



Analyzing the email journey via the envelope headers

Received: headers

In a previous [article](#), 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 very simple email, sent directly from a workstation to a mail server running Postfix (open source mail server software), for a user having its 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/
6zofNUT3QcHmUYDfLFN9Kro1NoEf4WlhDEVH9KasRsxyy9ywDpSY+lpDMpAeNyBR4g
IsVBITnzLsh6GktizTwY2QTP1Eery4y2q/
i8LsBp2fH0WwVWJTxFufcTCGwn8BCOTjHWDwc0FYeLj8FdPKX51t8Agv/
VCEqBjrPv9+E8MHVFG89xrLyNAPEpKwTc6RKooII60/4Cb8X19sTkDqca0FKjQ0ook
```

Opr5RraEh7fDo9i9NRERXNbaJ7XD19AHD8At9KXuuJqLvhmrm+XVHMMf52ZLzJZCu
GFcQgD8g6K7z0D6Id3XFANUog==
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=AFRJ00yIK8TufnrqVGHwr8mtiFFf06e0CsC0aCfF62s=;
b=LHvE2XYt1sGrijaR9l+ZjdAWWax8QEx19m2k/
WWua1+jomH8qFHKLYRfC7n8L1G0nrE8gJhQcQyFAaIf0YUHpM/
V5rzX1NFrTXATASV9bwUAvjChqBDy8KP7xaCCaGVq1ntL6syvyJRopzzoZjgD+P
FqYS9Kcfunfa0XjP4EzHX0uhWFZHC0nY87K+NYfCBvdeZ1AWAXw2tJBno+W00glbac
pJm7b0EVJQ0SmQL9dUErOLRVPBi1LOmnt1fd9hNkxqtoj8qwwAHCux81s9JcJwGzD/
MP+11Ui9hjP1DTUdeMtfqJ48RxDYSyHDwA9KmUqCVK/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=AFRJ00yIK8TufnrqVGHwr8mtiFFf06e0CsC0aCfF62s=;
b=ULBWNbP9V1dJ0w9s4i9yG8r5jcUUjXkSkbcrR4m4Mbvor+Y4cDZB9H8T7e2vbyIx
5AI4WY20zjW1r2jqQpGOWPMJBTMqhet5gdPf/
eUvpCGszxkBIbo8X3eEm1ue8XXye09jUUn06wTUGvmY115DWefd1vGVNHTYAUZ40I
KQoLnchsAYLNjWRJaALj08BHWBg8piZpQL6f0PeQLfdMHNgMTjrX+1qVy1Xzqc1baD
XR75uJW81pkPe8w1BA7Ds1xsNRKxD5iXVFDp5BPA3t1XcjDe50h8RdyIzmCRSlzzsr
4ldRi2o0dyw7Tp8a9BZAVQMR4GwPn3zWSESaMs6R1fQ==
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/1+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-s1blob-mailprops:
ajlDcABzOp5vGNUQg9WyIGGBvourDcGtzrOV4dPOVU9n7Vpw/
ILwGR9QFjXxBX+EI73QUNMynRVU1YIKob4i0fnzjXFbqPTyedYr4l4GEDdQKllynzo
AlROwtTUqdUneiqN+bPiUgm/t5U58P/
