# Analyzing the email journey via the envelope headers

## Received: headers

* 1. In a previous [article](https://blog.osix.be/email-headers), we have described the envelope and email headers.

Among the envelope headers, the ***Received:*** headers are very interesting to trace the email path. They are normally added by every transport service relaying the email. These headers mention:

* the name and IP address of the machine sending the mail (the ***from*** part),
* the name of the machine receiving the mail (the ***by*** part),
* the time the email has been received,
* and the address of the recipient.

## **A** simple example

This is a simple email, sent from a workstation directly connected to the mail server *mailserver,* running Postfix (open source mail server software), for a user having his mailbox on the server itself.

From - Sun Feb 25 16:59:03 2024

X-Account-Key: account7

X-UIDL: 0000001065454373

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.

In this example, there is only a single ***Received:*** field as there is only one hop between the sending workstation at address 192.168.50.32 and '*mailserver'*, but usually there are several ones, listed in the reverse order, i.e. generally, the first header is at the bottom of the list and the last one is at the top.

## A real life example

Received: from EUR02-AM0-obe.outbound.protection.outlook.com (Unknown [10.244.15.125])

by c1bf3b2951b1 (Haraka/3.0.2) with ESMTP id 2030C8E2-861D-40B5-A45C-40A4D6395AF4.1

envelope-from <pltrash2@outlook.com>;

Sat, 10 Feb 2024 17:06:36 +0000

ARC-Seal: i=1; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv=none;

b=Nj+vgQ59oCQJ3LNihZyDOAKZEYW/6zofNUT3QcHmUYDfLFN9KrolNoEf4WlhDEVH9KasRsxyy9ywDpSY+lpDMpAeNybR4gIsVBITnzLsh6GktizTwY2QTP1Eery4y2q/i8LsBp2fH0WwVWJTXFufcTCGwn8BCOTjHWDwc0FYeLj8FdPKX5lt8Agv/VCEqBjrPv9+E8MHVFG89xrLyNAPEpKwTc6RKooII60/4Cb8X19sTkDqcaOFKjQ0ookOprr5RraEh7fDo9i9NRERXNbaJ7XDl9AHD8At9KXuuJqLvhmrm+XVHMMf52ZLzJZCuGFcQgD8g6K7z0D6Id3XFANUog==

ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;

s=arcselector9901;

h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-MessageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-Exchange-AntiSpam-MessageData-1;

bh=AFRJ0OyIK8TufnrqVGHwr8mtiFFfO6e0CsC0aCfF62s=;

b=LHvE2XYtlsGrijaR9l+ZjdAWWax8QExl9m2k/WWual+jomH8qFHkLYRfC7n8L1GOnrE8gJhQcqyFAaIf0YUHpM/V5rzX1NFrTXATASWSVy9bwUAvjChqBDy8KP7xaCCaGVqlntL6syvyJRopzzoZjgD+PFqYS9KcfunfaOXjP4EzHX0uhWFZHc0nY87K+NYfCBvdeZlAWAXw2tJBno+WO0glbacpJm7b0EVJQ0SmQL9dUErOLRVPBiiLOmntlfd9hNkxqtoj8qwvAHcux81s9JcjwGzD/MP+1lUi9hjPlDTUdeMtfqJ48RxDYSyHDwA9KmUqCVK/yWY6amvFrY0URg==

ARC-Authentication-Results: i=1; mx.microsoft.com 1; spf=none; dmarc=none;

dkim=none; arc=none

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=outlook.com;

s=selector1;

h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck;

bh=AFRJ0OyIK8TufnrqVGHwr8mtiFFfO6e0CsC0aCfF62s=;

b=ULBWNbP9V1dJ0w9s4i9yG8r5jcUUjXkSkbcrR4m4Mbvor+Y4cDZB9H8T7e2vbyIx5AI4WY2OzjW1r2jqQpGOWPMJBTMqhet5gdPf/eUvpCGszxkBIbo8X3eEmlue8XXyeO9jUUonO6wTUGvmYl15DWefdlvGVNHTYAUZ40IKQoLnchsAYLNjWRJaALjO8BHWBg8piZpQL6fOPeQLfdMHNgMTjrX+lqVylXzqc1baDXR75uJW8lpkPe8w1BA7DslxsNRKxD5iXVFdP5BPA3tlXcjDe50h8RdyIzmCRSlzzsr4ldRi2o0dyw7Tp8a9BZAVQMR4GwPn3zWSESaMs6RlfQ==

