want the loop to go through. The syntax of a for statement is

```
for counter := initialValue to finalValue do statement
or
for counter := initialValue downto finalValue do statement
where
```

counter is a local variable (declared in the block containing the For statement) of ordinal type, without any qualifiers.

initialValue and finalValue are expressions that are assignment-compatible with counter.

statement is a simple or structured statement that does not change the value of counter.

The for statement assigns the value of initialValue to counter, then executes statement repeatedly, incrementing or decrementing counter after each iteration. (The for...to syntax increments counter, while the for...downto syntax decrements it.) When counter returns the same value as finalValue, statement is executed once more and the for statement terminates. In other words, statement is executed once for every value in the range from initialValue to finalValue. If initialValue is equal to finalValue, statement is executed exactly once. If initialValue is greater than finalValue in a for...to statement, or less than finalValue in a for...downto statement, then statement is never executed. After the for

statement terminates, the value of counter is undefined.

For purposes of controlling execution of the loop, the expressions `initialValue` and `finalValue` are evaluated only once, before the loop begins. Hence the `for...to` statement is almost, but not quite, equivalent to this `while` construction:

```
begin
  counter := initialValue;
  while counter <= finalValue do
    begin
      statement;
      counter := Succ(counter);
    end;
  end
end
```

The difference between this construction and the `for...to` statement is that the `while` loop re-evaluates `finalValue` before each iteration. This can result in noticeably slower performance if `finalValue` is a complex expression, and it also means that changes to the value of `finalValue` within statement can affect execution of the loop.

Examples of `for` statements:

```
for I := 65 to 123 do
  S := S + Chr(i);
for I := Length(S) downto 0 do
  N := N + Copy(S,1,1);
for I := 1 to 10 do
  for J := 1 to 10 do
    begin
      some operatos
    end;
```

## Case Statements

The case statement provides a readable alternative to complex nested if conditionals. A case statement has the form

```
case selectorExpression of
  caseList1: statement1;
  ...
  caseListn: statementn;
end
```

where selectorExpression is any expression of an ordinal type (string types are invalid) and each caseList is one of the following:

A numeral, declared constant, or other expression that the compiler can evaluate without executing your program. It must be of an ordinal type compatible with selectorExpression. Thus 7, True, 4 + 5 \* 3, 'A', and Integer('A') can all be used as caseLists, but variables and most function calls cannot. (A few built-in functions can occur in a caseList.)

A subrange having the form First..Last, where First and Last both satisfy the criterion above and First is less than or equal to Last.

A list having the form item1, ..., itemn, where each item satisfies one of the criteria above.

Each value represented by a caseList must be unique in the case statement; subranges and lists cannot overlap. A case statement can have a final else clause:

```
case selectorExpression of
  caseList1: statement1;
  ...
  caseListn: statementn;
```

```
else
  statements;
end
```

where statements is a semicolon-delimited sequence of statements. When a case statement is executed, at most one of statement1 ... statementn is executed. Whichever caseList has a value equal to that of selectorExpression determines the statement to be used. If none of the caseLists has the same value as selectorExpression, then the statements in the else clause (if there is one) are executed.

The case statement

```
case I of
  1..5: Caption := 'Low';
  6..9: Caption := 'High';
  0, 10..99: Caption := 'Out of range';
else
  Caption := '';
end;
```

is equivalent to the nested conditional

```
if I in [1..5] then
  Caption := 'Low'
else if I in [6..10] then
  Caption := 'High'
else if (I = 0) or (I in [10..99]) then
  Caption := 'Out of range'
else
  Caption := '';
```

## If Statements

There are two forms of if statement: if...then and the if...then...else. The

syntax of an if...then statement is

if expression then statement

where expression returns a Boolean value. If expression is True, then statement is executed; otherwise it is not. For example,

```
if J <> 0 then Result := I/J;
```

The syntax of an if...then...else statement is  
if expression then statement1 else statement2

where expression returns a Boolean value. If expression is True, then statement1 is executed; otherwise statement2 is executed. For example,  
if J = 0 then

```
    Exit  
else  
    Result := I/J;
```

The then and else clauses contain one statement each, but it can be a structured statement. For example,

```
if J <> 0 then  
begin  
    Result := I/J;  
    Count := Count + 1;  
end  
else if Count = Last then  
    Done := True  
else  
    Exit;
```

Notice that there is never a semicolon between the then clause and the

word else. You can place a semicolon after an entire if statement to separate it from the next statement in its block, but the then and else clauses require nothing more than a space or carriage return between them. Placing a semicolon immediately before else (in an if statement) is a common programming error.

## Character Strings

You can assign the value of a string constant—or any other expression that returns a string—to a variable. The length of the string changes dynamically when the assignment is made. Examples:

```
MyString := 'Hello Alex!';  
MyString := 'Hello ' + 'Alex';  
MyString := MyString + '!';  
MyString := ' ';           { space }  
MyString := '';            { empty string }
```

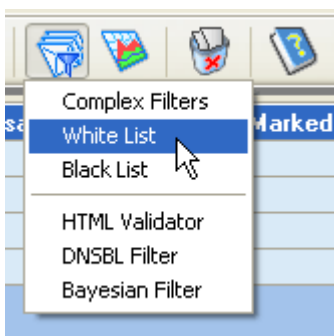
## Adding Emails to Whitelist

For your convenience and saving time, you can let SpamCombat automatically flag emails you receive from known sources as good. You can whitelist messages based on some words or regular expressions in the message header and/or body, and by the sender's IP address(es).

**Important!** If you are concerned about your computer's security, we do not recommend that you whitelist all the email addresses from an Outlook or any other address book. You may receive an email coming from your friend's email address but actually this may be an email with a virus. You should better train SpamCombat to categorize the emails sent by people you know as good.

To add emails to Whitelist:

1) double click the mouse on the Whitelist item at the program's left pane, or click Filters and select Whitelist



2) enter any name into **Name** field (not required but useful);

3) select a field where the program will look for the specified text or regular expression. From the drop down menu you can select any of the standard fields the message header includes, and some additional fields that allows parsing the message body:

Message Body & Subject:

Message Body:

Message Source:

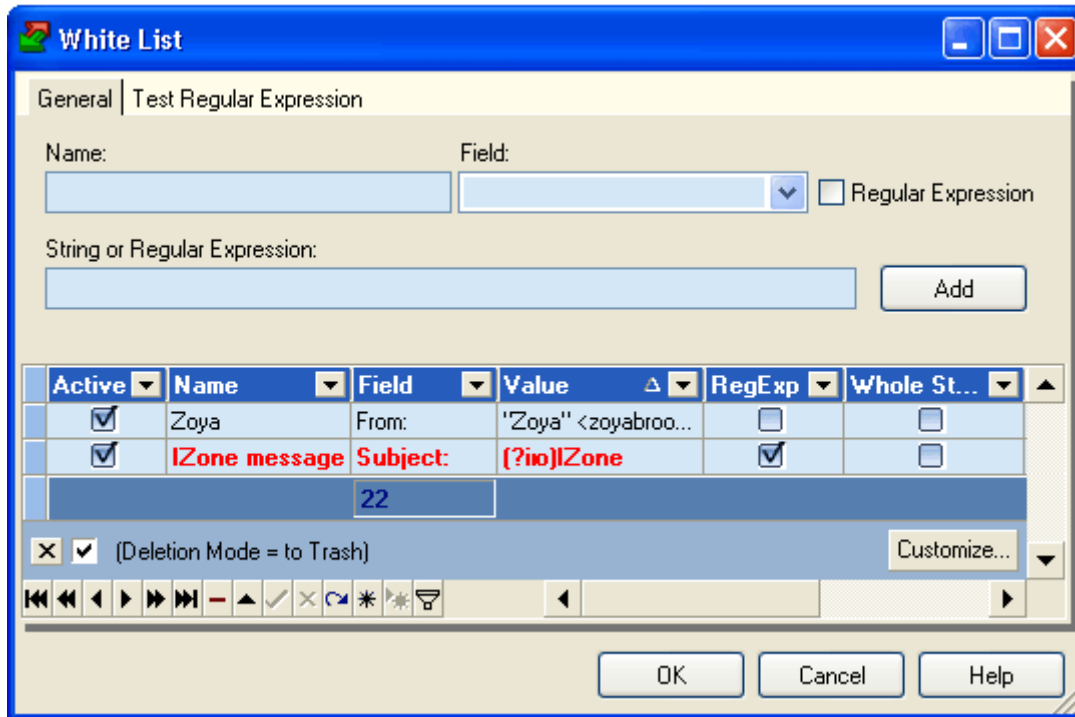
Viewable Body & Subject: (includes a stripped HTML, plain text part and subject)

Viewable HTML: (includes only a stripped HTML you can see when you receive an email)

4) enter a string or regular expression. If you add a regular expression, check **Regular Expression** checkbox. It is a good idea to test your regular expression before you add it to the Whitelist. To do this, click **Test Regular Expression** tab.

5) click **Add**.

The record is added to the grid. Not working regular expressions will be shown by **red** within the grid. You should either correct, or deactivate them.



The grid columns denote:

**Active** - status: enabled or disabled. Click the mouse on the checkbox to change the status.

**Field** - field name from the message header or message body that contains this string or regular expression

**Name** - short description of the string or regular expression

**Value** - string or regular expression used to whitelist emails

**Reg Exp** - shows if the string is a regular expression or not


**Whole String** - when this checkbox is checked, the selected field must contain only the defined value with no other words or characters

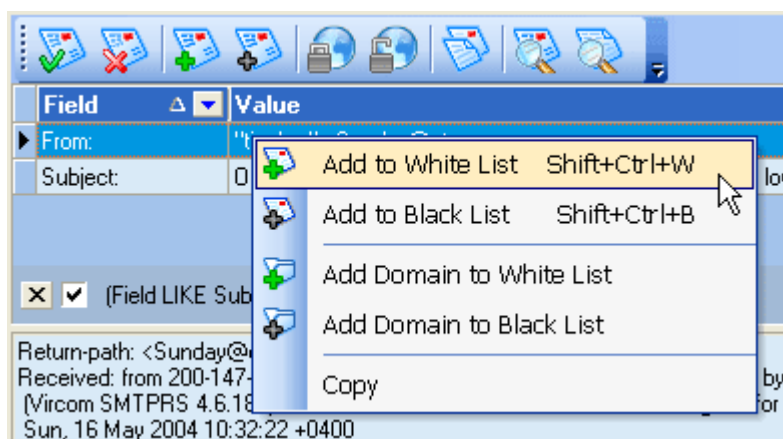
**HitRate** - shows how many times the whitelist filter worked since a user has begun working with the SpamCombat

**Last Action** - date and time when the whitelist filter last worked

**Expire** - expire period for the whitelist filter. When it is over, the record is automatically deactivated.

**Day Passed** - progressive bar showing how many days of the expire period passed

You can also add any fields from the message header to the Whitelist directly from the main window. Select a header field in the message preview screen and click  **Add to White List** button, or click the right mouse button and select **Add to White List** option. The whole value of the appropriate field is added to the Whitelist. Or, you can just drag and drop the header field straight to the Whitelist.



Duplicated records are not added to the Whitelist.

### 💡 Tips:

To whitelist emails by the sender's domain, highlight FROM header field, click the right mouse button and then select **Add Domain to Whitelist** option. Or, you can manually add this regular expression `(?iU)[\S\d\.] +@domain.com` to the Whitelist.

To whitelist emails by the sender's IP address(es), select **IP Address** in the **Field** and type the IP address in the input string. Click **Add**. The simplest case is to whitelist a single IP address: 127.0.0.1

You can also add a subset of IP addresses by entering the first and last IPs of the range separated by dash:

127.0.0.1-127.0.0.254

127.0.0.1-127.0.254.254

or use network prefix notation:

127.0.0.1/24

127.0.0.1/16

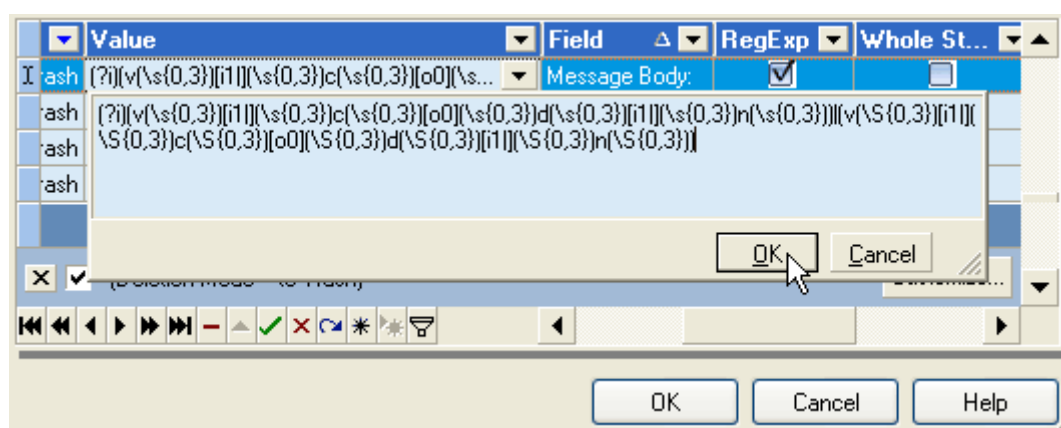
SpamCombat works with B and C classes of IP addresses only.

When you select **FROM** field to whitelist emails, only the email address with no additional characters is extracted and added. To add the whole value of FROM field to the Whitelist, just drag the selected string and drop it to the Whitelist.

## Working with Whitelist

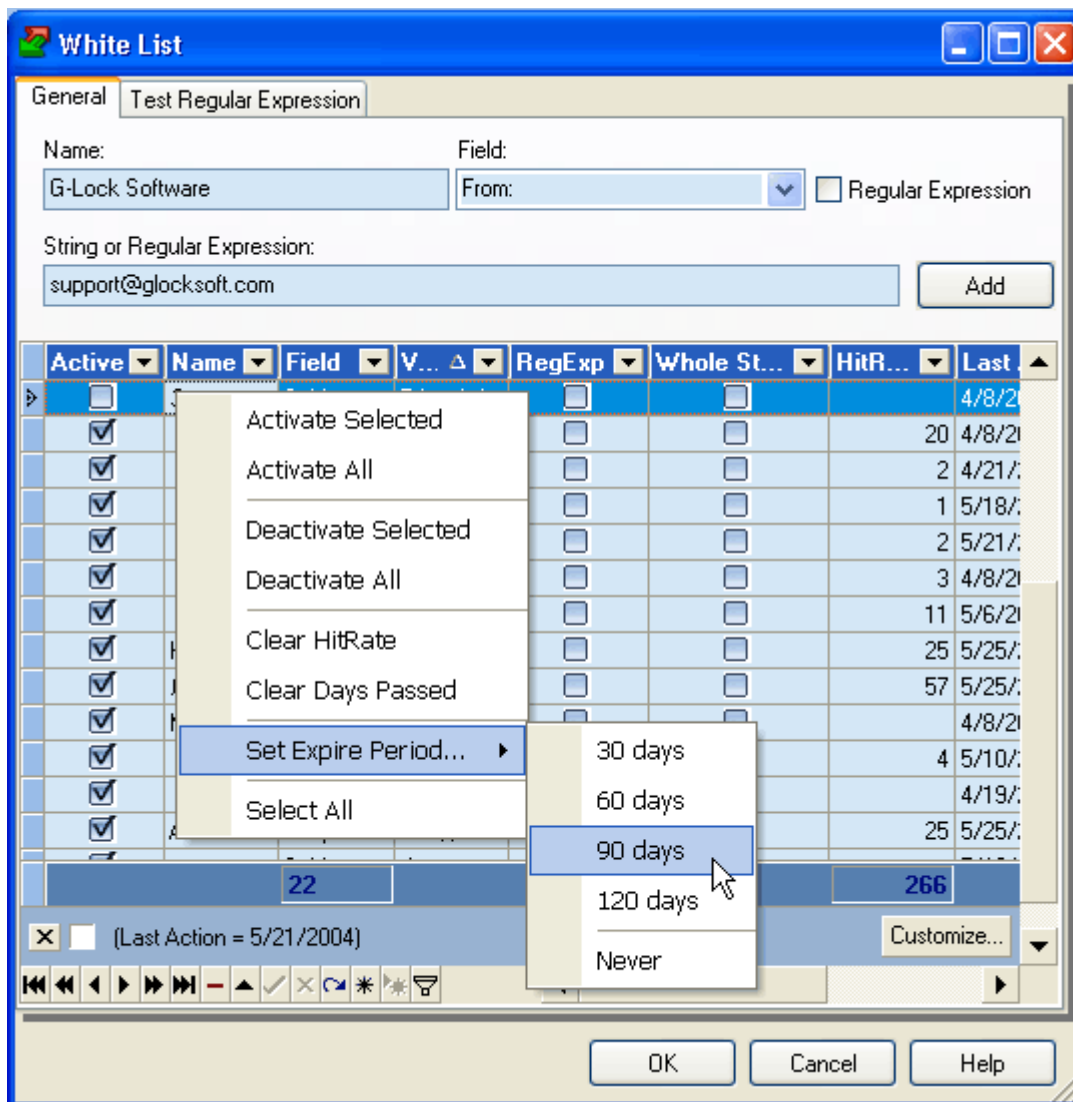
To edit a record within the grid, select it and press Enter on your keyboard. The record will become available for editing.

