

SCAMMERS, EMAILS AN EMAIL HEADERS

by the TRANSLATOR SCAMMERS INTELLIGENCE GROUP

www.translator-scammers.com • mail@translator-scammers.com

Last revision: **January 14, 2020**

Circulation: **Worldwide**

Special instructions: **Sharing of this document is appreciated**

The whole scamming operation described in the **TRANSLATOR SCAMMERS DIRECTORY** is based on one thing, and one thing only: an email address (or several email addresses) created and operated by the scammers as their point of contact.

For each CV or identity they hijack, scammers create one fake identity and, you guessed it, one (at least) an email address. Let's see some examples:

Name used by the scammers	Email(s) used by the scammer	Real Translator – Scam Victim
Helen Pollex	helenpollex@gmail.com	Dmytro V. Rachek (Ukraine)
Lee Fuxiang	fuxiang@hotmail.com fuxiangliu6@gmail.com fuxianing.liu@gmail.com lee-fuxiang@hotmail.com leefuxiang2@gmail.com leefuxiang44@gmail.com	Liu Fuxiang (China)
Prema Alexander	prema.alexander@hotmail.com prema.alexander@yahoo.com premaalexander94@gmail.com	Evgueni Terekhin (Russia)

Why two or three email addresses?

Normally, the scammers will create two email addresses for each identity they hijack or create. However, **if the scammer sends his email from a Gmail address, this is probably the only one created/used** for his operation (but not always, as we'll see below). Because their email is usually sent from a Gmail account, scammers close this account (once exposed, or just to bypass spam filters) and create a new Gmail address to send their Hotmail emails (see "*Lee Fuxiang*" above).

But, if the scammers' email is sent from a Hotmail (or other free email account), **the return path of the message is routed to their email address from Gmail.**

Why do they do that? **Simply because the emails sent from Gmail/Outlook will ONLY trace back to Google IP addresses (in the USA), thus making it impossible to geographically locate the scammer. It is also true that all other free email addresses also trace back to the provider's routers.**

Other times, the scammer sends his email from a Gmail account, without a return path to another free email address (Hotmail, etc.). Sometimes, this free email the address is shown on the scammed CV, without any mention to the Gmail address.

Here is how the system works:

Mail sent from	Return path to Gmail	Email(s) shown on CV	Comments
Gmail	Y	Gmail	Very common
Hotmail (or other)	Y	Gmail + Hotmail	Extremely common
Hotmail (or other)	N	Gmail + Hotmail	Very uncommon
Gmail or Hotmail	Y	None	Extremely uncommon

Note: scammers may also use other free email accounts, like live.com, ymail.com, outlook.com, etc.

When their name and emails become known and exposed, scammers close the Gmail account (e.g. leefuxiang2@gmail.com) and create another Gmail address (leefuxiang44@gmail.com) to continue their scamming operation...

CURRICULUM VITAE	
NAME:	Loredana Stefanelli
ADDRESS:	Via Antonio Moscatelli 102 – Mentana (RM)
TELEPHONE NO.:	
E-mail:	loredana.stefanelli@yahoo.com loredana.stefanelli@gmail.com
DATE OF BIRTH:	02/13/1975
STATUS:	single

Typical CV sent by scammers, with 2 email free addresses

For layout reasons, the **TRANSLATOR SCAMMERS DIRECTORY** lists only one email address (usually the one openly visible by the email recipient) for each scammer's name exposed. In a separate file (.TXT format), you may download ALL emails used by the scammers. **This file is constantly updated** and you should check it, if you want to look up a scammer's email address.

[CLICK TO ACCESS ALL THE EMAILS USED BY THE SCAMMERS](#)

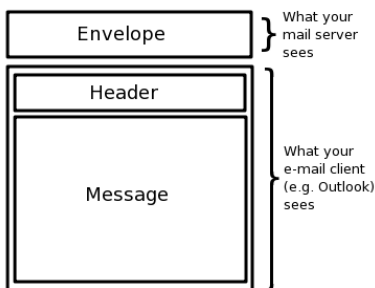
Therefore, to detect and expose both emails addresses used by the scammers (cases highlighted in the table above), and thus harming his operation to the maximum extent possible, **one has to look into the "header" of the email message received from the scammers.**

Newest trend

With their operation now fully uncovered, **scammers are now, more and more, sending their scamming emails from one email address ONLY.** Of course, this email address is ALWAYS a free email account: Gmail, Hotmail, Yahoo, Outlook, etc.

What is the email header?

In an e-mail, the body (content text) is always preceded by header lines that identify particular routing information of the message, including the sender, recipient, date and subject. Some headers are mandatory, such as the FROM, TO and DATE headers. Others are optional, but very commonly used, such as SUBJECT and CC. Other headers include the sending time stamps and the receiving time stamps of all mail transfer agents that have received and sent the message. In other words, any time a message is transferred from one user to another (i.e. when it is sent or forwarded), the message is date/time stamped by a mail transfer agent (MTA) – a computer program or software agent that facilitates the transfer of email message from one computer to another. This date/time stamp, like FROM, TO, and SUBJECT, becomes one of the many headers that precede the body of an email.



