SpoofMail V1.1.7 - Sanderson Forensics 2002

What is SpoofMail

SpoofMail is an SMTP client program that provides the user with complete control over the client side of the dialog between the SpoofMail mail client and an SMTP server. SpoofMail is designed to be an educational tool and designed mainly as a training tool for those who may be involved in the tracing of internet e-mail.

What can SpoofMail do

SpoofMail allows the user to create a basic e-mail message and to send it to one or more recipients. The sender of the e-mail can be forged as can various other factors, such as additional headers and fake recipients.

SpoofMail also shows both sides of the dialog between the client and the SMTP server as the message is sent.

SpoofMail also includes a 'playground' area where individual commands can be sent to an SMTP client and the results of those commands displayed.

In order to facilitate the sending of e-mails using the SMTP protocol, the relevant RFCs are also provided RFC 821 – "Simple Mail Transport Protocol" and RFC 822 – "Standard for the format of ARPA internet text messages"

What can't SpoofMail do

SpoofMail does not support the mailing of attachments.

Disclaimer

SpoofMail is an educational tool only; to this end each e-mail message sent by SpoofMail has a disclaimer appended to the message that is not within the control of the sender (see below).

It is up to the user to ensure that he or she has the relevant authority and rights to the particular SMTP server used to send an e-mail.

