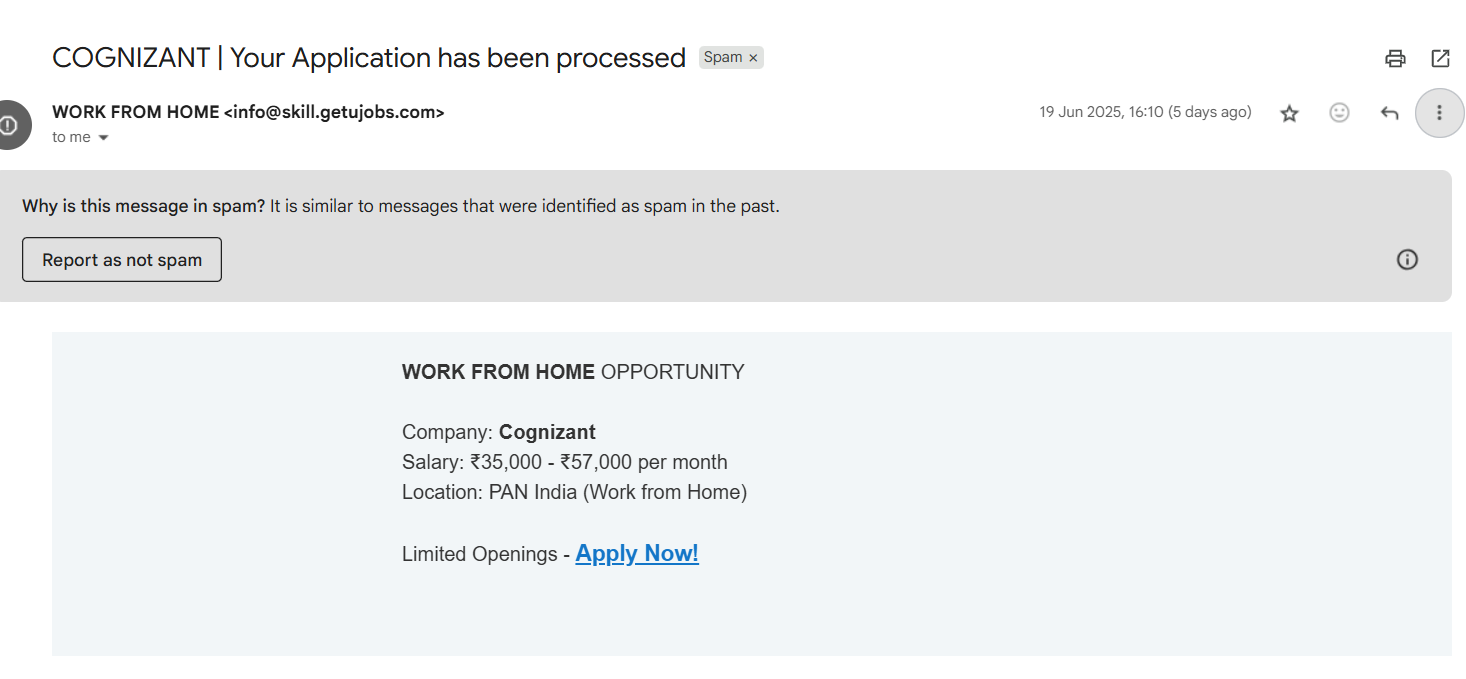
TASK-2: **Analyze a Phishing Email Sample**

**Step 1: Obtain a Sample Phishing Email**

* **Email Subject:** *COGNIZANT | Your Application has been processed*
* **Sender Email:** info@skill.getujobs.com
* **Date:** 19 June 2025
* **Claim:** Work-from-home opportunity at Cognizant

