Email Header Analysis & Phishing Investigation

Project Overview

Project Title:
Email Header Analysis & Threat Intelligence Investigation (SOC Lab)

Objective:
To analyze a suspicious email received in Yahoo Mail by performing detailed email header analysis, domain reputation checks, IP reputation analysis, and threat intelligence correlation to determine whether the email is malicious or benign.

Skills Demonstrated:

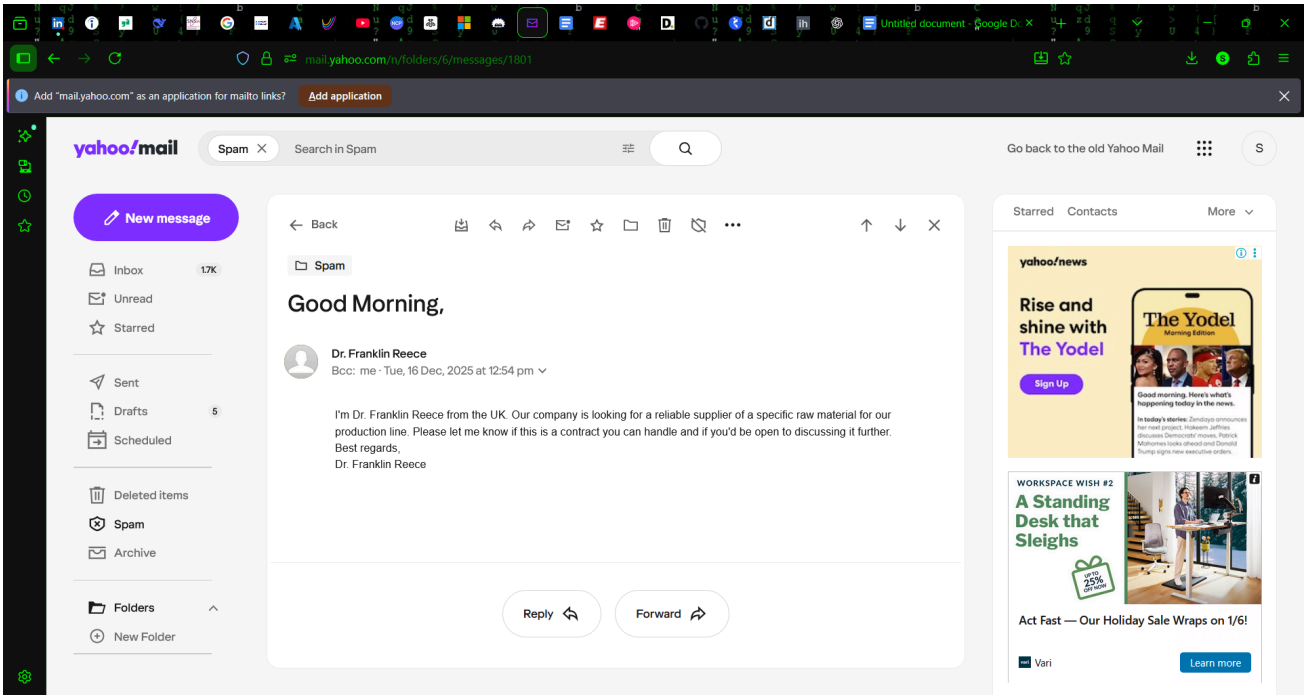
- Email header analysis
- SPF / DKIM / DMARC validation
- WHOIS domain analysis
- IP reputation analysis
- Threat intelligence correlation
- SOC-style investigation & documentation

Suspicious Email Identification

A suspicious email titled **"Good Morning,"** was received in the **Spam folder** of Yahoo Mail.
The sender claimed to be a foreign supplier requesting business engagement, which is a **common phishing and BEC (Business Email Compromise) tactic**.

