Ex. No 4: Analyze email headers and detect email spoofing using Mail Header Analyzer

AIM:

To analyze email headers and detect possible spoofing or malicious activity using Mail Header Analyzer.

Requirements:

- Mail Header Analyzer tool
- Any email client (Gmail/Outlook/Yahoo) with suspicious email samples

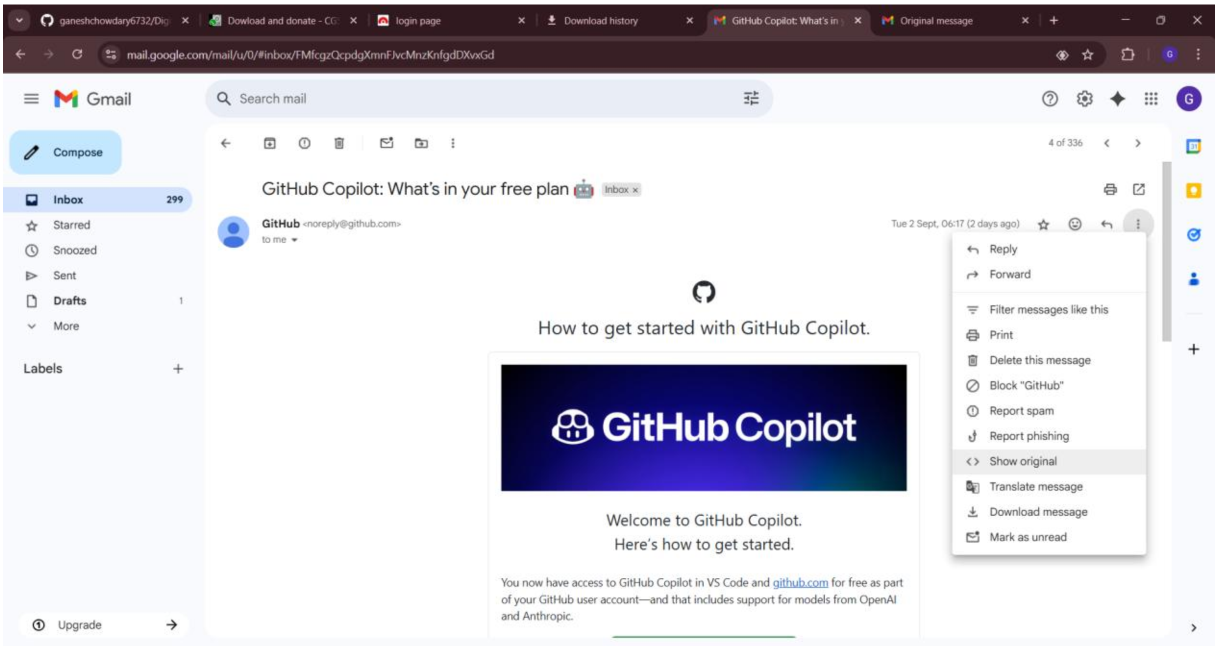
Description:

An email header contains routing information, including sender, recipient, subject, and most importantly, the path the email took across servers. Attackers often forge headers to trick recipients called email spoofing.

By analyzing headers, we can identify:

- Real sender IP address
- Authentication results (SPF, DKIM, DMARC)
- Time delays between servers
- Signs of spoofing/phishing

Step-1: First get the email header for that open the gmail, select the mail and click the three dots, choose the show original



