

How to get email headers



Sri Lanka Computer Emergency Readiness Team | Coordination Center

The following guide will provide instructions on how to extract headers from various email clients and programs.

Index

- 1. Outlook**
 - 1.1 Outlook Express 4, 5 and 6..... 5
 - 1.2 Outlook 98, Outlook 2000, Outlook 2003..... 6
 - 1.3 Outlook 2007 7
 - 1.4 Outlook Express for Macintosh 7
 - 1.5 Outlook Web Access (OWA)..... 7

- 2. Microsoft Exchange 8**

- 3. Hotmail 9**

- 4. Gmail.....10**

- 5. Yahoo Mail11**

- 6. Evolution12**

- 7. AOL13**

- 8. Thunderbird14**

- 9. XtraMail.....15**

- 10. Microsoft Entourage (Office X for Mac)16**

- 11. Eudora17**
 - 11.1 Eudora for Mac.....17
 - 11.2 Eudora for the PC - non-HTML mail.....17
 - 11.3 Eudora for the PC - HTML mail.....17

- 12. Lotus Notes v.5.x (easier method)**
 - 12.1 Lotus Notes (v.4.x and v.5.x)19
 - 12.2 Lotus Notes v.4.x.....19
 - 12.3 Lotus Notes v.5.x.....19
 - 12.4 Lotus Notes v.5.x (easier method)19

13. Pegasus Mail	20
14. Claris EMailer	
14.1 Version 2.0 and higher	21
14.2 Versions earlier than 2.0	21
15. kmail (KDE Desktop)	22
16. GNU/ Emacs integrated email	23
17. Juno Version 4+	24
18. The Bat!	25
18.1 For The Bat! v1.53bis	25
19. Novell GroupWise	26
20. Fort Agent	
20.1 Fort Agent versions 1.5 to 1.8	27
21. Sylpheed	28
22. Excite web-mail	29
23. Netscape Webmail	30
24. Blitzmail	31
25. Operamail	32
26. GNU/Emacs integrated email	33
27. Pegasus Mail	34
28. Mac Mail (OS X Mail)	35
29. Microsoft Entourage	36

1. Outlook

1.1 Outlook Express 4, 5 and 6

- Start by opening the message in its own window (or when viewing the message in the preview pane).

Then, With the keyboard:

- CTRL & F3 (Message Source Window)
- CTRL & A (select all)
- CTRL & C (copy)
- ALT & F4 (close)

With the mouse:

- Click the "File" menu
- Click "Properties"
- Click the "Details" tab
- Click "Message Source"
- Highlight, copy and paste everything from this window (Ctrl-A, Ctrl-C)

With viruses, worms and Trojans being spread via email, many users now work with the preview screen in Outlook Express turned off. Viewing the contents of email in the preview screen is no different than opening the message. If the email has malicious content, it may execute in the preview screen. The following is instructions to obtain the full message source if you have the preview panel turned off:

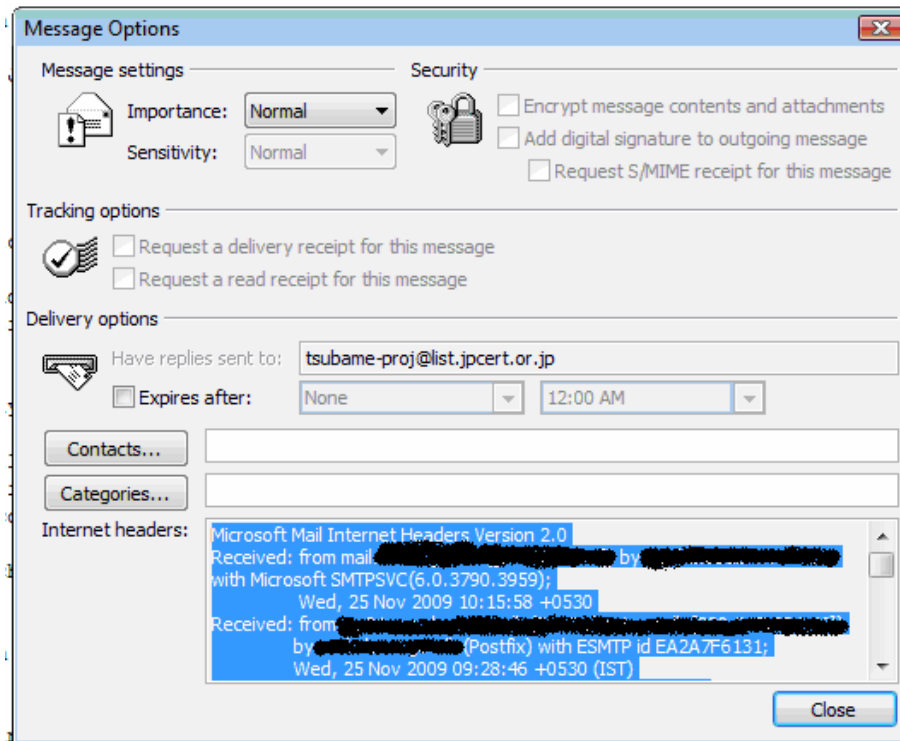
Using the keyboard:

- Highlight the message in the folder
- Press alt & enter - this will open a message information window
- Press Ctrl & Tab - this changes to the "Details" tab
- Press Alt & m - the opens the message source
- Press Ctrl & a - to select all the text
- Press Ctrl & c - to copy the selected text to the clipboard
- Press Alt & F4 - to close the message source window
- Press the Esc key - to close the information window

Outlook 97Microsoft Outlook 97 may require an update called the Internet Mail Enhancement Patch in order to display the email headers.

1.2 Outlook 98, Outlook 2000, Outlook 2003

- Open the message in a separate window (double click).
- Under the View menu select Options.
- Copy the text in the Internet Headers window (unfortunately it doesn't include the message itself).



- Paste it on WordPad or Notepad for your ease reference.

1.3 Outlook 2007

- In Outlook 2007 you can view the headers without opening the message. Just right click on the email message in your Inbox and choose Message Options. This will show you the headers.

Or

- Open the email message by double clicking on it.
- Outlook 2007 has a new ribbon user interface. Look at the right of Options and you will see an arrow.
- Click on the arrow and in the bottom section there is the message options menu with internet headers.
- This will show you the email headers.

1.4 Outlook Express for Macintosh

- Select the email.
- From the View menu, choose Source.
- A new window will appear containing the email with full headers.
- Press command + a, to select all, then command + c to copy.

1.5 Outlook Web Access (OWA)

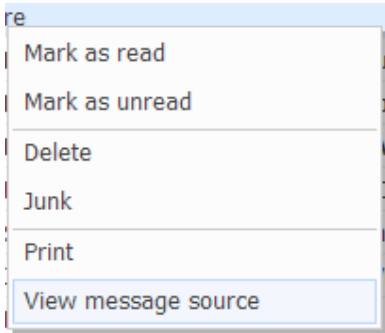
- Left click on the letter you want to open and click on properties.
- When that opens click on the details tab.
- Then on message source.
- This will open the email so the full headers will be available for viewing
- Select and copy the text then paste it.

2. Microsoft Exchange

- Click the "File" menu
- Click "Properties"
- Click the "Details" tab
- Click "Message Source"
- Highlight, copy and paste everything from the "Message Source" window (Ctrl-A, Ctrl-C)

3. Hotmail

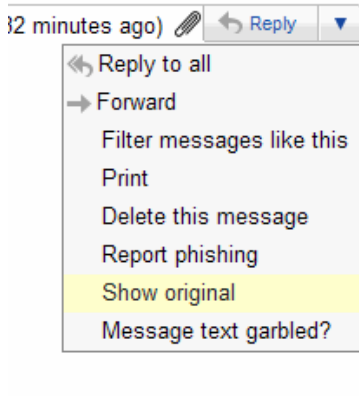
- Log into Hotmail.
- To view the full email message header, right click the email message displayed in your list of messages.
- A menu will pop-up. Click on the View source option in this menu.



