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

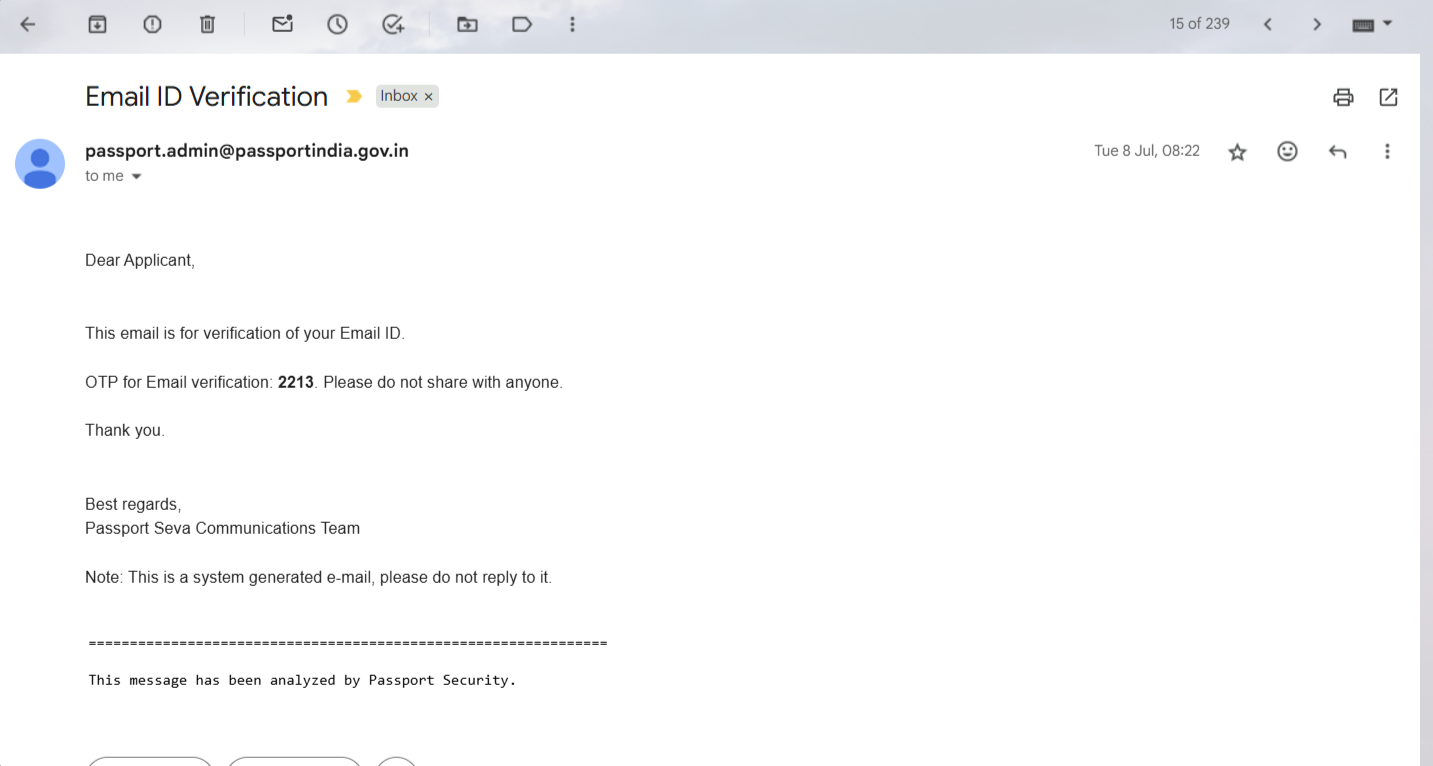
🔧 **Tools Used:**

* Hunter.io (Web-based)