Header	Meaning
To:	E-mail address(es) of primary recipient(s)
Cc:	E-mail address(es) of secondary recipient(s)
Bcc:	E-mail address(es) for blind carbon copies
From:	Person or people who created the message
Sender:	E-mail address of the actual sender
Received:	Line added by each transfer agent along the route
Return-Path:	Can be used to identify a path back to the sender

Reading the full email headers

Email headers determine where a message is sent from, and records the specific path the message follows as it passes through each mail server.

To read a message header, **follow the path of a message chronologically, by reading from the bottom of the header, and working your way up.**

Here's an example of a message header for an email sent from **Scammer@free_email.com** to **MrClient@client_company.com**:

Delivered-To: **MrClient@client_company.com**
 Received: by 10.36.81.3 with SMTP id e3cs239nzb; Tue, 29 Mar 2005 15:11:47 -0800 (PST)
 Return-Path:
 Received: from mail.free_email.com (mail.free_email.com [111.111.11.111]) by mx.gmail.com with SMTP id h19si826631rnb.2005.03.29.15.11.46; Tue, 29 Mar 2005 15:11:47 -0800 (PST)
 Message-ID: <20050329231145.62086.mail@mail.free_email.com>
 Received: from [11.11.111.111] by mail.free_email.com via HTTP; Tue, 29 Mar 2005 15:11:45 PST
 Date: Tue, 29 Mar 2005 15:11:45 -0800 (PST)
 From: Scammer
 Subject: Hello
 To: Mr Client

In the example above, headers were added to the message three times:

1. When **Scammer** composes the email:

Date: Tue, 29 Mar 2005 15:11:45 -0800 (PST)
From: Scammer
Subject: Hello
To: Mr Client

2. When the email is sent through the servers of **Scammer's email provider**, mail.free_email.com

Message-ID: <20050329231145.62086.mail@mail.free_email.com>
Received: from [11.11.111.111] by mail.free_email.com via HTTP; Tue, 29 Mar 2005 15:11:45 PST

3. When the message transfers from the **Scammer's email provider** to the **Clients's email address**:

Delivered-To: MrClient@client_company.com
Received: by 10.36.81.3 with SMTP id e3cs239nzb; Tue, 29 Mar 2005 15:11:47 -0800 (PST)
Return-Path: Scammer@free_email.com
Received: from mail.free_email.com (mail.free_email.com [111.111.11.111]) by mx.gmail.com with SMTP id h19si826631rnb; Tue, 29 Mar 2005 15:11:47 -0800 (PST)

Below is a description of each section of the email header:

Delivered-To: MrClient@client_company.com
The email address the message will be delivered to.

Received: by 10.36.81.3 with SMTP id e3cs239nzb;
Tue, 29 Mar 2005 15:11:47 -0800 (PST)
The time the message reached Gmail's servers.

Return-Path: Scammer@free_email.com
The address from which the message was sent.

Received: from mail.free_email.com
(mail.free_email.com [111.111.11.111])
by mx.gmail.com with SMTP id h19si826631rnb.2005.03.29.15.11.46;
Tue, 29 Mar 2005 15:11:47 -0800 (PST)
The message was received from mail.free_email.com, by a Gmail server on March 29, 2005 at approximately 3:11 pm.

Message-ID: 20050329231145.62086.mail@mail.free_email.com
A unique number assigned by mail.free_email.com to identify the message.

Received: from [11.11.111.111] by mail.free_email.com via HTTP;
Tue, 29 Mar 2005 15:11:45 PST
The Scammer used an email composition program to write the message, and it was then received by the email servers of mail.free_email.com. The sender's IP address is [11.11.111.111]

Date: Tue, 29 Mar 2005 15:11:45 -0800 (PST)
From: Scammer
Subject: Hello
To: Mr Client
Date, sender, subject, and destination – the Scammer entered this information (except for the date) when the email was composed.