Received: from AS8P189MB1621.EURP189.PROD.OUTLOOK.COM (2603:10a6:20b:393::12)

by AS1P189MB1864.EURP189.PROD.OUTLOOK.COM (2603:10a6:20b:4a6::18) with

Microsoft SMTP Server (version=TLS1\_2,

cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id 15.20.7270.32; Sat, 10 Feb

2024 17:06:35 +0000

Received: from AS8P189MB1621.EURP189.PROD.OUTLOOK.COM

([fe80::d55d:5c92:531c:341]) by AS8P189MB1621.EURP189.PROD.OUTLOOK.COM

([fe80::d55d:5c92:531c:341%4]) with mapi id 15.20.7270.033; Sat, 10 Feb 2024

17:06:35 +0000

From: Philippe Leclercq <pltrash2@outlook.com>

To: "kevad13210@tospage.com" <kevad13210@tospage.com>

Subject: Test mail

Thread-Topic: Test mail

Thread-Index: AQHaXEOADyMCCu4wgUWKYEaxnfKqCA==

Date: Sat, 10 Feb 2024 17:06:35 +0000

Message-ID:

<AS8P189MB1621A0A78523CB097358B05D8E4A2@AS8P189MB1621.EURP189.PROD.OUTLOOK.COM>

Accept-Language: en-GB, en-US

Content-Language: en-US

X-MS-Has-Attach:

X-MS-TNEF-Correlator:

msip\_labels:

x-ms-exchange-messagesentrepresentingtype: 1

x-tmn: [hIFZVD4B9kzzpYHGFeksyFp3tcJ2Jy8k1Det+rwx/l+QDq/JN31ZU2fZE4kMEdhC]

x-ms-publictraffictype: Email

x-ms-traffictypediagnostic: AS8P189MB1621:EE\_|AS1P189MB1864:EE\_

x-ms-office365-filtering-correlation-id: 07e4ed8d-21a1-406e-1966-08dc2a5aa350

x-ms-exchange-slblob-mailprops:



x-microsoft-antispam: BCL:0;

x-microsoft-antispam-message-info:



x-ms-exchange-antispam-messagedata-chunkcount: 1

x-ms-exchange-antispam-messagedata-0:

=?iso-8859-1?Q?QHINCZlcrnB7TvQ9sM9lDvmxH4U0PXsAPb4Zhh073E2+VoNf9QfZw0cKwO?=

=?iso-8859-1?Q?mLTZJtHF5Q85acxshI43O+wxgCCDKDlzz6ChVQzCf5h1cDDSN1uNg+ZmH3?=

=?iso-8859-1?Q?uO+uY1FOGPt1dY+P37N2EMgG6MjELjxGSoNF0ep8F59zTXqbdETiUxXIyb?=

=?iso-8859-1?Q?JuNOFYl31gtptBFY1qI0n18YFMH7sKS2Zok7nGnUABHOzLKEn+1pITvjRt?=

=?iso-8859-1?Q?Rz1V2y8lecWYJudiMgtxsqv1LnObLQ7WgFRJavWnu3WKmiE7HggA6mJd5W?=

=?iso-8859-1?Q?CqnRKcaf+RRCoZvI2xJBJ/pLlPagEz9qvOx0VztFpooAdENh7nxtxSXptF?=

=?iso-8859-1?Q?vF0yZzVXGQVzkDDCnWDyFr13mtlFISZHQkiT5wut9azMHZ7YlnBy/aJ2WZ?=

=?iso-8859-1?Q?Nh3MBDxooNhA9/yfVG7aPY4i2RVNVzWgS0LGlNY4iNEfBEM9d+pjyKPI2G?=

=?iso-8859-1?Q?wHdPl/zrDB6Y8GauCTgtDK1A6oAOAiPiqveW8ZwLp7Mwr9SJg3dwvhP6ee?=

=?iso-8859-1?Q?TXyHS+Tgt2wQ5ICJ6IIbBmeT59VLASNDvsgNJI7fk6bfr9isf4rAQ3Wp6f?=

=?iso-8859-1?Q?3tauhqNy5tpfM6Lw+FbPx6T5iwKt3vdH14/OGmMMh+S+OzA11Ce2vb+K7e?=

=?iso-8859-1?Q?ye04TklT9Rw4DiqJhiHWcPuLWnSG8Lgg+PuLddrCiIasdbCDgO3Ux8vP3A?=

=?iso-8859-1?Q?9mH2dRbSu7nt1GULqRfI66kklAqWsYF2t9YQXMiDl1SsIit4uCyHfCYCL4?=

=?iso-8859-1?Q?C4MwO25zoXSIjhm+i2XQ8JFtf1KbeonZyEH7rMP310EsK6cb4p8H1ZGP4p?=

=?iso-8859-1?Q?xU0o0WpAf/xXZHu9j/0nBf6Ha8L3E1OETuNUtrDoa0VdbmDJmNsBQlCJRr?=

=?iso-8859-1?Q?yqnU3qXcR3PsSvHr6xJ3thXrCbkTntVgL5yc6Y7MBus7CuCzwPHSTpLZw6?=

=?iso-8859-1?Q?CCaKfNSRiCWzCLZBBjGx0vgOMeMGgRqbdsjSElA7bBFiq4474AhzeH8L8z?=

=?iso-8859-1?Q?rZBMxABW1QMb2NhPKfLRvZ+ig5JIKJ+IJ1jznWaPqATS5hZ7YbZUHaAdLP?=

=?iso-8859-1?Q?kE2a6cflfyXxh1nwLMu6UhgdIxPYQAo7RHCYqX1SMC4CHudgZ3cKdLaopT?=

=?iso-8859-1?Q?DwZmRyDR4bZza8ag5iyu0LAeIlqmi4iR/ccOQV8uemRbk0WaHTu6Hvr05E?=

=?iso-8859-1?Q?0rWXUtFg3WBHr5EA4682aTKPijC3/RoRrfRr3shCDbav+TJ4rxFfcxtKmB?=

=?iso-8859-1?Q?b7jgRhlz2AQj7QhtKNzm24wg1mbZS79yschIPMU3y2viYrDDkCPEAq3C2W?=

=?iso-8859-1?Q?JqKSP7U4C0e+9RurUBvPyd/AYg=3D=3D?=

Content-Type: text/plain; charset="iso-8859-1"

Content-Transfer-Encoding: quoted-printable

MIME-Version: 1.0

X-OriginatorOrg: outlook.com

X-MS-Exchange-CrossTenant-AuthAs: Internal

X-MS-Exchange-CrossTenant-AuthSource: AS8P189MB1621.EURP189.PROD.OUTLOOK.COM

X-MS-Exchange-CrossTenant-RMS-PersistedConsumerOrg: 00000000-0000-0000-0000-000000000000

X-MS-Exchange-CrossTenant-Network-Message-Id: 07e4ed8d-21a1-406e-1966-08dc2a5aa350

X-MS-Exchange-CrossTenant-rms-persistedconsumerorg: 00000000-0000-0000-0000-000000000000

X-MS-Exchange-CrossTenant-originalarrivaltime: 10 Feb 2024 17:06:35.4565

(UTC)

X-MS-Exchange-CrossTenant-fromentityheader: Hosted

X-MS-Exchange-CrossTenant-id: 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa

X-MS-Exchange-Transport-CrossTenantHeadersStamped: AS1P189MB1864

This is a test.=0A=

The mandatory headers ***From:***, ***To:***, ***Date:*** are well visible and highlighted. There is no difficulty to see who sent it and who it was destined to.