When you edit the field Value, click either OK or Cancel on the edit screen to save or cancel the changes you made.



When you finished editing the Whitelist filters, click OK at the bottom of the screen to save the changes.

If you click the right mouse button on the selected filter within the grid, you'll see the following menu:



**Activate Selected** - allows you to activate the selected filter

**Activate All** - allows you to activate all the filter

**Deactivate Selected** - allows you to deactivate the selected filter

**Deactivate All** - allows you to deactivate all the filters

**Clear HitRate** - allows you to set the HitRate statistics to 0. Although the HitRate is cleared, you should click OK to save the changes.

**Clear Days Passed** - clears the progressing bar so that the expiration period for the selected filter restarts

**Set Expire Period** - allows you to set the expire period for the filter: 30, 60, 90, 120 days, or never. Or you can enter any quantity of days by yourself.

**Select All** - allows you to select all the filters within the grid

At the bottom of the grid there is also a range of buttons you can use to work with the whitelist filters. Put the cursor to the button to know its function.

For easy search for a string or regular expression within the grid, you can use an incremental search. An incremental search allows you to locate a record within the grid by matching the initial characters of a record field.

To search for a record by a field value, focus on a record cell within the appropriate column and type the search text. If the grid contains a record with a value that starts with the search text, the record is focused.

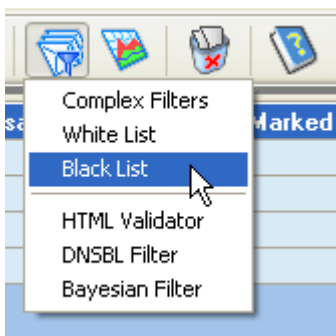
For your convenience you can sort and filter the records within the grid as you want. See **Sorting and Filtering Emails**

### Adding Emails to Blacklist

The Blacklist stands opposite the Whitelist. Here you can add suspicious, unknown, or unwanted emails and their senders. SpamCombat is provided with a solid Blacklist that detects the most known kinds of spam and virus emails. The default system blacklist filters are shown by the navy color within the grid. You can edit them as you want.

To add emails to Blacklist:

1) double click the mouse on the Blacklist item at the program's left pane, or click Filters and select Blacklist



2) enter any name into Name field (not required but useful);

3) select a field where the program will look for the specified text or regular expression. From the drop down menu you can select any of the standard fields the message header includes, and some additional fields that allows parsing the message body:

Message Body & Subject:

Message Body:

Message Source:

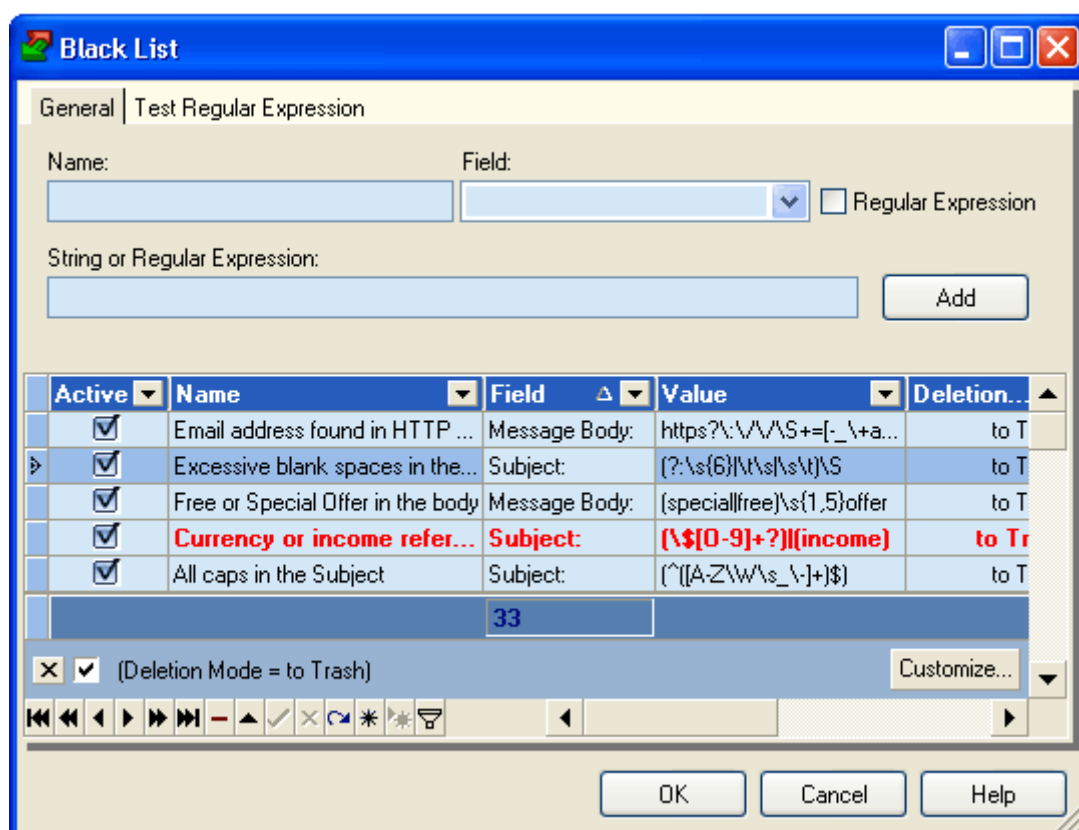
Viewable Body & Subject: (includes a stripped HTML, plain text part and subject)

Viewable HTML: (includes only a stripped HTML you can see when you receive an email)

4) enter a string or regular expression. If you use a regular expression, check **Regular Expression** checkbox. It is a good idea to test your regular expression before you add it to the Blacklist. To do this, click **Test Regular Expression** tab.

5) click **Add**.

The record is added to the grid. Your own blacklist filters will be shown by **black**. Wrong (not working) regular expressions within the grid will be marked by **red**. You should either correct, or deactivate them.



The grid columns denote:

**Active** - status: enabled or disabled. Click the mouse on the checkbox to change the status.

**Field** - field name from the message header or message body that contains this string or regular expression


**Deletion Mode** - deletion mode for blacklisted emails:

**to Trash** - emails are moved to **Deleted Items** folder after you click **Delete** button

**Permanently** - emails are deleted permanently and not saved to the disk after you click **Delete** button

**Move to Trash During Mail Check** - emails are moved to **Deleted Items** folder during the accounts check

**Delete During Mail Check** - emails are deleted permanently during the accounts check

 **Note:** If auto-deleting spam emails in the Automation settings is enabled, **Delete Permanently** and **Delete During Mail Check** modes work similarly: the emails are permanently deleted during mail check. The filters with **Delete During Mail Check** deletion mode are executed the first.

**Name** - short description of the string or regular expression

**Value** - string or regular expression used to blacklist emails

**Reg Exp** - shows if the string is a regular expression or not


**Whole String** - when this checkbox is checked, the selected field must contain only the defined value with no other words or characters

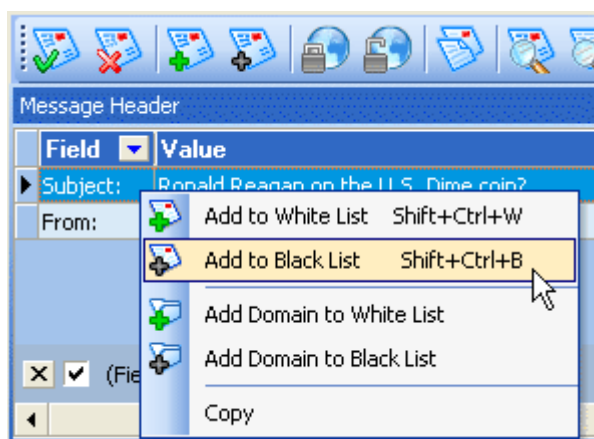
**HitRate** - shows on how many times the blacklist filter worked since a user has begun working with the SpamCombat

**Last Action** - date and time when the blacklist filter last worked

**Expire** - expire period for the blacklist filter. When it is over, the record is automatically deactivated.

**Day Passed** - progressive bar showing how many days of the expire period passed

You can also add any fields from the message header to the Blacklist directly from the main window. Select a header field in the message preview screen and click  **Add to Black List** button, or click the right mouse button and select **Add to Black List** option. The whole value of the appropriate field is added to the Blacklist. Or, you can just drag and drop the header field straight to the Blacklist.



Duplicated records are not added to the Blacklist.

### 💡 Tips:

To blacklist emails by the sender's domain, highlight FROM header field, click the right mouse button and then select **Add Domain to Blacklist** option. Or, you can manually add this regular expression `(?iU)[\S\d\.] + @domain.com` to the Blacklist.

To blacklist emails by the sender's IP address(es), select **IP Address** in the **Field** and type the IP address in the input string. Click **Add**. The simplest case is to whitelist a single IP address: 127.0.0.1

You can also add a subset of IP addresses by entering the first and last IPs of the range separated by dash:

127.0.0.1-127.0.0.254

127.0.0.1-127.0.254.254

or use network prefix notation:

127.0.0.1/24

127.0.0.1/16

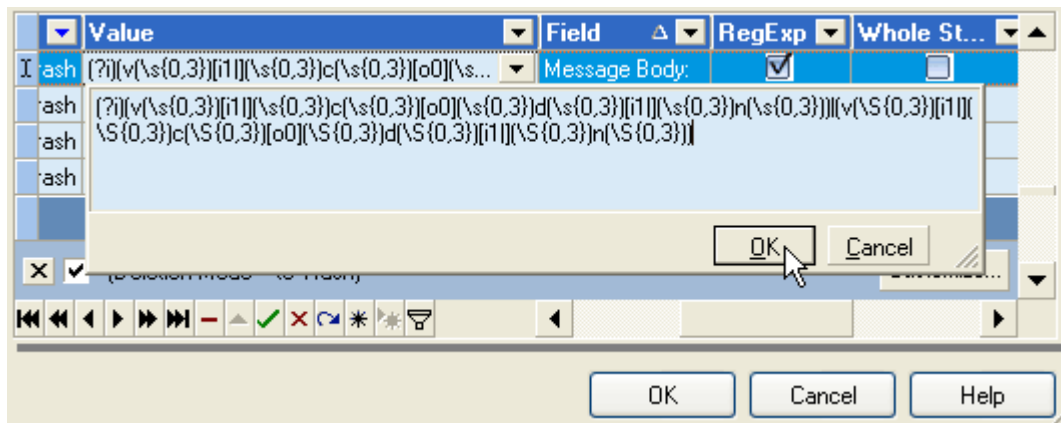
SpamCombat works with B and C classes of IP addresses only.

When you select **FROM** field to blacklist emails, only the email address with no additional characters is extracted and added. To add the whole value of FROM field to the Blacklist, just drag the selected string and drop it to the Blacklist.

To edit a string within the grid, select the string you want to edit and press **Enter** on your keyboard. The string will become highlighted and available for editing.

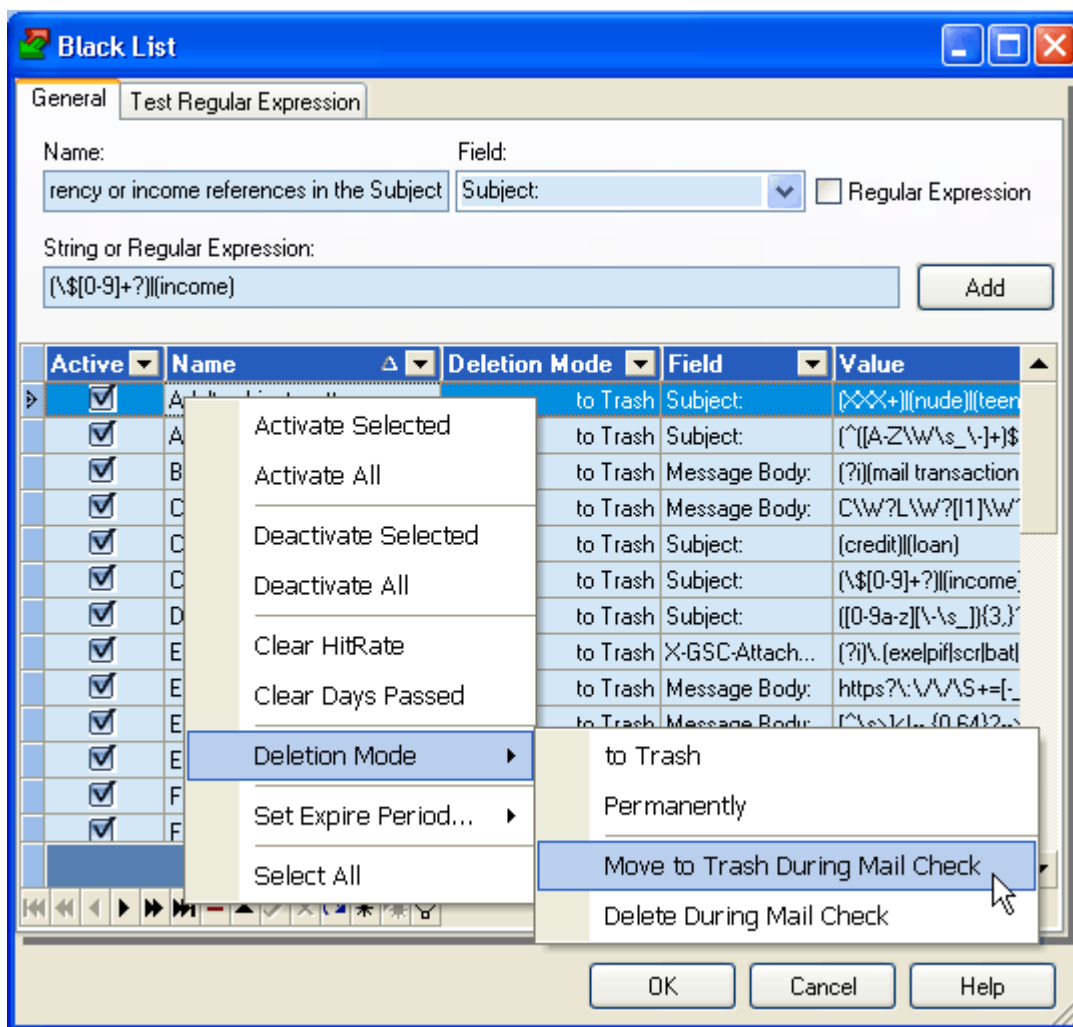
## Working with Blacklist

To edit a record within the grid, select it and press **Enter** on your keyboard. The string will become available for editing. When you edit the field Value, click either OK or Cancel to save or cancel the changes you made.



When you finished editing the Blacklist filters, click OK at the bottom of the screen to save the changes.

If you click the right mouse button on the selected filter within the grid, you'll see the following menu:



**Activate Selected** - allows you to activate the selected filter

**Activate All** - allows you to activate all the filters

**Deactivate Selected** - allows you to deactivate the selected filters

**Deactivate All** - allows you to deactivate all the filters

**Clear HitRate** - allows you to set the HitRate statistics in the selected string to 0. Although the HitRate is cleared, you should click OK to save the changes.

**Clear Days Passed** - clears the progressing bar so that the expire period for the selected filter restarts

**Deletion Mode** - allows you to set a deletion mode for spam emails detected by the selected filter: Move to Trash, Delete Permanently, Move

to Trash During Mail Check, or Delete During Mail Check.

**Set Expire Period** - allows you to set the expiration period for the filter: 30, 60, 90, 120 days, or never. Or you can enter any quantity of days by yourself.

**Select All** - allows you to select all the filters within the grid

At the bottom of the grid there is also a range of buttons you can use to work with the whitelist filters. Put the cursor to the button to know its function.

For easy search for a string or regular expression within the grid, you can use an incremental search. An incremental search allows you to locate a record within the grid by matching the initial characters of a record field.