FLypQTYvtlB8K0cNwIQmOxNNNq242pkA+fcI4QUvJgrkdCXPV2Y0FTPv/
JZpMioSPsnYZE1weiZmK71gx/tXNyApNUKkHtw8/
PeWHQmdEv2KknzewE1aojYg9VOPGzEL5KxkLvnnLeogkdAShUcyth+peSKs6B5qu1P
of/k6kxfBsh70JexN0GeDwOWCmNufn4bC8rK2VkmV/
8i0y2LINhMfZnWJTupBCIhaURdHh0R546kMFSkq4GpJIRH9x8tAm57Fenoz7Nwca8h
CcRUQlyEXHjwxlGZy8pHG/ubd0hRwsQHCUIWL/
cQd6iAWMDv9hqmoNsUvWeyLQfws2KLkVSNLjqehadUcZCu7VlSC6RxPn+eVErrbGjt
UE39cetBr7nRJvQUkixBr1gRCYjEuB3vC+Mp8Z0z99sdtGk08DE8AHFzINMT0ctu2Q
=
x-microsoft-antispam: BCL:0;
x-microsoft-antispam-message-info:
sz7Buq//
Pv1dj5r3czfKHNjHWwrQ1z01KAMVz+84IA7151XijwCTE49NWTjjSoYssRc0ZRCOM0
/VkwBV29pENCIK3/95WeGMVlRsJ09J/YktB12I19e5JV56y2hmn3ZHGBeo2/
1b8xEXR0SgozMnWPe0qPWKcLZ4neeXI9Vm6Fwhz/
cuS+jBrccusaqnJEvJHq7qhAfX5j7LpJWZb6bB3C9eQptmbjbmXG5xkkS1faPvfNSO
VI0I+eQYN+xFexSFVHHJYpozApqpAmsGDtOfLdVkp1WgIFL2zX1m1tTVGJUuAzWuyB
8VnSOah7pzkuwwmuAkJS8YZLkkmHQuHYOQWJGcjhAbUQtIU7z/x/X24wvtK/
NwLn8/ZP/FI/GMAjG/
pB71lLLqr0ZY2I+ps2rHrzMRF3kT0FS8G2+XttXeSxgj2w12ZrCpyZvobWVBcdBV00
gpCLq1iob31g9107sVVAGBtUSDKphscCsG8BA8JYAXijrJaVRwPiG1F7qNpJbWLiL8
peosJpdUFe4yHF/dB8DWeJF9v4iohi4ta4PggZzn+V41UH1cNpz5T1M+CXTh
x-ms-exchange-antispam-messagedata-chunkcount: 1
x-ms-exchange-antispam-messagedata-0:
=?iso-8859-1?Q?
QHINCZlcrnB7TvQ9sM9lDvmxH4U0PXsAPb4Zhh073E2+VoNf9QfZw0cKw0?=
=?iso-8859-1?Q?
mLTZJtHF5Q85acxshI430+wxgCCDKDlzz6ChVQzCf5h1cDDSN1uNg+ZmH3?=
=?iso-8859-1?Q?
u0+uY1FOGPt1dY+P37N2EMgG6MjELjxGSoNF0ep8F59zTXqbdETiUxXIyb?=
=?iso-8859-1?Q?
JuNOFYl31gtptBFY1qI0n18YFMH7sKS2Zok7nGnUABH0zLKEn+1pITvjRt?=

=?iso-8859-1?Q?
Rz1V2y8lEcWYJudiMgtxsqv1Ln0bLQ7WgFRJavWnu3WKmiE7HggA6mJd5W?=
=?iso-8859-1?Q?CqnRKcaf+RRCoZvI2xJBj/
pLlPagEz9qv0x0VztFpooAdENh7nxtxSXptF?=
=?iso-8859-1?Q?
vF0yZzVXGQVzkDDCnWDyFr13mtlFISZHQkiT5wut9azMHZ7YlnBy/aJ2WZ?=
=?iso-8859-1?Q?Nh3MBDxooNhA9/
yFVG7aPY4i2RVNVzWgSOLG1NY4iNEfBEM9d+pjyKPI2G?=
=?iso-8859-1?Q?wHdPl/
zrDB6Y8GauCTgtDK1A6oA0AiPiqveW8ZwLp7Mwr9SJg3dwvhP6ee?=
=?iso-8859-1?Q?