Let's try to follow the email's journey.

The first hop is described by the ***Received:*** header nearest to the bottom:

Received: from AS8P189MB1621.EURP189.PROD.OUTLOOK.COM

([fe80::d55d:5c92:531c:341]) by AS8P189MB1621.EURP189.PROD.OUTLOOK.COM

([fe80::d55d:5c92:531c:341%4]) with mapi id 15.20.7270.033; Sat, 10 Feb 2024

17:06:35 +0000

The machine which originally sent the email (on which it has been created) is *AS8P189MB1621.EURP189.PROD.OUTLOOK.COM*. Since the sender has an address ending in *@outlook.com*, it is hardly surprising :-). Its IP address is [fe80::d55d:5c92:531c:341]; it is an IPv6 address.

The first machine which received the email is *AS8P189MB1621.EURP189.PROD.OUTLOOK.COM*. Dang, it is the same as the sender! How is it possible?

Well, it is not unusual for a mail server to have several programs handling the mail transport, for example first a Mail User Agent (the interface with the user), then an anti-malware program examining the content of the email. This second program can run on the same machine, so the email can travel several hops on the same server.

The second hop is listed in the Received header just above the first one:

Received: from AS8P189MB1621.EURP189.PROD.OUTLOOK.COM (2603:10a6:20b:393::12)

by AS1P189MB1864.EURP189.PROD.OUTLOOK.COM (2603:10a6:20b:4a6::18) with

Microsoft SMTP Server (version=TLS1\_2,

cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id 15.20.7270.32; Sat, 10 Feb

2024 17:06:35 +0000

This time, the email was sent from *AS8P189MB1621.EURP189.PROD.OUTLOOK.COM* to *AS1P189MB1864.EURP189.PROD.OUTLOOK.COM*.

The third hop is:

Received: from EUR02-AM0-obe.outbound.protection.outlook.com (Unknown [10.244.15.125])

by c1bf3b2951b1 (Haraka/3.0.2) with ESMTP id 2030C8E2-861D-40B5-A45C-40A4D6395AF4.1

envelope-from <pltrash2@outlook.com>;

Sat, 10 Feb 2024 17:06:36 +0000

This time, the email was sent from *EUR02-AM0-obe.outbound.protection.outlook.com* to *c1bf3b2951b1*, its final destination.

We can now trace the email journey:

*AS8P189MB1621.EURP189.PROD.OUTLOOK.COM -> AS8P189MB1621.EURP189.PROD.OUTLOOK.COM -> AS1P189MB1864.EURP189.PROD.OUTLOOK.COM -> ? -> EUR02-AM0-obe.outbound.protection.outlook.com -> c1bf3b2951b1*

We have a gap in the path because we do not see the transition between *AS1P189MB1864.EURP189.PROD.OUTLOOK.COM* and *EUR02-AM0-obe.outbound.protection.outlook.com*. But we can see from their domain names that they both belong to *outlook.com* (aka Microsoft). It often happens that servers internal to an organization do not record their transport, or even that a same machine has a dual connectivity to the inside and outside of a company and carries different names (and IP addresses) depending on the side we are on. This is not suspicious if the gap is inside the same company.

All other headers are optional headers added by the various agents, used by various softwares to perform their functions (routing, validating, examining, virus scanning the emails...). We will describe a few of them in some following articles.

What can we deduce from this first analysis?