mail.google.com/mail/u/0/#inbox/FMfcgzQcpdgXmnFJvcMnzKnfgdDXvxGd

GitHub Copilot: What's in your free plan 🤖

GitHub <noreply@github.com>
to me

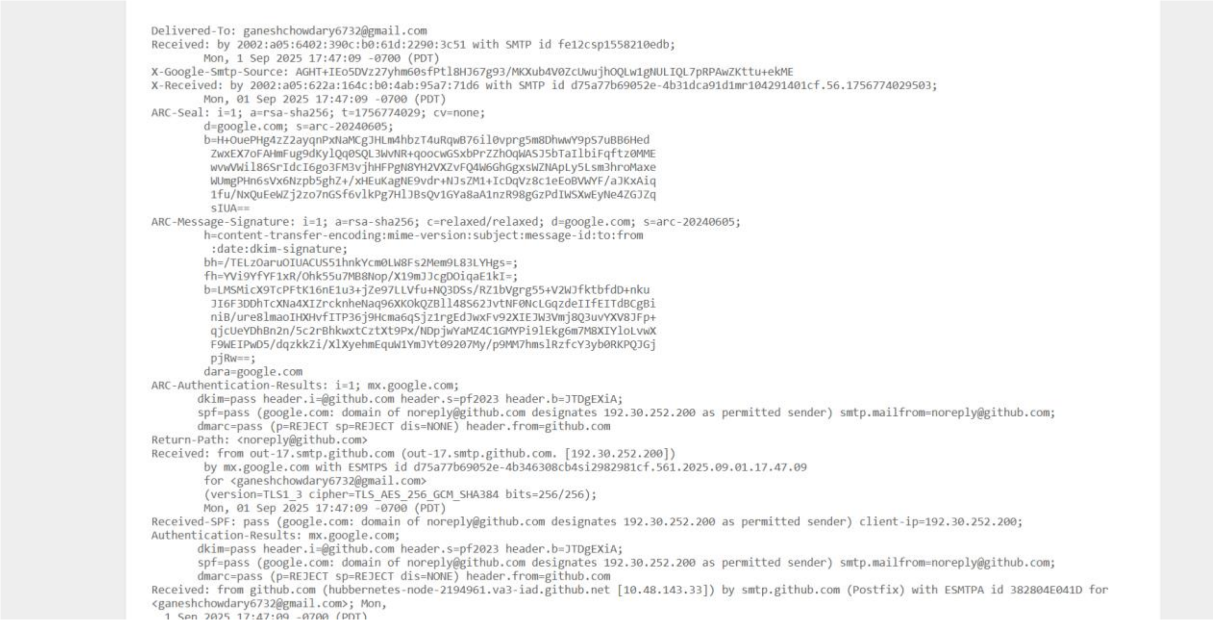
Tue 2 Sept, 06:17 (2 days ago)

How to get started with GitHub Copilot.

Welcome to GitHub Copilot.
Here's how to get started.

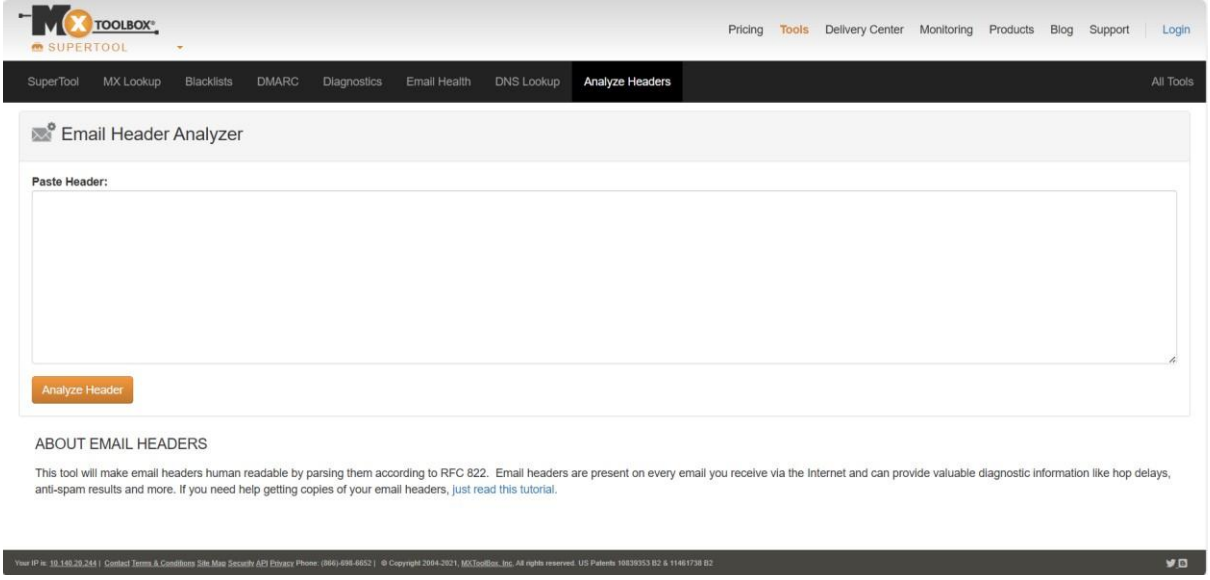
You now have access to GitHub Copilot in VS Code and github.com for free as part of your GitHub user account—and that includes support for models from OpenAI and Anthropic.

