Email and envelope headers

Why learning about email headers?

Interpreting email headers is an essential skill when dealing with email-related issues or investigating the source of an email. Email headers contain valuable information about the path an email took from the sender to the recipient. It allows debugging email issues like non-delivery and detecting fraud or phishing.

In this article, we will learn how to interpret the basic data of email headers.

What are email headers?

An email has more raw content than what your email client (Outlook, Gmail, Thunderbird or your webmail interface) shows you. The various actors sending, transporting and receiving your email add content to it along its way. These data are contained in a set of lines at the top of the email, above the content, called the headers.

Note: the original definition of the email header in RFC 822 calls the whole set of headers "the header", composed of fields. The more recent RFC 2076 calls the set of headers "heading" and each separate entry a header. In the following text, we will follow this latest convention.

A header is composed of a header name, a colon (:) and header value(s).

A reminder about SMTP

In another previous [article](#) , we have explained the SMTP protocol.

Remember: the transmission of an email from a User Agent (MUA or mail client) to an email relay (MTA) occurs via the following dialog:

- `HELO/EHLO`: used by the client to identify itself;

- `MAIL FROM`: used by the client to identify the sender;

- `RCPT TO`: used by the client to identify the recipient;

- `DATA`: introduces the real content of the email. The end of the data is marked by a line only containing a sigle dot (".").

- `QUIT`: closes the conversation.

Envelope and email

You can consider that the content transmitted by the various components handling your email is divided in two parts.

Part 1: the envelope

The *envelope* shows data needed to transport your email. In the traditional mail, this is the equivalent of what is written on the outside of the envelope you put your letter in.
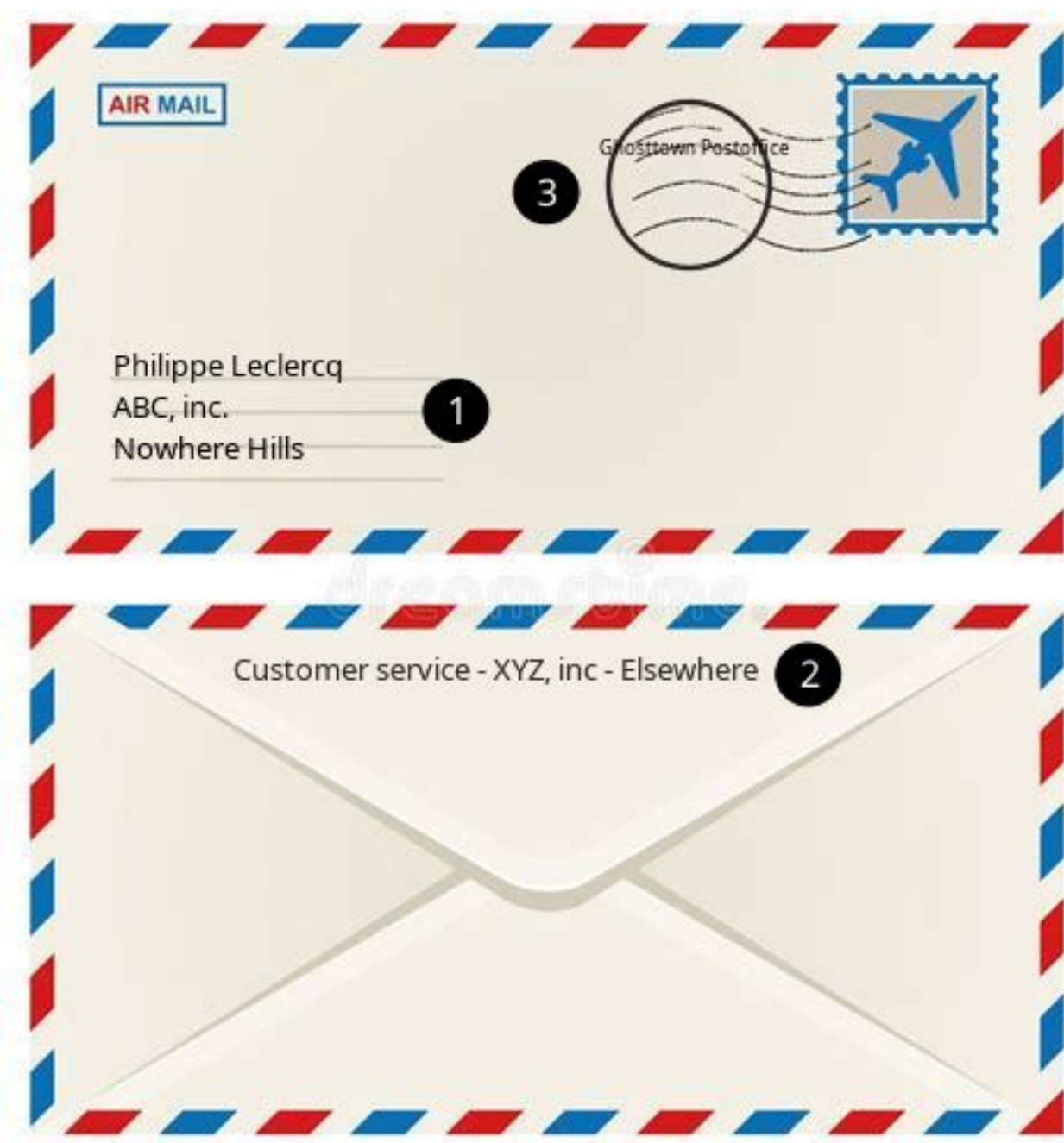
There is:

1. the name and postal address of the recipient;

2. the name and postal address of the sender, that can be used by the postal service to return mail if it cannot be delivered;

3. the stamp of the postal service that transported your mail. Each post office could add its stamp.

Note that the postal service will not (normally) open the envelope.

The HELO/EHLO, MAIL FROM and RCPT TO are the *envelope* headers, belonging to the SMTP layer. They *may* be altered during the email's journey.

Part 2: the mail itself

Inside the envelope, there is a letter with the actual content you want your addressee to read.

Jack Smith

XYZ, inc, Elsewhere,

☎ ⌕

February 25, 2024

Jack Smith, XYZ, inc, Elsewhere,

Philippe Leclercq
ABC, inc
Nowhere Hills

Subject: Invitation

Dear Philippe,

Lorem ipsum dolor sit amet, consectetur adipiscing elit, ...

The *email* part is similar, and appears after the DATA tag in the SMTP conversation.