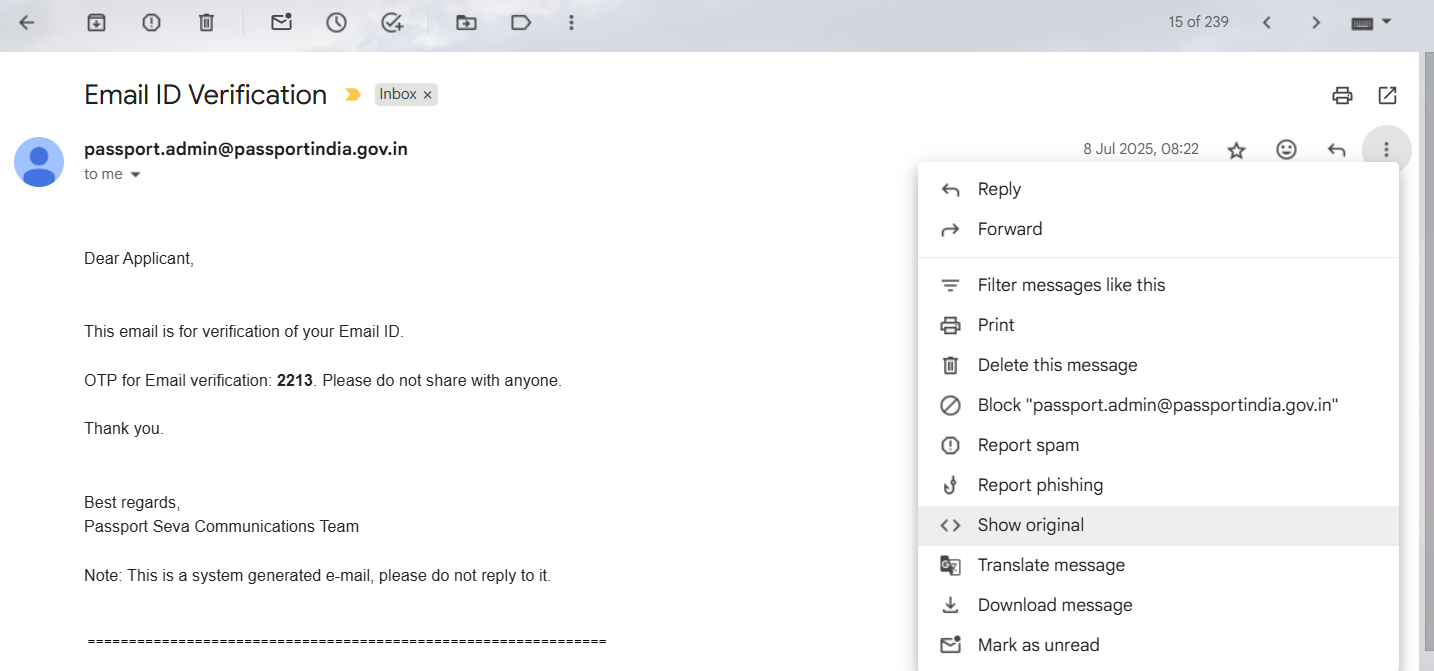
**PART A: Email Header Analysis:**

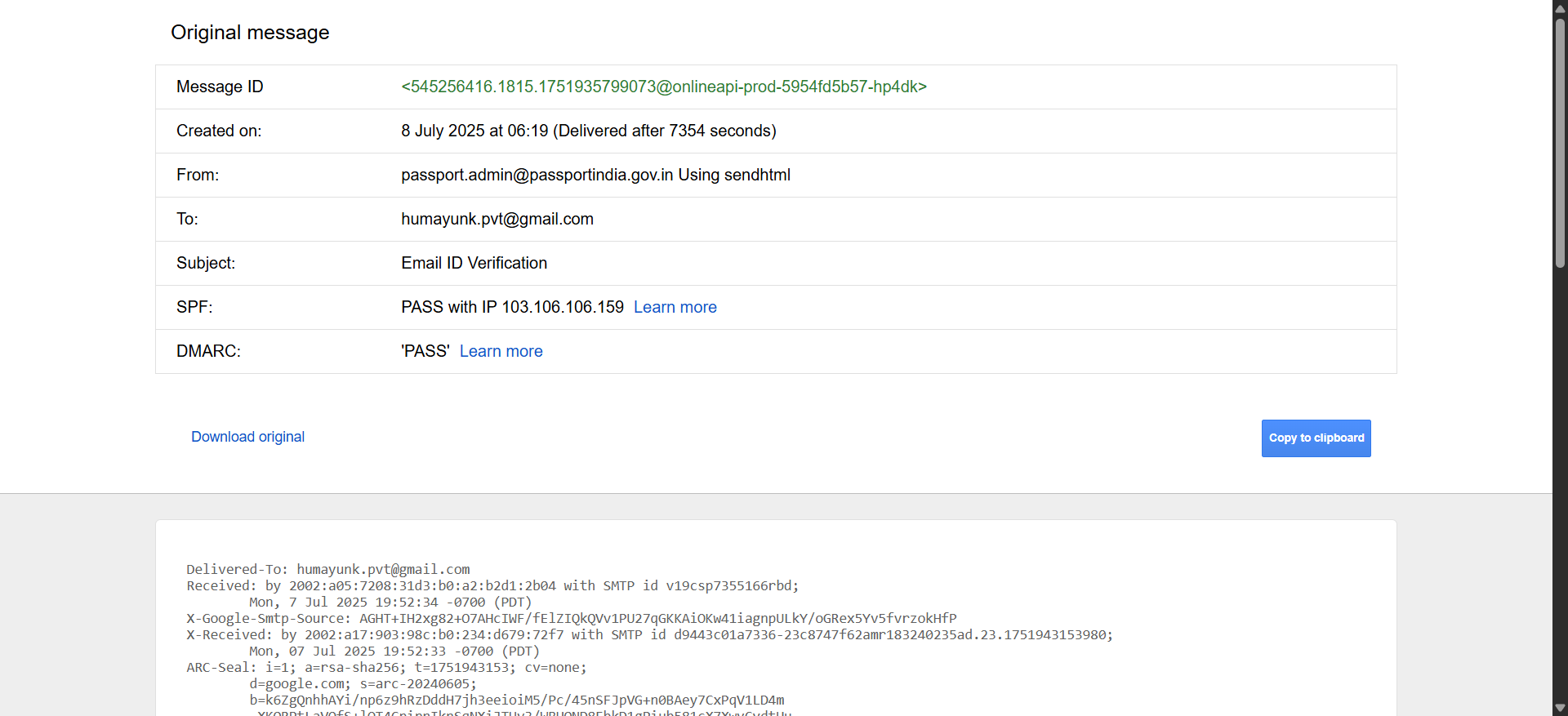
**Step-by-Step Procedure:**

1. **Access the Email:**
   * Open your email client (e.g., Gmail or Outlook).
