Experiment 01

Aim:

1. Perform **Email Header Analysis** to extract valuable information such as:
   - Sender IP address
   - Email servers involved
   - Routing path
2. Conduct **Email Address Enumeration** to verify and identify valid email addresses associated with a target domain using tools like **The Harvester** or **Hunter.io**.

Theory:

1. Email Header Analysis

Email headers contain metadata that tracks an email's journey from the sender to the recipient. Analyzing headers helps:

- Trace back the sender
- Detect spoofed or phishing emails
- Understand the mail flow and potential security threats

Key Components in Headers:

Header	Description
Received:	Shows the mail servers the email passed through
X-Originating-IP:	May reveal the sender's original IP
User-Agent: / X-Mailer:	Reveals the email client used
Date:	Shows when the email was sent
From:	Displays the sender's email address

---

2. Email Address Enumeration

This process is used to **discover valid email addresses** within a particular domain. It helps:

- Map potential targets in an organization
- Conduct social engineering or phishing simulations (for ethical testing)

- Gather intelligence for OSINT operations

🔧 **Tools Used:**

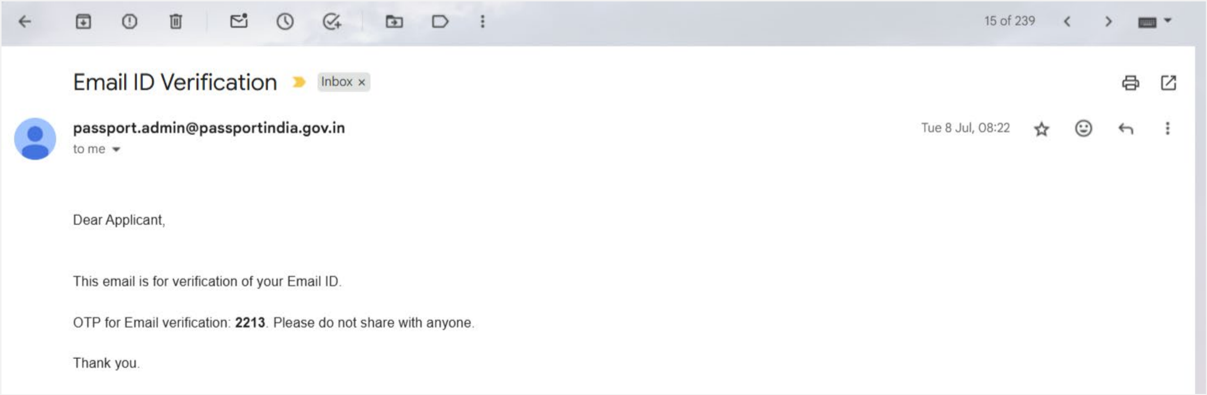
- Hunter.io (Web-based)

PART A: Email Header Analysis:

Step-by-Step Procedure:

1. Access the Email:

- Open your email client (e.g., Gmail or Outlook).
- Locate a suspicious or test email.



Email ID Verification Inbox ×

passport.admin@passportindia.gov.in
to me

Tue 8 Jul, 08:22

Dear Applicant,

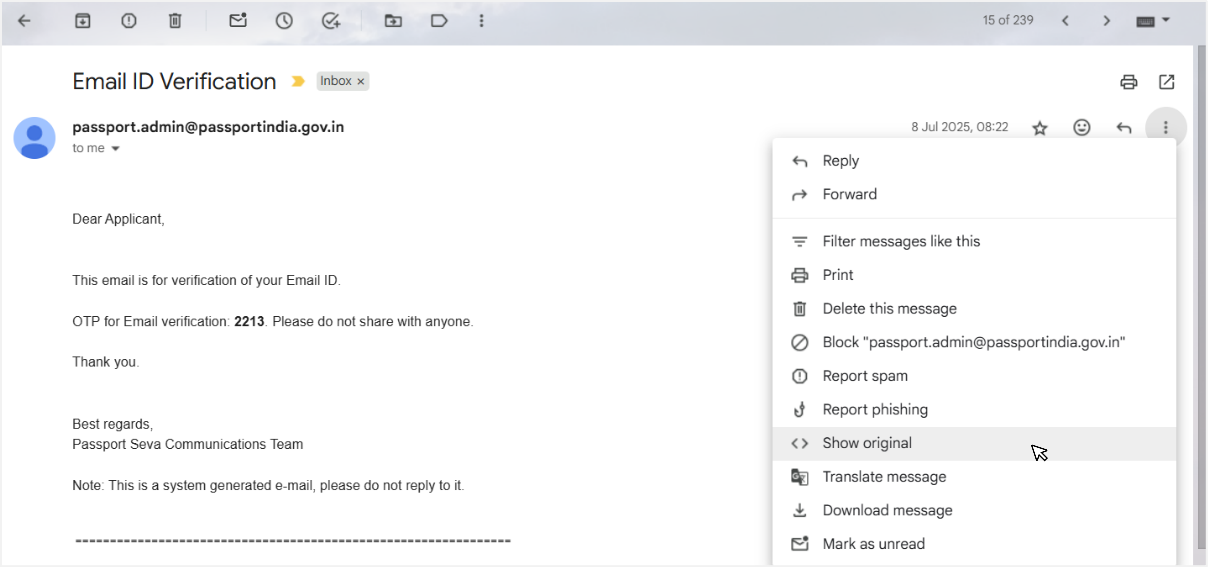
This email is for verification of your Email ID.