Observed Red Flags:

- Generic subject line
- Business solicitation from unknown sender
- Email delivered to spam folder
- External sender domain

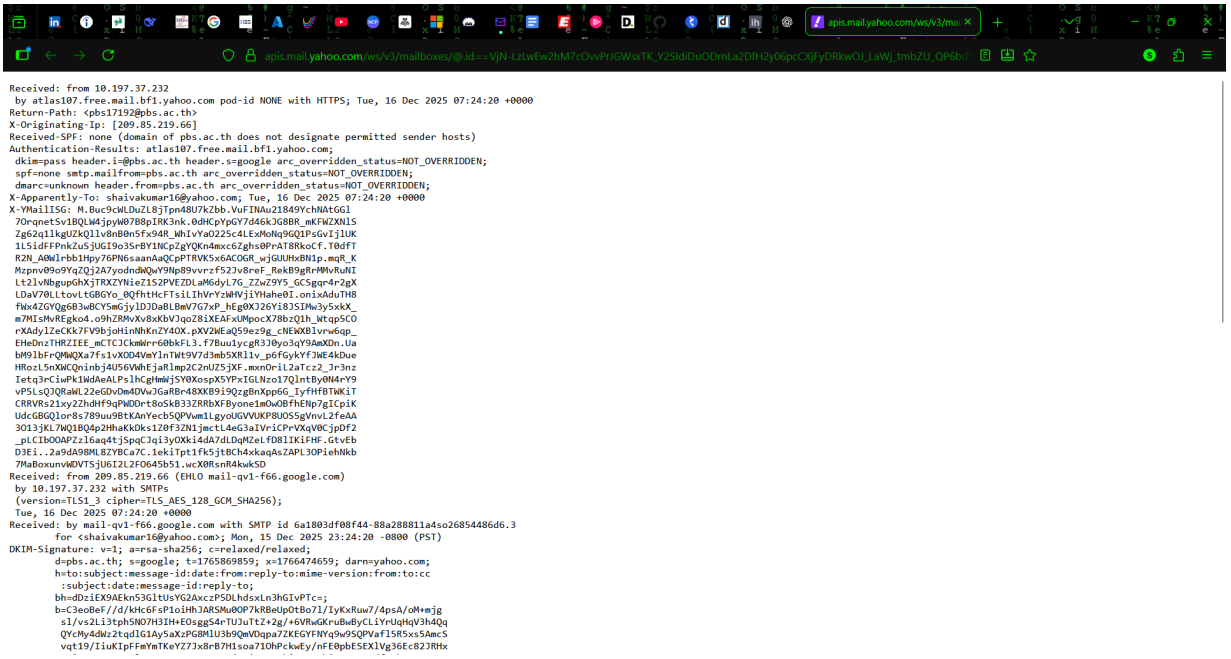


Email Header Extraction

Since Yahoo Mail does not provide a direct “Copy Headers” option, the **“View Raw Message”** feature was used.

Action Performed:

- Opened email
- Selected **More options → View Raw Message**
- Copied the **entire raw email header**



