



# **SMTP Analyzer**

**Version 1.0**

*User's Guide*

## Table of Contents

Product Overview.....	3
Using SMTP Analyzer.....	4
Working with the viewer .....	4
Viewing message headers .....	5
Applying Search Criteria.....	6
Copying Rows.....	7
Troubleshooting.....	8
Contact Information.....	10

## Product Overview

SMTP Analyzer is designed to aid the process of tracking the emails flowing through your SMTP server. Developed to work with Microsoft® Exchange Server 2000/2003 and the IIS SMTP Server, this product rids you of the need to pore over the default SMTP logs or dig through Exchange's Message Tracker. All of the information about your SMTP traffic is gathered into a single SQL Server database. An easy-to-use viewer allows you to provide relevant search criteria, quickly narrowing down to just the information you want to see.

1. SMTP Analyzer works by hooking into the SMTP sinks provided by Exchange and IIS. By hooking into the relevant sinks, SMTP Analyzer can keep track of inbound and outbound SMTP traffic. For outbound mail, status messages from the receiving SMTP server are tracked, including information about delivery delays that might not always reach the sender of the email.

## Using SMTP Analyzer

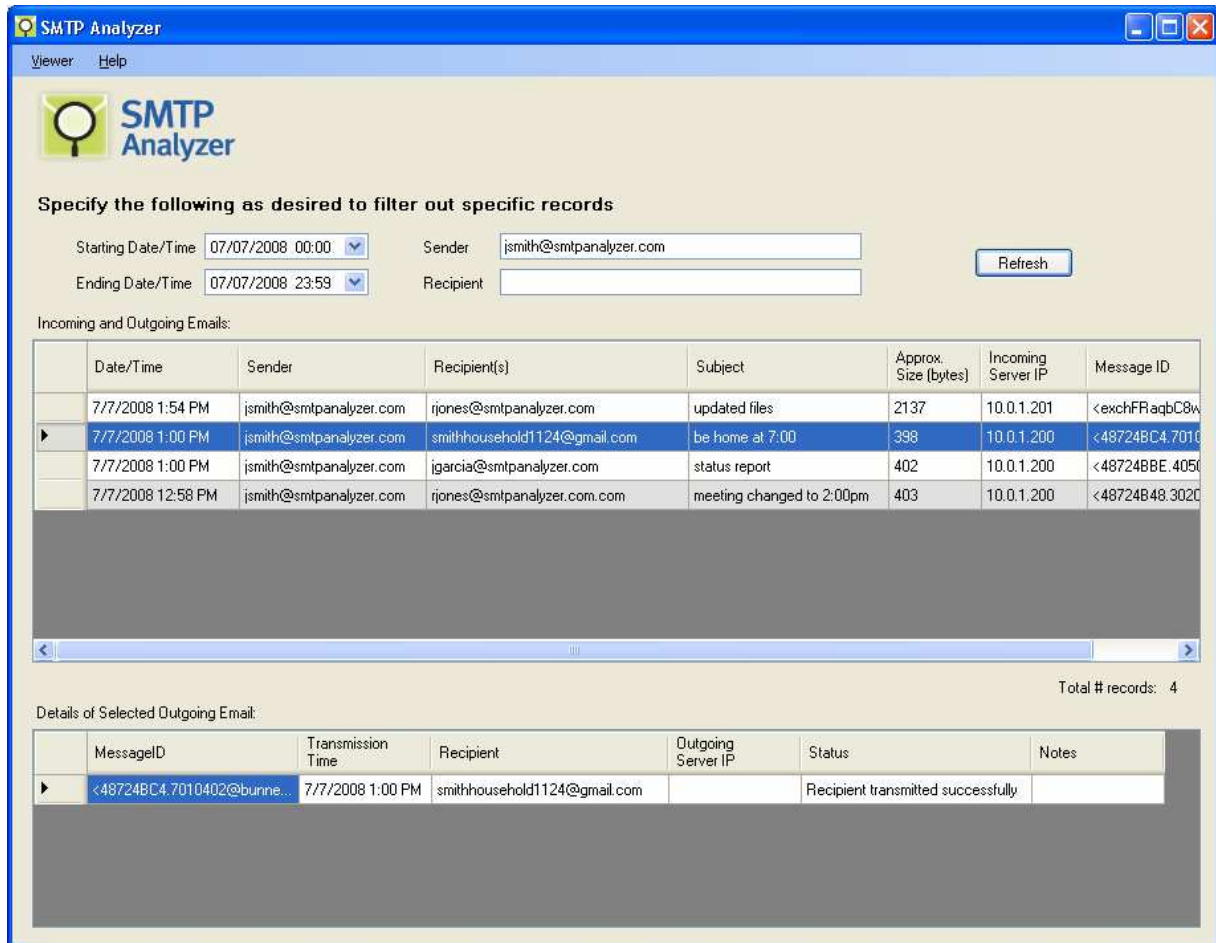
To view the emails logged by SMTP Analyzer, go to Start→All Programs→SMTP Analyzer→SMTP Analyzer Viewer. This will start the viewer.