OTP for Email verification: **2213**. Please do not share with anyone.

Thank you.

2. View Full Headers:

- In Gmail: Click on the three-dot menu → *Show Original*.
- In Outlook: Right-click the message → *View Source* or *Message Options*.



Email ID Verification Inbox ×

passport.admin@passportindia.gov.in
to me

8 Jul 2025, 08:22

Dear Applicant,

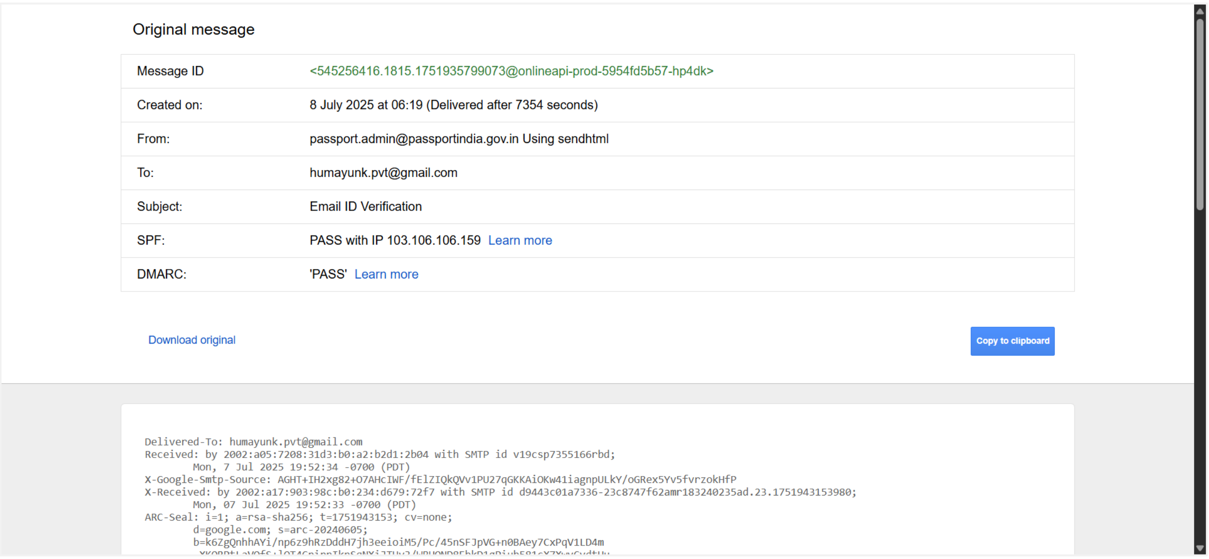
This email is for verification of your Email ID.

OTP for Email verification: **2213**. Please do not share with anyone.

Thank you.

Best regards,
Passport Seva Communications Team

Note: This is a system generated e-mail, please do not reply to it.