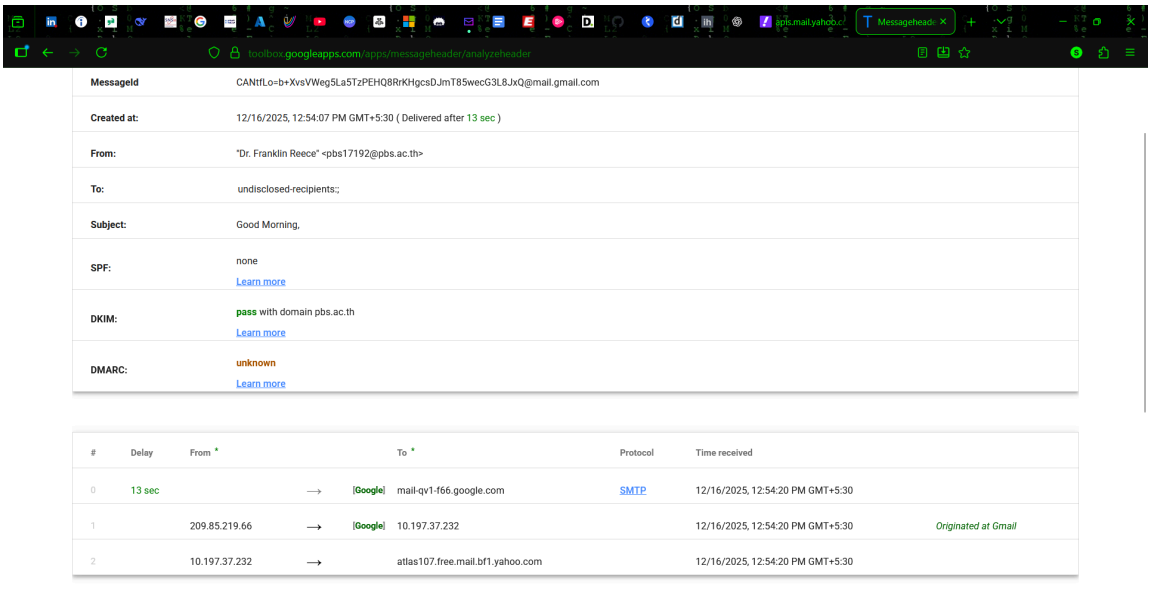
```
Received: from 10.197.37.232
 by atlas107.free.mail.bf1.yahoo.com pod-id NONE with HTTPS; Tue, 16 Dec 2025 07:24:20 +0000
Return-Path: <pbs17192@pbs.ac.th>
X-Originating-Ip: [209.85.219.66]
Received-SPF: none (domain of pbs.ac.th does not designate permitted sender hosts)
Authentication-Results: atlas107.free.mail.bf1.yahoo.com;
 dkim=pass header.i=@pbs.ac.th header.s=google arc_overridden_status=NOT_OVERRIDDEN;
 spf=none smtp.mailfrom=pbs.ac.th arc_overridden_status=NOT_OVERRIDDEN;
 dmarc=unknown header.from=pbs.ac.th arc_overridden_status=NOT_OVERRIDDEN;
X-Apparently-To: shaivakumar16@yahoo.com; Tue, 16 Dec 2025 07:24:20 +0000
X-YMailISG: M.Buc9cWLDuZL8jTpn48U7kZbb.VuFINAu21849YchNAtGGl
 7OrqnetSv1BQLW4jpyW07B8pIRK3nk.0dHCpYpGY7d46kJG8BR_mKFWZXNlS
 Zg62q1lkgUZkQllv8nB0n5fx94R_WhIvYaO225c4LExMoNq9GQ1PsGvIjlUK
 1l5idFFPnkZuSjUGI9o3SrBY1NCpZgYQKn4mxc6Zghs0PrAI8RkoCf.T0dFT
 RZN_A0WlrbbiHpy76PN6saanAqQCpPTRVK5x6ACOGR_wjGUUHxBN1p.mqR_K
 Mzpnv09o9YqZQj2A7yodndWQwY9Np89vvrzf52Jv8reF_RekB9gRrMMvRuNI
 Lt2lvNbgupGhXjTRXZYNieZ1S2PVEZDLaM6dyL7G_ZZwZ9Y5_GCSgqr4r2gX
 LDaV70LLtovLtGBGYo_0QfhtHcFTsiLIhVrYzWHVjiYHahe0I.onixAduTH8
 fWx4ZGYQg6B3wBCY5mGjylDJDaBLBmV7G7xP_hEg0XJ26Yi8JSIMw3y5xkX_
 m7MIsMvREgko4.o9hZRMvXv8xKbVJqoZ8iXEAFxUMpocX78bzQ1h_Wtqp5CO
 rXAdylZeCKk7FV9bjoHinNhKnZY4OX.pXV2WEaQ59ez9g_cNEWXBlvrw6qp_
 EHeDnzTHRZIEE_mCTCJCkmWvr60bkFl3.f7Buu1ycgR3J0yo3qY9AmXDn.Ua
 bM9lbFrQMWQXa7fs1vXOD4VmYlnTWt9V7d3mb5XRl1v_p6fGykYfJWE4kDue