Analyzing the scammer's email headers

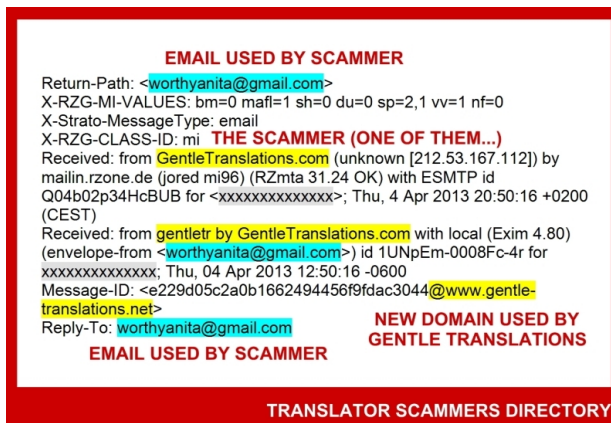
The image below shows the email header of a message sent by a scammer called "Tomas Skold" routed (not sent) from his email account **TomasGSkold@hotmail.com**. The actual sending account was his Gmail account: **tomasgskold@gmail.com**.

```
MIME-Version: 1.0
X-Received: by 10.194.123.227 with SMTP id md3mr13096412wjb.17.1378738531355;
Mon, 09 Sep 2013 07:55:31 -0700 (PDT)
Reply-To: TomasGSkold@hotmail.com
Sender: tomasgskold@gmail.com
Received: by 10.195.12.137 with HTTP; Mon, 9 Sep 2013 07:55:30 -0700 (PDT)
In-Reply-To: <CAH8hVZDmtgX7E0f9-7wKfWdo9+Zi2EZPUAQoFEQgzxHwX-5Cg@mail.gmail.com>
References: <CAH8hVZDmtgX7E0f9-7wKfWdo9+Zi2EZPUAQoFEQgzxHwX-5Cg@mail.gmail.com>
Date: Mon, 9 Sep 2013 16:55:30 +0200
X-Google-Sender-Auth: i96HoZitZbgT3p1R8cqVmkQQ6M
Message-ID: <CAH8hVZDeaatTPNwuyrBuwu164W15CNV-H0PMxkv683B0NPw07Q@mail.gmail.com>
Subject: Fwd: English <>German Translator
From: Tomas Skold <TomasGSkold@hotmail.com>
To: undisclosed-recipients;
Content-Type: multipart/mixed; boundary=089e01229a58666a1c04e5f49440
Bcc:
X-Antivirus: AVG for E-mail 2013.0.3392 [3222/6649]
X-AVG-ID: ID582EE1B4-IDC08F5C
```

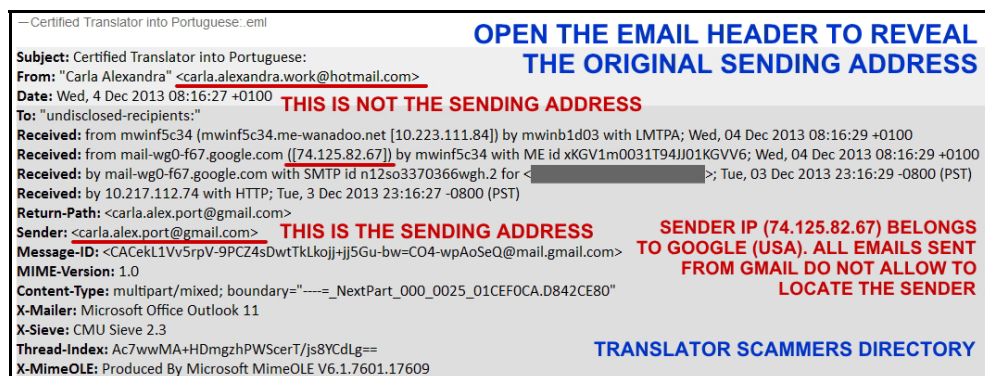
TRANSLATOR SCAMMERS DIRECTORY

But, unless we open the email header, we do not see this information, but only the *From field: Tomas Skold <tomasGSkold@hotmail.com>*. In other words, we would miss the most important email address used by the scammer: his Gmail address used to send the fake CVs.

Sometimes, the email header can also reveal other important information. In the case below, we can see that mail sent from a *Anita Worthy* using the Gmail address *worthyanita@gmail.com* was, in fact, sent by the infamous scammers' joint called *Gentle Translations*:



Below, is another example of an email header with the sending email address exposed. A scammer called "*Carla Alexandra*" routed (not sent) her email account *carla.alexandra.work@hotmail.com* from "her" Gmail address: *carla.alex.port@gmail.com*.

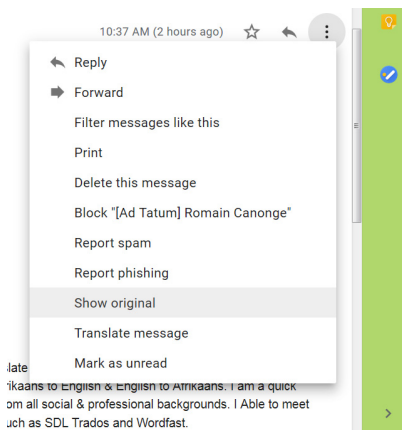


Opening the email headers

It depends on the email client (program) you're using. Below, we have listed the instructions for the most common email clients. If you use another program to send/receive your electronic mail, you may have to find the instructions on Google or by contacting the developers of the program.