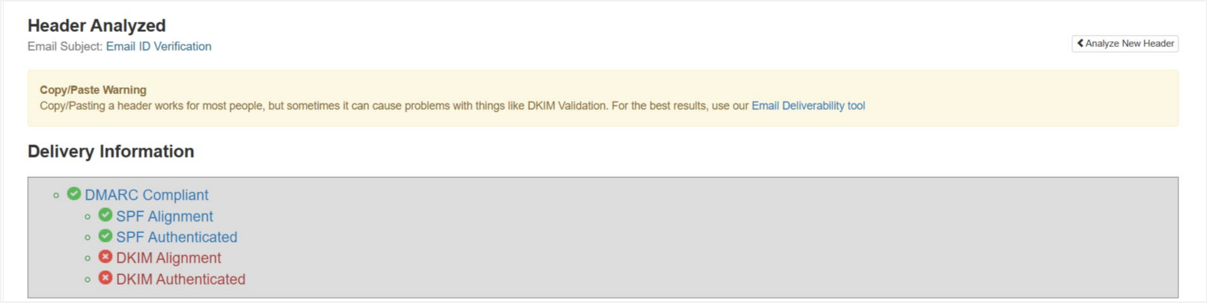
Original message

Message ID	<545256416.1815.1751935799073@onlineapi-prod-5954fd5b57-hp4dk>
Created on:	8 July 2025 at 06:19 (Delivered after 7354 seconds)
From:	passport.admin@passportindia.gov.in Using sendhtml
To:	humayunk.pvt@gmail.com
Subject:	Email ID Verification
SPF:	PASS with IP 103.106.106.159 Learn more
DMARC:	'PASS' Learn more

```
Delivered-To: humayunk.pvt@gmail.com
Received: by 2002:a05:7208:31d3:b0:a2:b2d1:2b04 with SMTP id v19csp7355166rbd;
        Mon, 7 Jul 2025 19:52:34 -0700 (PDT)
X-Google-Smtp-Source: AGHT+IH2xg82+O7AHcIWF/fElZIQkQVv1PU27qGKKAiOKw41iagnpULkY/oGRex5Yv5fvrzokHfP
X-Received: by 2002:a17:903:98c:b0:234:d679:72f7 with SMTP id d9443c01a7336-23c8747f62amr183240235ad.23.1751943153980;
        Mon, 07 Jul 2025 19:52:33 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1751943153; cv=none;
        d=google.com; s=arc-20240605;
        b=k6ZgQnhhAYi/np6z9hRzDddH7jh3eeioiM5/Pc/45nSFJpVG+n0BAey7CxPqV1LD4m
```

3. **Analyze the "Received" Fields:**
   - Identify the mail servers and routing hops.
   - The **first "Received"** line (at the bottom) is usually the original sender's server.
4. **Locate IP Addresses:**
   - Use the IPs found in Received or X-Originating-IP headers.
5. **Geo-locate IPs (Optional):**
   - Use websites like iplocation.net or geoiptool.com.
6. **Check Email Client Info:**
   - Look for User-Agent: or X-Mailer: to determine the sender's software.

Using MX Analyzer Tool:



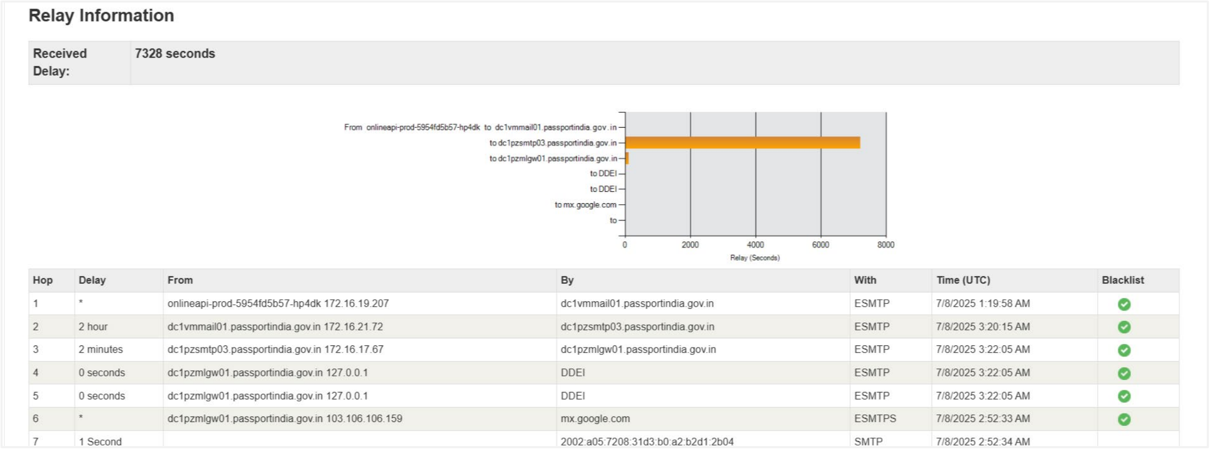
Header Analyzed

Email Subject: Email ID Verification

Copy/Paste Warning
Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our Email Deliverability tool