   * Locate a suspicious or test email.



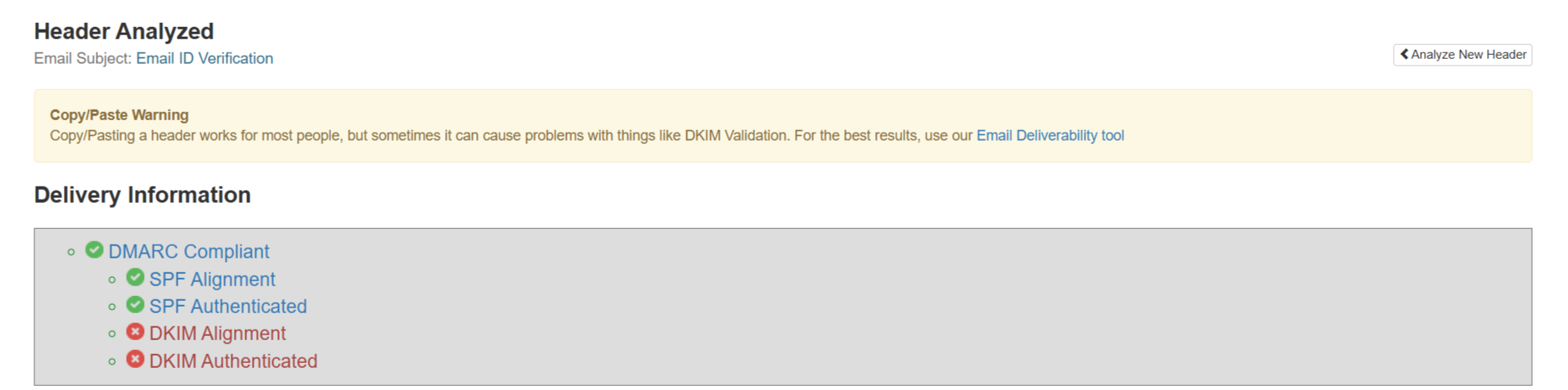
1. **View Full Headers:**
   * In Gmail: Click on the three-dot menu → *Show Original*.
   * In Outlook: Right-click the message → *View Source* or *Message Options*.

