



Pinjo revealer 2.0
SPAMFILTER TECHNOLOGY

User Manual

Basic installation	3
Note.....	3
Windows	4
Status window	4
Mail window	6
Filtering window	8
Relaying window	13
Virus check window	15
Thread window	18
Statistics window	19
Manual Configuration	21
Settings file	21

Basic installation

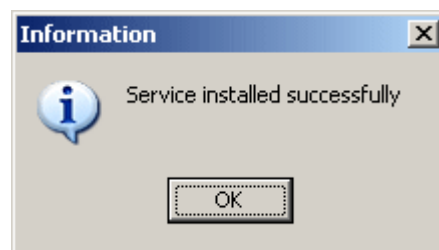
Pinjo is built to have an intuitive user interface. Easy to use menu's should do the job for you and most settings can be done within this user interface.

When running the setup program of Pinjo, and clicking the 'Setup' button on the screen, only few questions will be asked you. The default directory where Pinjo will be installed is "c:\Program Files\Pinjo Software\Pinjo revealer". Furthermore a Program group called Pinjo revealer will be created. Both mentioned settings can be modified by the user during installation.

When starting Pinjo the first time the settings that should be adjusted first are on the Mail Window screen.

Note

On installation Pinjo will be setup as a normal program that can be started manually. If you want Pinjo to run as a service then use the commandline option '-install' once. eg. "`<Program Files>\Pinjo Software\Pinjo\Pinjo.exe -install`". A popup box should come up saying 'Service installed successfully'



Windows

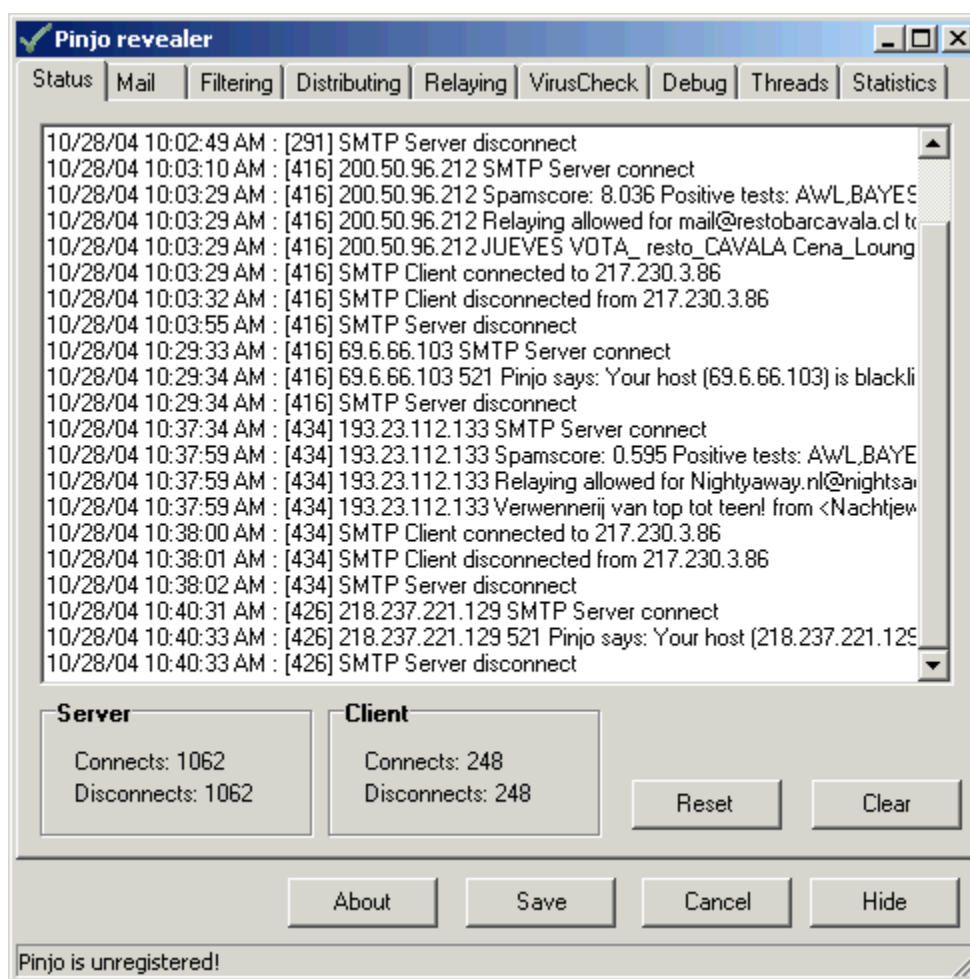
Status window

The screen that will popup first when starting Pinjo is the Status window (or when running Pinjo as a service when double-clicking the tray icon). This window shows all incoming connections, the results of the blacklist querying and some other statistical information.

Logging window

Server and Client panels

Reset and Clear buttons



Logging window

The logging window shows all kinds of information about incoming SMTP connections. Every line in the log window (and also in the log file) is preceded by a time mark value of the following event in the format dd/mm/yy hh:mm:ss. After the time mark the threadid is shown in the format [1234]. The threadid is the referrer of the task executed and can be used to find out what events belong to

the same connection.

The messages that can be seen after the threadid can be numerous like Connect and Disconnect of server and client, results of blacklist queries and relaying information.

The logging window will keep a history of 1000 lines. If you need to look back further the logfiles have to be checked.

Server and Client panels

The Server and Client panels contain information about the number of connects and disconnects occurred. The Server panel contains the information about incoming connections and the Client panel of outgoing connections. Some mailservers send multiple messages in a single connection. So sometimes the number of client connections can be higher as the number of server connections.