 HRozL5nXWCQninbj4U56VWhEjaRlmp2C2nUZ5jXF.mxnOriL2aTcz2_Jr3nz
 Ietq3rCiwPk1WdAeALPslhCgHmWjSY0XospX5YPxIGLNzo17QlntBy0N4rY9
 vP5LsQJQRaWL22eGDvDm4DVwJGaRBr48XKB9i9QzgBnXpp6G_IyfHfBTWKiT
 CRRVRs21xy2ZhdHf9qPWDDrt8oSkB33ZRRbXFByone1mOwOBfhENp7gICpiK
 UdcGBGQlor8s789uu9BtKAnYecb5QPVwm1LgyoUGVVUKP8UO5SgVnvL2feAA
 3O13jKL7WQ1BQ4p2HhaKkDks1Z0f3ZN1jmctL4eG3aIVriCPrVXqV0CjpDF2
 _pLCIbOOAPZzl6aq4tjSpqCJqi3yOXki4dA7dLDqMZelfD81IKiFHF.GtvEb
 D3Ei..2a9dA98ML8ZYBCa7C.1ekiTpt1fk5jtBCh4xkaqAsZAPl3OPiehNkb
 7MaBoxunvWDVTSjU6I2L2FO645b51.wcX0RsnR4kwk5D
Received: from 209.85.219.66 (EHLO mail-qv1-f66.google.com)
 by 10.197.37.232 with SMTPs
 (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256);
 Tue, 16 Dec 2025 07:24:20 +0000
Received: by mail-qv1-f66.google.com with SMTP id 6a1803df08f44-88a288811a4so26854486d6.3
        for <shaivakumar16@yahoo.com>; Mon, 15 Dec 2025 23:24:20 -0800 (PST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=pbs.ac.th; s=google; t=1765869859; x=1766474659; darn=yahoo.com;
        h=to:subject:message-id:date:from:reply-to:mime-version:from:to:cc
         :subject:date:message-id:reply-to;
        bh=dDziEX9AEkn53GltUsYG2AxczP5DLhdsxLn3hGIvPTc=;
        b=C3eoBeF//d/kHc6FsP1oiHhJARSMuOOP7kRBeUpOtBo7l/IyKxRuw7/4psA/oM+mjg
         sl/vs2Li3tph5NO7H3IH+EOsggS4rTUJuTtZ+2g/+6V8uGKruBwByCLiYrUqHqV3h4Qq
         QYcMy4dWz2tqdlG1Ay5aXzPG8MlU3b9QmVDqpa7ZKEGYFNYq9w9SQPVaf15R5xs5AmcS
         vqt19/IiuKIpFFmYmTKeYZ7Jx8rB7H1soa71OhPckwEy/nFE0pbESEXlVg36Ec82JRHx
```