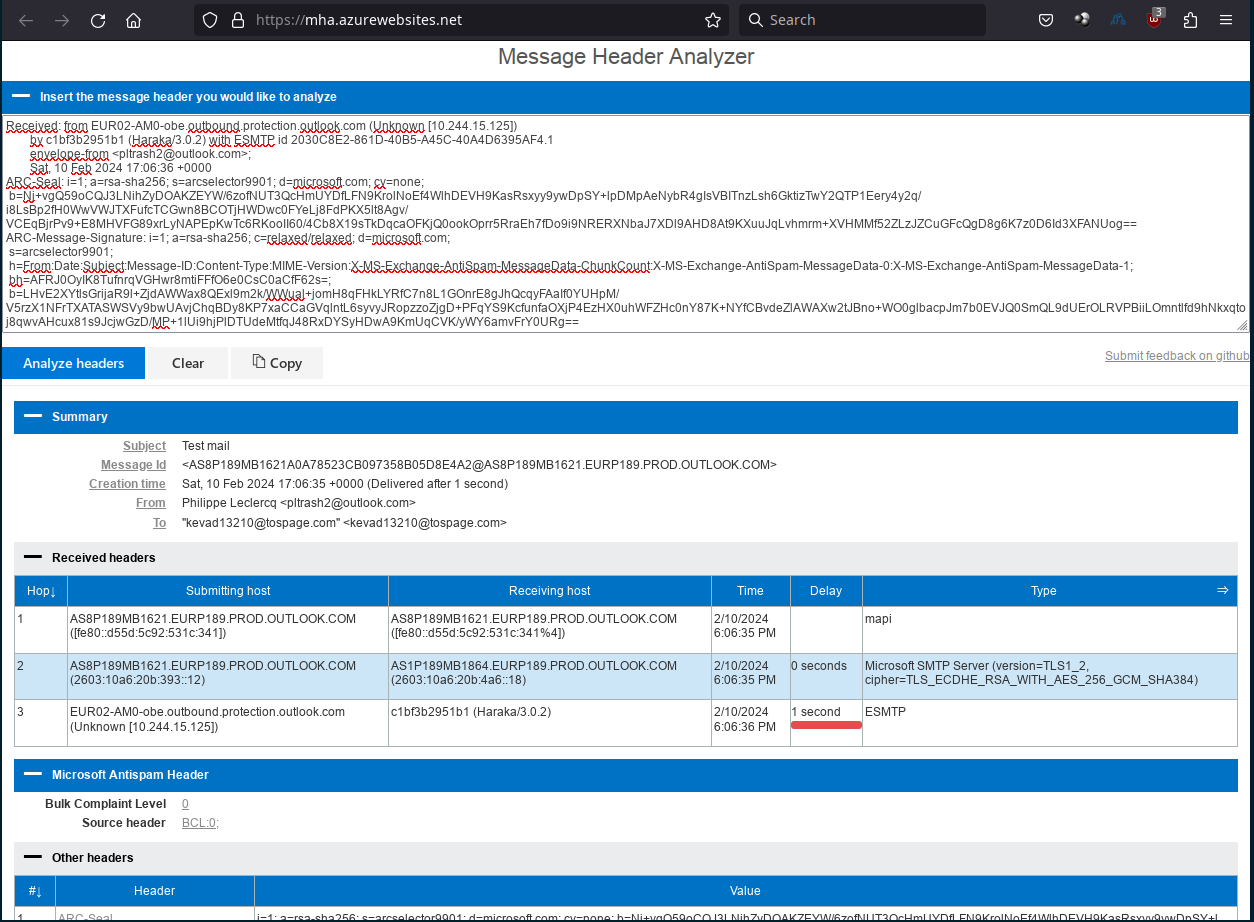
* the email address of the sender is *pltrash2@outlook.com*, and his display name is *Philippe Leclercq*;
* the email has been handled by the servers in the *outlook.com* domain, so we can be reasonably sure that the sender has not tampered with his mail address;
* the email is targeted to *kevad13210@tospage.com*. The email has indeed been received by this user.

## Tools for analyzing headers

Sifting through long lists of headers is cumbersome, time consuming and prone to errors. Fortunately, some online tools can make it easier and faster.

