

## 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

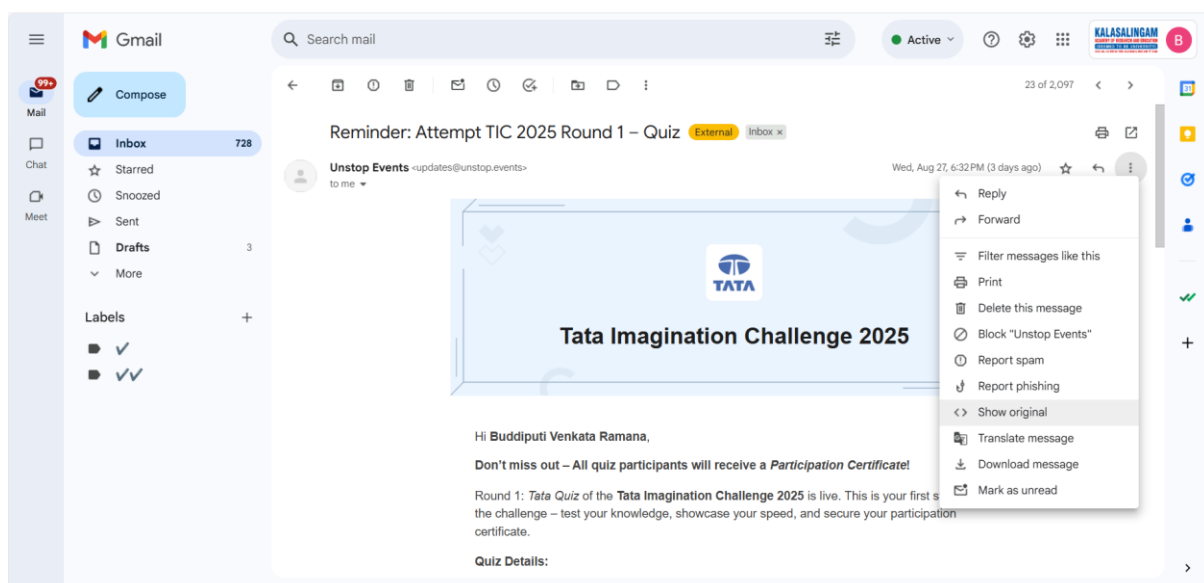
### Description:

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



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

**TOOLBOX**  
SUPERTOOL

PricingToolsDelivery CenterMonitoringProductsBlogSupportLogin

SuperToolMX LookupBlacklistsDMARCDiagnosticsEmail HealthDNS Lookup**Analyze Headers**All Tools

Email Header Analyzer

Paste Header:

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 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.](#)

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

TOOLBOX

SUPERTOOL

Pricing

Tools

Delivery Center

Monitoring

Products

Blog

Support

Login

SuperTool

MX Lookup

Blacklists

DMARC

Diagnostics

Email Health

DNS Lookup

Analyze Headers

All Tools

Email Header Analyzer

Paste Header:

Delivered-To: 99230040264@klu.ac.in  
Received: by 2002:a05:6358:5e10:b0:1f8:bdb6:68af with SMTP id q16csp200636nm;  
Wed, 27 Aug 2025 06:02:11 -0700 (PDT)  
X-Google-Smtp-Source: AGHT+IEFzvZKTZ4kzyuQDteYZEcdXVz2try5aIGPBILBCL4NhbsJk0nxvLKemhqEs5aWYqWuL8  
X-Received: by 2002:a05:6a20:244e:b0:233:f0c6:a8a4 with SMTP id adf61e73a8af0-24340cd2b35mr26883742637.31.1756299730864;  
Wed, 27 Aug 2025 06:02:10 -0700 (PDT)  
ARC-Seal: i=1; a=rsa-sha256; t=1756299730; cv=none;  
d=google.com; s=arc-20240605;  
b=WQIR7ICAAYmHh6ddyRjWcZ+foVeQ7GFhQlK7hBsYwued5s7QZKRryEzmZ0prT+  
/KLDsmjCaIMR4WJqLP4/Y0Amb6V0HF/sbbezlb+1z3sEYib9CxPCpVrOcidD5/zFX1oA