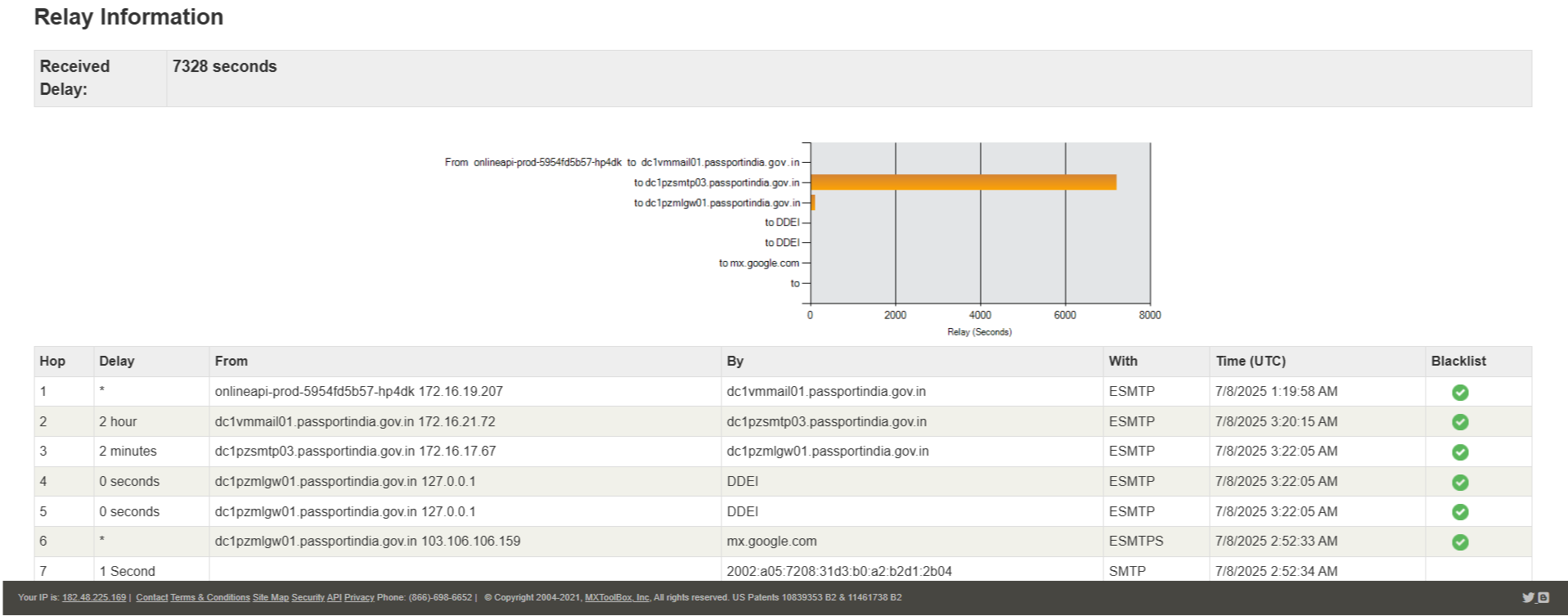


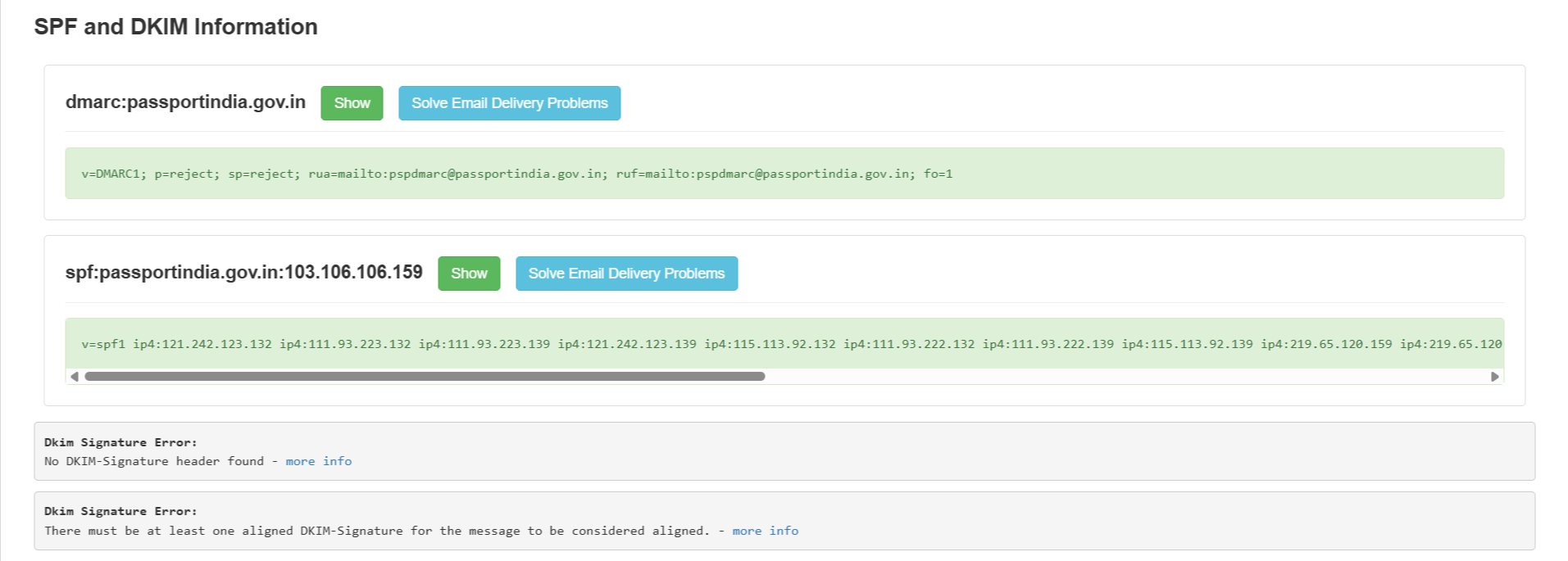


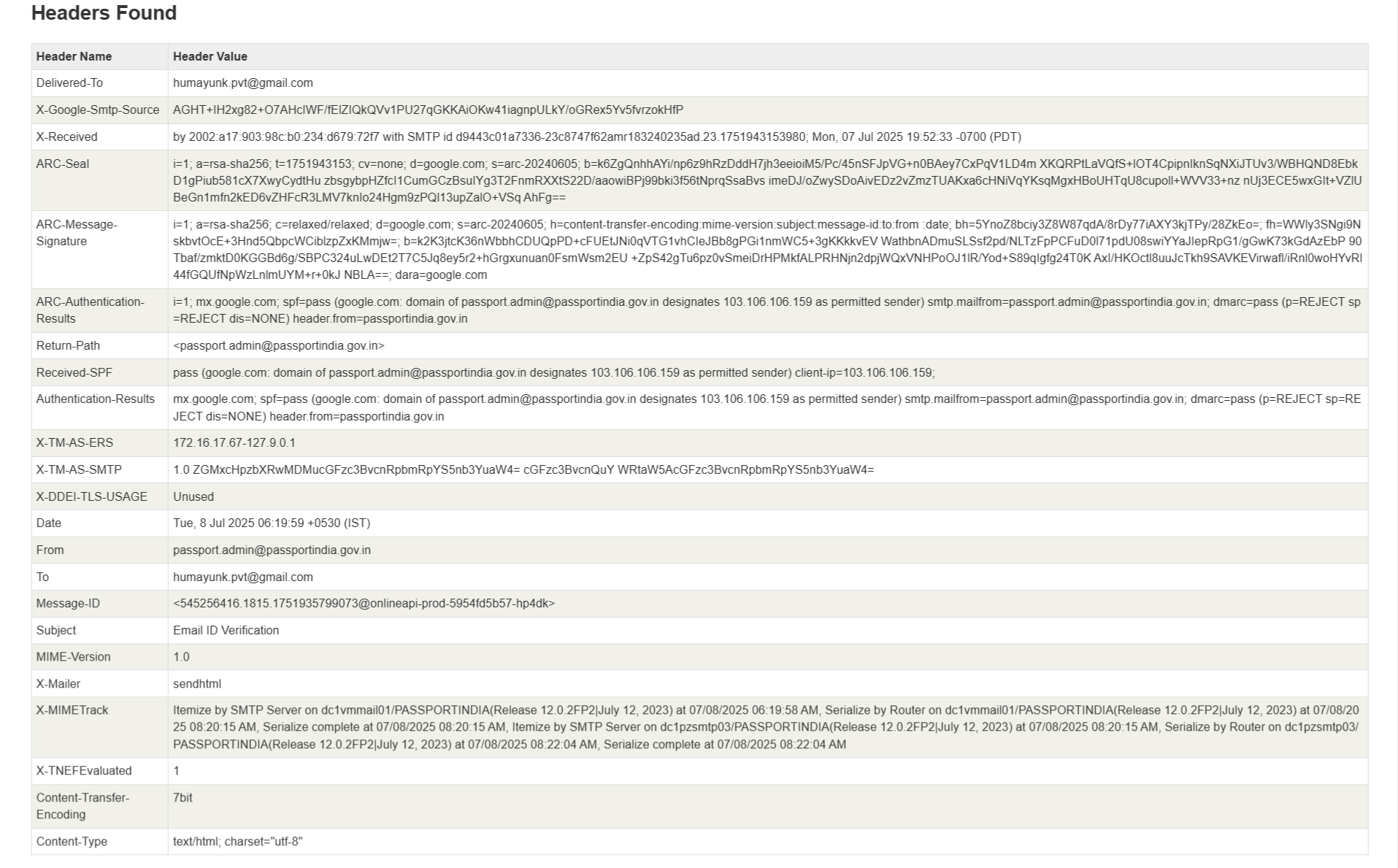
1. **Analyze the "Received" Fields:**
   * Identify the mail servers and routing hops.
   * The **first "Received"** line (at the bottom) is usually the original sender’s server.
2. **Locate IP Addresses:**
   * Use the IPs found in Received or X-Originating-IP headers.
3. **Geo-locate IPs (Optional):**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