To search a record by a field value, focus on a record cell within the appropriate column and type the search text. If the grid contains a record with a value that starts with the search text, the record is focused.

For your convenience you can sort and filter the records within the grid as you want. See **Sorting & Filtering Emails**

## Blocking Spam by Country of Origin

One of the particularities of G-Lock SpamCombat is the capability to determine an email's "country-of-origin" and use this information to block messages from any specified country. The connecting mail server's IP address is used by G-Lock SpamCombat to determine an email's country of origin.

About a dozen countries are notorious for sending spam. China, Korea and Russia are among the top spam producing countries. With the "Country-Of-Origin" filtering capability of G-Lock SpamCombat you can block all email originating from these countries with one mouse click. You can select yourself which countries to block and instantly reduce spam volumes.

You wait for the spam to arrive. You will see the country the email originates from in the **Country** column.

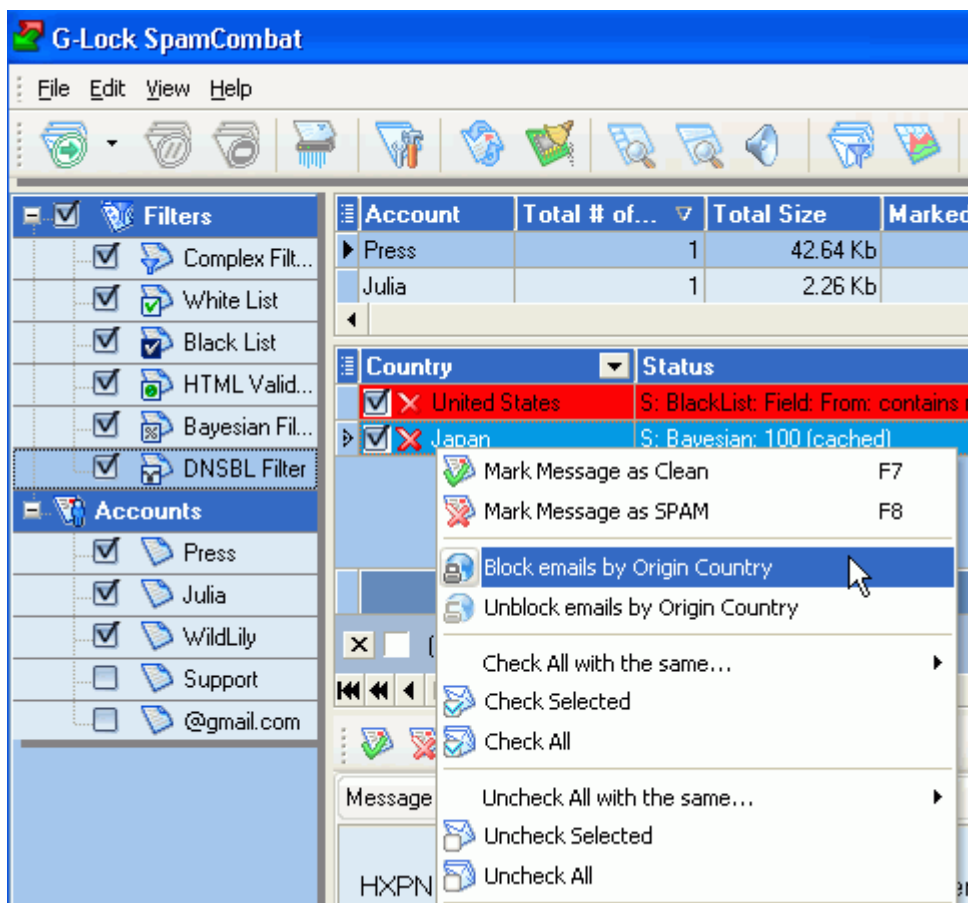
**To block all the emails from the specific country:**

- 1) Click the right mouse button on the line with the message.
- 2) Select **"Block emails by Origin Country"** from the menu.

SpamCombat will add that country name to the blacklist and all further emails you will receive from that country will be blocked by the blacklist.

**To delete a country name from the blacklist:**

- 1) click the right mouse on the line with the message.
- 2) select **"Unblock emails by Origin Country"** from the menu.



The total number of countries G-Lock SpamCombat recognizes is 232.

Here is a list of country names:

Code	Country Name
US	United States
JP	Japan
GB	United Kingdom
CN	China
DE	Germany
CA	Canada
FR	France
KR	Korea, Republic of
NL	Netherlands
AU	Australia
IT	Italy

ES Spain  
SE Sweden  
BR Brazil  
CH Switzerland  
EU Europe  
TW Taiwan  
MX Mexico  
RU Russian Federation  
NO Norway  
FI Finland  
PL Poland  
ZA South Africa  
AT Austria  
DK Denmark  
IN India  
BE Belgium  
HK Hong Kong  
TR Turkey  
IL Israel  
CZ Czech Republic  
NZ New Zealand  
IE Ireland  
RO Romania  
AR Argentina  
PT Portugal  
CL Chile  
HU Hungary  
ID Indonesia  
TH Thailand  
GR Greece  
SG Singapore  
MY Malaysia  
VE Venezuela

PH Philippines  
A2 Satellite Provider  
UA Ukraine  
BG Bulgaria  
CO Colombia  
SK Slovakia  
SA Saudi Arabia  
EG Egypt  
LT Lithuania  
CR Costa Rica  
AE United Arab Emirates  
SI Slovenia  
IR Iran, Islamic Republic of  
LV Latvia  
LU Luxembourg  
PE Peru  
EE Estonia  
PA Panama  
VN Vietnam  
CS Serbia and Montenegro  
PR Puerto Rico  
IS Iceland  
A1 Anonymous Proxy  
HR Croatia  
KW Kuwait  
TN Tunisia  
MA Morocco  
PK Pakistan  
EC Ecuador  
UY Uruguay  
KZ Kazakhstan  
BO Bolivia  
CY Cyprus

SV El Salvador  
BD Bangladesh  
NG Nigeria  
DZ Algeria  
GT Guatemala  
KE Kenya  
AG Antigua and Barbuda  
QA Qatar  
LK Sri Lanka  
PS Palestinian Territory  
OM Oman  
AN Netherlands Antilles  
MT Malta  
LB Lebanon  
DO Dominican Republic  
JO Jordan  
GE Georgia  
MK Macedonia, the Former Yugoslav Republic of  
BA Bosnia and Herzegovina  
MD Moldova, Republic of  
MO Macao  
BN Brunei Darussalam  
BY Belarus  
TT Trinidad and Tobago  
GU Guam  
AZ Azerbaijan  
UZ Uzbekistan  
JM Jamaica  
SY Syrian Arab Republic  
BH Bahrain  
GH Ghana  
HN Honduras  
MU Mauritius

CU Cuba  
VI Virgin Islands, U.S.  
AM Armenia  
BZ Belize  
NI Nicaragua  
FJ Fiji  
UG Uganda  
BT Bhutan  
KG Kyrgyzstan  
BM Bermuda  
TZ Tanzania, United Republic of  
PY Paraguay  
MN Mongolia  
BW Botswana  
AP Asia/Pacific Region  
MC Monaco  
GN Guinea  
BS Bahamas  
LI Liechtenstein  
IQ Iraq  
BB Barbados  
SD Sudan  
KH Cambodia  
NA Namibia  
CI Cote D'Ivoire  
NP Nepal  
MQ Martinique  
SZ Swaziland  
RE Reunion  
SN Senegal  
GI Gibraltar  
CM Cameroon  
NC New Caledonia

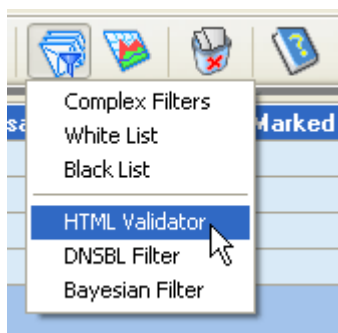
AF Afghanistan  
PF French Polynesia  
GP Guadeloupe  
HT Haiti  
MZ Mozambique  
ZW Zimbabwe  
AL Albania  
LY Libyan Arab Jamahiriya  
FO Faroe Islands  
AO Angola  
AW Aruba  
KY Cayman Islands  
YE Yemen  
TJ Tajikistan  
PG Papua New Guinea  
MG Madagascar  
AD Andorra  
GY Guyana  
LA Lao People's Democratic Republic  
GA Gabon  
ZM Zambia  
SR Suriname  
SM San Marino  
SL Sierra Leone  
GF French Guiana  
ET Ethiopia  
ML Mali  
GL Greenland  
TG Togo  
VA Holy See (Vatican City State)  
MR Mauritania  
BF Burkina Faso  
MP Northern Mariana Islands

MV Maldives  
SC Seychelles  
RW Rwanda  
KN Saint Kitts and Nevis  
MM Myanmar  
GM Gambia  
MW Malawi  
SB Solomon Islands  
AI Anguilla  
WS Samoa  
GD Grenada  
TV Tuvalu  
KP Korea, Democratic People's Republic of  
NR Nauru  
CK Cook Islands  
TC Turks and Caicos Islands  
BJ Benin  
LC Saint Lucia  
VG Virgin Islands, British  
VC Saint Vincent and the Grenadines  
VU Vanuatu  
NE Niger  
DM Dominica  
AS American Samoa  
LS Lesotho  
CD Congo  
TO Tonga  
PW Palau  
TM Turkmenistan  
DJ Djibouti  
ER Eritrea  
FM Micronesia, Federated States of  
IO British Indian Ocean Territory

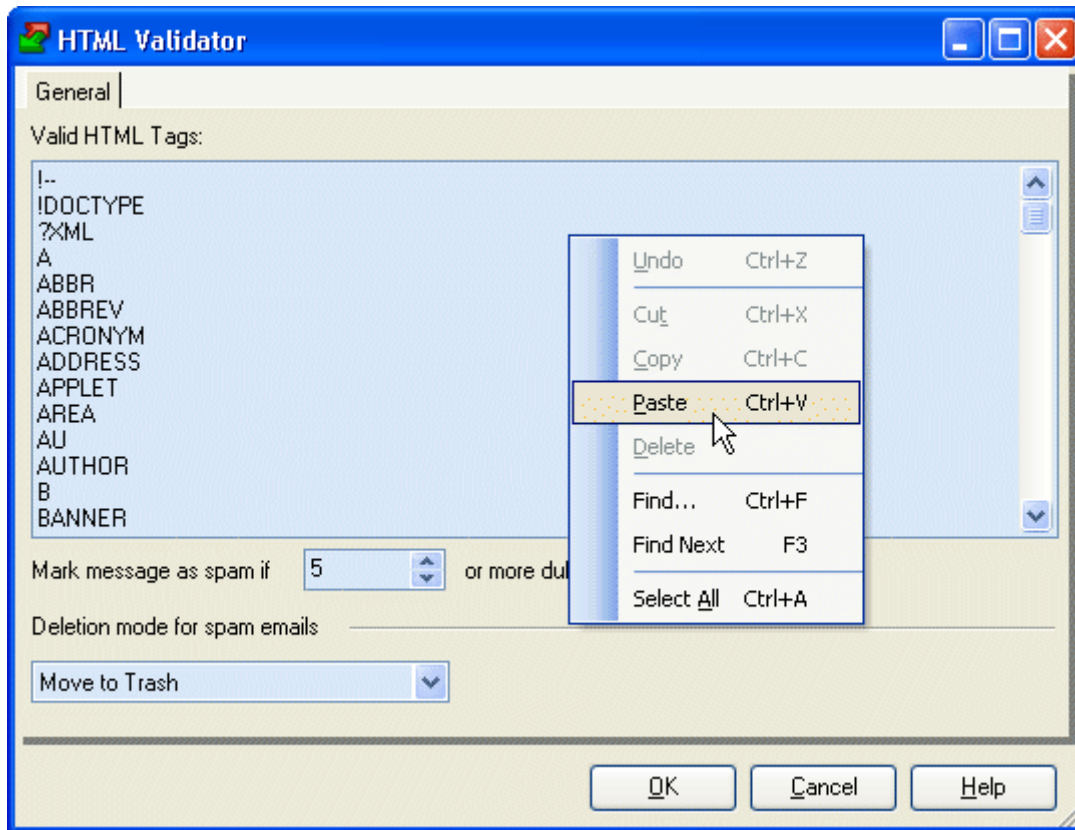
KI Kiribati  
CV Cape Verde  
LR Liberia  
BI Burundi  
CG Congo  
GW Guinea-Bissau  
CF Central African Republic  
SO Somalia  
PM Saint Pierre and Miquelon  
GQ Equatorial Guinea  
NF Norfolk Island  
FK Falkland Islands (Malvinas)  
NU Niue  
MS Montserrat  
MH Marshall Islands  
TD Chad  
TF French Southern Territories  
ST Sao Tome and Principe  
KM Comoros  
YT Mayotte  
WF Wallis and Futuna  
UM United States Minor Outlying Islands  
TK Tokelau

### Working with HTML Validator

**HTML Validator** is a filter that parses the HTML part of the incoming email and checks the HTML tags for validity. If xx dubious HTML tags are found, the message is considered spam. The HTML Validator also detects the unreadable font size (0,1 px) and incorrect color of HTML tags. To open the HTML Validator settings, click **Filters** button on the program's Toolbar and select **HTML Validator**. Or, double click the mouse on the **HTML Validator** at the left pane of the program's main window.



SpamCombat is provided with a list of valid HTML tags. You can remove HTML tags or add new tags you see appropriate. The HTML tags must be entered one per line.



Select a deletion mode for spam emails detected by the HTML Validator:

**Move to Trash** - spam emails detected by the HTML Validator will be deleted from the mail server and moved to Deleted Items folder (saved to the disk)

**Delete Permanently** - spam emails detected by the HTML Validator will be deleted from the mail server without being saved to the disk

**Move to Trash During Mail Check** - emails are moved to Deleted Items folder during the accounts check


**Delete Permanently During Mail Check** - emails are deleted permanently during the accounts check

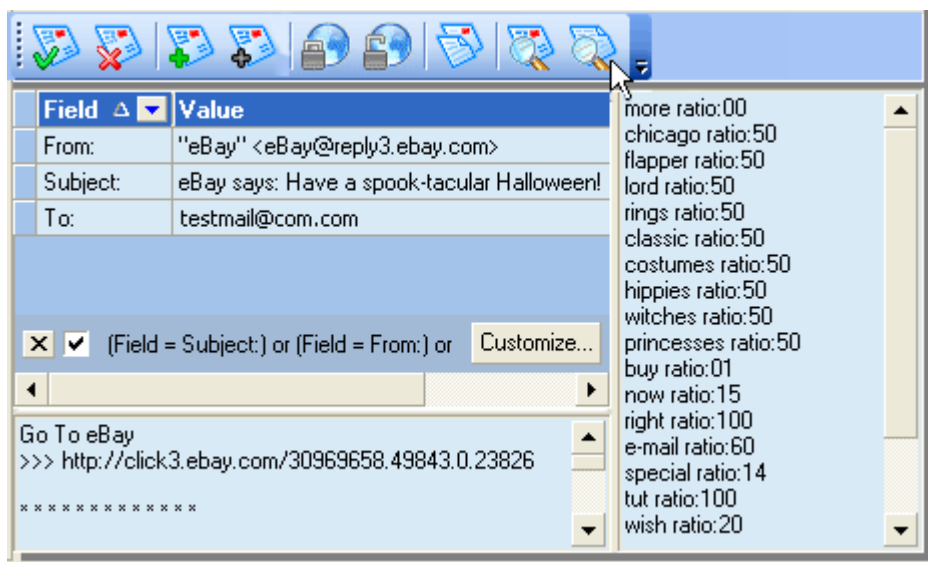
### Working with Bayesian Filter



**Bayesian filter** is the most powerful filter that detects up to 99.5% of spam emails.


The Bayesian filter is based on statistical methods, which give a probability for an email belonging to a given class: spam and not-spam usually. The Bayesian filter resorts to mathematical calculation to identify spam emails. It takes the decision whether the email is spam or normal by analyzing the words in the message content. Each word within a new incoming message is flagged depending on its popularity in the past: a word that occurs only in the messages marked as spam gets 0.99 ratio and a word that occurs only in the 'good' emails gets 0.0 ratio. Unknown words get 0.2 ratio. The ratio of all of the words within the message form 'score'. Depending on the score the Bayesian filter marks the message as 'good' or spam. If the score is greater than the spam threshold, the message is considered spam (by default the spam threshold is 90). You can read more about the Bayesian filter here

<http://www.paulgraham.com/better.html>

SpamCombat shows you the ratio of each word within the message in the separate window. Select the message with "Bayesian:..." record in the status column and click  **View/Hide Interesting Words** option. An informative window with the words and their ratio comes up.