A minimal set of email headers will contain:

- From: or Reply-To: the sender's address
- To: the recipient's email address
- Date: when it was sent

A minimal example

We will send a very simple message directly via telnet (without email client) to a mail server.

```
telnet mailserver 25
Trying 192.168.50.214...
```

```
Connected to mailserver.int.osix.be.
Escape character is '^]'.
220 mailserver ESMTP Postfix (Debian/GNU)
HELO gandalf
250 mailserver
MAIL FROM: Jack.Smith@mydomain.com
250 2.1.0 Ok
RCPT TO: pleclercq@mydomain.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Test.
.
250 2.0.0 Ok: queued as 4B76334DA
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

The complete source of the received message is:

```
From - Sun Feb 25 16:48:01 2024
X-Account-Key: account7
X-UIDL: 0000000e65454373
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Return-Path: <Jack.Smith@mydomain.com>
X-Original-To: pleclercq@mydomain.com
Delivered-To: pleclercq@mydomain.com
Received: from gandalf (unknown [192.168.50.31])
by mailserver (Postfix) with SMTP id 4B76334DA
for <pleclercq@mydomain.com>; Sun, 25 Feb 2024 16:46:36 +0100
(CET)

Test.
```

The envelope headers are minimal:

- RFC 5321 mandates that the MAIL FROM value is copied by the final MTA into a header, usually the Return-Path: one. It is the case here.

- The final MTA has also set the Delivered-To header to the recipient's address.

- A Received: header has been added by the mail server, containing the name and IP address of the sending machine (*gandalf, 192.168.50.31*), the name of the receiving machine (*mailserver*), the recipient's address and a timestamp. If there

are several hops, each MTA will add its own `Received:` header to trace the email journey.

As explained earlier, these envelope headers show the 'transport' part of the protocol.

The mail headers themselves are absent. There are no `From:`, `To:` or `Subject:` mail headers since they were not present in the DATA part.

The X-headers are proprietary, non official data used by the email client and server software.

This is how it is displayed at the recipient's end:
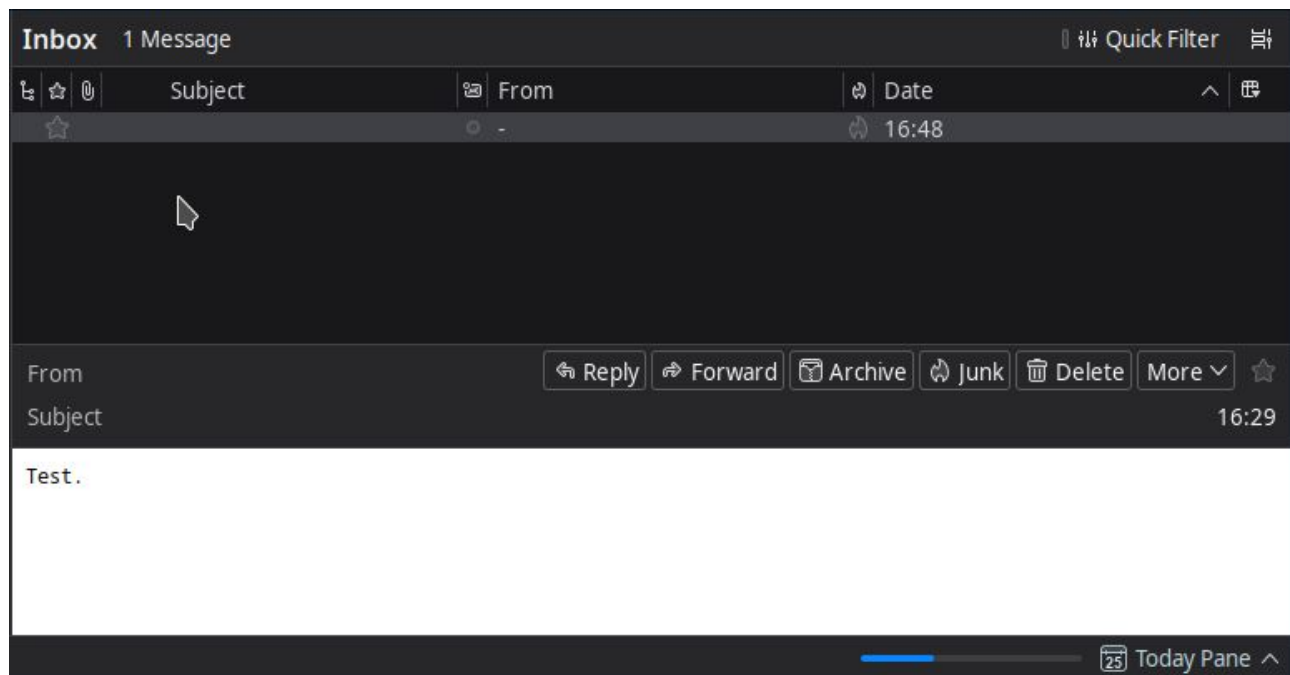
There are no `From`, `To` and `Subject` fields in the DATA area, so the email client cannot copy them and leaves them blank.

A more complete example

Let's send a more complete email with `From:`, `To:` and `Subject:` fields in the DATA section.

```
telnet mailserver 25
Trying 192.168.50.214...
Connected to mailserver.int.osix.be.
Escape character is '^]'.
220 mailserver ESMTP Postfix (Debian/GNU)
HELO gandalf
250 mailserver
MAIL FROM: Jack.Smith@mydomain.com
250 2.1.0 Ok
RCPT TO: pleclercq@mydomain.com
250 2.1.5 Ok
DATA
```

```
354 End data with <CR><LF>.<CR><LF>
From: Jack.Smith@mydomain.com
To: pleclercq@mydomain.com
Subject: Test email
Test.
.
250 2.0.0 Ok: queued as 8FCE834DA
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```
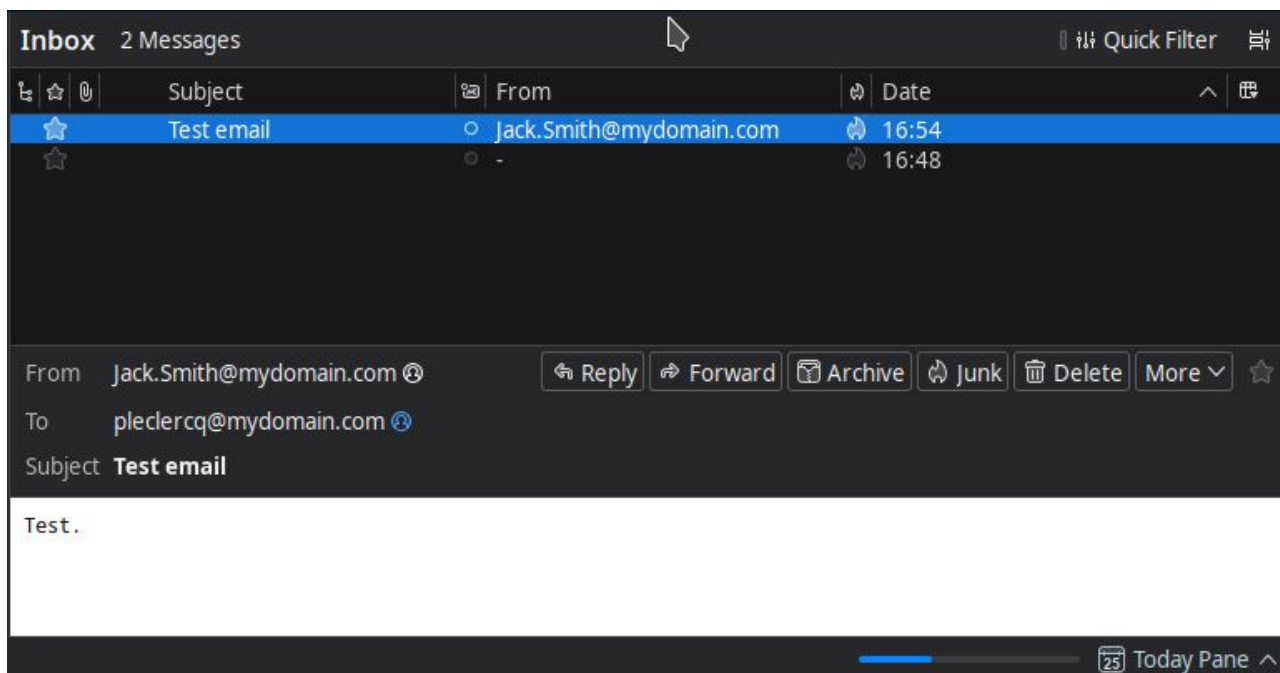
The complete source of the received message is:

```
From - Sun Feb 25 16:54:08 2024
X-Account-Key: account7
X-UIDL: 0000000f65454373
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Return-Path: <Jack.Smith@mydomain.com>
X-Original-To: pleclercq@mydomain.com
Delivered-To: pleclercq@mydomain.com
Received: from gandalf (unknown [192.168.50.31])
by mailserver (Postfix) with SMTP id 8FCE834DA
for <pleclercq@mydomain.com>; Sun, 25 Feb 2024 16:52:06 +0100
(CET)
From: Jack.Smith@mydomain.com
To: pleclercq@mydomain.com
Subject: Test email

Test.
```