**Using MX Analyzer Tool:**

****

****

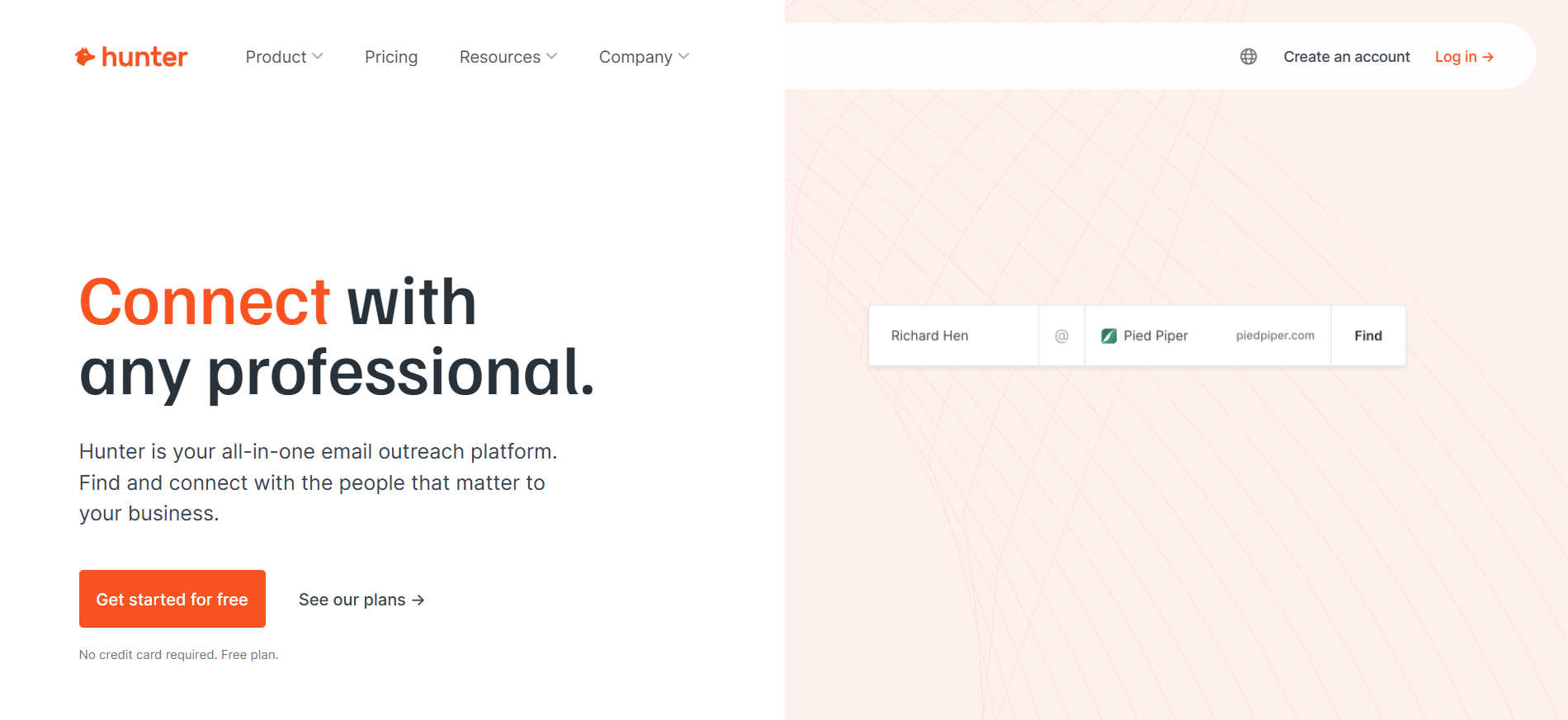