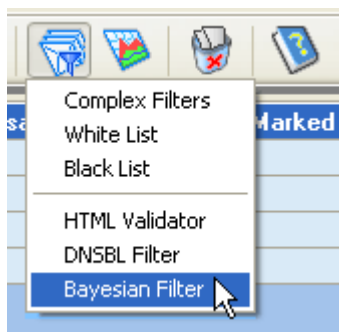


**IMPORTANT!** To get the best performance of the program, you ought to train the Bayesian filter to categorize incoming emails either as spam or normal. You should view all the emails and if they were not properly categorized, you should re-categorize those emails using  **Mark Message as Spam** and  **Mark Message as Clean** buttons. The Bayesian filter learns from its mistakes and next time it will classify the messages properly. The more you train SpamCombat, the more its accuracy increases.

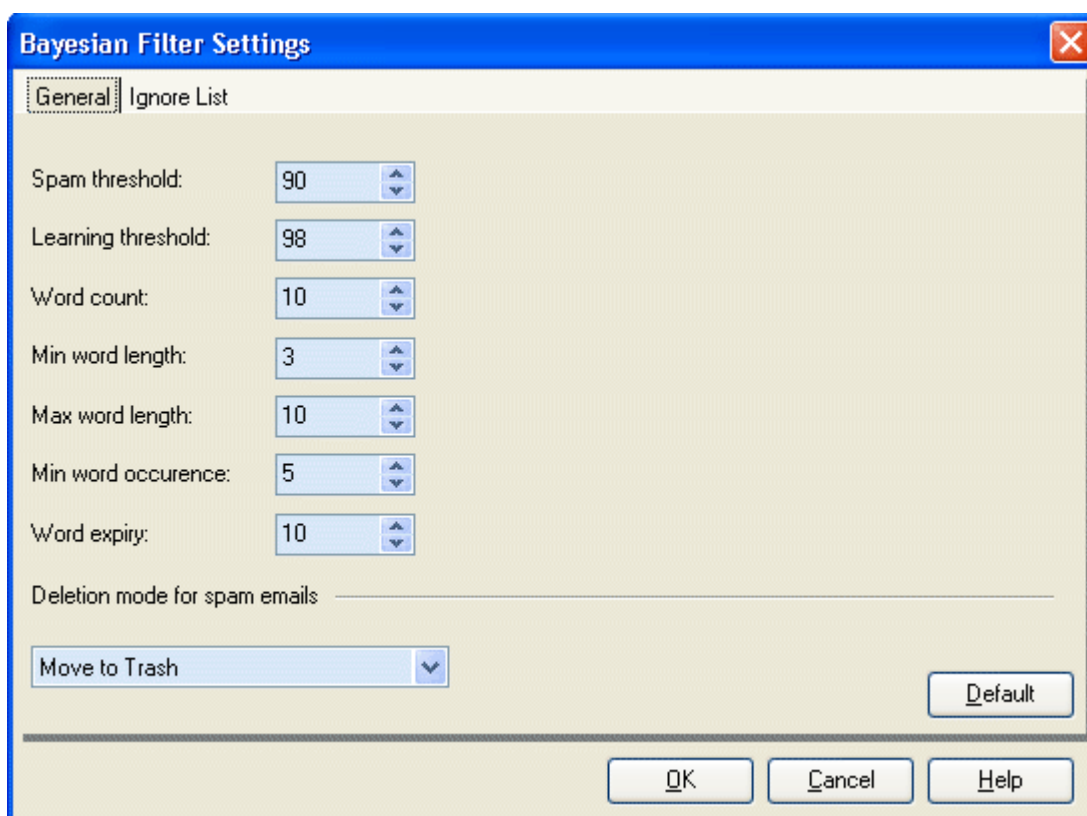
If the number of significant words in the message is less than it is set in the Bayesian Filter Settings, the Bayesian filter is not applied to the message and the email is marked by  icon. Such emails should be either whitelisted, or blacklisted by a user. If there is enough words but the email is still not resolved by the Bayesian filter, it appears with  icon. A user should manually categorize such emails as spam or good to train the Bayesian filter.

## Bayesian Filter Settings

To open the Bayesian filter settings, double click the mouse on the Bayesian Filter item at the left pane, or click Filters button on the Toolbar and select Bayesian Filter.



You can use the default Bayesian filter settings if you are not familiar with the Bayesian filter. Or, you can adjust these settings as you like.



**Spam threshold** - the default value is 90. Increasing the spam threshold reduces the number of false classifications, decreasing it makes the filter

think more email should be tagged as spam. Any word with a ratio below this threshold is considered a clean word.

**Learning threshold** - the default value is 98. Any word with a ratio greater than or equal to this is added to the database classed as spam.

**Word count** - the default value is 15. The number of significant words used to filter the message. Fewer words mean the filter is more aggressive, more words checked mean more spam words is needed to be present for an email to be classified as spam. **ATTENTION!** If the SpamCombat extracts 15 or more words from the message, the Bayesian filter learns from this message. If the message has less than 15 words, the filter does not learn from such emails even if you categorize them by yourself. It is not recommended that you decrease the number of words because it will result in an increasing number of false positives, i.e. more good emails will be marked as spam. At least, you can set 10 words but not less.

**Min word length** - the default value is 3. The minimum length of the words used to filter the message.

**Max word length** - the default value is 15. The maximum length of the words used to filter the message.

**Min word occurrence** - the default value is 5. The minimum number of times a word has to appear before it is used in filtering. A low setting will make the Bayesian filter more "trigger-happy" letting it mark emails based on less data.

**Word expiry** - the default value is 30. Every word is tagged with the time it was last encountered. This threshold ensures that words that haven't occurred recently are removed from the database. If the word does not occur in the messages within the specified number of days, it is removed from the database.

To restore the default values, click **Default** button.

Select a deletion mode for spam emails detected by the Bayesian filter:

**Move to Trash** - spam emails detected by the Bayesian filter will be deleted from the mail server and moved to Deleted Items folder (saved to the disk)

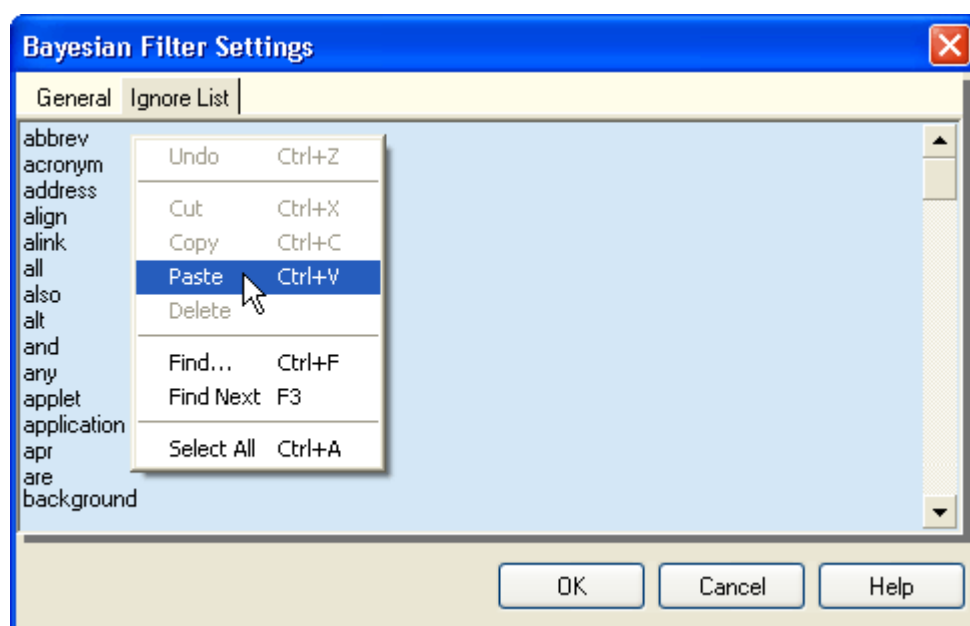
**Delete Permanently** - spam emails detected by the Bayesian filter will be deleted from the mail server without being saved to the disk

**Move to Trash During Mail Check** - emails are moved to Deleted Items folder during the accounts check

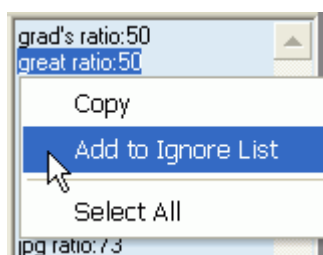
**Delete Permanently During Mail Check** - emails are deleted permanently during the accounts check

## Ignore List

**Ignore List** is a list of words the Bayesian filter must ignore when classifying the messages as spam or good. The Ignore List usually includes most common words that can be found in email messages. You can view the default Ignore List if you click **Ignore List** tab in the **Bayesian Filter Settings**.



You can remove words from the Ignore List, or add other words you see appropriate. To delete a word, use **Delete** button on the keyboard. To add a new word, put the cursor at the place where you want to insert the word and type it. The words must be entered in column one per line. Also, you can add the words to the Ignore List directly from the SpamCombat main screen. Select the word(s) in the **Interesting Words** frame, click the right mouse button and select **Add to Ignore List** option:

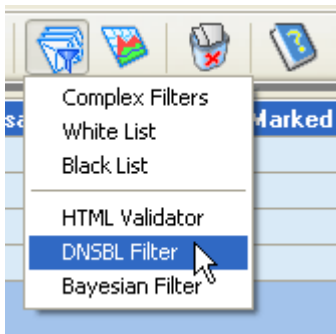


### Working with DNSBL Filter

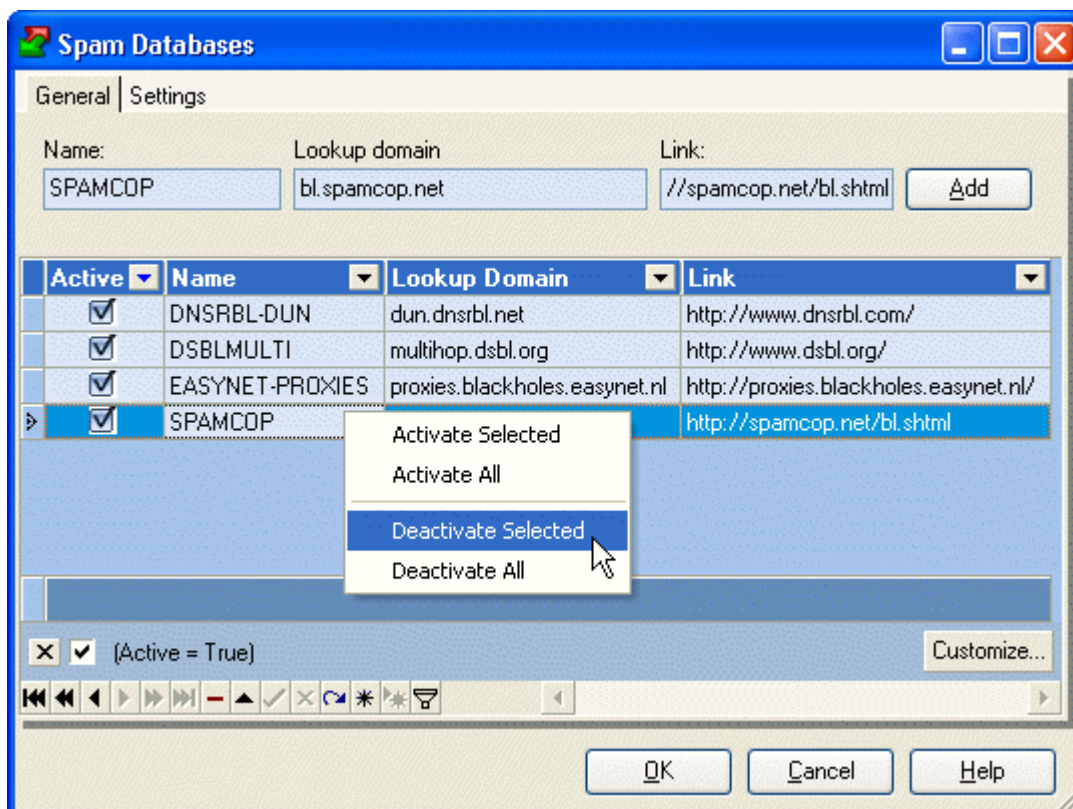
DNSBL Filter checks the sender's IP address against the most known blacklists in DNS-Based spam databases.

To view a list of spam databases provided with SpamCombat, click **Filters** button on the program's Toolbar and select **DNSBL Filter**.

Or, double click the mouse on **DNSBL Filter** at the left pane of the program's main window.



You can see the spam databases, their lookup domains and links within the grid.



To add a spam database, enter its name, lookup domain and URL. Click **Add**.

You can update the SpamCombat DNSBL database by yourself.

Follow this URL <http://www.declude.com/junkmail/support/ip4r.htm> to view the list of active spam databases. Enter the sender's IP address and click **Lookup IP** to get the list of spam databases where this IP is listed. Then return to the previous page, copy the name, lookup domain and the URL of the appropriate blacklists and add them to the SpamCombat DNSBL filter.

Inactive blacklists within the SpamCombat DNSBL filter can be disabled or removed from the database.

Clicking the right mouse button on the selected record within the grid brings the following options:

**Activate Selected** - allows you to activate the selected items

**Activate All** - allows you to activate all the items

**Deactivate Selected** - allows you to deactivate the selected items

**Deactivate All** - allows you to deactivate all the items

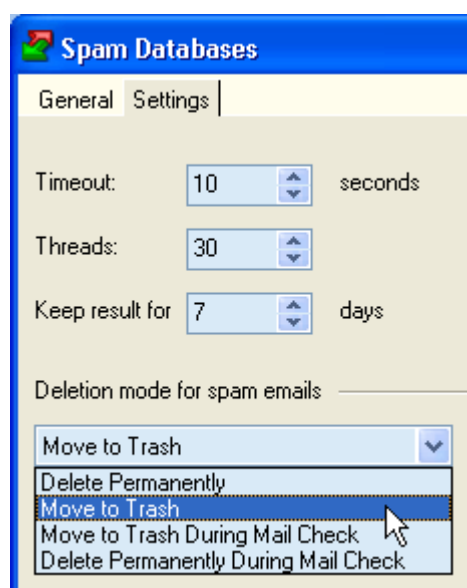
At the bottom of the grid there is also a range of buttons you can use to work with the spam databases. Put the cursor to the button to know its function.

To easily search for a record within the grid, you can use an incremental search. An incremental search allows you to locate a record within the grid by matching the initial characters of a record field.

For your convenience you can sort and filter the records within the grid as you want.

## DNSBL Filter Settings

Click **Settings** tab in Spam Databases screen to specify DNSBL filter settings.



**Timeout xx seconds** - time limit to be used by the program to connect to the spam databases.

**Threads** - maximum number of spam databases the program connects to simultaneously.

**Keep result for xx days** - SpamCombat will keep the information about whether the IP address is listed in spam databases for xx days. This option allows SpamCombat not to overload the DNS server with queries.

Select a deletion mode for spam emails detected by the DNSBL filter:

**Move to Trash** - spam emails detected by the DNSBL filter will be deleted from the mail server and moved to Deleted Items folder (saved to the disk)

**Delete Permanently** - spam emails detected by the DNSBL filter will be

deleted from the mail server without being saved to the disk

**Move to Trash During Mail Check** - emails are moved to Deleted Items folder during the accounts check

**Delete Permanently During Mail Check** - emails are deleted permanently during the accounts check

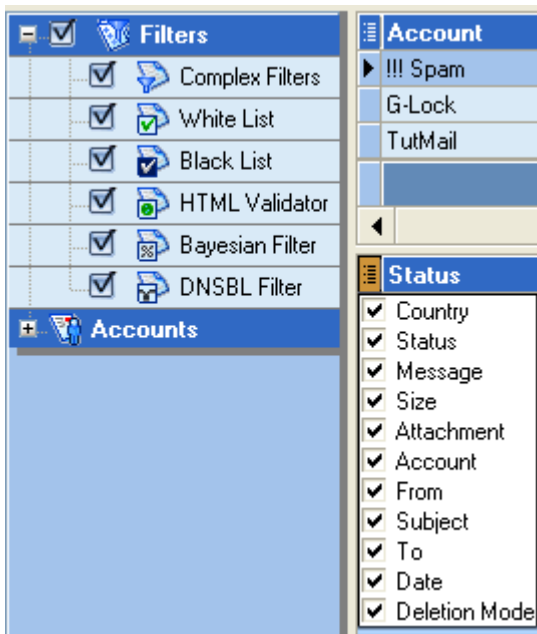
---

## Working with Emails

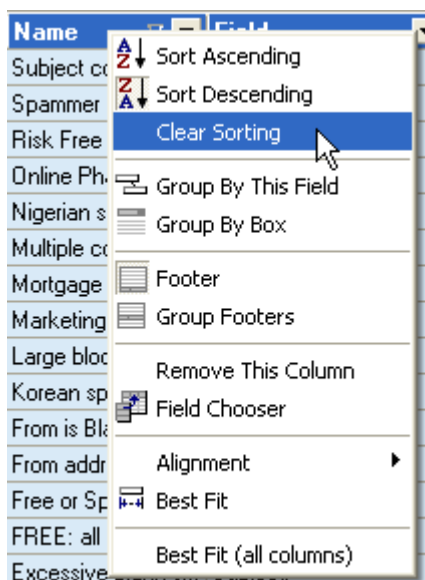
### Sorting and Filtering Emails

Here we'll describe all the features of SpamCombat that can help you arrange the records within the grid in most handy way for you. Using these procedures you can easily manage the emails in the program's main screen, deleted messages, filters in Complex Filters, Whitelist, Blacklist, and DNSBL, and the records in the General Statistics table.