### Microsoft Message Header Analyzer

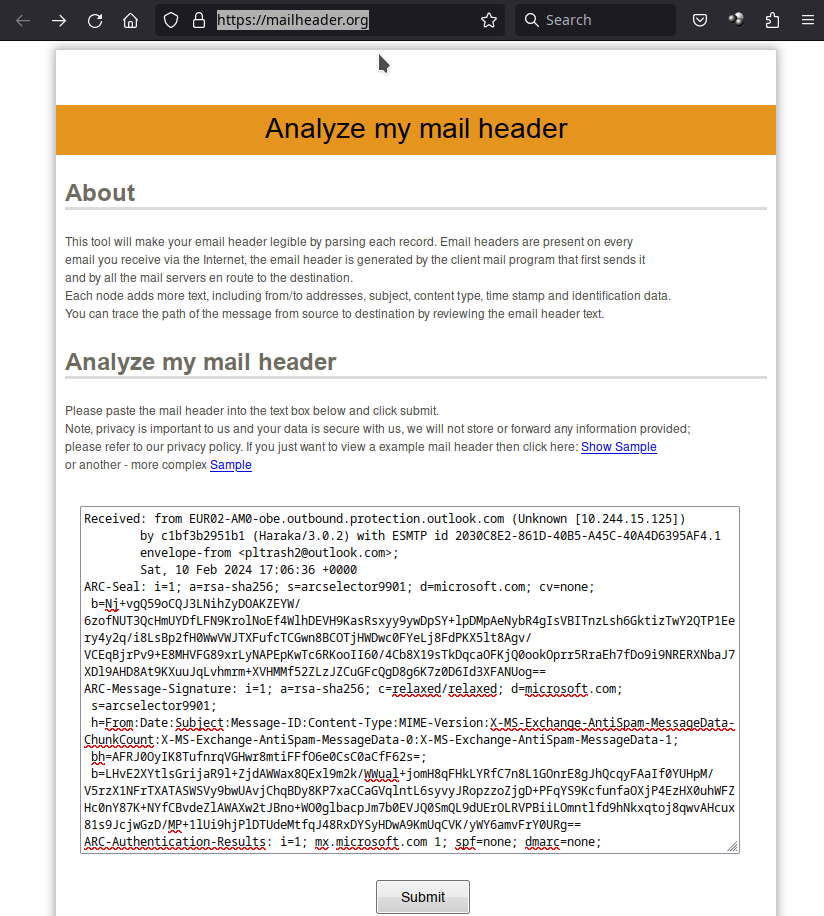
Go to <https://mha.azurewebsites.net/>, paste the headers in the upper window, click "***Analyze headers***", and look at the result. The various headers are isolated, and the Received headers are displayed in their 'right' chronological order.

Compare this image with the path we found in the second example above.