Delivery Information

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

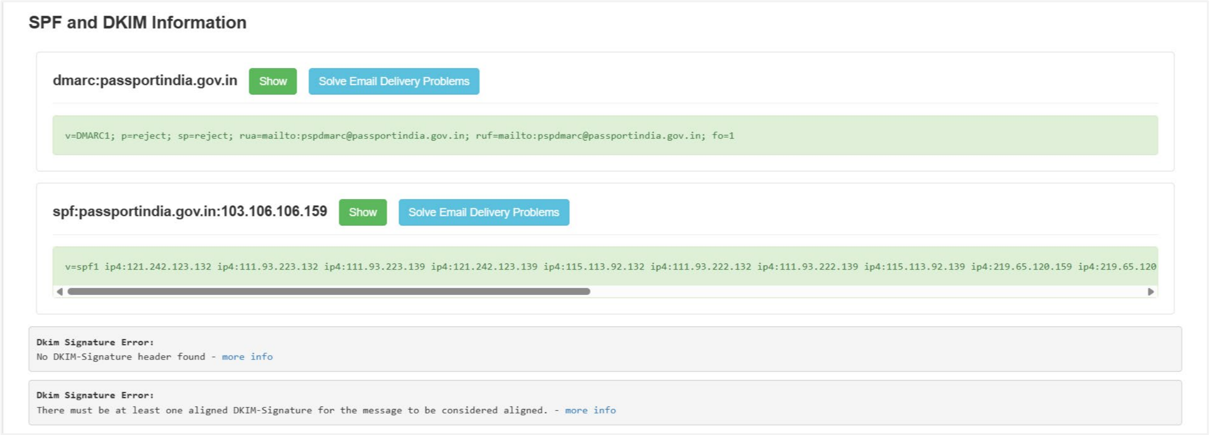


Relay Information

Received Delay:	7328 seconds

From onlineapi-prod-5954fd5b57-hp4dk to dc1vmmail01.passportindia.gov.in
to dc1pzsmtp03.passportindia.gov.in
to dc1pzmlgw01.passportindia.gov.in
to DDEI
to DDEI
to mx.google.com
to
0
2000
4000
6000
8000
Relay (Seconds)

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	onlineapi-prod-5954fd5b57-hp4dk 172.16.19.207	dc1vmmail01.passportindia.gov.in	ESMTP	7/8/2025 1:19:58 AM	✓
2	2 hour	dc1vmmail01.passportindia.gov.in 172.16.21.72	dc1pzsmtp03.passportindia.gov.in	ESMTP	7/8/2025 3:20:15 AM	✓
3	2 minutes	dc1pzsmtp03.passportindia.gov.in 172.16.17.67	dc1pzmlgw01.passportindia.gov.in	ESMTP	7/8/2025 3:22:05 AM	✓
4	0 seconds	dc1pzmlgw01.passportindia.gov.in 127.0.0.1	DDEI	ESMTP	7/8/2025 3:22:05 AM	✓
5	0 seconds	dc1pzmlgw01.passportindia.gov.in 127.0.0.1	DDEI	ESMTP	7/8/2025 3:22:05 AM	✓
6	*	dc1pzmlgw01.passportindia.gov.in 103.106.106.159	mx.google.com	ESMTPS	7/8/2025 2:52:33 AM	✓
7	1 Second		2002:a05:7208:31d3:b0:a2:b2d1:2b04	SMTP	7/8/2025 2:52:34 AM	