To quickly hide the columns within the grid, click the mouse at the right top corner in the grid and uncheck the columns you want to hide. To show the columns, check the appropriate checkboxes:



If you click the right mouse button on a column name, the following menu pops up:



**Sort Ascending** - sorts the records in ascending order

**Sort Descending** - sorts the records in descending order

**Clear Sorting** - clears sorting for a column

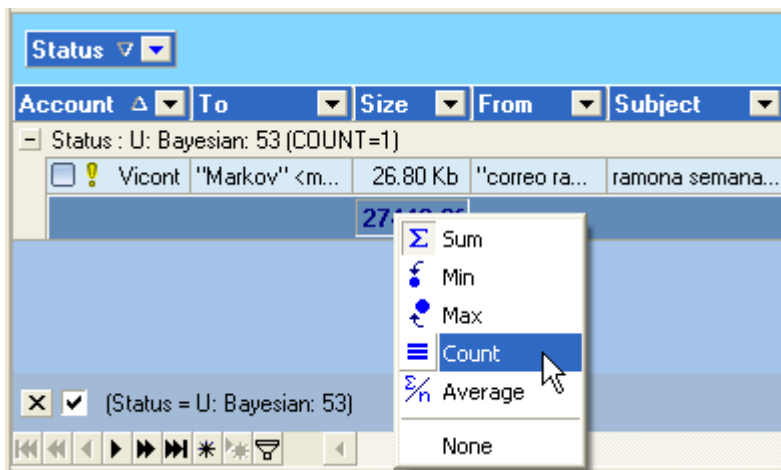
**Group By This Field** - groups the records by the appropriate column. To restore the grid, just drag and drop the column to its place.

Status ▾					
Account ▴ ▾	From ▾	Subject ▾	To ▾	Size ▾	Date ▾
- Status : U: Bayesian: 53 (COUNT=1)					
<input type="checkbox"/> ! Vicont	"correo ra...	ramona semana...	" Vicont" <m...	26.80 Kb	10/7/2003 9:...
+ Status : U: Bayesian: 50 (COUNT=5)					
+ Status : S: Dubious HTML tags: 0:P, /0:P, (COUNT=1)					
+ Status : S: Bayesian: 99 (COUNT=9)					
+ Status : S: Bayesian: 100 (COUNT=18)					
- Status : N: Bayesian: 9 (COUNT=1)					
<input checked="" type="checkbox"/> Vicont	ariels_3141...	g00d dubt c0ns...	" Vicont" <m...	1.60 Kb	10/9/2003 1:...
+ Status : N: Bayesian: 0 (COUNT=1)					

**Group By Box** - enables/disables the grouping panel.

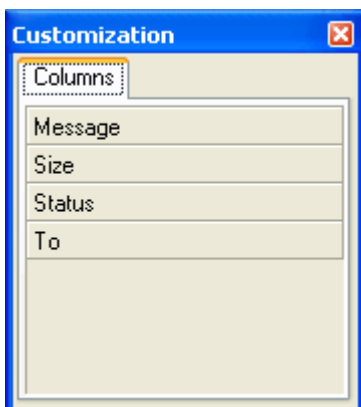
**Footer** - shows/hides the footer. If you click the right mouse button on the footer, you can execute mathematical operations with the numeric columns (Message# and Size): calculate the summary, get the minimum, maximum, and average value.

**Group Footers** - shows/hides group footers.



**Remove This Column** - removes the columns from the grid.

**Field Chooser** – allows restoring the removed columns. To restore the columns, just drag and drop them back to the grid.



**Alignment** - aligns the items left, right or center

**Best Fit** - calculates the width of the appropriate column so that its content is fully displayed within the cell

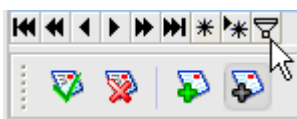
**Best Fit (all columns)** - calculates the width of all the columns so that their contents are fully displayed within grid cells

You can sort the emails in ascending and descending order by clicking the mouse on the column title.

💡 **Tip:** To sort the emails by more than one column at a time, click the column title to sort the items by this column. Now hold down **Shift** on the keyboard and click another column title. You'll get the items sorted by these two columns.

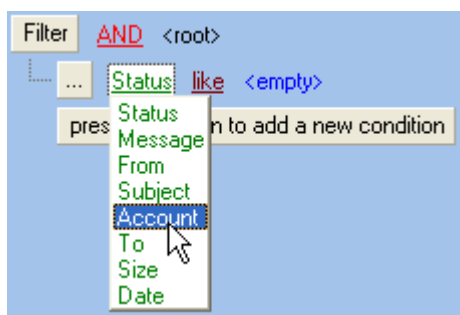
To change the order of the columns, drag and drop a column at the place where you want it to be.

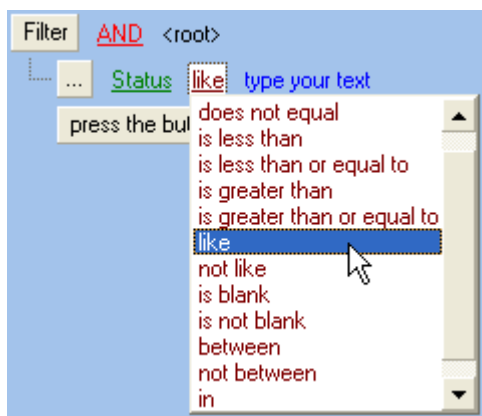
To filter the emails, click **Filter** button at the bottom of the grid and build your filter:



Select the principle the filter will work on: **AND**, **OR**, **NOT AND**, **NOT OR**.

Set the filter conditions by choosing them from the drop down menus as shown below:

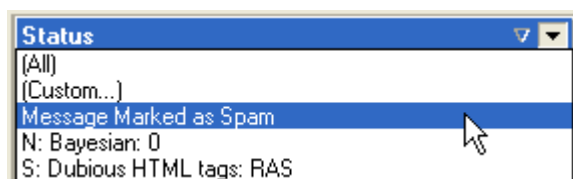




When done, click OK.

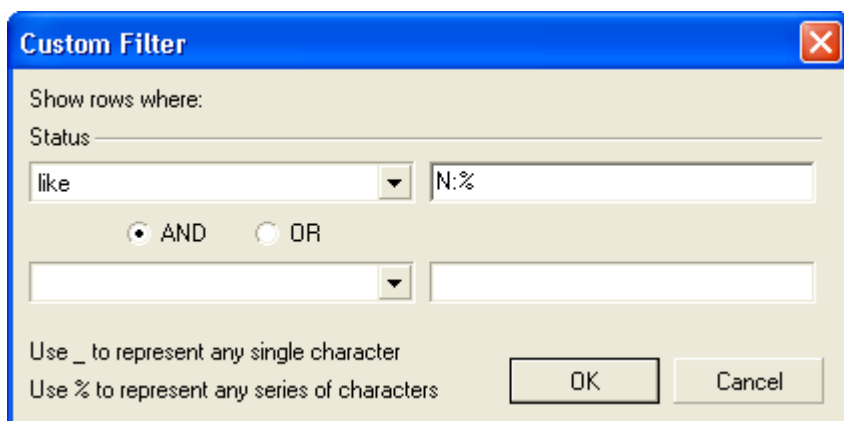
For your convenience you can save the filter to a file by clicking **Save As** button and load it when needed by clicking **Open**.

To filter the emails by the appropriate column within the grid, click a black down arrow and select a filter condition:



Select **All** to show all the emails.

Select **Custom...** to set up your own filter:



Here are several examples of filters you can use:

**Status like N:%** - shows only good emails

**Status like S:%** - shows only spam emails

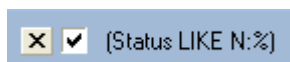
**Status like U:%** - shows unresolved emails

**Status like N: BlackList:%** - shows the emails that came under the blacklist


**Status like N: WhiteList:%** - shows the emails that came under the whitelist

**Status NOT LIKE %(Cached)** - shows only new emails. Cached messages are hidden.

When finished, click OK to apply the filter. The filter conditions will appear under the grid:

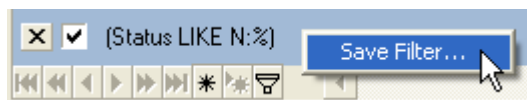


To deactivate the filter, just uncheck this checkbox.

To remove the filter, click  **Delete** button.

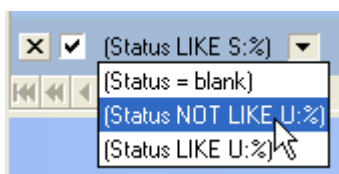
To edit the filter, click **Customize** button.

To save this filter, click the right mouse button and select **Save Filter...**

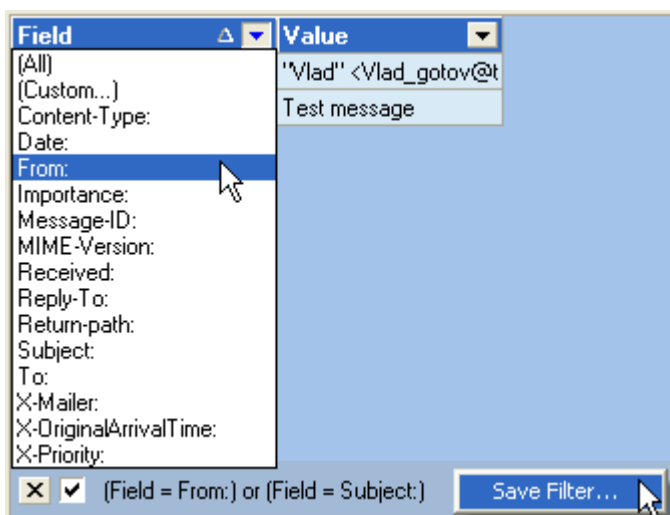


Type a file name to save your filter and click **Save**. As soon as the filter is saved, it becomes available from the filter drop down menu in the **Status** column.

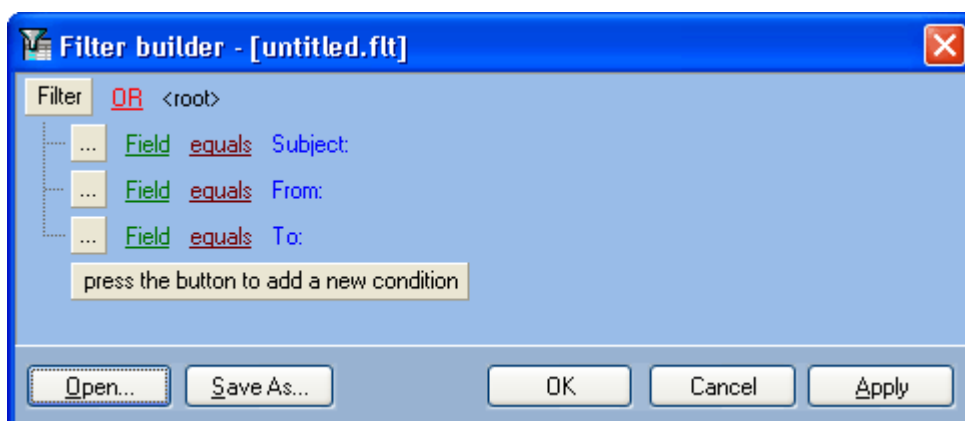
If you setup more than one custom filter, you can easily switch between them by clicking a black down arrow:



You can also filter the fields in the message header. The procedures are quite the same. Just click the black down arrow in the **Field** or **Value** column and select the header field or field value to show. All other fields will be hidden.



Select **Custom...** to build your own filter. You can then save the filter if you click **Save As...** button. When the filter is saved, you can apply it by selecting from the filter drop down menu in the **Field** column.



## Managing Deleted Emails

**Attention!** The messages you delete from the server are moved to **Deleted Items** folder only if they have the deletion mode **Move to Trash** in the SpamCombat main screen.

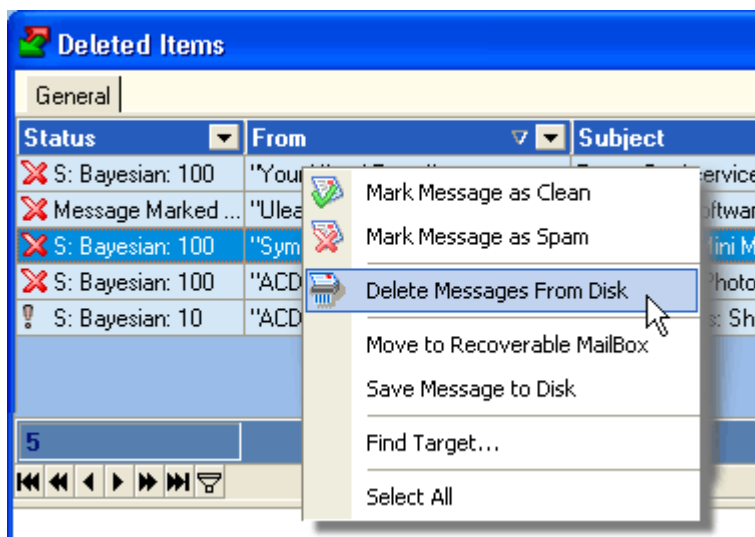
The **Deleted Items** folder is stored in the SpamCombat directory:  
...\G-Lock SpamCombat\Profiles\Default\Deleted\

For your convenience you can choose a different location to store deleted messages. See **Automation Settings**.

To view the deleted messages, click  **Deleted Items** button on the program's Toolbar.

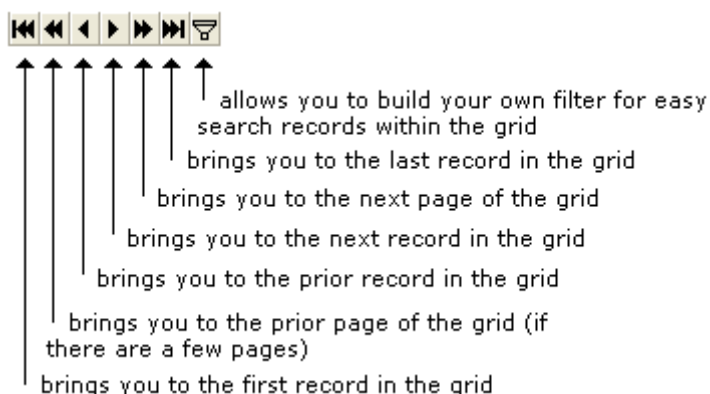
The grid shows the details of the deleted messages: Status, Account, From, Subject, To, Date. If you select an email within the grid and click the right mouse button on it, you can:

- mark the selected message as clean
- mark the selected message as spam
- delete the selected message from the disk
- move the selected message to the Recoverable mailbox for further receiving with an email client.
- save the selected email to the disk
- locate the selected email on the disk (Find Target...).









The Bayesian filter learns from the deleted emails as well. If you notice a good message that was classified as spam and deleted, you can re-categorize this email to good.