Step-2: Click the show original then you will see the original message with sender and receiver details



```
Delivered-To: ganeshchowdary6732@gmail.com
Received: by 2002:a05:6402:390c:b0:61d:2290:3c51 with SMTP id fe12csp1558210edb;
        Mon, 1 Sep 2025 17:47:09 -0700 (PDT)
X-Google-Smtp-Source: AGHT+IEo5DVz27yhm60sfPtl8HJ67g93/MKXub4V0ZcUwujhOQLw1gNULIQL7pRPAwZKttu+ekME
X-Received: by 2002:a05:622a:164c:b0:4ab:95a7:71d6 with SMTP id d75a77b69052e-4b31dca91d1mr104291401cf.56.1756774029503;
        Mon, 01 Sep 2025 17:47:09 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1756774029; cv=none;
        d=google.com; s=arc-20240605;
        b=H+OuePHg4zZ2ayqnPxNaMCgJHLm4hbzT4uRqwB76il0vprg5m8DhwwY9pS7uBB6Hed
         ZwxEX7oFAHmFug9dKylQq0SQL3WvNR+qoocwGSxbPrZZhOqWASJ5bTaIlbiFqftz0MME
         wvwVWil86SrIdcI6go3FM3vjhHFPgN8YH2VXZvFQ4W6GhGgxsWZNApLy5Lsm3hroMaxe
         WUmgPHn6sVx6Nzpb5ghZ+/xHEuKagNE9vdr+NJsZM1+IcDqVz8c1eEoBVWYF/aJKxAiq
         1fu/NxQuEeWZj2zo7nGSf6vlkPg7HlJBsQv1GYa8aA1nzR98gGzPdIWSXwEyNe4ZGJZq
         sIUA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605;
        h=content-transfer-encoding:mime-version:subject:message-id:to:from
         :date:dkim-signature;
        bh=/TELzOaruOIUACUS51hnkYcm0LW8Fs2Mem9L83LYHgs=;
        fh=YVi9YfYF1xR/Ohk55u7MB8Nop/X19mJJcgDOiqaE1kI=;
        b=LMSMicX9TcPFtK16nE1u3+jZe97LLVfu+NQ3DSs/RZ1bVgrg55+V2WJfktbfdD+nku
         JI6F3DDhTcXNa4XIZrcknheNaq96XKOkQZBll48S62JvtNF0NcLGqzdeIIfEITdBCgBi
         niB/ure8lmaoIHXHvfITP36j9Hcma6qSjz1rgEdJwxFv92XIEJW3Vmj8Q3uvYXV8JFp+
         qjcUeYDhBn2n/5c2rBhkwxtCztXt9Px/NDpjwYaMZ4C1GMYPi9lEkg6m7M8XIYloLvwX
         F9WEIPwD5/dqzkkZi/XlXyehmEquW1YmJYt09207My/p9MM7hmslRzfcY3yb0RKPQJGj
         pjRw==;
        dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@github.com header.s=pf2023 header.b=JTDgEXiA;
       spf=pass (google.com: domain of noreply@github.com designates 192.30.252.200 as permitted sender) smtp.mailfrom=noreply@github.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=github.com
Return-Path: <noreply@github.com>
Received: from out-17.smtp.github.com (out-17.smtp.github.com. [192.30.252.200])
        by mx.google.com with ESMTPS id d75a77b69052e-4b346308cb4si2982981cf.561.2025.09.01.17.47.09
        for <ganeshchowdary6732@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Mon, 01 Sep 2025 17:47:09 -0700 (PDT)
Received-SPF: pass (google.com: domain of noreply@github.com designates 192.30.252.200 as permitted sender) client-ip=192.30.252.200;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@github.com header.s=pf2023 header.b=JTDgEXiA;
       spf=pass (google.com: domain of noreply@github.com designates 192.30.252.200 as permitted sender) smtp.mailfrom=noreply@github.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=github.com
Received: from github.com (hubbernetes-node-2194961.va3-iad.github.net [10.48.143.33]) by smtp.github.com (Postfix) with ESMTPA id 382804E041D for
<ganeshchowdary6732@gmail.com>; Mon,
  1 Sep 2025 17:47:09 -0700 (PDT)
```