Email Header Analysis (Google Admin Toolbox)

The copied raw headers were analyzed using **Google Admin Toolbox – Messageheader Analyzer**.

Key Findings:

- Message originated from **Google mail servers**
- Sender domain: `pbs.ac.th`
- Email was relayed through Gmail infrastructure
- Message delivery time was normal (no delay anomalies)



MessageId	CANtfLo=b+XvsVWeg5La5TzPEHQ8RrKHgcsDJmT85wecG3L8JxQ@mail.gmail.com
Created at:	12/16/2025, 12:54:07 PM GMT+5:30 (Delivered after 13 sec)
From:	"Dr. Franklin Reece" <pbs17192@pbs.ac.th>
To:	undisclosed-recipients:;
Subject:	Good Morning,
SPF:	none Learn more
DKIM:	pass with domain pbs.ac.th Learn more
DMARC:	unknown Learn more

#	Delay	From		To	Protocol	Time received	
0	13 sec		→ [Google]	mail-qv1-f66.google.com	SMTP	12/16/2025, 12:54:20 PM GMT+5:30	
1		209.85.219.66	→ [Google]	10.197.37.232		12/16/2025, 12:54:20 PM GMT+5:30	*Originated at Gmail*
2		10.197.37.232	→	atlas107.free.mail.bf1.yahoo.com		12/16/2025, 12:54:20 PM GMT+5:30	

Authentication Results Analysis (SPF / DKIM / DMARC)

Mechanism	Result	Observation
SPF	**None**	Domain did not explicitly authorize sender
DKIM	**Pass**	Email cryptographically signed
DMARC	**Unknown**	Domain lacks DMARC policy

Security Insight:
Even though DKIM passed, **SPF = none** and **DMARC = unknown** reduce trust and indicate **weak domain email security posture**.