SPF and DKIM Information

dmarc:passportindia.gov.in

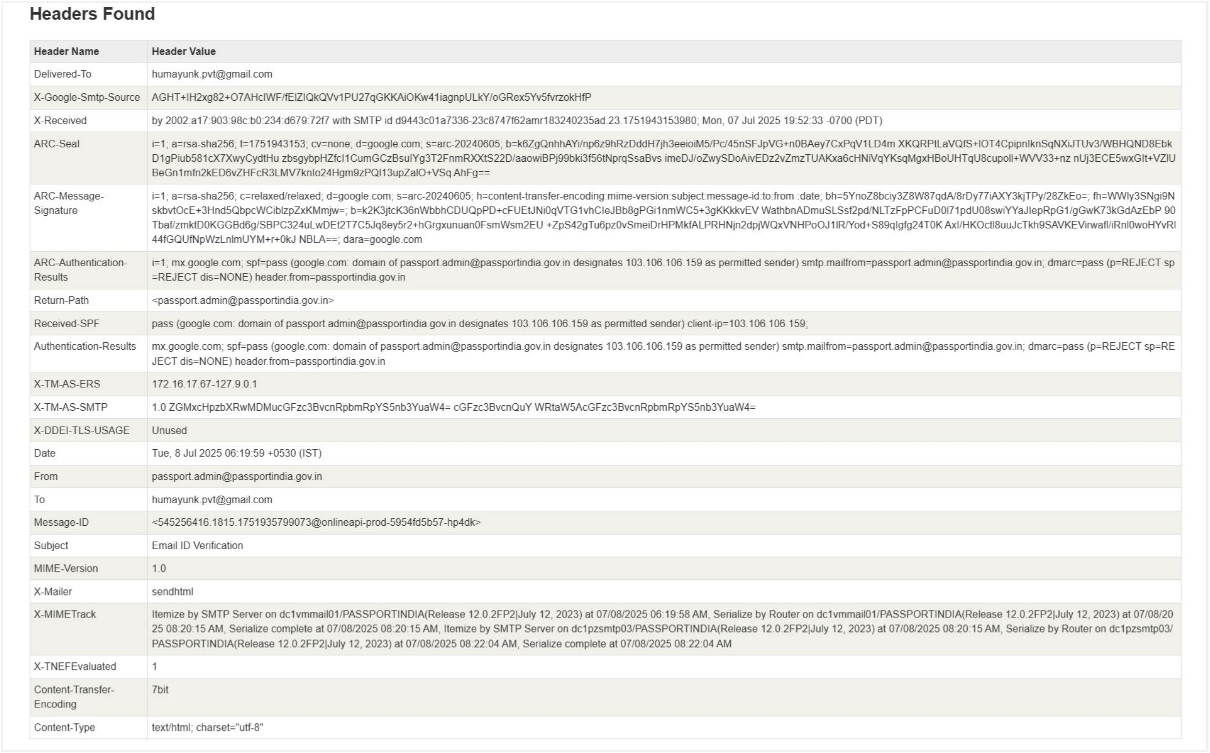
```
v=DMARC1; p=reject; sp=reject; rua=mailto:pspdmarc@passportindia.gov.in; ruf=mailto:pspdmarc@passportindia.gov.in; fo=1
```

spf:passportindia.gov.in:103.106.106.159

```
v=spf1 ip4:121.242.123.132 ip4:111.93.223.132 ip4:111.93.223.139 ip4:121.242.123.139 ip4:115.113.92.132 ip4:111.93.222.132 ip4:111.93.222.139 ip4:115.113.92.139 ip4:219.65.120.159 ip4:219.65.120
```

```
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
```