****

****

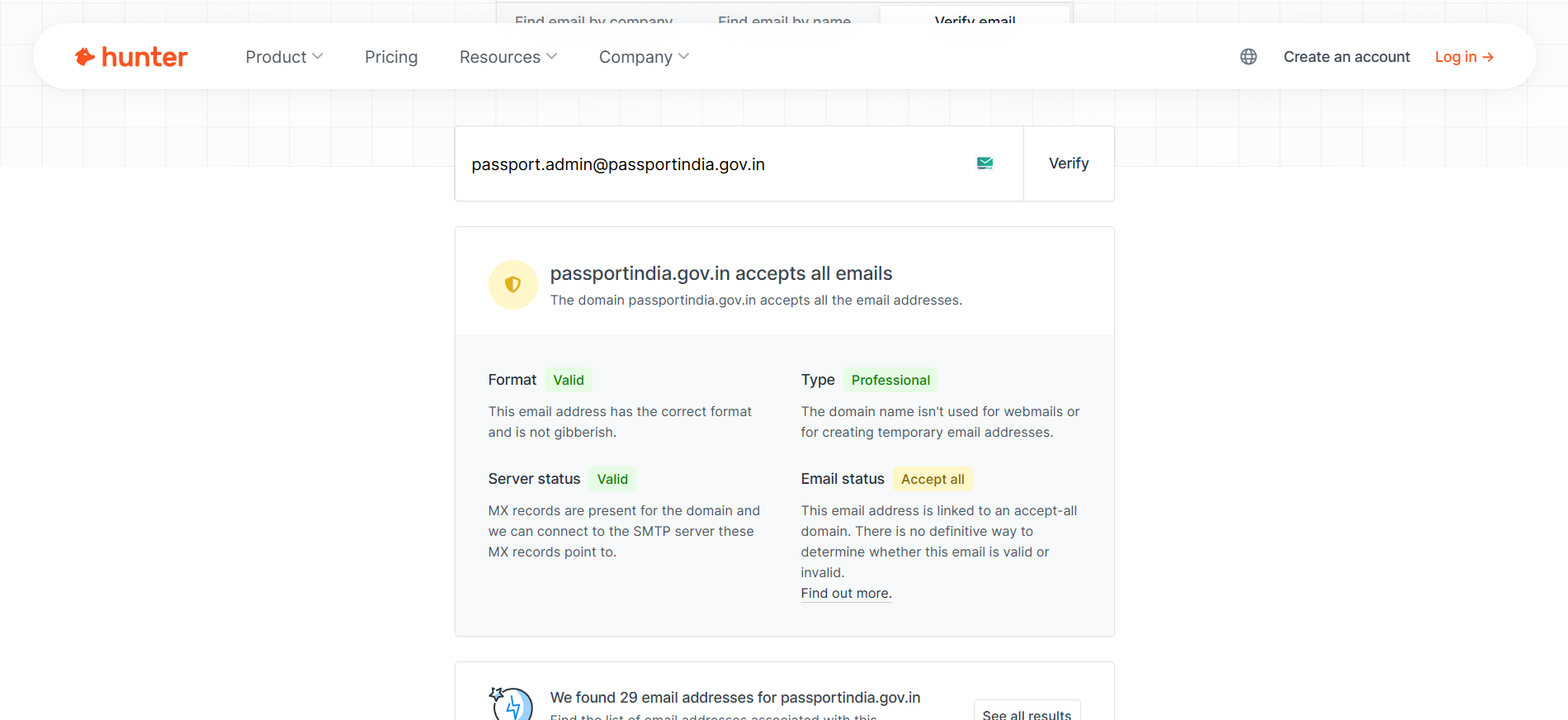
**PART B: Email Enumeration using Hunter.io**