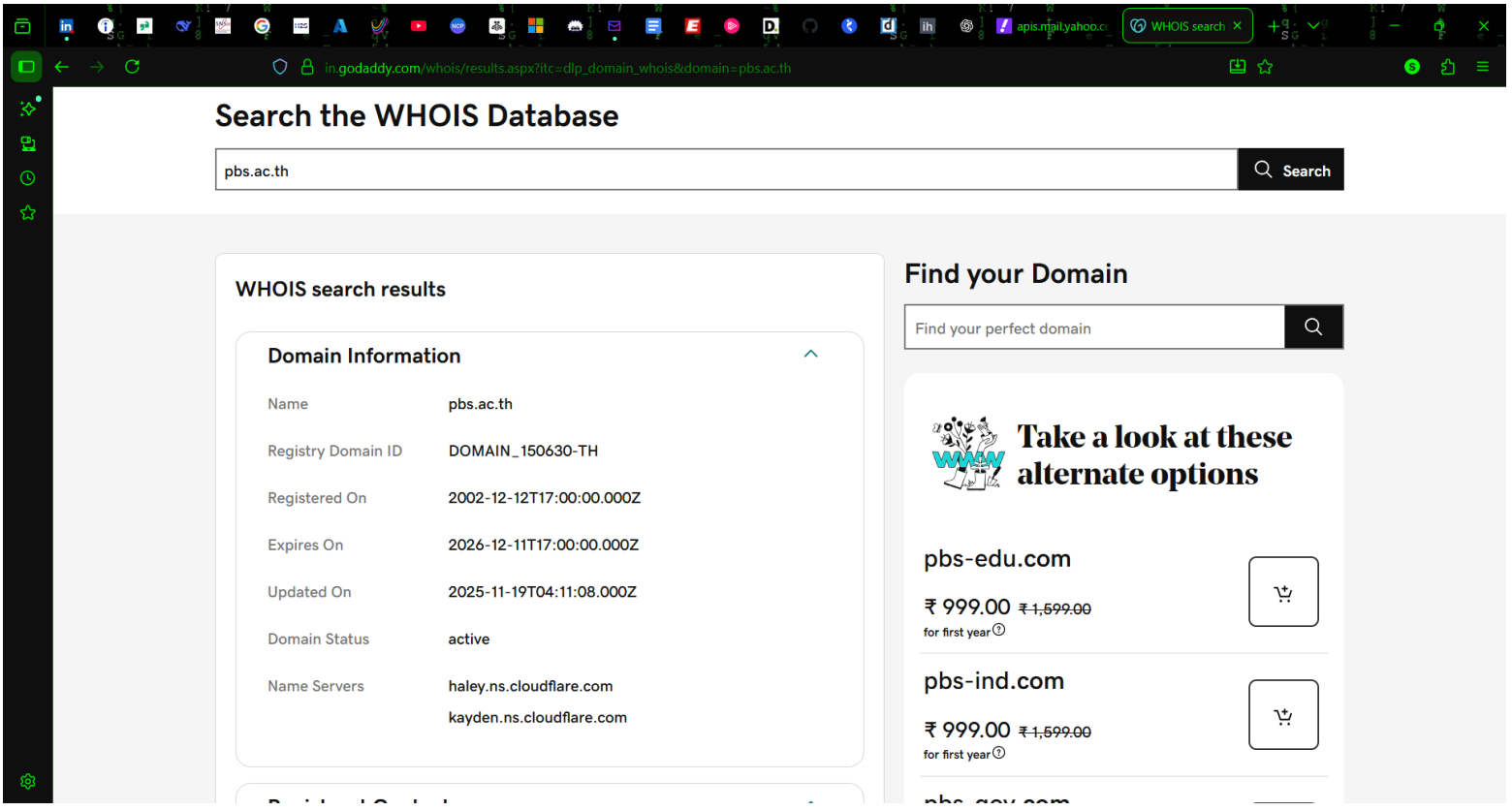
Sender Domain WHOIS Analysis

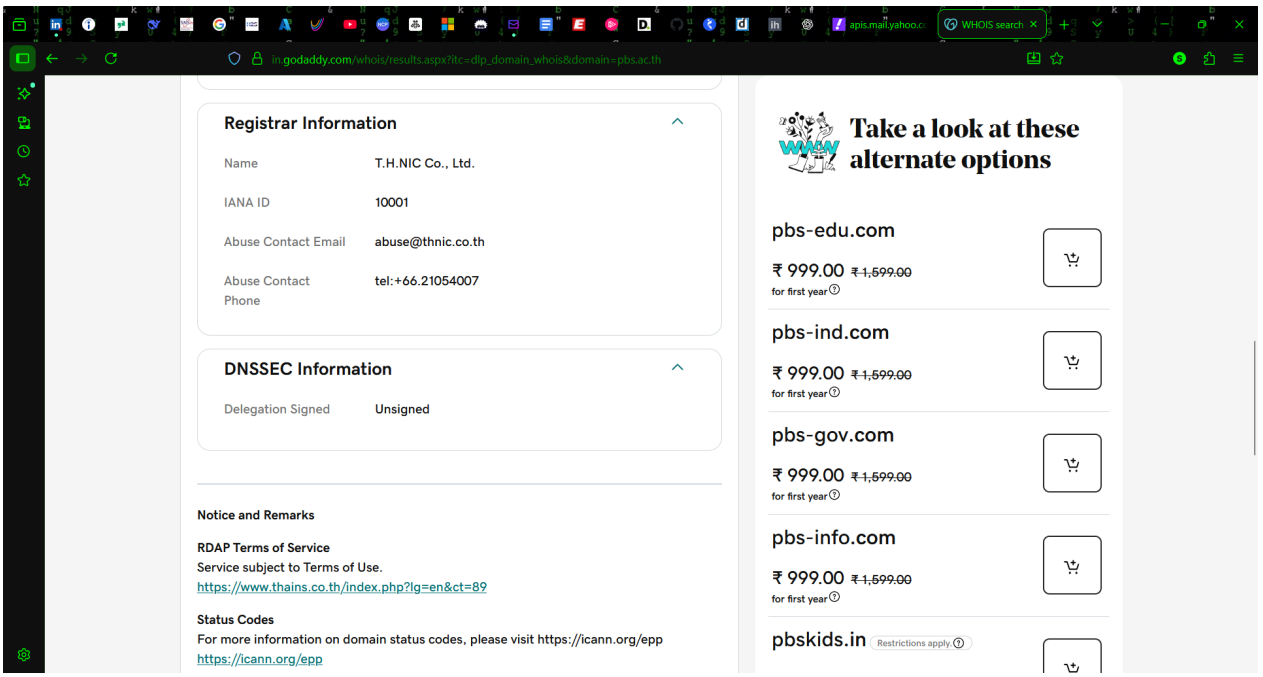
The sender domain `pbs.ac.th` was investigated using WHOIS lookup.

Findings:

- Domain registered in **2002**
- Registrar: **T.H.NIC Co., Ltd**
- Domain status: **Active**
- Name servers hosted via **Cloudflare**

Conclusion:
Domain itself appears legitimate and long-standing, but this **does not guarantee sender legitimacy**, as accounts can be compromised.