- A new window will open. This window will display the full email headers.

4. Gmail

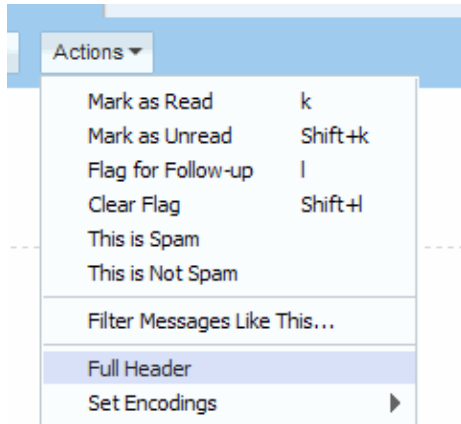
- Log into your Gmail Account
- open the Email whose headers you want to view
- Click on the more options link in the message next to the date of the email. If the link says hide options then do not worry u have already clicked on the more options link.
- Now click the link called show original.



- This will bring up a new window with headers and the body of the message.
- You may copy the headers and use my IP address detection script to ease the process.
Or
- if you want to manually find the IP address, look for
Received: from followed by the IP address between square brackets [].
Eg: Received: from [69.138.30.1] by web31804.mail.mud.yahoo.com.
- If you find more than one Received: from patterns, select the last one.
- Track the IP address of the sender.

5. Yahoo Mail

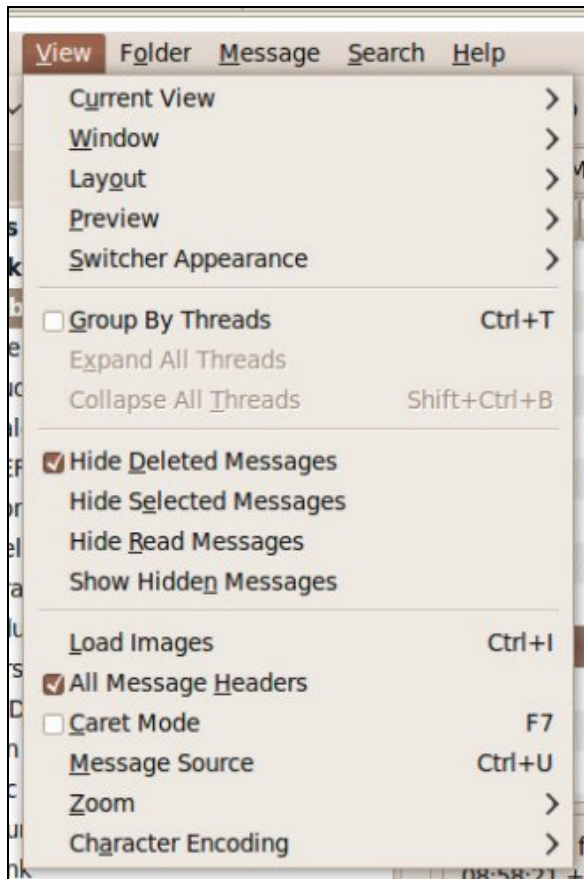
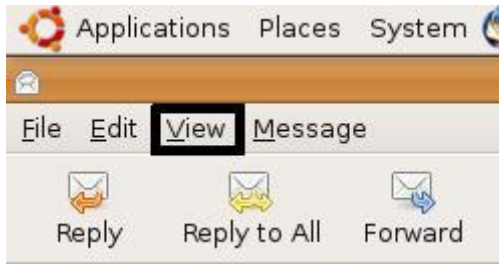
- Log into your Yahoo! Mail account.
- Click on the email and open it
- Click on Actions > Full Header