**Step-by-Step Procedure:**

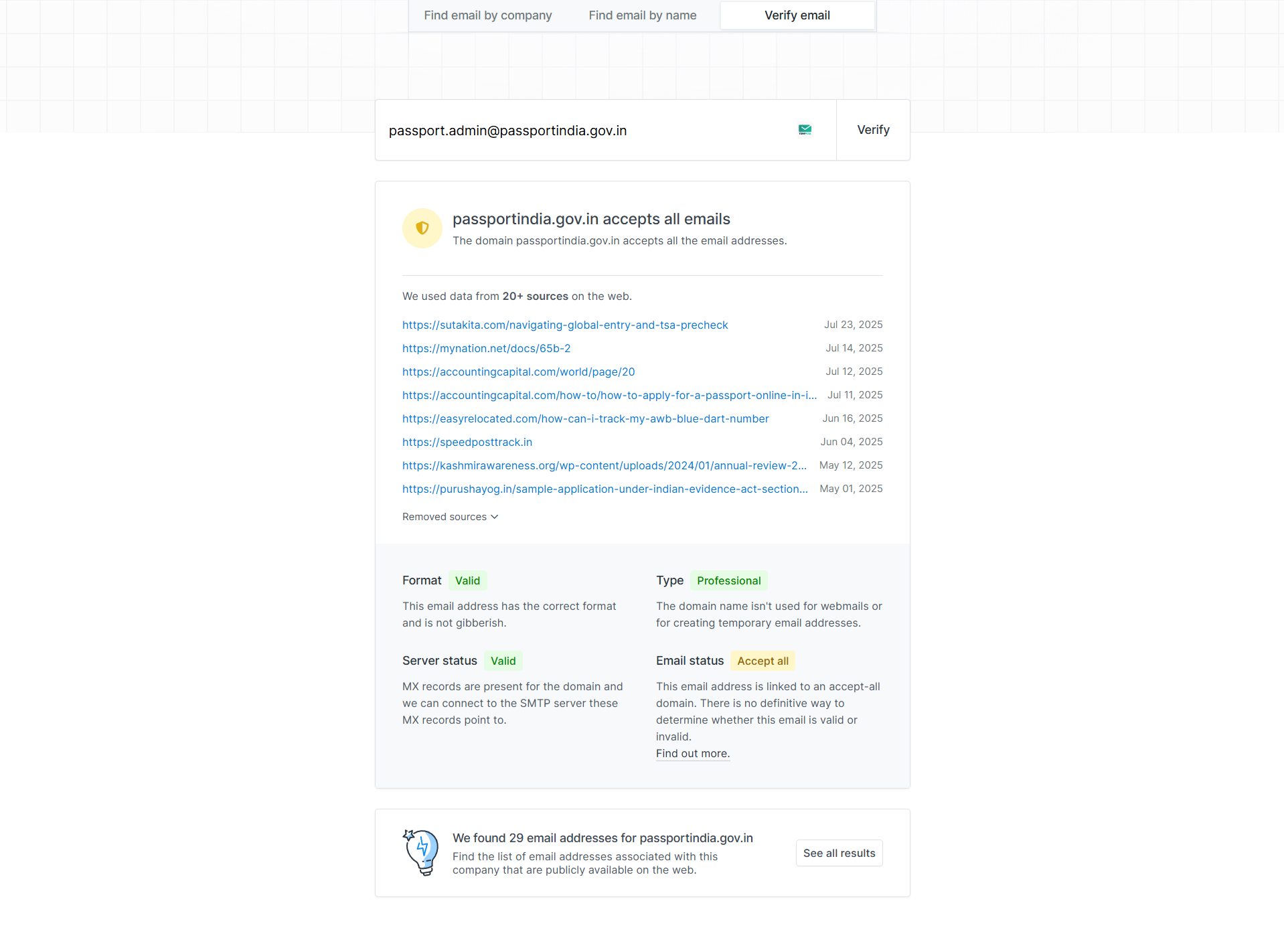
1. **Go to Hunter.io:**
   * Open <https://hunter.io> in your browser.



1. **Search for Emails:**
   * Enter the **target domain** (e.g., example.com) in the search bar.



1. **Analyze the Results:**
   * View the list of found emails along with job titles, sources, and confidence scores.



**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.