Step-3: Use Mail Header Analyzer tool for easy reading and analysis

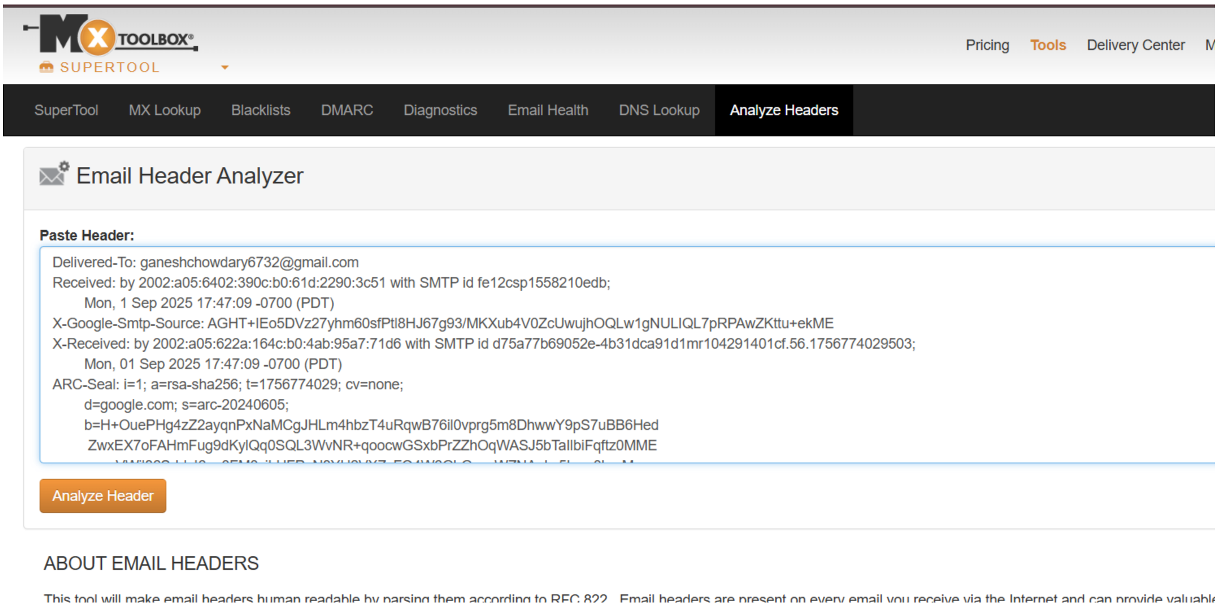


ABOUT EMAIL HEADERS

This tool will make email headers human readable by parsing them according to RFC 822. Email headers are present on every email you receive via the Internet and can provide valuable diagnostic information like hop delays, anti-spam results and more. If you need help getting copies of your email headers, just read this tutorial.

Your IP is: 10.140.20.244 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866)-698-6652 | © Copyright 2004-2021, MXToolBox, Inc. All rights reserved. US Patents 10839353 B2 & 11461738 B2

Step-4: Copy and paste the entire header text and click Analyze header



Email Header Analyzer

Paste Header:

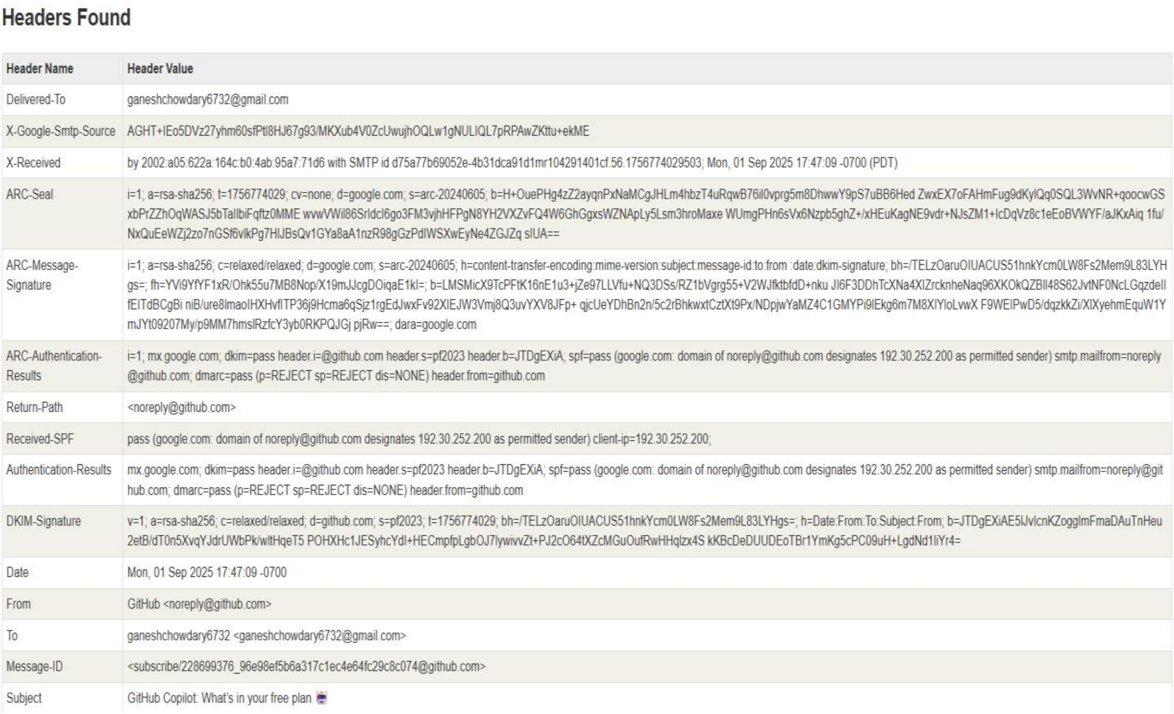
```
Delivered-To: ganeshchowdary6732@gmail.com
Received: by 2002:a05:6402:390c:b0:61d:2290:3c51 with SMTP id fe12csp1558210edb;
        Mon, 1 Sep 2025 17:47:09 -0700 (PDT)
X-Google-Smtp-Source: AGHT+IEo5DVz27yhm60sfPtl8HJ67g93/MKXub4V0ZcUwujhOQLw1gNULIQL7pRPAwZKttu+ekME
X-Received: by 2002:a05:622a:164c:b0:4ab:95a7:71d6 with SMTP id d75a77b69052e-4b31dca91d1mr104291401cf.56.1756774029503;
        Mon, 01 Sep 2025 17:47:09 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1756774029; cv=none;
        d=google.com; s=arc-20240605;
        b=H+OuePHg4zZ2ayqnPxNaMCgJHLm4hbzT4uRqwB76il0vprg5m8DhwwY9pS7uBB6Hed
         ZwxEX7oFAHmFug9dKylQq0SQL3WvNR+qoocwGSxbPrZZhOqWASJ5bTallbiFqftz0MME
```