TXyHS+Tgt2wQ5ICJ6IIbBmeT59VLASNDvsgNJI7fk6bfr9isf4rAQ3Wp6f?=
=?iso-8859-1?Q?3tauHQny5tpfM6Lw+FbPx6T5iwKt3vdH14/
OGmMMh+S+OzA11Ce2vb+K7e?=
=?iso-8859-1?Q?
ye04Tk1T9Rw4DiqJhiHwCpuLWnSG8Lgg+PuLddrCiIasdbCDg03Ux8vP3A?=
=?iso-8859-1?Q?
9mH2dRbSu7nt1GULqRfI66kk1AqWsYF2t9YQXMiD11SsIit4uCyHfCYCL4?=
=?iso-8859-1?Q?
C4Mw025zoXSIjhm+i2XQ8JFtf1KbeonZyEH7rMP310EsK6cb4p8H1ZGP4p?=
=?iso-8859-1?Q?xU0o0WpAf/xXZHu9j/
OnBf6Ha8L3E10ETuNUTrDoa0VdbmDJmNsBQ1CJRr?=
=?iso-8859-1?Q?
yqnU3qXcR3PsSvHr6xJ3thXrCbKtntVgL5yc6Y7MBus7CuCzwPHSTpLZw6?=
=?iso-8859-1?Q?
CCakfNSRiCWzCLZBBjGx0vgOMeMGgRqbdsjSE1A7bBFiq4474AhzeH8L8z?=
=?iso-8859-1?Q?
rZBMxABW1QMb2NhPKfLRvZ+ig5JIKJ+IJ1jznWaPqATS5hZ7YbZUHaAdLP?=
=?iso-8859-1?Q?
kE2a6cf1fyXxh1nwLMu6UhgdIxPYQAo7RHcyqX1SMC4CHudgZ3cKdLaopT?=
=?iso-8859-1?Q?DwZmRyDR4bZza8ag5iyu0LAeIlqmi4iR/
cc0QV8uemRbk0WaHTu6Hvr05E?=
=?iso-8859-1?Q?OrWXUtFg3WBHr5EA4682aTKPijC3/
RoRrfRr3shCDbav+TJ4rxFfcxtKmB?=
=?iso-8859-1?Q?
b7jgRh1z2AQj7QhtKNzm24wg1mbZS79yschIPMU3y2viYrDDkCPEAq3C2W?=
=?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-aaaaaaaaaaaaa
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.

The screenshot shows the Microsoft Message Header Analyzer web application. The top section is a text input area where the email header has been pasted. Below this, there are buttons for "Analyze headers", "Clear", and "Copy". The "Analyze headers" button has been clicked, and the results are displayed in a structured format.

Summary

Subject: Test mail
Message Id: <AS8P189MB1621A0A78523CB097358B05D8E4A2@AS8P189MB1621.EURP189.PROD.OUTLOOK.COM>
Creation time: Sat, 10 Feb 2024 17:06:35 +0000 (Delivered after 1 second)
From: Philippe Leclercq <pltrash2@outlook.com>
To: "kevad13210@tospage.com" <kevad13210@tospage.com>

Received headers

Hop	Submitting host	Receiving host	Time	Delay	Type
1	AS8P189MB1621.EURP189.PROD.OUTLOOK.COM (ffe80:d55d:5c92:531c:3411)	AS8P189MB1621.EURP189.PROD.OUTLOOK.COM (ffe80:d55d:5c92:531c:3411%4)	2/10/2024 6:06:35 PM		mapl
2	AS8P189MB1621.EURP189.PROD.OUTLOOK.COM (2603:10a6:20b:393::12)	AS1P189MB1864.EURP189.PROD.OUTLOOK.COM (2603:10a6:20b:4a6::18)	2/10/2024 6:06:35 PM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
3	EUR02-AM0-obe.outbound.protection.outlook.com (Unknown [10.244.15.125])	c1bf3b2951b1 (Haraka/3.0.2)	2/10/2024 6:06:36 PM	1 second	ESMTP

Microsoft Antispam Header

Bulk Complaint Level: 0
Source header: BCL:0

Other headers