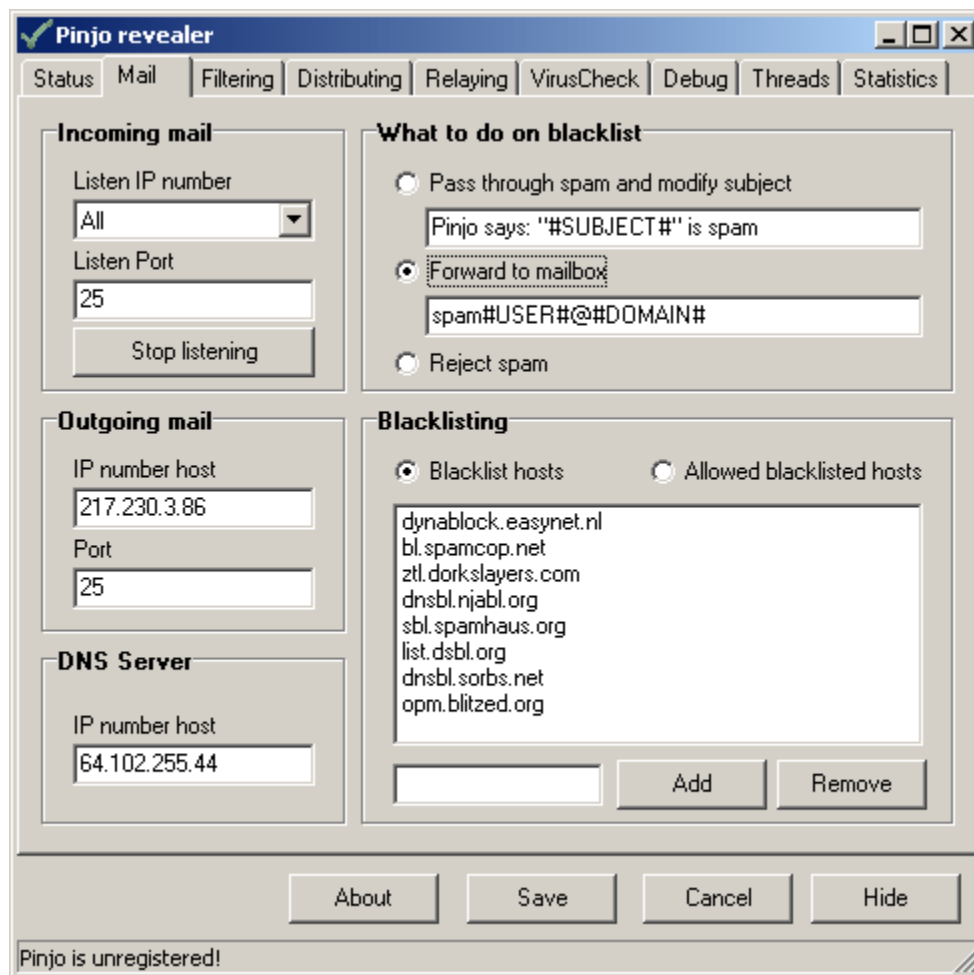
Reset and Clear buttons

The Reset button clears the counters of the Server Panel. The Clear button clears the logwindow.

Mail window

The mail window contains all settings necessary for connections between the internet and the internal mailservers. Also the black- and whitelists hosts and the DNS Server must be defined here

Incoming mail
Outgoing mail
DNS Server
What to do
Blacklisting



Incoming mail

The incoming mail properties represent the ip numbers and the port on which Pinjo should be listening. By default Pinjo will listen to all IP numbers assigned to your server. The pulldownbox 'Listen IP number' contains all available IP numbers on your server. When selecting one and clicking the Save button, new settings will be applied and saved.

Outgoing mail

The outgoing mail properties represent the ip numbers and the port where Pinjo should sent the checked mailmessages. When clicking the Save button, new settings will be applied and saved.

DNS Server

This is the IP address of the DNS server that Pinjo will use for the blacklist lookups. This doesnt need to be the same DNS server that you use on your system.

What to do

The 'What to do' panel gives you the options to pass through or reject mail.

If you select the Pass through and modify subject option, all mailmessages will be forwarded with possible Subject modification. The original subject is referred to as #SUBJECT#. So a spammessage with the subject 'Mortgage rates' will be modified to 'Pinjo says: "Mortgage rates" is spam' if you use default setting from Pinjo.

Its also possible to choose for no subject modification. Spammail can still be detected since a header variable is added with the name X-Spam-Status. In case of spam the value of this variable will be 'Positive', in case of non-spam the value will be 'Negative'. If you select the Reject spam all detected spam messages will be denied. This will be done right away at the start. Pinjo will return the message '521 Pinjo says: Your host ('[ip number]') is blacklisted on [blacklist]'. After the message is sent to the server Pinjo will disconnect. Traffic is reduced to a minimum this way.

Blacklisting

In the blacklisting panel the hosts can be entered on which checking has to be done. Checking on all hosts here is done simultaneously, so it doesn't make a difference in what order they are in the list. IP are numbers checked in reversed notation since most blacklist work this way. So if a host with IP number 93.233.77.22 is checked on server blacklist.com a query is done as 22.77.233.93.blacklist.com.

In the 'Allowed blacklist hosts' the IP numbers of hosts that are blacklisted can be entered so they will be explicitly permitted although they are blacklisted.

Adding and Removing is done by using the appropriate buttons.

Changes to the black and white-lists will be active immediatly. To save the changes the Save button should be pressed.

