Decoding Email Legitimacy: Assessing the Veracity of Sender Identities

Email Header Analysis

Terms:

Sender Policy Framework (SPF):

SPF is a system for preventing forged sender addresses. The SPF field also lists the mail servers that are authorised to transmit messages from the specified (sender) domain. SPF prevents bogus sender email addresses as a result. Although the outcome (Received-SPF) might be neutral, pass, or fail, this the receiving mail server runs a DNS query to find the sender's domain's SPF record during the SPF evaluation. Following that, it makes a comparison between the IP address of the email's sending server and the list of authorised IP addresses included in the SPF record. The SPF check is successful if the IP address of the transmitting server matches one of the permitted IP addresses, suggesting that the email is probably valid.

SPF shouldn't be used to verify the email's validity. The sample that follows was taken from a phoney email.

```
Received: from ww-2220.innovativemails.com (ww-2220.innovativemails.com.
[103.251.22.20])
      by mx.google.com with ESMTPS id v202-
20020a6361d3000000b0053b887d3d4dsi2293149pgb.291.2023.06.21.05.57.19
      for <[redacted]@gmail.com>
      (version=TLS1_2 cipher=ECDHE-ECDSA-CHACHA20-POLY1305 bits=256/256);
      Wed, 21 Jun 2023 05:57:21 -0700 (PDT)
Received-SPF: pass (google.com: domain of 4_287025_392000103-
nukalanavinkumar44=gmail.com-ad@ww-2213.innovativemails.com designates
103.251.22.20 as permitted sender) client-ip=103.251.22.20;
Authentication-Results: mx.google.com;
```

```
Received: from sv323.xserver.jp (sv323.xserver.jp. [219.94.203.163])
        by mx.google.com with ESMTPS id
j17si21147467pll.154.2021.06.01.07.09.37
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 01 Jun 2021 07:09:38 -0700 (PDT)
Received-SPF: neutral (google.com: 219.94.203.163 is neither permitted nor
denied by best guess record for domain of n-satou@saho.co.jp) client-
ip=219.94.203.163;
```

Pass: The SPF check is successful if the transmitting server's IP address complies with one of the authorised IP addresses listed in the SPF record, and the result is "pass." This suggests that the email is probably real and originates from a trusted source.

Neutral: When the IP address of the transmitting server is not expressly stated in the SPF record as being authorised or not, the SPF result is "neutral." This implies that the SPF check does not give a definite indicator of the email's validity. Depending on how it is configured, the receiving mail server can handle this result differently.

Fail: If the SPF check fails, it signifies that none of the authorised IP addresses listed in the SPF record correspond to the transmitting server's IP address. The SPF outcome in this instance is "fail." This might mean that the email was sent fraudulently or by an unreliable source. The receiving mail server may take steps like rejecting or flagging the email as suspicious.

Domain Keys Identified Mail (DKIM)

A domain name can be linked to an email using the DKIM technique. DKIM enables an organisation to verify the communication's real ownership and unaltered transit of the message by examining the (cryptographic) signature.


```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=mailers.zomato.com; h=content-
transfer-encoding:content-type:from:mime-version:subject: x-feedback-id:to:list-
unsubscribe:cc:content-type:from:subject:to; s=zct;
bh=v6RmWJ6WlVY896c2t/ZXMBMcpGjBoPaQGgm/UWCqXzg=;
b=lwIYcFfZ+sAKmyRTYg53fZNRAahwrKbtgQVhkcL2g5Ul/tPJxwy+q3H3JTJpUdHHz5ii
NGdJBOJtxENVDk8p3FifmDR34ccPy/2UeIiU4dQfFtci4x/7jAMqJ9JzQpabSQ2hqs6MgU
ptGYZlCB4TGPxyjsByl7eenlTnBuNFkb0YlEz0QJCW9AG2px6uOnAQ5jEEej8bGr65T9o6
2Oc8wD3/IiaCfrjG1+pio8eV5k0J5jauFgXn4cLBLY1wx5g7M/R1JtKVGCMjPouDue/h+9
UffR3Wgj3PJBtpGTCjoJs3SoqanBmgMNL5oA/Q5TnM7z3CQljiIuuXrx9dzDEQQg==
```


If the DMIK is legit and can be confirmed as originating from a real domain, you will see the following message: dkim=pass

During the analysis of any email header, if the DKIM is missing, you may see something similar to the following message.