At the bottom of the grid there is a range of useful buttons:



You can also use the buttons on the toolbar to work with deleted emails:

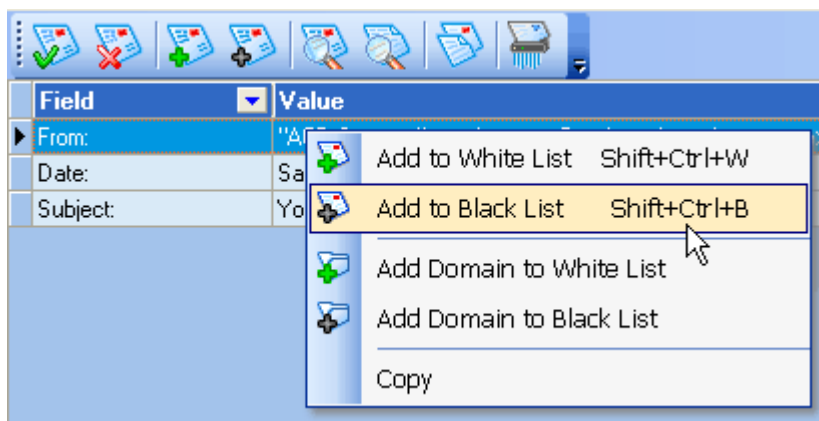
-  Mark Message as Clean
-  Mark Message as SPAM
-  Add to White List
-  Add to Black List
-  View/Hide Message Header
-  View/Hide Interesting Words (used by the Bayesian filter)

-  View HTML/Message Source/Decoded Message
-  Delete From Disk

At the bottom screen you can view deleted emails in either of these formats: HTML, message source (RAW message code), or decoded message (message body). To switch between the formats, click  **View HTML/Message Source/Decoded Message** button.

Viewing emails in the HTML format is absolutely safe. No pictures are actually downloaded; no hidden scripts or codes are executed. You can see only a picture frames in the preview screen. If you put the cursor to the picture frame, at the bottom of the SpamCombat main screen you will see the URL of this picture and the URL the picture includes (if there is any URL). If you click the right mouse button on the picture frame, you can either open the picture with your browser, or copy the URL the picture includes to the clipboard, or open this URL with your Internet browser.

You can also whitelist or blacklist emails from the preview screen. To do this, select a field from the message header, click the right mouse button, and then select the appropriate menu:



#### **Notes:**

Deleted emails are stored on the disk for as many days as you specified in the **Automation Settings**. After that the program deletes them from the disk.

If an email has the size more than 5Kb, only the defined number of lines from the message body is saved. See **General Settings**. If the message size is less than 5Kb, the entire message body is saved to the disk.

If you save a message to a file with .eml extension, you can then open it in your email client with a double mouse click.

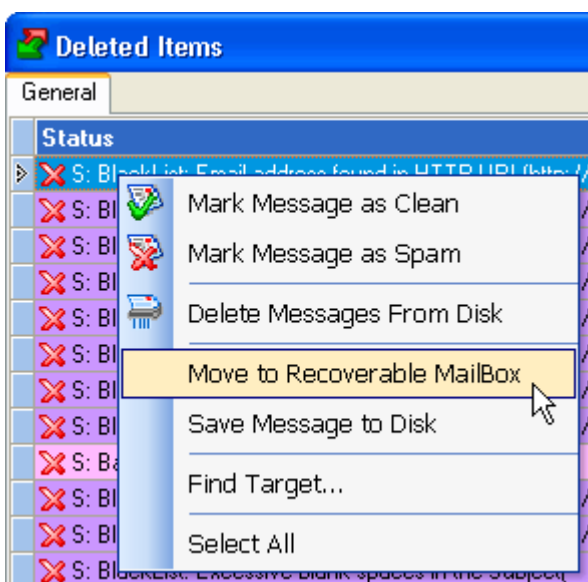
## Recovering Deleted Emails

If a good email was accidentally marked as spam and moved to Deleted Items folder, SpamCombat lets you restore this email from the trash for further receiving with your email client.

### To recover an email:

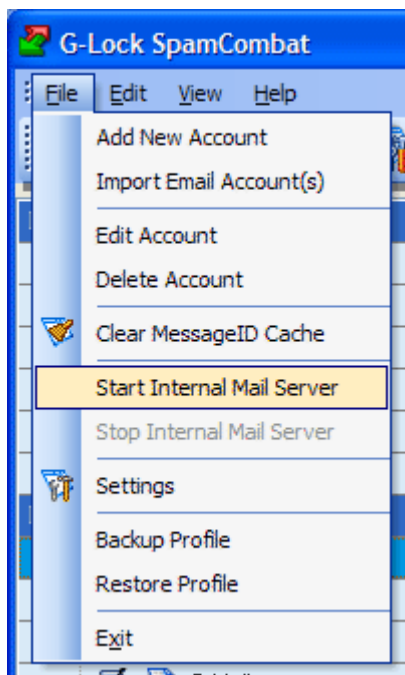
1) create in your email client a POP3 account with the same parameters (account name and password) as in the Internal Mail Server settings in SpamCombat. SpamCombat has the Internal Mail Server settings pre-setup: Account Name - SpamCombat, password - SpamCombat, and port - 110. You can either use these default parameters to create an account in your email client, or you can change the default account name and password to your own.


2) move an email (emails) you want to restore to the Recoverable mailbox in SpamCombat. To do this, open Deleted Items folder, select an email (emails), click the right mouse button and select Move to Recoverable Mailbox menu.



3) start the Internal Mail Server in SpamCombat. To do this, click **File** and

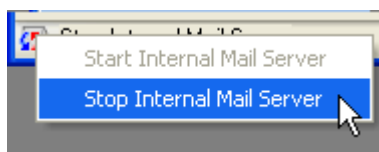
select **Start Internal Mail Server**.




When the Internal Mail Server is started, you can see the  icon at the left bottom corner of the SpamCombat screen.

4) select the account in your email client you've just setup to receive emails from the Recoverable mailbox in SpamCombat.

To stop the Internal Mail Server after you recovered the emails, click on the icon and select the appropriate menu.

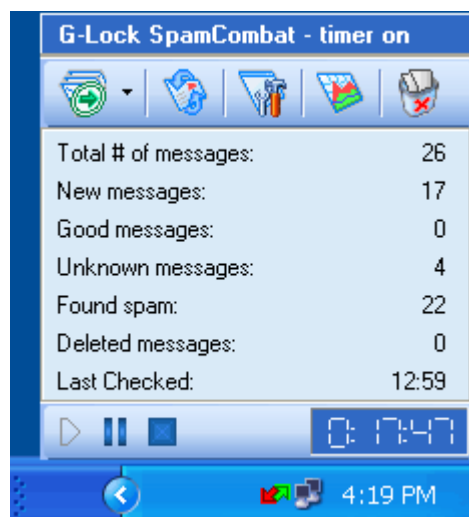


 **Note:** If you recover a deleted email, only the defined number of lines from the message body will be recovered if an email has the size more than 5Kb. See **General Settings**. If the message size is less than 5Kb, the entire message body will be recovered.

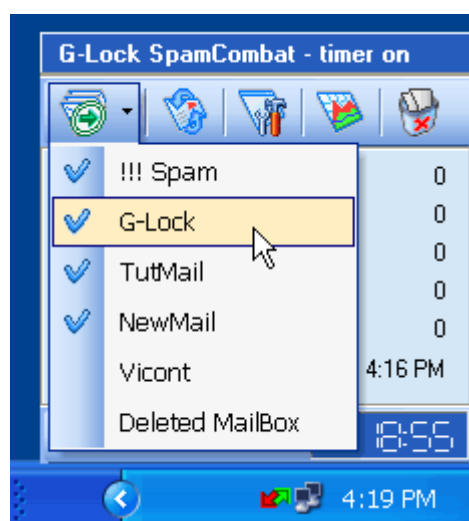
## Working with SpamCombat in System Tray


To minimize SpamCombat to the system tray after it is closed, check **Minimize to system tray** option in the program's General Settings.

If you put the mouse on the SpamCombat icon in the system tray, the program's lite screen is displayed.

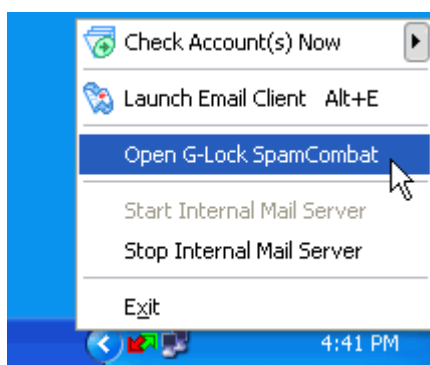


Here you can see the statistics on your incoming emails: total of messages, quantity of new, good, unknown (not resolved) and spam emails found by the program. You can also select the account to check for incoming emails and click **Start**, launch your default email client when spam emails are deleted, adjust the program's settings, and view deleted messages. There are also **Start Timer**, **Pause Timer**, and **Disable Timer** buttons you can use to control the accounts auto-check mode.



The time SpamCombat is retrieving emails being minimized to the system tray, its icon is blinking. If new emails arrived, the usual icon changes to  in the system tray. If the timer is on, the SpamCombat icon notifying you about new emails does not change to its normal state between the sessions regardless of whether new emails were retrieved during the last auto-check or earlier.

To open the SpamCombat main window, double click the mouse on the title bar on the lite screen. Or, click the right mouse button on the program's icon and select **Open G-Lock SpamCombat**.



To start SpamCombat, click **Check Account(s) Now** and select the account(s).

To open your email client, click **Launch Email Client**.

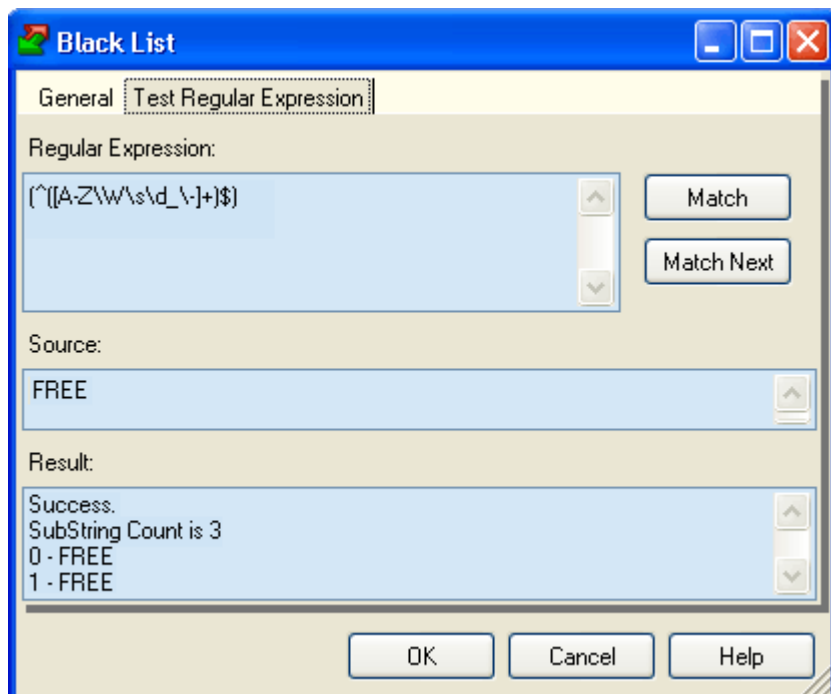
To start the Internal Mail Server, click **Start Mail Server**.

To stop the Internal Mail Server, click **Stop Mail Server**.

To exit SpamCombat, click **Exit**.

## Test Regular Expressions

If you use regular expressions in the SpamCombat filters, it is rather prudent to check whether the regular expression works properly. To do this, click **Test Regular Expression** tab.



Type a regular expression in the appropriate window. Enter the text that this regular expression must match in the **Source** window and click **Match**. To find the next regular expression that matches the same mask, click **Match Next**. The **Result** window will show you the searching results.

## About Regular Expressions

This topic describes in general terms the syntax and semantics of the regular expressions supported by G-Lock SpamCombat. If want to learn more about regular expressions, here are a few good sources to refer:

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/js56jsgrpRegExpSyntax.asp>

<http://www.regular-expressions.info/>

A regular expression is a pattern that is matched against a subject string from left to right. Most characters stand for themselves in a pattern, and match the corresponding characters in the subject. As a trivial example, the pattern

The quick brown fox

matches a portion of a subject string that is identical to itself. The power of regular expressions comes from the ability to include alternatives and repetitions in the pattern. These are encoded in the pattern by the use of meta-characters, which do not stand for themselves but instead are interpreted in some special way.

There are two different sets of meta-characters: those that are recognized anywhere in the pattern except within square brackets, and those that are recognized in square brackets.

Outside square brackets, the meta-characters are as follows:

- \ (backslash) - general escape character with several uses
- ^ (circumflex) - asserts start of string (or line, in multiline mode)
- \$ (dollar) - asserts end of string (or line, in multiline mode)
- . (full stop (period, dot)) - matches any character except newline (by default)

[ ] (square brackets) - start and end character class definition  
| (vertical bar) - starts of alternative branch  
( ) (round brackets) - start and end subpattern  
? extends the meaning of (also 0 or 1 quantifier, also quantifier minimizer

- \* 0 or more quantifier
- + 1 or more quantifier  
also "possessive quantifier"
- { start min/max quantifier

Part of a pattern that is in square brackets is called a "character class". In a character class the only meta-characters are:

- \ general escape character
- ^ negates the class, but only if the first character
- indicates character range
- [ opens a character class
- ] terminates the character class

Let's describe each of these meta-characters in details.

## Backslash (\)

The backslash character has several uses:

1) if it is followed by a non-alphameric character, it takes away any special meaning that character may have. This use of backslash as an escape character applies both inside and outside character classes.

For example, if you want to match a \* character, you write \\* in the pattern. This escaping action applies whether or not the following character would otherwise be interpreted as a meta-character, so it is always safe to precede a non-alphameric with backslash to specify that it stands for itself. In particular, if you want to match a backslash, you write \\.

2) the second use of backslash provides a way of encoding non-printing characters in patterns in a visible manner. There is no restriction on the appearance of non-printing characters, apart from the binary zero that terminates a pattern, but when a pattern is being prepared by text editing, it is usually easier to use one of the following escape sequences than the binary character it represents:

- `\a` alarm, that is, the BEL character (hex 07)
- `\cx` "control-x", where x is any character
- `\e` escape (hex 1B)
- `\f` formfeed (hex 0C)
- `\n` newline (hex 0A)
- `\r` carriage return (hex 0D)
- `\t` tab (hex 09)
- `\ddd` character with octal code ddd, or backreference
- `\xhh` character with hex code hh
- `\x{hhh..}` character with hex code hhh... (UTF-8 mode only)

3) the third use of backslash is for specifying generic character types:

- `\d` any decimal digit
- `\D` any character that is not a decimal digit
- `\s` any whitespace character
- `\S` any character that is not a whitespace character
- `\w` any "word" character
- `\W` any "non-word" character

Each pair of escape sequences partitions is the complete set of characters into two disjoint sets. Any given character matches one, and only one, of each pair.

4) the fourth use of backslash is for certain simple assertions. An assertion specifies a condition that has to be met at a particular point in a match, without consuming any characters from the subject string. The backslashed assertions are:

- `\b` matches at a word boundary
- `\B` matches when not at a word boundary
- `\A` matches at start of subject
- `\Z` matches at end of subject or before newline at end
- `\z` matches at end of subject
- `\G` matches at first matching position in subject

These assertions may not appear in character classes (but note that `\b` has a different meaning, namely the backspace character, inside a character class).

## Circumflex (^)

Outside a character class, in the default matching mode, the circumflex character is an assertion which is true only if the current matching point is at the start of the subject string.

Inside a character class, circumflex has an entirely different meaning. Circumflex need not be the first character of the pattern if a number of alternatives are involved, but it should be the first thing in each alternative in which it appears if the pattern is ever to match that branch. If all possible alternatives start with a circumflex, that is, if the pattern is constrained to match only at the start of the subject, it is said to be an "anchored" pattern.

## Dollar (\$)

A dollar character is an assertion which is true only if the current matching point is at the end of the subject string, or immediately before a newline character that is the last character in the string (by default). Dollar need not be the last character of the pattern if a number of alternatives are involved, but it should be the last item in any branch in which it appears. Dollar has no special meaning in a character class.

## Full stop (period, dot) (.)

Outside a character class, a dot in the pattern matches any one character in the subject, including a non-printing character, but not (by default) newline. The handling of dot is entirely independent of the handling of circumflex and dollar, the only relationship being that they both involve newline characters. Dot has no special meaning in a character class.

## Square brackets []

An opening square bracket introduces a character class, terminated by a closing square bracket. A closing square bracket on its own is not special. If a closing square bracket is required as a member of the class, it should be the first data character in the class (after an initial circumflex, if present) or escaped with a backslash.