Analyze Header

ABOUT EMAIL HEADERS

This tool will make email headers human readable by parsing them according to RFC 822. Email headers are present on every email you receive via the Internet and can provide valuabl

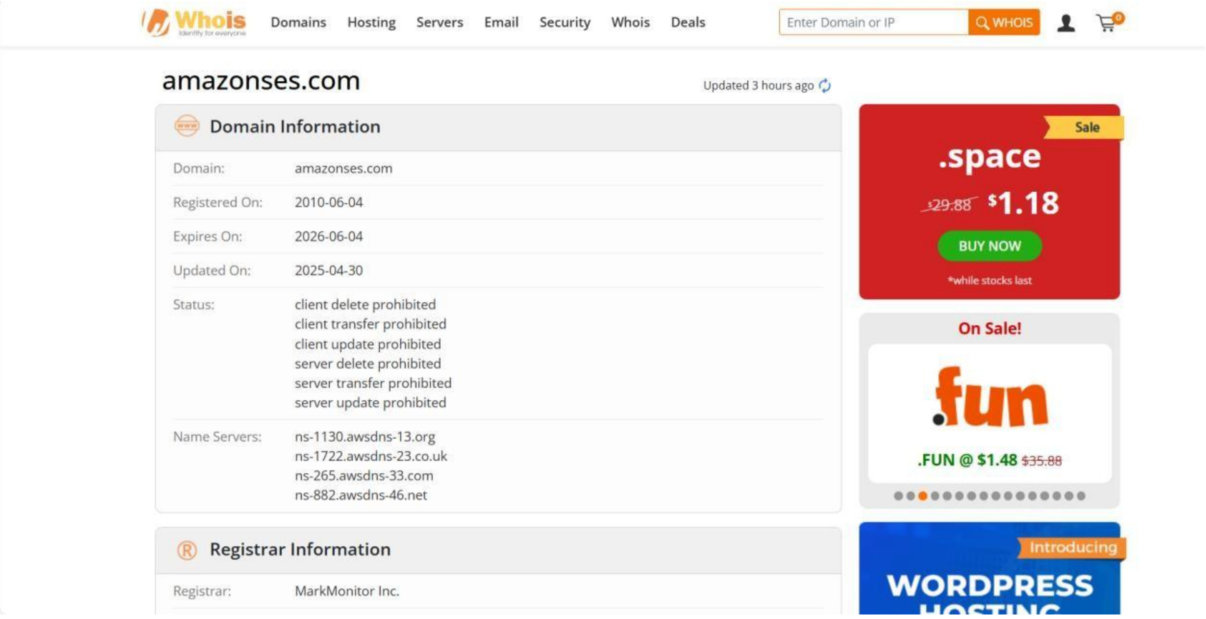
Step-5: Identify Key Header Fields (From, To, Subject, Date, Return-Path, Received, MessageID, SPF/DKIM/DMARC)