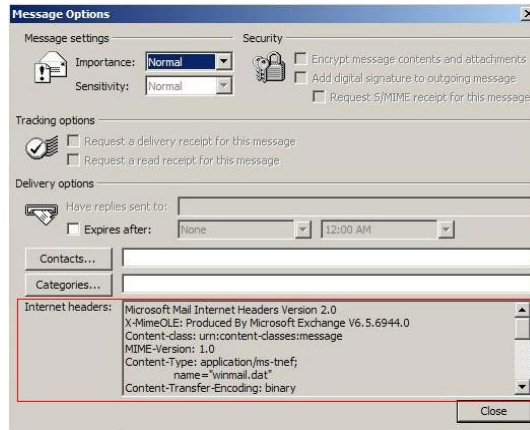
Gmail

1. To begin, open the email message in a new window by double-clicking on it.
2. On this new window menu, click on the **Circle with the 3 Dots**, and on the dropdown menu click on "Show original".
3. The full headers will appear in a new window, simply right-click inside the headers and choose Select All, then right-click again and choose Copy.



Outlook 2003

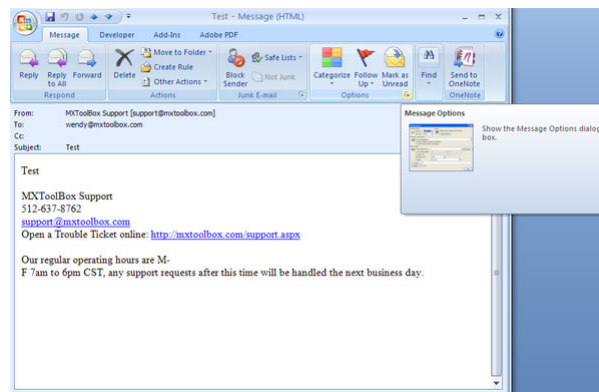
1. To begin, open the email message in a new window by double-clicking on it.
2. On this new window menu, go to View -> Options. If you do not see options, you may have to reveal it by clicking on the two down arrows at the bottom of the menu.



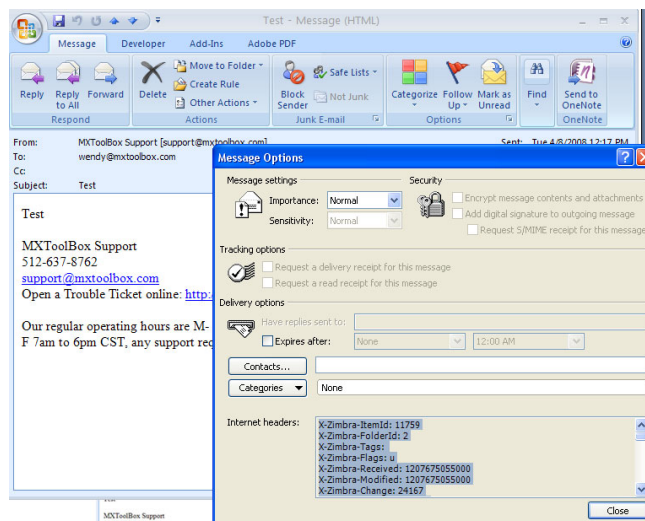
3. This will have brought up the Message Options window. The last component of this is the Internet Headers. Right-click inside the headers and choose Select All, then right-click again and choose Copy.
4. Close the Message Options window.

Outlook 2007

1. Double click on the email message so that it is opened in its own window. If you are new to Outlook 2007, you will be working on what is called the Ribbon. This is a series of tabs across the top of the message, Message, Developer etc.
2. On the Message tab, in the Options section there is a little button with an arrow in it. Click on it and you have the message options menu with the internet headers in the bottom section.



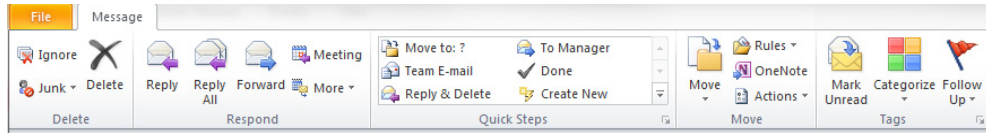
3. This will have brought up the Message Options window. The last component of this is the Internet Headers.
4. Right-click inside the headers and choose Select All, then right-click again and choose Copy.