Source IP Address Analysis

From the headers, the originating IP was identified as:

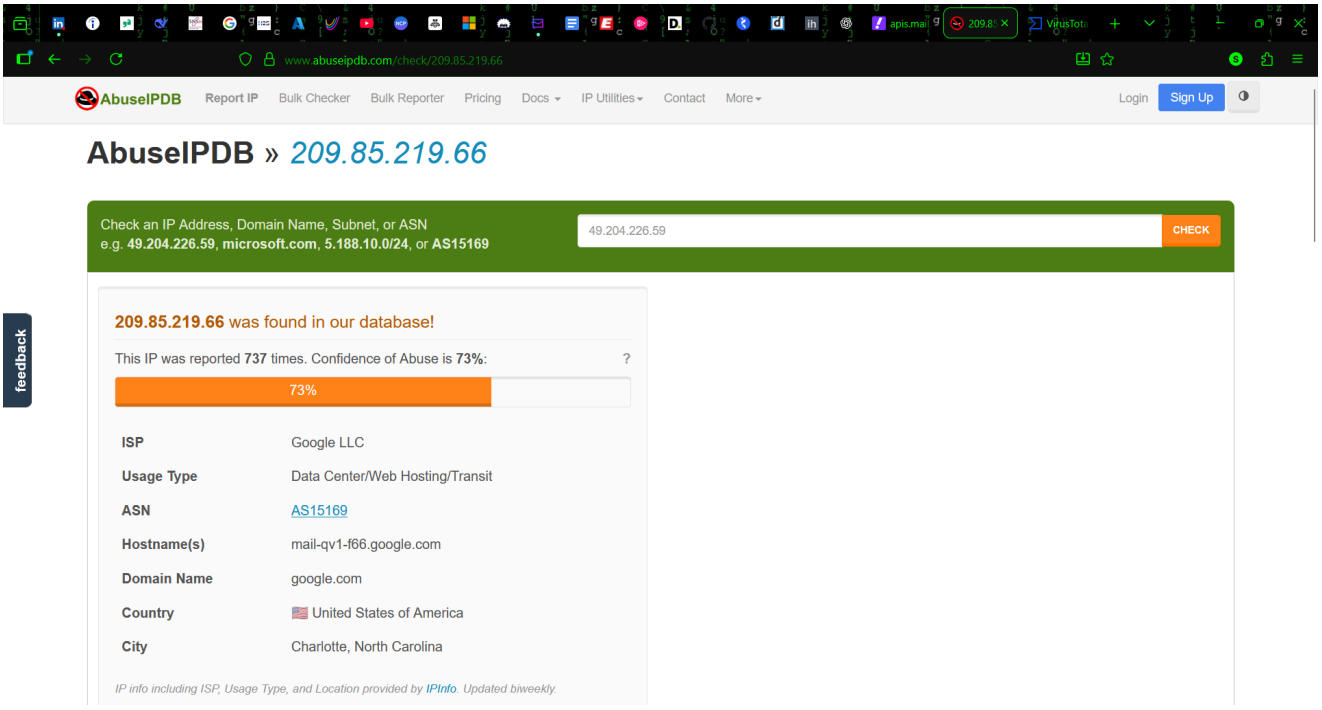
`209.85.219.66`
This IP belongs to **Google LLC (AS15169)**.

AbuseIPDB Analysis

Results:

- Reported **737 times**
- Confidence of abuse: **73%**
- Categories: Email spam, brute force, port scanning

Interpretation:
The IP belongs to Google mail infrastructure, meaning abuse reports are likely due to **misused or compromised Gmail accounts**.