A matched character must be in the set of characters defined by the class, unless the first character in the class definition is a circumflex, in which case the subject character must not be in the set defined by the class. If a circumflex is actually required as a member of the class, ensure it is not the first character, or escape it with a backslash.

For example, the character class [aeiou] matches any lower case vowel, while [^aeiou] matches any character that is not a lower case vowel. Note that a circumflex is just a convenient notation for specifying the characters that are in the class by enumerating those that are not. It is not an assertion: it still consumes a character from the subject string, and fails if the current pointer is at the end of the string.

When caseless matching is set ((?i) characters are used to set a case insensitivity in the regular expression, for example, [(?i)aeiou]), any letters in a class represent both their upper case and lower case versions, so for example, a caseless [aeiou] matches "A" as well as "a", and a caseless

[^aeiou] does not match "A", whereas a careful version would.

## Minus (-)

The minus (hyphen) character can be used to specify a range of characters in a character class. For example, [d-m] matches any letter between d and m, inclusive. If a minus character is required in a class, it must be escaped with a backslash or appear in a position where it cannot be interpreted as indicating a range, typically as the first or last character in the class.

All non-alphanumeric characters other than \, -, ^ (at the start) and the terminating ] are non-special in character classes, but it does no harm if they are escaped.

## Vertical bar (|)

Vertical bar characters are used to separate alternative patterns. For example, the pattern

gilbert|Sullivan

matches either "gilbert" or "sullivan". Any number of alternatives may appear, and an empty alternative is permitted (matching the empty string). The matching process tries each alternative in turn, from left to right, and the first one that succeeds is used. If the alternatives are within a subpattern (defined below), "succeeds" means matching the rest of the main pattern as well as the alternative in the subpattern.

## Round brackets ()

Round brackets are used as subpattern delimiters. Marking part of a pattern as a subpattern does two things:

1. It localizes a set of alternatives. For example, the pattern

```
cat(aract|erpillar|)
```

matches one of the words "cat", "cataract", or "caterpillar". Without the parentheses, it would match "cataract", "erpillar" or the empty string.

2. It sets up the subpattern as a capturing subpattern (as defined above). Opening parentheses are counted from left to right (starting from 1) to obtain the numbers of the capturing subpatterns.

For example, if the string "the red king" is matched against the pattern  
the ((red|white) (king|queen))

the captured substrings are "red king", "red", and "king", and are numbered 1, 2, and 3, respectively.

The fact that plain parentheses fulfil two functions is not always helpful. There are often times when a grouping subpattern is required without a capturing requirement. If an opening parenthesis is followed by a question mark and a colon, the subpattern does not do any capturing, and is not counted when computing the number of any subsequent capturing subpatterns. For example, if the string "the white queen" is matched against the pattern

```
the ((?:red|white) (king|queen))
```

the captured substrings are "white queen" and "queen", and are numbered 1 and 2. The maximum number of capturing subpatterns is 65535, and the maximum depth of nesting of all subpatterns, both capturing and non-capturing, is 200.

## Quantifiers

The quantifiers can follow any of the following items:

- a literal data character
- the . metacharacter
- the \C escape sequence
- escapes such as \d that match single characters
- a character class
- a back reference (see next section)
- a parenthesized subpattern (unless it is an assertion)

The general repetition quantifier specifies a minimum and maximum number of permitted matches, by giving the two numbers in curly brackets (braces), separated by a comma. The numbers must be less than 65536, and the first must be less than or equal to the second. For example:

`z{2,4}`

matches "zz", "zzz", or "zzzz". A closing brace on its own is not a special character. If the second number is omitted, but the comma is present, there is no upper limit; if both the second number and the comma are omitted, the quantifier specifies an exact number of required matches. Thus

`[aeiou]{3,}`

matches at least 3 successive vowels, but may match many more, while

`\d{8}`

matches exactly 8 digits. An opening curly bracket that appears in a position where a quantifier is not allowed, or one that does not match the syntax of a quantifier, is taken as a literal character. For example, `{,6}` is

not a quantifier, but a literal string of four characters.

The quantifier {0} is permitted, causing the expression to behave as if the previous item and the quantifier were not present.

For convenience the three most common quantifiers have single-character abbreviations:

- \* is equivalent to {0,}
- + is equivalent to {1,}
- ? is equivalent to {0,1}

By default, the quantifiers are "greedy", that is, they match as much as possible (up to the maximum number of permitted times), without causing the rest of the pattern to fail. The classic example of where this gives problems is in trying to match comments in C programs. These appear between the sequences /\* and \*/ and within the sequence, individual \* and / characters may appear. An attempt to match C comments by applying the pattern

```
\/\.*\*/
```

to the string

```
/* first command */ not comment /* second comment */
```

fails, because it matches the entire string owing to the greediness of the .\* item.

However, if a quantifier is followed by a question mark, it ceases to be greedy, and instead matches the minimum number of times possible, so the pattern

`^.*?\*/`

does the right thing with the C comments. The meaning of the various quantifiers is not otherwise changed, just the preferred number of matches. Do not confuse this use of question mark with its use as a quantifier in its own right. Because it has two uses, it can sometimes appear doubled, as in

`\d??\d`


which matches one digit by preference, but can match two if that is the only way the rest of the pattern matches.

## SpamCombat Command-Line Switches

There is the only G-Lock SpamCombat command-line switch: **Auto**. If you start the program with the `spamcombat.exe Auto`, the program will check your accounts, delete spam emails and automatically exit.

---

## Viewing SpamCombat Statistics

To view the SpamCombat statistics, click  **Statistics** button on the program's Toolbar.

### General Table

Here you can view general SpamCombat statistics on processed messages since the first installation of the program. The data is assembled in a table with numerous columns:

**Account** - your POP3/IMAP accounts

**Date** - date the statistics is gathered on

**Processed** - total of emails processed on the appropriate date

**Deleted** - total of emails deleted on the appropriate date

**Whitelist** - total of whitelisted emails received on the appropriate date

**Blacklist** - total of blacklisted emails received on the appropriate date

**HTML Filter** - total of spam emails detected by HTML Validator

**DNSBL** - total of spam emails detected by DNSBL filter

**Bayesian Good** - total of good emails resolved by the Bayesian Filter

**Bayesian Spam** - total of spam emails resolved by the Bayesian Filter

**Bayesian Unknown** - total of emails not resolved by the Bayesian Filter

**Reclassified to Good** - total of emails reclassified to good by a user

**Reclassified to Spam** - total of emails reclassified to spam by a user

**Unknown** - total of emails which were not caught by any of the filters

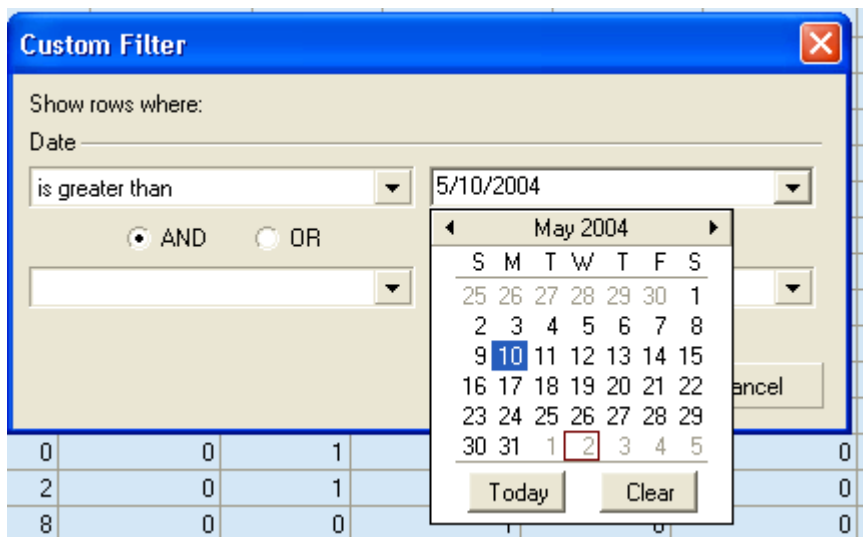
Date ▼	Ac... ▲ ▼	Processed ▼	Deleted ▼	B. Spam ▼	Black List ▼	Html Filter ▼	DNSBL ▼
6/14/2004	G-Lock	5	2	3	1	1	0
6/11/2004	G-Lock	1	0	0	0	1	0
6/9/2004	G-Lock	1	0	0	0	0	0
6/7/2004	G-Lock	4	4	0	2	0	1
6/2/2004	G-Lock	1	1	1	0	0	0
6/1/2004	G-Lock	1	1	1	0	0	0
5/31/2004	G-Lock	2	2	0	2	0	0
5/27/2004	G-Lock	1	1	1	0	0	0
5/26/2004	G-Lock	1	1	1	0	0	0
5/24/2004	G-Lock	2	2	0	0	0	2
5/21/2004	G-Lock	2	1	1	1	0	0
5/20/2004	G-Lock	1	1	1	0	0	0
5/19/2004	G-Lock	2	2	0	0	0	2
5/18/2004	G-Lock	2	1	0	0	0	0
5/17/2004	G-Lock	10	9	2	1	0	4
5/14/2004	G-Lock	2	2	0	0	0	2
		<b>769</b>	<b>468</b>	<b>241</b>	<b>211</b>	<b>3</b>	<b>40</b>

☒ (Date > 5/1/2004) Customize...

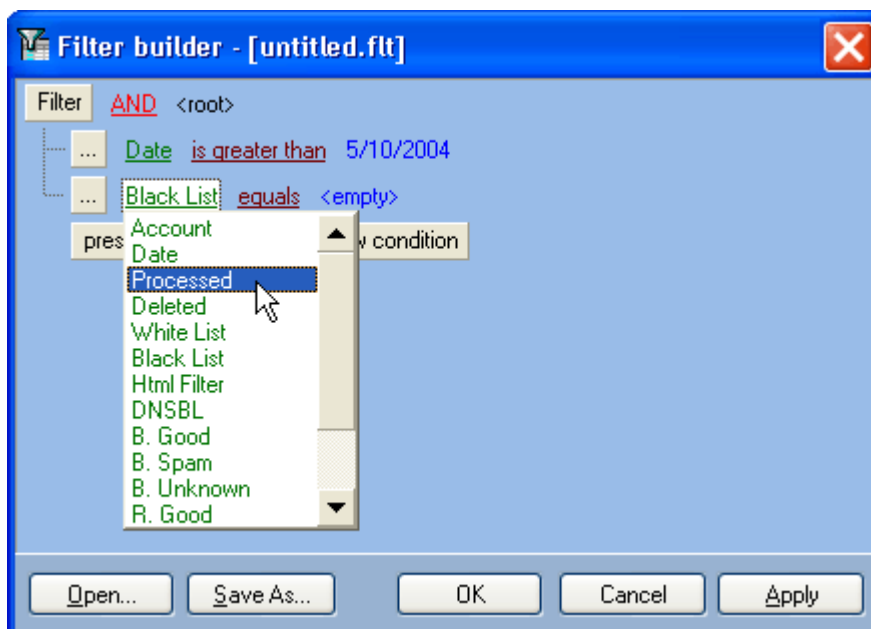
## Sorting and Filtering Statistics

At the bottom of the table there is a range of useful buttons that help you work with the data. Put the cursor to the button to know its function. You can sort and filter the data within the grid as you like. For example, to view the statistics for a specific account only, click a black down arrow in the Account column and select the account name.

To view the statistics only on a specific date, click a black down arrow in the Date column and select the desired date. If you select Custom..., you can build the filter to show the statistics for a period of time:

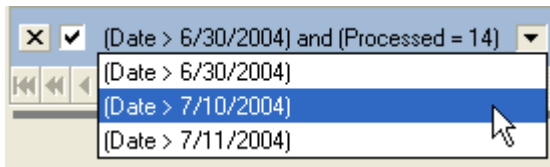


If you click **Customize...** button, the Filter Builder will open where you can add more conditions to refine your filter.



Using the procedure above, you can filter the statistics by all the columns within the grid.

If you setup more than one custom filter, you can easily switch between them by clicking a black down arrow:



If you have the statistics within the General table filtered, this filter is also applied to other diagrams: Assembled Diagram, Filters Rating, Bayesian Efficiency, and SpamCombat Efficiency.

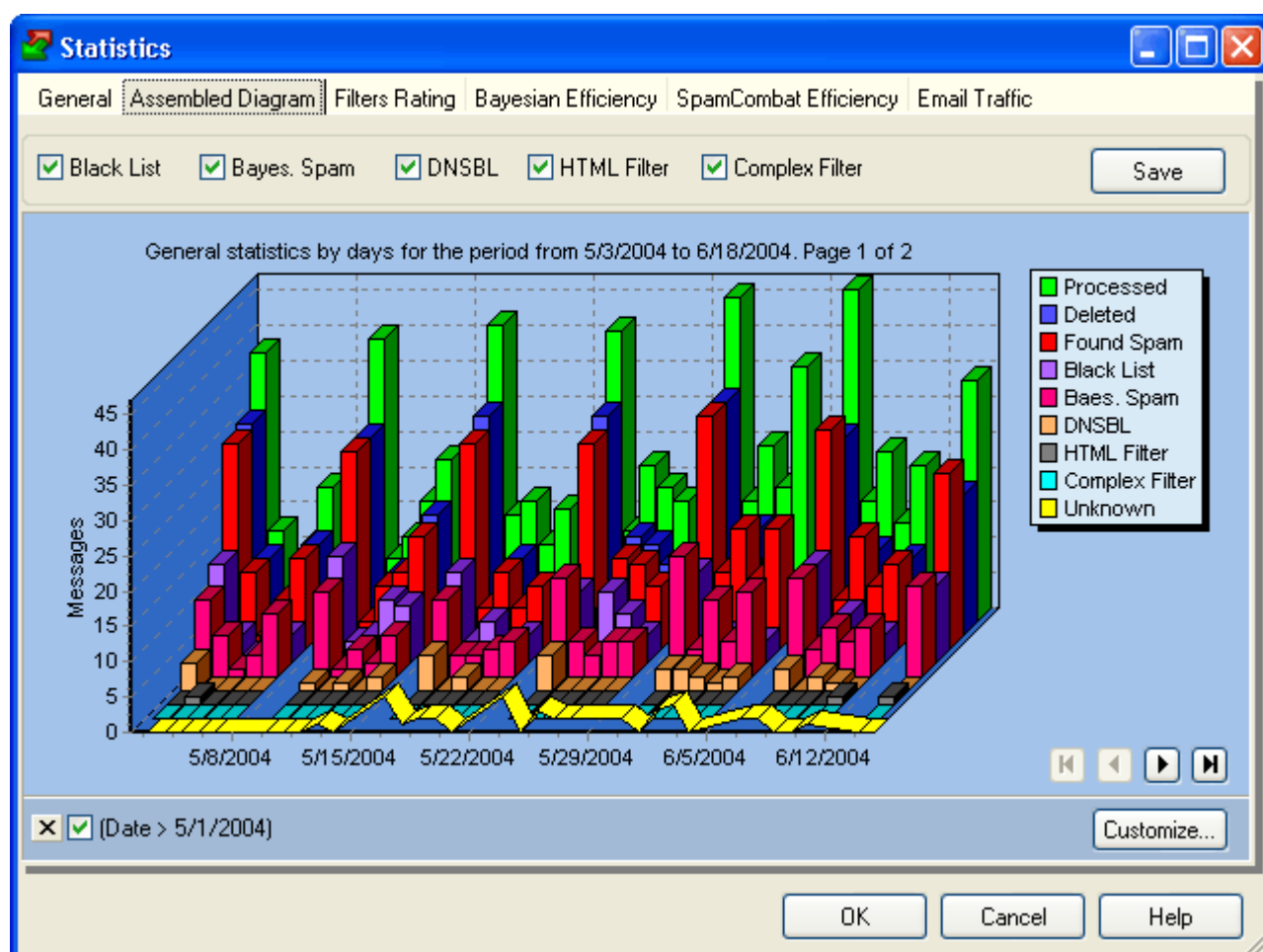
### Deleting Statistics

To delete the records from the General Statistics table, select the string(s) you want to delete and press Del on the keyboard, or click "-" button at the bottom of the table. Click OK to save the changes, or Cancel to cancel them. The changes you make in the General Statistics table are also applied to all others diagrams.