Dkim Signature Error: No DKIM-Signature header found -more info
Dkim Signature Error: There must be at least one aligned DKIM-Signature for the message to be considered aligned – more info

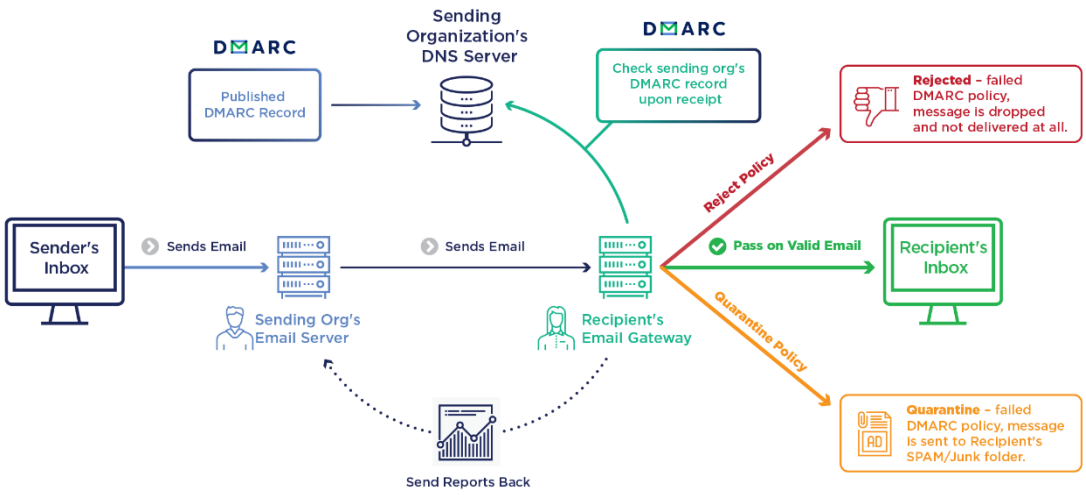
The absence of the DKIM just shows that the sender was not following the protocol; not all senders, legitimate or not, will utilise DKIM; nonetheless, the absence of both DKIM and SPF results in the absence of DMARC.

Domain Based Message Authentication Reporting (DMARC)

An email authentication system called Domain-based Message Authentication, Reporting, and Conformance (DMARC) expands upon the SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) methods. By providing an email sender and recipient with a set of guidelines for acceptable behaviour, DMARC helps protect users against email spoofing, phishing, and domain impersonation.

The DMARC gives the sender reports on who is attempting to send messages using their domain as part of the validation process. As new hazards surface, the sender may adjust their policy thanks to

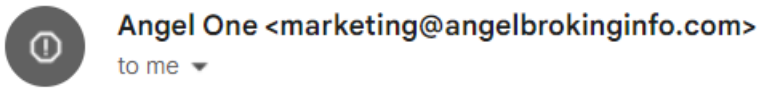
this visibility. By lessening nonvalidated or fraudulent email risks, DMARC aids businesses in building brand confidence.



Examine a sample mail:

Dear Naveen, your Angle One account is locked, and I kindly request you to share your bank account details (Account Holder Name, Account Number, Branch Name, IFSC Code) to assist in unlocking my account. Your cooperation is highly appreciated. Thank you.

Examine the senders' address.