Headers Found

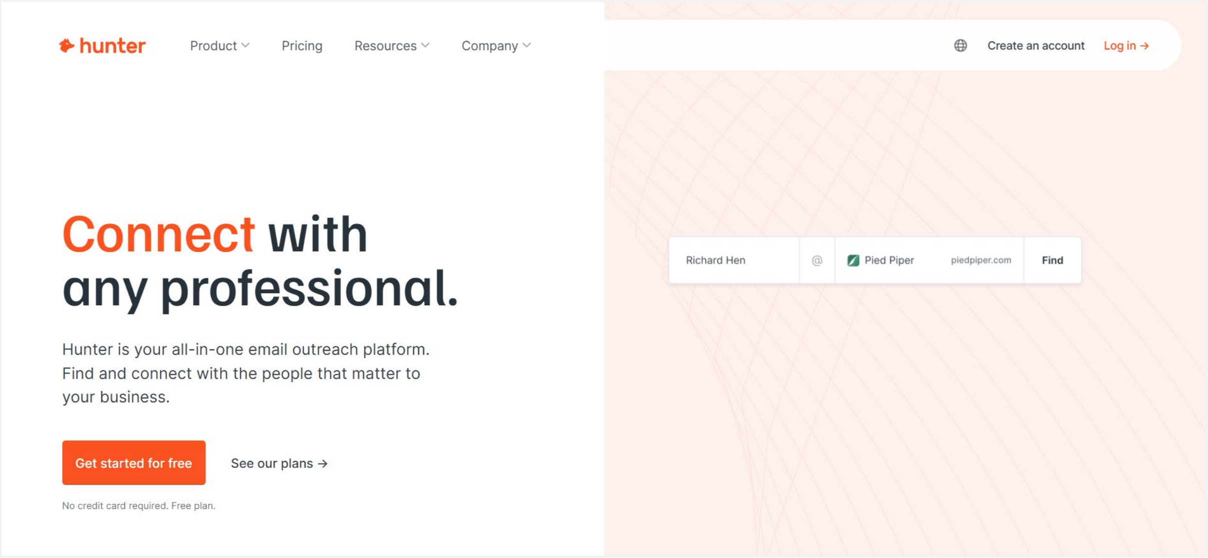
Header Name	Header Value
Delivered-To	humayunk.pvt@gmail.com
X-Google-Smtp-Source	AGHT+IH2xg82+O7AHclWF/fEIZIQkQVv1PU27qGKKAiOKw41iagnpULkY/oGRex5Yv5fvrzokHfP
X-Received	by 2002:a17:903:98c:b0:234:d679:72f7 with SMTP id d9443c01a7336-23c8747f62amr183240235ad.23.1751943153980; Mon, 07 Jul 2025 19:52:33 -0700 (PDT)
ARC-Seal	i=1; a=rsa-sha256; t=1751943153; cv=none; d=google.com; s=arc-20240605; b=k6ZgQnhhAYi/np6z9hRzDddH7jh3eeioiM5/Pc/45nSFJpVG+n0BAey7CxPqV1LD4m XKQRPtLaVQfS+IOT4CpipnlknSqNXiJTUv3/WBHQND8Ebk D1gPiub581cX7XwyCydtHu zbsgybpHZfcl1CumGCzBsulYg3T2FnmRXXtS22D/aaowiBPj99bki3f56tNprqSsaBvs imeDJ/oZwySDoAivEDz2vZmzTUAKxa6cHNiVqYKsqMgxHBoUHTqU8cupoll+WVV33+nz nUj3ECE5wxGlt+VZlU BeGn1mfn2kED6vZHFcR3LMV7knlo24Hgm9zPQl13upZalO+VSq AhFg==
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; bh=5YnoZ8bciy3Z8W87qdA/8rDy77iAXY3kjTPy/28ZkEo=; fh=WWly3SNgi9N skbvtOcE+3Hnd5QbpcWCiblzpZxKMmjw=; b=k2K3jtcK36nWbbhCDUQpPD+cFUEtJNi0qVTG1vhCleJBb8gPGi1nmWC5+3gKKkkvEV WathbnADmuSLSsf2pd/NLTzFpPCFuD0l71pdU08swiYYaJlepRpG1/gGwK73kGdAzEbP 90 Tbaf/zmktD0KGGBd6g/SBPC324uLwDEt2T7C5Jq8ey5r2+hGrgxunuan0FsmWsm2EU +ZpS42gTu6pz0vSmeiDrHPMkfALPRHNjn2dpjWQxVNHPoOJ1lR/Yod+S89qlgfg24T0K Axl/HKOctl8uuJcTkh9SAVKEVirwafl/iRnl0woHYvRl 44fGQUfNpWzLnlmUYM+r+0kJ NBLA==; dara=google.com
ARC-Authentication-Results	i=1; mx.google.com; spf=pass (google.com: domain of passport.admin@passportindia.gov.in designates 103.106.106.159 as permitted sender) smtp.mailfrom=passport.admin@passportindia.gov.in; dmarc=pass (p=REJECT sp =REJECT dis=NONE) header.from=passportindia.gov.in
Return-Path	<passport.admin@passportindia.gov.in>
Received-SPF	pass (google.com: domain of passport.admin@passportindia.gov.in designates 103.106.106.159 as permitted sender) client-ip=103.106.106.159;
Authentication-Results	mx.google.com; spf=pass (google.com: domain of passport.admin@passportindia.gov.in designates 103.106.106.159 as permitted sender) smtp.mailfrom=passport.admin@passportindia.gov.in; dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=passportindia.gov.in
X-TM-AS-ERS	172.16.17.67-127.9.0.1
X-TM-AS-SMTP	1.0 ZGMxcHpzbXRwMDMucGFzc3BvcnRpbmRpYS5nb3YuaW4= cGFzc3BvcnQuY WRtaW5AcGFzc3BvcnRpbmRpYS5nb3YuaW4=
X-DDEI-TLS-USAGE	Unused
Date	Tue, 8 Jul 2025 06:19:59 +0530 (IST)
From	passport.admin@passportindia.gov.in
To	humayunk.pvt@gmail.com
Message-ID	<545256416.1815.1751935799073@onlineapi-prod-5954fd5b57-hp4dk>
Subject	Email ID Verification
MIME-Version	1.0
X-Mailer	sendhtml
X-MIMETrack	Itemize by SMTP Server on dc1vmmail01/PASSPORTINDIA(Release 12.0.2FP2|July 12, 2023) at 07/08/2025 06:19:58 AM, Serialize by Router on dc1vmmail01/PASSPORTINDIA(Release 12.0.2FP2|July 12, 2023) at 07/08/2025 08:20:15 AM, Serialize complete at 07/08/2025 08:20:15 AM, Itemize by SMTP Server on dc1pzsmtp03/PASSPORTINDIA(Release 12.0.2FP2|July 12, 2023) at 07/08/2025 08:20:15 AM, Serialize by Router on dc1pzsmtp03/ PASSPORTINDIA(Release 12.0.2FP2|July 12, 2023) at 07/08/2025 08:22:04 AM, Serialize complete at 07/08/2025 08:22:04 AM
X-TNEFEvaluated	1
Content-Transfer-Encoding	7bit
Content-Type	text/html; charset="utf-8"