 **Note:** if you are editing the statistics when SpamCombat is active, the changes may not be saved.

## Assembled Diagram

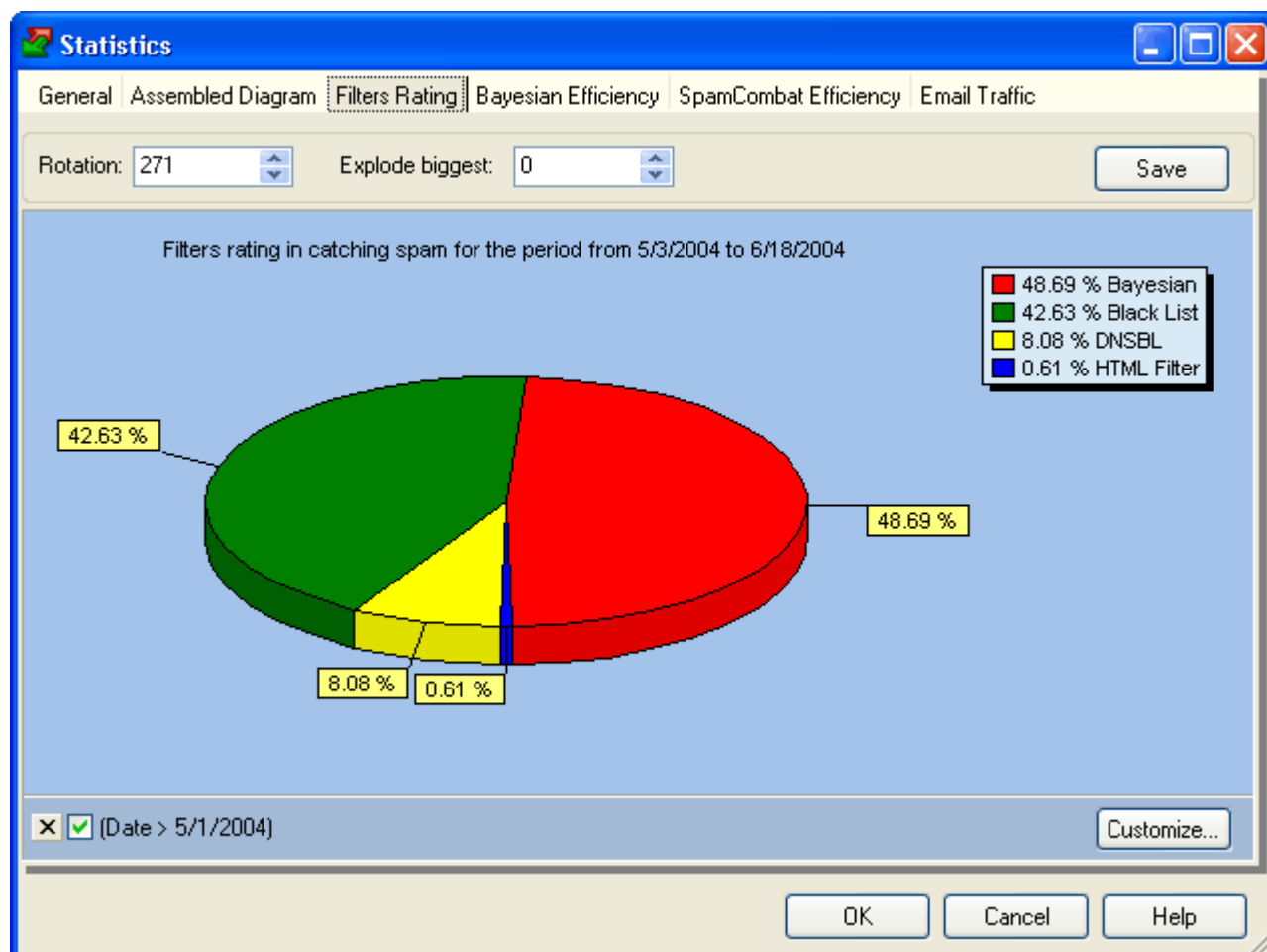
If you click **Assembled Diagram** tab, you can see the statistics as a diagram. There are 5 checkboxes at the top of the screen: **Black List**, **Bayesian Spam**, **DNSBL**, **HTML Filter**, and **Complex Filter**. Check (uncheck) a checkbox to show (hide) the statistics on spam emails caught by the appropriate filter.



To save the diagram to a file of the .bmp format, click **Save** button.

## Filters Rating

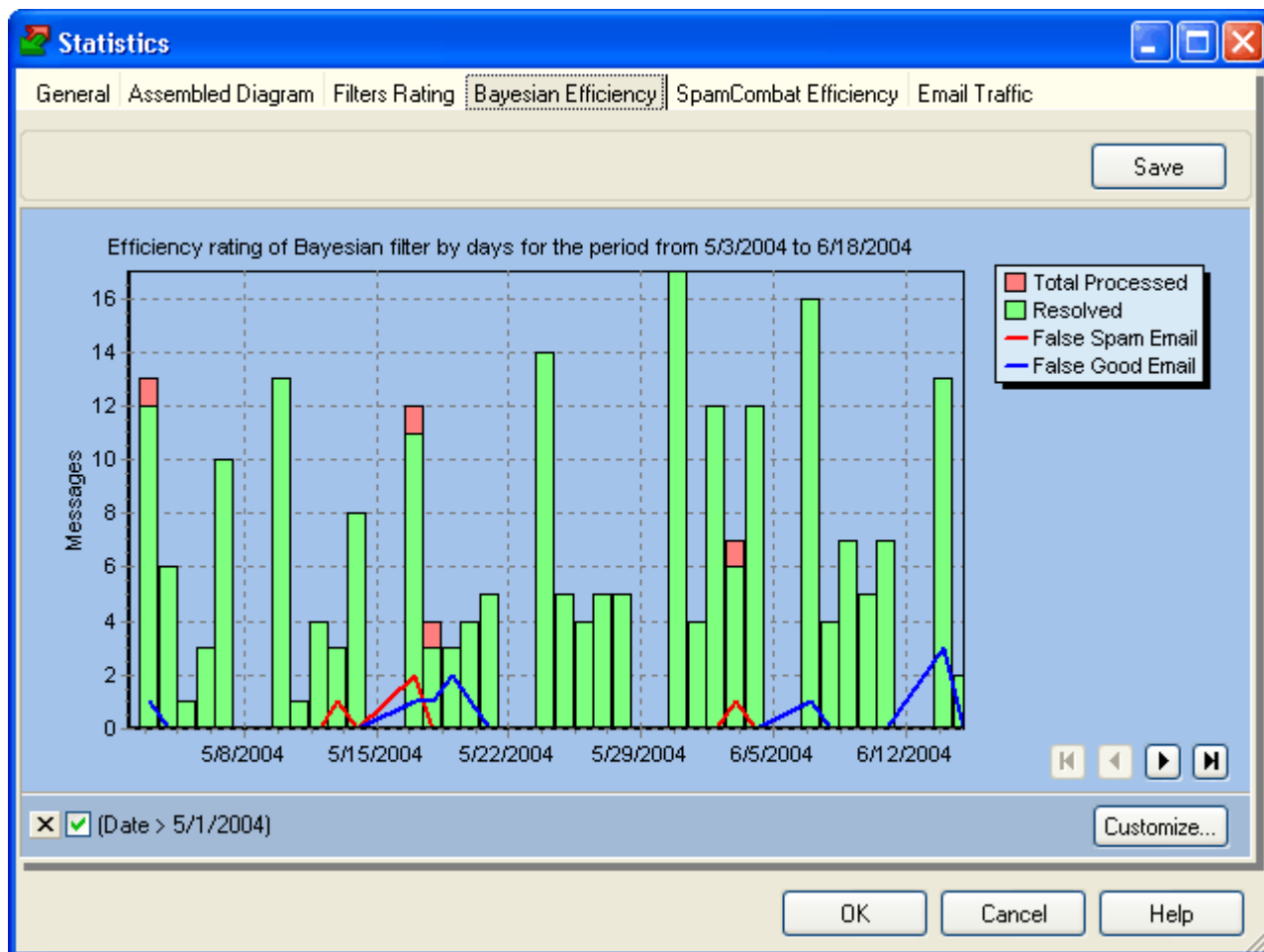
**Filters Rating** shows the percentage of spam emails detected by the SpamCombat filters: Black List, Bayesian, HTML Validator, and DNSBL filter. To adjust the diagram for best viewing, use **Rotation** and **Explode biggest** boxes.



To save the diagram to a file of the .bmp format, click **Save** button.

## Bayesian Efficiency

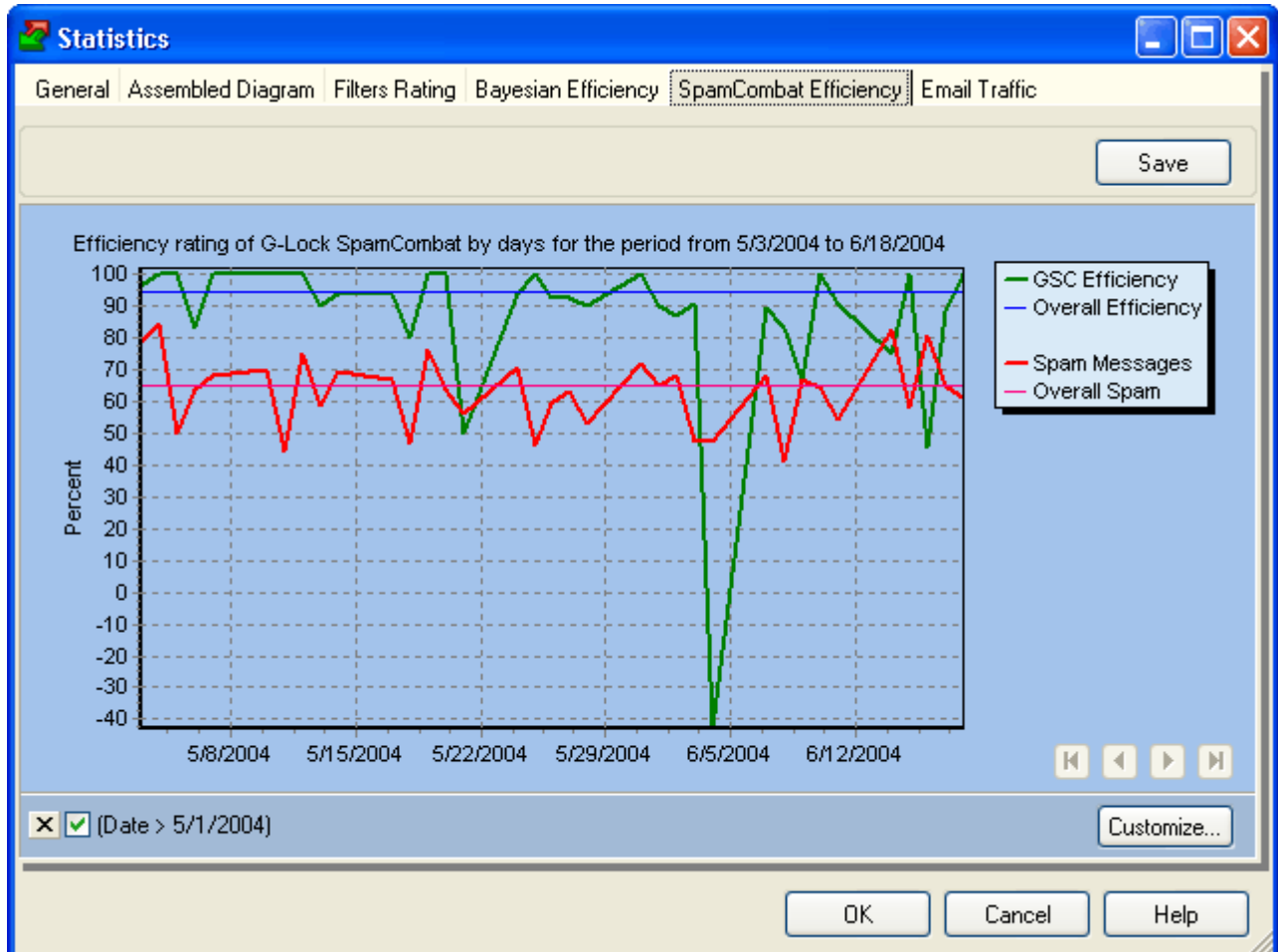
Bayesian Efficiency diagram shows the total of messages processed by the Bayesian filter and the percentage of emails resolved properly as good/spam. Here you can also see how many emails were falsely classified as good and spam.



To save the diagram to a file of the .bmp format, click **Save** button.

## SpamCombat Efficiency

SpamCombat Efficiency diagram shows the total of spam emails you received for a period of time and how many of them were detected by the SpamCombat.



To save the diagram to a file of the .bmp format, click **Save** button.

## Email Traffic

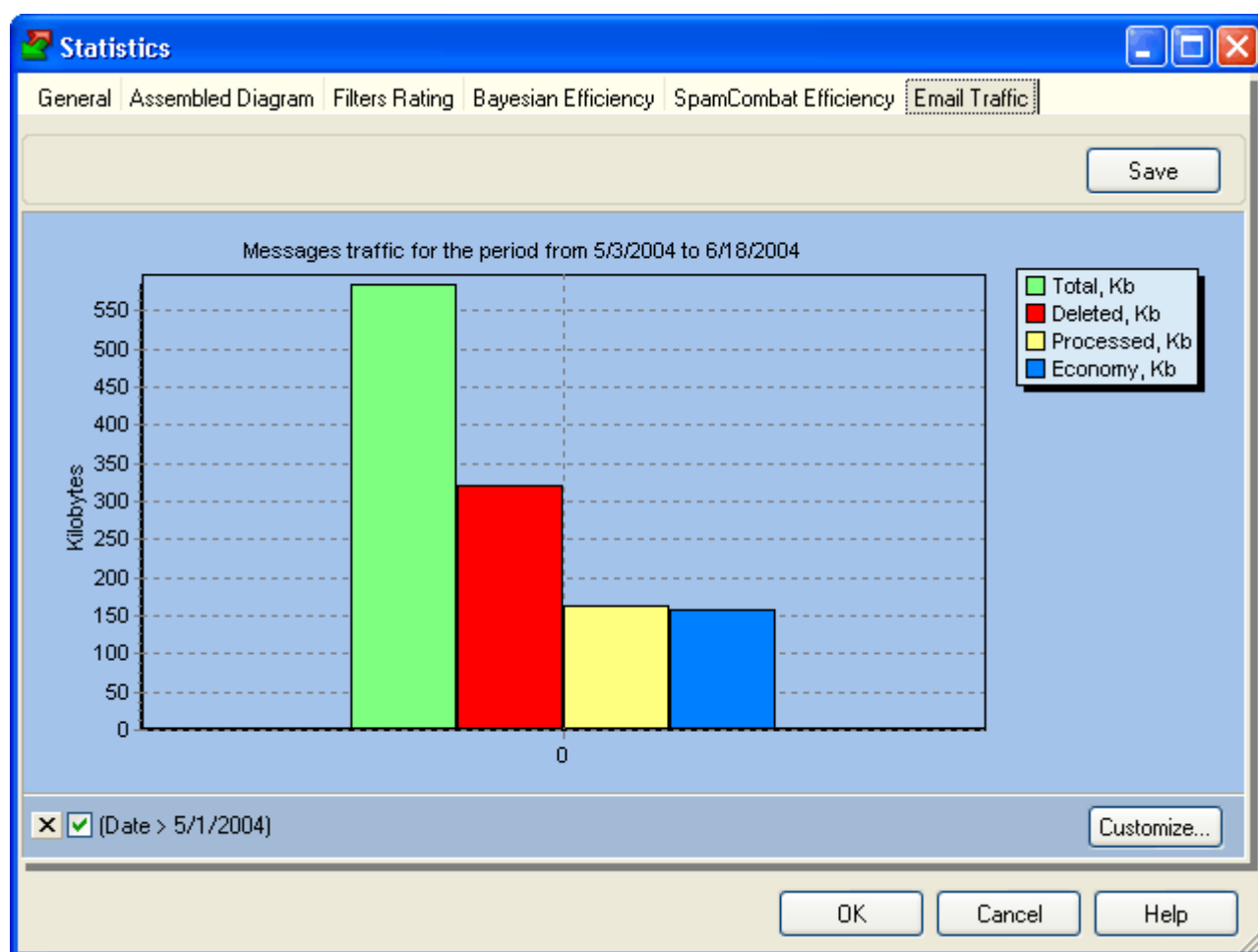
This tab shows the information about your email traffic:

**Total, Kb** - total size of email messages on your POP3 accounts (checked with SpamCombat)

**Deleted, Kb** - size of email messages deleted with SpamCombat

**Processed, Kb** - quantity of kilobytes received with SpamCombat (messages headers and a number of lines from the message body)

**Economy, Kb** - quantity of kilobytes you saved with SpamCombat



To save the diagram to a file of the .bmp format, click **Save** button.