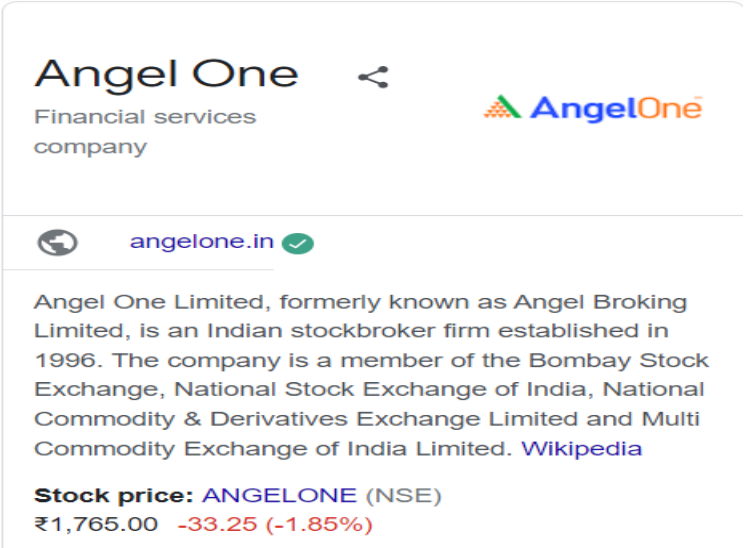


Starting with the sender's email, we see that the message is probably bogus. Not even an attempt to spoof the address to indicate it came from Angle one. This email appears to have originated from a mail server located in Mumbai, India.

Verify the information in the mail with google info:

We next do a Google search to gather information about the Angle one and if **marketing@angleborkinginfo.com** is an actual mail of **Angle One.**

First, let us look at what we know about the Angle One.



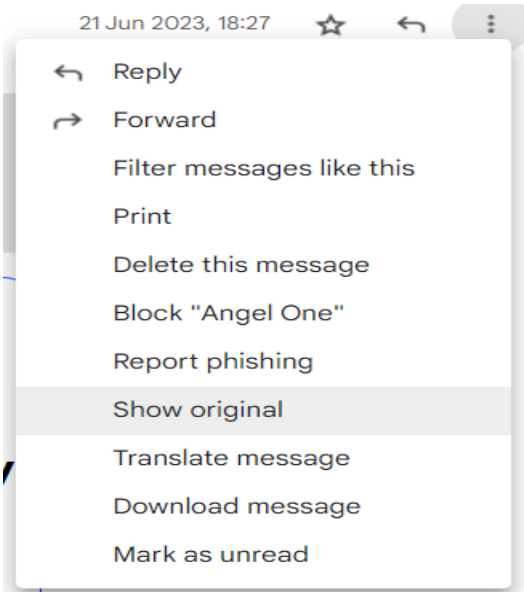
Email Header Analysis.

As we continue with our investigation, we look at the header data to determine who sent this email and where it came from. If we're lucky, we might even be able to use Google Earth to look up the sender's IP address and determine their precise location.

Viewing email headers

Using the built-in tools offered by both providers is the simplest way to see the header information of an email sent to a Gmail or Yahoo account.

Open the email and expand the settings in the viewing window to the right to see the email's header information in Gmail's webmail. Choose "show original" from the context menu.



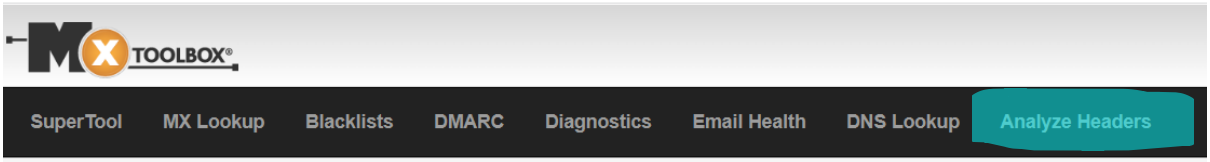
The header information is displayed. We are given the information in two parts. A synopsis of the email appears in the first.