Analyze Header

Loading

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 10.188.28.241 | Contact Us & Conditions Site Map Security API Privacy Policy (866) 498-6652 | © Copyright 2004-2021, MXToolbox, Inc. All rights reserved. US Patents 10039353 B2 & 11461738 B2

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

Headers Found

Header Name	Header Value
Delivered-To	99230040264@klu.ac.in
X-Google-Smtp-Source	AGHT+IEFzvZKTZ4kzyuQDteYZEcdXVz2try5aIGPBILBCL4NhbsJk0nxvLKemhqEs5aWYqWuL8
X-Received	by 2002:a05:6a20:244e:b0:233:f0c6:a8a4 with SMTP id adf61e73a8af0-24340cd2b35mr26883742637.31.1756299730864, Wed, 27 Aug 2025 06:02:10 -0700 (PDT)
ARC-Seal	i=1; a=rsa-sha256; t=1756299730; cv=none; d=google.com; s=arc-20240605; b=WQIR7ICAAYmHh6ddyRjWcZ+foVeQ7GFhQlK7hBsYwued5s7QZKRryEzmZ0prT+ /KLDsmjCaIMR4WJqLP4/Y0Amb6V0HF/sbbezlb+1z3sEYib9CxPCpVrOcidD5/zFX1oA
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/signed; d=google.com; s=arc-20240605; h=feedback-id mime-version to:from:subject:date:message-id:dkim-signature:dkim-signature; bh=w2rsMGtzOQUZFNK62cQQyD0zq90Vtrt+5uJRLVyoZU; fh=vwed+KA45dpE2pxQCKDZKqy93G5h7nkEvLZ8ioM20; b=HxftXtgrRrIDxeG1NHPiIDZBF5leCvHRDu8+3TKzUY01kv+guH0h9vUQHqVYVWZm 9Zr5V5CEOuarpDhC7CoJvrugP1DaMuUoe4C+imur2IUvgCAQVU2oCh8Cw8Sy5N6m 4F52jTfnJfoW7rkHNzxv4SG5jNvvoF+DcpC6/3aW1/IDIGmdFOl8WmUMmbYh 2/K8OCnGgrdvPRg+9yZxQzE9eLUFIPC/P5HiQw2+toL0poG/Us6adMBuXnWM0+Kbd uOakY5538W8YyukRIgIfl/gwmKWxVLRhMLD/DO2/1UHVCMYAUHIGLanntsJdzUzQV szfA==; dara=google.com
ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@unstop.events header.s=miw2ywkq5msh5mkd7fanwdihfym6bwge header.b=Jjd+Uo1L; dkim=pass header.i=@amazonse.com header.s=dvogjbaa3ou3tduyzyv4rj5kuzdi4h header.b=BnPlkmP; spf=pass (google.com. domain of 01090198eb9f198e-c991a5bf-503e-40df-a544-100947516c77-0000000@emails.unstop.events designates 76.223.152.11 as permitted sender) smtp.mailfrom=01090198eb9f198e-c991a5bf-503e-40df-a544-100947516c77-0000000@emails.unstop.events; dmARC=pass (p=NONE sp=NONE dis=NONE) header.from=unstop.events
Return-Path	<01090198eb9f198e-c991a5bf-503e-40df-a544-100947516c77-0000000@emails.unstop.events>
Received-SPF	pass (google.com. domain of 01090198eb9f198e-c991a5bf-503e-40df-a544-100947516c77-0000000@emails.unstop.events designates 76.223.152.11 as permitted sender) client-ip=76.223.152.11;
Authentication-Results	mx.google.com; dkim=pass header.i=@unstop.events header.s=miw2ywkq5msh5mkd7fanwdihfym6bwge header.b=Jjd+Uo1L; dkim=pass header.i=@amazonse.com header.s=dvogjbaa3ou3tduyzyv4rj5kuzdi4h header.b=BnPlkmP; spf=pass (google.com. domain of 01090198eb9f198e-c991a5bf-503e-40df-a544-100947516c77-0000000@emails.unstop.events designates 76.223.152.11 as permitted sender) smtp.mailfrom=01090198eb9f198e-c991a5bf-503e-40df-a544-100947516c77-0000000@emails.unstop.events; dmARC=pass (p=NONE sp=NONE dis=NONE) header.from=unstop.events
DKIM-Signature	v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; s=miw2ywkq5msh5mkd7fanwdihfym6bwge; d=unstop.events; t=1756299729; h=Message-ID:Date:Subject:From:To:MIME-Version:Content-Type; bh=2C+bnv3lvocYHshveHPBo1d4G+8HDSKdRmr+4wPLY=; b=Jjd+Uo1L4MFDlou+sAQ++25fvcHxLzRvzG1p5rIOBF56uqJlr82aWzBzKdFwM bT2zup4MjgIBDPyGCZnm6+hyRAPC8ME1He4AQJLLbbIVYZBDIXPL59NvHh0wqO6x XdyxZU2B87U4VOOKcal409stYYHmW99awH111YEtpx3afDJGCPVLCnk1Q3bEGipO 0aBsR9hwrm7ke8PDsDncqJUMX0JACLO+umpb8qr8xybh6g4hXhX6TJQHEP8/B3j 6NEu3EeKArj6+7VxuX9DXKxaQ2DJRXNKu93r11P4OhJR3bMmavniD5yRAoRZBkqQpD 8Jfn2vMWkw==
Message-ID	<01090198eb9f198e-c991a5bf-503e-40df-a544-100947516c77-0000000@ap-south-1.amazonaws.com>
Date	Wed, 27 Aug 2025 13:02:09 +0000
Subject	Reminder: Attempt TIC 2025 Round 1 - Quiz