- Once you click on "Full Header" the header will show on a separate window.
- Look for Received: from followed by the IP address between square brackets []. That is be the IP address of the sender.
- If there are many instances of Received: from with the IP address, select the IP address in the last pattern.
- If there are no instances of Received: from with the IP address, select the first IP address in X-Originating-IP.
- Track the IP address of the sender

6. Evolution

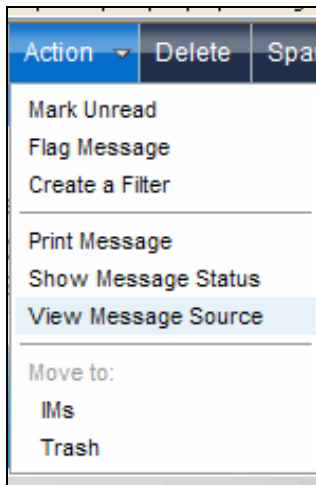
- Double click open the e-mail
- Select “All Message Headers” from the “View” menu.



7. AOL Mail

If the email is sent from anywhere OTHER than AOL, and you are receiving it in AOL, then open the email you want to trace, or have your client open the email, and look for the link Details. This link is usually just below the To: email in the email message. If the email is sent from an AOL user to another AOL user then our Reverse AOL Screen name search can get you the sender's information.

- Open the message
- Select "Actions" > "View Message Source"



- Once you click on "View Message Source" the header will show on a separate window.
- Look for Received: from followed by the IP address between square brackets []. That is be the IP address of the sender.
- If there are many instances of Received: from with the IP address, select the IP address in the last.
- Track the IP address of the sender

8. Thunderbird

(Firefox - Mozilla) To view email headers,

Go to "View" > "Headers" and select "All" to view email headers.

9. XtraMail

- Log into XtraMail
- Click on "Options" in the Left-hand navigation bar.
- Click the "Display" button.
- Change the "Message Headers" option to "Full".
- Click the "OK" button.

10. Microsoft Entourage (Office X for Mac)

- After clicking on the message, select "Source" from the View menu
- A new window will open showing the full message source with complete headers.
- Copy and paste

– Mac OS X

- Select a message
- Select menu item Message, Show, Raw Source.
- Click on the resulting text
- Click Edit, Select All, then Edit, Copy
- Paste Netscape Preferred method:
- Click on the "View" menu,
- then "Page Source," (ctrl-U in windows, meta-U in UNIX, ?-U on the Mac) then copy the contents of the window (Ctrl-A, Ctrl-C windows).

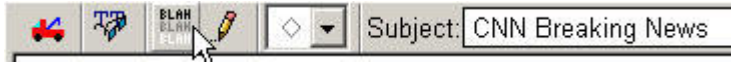
Old versions:

- Click on the "View" > "Headers" > "All."

Note: This method will not work correctly with HTML.

11. Eudora

- Open the message so you can see it on your screen.
- Click on the "Blah Blah Blah" when reading the message.



- Highlight and copy the Full Headers

11.1 Eudora for Mac:

- Open the email and click the button on the upper left hand corner of the message. This shows the extended headers.
- Select the whole message including headers and paste. Eudora for the PC - there are 2 slightly different methods depending on whether the mail contains HTML or not. In any case, to prepare for HTML email, you should turn off the use of Microsoft's HTML viewer.

To do so, click Tools, then Options, then Viewing Mail. Uncheck the box labeled "Use Microsoft's viewer." How to know if it's HTML mail: once you have opened the email, look near the bottom of the headers (see below for revealing headers) for a line like the following: Content-Type: text/html ... you can frequently spot HTML email because it has font effects, pictures, etc but this is not always true so you have to take a quick look at the headers.