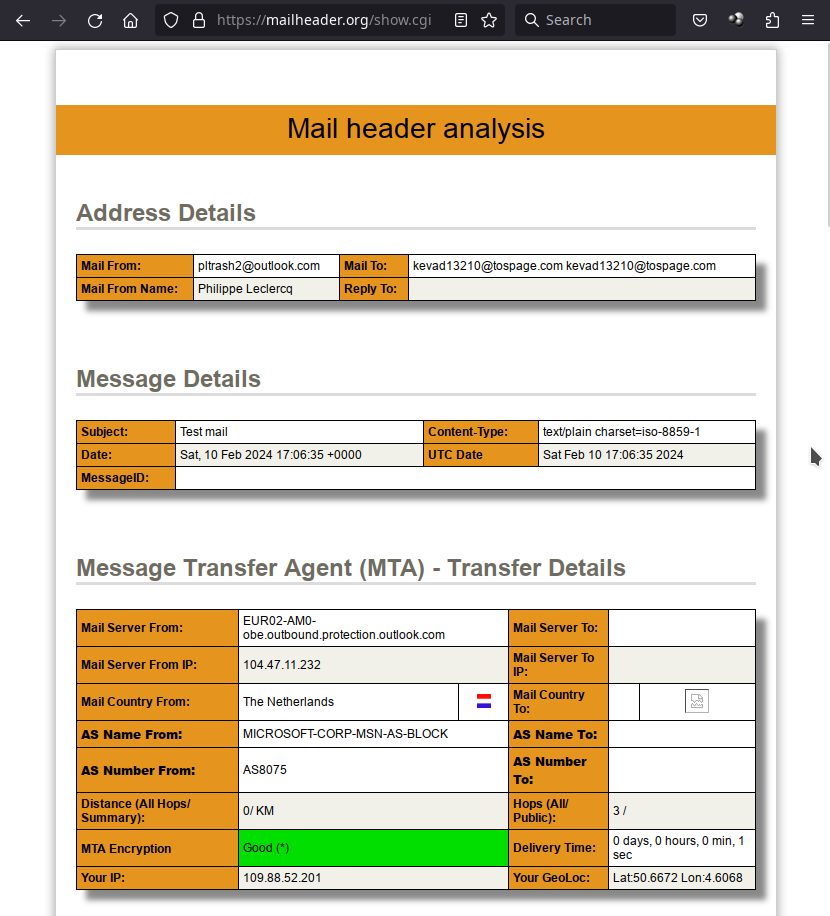
This is the most user friendly analyzer for a first experience.

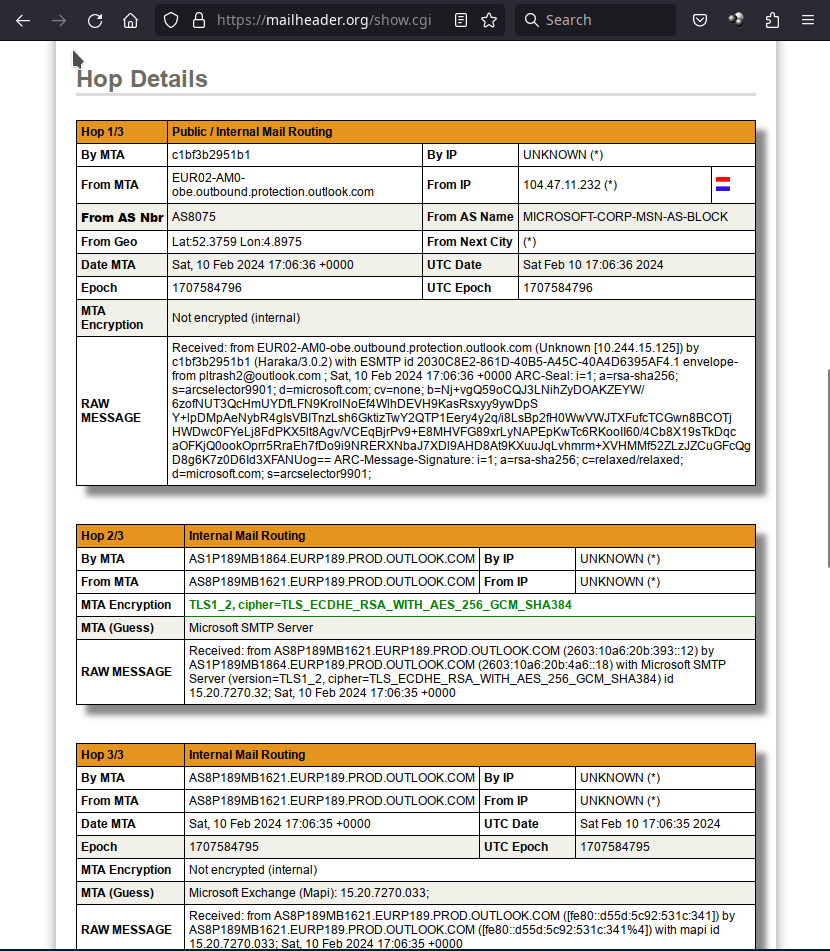
### Mailheader.org

Go to <https://mailheader.org/>, paste your header in the text box and press ***Submit***.