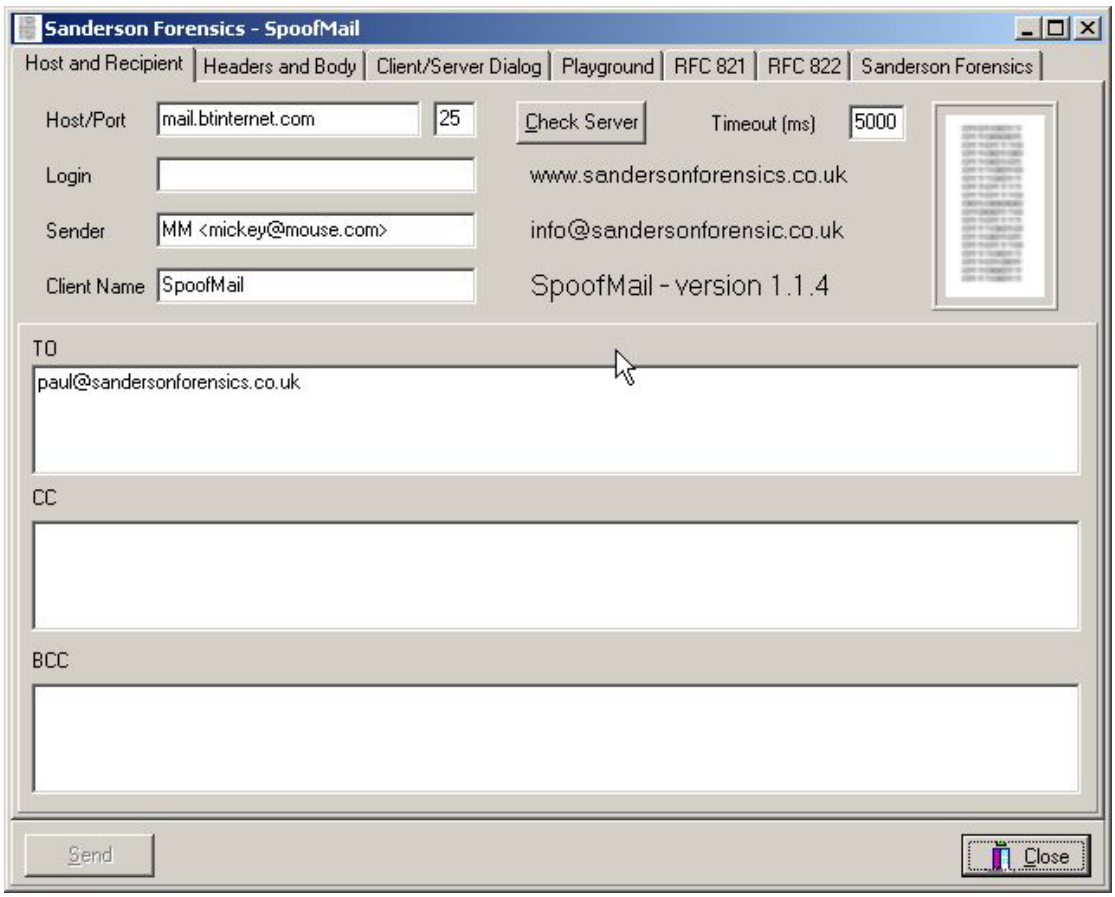
==========

Disclaimer
The contents and the header of this message have been
created by SpoofMail for demonstration/educational purposes
only. Pretty much all of the information in the message
including the header information and in particular the sender
may and probably has been forged.
Want more information? http://www.sandersonforensics.co.uk

==========

Using SpoofMail

When SpoofMail is first run the following dialog is displayed:



The user should insert a valid SMTP client in the Host box, normally this would be the users own SMTP server. The Port box would normally be left at 25 as this is the default port for an SMTP sever to listen on.

The Login box would normally contain the users login name all not all servers require this.

If you have a slow connection or are having connection problems the timeout value can be increased appropriately.