11.2 Eudora for the PC - non-HTML mail:

- Open the email by double clicking on the subject line. Click the button to reveal the headers.
- Place your cursor anywhere in the body of the email and select the entire message (Edit/Select All or Ctrl-A)
- Copy the entire email (right click and click copy OR Ctrl/C OR Edit/Copy)
- Paste (right click/paste or Ctrl/V).

11.3 Eudora for the PC - HTML mail:

- Open the email and click the button to reveal the headers.
- Highlight the headers only. Copy and paste the headers.
- Hit enter twice after the pasted headers to force a blank line after the headers.
- Back in Eudora window, place your cursor anywhere in the body of the message and right click and click "view source". A new window will open.

- In the new window, select all (as above) and copy the contents of the new window.
- Paste
- Pine If the feature is enabled, you simply press "H" to toggle full headers. If the feature is not enabled, you must enable it first: From the main menu, press (S)etup, (C)onfig. Scroll down about 40 lines to the option labeled "enable-full-header-cmd." Press [ENTER]. Press (E)xit, (Y)es - to save. Then you can return to the message window and use "H" to display the headers.

12. Lotus Notes

12.1 Lotus Notes (v.4.x and v.5.x)

Open the email,

Click on "Actions" then on "Delivery Information."

Next, you have to pick out the internet-style mail header information from the window that appears when you select Delivery Information.

12.2 Lotus Notes v.4.x

Look for the first line that begins with "Received". There should be a blank line just above it.

Then, scroll down to the next blank line.

The stuff in-between the two blank lines are the headers you need.

12.3 Lotus Notes v.5.x

Look for the separator line that reads ----- Additional Header ----- . Select everything from there down to the next separator line, usually ----- Routing Information ----- . The stuff in between the two separator lines are the headers you need.

12.4 Lotus Notes v.5.x (easier method)

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

13. Pegasus Mail

In the New Mail or other folder window:

- Right click the message, and select Message Properties.
- In the right hand column uncheck the box beside Contains HTML data.
- Click OK. That should allow you to see the message as a text message only.
- Click Ctrl-H to bring up the full headers.
- Another way:
- Highlight the HTML in the new mail folder
- Open a new email message
- Drag the HTML onto the new message
- In the dialog that appears select "Show All Headers"
- Highlight the entire message, then copy to clipboard
- Paste

14. Claris EMailer

14.1 Version 2.0 and higher

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

14.2 Versions earlier than 2.0

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

15. kmail (KDE Desktop)

In the KDE Mail Client that comes with the KDE desktop for Linux,
Select Message > View Source.

Copy and paste the text from the "Message as Plain Text" window.

16. GNU/ Emacs integrated email

- Press the keys 'W', then 'v' in the summary or mail buffer.
- Another method of temporarily switching to ALL headers is by pressing "Ctrl-u g" on the article in the summary buffer.
- Mail WarriorTo get full "message source"
- When viewing the message, click File, then Save Message As.
- A standard save window will appear.
- Save the message as a .txt file (document.txt).
- Open the file you created, select all (ctrl-A) and copy (ctrl-c).
- And paste (ctrl-v). These instructions written for v.3.5

17. Juno Version 4+

- On the drop down menu "Options", choose "Email Options... (press ctrl-E)
- Under "Show Message Headers", select the "full" option.
- 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. To get the full source, including HTML codes:

- In the Juno mail client, click "file" and then "Save Message as Text File...(ctrl-T).
- Give the file a name which you will remember (many people save temporary files to the desktop).
- Double-click on the resulting file and then cut-and-paste the contents.
- MuttTo get mutt (the mail user agent) to forward the full headers (not display them for viewing), use the command "unset forward decode" in your rc file or directly in the command interface.

18. The Bat!

To get the full text of an HTML message from TheBat email software in preparation for pasting it:-

- Message -> Save As -> Save as Type - I - Select Unix Mailboxes[* .mbx] - Open the file in your preferred editor, then simply cut and paste.