#	Header	Value
1	ARC-Selector	i=1; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cy=none; b=Nj+vgQ59oCQJ3LNIhZyDOAKZEYw6zofNUt3QcHmUYDILFN9KrollNoE4WihDEVH9KasRxsyy9ywDpSY+lpDMPAeNybR4glsVBItNzsh6GktzTwY2QTP1Eery4y2q/i8LsBp2fH0WwVWJTXFufcTCGwn8BCOTJHWDwc0FYeLj8fDPKX5t8Agv/VCEqBjPv9+E8MHVFG89xrlYNAPEpKwTc6RKooli60/4Cb8X19sTKDqcaOFKjQ0ookOpr5RraEh7fDo9i9NRERXNbaJ7XD9AH0D8A9KXuuJqLvhmm+XVHMM52ZLzJZCuGfCqgD8g6K7z0D6ld3XFANUog==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; b=AFRj00yK8TuhqVGHw8miffFOe9C3C0aCf62s+; b=LHvE2Xy8GjaR9+ZdAWWax8QEx9m2kVWUg+JomH8qFHkLYRfC7n8L1GOnrE8gJhQcayFaalf0YUHpM/V5rZx1NfTXATASVSYy9bwUAvjChqBDy8KP7aCcaGVqlnL6syyvJRoPzzoZjpD+PFqYS9KctunfaOXjP4EzH0uhWFZHC0nY87K+NYfCvdeZiAWAxw2UjBno+WO0gibacpJm7b0EVJQ0Sml9dUeOLRVPBilOmtf9hNkxqtoJ8qwwAHcux81s9UjwGzDMP+1IU9hjPDTUdeMtfqJ48RxDYSyHDwA9KmUqCVKYWY6amvFryOURg==

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.

← → ↺ 🏠 🛡️ <https://mailheader.org> ☆ 🔍 Search 📧 🔄 📁 ☰

Analyze my mail header

About

This tool will make your email header legible by parsing each record. Email headers are present on every email you receive via the Internet, the email header is generated by the client mail program that first sends it and by all the mail servers en route to the destination.

Each node adds more text, including from/to addresses, subject, content type, time stamp and identification data. You can trace the path of the message from source to destination by reviewing the email header text.

Analyze my mail header

Please paste the mail header into the text box below and click submit.

Note, privacy is important to us and your data is secure with us, we will not store or forward any information provided; please refer to our [privacy policy](#). If you just want to view a example mail header then click here: [Show Sample](#) or another - more complex [Sample](#)

```
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/
6zofNUT3QcHmUYDFLFN9KrolNoEf4WlhDEVH9KasRxsxy9ywDpSY+lpDMPAeNybR4gIsVBITnzLsh6GktizTwY2QTP1Ee
ry4y2q/i8LsBp2fH0WwVJTXFufcTCGwn8BCOTjHWDwc0FyElj8FdPKX5lt8Agv/
VCEqBjrPv9+E8MHVFG89xrLyNAPEpKwTc6RKooII60/4Cb8X19sTkDqca0FKjQ00ok0pir5RiaEh7fDo9i9NRERXNbaJ7
XD19AHD8At9KXuuJqLvhmzm+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=AFRj00yIK8TufnrqVGHwr8mtiFF06e0CsC0aCff62s=;
  b=LHvE2XYtIsGrijaR9l+ZjdAWWax8QEx19m2k/WWual+jomH8qFHkLYRfC7n8L1G0nrE8gJhQcqyFAaIf0YUHpM/
V5rzX1NFITXATASWSVy9bwUAvjChqBDy8KP7xaCCaGVqIntL6syvyJRopzzoZjgD+PFqYS9Kcunfa0XjP4EzHX0uhWFZ
Hc0nY87K+NYfCBvdeZlAWAXw2tJBno+W00glbacpJm7b0EVJQ05mQL9dUEr0LRVPBiiL0mntlfd9hNkxqtoj8qvvAHCux
81s9JcjwGZD/MP+1lUi9hjP1DTUdeMtfqJ48RxDYsyHDwA9KmUqCVK/yWY6amvFrY0URg==
ARC-Authentication-Results: i=1; mx.microsoft.com 1; spf=none; dmarc=none;
```

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...