Headers Found

Header Name	Header Value
Delivered-To	ganeshchowdary6732@gmail.com
X-Google-Smtp-Source	AGHT+IEo5DVz27yhm60sfPtl8HJ67g93/MKXub4V0ZcUwujhOQLw1gNULIQL7pRPAwZKttu+ekME
X-Received	by 2002:a05:622a:164c:b0:4ab:95a7:71d6 with SMTP id d75a77b69052e-4b31dca91d1mr104291401cf.56.1756774029503; Mon, 01 Sep 2025 17:47:09 -0700 (PDT)
ARC-Seal	i=1; a=rsa-sha256; t=1756774029; cv=none; d=google.com; s=arc-20240605; b=H+OuePHg4zZ2ayqnPxNaMCgJHLm4hbzT4uRqwB76il0vprg5m8DhwwY9pS7uBB6Hed ZwxEX7oFAHmFug9dKylQq0SQL3WvNR+qoocwGSxbPrZZhOqWASJ5bTallbiFqftz0MME wwVWil86Srldcl6go3FM3vjhHFPgN8YH2VXZvFQ4W6GhGgxsWZNApLy5Lsm3hroMaxe WUmgPHn6sVx6Nzpb5ghZ+/xHEuKagNE9vdr+NJsZM1+IcDqVz8c1eEoBVWYF/aJKxAiq 1fu/NxQuEeWZj2zo7nGSf6vlkPg7HIJBsQv1GYa8aA1nzR98gGzPdlWSXwEyNe4ZGJZq slUA==
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605; h=content-transfer-encoding:mime-version:subject:message-id:to:from :date:dkim-signature; bh=/TELzOaruOIUACUS51hnkYcm0LW8Fs2Mem9L83LYHgs=; fh=YVi9YfYF1xR/Ohk55u7MB8Nop/X19mJJcgDOiqaE1kI=; b=LMSMicX9TcPFtK16nE1u3+jZe97LLVfu+NQ3DSs/RZ1bVgrg55+V2WJfktbfdD+nku JI6F3DDhTcXNa4XIZrcknheNaq96XKOkQZBlI48S62JvtNF0NcLGqzdelIfEITdBCgBi niB/ure8lmaoIHXHvfITP36j9Hcma6qSjz1rgEdJwxFv92XIEJW3Vmj8Q3uvYXV8JFp+ qjcUeYDhBn2n/5c2rBhkwxtCztXt9Px/NDpjwYaMZ4C1GMYPi9lEkg6m7M8XIYloLvwX F9WEIPwD5/dqzkkZi/XIXyehmEquW1YmJYt09207My/p9MM7hmslRzfcY3yb0RKPQJGj pjRw==; dara=google.com
ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@github.com header.s=pf2023 header.b=JTDgEXiA; spf=pass (google.com: domain of noreply@github.com designates 192.30.252.200 as permitted sender) smtp.mailfrom=noreply@github.com; dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=github.com
Return-Path	<noreply@github.com>
Received-SPF	pass (google.com: domain of noreply@github.com designates 192.30.252.200 as permitted sender) client-ip=192.30.252.200;
Authentication-Results	mx.google.com; dkim=pass header.i=@github.com header.s=pf2023 header.b=JTDgEXiA; spf=pass (google.com: domain of noreply@github.com designates 192.30.252.200 as permitted sender) smtp.mailfrom=noreply@github.com; dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=github.com
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=github.com; s=pf2023; t=1756774029; bh=/TELzOaruOIUACUS51hnkYcm0LW8Fs2Mem9L83LYHgs=; h=Date:From:To:Subject:From; b=JTDgEXiAE5lJvlcnKZogglmFmaDAuTnHeu2etB/dT0n5XvqYJdrUWbPk/wltHqeT5 POHXHc1JESyhcYdl+HECmpfpLgbOJ7lywivvZt+PJ2cO64tXZcMGuOufRwHHqlzx4S kKBcDeDUUDEoTBr1YmKg5cPC09uH+LgdNd1liYr4=
Date	Mon, 01 Sep 2025 17:47:09 -0700
From	GitHub <noreply@github.com>
To	ganeshchowdary6732 <ganeshchowdary6732@gmail.com>
Message-ID	<subscribe/228699376_96e98ef5b6a317c1ec4e64fc29c8c074@github.com>
Subject	GitHub Copilot: What's in your free plan 🤖

Step-6: Check for IP Addresses and Hostnames, use tools like WHOIS or online IP lookup services to identify the geographical location and ownership of the IP addresses found in the Received lines. Check if any IP addresses are suspicious or if the hostname does not match the expected sending server.