PART B: Email Enumeration using Hunter.io

Step-by-Step Procedure:

1. Go to Hunter.io:

- Open https://hunter.io in your browser.



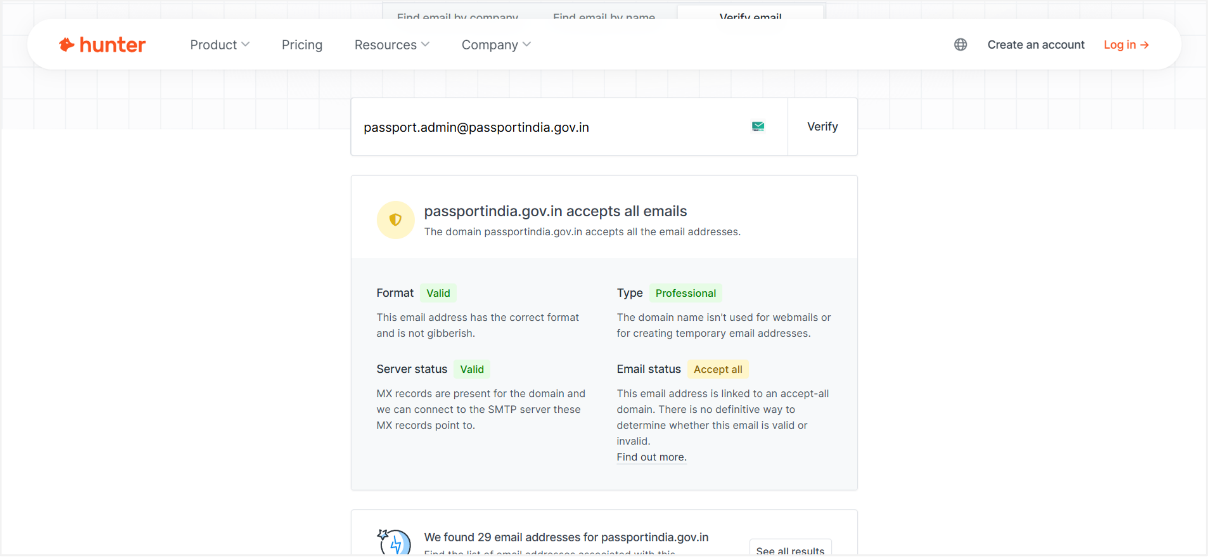
Connect with any professional.

Hunter is your all-in-one email outreach platform. Find and connect with the people that matter to your business.

No credit card required. Free plan.

2. Search for Emails:

- Enter the **target domain** (e.g., example.com) in the search bar.



passport.admin@passportindia.gov.in

passportindia.gov.in accepts all emails

The domain passportindia.gov.in accepts all the email addresses.

Format Valid

This email address has the correct format and is not gibberish.

Type Professional

The domain name isn't used for webmails or for creating temporary email addresses.

Server status Valid

MX records are present for the domain and we can connect to the SMTP server these MX records point to.

Email status Accept all

This email address is linked to an accept-all domain. There is no definitive way to determine whether this email is valid or invalid.