The `From:`, `To:` and `Subject:` email headers have now been filled with the corresponding fields from the DATA part.

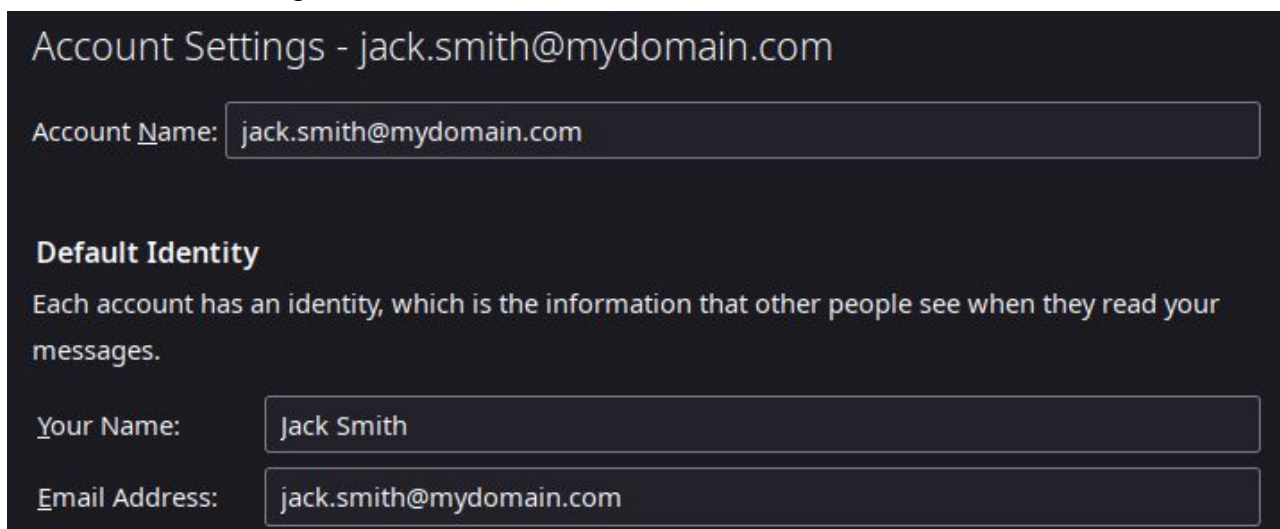This is now how it is displayed at the recipient's end:

The fields displayed in the email client have been extracted from the email headers.
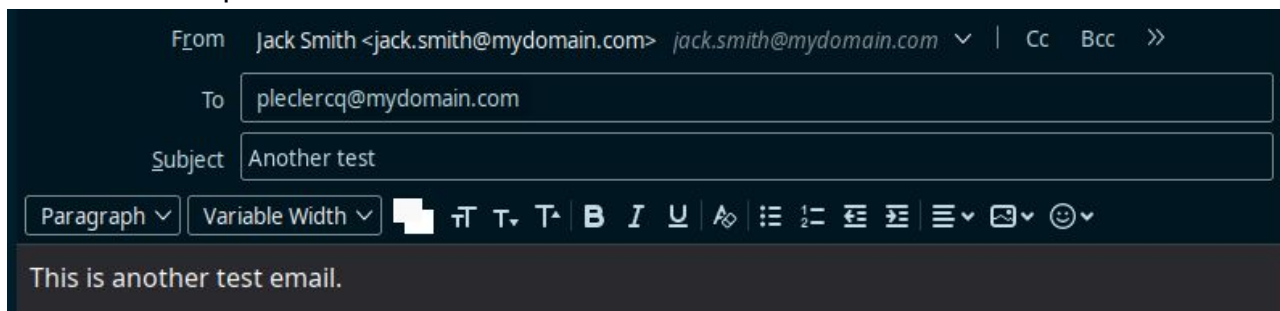
An example with email client

Let's now use a regular email client to send a mail.

These are the settings for the sender's email client:



This is the composed email:

And the complete content:

```
From – Sun Feb 25 16:59:03 2024
```

```
X-Account-Key: account7
X-UIDL: 00000001065454373
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Return-Path: <jack.smith@mydomain.com>
X-Original-To: pleclercq@mydomain.com
Delivered-To: pleclercq@mydomain.com
Received: from [192.168.50.31] (unknown [192.168.50.31])
by mailserver (Postfix) with ESMTP id AD50834DA
for <pleclercq@mydomain.com>; Sun, 25 Feb 2024 16:58:48 +0100
(CET)
Message-ID: <a5022c36-ee41-448a-9864-d13cfacc97bb@mydomain.com>
Date: Sun, 25 Feb 2024 16:58:48 +0100
MIME-Version: 1.0
User-Agent: Mozilla Thunderbird
Content-Language: en-GB
To: pleclercq@mydomain.com
From: Jack Smith <jack.smith@mydomain.com>
Subject: Another test
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit


This is another test email.
```