The sender box is the e-mail address of the sender, this should be a valid e-mail address in that it follows the standard for e-mail address i.e. name@domain. The address does not have to exist it just needs to follow the proper form. Examples are:

Sandy771@btopenworld.com
Paul Sanderson <sandy771@btopenworld.com>
sandy771@btopenworld.com Paul Sanderson

Either use SpoofMail for the name of the client or choose another name (remember to check for it in the received headers)

Use the “Check Server” button to validate whether the server selected in the host box has a listening SMTP service on the selected port.

The To, Cc and Bcc boxes can contain t he e-mail addresses of one or more intended recipients. The entries in these boxes can take two forms:

e-mail addresses only - i.e.

paul@sandersonforensics.co.uk
sandy771@btopenworld.com
…

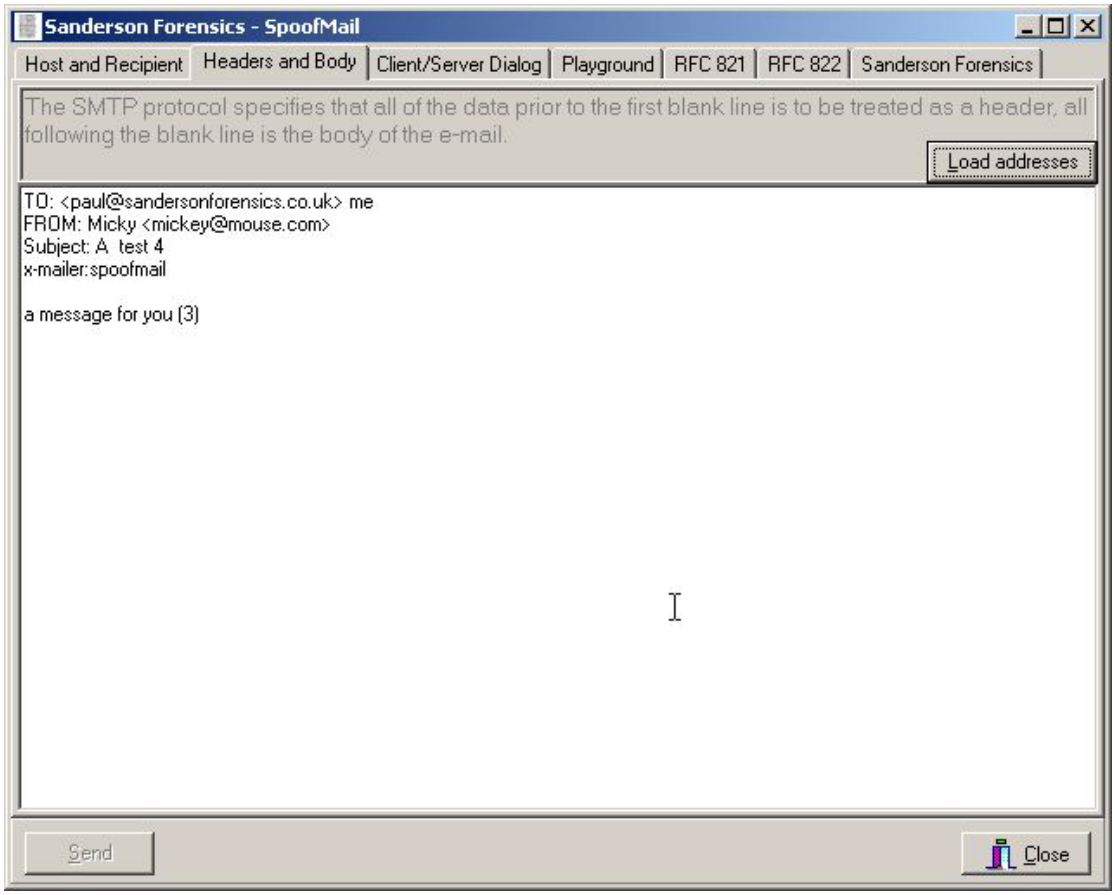
or e-mail address and alias – i.e.
<paul@sandersonforensics.co.uk> Paul Sanderson
<sandy771@btopenworld.com> Sandy Sanderson
…

