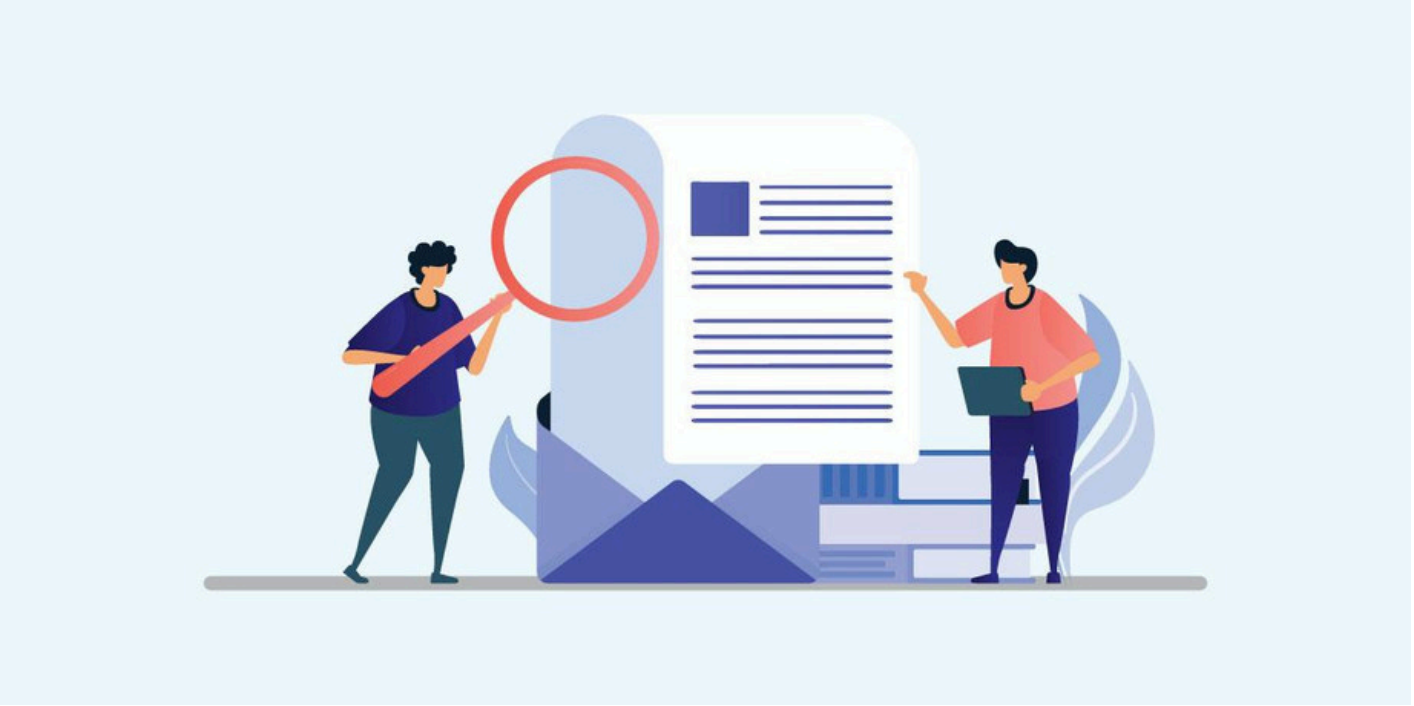
How to trace an email address



The existence of the Internet has radically transformed our daily lives. It is hard to imagine a time before the Internet revolution. So many services are easily available at our fingertips, thanks to the Internet.

With a few clicks and some typing, you can pay your bills, apply for loans, connect with people globally and so much more. Work productivity has skyrocket due to the ease of collaboration with colleagues and customers. Families can keep in touch using apps or websites, via email or chat or video calls.

The benefits are tremendous but there are those who seek to abuse the Internet such as scammers. Often, you hear stories of people falling prey to online scams, usually via forged or phishing emails. Another bane of the Internet is spam emails, not to mention the viruses that can arrive in your email inbox.