Original message

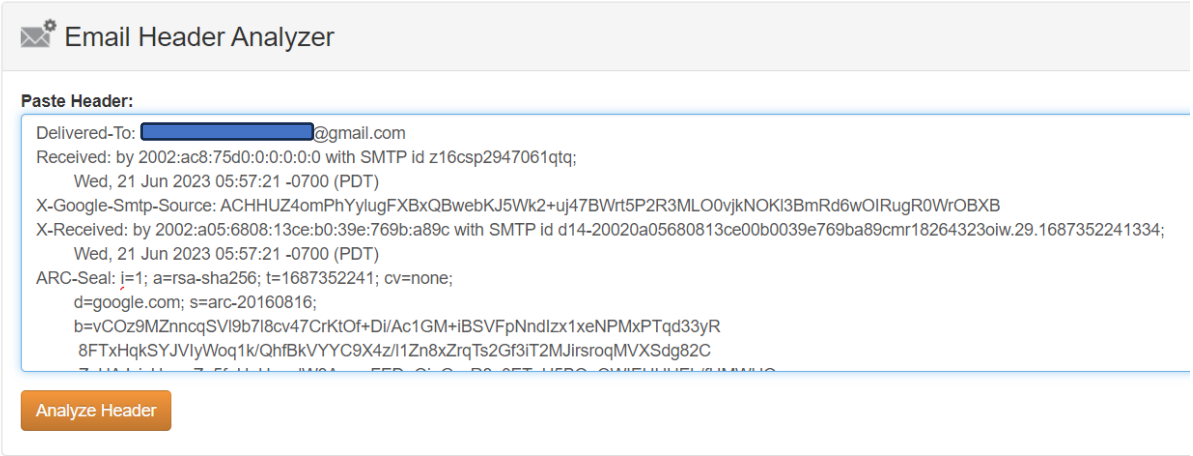
Message ID	<0fe9e4513b65f5ef7f4de40a0c171b64@angelbrokinginfo.com>
Created on:	21 June 2023 at 18:27 (Delivered after 2 seconds)
From:	Angel One <marketing@angelbrokinginfo.com>
To:	[redacted]
Subject:	Naveen, You are few steps away from getting your Demat Account
SPF:	PASS with IP 103.251.22.20 Learn more
DKIM:	'PASS' with domain angelbrokinginfo.com Learn more
DMARC:	'PASS' Learn more

The second or bottom part shows the header information. To help us better analyze the header information were going to use an online tool provided by **MXToolbox**. In the bottom right corner of your email header summary, click on the blue box marked, Copy to clipboard.

From the taskbar, click the link for Analyse Headers.



After pasting the header data into the text box, select the orange "Analyse Header" button in the bottom left-hand corner.



The MXToolbox Header Analysis tool breaks up the email header into smaller, manageable chunks. 7 Starting at the top of the results, we get a summary of the delivery information.

Header Analyzed

Email Subject: Naveen, You are few steps away from getting your Demat Account

Delivery Information

- DMARC Compliant
  - SPF Alignment
  - SPF Authenticated
  - DKIM Alignment
  - DKIM Authenticated

To pass DMARC authentication, a message must both Pass and Align for either SPF or DKIM. Even if a message passed authentication for both SPF and DKIM, it could still fail DMARC authentication if one of them does not “align” with the sender’s policy.

If SPF Passes, the message was delivered from an IP address published in the SPF policy of the SMTP envelope “mail from:” (mfrom) domain, and if the DKIM Passes, the message was correctly signed by the d= domain in the DKIM header.

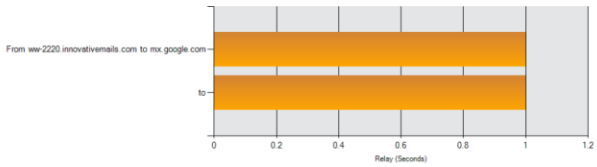
DKIM Aligns, means the header visible to the recipient matches the d= domain in the DKIM header.

SPF Aligns, means the header visible to the recipient matches the domain used to authenticate SPF. (e.g., the envelope “mail from:” domain)

When a message is aligned, the email recipient knows from which domain the message originated from.