Not that in this form the e-mail address is contained within angled brackets.

The two forms can also be intermixed – i.e.
<paul@sandersonforensics.co.uk> Paul Sanderson
sandy771@btopenworld.com

The entries on this page **and only** the entries on this page determine who will receive the messages.

Click on the tab for Headers and Body to add and manipulate the same:



The user now gets to add the body of the e-mail and more importantly add and adjust the headers.

The first thing to do is to click on the Load Addresses button at the top left of the screen. This will add headers to the e-mail so that the recipient will see who the message has been sent to and CC'd to. Note that the SMTP protocol uses the To: and CC: header purely for display purposes, then entries here have no effect on who will eventually receive the e-mail – just on what they will see.

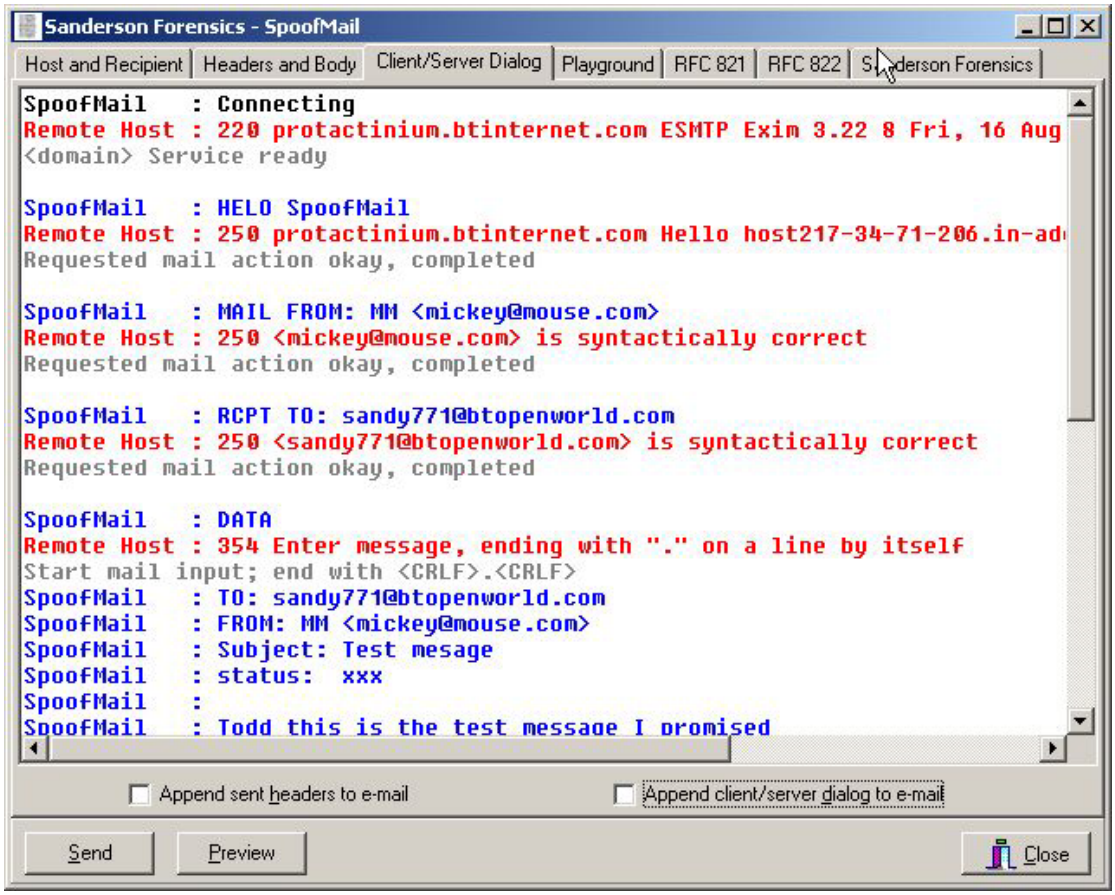
The important this to remember about the specification for the SMTP service (see RFC 821) is that everything up until the first blank line is considered a header, everything after this blank line is considered the body.

Add some additional headers such as Subject:, Message-ID:, Date: (have a look at one of your own messages for ideas), also consider adding Received: headers.

Leave a blank line and add a body to your message.

Now select the Client/server dialog tab

When this tab is selected the Send button is enabled and the user can send his or her message:



SpoofMail will now display the dialog between the SpoofMail client and the SMTP server.

The first message SpoofMail displays is in a black font, this is purely for information and indicates that the SpoofMail client is attempting a TCP connect to the SMTP server designated in the Host box.

The server will respond in text with a banner, this will be displayed in red text. All communication between the client and server from this point forward is text based, in fact a simple Telnet client could be used instead of SpoofMail to achieve exactly the same results.

All communications from the SMTP server to SpoofMail is displayed in a red font. All communication from SpoofMail to the SMTP server is displayed in a blue font. Additional commentary is added by SpoofMail in Grey.

SpoofMail will display the full transaction re the sending of your e-mail in the dialog box.

Note that the SMTP server did not squeak at the invalid e-mail address i.e. the CC:sandy line. This is because the CC line is a header and is purely for information.