amazonses.com

Updated 3 hours ago

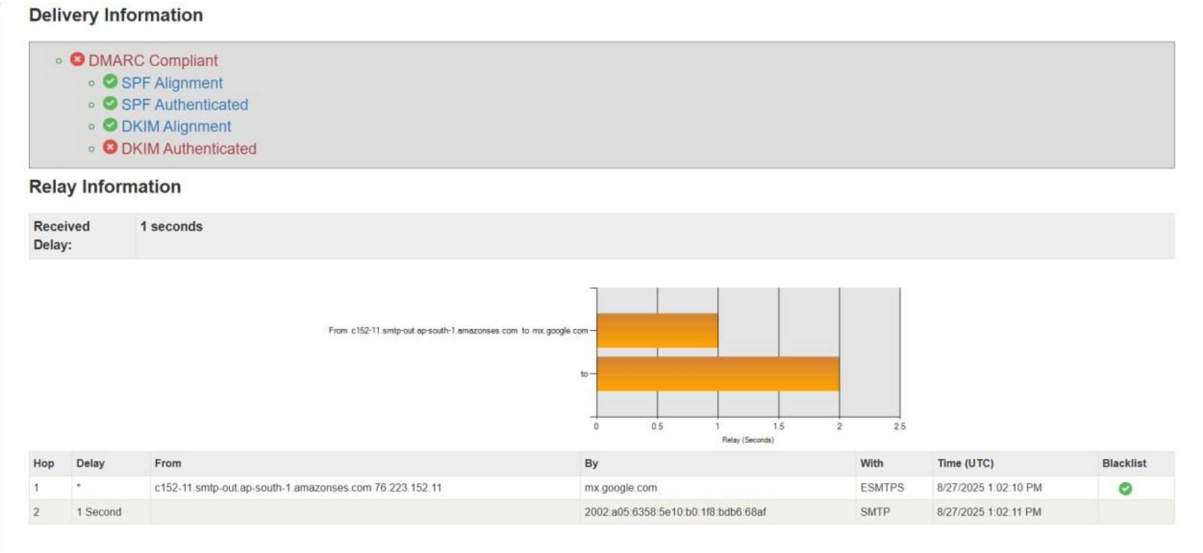
Domain Information

Domain:	amazonses.com
Registered On:	2010-06-04
Expires On:	2026-06-04
Updated On:	2025-04-30
Status:	client delete prohibited client transfer prohibited client update prohibited server delete prohibited server transfer prohibited server update prohibited
Name Servers:	ns-1130.awsdns-13.org ns-1722.awsdns-23.co.uk ns-265.awsdns-33.com ns-882.awsdns-46.net

Registrar Information

Registrar:	MarkMonitor Inc.

Step-7: Examine the SPF, DKIM, and DMARC Results


From c152-11.smtp-out.ap-south-1.amazonses.com to mx.google.com
to
0
0.5
1
1.5
2
2.5
Relay (Seconds)

Delivery Information

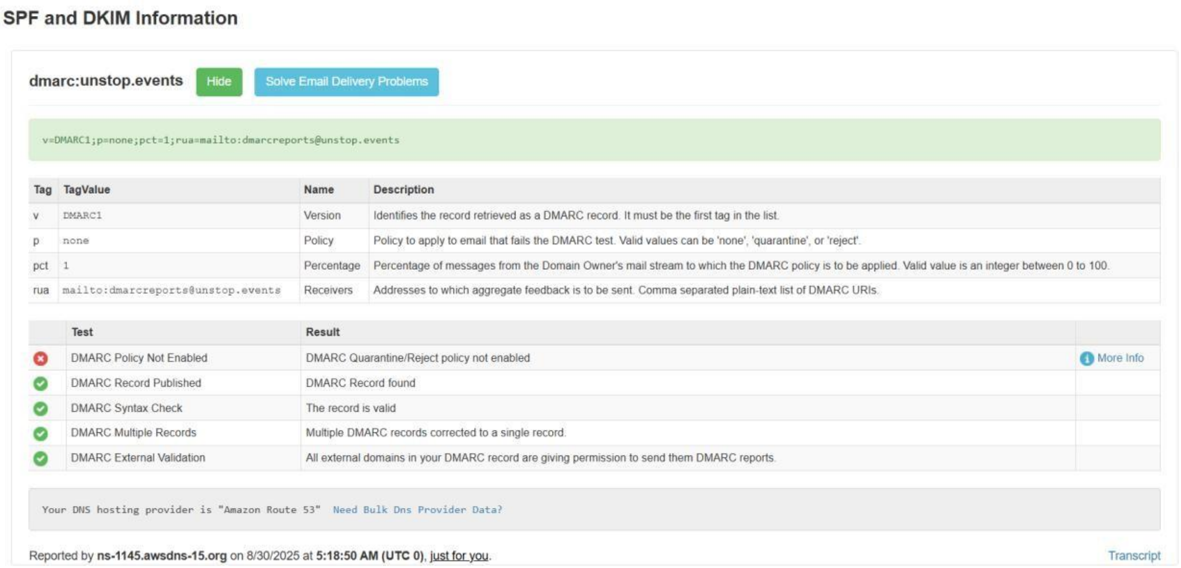
- ✗ DMARC Compliant
  - ✓ SPF Alignment
  - ✓ SPF Authenticated
  - ✓ DKIM Alignment
  - ✗ DKIM Authenticated

Relay Information

Received Delay:	1 seconds

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	c152-11.smtp-out.ap-south-1.amazonses.com 76.223.152.11	mx.google.com	ESMTPS	8/27/2025 1:02:10 PM	✓
2	1 Second		2002:a05:6358:5e10:b0:1f8:bdb6:68af	SMTP	8/27/2025 1:02:11 PM	

- SPF - Sender Policy Framework → Checks if the sender's server/IP is allowed for that domain
- DKIM DomainKeys Identified Mail → Ensures email content wasn't changed.