Why email address tracing is a necessity

Email is a wonderful invention and made life easier for people in their lives and work. Before the advent of email and the Internet, you would need to make phone calls if you need to contact someone. Either that, or you need to send snail mails or faxes to send someone a message or information.

Alas, with all things, there are upsides and downsides to email. Scammers also find it easier to reach their victims with emails. Scam and phishing emails are clogging everyone's inbox on a daily basis.
This is why email address header tracing is an important tool to find out who is sending those emails. With the IP address of the culprit, you can file an abuse complaint with the respective ISP or email providers.

What is email header?

Email headers are snippets of metadata that can be found inside every email you send or receive. Starting with the email client that sent out the email, these bits of info are tagged into each email. As the email travels through the Internet via various email servers or relays, more info is appended to the headers at each hop along the way to the destination.

Headers are normally not visible to the email recipients as they are only useful in certain circumstances like troubleshooting email delivery issues. The headers should include info like the IP address of the sender, email's route, content type, dates/timestamps, etc.

How to view the email header

As mentioned above, email headers are hidden by default in most email clients. Follow the below steps to unveil the email headers for your email clients. The Gmail, Microsoft Outlook, Yahoo, Outlook.com examples are shown below.

Gmail

1. Open the email that you want to view the headers.
2. Click the **More icon** next to the Reply icon.
3. Select **Show Original**.
4. A new window with the full headers and HTML source of the email will be opened.

Microsoft Outlook

1. Double-click an email message to open it outside of the Reading Pane.
2. Click **File** > **Properties**.
3. Headers will be displayed within the **Internet Headers** area in a new dialog box.

Outlook.com

1. Open the email that you want to view the headers.
2. Click the **More icon** and then select **View**.
3. Select **View message source**.
4. A new dialog box with the full headers and HTML source of the email will be opened.

Yahoo Mail New Version

1. Open the email that you want to view the headers.
2. Click the **More icon** and then select **View Raw Message**.
3. A new window with the full headers and HTML source of the email will be opened.

Yahoo Mail Classic Version

1. Open the email that you want to view the headers.
2. Select **Raw Message**.
3. A new window with the full headers and HTML source of the email will be opened.

For more info, please see https://www.ip2location.com/how-to-get-email-header.