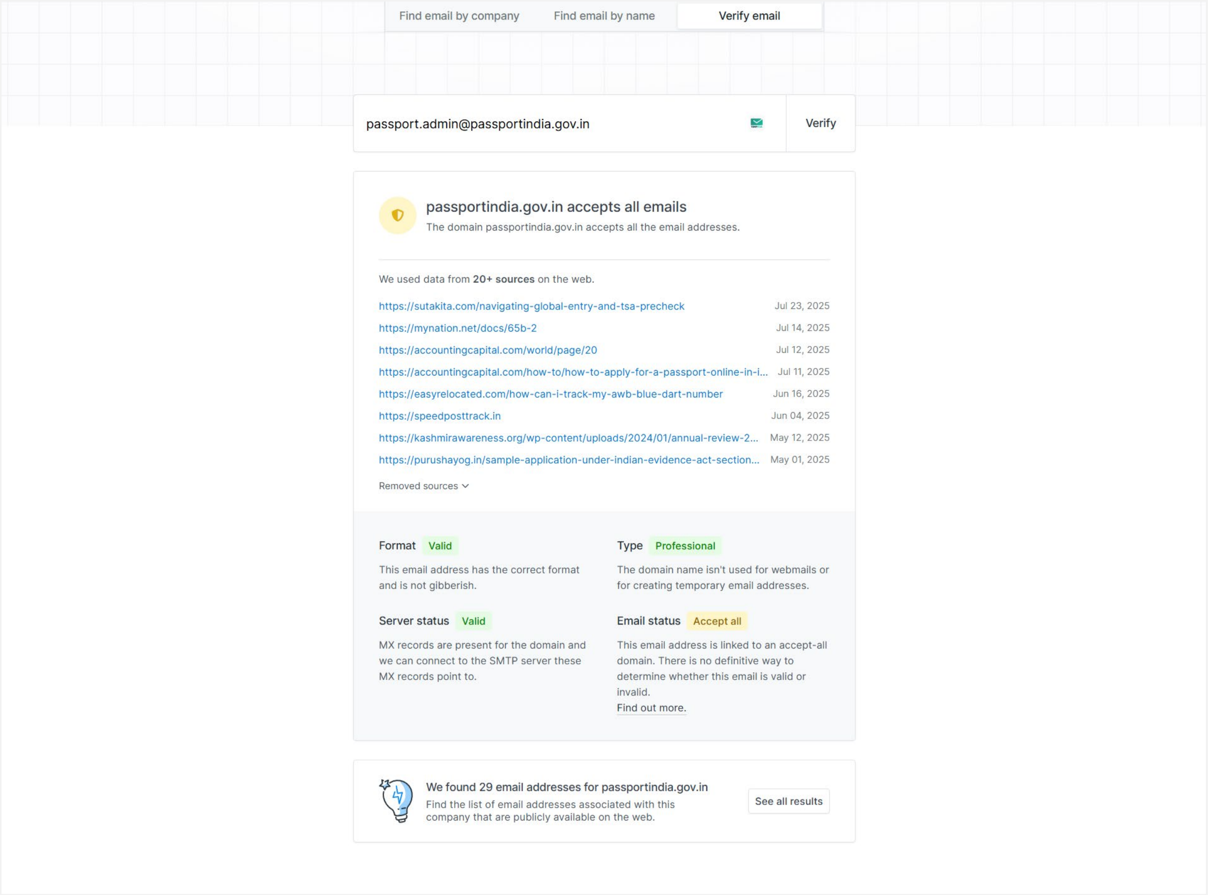
Find out more.

We found 29 email addresses for passportindia.gov.in

Find the list of email addresses associated with this

3. Analyze the Results:

- View the list of found emails along with job titles, sources, and confidence scores.



passport.admin@passportindia.gov.in

passportindia.gov.in accepts all emails

The domain passportindia.gov.in accepts all the email addresses.

We used data from **20+ sources** on the web.

https://sutakita.com/navigating-global-entry-and-tsa-precheck	Jul 23, 2025
https://mynation.net/docs/65b-2	Jul 14, 2025
https://accountingcapital.com/world/page/20	Jul 12, 2025
https://accountingcapital.com/how-to/how-to-apply-for-a-passport-online-in-i...	Jul 11, 2025
https://easyrelocated.com/how-can-i-track-my-awb-blue-dart-number	Jun 16, 2025
https://speedposttrack.in	Jun 04, 2025
https://kashmirawareness.org/wp-content/uploads/2024/01/annual-review-2...	May 12, 2025
https://purushayog.in/sample-application-under-indian-evidence-act-section...	May 01, 2025

Removed sources ⌄

Format Valid

This email address has the correct format and is not gibberish.

Type Professional

The domain name isn't used for webmails or for creating temporary email addresses.

Server status Valid

MX records are present for the domain and we can connect to the SMTP server these MX records point to.

Email status Accept all

This email address is linked to an accept-all domain. There is no definitive way to determine whether this email is valid or invalid.
Find out more.

We found 29 email addresses for passportindia.gov.in

Find the list of email addresses associated with this company that are publicly available on the web.

Conclusion

In this experiment, we successfully:

- **Analyzed email headers** to extract the sender's IP address, routing information, and metadata like email clients.
- **Enumerated email addresses** linked to a domain using tools like **Hunter.io**, which can help in OSINT investigations or security assessments.

This practical strengthens our understanding of how cyber investigators and security analysts trace and gather email-based intelligence using OSINT techniques.