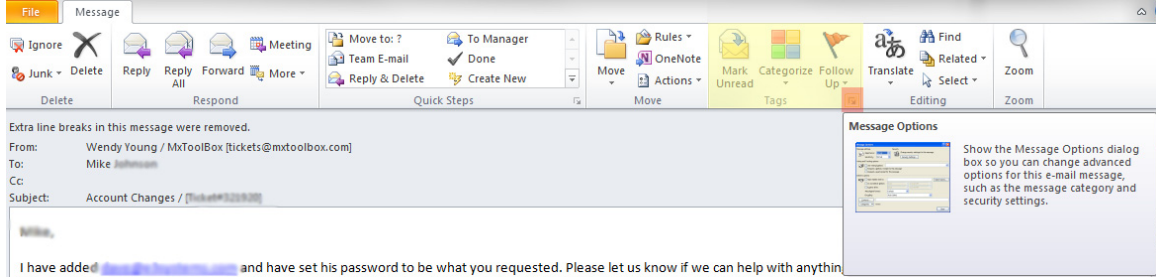
5. Close the Message Options window.

Outlook 2010

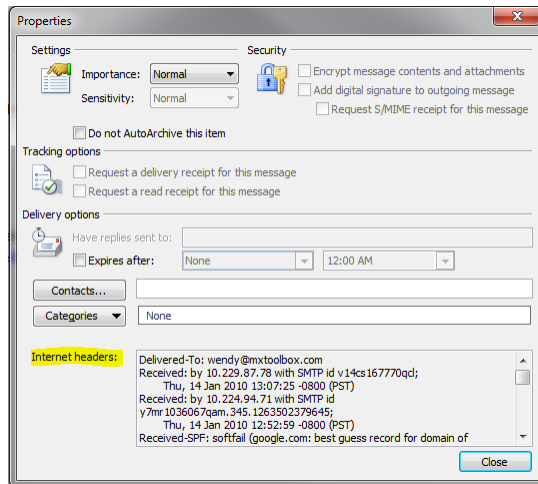
1. Double click on the email message so that it is opened in its own window.



2. On the Message tab, in the Options section there is a little button with an arrow in it. Click on it and you have the message options menu with the internet headers in the bottom section.



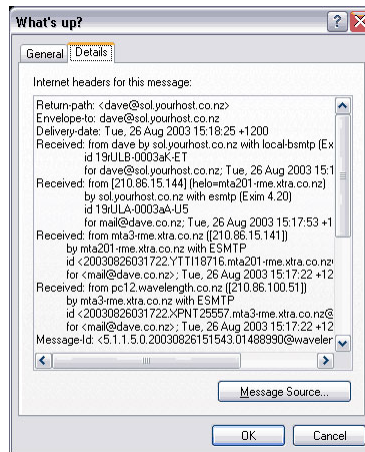
3. This will bring up the Message Options window. The last component of this is the Internet Headers.



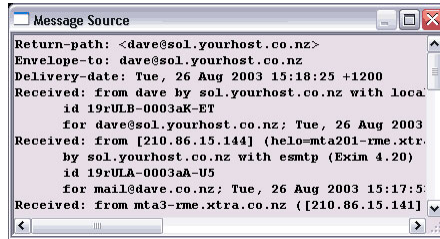
4. Right-click inside the headers and choose Select All, then right-click again and choose Copy.
5. Close the Message Options window.

Outlook Express

1. To begin, open the email message in a new window by double-clicking on it.
2. From the File menu, click Properties.
3. Click the Details tab.



4. Click Message Source. A new window will open containing all the headers and original message:



5. Right-click anywhere inside this window and choose Select All.
6. Right-click again and choose Copy.
7. Close this window, the details window and the message window (so you are back to the main Outlook Express program).

Outlook 97

To view headers in Outlook 97, it may require the update: [Internet Mail Enhancement Patch](#)

1. If you already have the update or just installed it, open any message and look for Internet headers on the Options tab. If you don't see the Options tab, choose View | Message Header to display it.

Outlook 98

1. Open the message you'd like to view headers for.
2. Click Options from the drop-down menus.
3. Near the bottom of the screen you'll see a section titled Internet Headers.
4. Right-click inside the headers and choose Select All, then right-click again and choose Copy.
5. Close the Message Source box.

Outlook 2000

1. Open the message you'd like to view headers for.
2. Select Options, then Full Headers.
3. Right-click inside the headers and choose Select All, then right-click again and choose Copy.
4. Close the Message Source box.

Outlook 2002

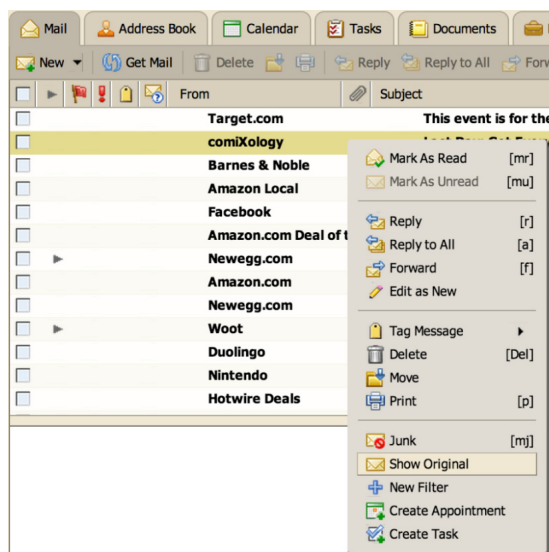
1. Open the message you'd like to view headers for.
2. Click Options from the drop-down menu.
3. A box called Message Options pops up.
4. Near the bottom of the box you'll see a text area titled Internet headers.
5. Right-click inside the headers and choose Select All, then right-click again and choose Copy.
6. Close the Message Source box.