This is how it is received:
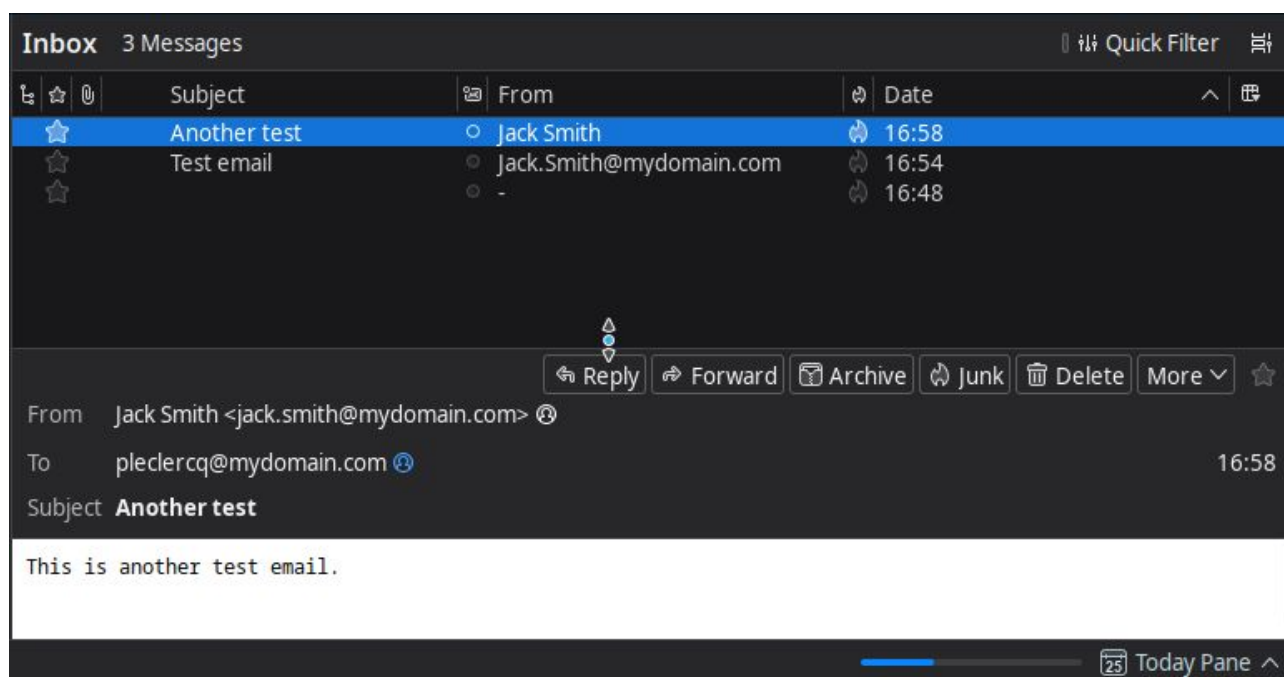
How to display the headers

As noted in the beginning of this article, and as displayed in the pictures of the mail client above, the recipient does not by default see the headers. However, most mail clients or webmail interfaces have an option to display the raw content received, including the headers.

Gmail

1. Click on the email you want to analyze, click on the three dots in the upper right corner, and select the *Show original* option.
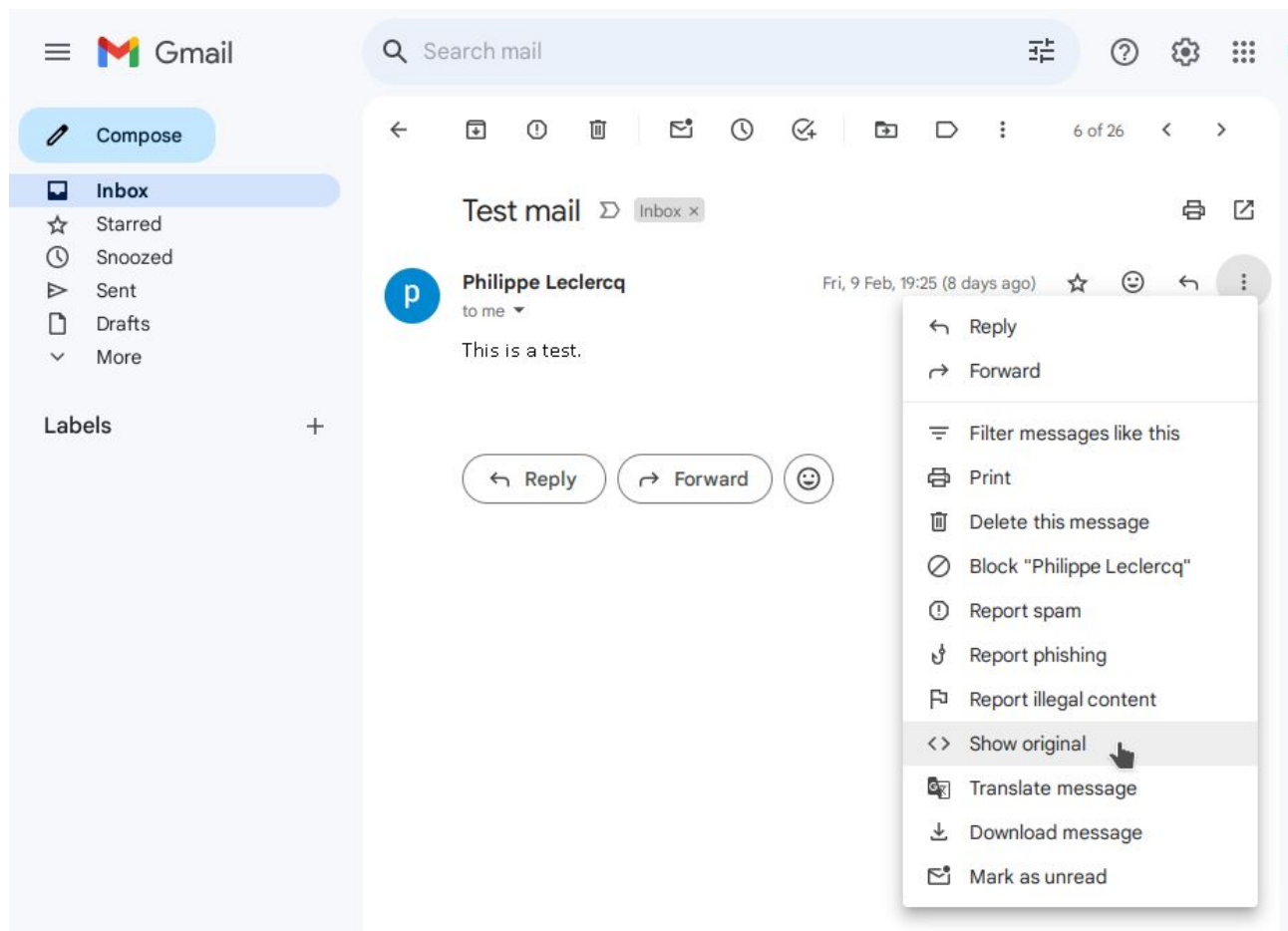
2. A new tab will open in the browser, showing the raw entire content of the email. You can copy it with the *Copy to clipboard* button.