Let’s breakdown the meaning of the data fields inside the email header

After you’ve gotten your header from your email client, you can take a close look at the various fields there. Check out this example header from a Gmail account.

```
Delivered-To: example@gmail.com
Received: by 2002:a5d:4b4c:0:0:0:0:0 with SMTP id w12csp303514wrs;
        Wed, 14 Dec 2022 07:58:57 -0800 (PST)
X-Google-Smtp-Source: AA0mqf7pEjHSwSKT5mAqYYFU8WgRF+X4WprbxGDHqKTHAGs05eoJPGPcthaW783FGBtnsroM+dmF
X-Received: by 2002:a0c:fe89:0:b0:4c7:5c88:8f54 with SMTP id d9-20020a0cfe89000000b004c75c888f54mr34965057qvs.45.1671033537288;
        Wed, 14 Dec 2022 07:58:57 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1671033537; cv=none;
        d=google.com; s=arc-20160816;
        b=R0IJRidVmciByAxoWoclpwHcUSOmPoH0aSiEZwk/6J4cJBOd9BJ5Ptx+f+Bs6IvosW
         IfSaCGYwPc5MFKkAsAOmnytH956YJHPTZ7v1jUF5eWxrYpeDcYH1X21SrNDcJjj6cGcE
         oWIZSg5eEi/1a4/j6wPJBblz6+et+lcL76o/75/1nFZnHu7WnhrpZZU5mSLFbSSW648U
         zcmBHxiLffh6AL2/BMFlw49jTEqM0rKhxtzMNLnzRWDD86nC/28p/fLiie+M+qTQax1a
         P25u4Gs4tunfVt1Ds/3rDDbJr76e+QzkhHNdkDrAJMG9sVmwocsBS0OOMak2LtkhjUeC
         l2og==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=content-transfer-encoding:message-id:to:from:subject:mime-version
         :date:sender:dkim-signature:dkim-signature;
        bh=7XqAp7Sh3UzqHI8tqjSXgcimcbfrpd8auRT/JbnECds=;
        b=HfHmCy6Tl0MXp6IAdLK04JmAG7QS6J63Bd6RTS6dXxfDsZbtnLtLgqDKNObYm4Y+bZ
         Gk0qEvh15S+T8ETRoGp+kwmt/8IlqJTlz4RE3Cw9vTcxJqXFpvEGuK6VXoKcSDiKj3t8
         FpXaWcSQsVt5Ka7fgkYUP33/gQ9Dbin1ZU1r5BheE8oc7T0rZjv4gb6c8OZ9IHIe9Gh4
         d0vx7mUm38isFulGnD2QBccHO88+6qilx2/x0NTagFzbL9YsbsrYOWnI/vRUe5XZwGtg
         IA22PezaGLwP0abwhIWQbgavhfbIq8jzW7DjCrZmKECVNdsoEb/jZZj5FFxU9YOQprIg
         SjtQ==
ARC-Authentication-Results: i=1; mx.google.com;
        dkim=pass header.i=@n.dribbble.com header.s=mailo header.b=mEIEKOMh;
        dkim=pass header.i=@mailgun.org header.s=mg header.b=O7zfEAkN;
        spf=pass (google.com: domain of bounce+f60f75.d62726-example=gmail.com@n.dribbble.com designates 69.72.39.54 as permitted sender) smtp.mailfrom="bounce+f60f75.d62726-example=gmail.com@n.dribbble.com";
        dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=n.dribbble.com
Return-Path: <bounce+f60f75.d62726-example=gmail.com@n.dribbble.com>
Received: from m39-54.mailgun.net (m39-54.mailgun.net. [69.72.39.54])
        by mx.google.com with UTF8SMTPS id jx11-20020a0562142b0b00b004c6798d73a2si54107qvb.378.2022.12.14.07.58.53
        for <example@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
        Wed, 14 Dec 2022 07:58:57 -0800 (PST)
Received-SPF: pass (google.com: domain of bounce+f60f75.d62726-example=gmail.com@n.dribbble.com designates 69.72.39.54 as permitted sender) client-ip=69.72.39.54;
Authentication-Results: mx.google.com;
        dkim=pass header.i=@n.dribbble.com header.s=mailo header.b=mEIEKOMh;
        dkim=pass header.i=@mailgun.org header.s=mg header.b=O7zfEAkN;
        spf=pass (google.com: domain of bounce+f60f75.d62726-example=gmail.com@n.dribbble.com designates 69.72.39.54 as permitted sender) smtp.mailfrom="bounce+f60f75.d62726-example=gmail.com@n.dribbble.com";
        dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=n.dribbble.com
DKIM-Signature: a=rsa-sha256; v=1; c=relaxed/relaxed; d=n.dribbble.com; q=dns/txt; s=mailo; t=1671033533; x=1671040733; h=Content-Transfer-Encoding: Content-Type: Message-Id: To: To: From: From: Subject: Subject: Mime-Version:
Date: Sender: Sender: X-Feedback-Id; bh=7XqAp7Sh3UzqHI8tqjSXgcimcbfrpd8auRT/JbnECds=; b=mEIEKOMhfg801fwxPJdmkzxGHYpW9MgqbUC1Lv5XOswPJrTJaAuaq6S2FHjztXqzbGbPTfLf /4cQdw8vttY3M3y5v0uDn3995u0HWVPYISne
3UGUPc6bDtxBoB4xsPixAMc+jFZWNrP+yjAx VU8xCeJ0SaOCdX4IXtlaW5WZITw=
DKIM-Signature: a=rsa-sha256; v=1; c=relaxed/relaxed; d=mailgun.org; q=dns/txt; s=mg; t=1671033533; x=1671040733; h=Content-Transfer-Encoding: Content-Type: Message-Id: To: To: From: From: Subject: Subject: Mime-Version:
Date: Sender: Sender: X-Feedback-Id; bh=7XqAp7Sh3UzqHI8tqjSXgcimcbfrpd8auRT/JbnECds=; b=O7zfEAkNmzmDQfuWdcIsr41T+uYwHWZ5mymzNN55zB1yvO4GdKZ/Cg2dYeP3R1s/1g1QzZtC zQYvBwNdYt1NS8ejJ1+Q2R/5Bgmnm
KiOrQlWZjr31i0J7tRoE6aD5MLixMTNRtSNywurXUnw 2FlhhEXTlhz8AnY4bk0tAHUBHtl=
X-Feedback-Id: 5e3ca0717add368f8a907820:mailgun
X-Mailgun-Sending-Ip: 69.72.39.54
X-Mailgun-Sid: WyIyMjRhYyIsIm15cmFmdWxsZXIyNEBnbWFpbC5jb20iLCJkNjI3MjYiXQ==
Received: from <unknown> (<unknown> []) by cd23d2332c6a with HTTP id 6399f2bc6a8bf0b4939958dc; Wed, 14 Dec 2022 15:04:40 GMT
X-Mailgun-Batch-Id: 6399e60822943ecb107b26bb
Sender: no-reply@n.dribbble.com
Date: Wed, 14 Dec 2022 15:04:40 +0000
Mime-Version: 1.0
Subject: Graphic design or visual design? ☒
From: Dribbble <no-reply@n.dribbble.com>
To: example@gmail.com
X-Mailgun-Tag: event-insider
X-Mailgun-Tag: broadcasts
X-Mailgun-Tag: insider
X-Mailgun-Deliver-By: Wed, 14 Dec 2022 15:58:52 +0000
Message-Id: <eb3d6fd8-248c-412f-95b5-48b3c0764ae1@n.dribbble.com>
X-Entity-ID: U0hEckoa/3R78nzLLCaPig==
Content-Type: multipart/alternative; boundary="141cb4ee1c5501184cef36d1d52f1a37"
```