Exchange/Microsoft

1. Click the "File" menu
2. Click "Properties"
3. Click the "Details" tab
4. Click "Message Source"
5. Highlight, copy and paste everything in the "Message Source" windows

Zimbra

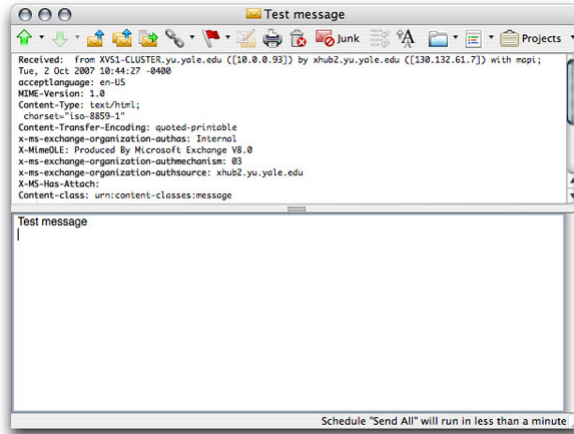
1. Right click the desired message and select Show Original



2. This will open a new window with the source headers.

Entourage

1. To begin, open the email message in a new window by double-clicking on it.
2. Choose View > Internet Headers.



3. Click inside the new box that appears in your message and choose Edit > Select All.
4. Click inside the box again and choose Edit > Copy.

Mac OS X Mail

1. To begin, open the email message in a new window by double-clicking on it.
2. View > Message > Raw Source



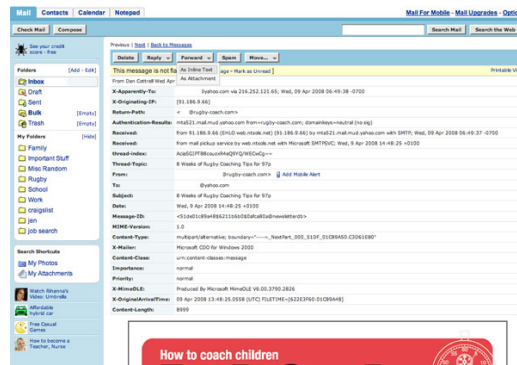
3. Copy the headers by right clicking, selecting all and then choosing copy.
4. Close the Message Source box.

Outlook Express for Macintosh

1. Select the email.
2. Choose View and then choose Source.
3. A new window will appear containing the email with full headers.
4. Press command + A, to select all, then command + C to copy.

Yahoo!

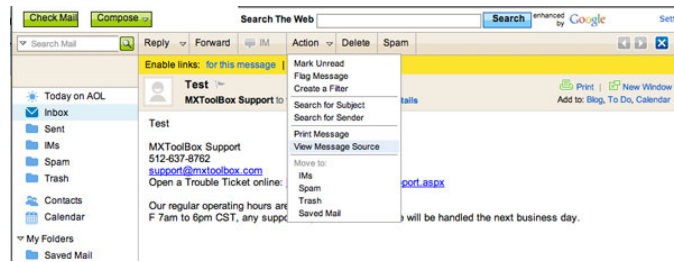
1. Go to Options > General Preferences
2. Under Mail Viewing Preferences, go to Message Headers, then select ALL.
3. Hit the small down arrow next to Forward and choose As Inline Text



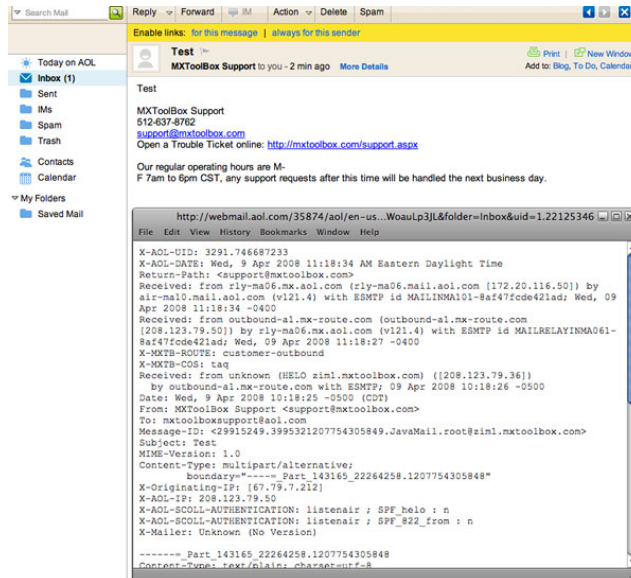
AOL

The email files are in an html format. The objective is to save the file in html format. This can be done as follows:

1. To begin, open the email message by clicking on it.
2. Click on Details (right above the To: and From: fields) and choose View Message Source.