Original message

Message ID	<AS8P189MB16214F3EA45F55D5BF8071068E4B2@AS8P189MB1621.EURP189.PROD.OUTLOOK.COM>
Created on:	9 February 2024 at 19:25 (Delivered after 1 second)
From:	Philippe Leclercq <pltrash2@outlook.com>
To:	"pltrash2@gmail.com" <pltrash2@gmail.com>
Subject:	Test mail
SPF:	PASS with IP 2a01:111:f403:2e07:0:0:0:801 Learn more
DKIM:	'PASS' with domain outlook.com Learn more
DMARC:	'PASS' Learn more

Download original   Copy to clipboard
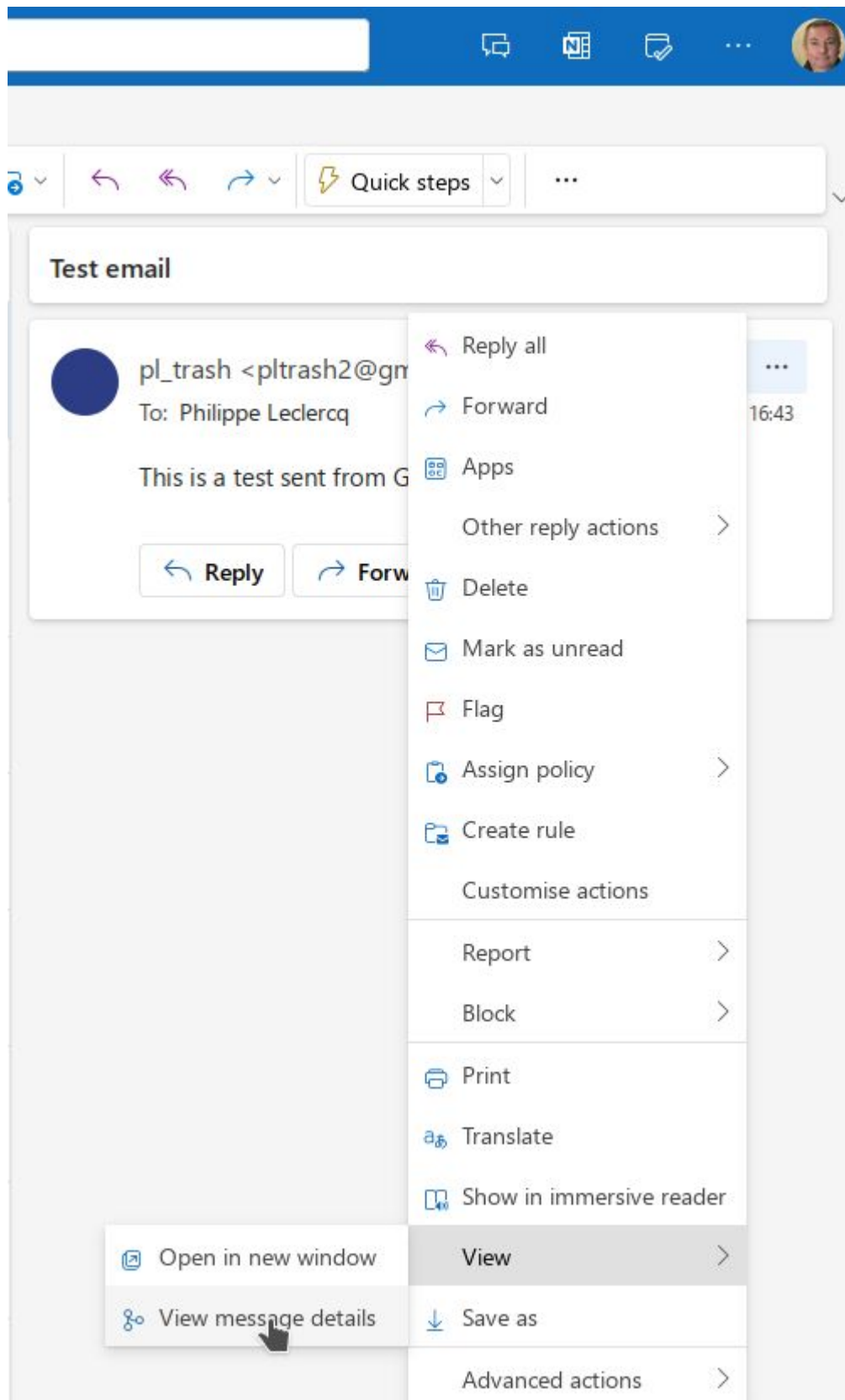
```
Delivered-To: pltrash2@gmail.com
Received: by 2002:a05:7412:b412:b0:fa:52c5:c6f5 with SMTP id du18csp1118088rdb;
        Fri, 9 Feb 2024 10:25:52 -0800 (PST)
X-Google-Smtp-Source: AGHT+IGeEaKzClk7bWmXNcuKcEVj2tEURmmYtWDoUH29dW5jTDGyh4ItqXfKqt9bRKVFeD3y+7EG
X-Received: by 2002:a37:c447:0:b0:785:5b28:eac8 with SMTP id
h7-20020a37c447000000b007855b28eac8mr2295064qkm.42.1707503152006;
        Fri, 09 Feb 2024 10:25:52 -0800 (PST)
ARC-Seal: i=2; a=rsa-sha256; t=1707503151; cv=pass;
        d=google.com; s=arc-20160816;
        b=hPPb3zvfaadhvhrS5Z/aKehJ9Cp1q/tsVCqRlUtzZGE6uB2GoiZwxpqjLkRUbljqwV
         KKJQFwE5kQl3Efc5FDCwokVn/m8gsV40iZ4LFsMLK8h/oeghz0BDuJG63XR23+AYhIRQ
         qJxjVMg5pSK9N85Io1N76vg6LlTeql2Y7y4qvfNixkLn7/WtlUaRxbEh9QYnp/T1jSfB
         58RECUPyEdHBqVRGj6oQLBSL9W65n3UGBHfKGW53PHdR/E6y7etmVuy/gpc1OzQ4Z21T
         q2pdGzFFrcy85fhGYyPUmKccNX6+k76jLXHrm8UsAWIVxha6ftb21sdUDuIWIEvhz5eR
         /H2w==
ARC-Message-Signature: i=2; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=mime-version:msip_labels:content-language:accept-language
         :message-id:date:thread-index:thread-topic:subject:to:from
         :dkim-signature;
        bh=R2qao3WRmZH91cOip/NjQRpctZG50vwDDLXFATvDnmo=;
        fh=GEIogK0mQ93mytaCBTCoZpyrY7PfoTl8z8No7Fv1vHA=;
        b=aN/X0QqYw4v8VN6FhH9CLAa7mJnhMjzjDkLJ4jqCgXYOsCK0HOIL21BWB0Sd7+tUcD
         yIfXDlRziKU6QRrUlDcGJpY6MarXJA9EK39zwkSPIizvk2wLK+6bSx+D/6eAMp592XNi
         iS/A2fPINjbNXr9XoxWlS9Tod5UhfrMK7cxLtZMadckyomWelzsXIsZeQaWzHS25VP0I
         x1Ab08Vjj44CD4ZSwspBh4n1XnM48IdkcyEqPL/+3Wik89XOXFpz2JlpKookH5qJULNF
         DnfqHZiWfqQjReCggBZyweRcirxXr1Tz0UtyAMd/EG7vHRSJ5ABno8xqjYWYeCC01qkQ
         1VhQ==;
        dara=google.com
ARC-Authentication-Results: i=2; mx.google.com;
        dkim=pass header.i=@outlook.com header.s=selector1 header.b=ObkTC2Hd;
        arc=pass (i=1);
        spf=pass (google.com: domain of pltrash2@outlook.com designates 2a01:111:f403:2e07::801 as
permitted sender) smtp.mailfrom=pltrash2@outlook.com;
```
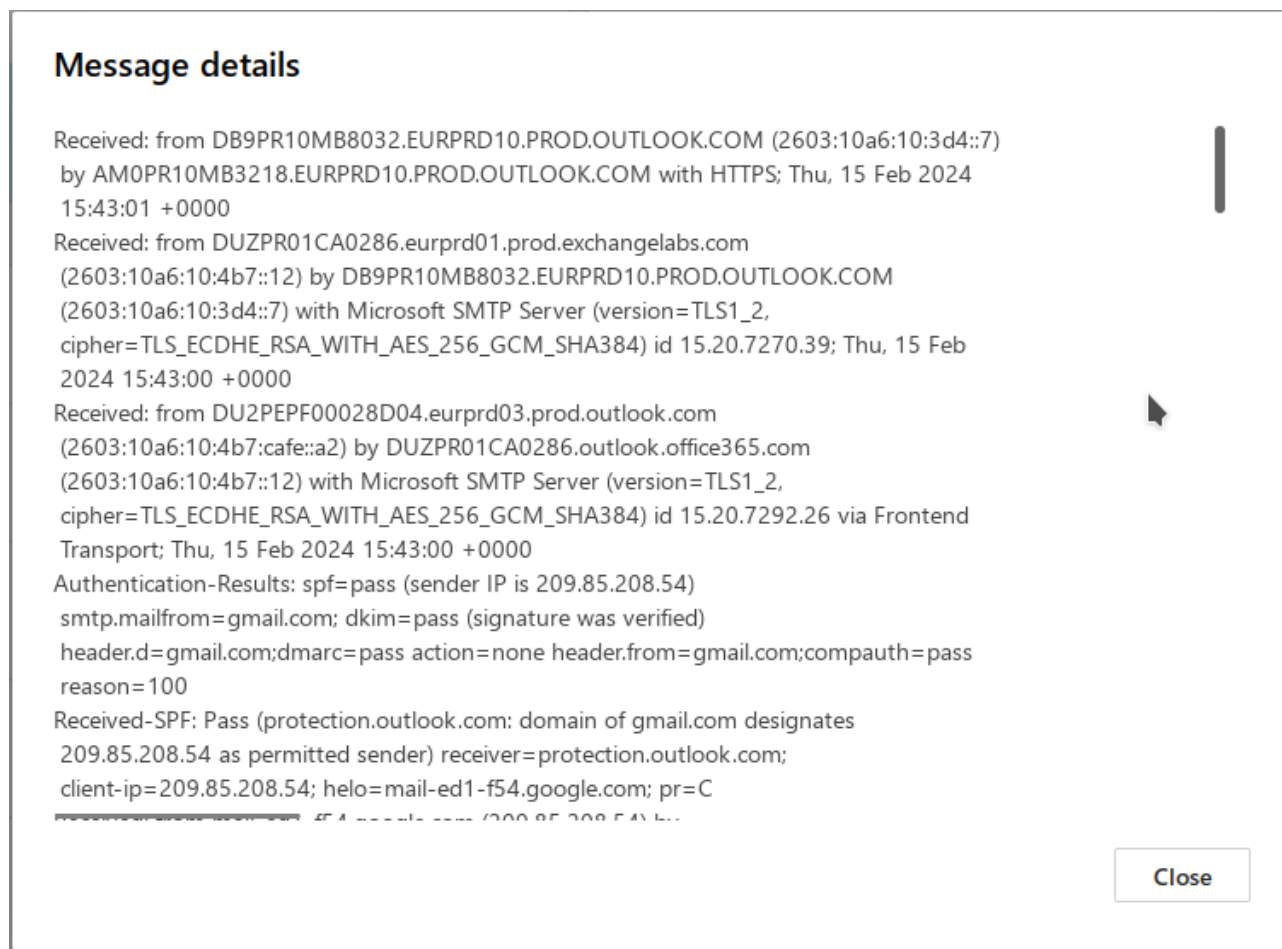
Microsoft Office 365