Your IP is 10.188.11.219 | Contact Us & Conditions Site Map Security API Privacy Policy (866) 498-6652 | © Copyright 2004-2021, MXToolbox, Inc. All rights reserved. US Patents 10039353 B2 & 11461738 B2

**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.

Whois

Domains

Hosting

Servers

Email

Security

Whois

Deals

Enter Domain or IP

WHOIS

amazonsses.com

Updated 3 hours ago

Domain Information

Domain: amazonsses.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.

.space

Sale

\$29.88 \$1.18

BUY NOW

\*while stocks last

On Sale!

fun

.FUN @ \$1.48 \$35.88

Introducing

WORDPRESS

HOSTING

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

Delivery Information

DMARC Compliant

SPF Alignment

SPF Authenticated

DKIM Alignment

DKIM Authenticated

Relay Information

Received Delay: 1 seconds

From c152-11.smtp-out.ap-south-1.amazonsses.com to mx.google.com

to

Relay (Seconds)

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	c152-11.smtp-out.ap-south-1.amazonsses.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

Hide

Solve Email Delivery Problems

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
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.

Transcript

spf:emails.unstop.events:76.223.152.11

Show

Solve Email Delivery Problems

v=spf1 include:amazonses.com ~all

dkim:unstop.events:mwl2ywkq5msh5mkd7fanwdihfym6bwge

Show

DKIM Public Record:

p=MIIBIjANBgkqhkiG9w0BAQFAADCAQ8AMIIBCgKCAQEAqk7VzL3HenRlc9nM5g0IdvmgZ1bCmL9dZgHX/BvEfAM5FKOdGQx6ZG032Y+LIEgbAemugFHUj=07OpzHd8umKO+Ji0IM2UhePAonLx8/i/K4mZayryB5gN1I559uwZgH8Cb503D5Q4z;

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+bm

dkim:amazonses.com:dvogjbaa3ou3tduyzyyu4rj5tkuzdi4h

Show

DKIM Public Record:

p=MIIGFMA8GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDeVbH8KdyqYHYJufCM8NGuu2FG1Lejf7b7cvcJ2Sh6UpKjDvFfHVg+b3fi9jIIQd56CWYPwFPjTA9JEI5eDhoFHAQI3vp8svakEQ4dgl0x+QR7znKjKH2d272/NkLP9TNEFg5dtnv0k3;

© 19, 148, 11, 218 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866) 698-6652 | © Copyright 2004-2021, MXToolBox, Inc. All rights reserved. US Patents 10839553 B2 & 11461738 B2