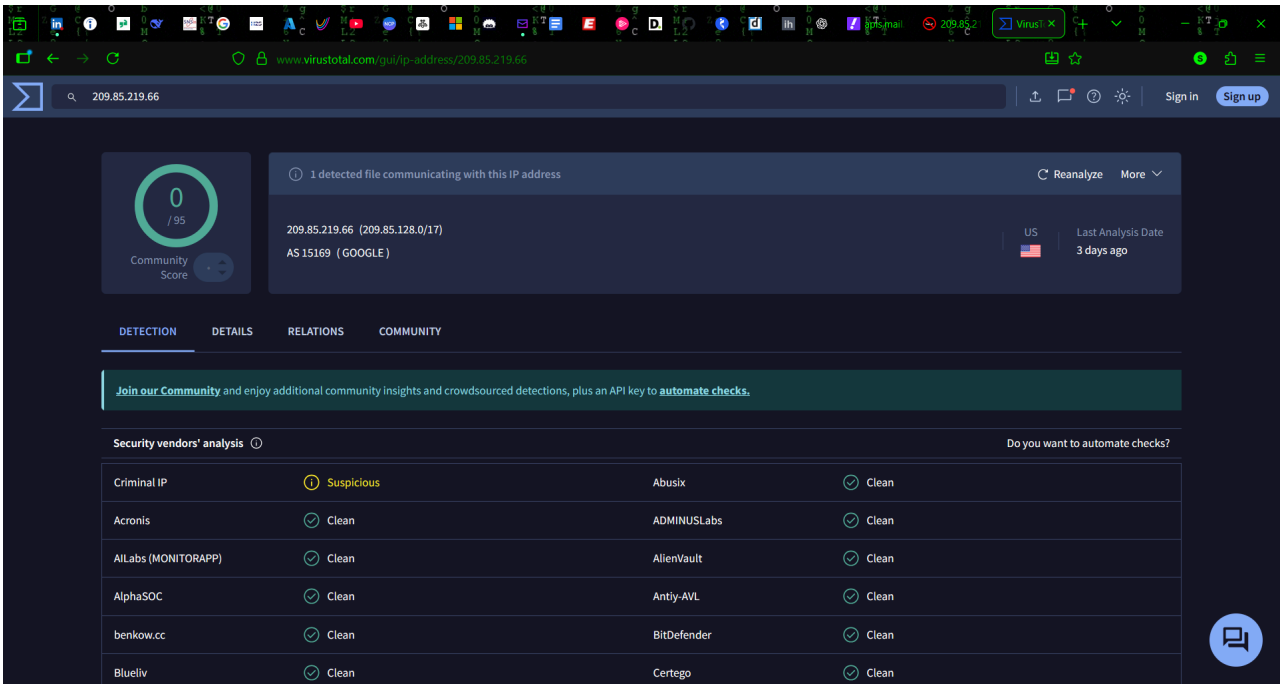
VirusTotal IP Reputation Check

The same IP was analyzed in VirusTotal.

Results:

- 0/95 vendors flagged as malicious
- One suspicious indicator by CriminalIP
- IP associated with Google infrastructure

Conclusion:
No direct malware association, but **email abuse behavior confirmed**.



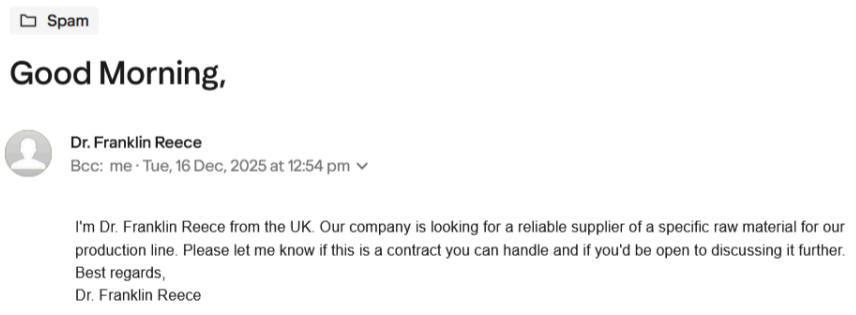
Email Content Analysis

Email Content Summary:

- No attachments
- No clickable links
- Social engineering attempt requesting business discussion
- Reply-to address differed from sender domain

Threat Assessment:

- Likely **Business Email Compromise (BEC) / Scam**
- Designed to initiate conversation before requesting sensitive or financial data



Final Incident Verdict

Classification:
Suspicious / Scam Email (Low-level Phishing / BEC Attempt)

Reasons:

- Weak email authentication (SPF none, DMARC unknown)
- High abuse reputation of sending IP
- Generic business lure content
- Delivered directly to spam

Recommended SOC Actions

- Mark email as **Spam**
- Block sender address
- Educate users about BEC-style scams
- Monitor for similar domains or sender patterns
- Improve email security policies (SPF, DMARC enforcement)