Filtering window

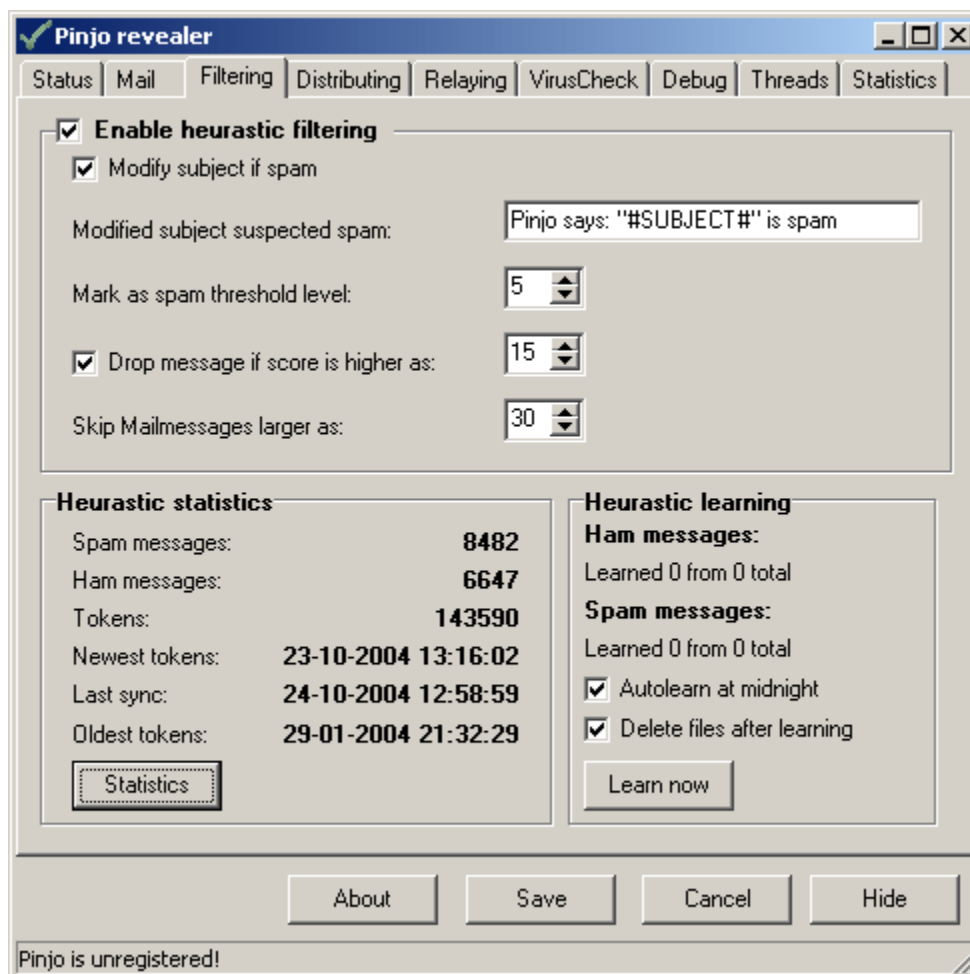
The filtering window contains all information about heuristic scanning. The complete mailmessage will be tested on multiple items, including bayesian analysis.

All these tests together result in a total score. The higher the score the more likely it is that the message is spam. It's also possible to modify the subject when the score exceeds a certain level.

Enable heuristic filtering

Heuristic statistics

Heuristic learning



Enable heuristic filtering

The **Enable heuristic filtering** checkbox will enable the heuristic scanning of mail messages and enable the concerning panel when checked.

Option available are:

Modify subject if spam

If checked this setting will enable the inputbox **Modify subject suspected spam**. Pinjo can modify

the subject if the score exceeds the value defined in **Mark as spam threshold level**

Modify subject suspected spam

This inputbox contains the new subject of the mail message in case the message will be marked as spam. The variable **#SUBJECT#** will be replaced by the original subject of the message.

Mark as spam threshold level

Here the level is specified at which the message must be marked as spam. If the determined score of the message exceeds this level, the message will be marked as spam. The default value is 5. This is a reasonable reliable score.

Drop message if score is higher as

This checkbox gives the possibility to drop the message at a certain score. Choose a score here where you are absolutely sure that the message will be spam. Default value is 15. Scores higher as 15 are most probably spam, as they have so much positive tests.

Skip mailmessages larger as

Since most spam messages or not particularly big, you can set the level when a message will be skipped for testing. Size is set in KiloBytes here.

Note: This skipping of messages ONLY involves the heuristic scanning. Viruschecking and others tests will always be done.

Heuristic statistics

The **Heuristic statistics** panel shows details about the bayesian database. Statistics information is only updated on pressing the **Statistics** button.

Spam messages

The number of messages in the database considered as spam.

Ham messages

The number of messages in the database considered as non spam (also called 'ham').

Tokens

The number of tokens in the database. A token is one word.

Newest tokens

Date of the last token in the database. It's possible that this value is a bit in the future.

Last sync time

Date and time of the last synchronisation of the database.

Oldest tokens

Date of the oldest tokens in the database. Tokens will not stay forever in the database. Older non used tokens will be removed from the database at sync times.

Heuristic learning

The **Heuristic learning** panel shows when and how the manual heuristic learning will be done. This learning is an addition to the the automatic learning. If messages are not marked as spam, or most surely or not spam, you can place a copy of those messages in the appropriate folder (./spam for spam and ./ham for non-spam). Pressing the **Learn now** button will analyse the message and update the heuristic database for statistical analysis.

Messages can only be learned once. If a message is already learned before, it will be skipped.

Autolearn at midnight

When checked, mailmessages placed in the appropriate folders will be automatically processes at midnight.

Delete files after learning

When checked, files processed for learning are deleted after processing. This will involve automatic and manual learning.

Distributing window

The distributing window contains all options for distributing mail to multiple mailservers. In this case you only need one version of Pinjo for several mailservers.