SPF and DKIM are only authentication mechanisms. Passing SPF or DKIM authentication only means the receiving organization can identify the actual sending domain. But typically, the end□user receiving the message never sees this domain. Instead, they see the “From:” address in the email header.

A message can pass both SPF and DKIM authentication and trick the end-user into thinking it came from someone else (i.e., spoofing). When a message is aligned, the friendly domain visible in the email client matches the domain used to authenticate with SPF or DKIM.



The header block will always start with a fresh Received: line added by the server relay each time it receives an SMTP message. A typical email sent to or received by a user on a business network may typically display many server relays both during and after delivery to the corporate email servers (companyserver.com). These will be listed in reverse chronological order, beginning at the bottom.

You may determine the message's route by looking at the information from the server relay in chronological order starting at the bottom and working your way up. The name and IP address of the sending server are added by each receiving mail server. The domain of the sender relay may be known from the server name.

This may merely direct you back to the location of the email servers or even the provider's corporate headquarters in the case of messages sent via Gmail and other significant email service providers.

If you are lucky, the headers will include an X-Originating-IP that may reveal the sender's internet service provider and narrow down the sender's location

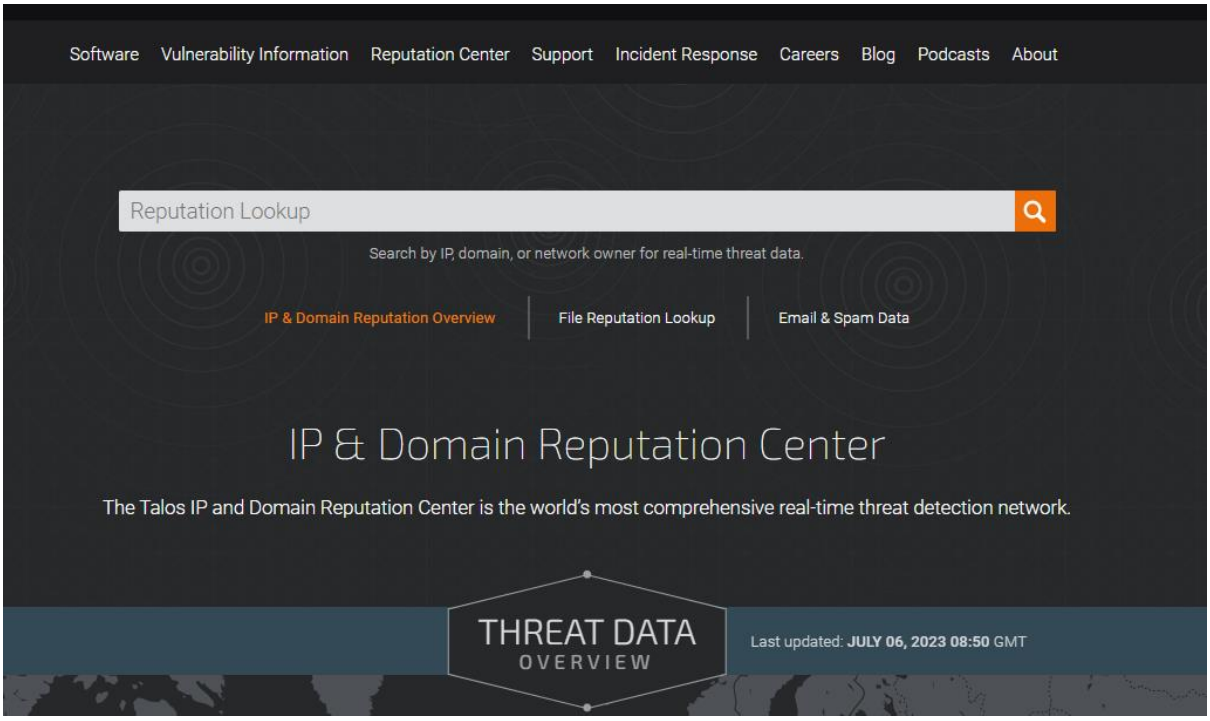
In the following image, we see the relay information starting at the bottom with the name and IP address of the sending mail server.