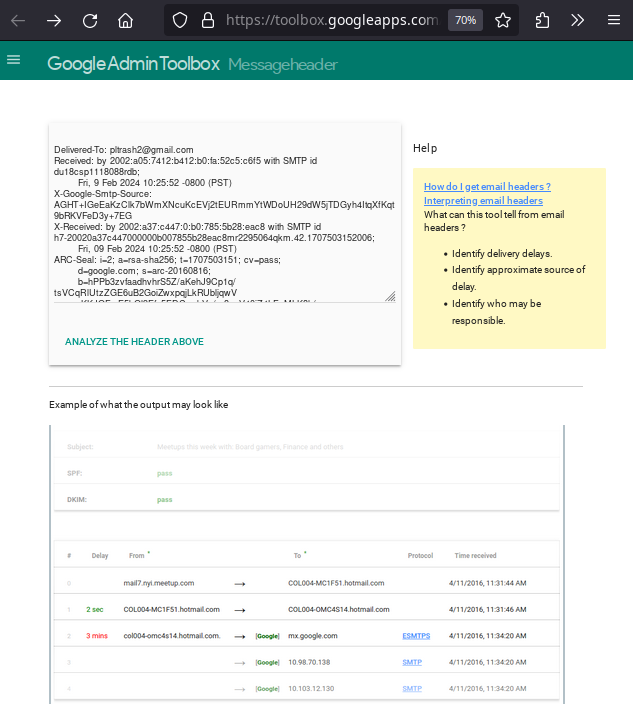
Wait a bit, and you will get a very detailed analysis of your headers, including the hop details (in the original REVERSE chronological order, though), and a deep analysis of various spam scoring, initial mail transfer agent...

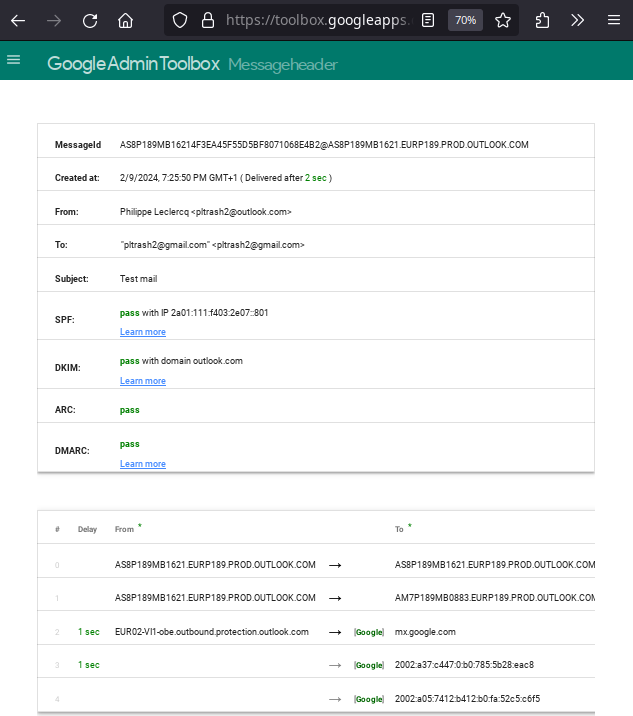


This is currently the best advanced online mail analyzer.

### Google Admin Toolbox Messageheader Tool

For Gmail users: go to <https://toolbox.googleapps.com/apps/messageheader>, paste the header in the upper window, and click on "***ANALYZE THE HEADER ABOVE***".

This will also order the hops chronologically.

Note that this tool tends to only work with mails received by Gmail.

## Conclusion

Decoding email and envelope headers, particularly the ***Received:*** headers, allows tracing the email journey and detecting potential fraudulent origin.