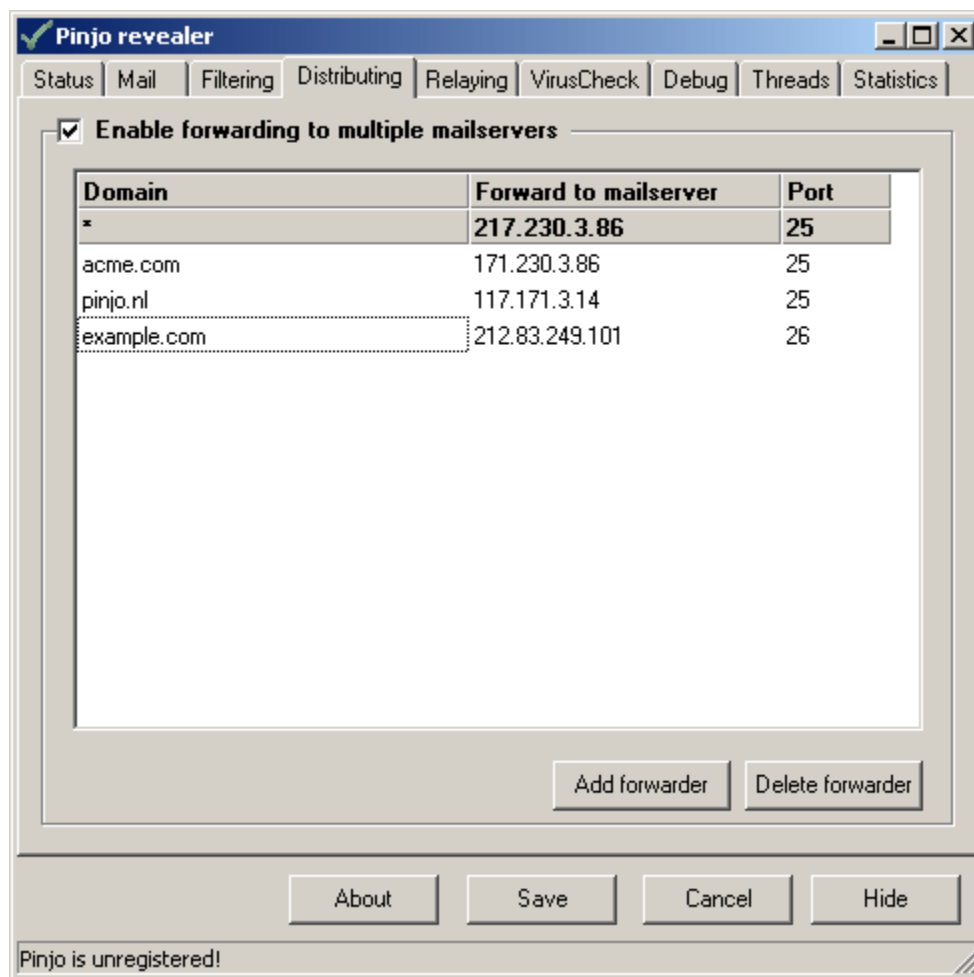
When activated mail will be forwarded to a mailserver in the list depending on the filled in domain. The * domain is the default outgoing mailserver from the Mail window. This means that all undefined mail will be forwarded to this server.

Enable forwarding to multiple mailservers

Domain list

Add forwarder

Delete forwarder



Enable forwarding to multiple mailservers

If enabled (checked) the lower pane is active and mail will be forwarded according to the rules defined. The * domain cannot be deleted from the list and will always be active. All undefined mail

will be forwarded to the default mailserver configured in the Mail window.

Domain list

In this list the different domains and mailservers Pinjo should forward your mail to can be configured. A match is done between the email-address and the domain list. If you enter a domain like '.com' all email addresses ending with '.com' will be relayed. This is obviously not a good solution. So more specific entering of domains is recommended like 'acme.com' or '@acme.com'.

Add forwarder

The Add forwarder button adds 1 extra empty field in the list. Non used empty fields will not be saved.