### *Working with the viewer*

By default, the viewer automatically loads the information for that day's traffic. You will notice two grids. The top lists individual emails arriving at your server, either destined for local delivery or routed to an external SMTP server. Details include the time at which the email arrived at your SMTP server<sup>1</sup>, the sender, recipients, and subject line. An approximate size of the email is also included, as well as the Message-ID, used to help identify individual messages. If a message was routed to another SMTP server, clicking anywhere in the row of the top list will populate the bottom list with delivery details, including the time at which the external SMTP server was contacted, the server's IP address, and status information.

---

<sup>1</sup> Timestamps shown in the viewer are relative to the system clock on the SMTP server on which the server component of SMTP Analyzer is installed. Therefore, all times will reflect the time zone of your mail server.



**Figure 1: Filtering emails by sender and date**

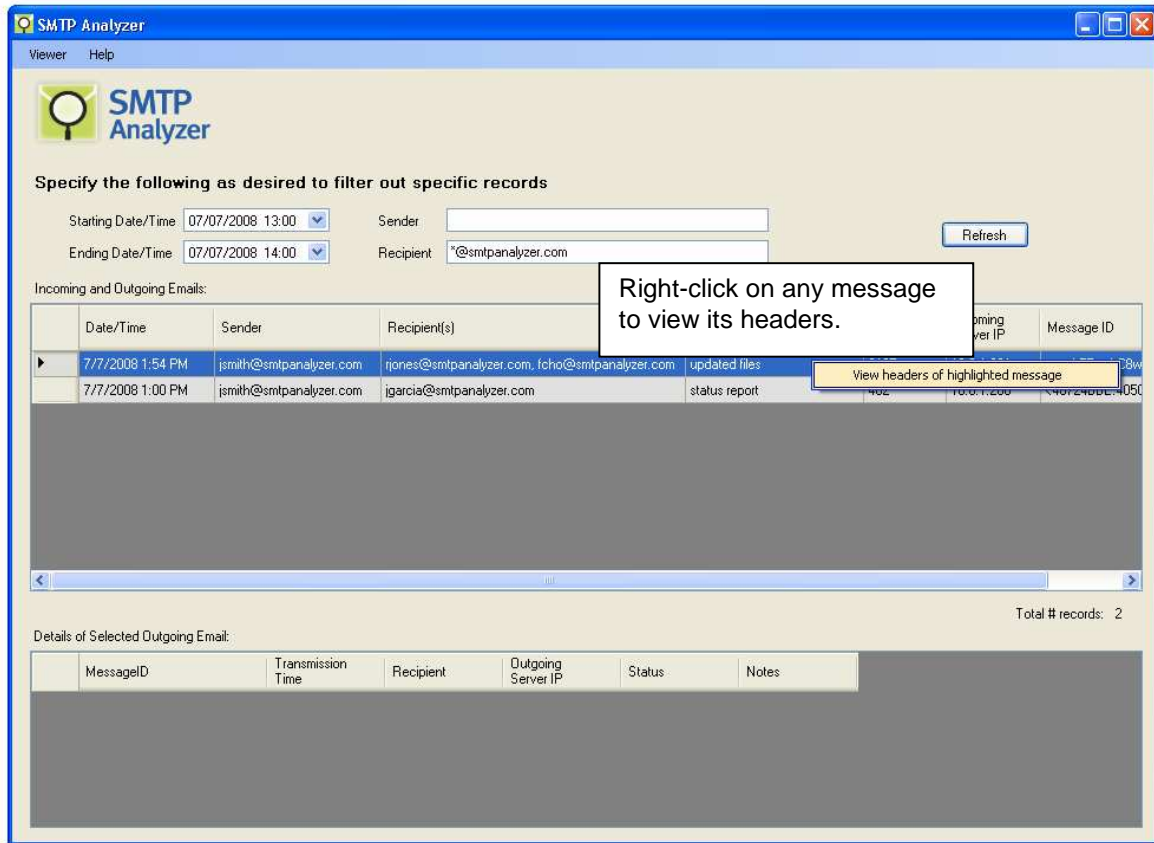
The information is loaded once by default when the application starts. To see any new emails that might have arrived, click the “Refresh” button.