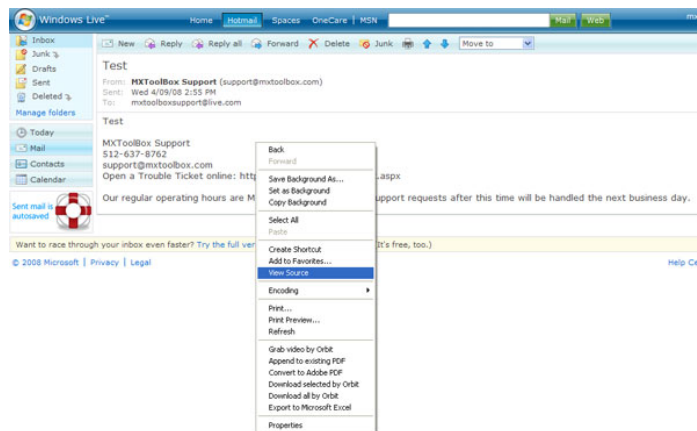
3. The full headers will appear in a new window, simply right-click inside the headers and choose Select All, then right-click again and choose Copy.



4. Close the Message Source box.


Hotmail

1. In the left pane, click Mail.
2. In the Folders list, click Inbox.
3. Once in the Inbox, click on the message that you are getting the headers for.
4. Right-click the message in the message list, and then click View source.



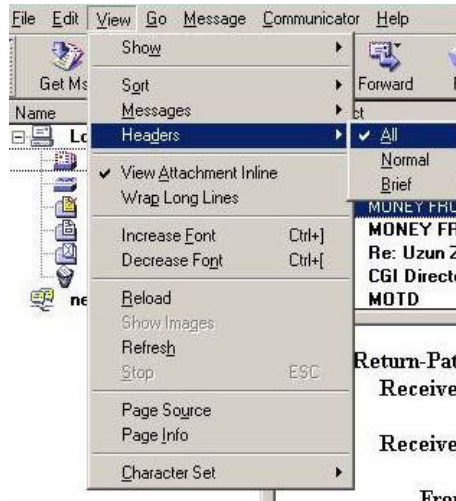
5. The full headers will appear in a new window, simply right-click inside the headers and choose Select All, then right-click again and choose Copy.
6. Close the Message Source box.

Eudora

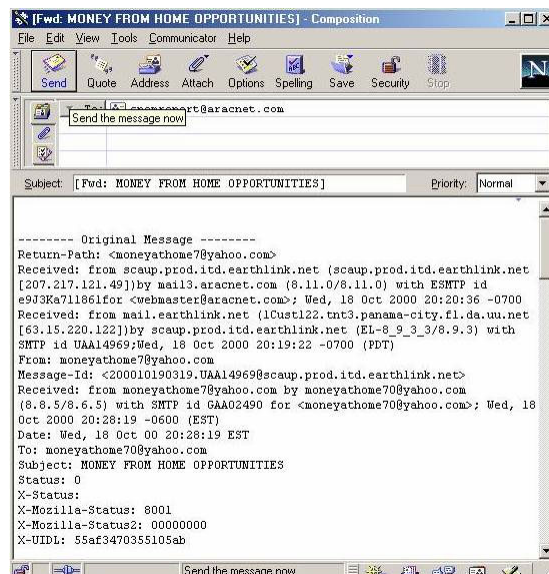
1. To begin, open the email message in a new window by double-clicking on it.
2. Click on the tool bar icon labeled blah, blah, blah. 
3. Copy the headers by right clicking, selecting all and then choosing copy.
4. Choose Edit > Copy.
5. Close the Message Source box.

Netscape, Mozilla or Thunderbird

1. To begin, open the email message in a new window by double-clicking on it.
2. Choose View > Headers > All



3. This will expand the top of your email message and it will now include the full headers.



Lotus Notes

Lotus Notes v.4.x

1. Look for the first line that begins with "Received". There should be a blank line just above it.
2. Then, scroll down to the next blank line. The data in-between the two blank lines are the headers you need.