← → ↺ 🏠 🛡️ 🔒 https://mailheader.org/show.cgi ⌨️ ☆ 🔍 Search 📧 🌐 📌 ☰

Mail header analysis

Address Details

Mail From:	pltrash2@outlook.com	Mail To:	kevad13210@tospage.com kevad13210@tospage.com
Mail From Name:	Philippe Leclercq	Reply To:	

Message Details

Subject:	Test mail	Content-Type:	text/plain charset=iso-8859-1
Date:	Sat, 10 Feb 2024 17:06:35 +0000	UTC Date	Sat Feb 10 17:06:35 2024
MessageID:			

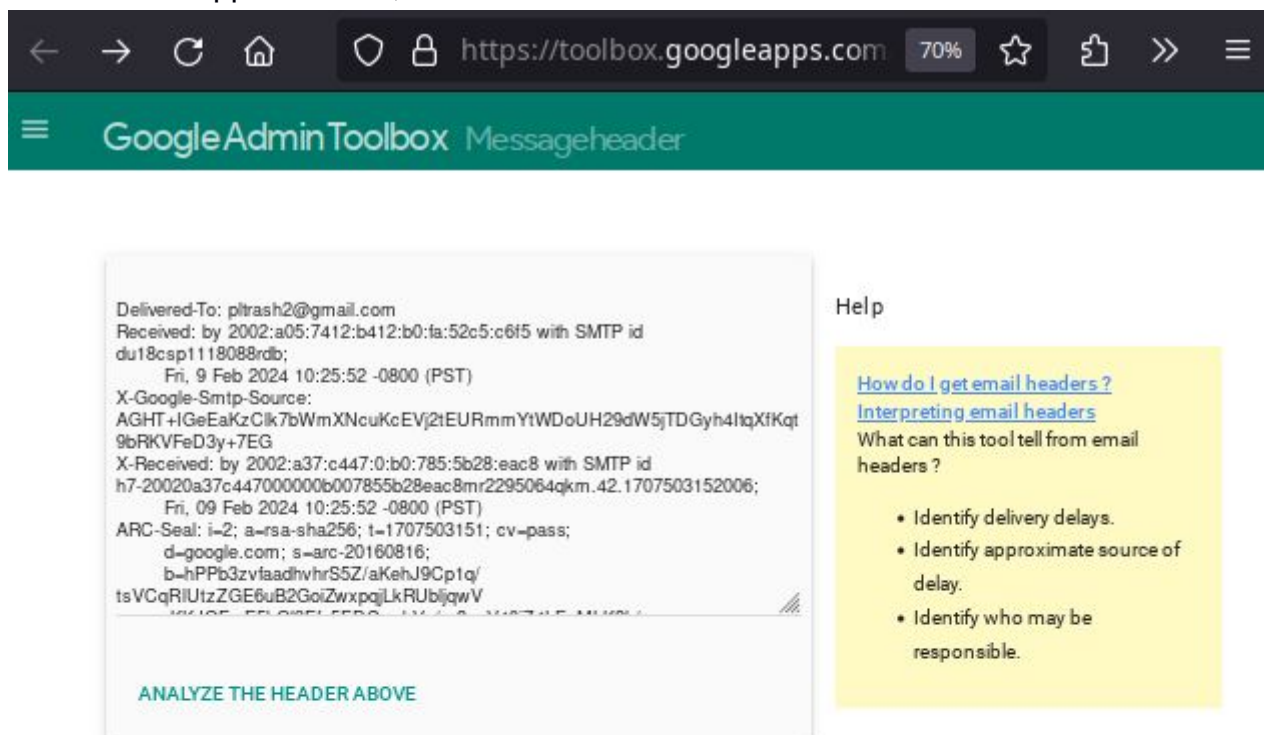
Message Transfer Agent (MTA) - Transfer Details

Mail Server From:	EUR02-AM0-obe.outbound.protection.outlook.com	Mail Server To:	
Mail Server From IP:	104.47.11.232	Mail Server To IP:	
Mail Country From:	The Netherlands 🇳🇱	Mail Country To:	🇺🇸
AS Name From:	MICROSOFT-CORP-MSN-AS-BLOCK	AS Name To:	
AS Number From:	AS8075	AS Number To:	
Distance (All Hops/Summary):	0/ KM	Hops (All/Public):	3 /
MTA Encryption	Good (*)	Delivery Time:	0 days, 0 hours, 0 min, 1 sec
Your IP:	109.88.52.201	Your GeoLoc:	Lat:50.6672 Lon:4.6068

This is currently the best advanced online mail analyzer.