18.1 For The Bat! v1.53bis:

- Select the message
- Click on the "Messages" menu - Select "View Source" - Alternatively, you may push F9 instead of the last two steps. Pronto mail (GTK/UNIX)
- Click "Message", then "View Source"
- Highlight the message source as normal with the mouse
- Copy using Control + C
- Paste StarOffice
- Right click on the container name in the explorer panel (either a top-level mail box or a specific mail folder).
- Select the Properties item from the pop-up menu.
- In the properties notebook, select the Headers tab.
- Click the "All" button on the right.
- Press "OK" and you're done, the complete header is available in the header panel and can be selected/pasted.

19. Novell GroupWise

- Open the message
- In the message window select: File > Attachments > View
- Select the Mime.822 attachment BlitzmailWith the message open, go to the Options menu and choose Verbose Header. This will put the full header inside the upper pane of the message's window.

20. Fort Agent

20.1 Fort Agent versions 1.5 to 1.8:

- Press CTRL-R to display in RAW mode
- CTRL-A and CTRL-C Don't forget to press CTRL-R again to display in normal mode after you do this.
- Ximian Evolution http://www.Ximian.com/products/ximian_evolution/
- Go to the "View" > "Message Display" and click on "Show Full Headers".

21. Sylpheed

Sylpheed is an email client for Linux, BSD and Unix systems. Sylpheed offers three ways to view the full source code of messages:

- Select the email
- Right click and mouse-over "View"
- Select "Source" from the popup menu

or

- Select the email * Left click on the "View" menu

- Select "View Source"

or....

- Select the email

Press Ctrl-U

22. Excite web-mail

To view the full header information with Excite Webmail:

- Sign in to your email account.
- Click on Preferences on the Email home page
- Click on Email Preferences
- Check the box to display headers
- Click on Save You can then see the headers in all messages in your folders.

23. Netscape Webmail

- While viewing the message, click on the yellow triangle to the right of the brief message headers.
- This will display the full headers along with the message body, which can be cut and pasted.
- To close the full headers and return to brief headers, click the yellow triangle again.

24. Blitzmail

- After opening the message, click on the Verbose Header link at the top of the window.

25. Operamail

- Choose Options and enable [x] Show Message Headers in Body of Message Lycos Mail (mailcity.com). When viewing an individual message, click on the tool bar menu item above the message "All Headers".
- Highlight and copy the complete message from the viewing window and paste it. One box.com Click on the subject of the email in your inbox or other folder. This displays the message. At the top of the message you will see the following links in the message frame right above the "reply" buttons: [folder name]: Prev | Next: Download Select "Download" from the above. A new browser window will spawn with both the headers and the message text. At this point, simply copy all the text and paste it.

26. GNU/Emacs integrated email

Press the keys 'W', then 'v' in the summary or mail buffer.

Another method of temporarily switching to ALL headers is by pressing "Ctrl-u g" on the article in the summary buffer.

27. Pegasus Mail

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

Another way:

- Highlight the HTML in the new mail folder
- Open a new email message
- Drag the HTML onto the new message
- In the dialog that appears select "Show All Headers"
- Highlight the entire message, then copy to clipboard
- Paste

28. Mac Mail (OS X Mail)

- Select a message
- Select menu item Message, Show, Raw Source.
- Click on the resulting text
- Click Edit, Select All, then Edit, Copy
- Paste

29. Microsoft Entourage

- After clicking on the message, select "Source" from the View menu
- A new window will open showing the full message source with complete headers.
- Copy and paste.

Nilusha Gunathilake
Information Security Engineer

Sri Lanka Computer Emergency Readiness Team | Coordination Center

Address: Room 2-119A,
BMICH,
Buddhaloka Mawatha,
Colombo 07,
Sri Lanka

Tel: +94 11 269 1692 /269 1064 / 267 9888

Fax: +94 11 269 1064

E-mail: slcert@slcert.gov.lk