1. Select the email you want to analyze in the left pane.
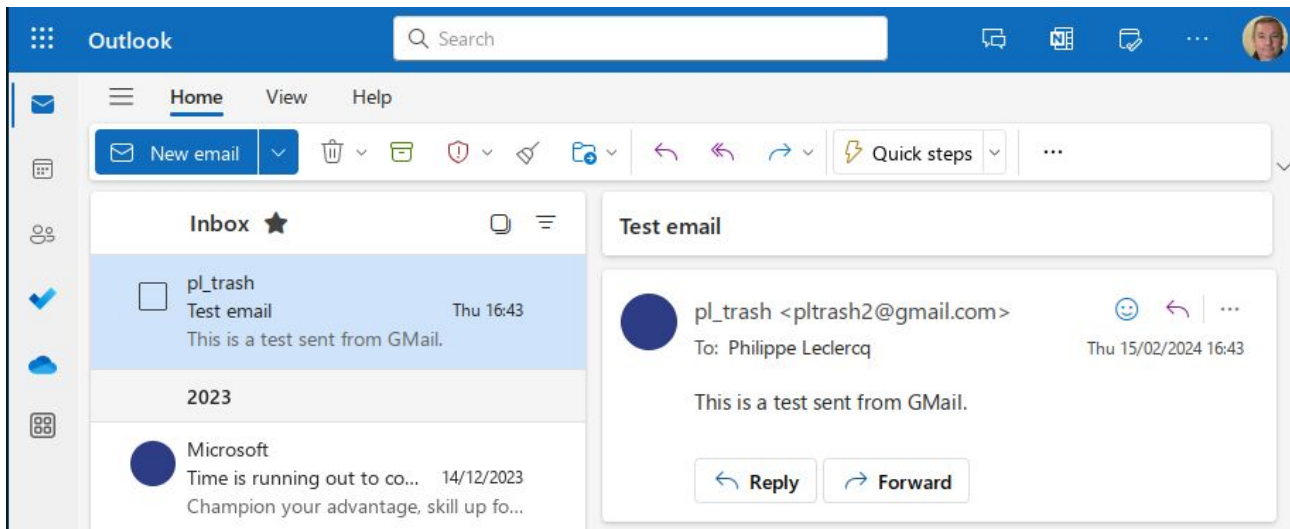
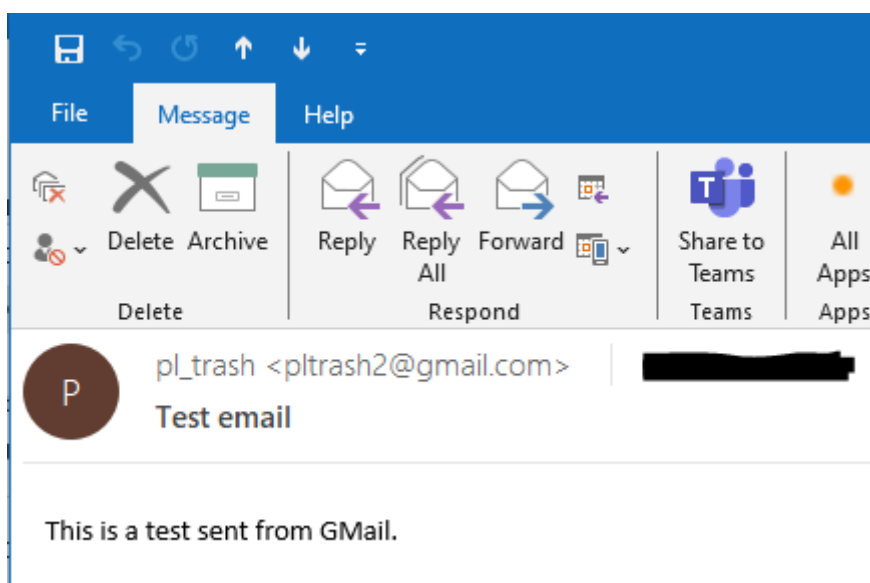2. Click on the three dots in the upper right corner, and select the *View -> View message details* option.