Lotus Notes v.5.x

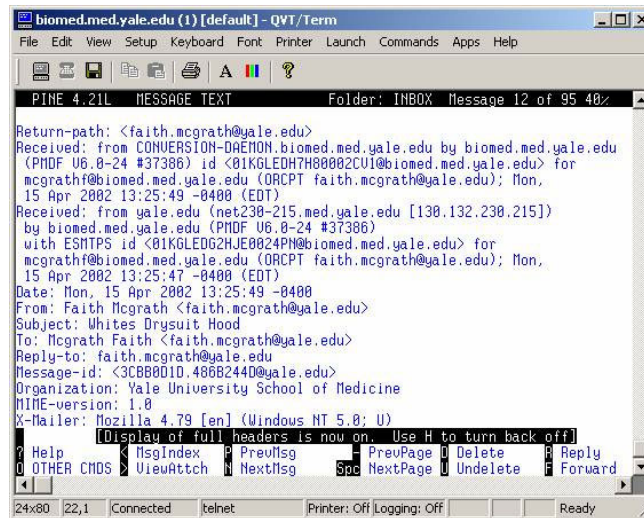
1. Open your inbox
2. Highlight the message that you wish to get header information for.
3. Choose File -> Export...
4. Type in a filename, leave the type as "Structured Text" and click Export
5. From the Dialog Box that comes up, choose "Selected Documents" and click OK
6. Now you can open that message you saved in WordPad and Cut and Paste it.

Pine

You must configure Pine to allow showing message headers. You may skip steps 1-6 below if you have performed this configuration.

1. Press the h key while viewing the message to show full headers. If this returns the error Command h not defined for this screen, do the following:
2. Go to the Pine start up screen.

3. Hit s for Setup.
4. Hit c for Config.
5. Scroll down to the section labeled Advanced Command Preferences.
6. Put an x for the enable-full-header-cmd feature.
7. Type E to exit Config, and Y to save changes.
8. The next time you read a message, type H and the full headers will be displayed at the top of the message. Type H again to hide the headers.



XtraMail

1. Log into XtraMail
2. Click on "Options" in the left-hand navigation bar.
3. Click the "Display" button.
4. Change the Message Headers option to "Full".
5. Click the OK button to confirm.

Pegasus Mail

1. In the New Mail or other folder window:
2. Right click the message, and select Message Properties.
3. In the right hand column uncheck the box beside Contains HTML data.
4. Click OK. That should allow you to see the message as a text message only.
5. Click Ctrl-H to bring up the full headers.

Claris Emailer

Version 2.0 and higher:

1. Use the "Show Long Headers" option in the "Mail" menu while you have the message open.

Versions earlier than 2.0:

1. Click the blue triangle near the "from" information to show additional message information
2. Click the "Show Original Headers..." button to bring up the full header info.

Mail Warrior

1. When viewing the message, click File, then Save Message As.
2. A standard save window will appear.
3. Save the message as a .txt file (document.txt).
4. Open the file you created, select all (ctrl-A) and copy (ctrl-c).
5. And paste (ctrl-v).

Juno Version 4+

1. On the drop down menu "Options"
2. Choose "Email Options" (press ctrl-E)
3. Under "Show Message Headers", select the "full" option.
4. Click the OK button to save the setting. Juno version 4+ can display MIME and HTML email, but does not provide a way of viewing the HTML Source for the message within Juno.

Novell GroupWise

1. Open the message
2. In the message window select: File > Attachments > View
3. Select the Mime.822 attachment

VERY IMPORTANT

To allow a more effective exposure of the scammers (i.e., all emails addresses they use) open the header of their email messages before you forwarding them to us.

Note about Gmail email addresses

Gmail doesn't recognize dots as characters within usernames, you can add or remove the dots from a Gmail address without changing the actual destination address; they'll all go to your inbox, and only yours. Gmail addresses are also NOT case sensitive. In short:

fake.translator.cv@gmail.com		THE SAME AS faketranslatorcv@gmail.com
fake.tran.slat.or.cv@gmail.com		
FAKETRANSLATORCV@gmail.com		

Free email accounts frequently used by the scammers

For their scamming of legitimate translators' CVs, besides the mail servers associated with their domains (e.g., languagemet.com and translationsecrets.com) use ONLY FREE EMAIL ACCOUNTS. When asked about the use of Gmail for their scamming business, scammers promptly deny it, claiming that they send mail only from their domains. This is, obviously, a blunt lie: LanguageMet, for instance, is known to use, at least, 26 Gmail addresses (e.g., languagemet32@gmail.com or languagemet74@gmail.com) and, at least, 25 addresses from their languagemet.com domain.

Because Gmail ONLY traces back to Google IP addresses (in the USA), thus making it impossible to geographically locate the sender, this is the choice platform for the scammers.

But, in their operation, they also use other email accounts:

att.net	outlook.sa
gmail.com	rocketmail.com
gmx.co.uk	windowlive.com
gmx.com	yahoo.co.in
hotmail.com	yahoo.co.uk
hotmail.es	yahoo.com
live.com	yahoo.fr
outlook.com	ymail.com

TRANSLATOR SCAMMERS DIRECTORY

by the TRANSLATOR SCAMMERS INTELLIGENCE GROUP

translator-scammers.com | translator.scammers@gmail.com | mail@translator-scammers.com