Outbound email messages (those destined for email servers other than the one on which the application is installed) will be highlighted in different colors if the message is not immediately sent successfully. Rows colored in red indicate that the message delivery failed. Orange rows indicate that the message has been delayed. For messages that were eventually sent successfully, the highlight color is slightly lighter. Therefore, messages that were delayed but have since been successfully transmitted, the rows are highlighted in a light orange color.

## Viewing message headers

When you install the application, you are given the option to save each email’s message headers to the database. If you have this capability turned on, you may right-click on any email message in the top list and choose “View message headers for highlighted message.” A second window will pop up, displaying the headers. If you did not choose this option at install, you may change it at any time by going to Start→All Programs→SMTP Analyzer→Configuration Tool and going to the “Application Settings” tab. Be advised that saving the message headers

will cause your database to grow in size considerably more quickly than just saving the standard information.



## Applying Search Criteria

The top section of the screen allows you to change your search criteria. The only criteria you must provide are the starting and ending dates for the date range you would like to examine. All other criteria are optional. The date range will look at the arrival time of the email message to determine which emails to display. So, for example, if you were to enter yesterday's date, all details for messages arriving yesterday would be displayed. For outbound messages, all delivery details for the selected email will be displayed, even if the interaction did not take place until, for example, the next day, in the case of a delayed delivery.

Optionally, you may provide a sender and/or recipient's email address. For example, to look at all emails sent to [support@smtpalyzer.com](mailto:support@smtpalyzer.com), type that address into the "Recipient" box. Asterisks may be used as wildcards when entering the sender and recipient. So, to see all emails sent to anyone at SMTP Analyzer, enter [\\*@smtpalyzer.com](mailto:*@smtpalyzer.com) in the "Recipient" box.

Note: the "Recipient" field includes all recipients of the email strung together into a comma-separated field, similar to the "To:" box in many messaging clients. If you want to see messages for which a user is the only recipient, enter his/her email address in the "Recipient" box. To see messages for which s/he may be one of many recipients, put asterisks around the email address (e.g., [\\*user@smtpalyzer.com](mailto:*user@smtpalyzer.com)).

Any time you change your search criteria, you must click the “Refresh” button in the upper-right corner of the screen to apply your changes. Search criteria are applied in an “AND” fashion (as opposed to an “OR”). Therefore, the more criteria you add, the fewer matching messages you will see. If an expected message is not visible in the list, remove some of the search criteria. Do not add additional criteria. Adding additional criteria will only filter down the list of matches even further.