The headers for the e-mail sent above are displayed below

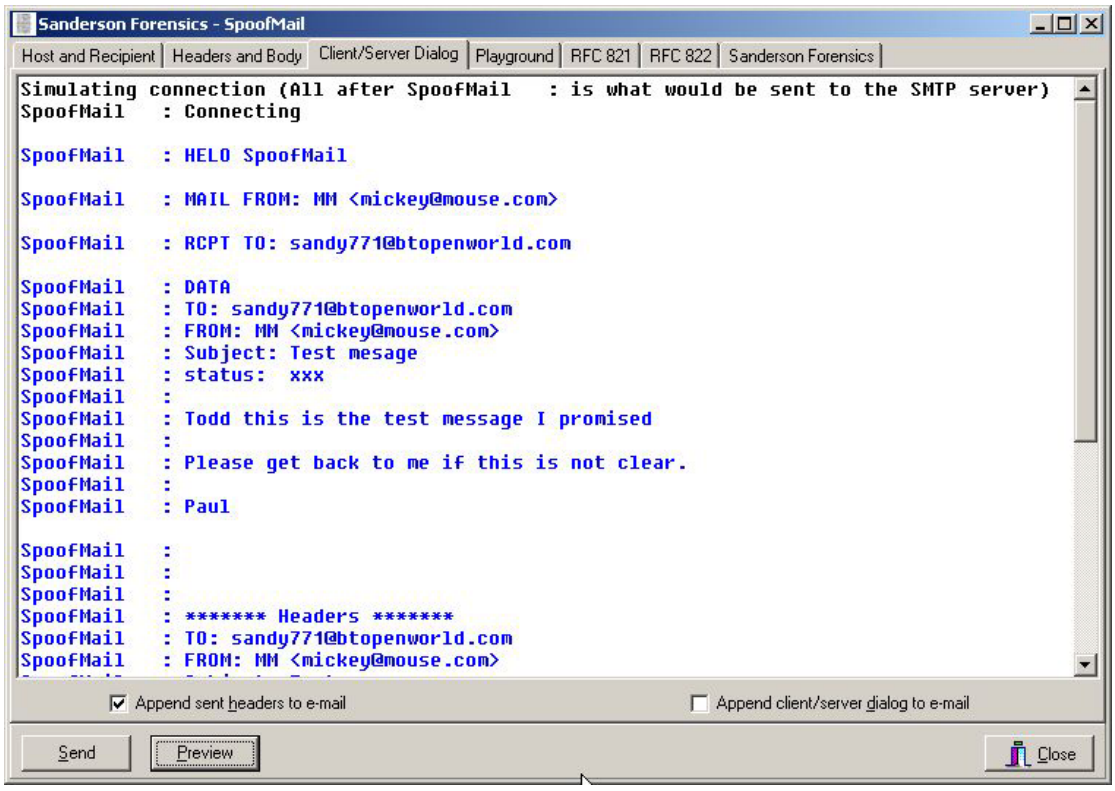
TO: <paul@sandersonforensics.co.uk> me
FROM: Micky <mickey@mouse.com>
Subject: A test 4
x-mailer:spoofmail

a message for you (3)

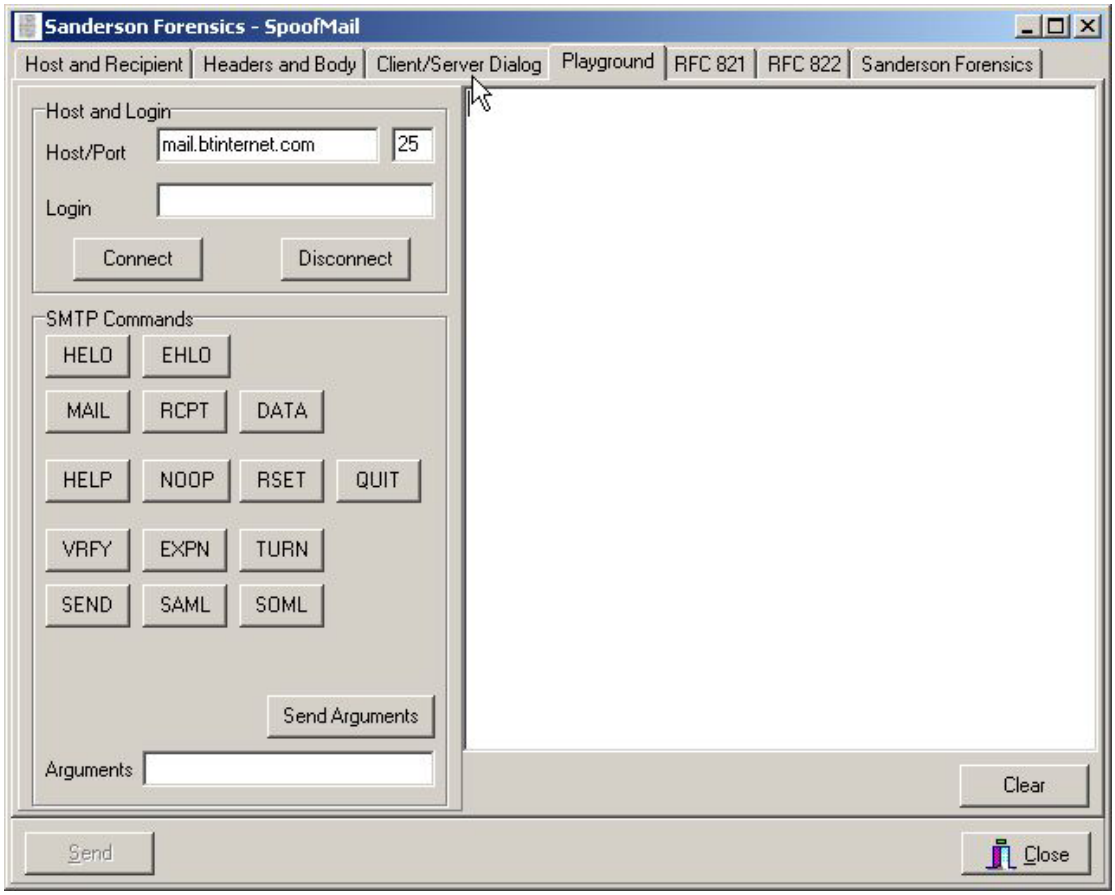
When you receive a test message note the headers that were added by SpoofMail and those that were added by the SMTP servers/receiving client.