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	ww-2220.innovativemails.com 103.251.22.20	mx.google.com	ESMTPS	6/21/2023 12:57:21 PM	✔
2	0 seconds		2002:ac8:75d0:0:0:0:0:0	SMTP	6/21/2023 12:57:21 PM	

The IP address or domain that sent the spam email to your email server should be noted when examining spam email headers from a network security viewpoint.

Verify the server's reputation:

To verify the reputation of a domain, you can use a free reputation service such as the one provided by Cisco https://www.senderbase.org



From our relay results, we see there is a server with a hostname of server **ww-2220.innovativemails.com** using an IP address of **103.251.22.20**. Using the Cisco Talos site, we can check the reputation of the server.

Lookup data results for IP Address

103.251.22.20

Search by IP, domain, or network owner for real-time threat data.

IP & Domain Reputation Overview | File Reputation Lookup | Email & Spam Data

LOCATION DATA

India

OWNER DETAILS

IP ADDRESS	103.251.22.20
FWD/REV DNS MATCH	Yes
HOSTNAME	ww-2220.innovativemails.com
DOMAIN	innovativemails.com
NETWORK OWNER	web werks india pvt.

CONTENT DETAILS

CONTENT CATEGORY	No established content categories

Think these category details are incorrect?

Submit Content Categorization Ticket

REPUTATION DETAILS

SENDER IP REPUTATION	Good	Submit Sender IP Reputation Ticket
WEB REPUTATION	Unknown	Submit Web Reputation Ticket

EMAIL VOLUME DATA

	LAST DAY	LAST MONTH
EMAIL VOLUME	2.6	4.7
VOLUME CHANGE	0%	
SPAM LEVEL	None	

BLOCK LISTS

BL.SPAMCOP.NET	Not Listed
CBL.ABUSEAT.ORG	Not Listed
PBL.SPAMHAUS.ORG	Not Listed
SBL.SPAMHAUS.ORG	Not Listed

TALOS SECURITY INTELLIGENCE BLOCK LIST

ADDED TO THE BLOCK LIST	No

We are trying to confirm the identity of the sender. So far, it looks good. So far, we know that reputation of the sending server is good, but Web reputation is Unknown and the email originated in India.

Note: You can analyse additional information

ADDITIONAL INFORMATION

IP ADDRESSES | WHOIS | EMAIL VOLUME HISTORY

Top IP Addresses used to send emails in 103.251.22.20 /24

IP ADDRESS	HOSTNAME	FWD/REV DNS MATCH	LAST DAY VOL.	LAST MONTH VOL.	BLOCK LISTS	EMAIL REP.
103.251.22.200	-	No	0.0	0.8	0	Neutral
103.251.22.21	ww-2221.innovativemails.com	Yes	2.6	4.6	0	Good
103.251.22.20	ww-2220.innovativemails.com	Yes	2.5	4.6	0	Good
103.251.22.19	ww-2219.innovativemails.com	Yes	2.9	4.6	0	Good
103.251.22.18	ww-2218.innovativemails.com	Yes	2.9	4.6	0	Good
103.251.22.17	ww-2217.innovativemails.com	Yes	2.8	4.6	0	Good
103.251.22.16	ww-2216.innovativemails.com	Yes	2.7	4.6	0	Good
103.251.22.15	ww-2215.innovativemails.com	Yes	0.0	0.5	0	Neutral
103.251.22.13	ww-2213.innovativemails.com	Yes	2.7	4.6	0	Good

IP locators

The Internet has dozens if not hundreds of free IP locator sites. They all have different features and return different results. I like the features of www.Opentracker.net . It returns plenty of information

about the IP address, but it also allows you to pinpoint the IP address location using satellite imaging and mapping.