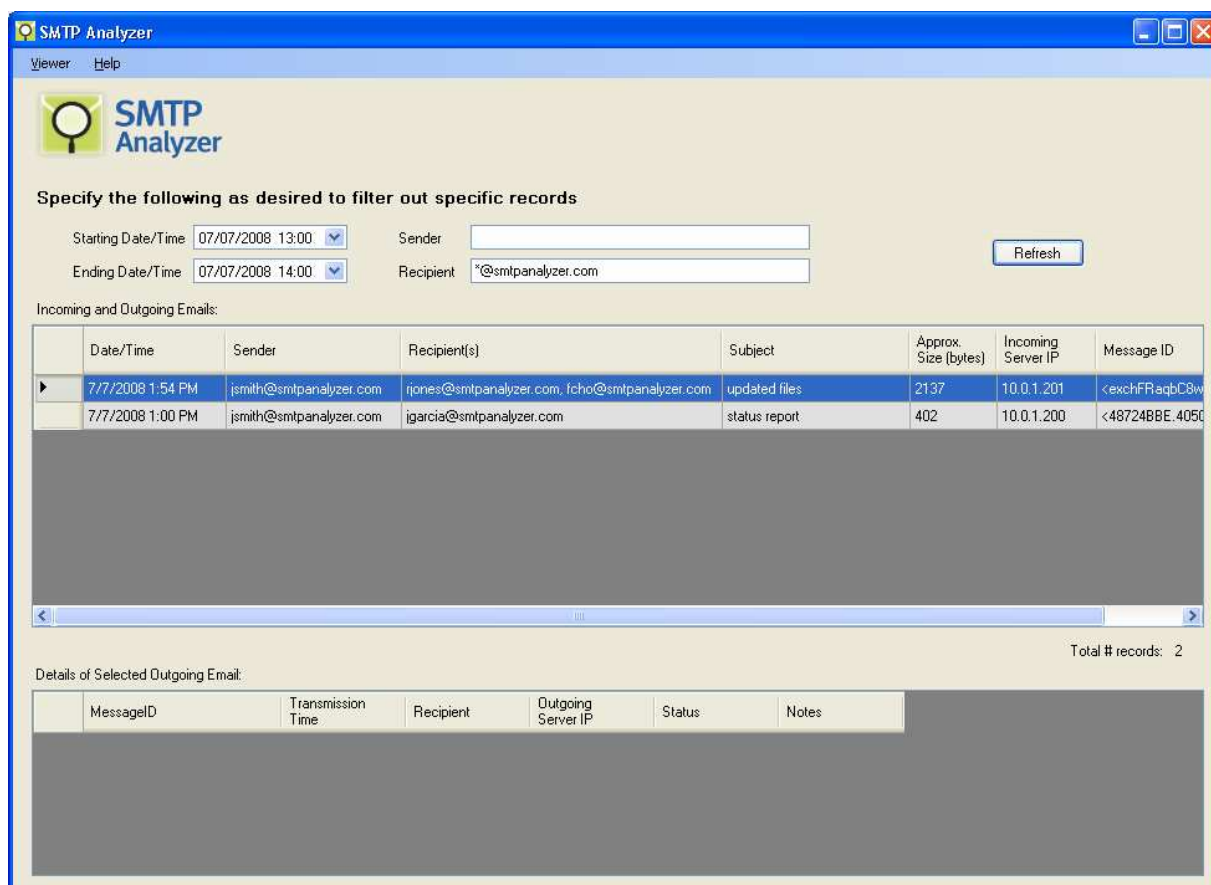


Figure 2: Emails sent to smtpalyzer.com between 2:00pm and 3:00pm

## Copying Rows

Rows in both grids can be copied into other documents as desired simply by doing a copy and paste. Individual rows may be highlighted simply by clicking on them. Multiple rows can be highlighted by Ctrl-clicking on individual rows or by clicking on one row, holding down the Shift key, and clicking on another row to select the rows in-between. Press Ctrl-c to copy the rows. They may then be pasted into another application (Microsoft Excel, Microsoft Word, etc.). To select all rows, you may click on a single row, press Ctrl-a to select all rows, then press Ctrl-c as usual to copy the rows to the clipboard.

## Troubleshooting

*Q: I don't see any emails in the viewer. Where are they?*

A: This can stem from a couple of issues.

1. Your search criteria may be too restrictive to show your email(s). Try removing restrictions on sender and recipient and expanding the date range. Click "Refresh" to update the viewer.
2. There may be an issue with your mail server or with the configuration of SMTP Analyzer. Try sending a test message from your email client, preferably to an address outside your SMTP server. Click "Refresh" in the viewer to update the list.
3. If the message does not appear, try sending a test message via telnet to ensure that the message is sent via SMTP. SMTP Analyzer does not track MAPI traffic. Some mail clients such as Outlook Web Access may only issue MAPI commands for emails that are destined for local delivery. To send an email via telnet, start up a command prompt and type the following. Press Enter at the end of every line (line breaks are crucial):

```
telnet <your mailserver> 25
ehlo
mail from: <your email address>
rcpt to: <the address that should receive the email>
data
subject: test email
testing SMTP Analyzer
```

Note the period on the last line. That will cause the email to be sent. To exit your telnet session, type "quit" and press Enter.