SPF and DKIM Information

dmarc:unstop.events

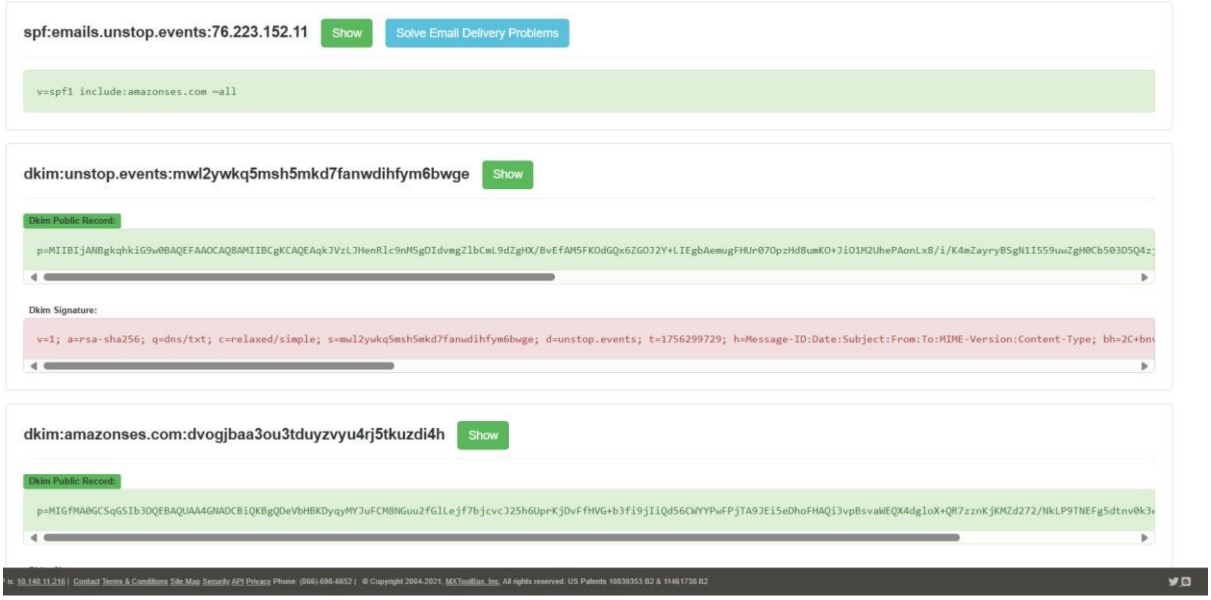
```
v=DMARC1;p=none;pct=1;rua=mailto:dmarcreports@unstop.events
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	none	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
pct	1	Percentage	Percentage of messages from the Domain Owner's mail stream to which the DMARC policy is to be applied. Valid value is an integer between 0 to 100.
rua	mailto:dmarcreports@unstop.events	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.

	Test	Result	
✗	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	ℹ More Info
✓	DMARC Record Published	DMARC Record found	
✓	DMARC Syntax Check	The record is valid	
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.	
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.	

```
Your DNS hosting provider is "Amazon Route 53"  Need Bulk Dns Provider Data?
```

Reported by **ns-1145.awsdns-15.org** on 8/30/2025 at **5:18:50 AM (UTC 0)**, just for you.



spf:emails.unstop.events:76.223.152.11

```
v=spf1 include:amazonses.com ~all
```

dkim:unstop.events:mwl2ywkq5msh5mkd7fanwdihfym6bwge

Dkim Public Record:

```
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqkJVzLJHenRlc9nM5gDIdvmgZlbCmL9dZgHX/BvEfAM5FKOdGQx6ZGOJ2Y+LIEgbAemugFHUr07OpzHd8umKO+JiO1M2UhePAonLx8/i/K4mZayryBSgN1I559uwZgH0Cb503D5Q4z
```

Dkim Signature:

```
v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; s=mwl2ywkq5msh5mkd7fanwdihfym6bwge; d=unstop.events; t=1756299729; h=Message-ID:Date:Subject:From:To:MIME-Version:Content-Type; bh=2C+bn
```

dkim:amazonses.com:dvogjbaa3ou3tduyzvyu4rj5tkuzdi4h

Dkim Public Record:

```
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDeVbHBKDyqyMYJuFCM8NGuu2fGlLejf7bjcvcJ25h6UprKjDvFfHVG+b3fi9jIiQd56CWYYPwFPjTA9JEi5eDhoFHAQi3vpBsvaWEQX4dgloX+QR7zznKjKMZd272/NkLP9TNEFg5dtnv0k3
```