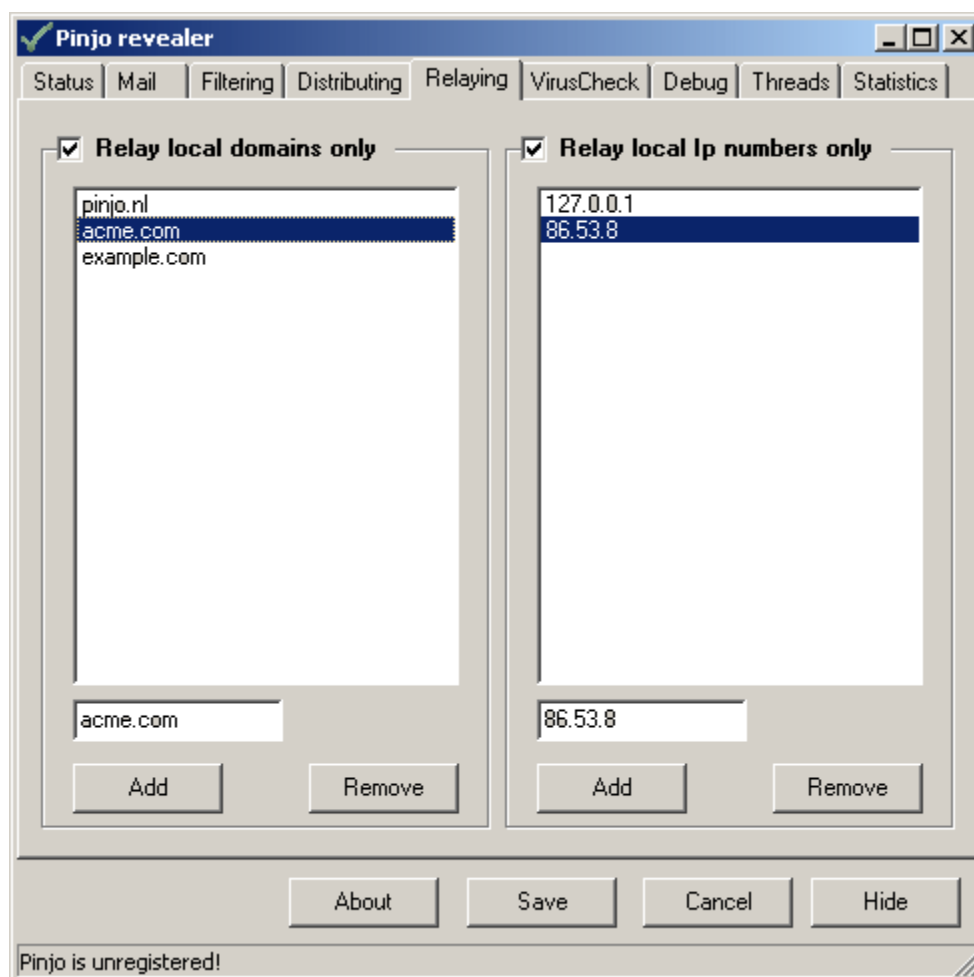
Delete forwarder

The Delete forwarder button deletes the current active row from the Domain list

Relaying window

The relaying window contains all options for relaying. These options prevent that your mailserver will be used as a forwarding server. If your mailserver relays unrestricted mail for everyone, there is a big chance your mailserver will end up on a blacklist itself. Once your mailserver is blacklisted large numbers of emailmessages will be denied by other servers. Besides that, once your server is blacklisted the process to remove it from that list again can be very time consuming.

Relay local domains only
Relay local Ip numbers only
Local Domains
Local Ip Numbers



Relay local domains only

The 'Relay local domains only' checkbox activates the 'Local Domains' list. If this is checked then only mail from and to the listed domains will be possible. Any other mail will be rejected with the warning '550 Pinjo says: not local address [emailaddress], not a gateway'. In this way your

mailserver cannot be used as a pass-through mailserver, saving you a lot of load.

Relay local Ip numbers only

The 'Relay local Ip numbers only' checkbox activates the 'Local Ip numbers' list. If this is checked then only mail with a from address that matches the 'Local Domains' list and an Ip number matching one of those in the 'Local Ip numbers' list will be relayed. This gives you an even better relaying protection.

Local Domains

In this list the domains your mailserver handles should be entered. A match is done between the email-address and the domain list. If you enter a domain like '.com' all email addresses ending with '.com' will be relayed. This is obviously not a good solution. So a bit more specific entering of domains is recommended like 'acme.com' or '@acme.com'

Local IP Numbers

In this list the IP numbers of your own users can be entered. A match is done between the start of the sending IP-number and the (parts of) ip numbers in the list. If you enter the number '194.171.50.' in the list, all ip numbers that start with that number will be allowed. In this case it will be the whole class C-address (194.171.50.0 - 194.171.50.255).

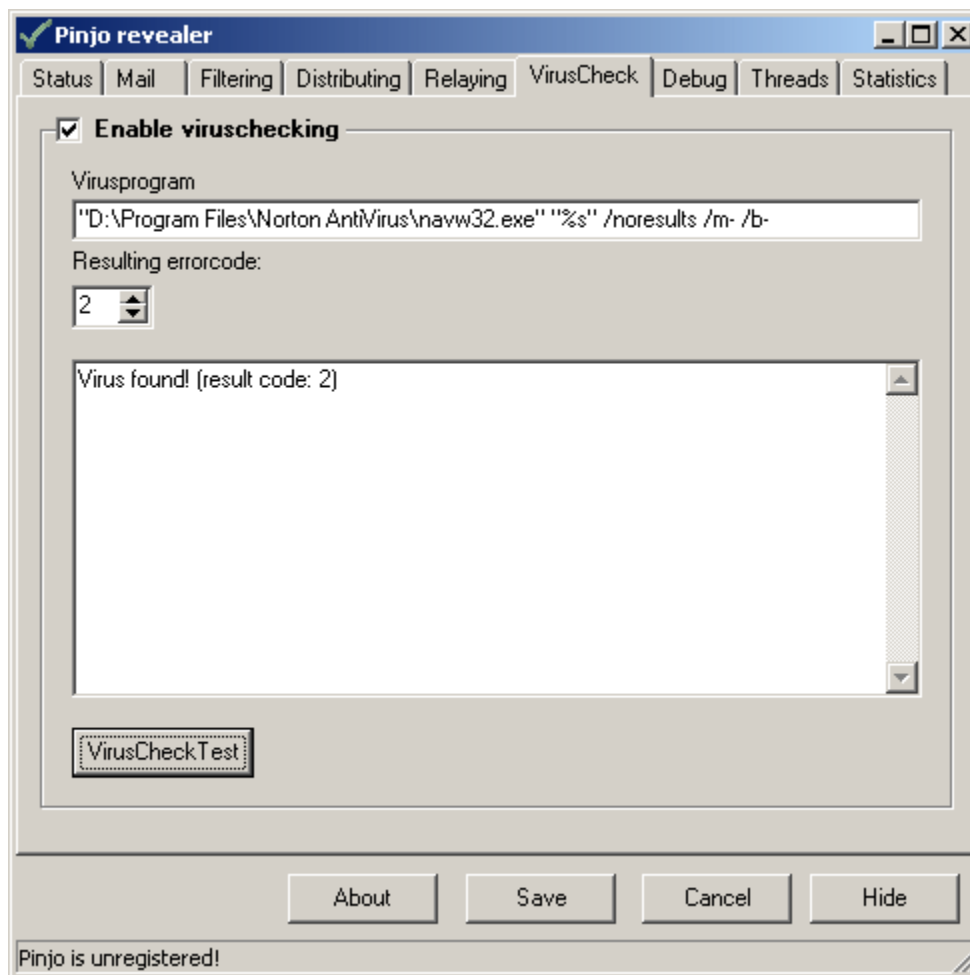
Subnet addressing is not possible yet.

Changes will be activated when pressing the Save button.