- **Delivered-To:** Displays the email recipient's information.
- **X-Google-Smtp-Source:** Shows the email transferring using a Gmail SMTP server.
- **X-Received:** Displays message received at the first server.
- **ARC-Seal:** Seals the ARC authentication results and the message signature.
- **ARC-Message-Signature:** The signature takes a snapshot of the message header information for validation.
- **ARC-Authentication-Results:** Stands for Authenticated Receive Chain. It is an authentication standard which verifies the identities of the email intermediaries and servers that forward email message to its final destination.
- **Return-Path:** The location where non-send or bounce messages end up.
- **Received:** The "Received" line lists each mail server that the email travels through before hitting recipient's inbox. The mail server on the top line is the last server the email went through and the bottom line is where the email originated.
- **Received-SPF:** Stands for Sender Policy Framework which authenticates email to stop sender address forgery.
- **Authentication-Results:** Contains a record of the authentication checks carried out.

- **DKIM-Signature:** Stands for DomainKeys Identified Mail which authenticates the email domain sent.
- **MIME-Version:** Stands for Multipurpose Internet Mail Extensions. It is the standard email format which allows various media attachments to the email.
- **From:** Indicates the email sender details.
- **To:** Indicates the email recipient details.
- **Message ID:** Indicates the unique ID that identifies the email.
- **Content-type:** Indicates whether the format of an email was HTML, TXT, or any other option.

Steps to trace the origin of the email

So, now let's trace the origin of the email and see what information we can glean from it. Copy the email headers from your email client and paste it into the Email Headers text box in https://www.ip2location.com/free/email-tracer then click on LOOKUP.

You will see the results as below:

With the IP address found inside the header, it is possible to retrieve its geolocation data. IP2Location data can show the geolocation information like country, region, city, ISP, area code, ZIP code, usage type and so much more.