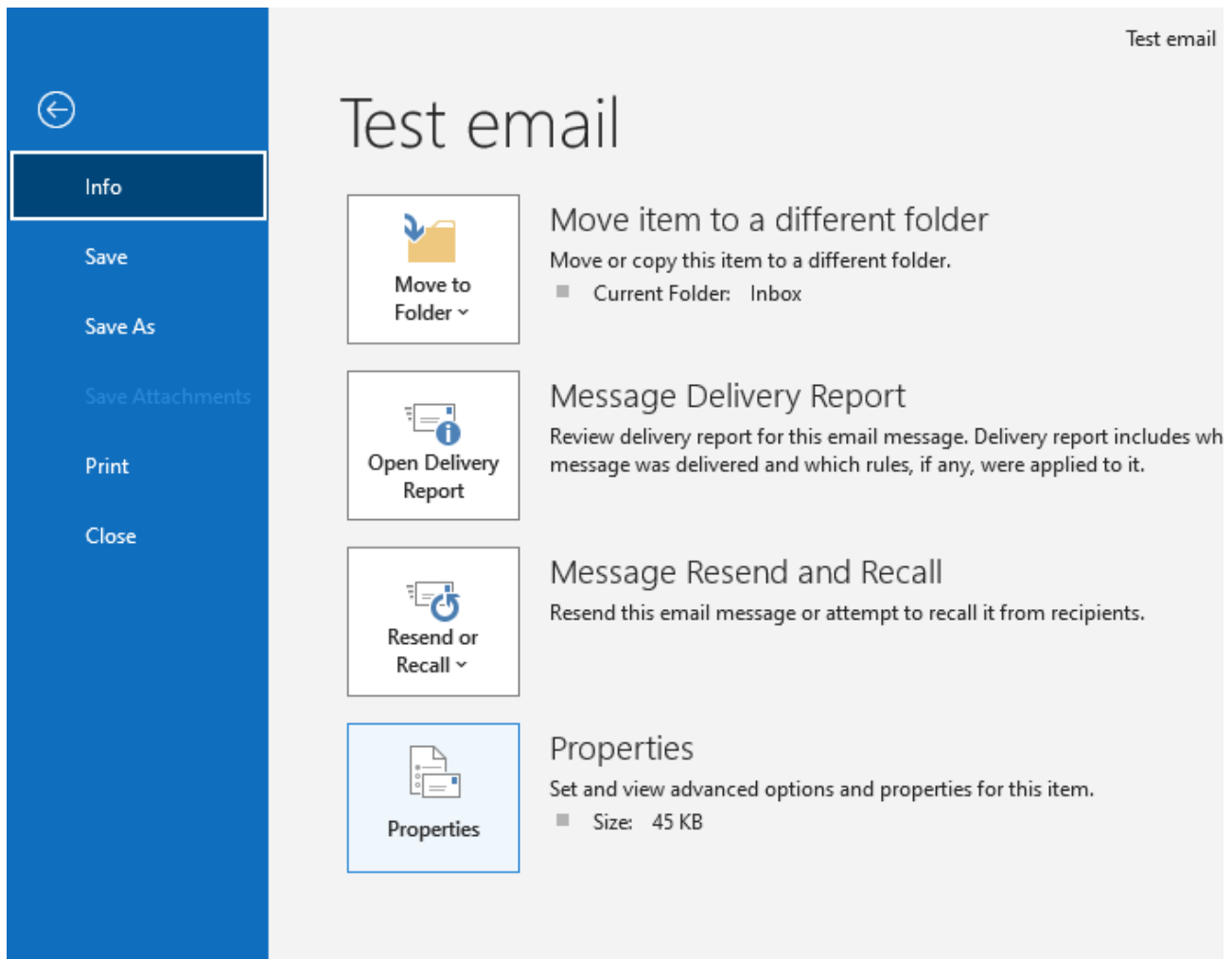3. A new window will pop up in the browser, showing the raw entire content of the email.

Message details

Received: from DB9PR10MB8032.EURPRD10.PROD.OUTLOOK.COM (2603:10a6:10:3d4::7)
by AM0PR10MB3218.EURPRD10.PROD.OUTLOOK.COM with HTTPS; Thu, 15 Feb 2024
15:43:01 +0000
Received: from DUZPR01CA0286.eurprd01.prod.exchangelabs.com
(2603:10a6:10:4b7::12) by DB9PR10MB8032.EURPRD10.PROD.OUTLOOK.COM
(2603:10a6:10:3d4::7) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7270.39; Thu, 15 Feb
2024 15:43:00 +0000
Received: from DU2PEPF00028D04.eurprd03.prod.outlook.com
(2603:10a6:10:4b7:cafe::a2) by DUZPR01CA0286.outlook.office365.com
(2603:10a6:10:4b7::12) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7292.26 via Frontend
Transport; Thu, 15 Feb 2024 15:43:00 +0000
Authentication-Results: spf=pass (sender IP is 209.85.208.54)
smtp.mailfrom=gmail.com; dkim=pass (signature was verified)
header.d=gmail.com;dmarc=pass action=none header.from=gmail.com;compauth=pass
reason=100
Received-SPF: Pass (protection.outlook.com: domain of gmail.com designates
209.85.208.54 as permitted sender) receiver=protection.outlook.com;
client-ip=209.85.208.54; helo=mail-ed1-f54.google.com; pr=C

Close

4. You can click in the window, select the whole text with <CTRL>-A, copy it with <CTRL>-C and paste it in another application (like a text editor) with <CTRL>-V.

Outlook

1. Double click on the email you want to analyze.

File   Message   Help

Delete Archive   Reply Reply Forward   Share to   All
                          All   Teams   Apps
Delete   Respond   Teams   Apps

P   pl_trash <pltrash2@gmail.com>
     Test email

This is a test sent from GMail.