Virus check window

The virus check window contains all information about the viruschecking parameters. Pinjo revealer doesn't have an own virusscanner implemented. Instead it can use your own virusscanner to scan your incoming mail messages for viruses. Most virus checker are able to produce an error code as output. Pinjo responds to that and refuses the message.

Enable viruschecking



Enable viruschecking

Enabling viruschecking makes it possible for you to protect your mailserver from viruses with a normal virusscanner.

The virusprogram inputbox contains the virusprogram and its parameters. The "%s" parameter is necessary because Pinjo will substitute it with the current temporary file. If the path to the virusprogram contains any spaces, quotes should be used.

The resulting errorcode box contains the errorcode or errorlevel the virusprogram reports when a virus is detected. By using the the VirusCheckTest button you can test if your settings are correct. You can use the eicar test virus in a file to see if your setup is correct. The resultpane gives the received errorcode and if your setting are correct it should say 'Virus found!' and the received errorlevel. In this way it's possible to adjust your settings.

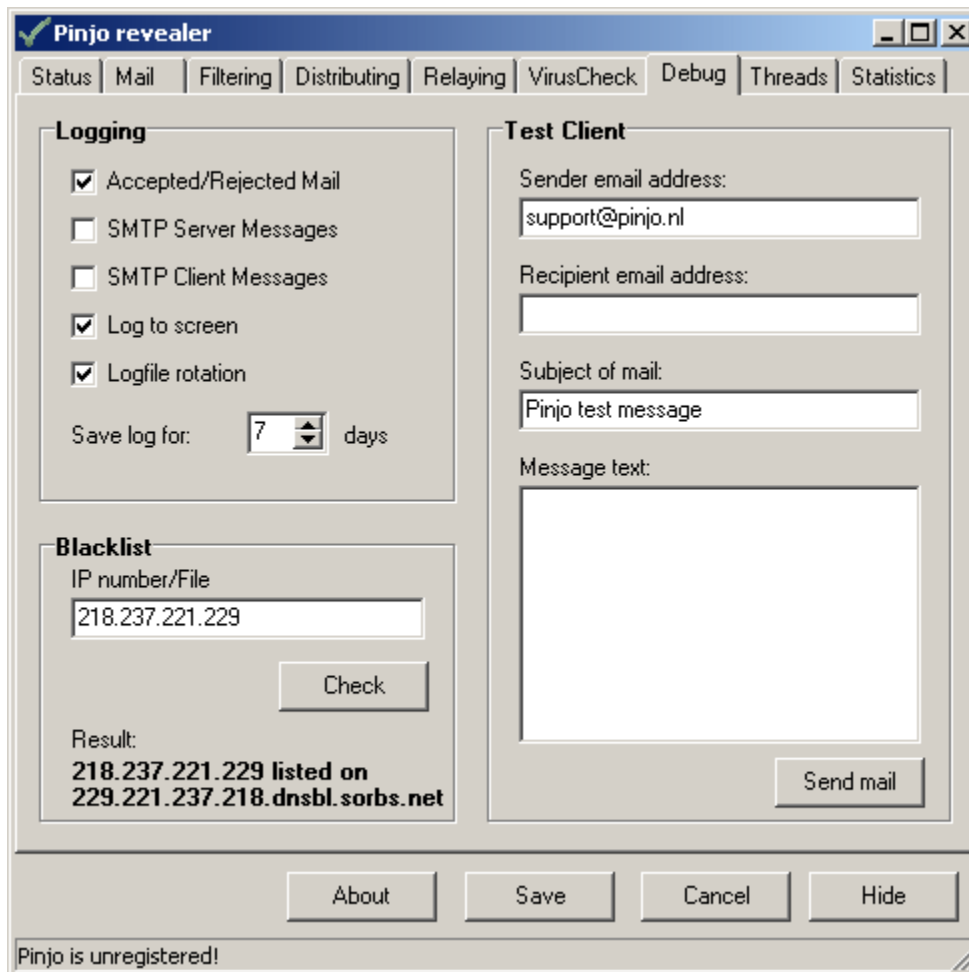
Debug window

The debug window contains options for debugging and checking settings. Also the logging options can be modified here.

Logging

Black list

Test client



Logging

The logging panel has several checkboxes to define the level of logging.

The Accepted/Rejected mail option shows you all default messages as Connect and Disconnect, the relaying messages and the results of the blacklists querying.

The SMTP Server Messages option shows all SMTP communication between the sending mailserver and Pinjo. This logging can be very verbose.

The SMTP Client Messages option shows all SMTP communication between Pinjo and your mailserver. This logging can also be very verbose.

The Log to screen option logs all output to the statusscreen. In case of debugging it can be useful to

disable this option, since all logging will be saved to a logfile
The Log file rotation option will close the logfile (Pinjo.log in the subdirectory 'log') at midnight every day. The file is renamed to the format 'Pinjo.[yymmdd].log'. Thus a log file from September 6, 2003 will be saved under the name 'Pinjo.030906.log'.
The Save log for input field is the number of days log files should be kept on the system before deletion.