4. If none of the above work, confirm your install by opening up a command prompt on your mail server and navigating to the folder to which you installed the product. Type the following:

```
cscript smtpreg.vbs /enum > sinks.txt
```

This will make a list of all SMTP sink bindings on that computer. You should see five sink bindings for SMTP Analyzer: SMTPAnalyzer\_Receiver, SMTPAnalyzer\_Sender\_EHLO, SMTPAnalyzer\_Sender\_RCPT, SMTPAnalyzer\_Sender\_EOD, and SMTPAnalyzer\_Sender\_QUIT. (Do a search in sinks.txt to find these.) If you don't see these, or only see some of them, your install has gotten corrupted. Follow the instructions in this document for "Reinstalling SMTP Analyzer" and test again.

*Q: How do I manage my database of emails? It's getting large.*

A: Because we have no way of knowing how many emails your server receives or how long you might want to keep them, SMTP Analyzer has no built-in mechanisms for purging or archiving "old" data. Since the data are stored in a standard SQL Server database, you have all of its mechanisms for moving and deleting data available.

Here are some useful links regarding maintenance of SQL Server. This is not a definitive list of information and should not be considered to be "advice." We have no knowledge of your individual setup and, therefore, cannot make individual recommendations. You perform any of the following at your own risk. The following are links to SQL Server Books Online, Microsoft's definitive source of information on SQL Server 2005 and SQL Server 2005 Express. If these

links become inactive, try going to <http://msdn.microsoft.com> and searching for "SQL Server" and your question.

- Homepage: <http://msdn.microsoft.com/en-us/library/ms130214.aspx>
- Backups: <http://msdn.microsoft.com/en-us/library/ms191239.aspx>
- Maintenance Plans: <http://msdn.microsoft.com/en-us/library/ms187658.aspx>  
Maintenance Plans help you ensure that your data are regularly backed up and checked for possible errors.
- Changing a login's password (ALTER LOGIN): <http://msdn.microsoft.com/en-us/library/ms189828.aspx>
- SQL Server Tools Tutorial: <http://msdn.microsoft.com/en-us/library/ms170486.aspx>

*Q: Our database has moved. How do I update SMTP Analyzer to point to the new location?*

A: To update the database connection information, go to Start→All Programs→SMTP Analyzer→Configuration Tool. This will start with the current database connection information. Change this as necessary and click "Save Settings." Start up the viewer to test. Note: if you have the components (viewer and/or server components) on multiple computers, you will need to perform this step on each computer.

*Q: Our mail server has moved to a different computer. What do I need to do to move SMTP Analyzer?*

A: If your database is still in the same location, you only need to uninstall SMTP Analyzer from your prior mail server and install it on the new server. (Look at your licensing agreement to ensure adherence to your license.) Read "Installing SMTP Analyzer" above, but *skip* step 1 of running DBCreate.sql--your database already exists. If your database server has changed as well, you can either move your existing database to the new server so that you have all of your email information in one place, or you can start from scratch performing a full install as described in "Installing SMTP Analyzer."

*Q: None of the above helped. What now?*

A: You can contact our Technical Support by emailing [support@smtpanalyzer.com](mailto:support@smtpanalyzer.com). Please include the following in your email to help us get started:

- Version of SMTP Analyzer
- Type and version number of your SMTP Server (i.e., Exchange vs. IIS)
- A listing of the sinks registered on your computer. Open up a command prompt on your mail server and navigate to the folder to which you installed the product. Type the following:  

```
      cscript smtpreg.vbs /enum > sinks.txt
```

  
This will make a list of all SMTP sink bindings on that computer in the file `sinks.txt`. Please include that file.
- A detailed description of the issue with steps to replicate

## Contact Information

SMTP Analyzer is owned by Wendt Enterprises, LLC.

Wendt Enterprises, LLC  
6300 Creedmoor Rd.  
Suite 170, Box 245  
Raleigh, NC 27612-6745

*For sales information:* [sales@smtpalyzer.com](mailto:sales@smtpalyzer.com)

*For technical support:* [support@smtpalyzer.com](mailto:support@smtpalyzer.com)

*For feature requests:* [requests@smtpalyzer.com](mailto:requests@smtpalyzer.com)

*Microsoft, Windows Server 2003, Windows Server 2000, Windows XP, SQL Server, and Microsoft .NET are trademarks of the Microsoft group of companies.*