The "Appended sent headers to e-mail" checkbox will append the headers from the Headers and body page to the e-mail. The "Append client/server dialog to e-mail" will do the same for any communication between the client and the server.

SpoofMail can also be used to display the commands that would be sent to a server, but without actually sending them. Press the Preview button to see this simulated dialog.



The Playground



The Playgound is an area to send individual commands to an SMTP server. You MUST connect and then the first command would normally be HELO – but try some others and see what happens. I suggest that one of the first commands you run is HELP – this will normally display the commands that are supported by this server.

Some commands require argument – i.e. MAIL needs the senders address, i.e. the return address, the argument should go in the arguments box at the bottom of the screen. To send an argument on its own (i.e. HeLo) use the send arguments button.

Read the RFC's and have a play – see what happens.

Other Tabs

SpoofMail can display the RFC's for the SMTP protocol and the format for internet e-mail as a ready reference, use the tabs as appropriate.

Finally a web browser linked to the Sanderson Forensics web site is presented on the final tab, use this if required to check for upgrades and new tools.

Things to try

Create your own Received headers to make tracing the e-mail more difficult. Look at what is sent by SpoofMail and what is received by the recipient, compare the headers and the order of the headers.

Use a single entry in the To box. In the headers box enter an additional recipient i.e the To: box contains
<Paul@sandersonforensics.co.uk> Paul

The headers section contains
To: <Paul@sandersonforensics.co.uk> Paul, <info@sandersonforensics.co.uk> Info

Watch what is sent in the client/server dialog, look at the genuine received e-mail see who the e-mail is addressed to. Confirm that the second apparent recipient did not receive the message.

Try sending a message with malformed addressees.

If you have legal access to an open relay mail server, try logging on to this rather than your normal mail serve r and send a mail or two – examine the received headers.

Use an alternative Client name for SpoofMail in the Client box and check the received headers.

Change History

Only non-development/debug releases are recorded below:

1.0.1

In Version 1.0.0 the From: header was inserted automatically by SpoofMail – this should have been under the control of the user and now is.

1.1.3

Added playground, RFC displays and Sanderson Forensic web page. Fixed various bugs.

1.1.4

Added option to check that server is accepting connections

Added option for user specified timeout

Force disclaimer when e-mail sent from playground

Fixed various other minor bugs.

1.1.5

Option to append the headers and or the client server dialog to the sent e-mail.

1.1.7

Added option to simulate message and preview dialog

First full release