Black list

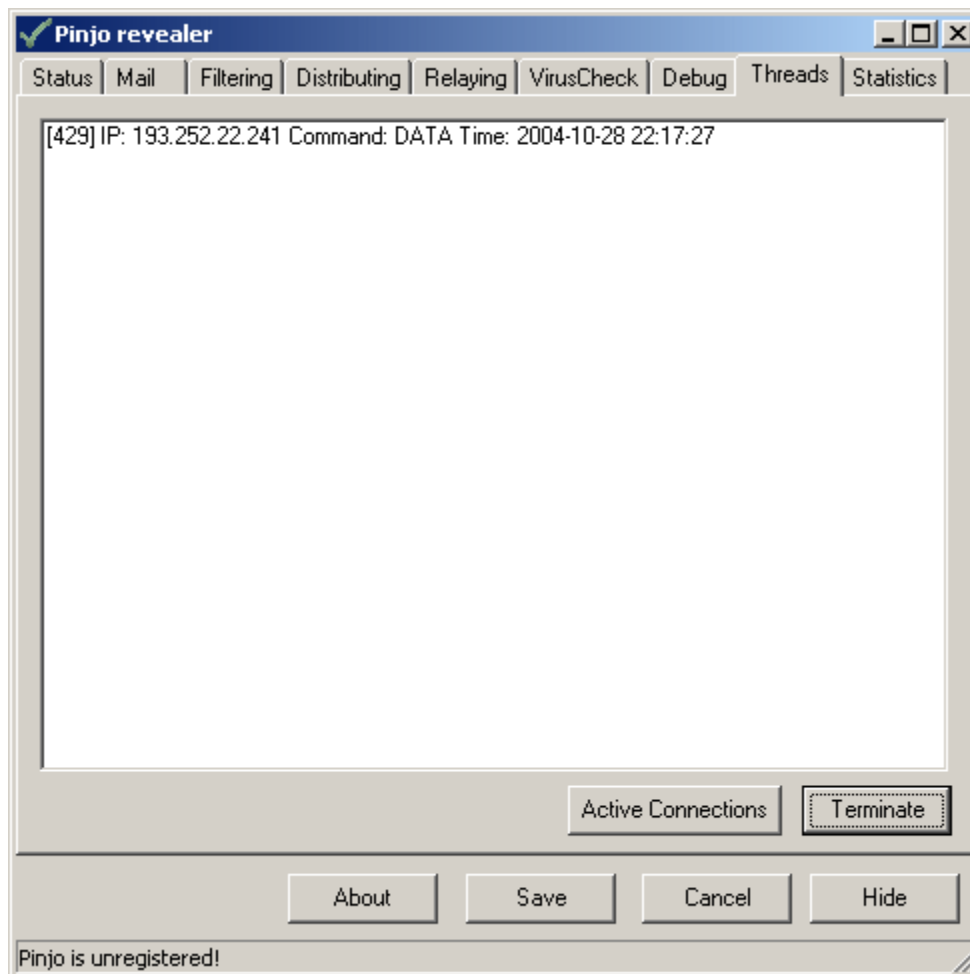
The black list panel provides you an inputbox to test the working of your blacklist. As an input the IP number of the host to test should be given here. The result will be shown in the same panel. Note that only the first reacting blacklistservers will be listed here.

Test client

Here you can test the functioning of your relaying options by entering different kind of emailaddresses. Only the domainrelaying can be tested here, not the Ip relaying. Any valid message should be sent to your mailbox. Error messages are returned to the screen as a popup box.

Thread window

The thread window contains the information about currently running threads.



Every line represents on thread. The line contains the threadid (in the format [1234]) followed by the IP number of the foreign mailhost. After that the last received command is shown together with its timestamp. Doubleclicking on a thread gives you information about the history of concerning thread. Every received command with the timestamp is shown then.

The button Active connections shows the currently active server and client threads. The number of client threads can never exceed the number of server connections. The button Terminate forces to close the currently selected thread.

Statistics window

The statistics window contains the information about the querying of the blacklist servers. This window consists of two panes. The upper pane (General Statistics) gives you information about Pinjo in general and the bottom pane (Blacklist Statistics) provides information about every blacklist server you have inserted.

General Statistics Blacklist Statistics

General statistics

Pinjo started on: **October 26, 2004 11:31:14**
 Last time cleared counters: **October 26, 2004 11:31:14**
 Total connections served: **1067**
 Mailmessages refused (detected): **899**
 Mailmessages passed through: **250**
 Blocked for relaying: **2**
 Blocked for blacklisting: **697**
 Viruses found: **4**
 Heuristic positives: **196**

Blacklist statistics

Hostname	TotalChecks	Timeout	Listed
bl.spamcop.net	1029	1	576
sbl.spamhaus.org	1029	3	31
list.dsbl.org	1029	4	465
combined.njabl.org	1029	1	252

Update Reset Counters

About Save Cancel Hide

Pinjo is unregistered!

General Statistics

Pinjo started on: the time and date Pinjo was started.

Last time cleared counters: Last time of clearing the counters. (Pushed the Reset Counters button)

Total connection served: The total number of connections that Pinjo has served.

Mailmessages refused: The total number of mailmessages refused (or detected as spam).

Mailmessages passed through: The total number of mailmessages passed through to the client. This

may also be positive marked spam.

Blocked for relaying: The number of mailmessages blocked because of relaying issues.

Blocked for blacklisting: The number of mailmessages blocked because of being listed on a blacklist server.

Blacklist Statistics

The lower pane has a table with the properties Hostname, TotalChecks, Timeouts and Listed. The same hosts as entered in the blacklistserver screen are visible here. The number of totalchecks represents the number of queries to that specific host, as the Listed column represents the number of positive queries (as possibly spam). If the number of timeouts is high you might consider increasing the 'DNSTimeout' value in the settingsfile.

The button Update updates the counters with the new values. This button is only necessary in case you leave this window open. Changing tabs or maximising Pinjo updates the counters automatically. The button Reset counters sets all the available counters on the statistics window to their initial value, The 'Last time cleared counters' value will be set to the current time.

Manual Configuration

Settings file

All the settings of Pinjo are stored in the file *Pinjo.ini*. This file is located in the directory where Pinjo is installed.

Most settings from the ini-file are configurable via the userinterface. The ini-file consists of 9 sections: Settings, Heuristic, Viruscheck, Debug, BlackLists, AllowedHosts, LocalDomains, LocalIp and Forward.

Settings
Heuristic
VirusCheck
Debug
BlackLists
AllowedHosts
LocalDomains
LocalIp
Forward

Values marked in **red** can only be configured directly in the settingsfile.