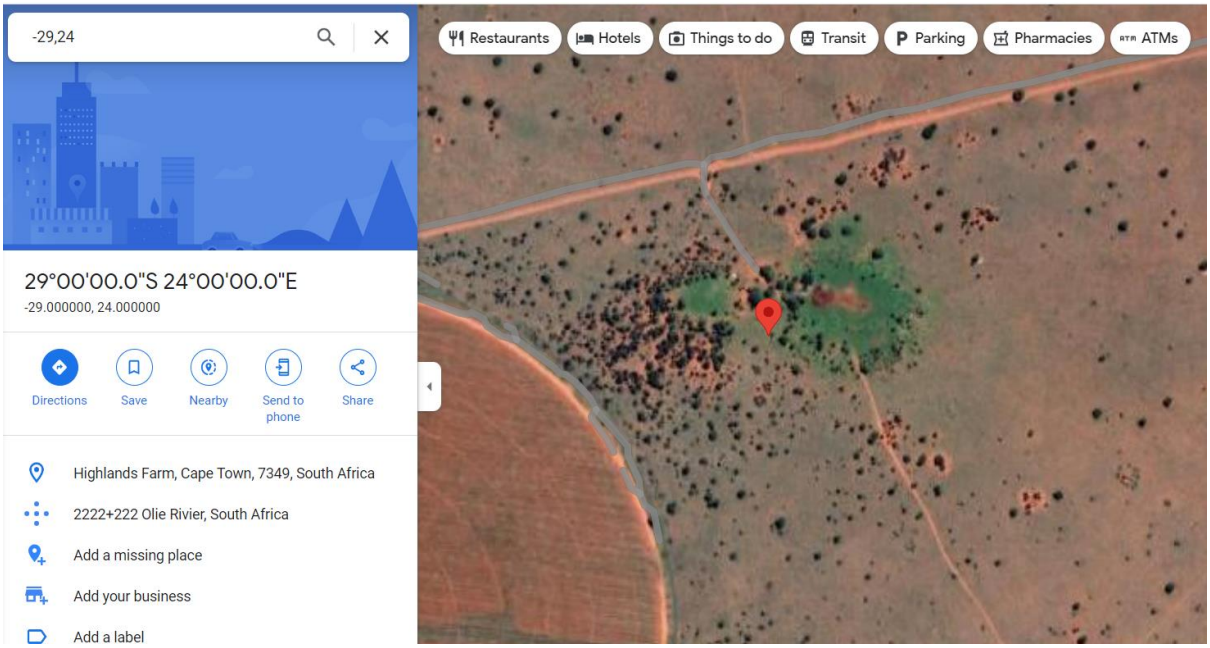
102.251.22.20 Click to search!

Summary of IP's Profile Details Copy

- IP address: **102.251.22.20**
- City: **Johannesburg**
- Region name: Gauteng
- Country name: South Africa
- Life Expectency: 51.1
- Avg income: **2,891** EUR
- Timezone: Africa/Johannesburg
- Sub continent: Southern Africa
- Country code: ZA
- Geo-targeting: **true**
- Latitude: -29.0
- Longitude: 24.0
- World currency: EUR
- EU member: false
- org: Telkom Internet
- isp: Telkom Internet
- Connection: Cable/DSL
- Continent: Africa
- Population: 40,377,000
- IP range tracked:
- Surface area: 1,221,037 km sq.
- GNP: 116,729 mln.
- Demographic data: **true**
- Ad (re)targeting: **true**

in this example, I can see where the device assigned the IP address **102.251.22.20** is located.

In our Google map, I have a red pin showing the server's location somewhere in Tokyo. By using Google Earth, I can see where the server is located in South Africa.



Locating the IP address of the sender

If the stars and the planets are all aligned correctly, you may be able to see the originating IP address located in the email header. Not always, but it's still worth investigating. Here is an example of what you might look for

```
Received: from ww-2220.innovativemails.com (ww-2220.innovativemails.com. [103.251.22.20])
```

As we can see the sender ip is originated in India.