OSIX

2. Click on *File -> Info -> Properties*.

3. A property window will pop up, showing the Internet headers in the bottom text box.

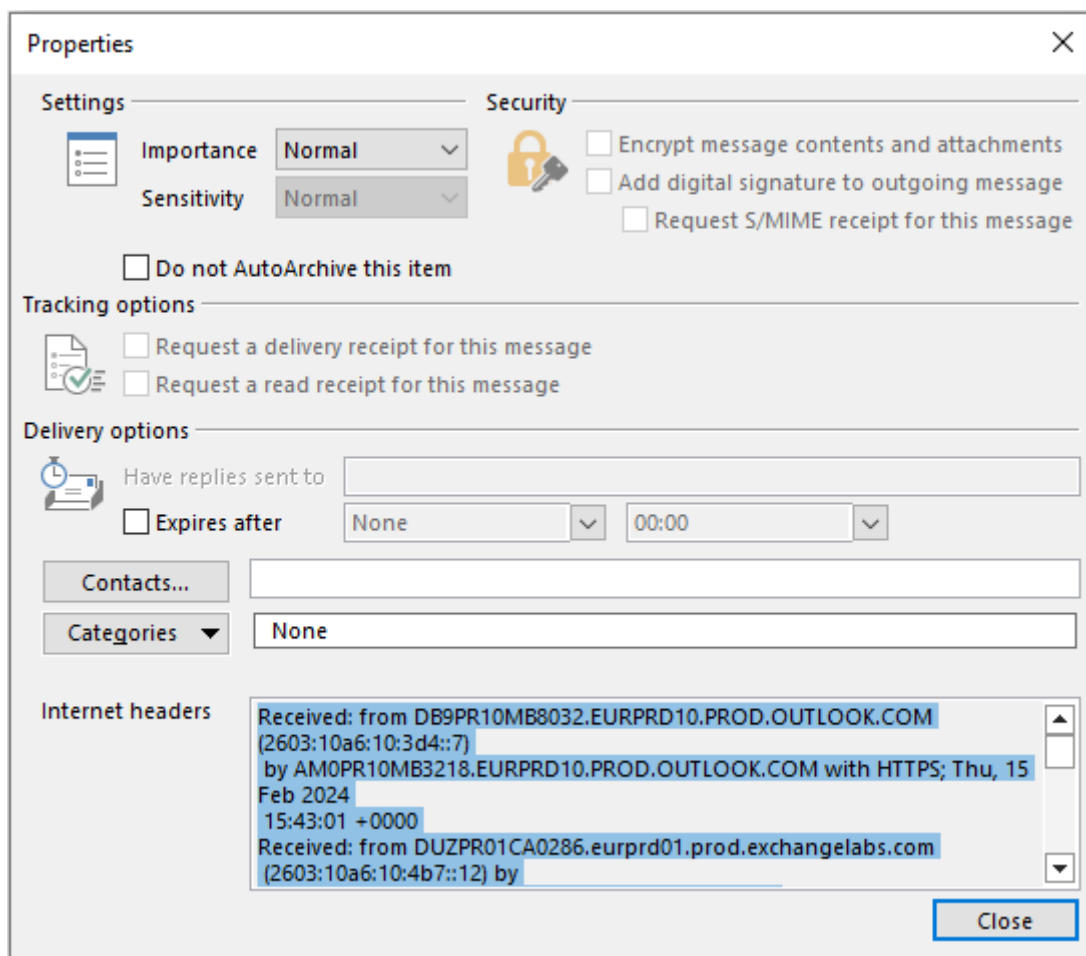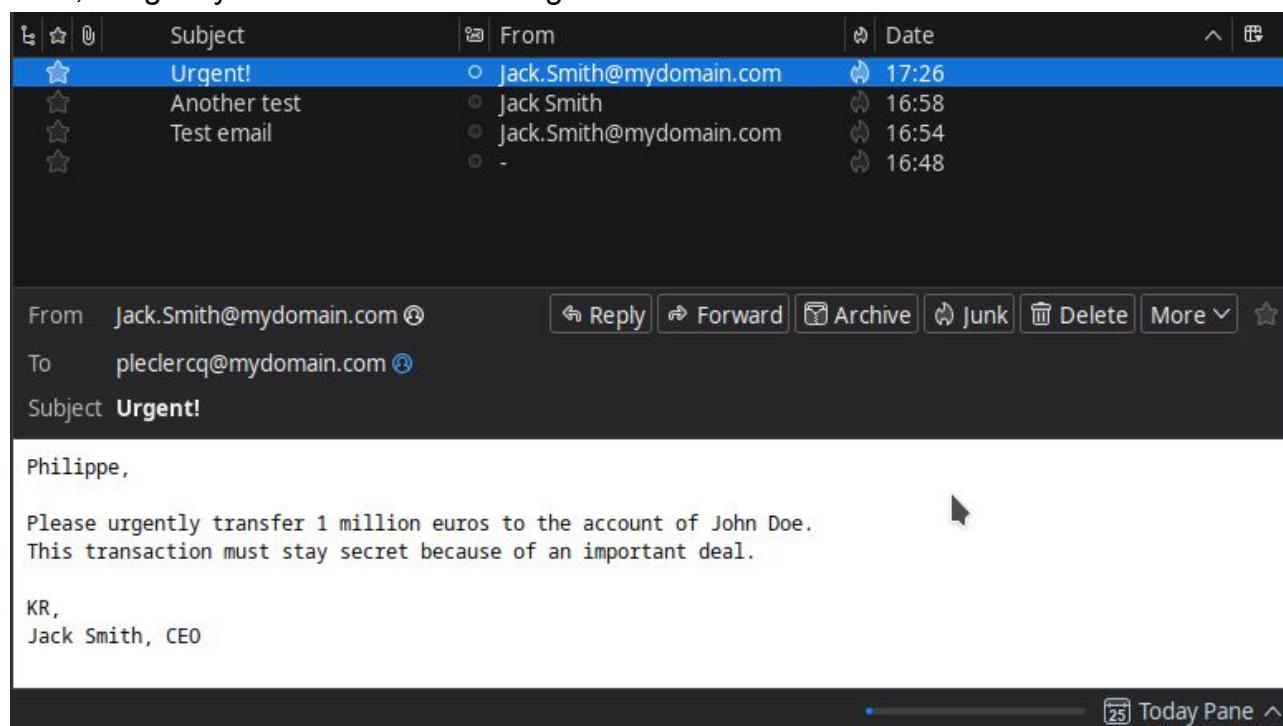4. To copy the headers, click into the text box, select the whole text with <CTRL>-A, copy it with <CTRL>-C and paste it in another application (like a text editor) with <CTRL>-V.

Detecting potential fraudulent email by analyzing headers

Now, imagine you receive the following email:

This is an unusual process, you are surprised. You try to call your Jack for confirmation, but he is abroad and unreachable. What to do next?

Well, let's look at the headers:

```
From - Sun Feb 25 17:26:18 2024
X-Account-Key: account7
X-UIDL: 0000001165454373
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Return-Path: <attacker@evil.corp>
X-Original-To: pleclercq@mydomain.com
Delivered-To: pleclercq@mydomain.com
Received: from attacker?evil.corp (unknown [192.168.50.202])
by mailserver (Postfix) with SMTP id 054DC34DA
for <pleclercq@mydomain.com>; Sun, 25 Feb 2024 17:22:04 +0100
(CET)
From: Jack.Smith@mydomain.com
To: pleclercq@mydomain.com
Subject: Urgent!


Philippe,


Please urgently transfer 1 million euros to the account of John
Doe.
This transaction must stay secret because of an important deal.


KR,
Jack Smith, CEO
```

Hmm. `Return-Path: <attacker@evil.corp>`.

This was NOT sent from Jack's account, but by an attacker spoofing his address. Bad luck for them, you spotted it. Good on you!

(BTW, this is an example of a frequent abuse called CEO fraud or BEC - Business Email Compromise. According to Barclays Bank and the Treasurer Magazine, CEO fraud targets more than 400 companies a day, of which 40% are small and medium entreprises, triggering losses of more than 3 billion $).