[Settings]

The settings section has all values for the server and client connection.

ListenIP

Contains the IP number where Pinjo is listening to. If empty Pinjo will be listening to all available IP numbers on the system.

ListenPort

Contains the port number where Pinjo is listening to. Default port 25 will be used.

OutgoingIP

Contains the IP number of your original mailserver. Pinjo will forward all mail to that mailserver.

OutgoingPort

Contains the port number where Pinjo will connect to. Default port 26 will be used.

DnsIP

The Ip number of the DNS Pinjo will use for blacklist lookups.

ServerTimeout

This is the timeout value of the server in case of no activity. Default this timeout will be 600 seconds or 10 minutes.

NewSubject

This is the new subject of your mailmessages in case of spam. Default it is 'Pinjo says: "#SUBJECT#" is spam' where #SUBJECT# will be replaced with the original subject of the mailmessage

ModifySubject

Setting to determine whether Pinjo should pass through spammail or reject it. Default value is 1 (meaning TRUE).

RelayLocalOnly

Setting to determine whether Pinjo should relay local domains only. Default value is 1 (meaning TRUE).

RelayLocalOnlyIP

Setting to determine whether Pinjo should relay local IP numbers only. Default value is 1 (meaning TRUE).

MaxConnections

Setting to limit the number of simultaneous incoming connections. Default value is unlimited.

ClearCounterOnRotate

Setting to clear the counters when rotating the logfiles. Since counters can increase to a large

number this might be useful. Note that this setting only applies to the counters on the statistics window. Default value is 0 (meaning FALSE).

DNSTimeout

Setting to change the timeout value of the blacklist servers. You might want to increase this if the number of Timeout values is large in the statistics window. Default value is 5 seconds.

MultipleMailForwarding

Setting to enable or disable the use of mail forwarding to multiple underlying mailservers. In this case you only need 1 version of Pinjo for multiple underlying mailservers. Default value is 0 (meaning not used: all mail will be forwarded to the default mailserver).

Forward

Specifies that spammail should be forwarded to an other emailaddress as stated in MailForwardAddress. The original user mailbox will remain clean from the specified messages.

MailForwardAddress

Specifies the address where mail should be forwarded to in case it's marked as spam. This setting is only valid in when the Forward setting is enabled. The use of the variables #USER# and #DOMAIN# make it possible to forward spam to a new mailbox for each user.

Eg. when using **spam#USER#@#DOMAIN#** as value, all spammail for user demo@example.com will be forwarded to spamdemo@example.com.

[Heuristic]

DoHeuristic

Setting to determine whether Pinjo should do heuristic email scanning. Default is 0 (meaning FALSE)

ModifySubject

Setting to determine whether Pinjo should change the subject when suspected spam. Default value is 1.

NewSubject

This is the new subject of your mailmessages in case of suspected heuristic spam. Default it is 'Pinjo suspects: "#SUBJECT#" is spam' where #SUBJECT# will be replaced with the original subject of the mailmessage.

Threshold

Specifies at which score mail should be marked as spam. Default mail will be marked as spam when the score is 5 or above.

MaxMailSize

Setting to prevent checking of large messages, which will probably not be spam after all. Default setting is 30 (KB). Mail messages larger as this value will not be checked.

HeuristicCheckTimeout

The maximum time a heuristic check should take. This is a built in precaution in case the external heuristic program stops responding. Pinjo will automatically terminate the process after the specified time. Time is specified in ms. default is 300000 which is 300 seconds.

DropAtScore

Specifies to drop the message if the score exceeds the value in setting **DropScore**

DropScore

Specifies the score threshold at which a mailmessage should be dropped instead of forwarded. Used in combination with **DropAtScore**

AutoLearnAtRotate

Specifies whether autolearning should be initiated at midnight after logfile rotation. Default is 1 (meaning TRUE)

DeleteFilesAfterLearn

Specifies whether Pinjo should delete the files after the learning process. Default is 1 (meaning TRUE)

[VirusCheck]

DoVirusCheck

Setting to determine whether Pinjo should check for viruses in email messages. Default is 0 (meaning FALSE)

VirusProgram

Specifies the commandline and parameters that should be executed to viruscheck a mail message. the variable %s should be used to specify the temporary mail message, and will be filled by Pinjo.

VirusCheckTimeout

The maximum time a virus check should take. This is a built in precaution in case the external

viruscheck program stops responding. Pinjo will automatically terminate the process after the specified time. Time is specified in ms. default is 30000 which is 30 seconds.

ResultCode

This setting should contain the return errorlevel of the virus check program when a virus is detected.

[Debug]

Acceptance

Setting to log all connects, disconnects, blacklist queries and relay statistics. Default is 0 (meaning FALSE)

SMTPServer

Setting to log all communication between the SMTP server and Pinjo. This logging can be very verbose. Default is 0 (meaning FALSE)

SMTPClient

Setting to log all communication between Pinjo and your mailserver. This logging can be very verbose. Default is 0 (meaning FALSE)

LogScreen

Logging to the statusscreen will be activated by this setting. Default is 0 (meaning FALSE)

LogFileRotation

If enabled logfile rotation will take place. Default is 0 (meaning FALSE)

LogFileWindowSize

Value of the logfile rotation window. Logfiles will be saved during the number of days entered here. Default is 7 days.

[BlackLists]

0..X

Names of the blacklist servers.

[AllowedHosts]

0..X

Names of the explicitly allowed servers. Mail from these servers will not be blocked when blacklisted.

[LocalDomains]

0..X

Names of the local domains.

[LocalIp]

0..X

Names of (parts of) the local IP numbers.

[Forward]

0..X

Domains (or parts of them), emailserver and portnumber comma-delimited where mail, according to the match rules, will be forwarded to.