Google Admin Toolbox Messageheader Tool

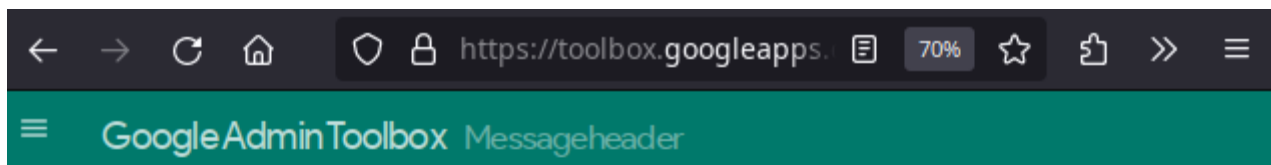
For Gmail users: go to <https://toolbox.googleapps.com/apps/messageheader>, paste the header in the upper window, and click on "ANALYZE THE HEADER ABOVE".



Example of what the output may look like

Subject: Meetups this week with: Board games, Finance and others						
SPF: pass						
DKIM: pass						
#	Delay	From *		To *	Protocol	Time received
0		mail7.ny1.meetup.com	→	COL004-MC1F51.hotmail.com		4/11/2016, 11:31:44 AM
1	2 sec	COL004-MC1F51.hotmail.com	→	COL004-OMC4S14.hotmail.com		4/11/2016, 11:31:46 AM
2	3 mins	col004-omc4s14.hotmail.com	→	[Google] mx.google.com	ESMTPS	4/11/2016, 11:34:20 AM
3			→	[Google] 10.98.70.138	SMTP	4/11/2016, 11:34:20 AM
4			→	[Google] 10.103.12.130	SMTP	4/11/2016, 11:34:20 AM

This will also order the hops chronologically.



MessageId	AS8P189MB16214F3EA45F55D5BF8071068E4B2@AS8P189MB1621.EURP189.PROD.OUTLOOK.COM
Created at:	2/9/2024, 7:25:50 PM GMT+1 (Delivered after 2 sec)
From:	Philippe Leclercq <pltrash2@outlook.com>
To:	"pltrash2@gmail.com" <pltrash2@gmail.com>
Subject:	Test mail
SPF:	pass with IP 2a01:111:f403:2e07::801 Learn more
DKIM:	pass with domain outlook.com Learn more
ARC:	pass
DMARC:	pass Learn more

#	Delay	From *		To *
0		AS8P189MB1621.EURP189.PROD.OUTLOOK.COM	→	AS8P189MB1621.EURP189.PROD.OUTLOOK.COM
1		AS8P189MB1621.EURP189.PROD.OUTLOOK.COM	→	AM7P189MB0883.EURP189.PROD.OUTLOOK.COM
2	1 sec	EUR02-VI1-obe.outbound.protection.outlook.com	→	[Google] mx.google.com
3	1 sec		→	[Google] 2002:a37:c447:0:b0:785:5b28:eac8
4			→	[Google] 2002:a05:7412:b412:b0:fa:52c5:c6f5