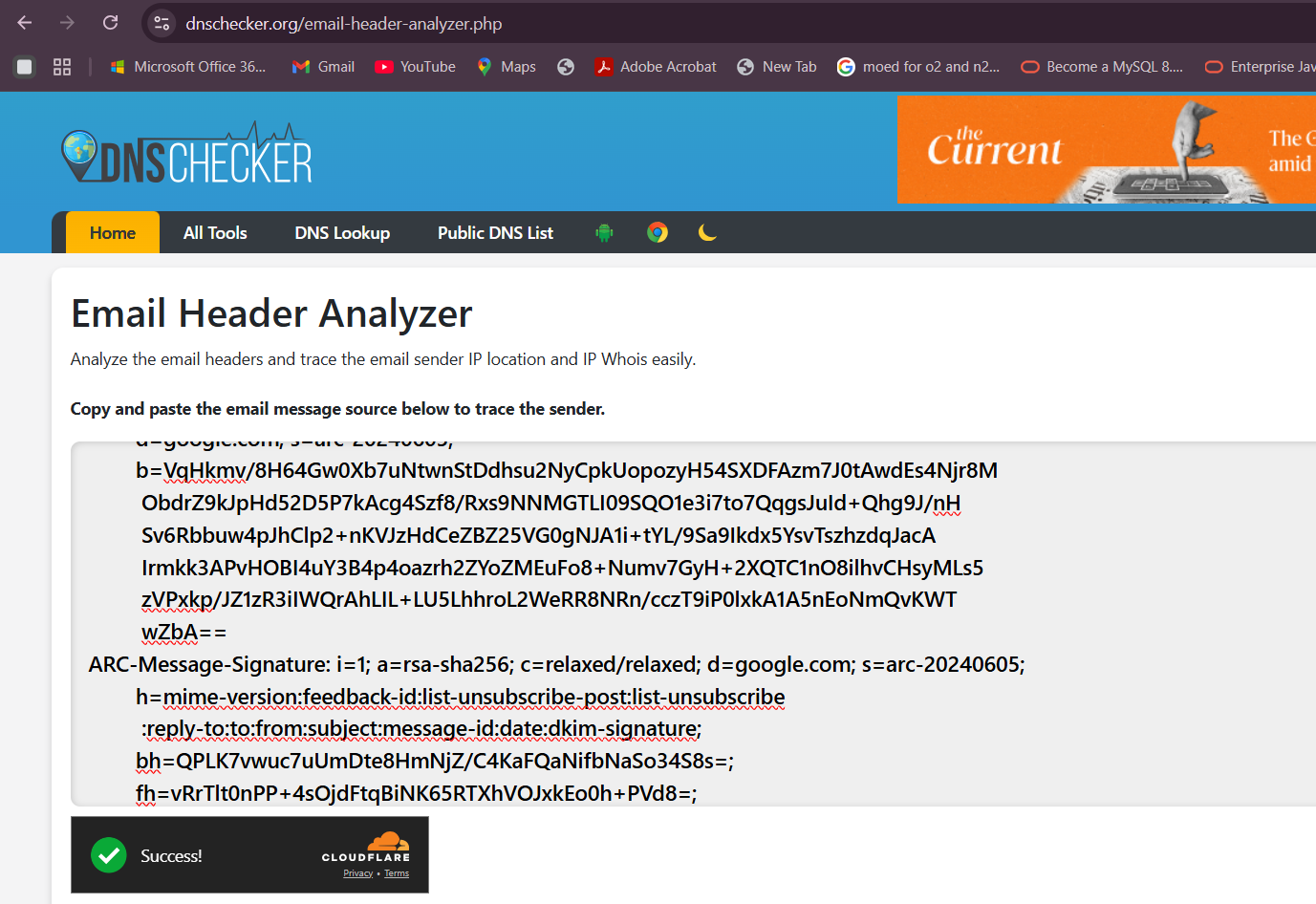


**Step 2: Examine Sender’s Email Address**

* The email claims to be from Cognizant but uses **@skill.getujobs.com** — **this is not an official Cognizant domain**.
* **Red Flag:** Fake or misleading domain name to **spoof a known company**.

**Step 3: Check Email Headers**

* Not visible in the screenshot, but they should be reviewed using tools like:
  + Google Admin Toolbox
  + DNSCHECKER.ORG ,MXToolbox Email Header Analyzer
* Look for:
  + SPF/DKIM failures
  + Return-path mismatches
  + IP geolocation anomalies



**Step 4: Identify Suspicious Links or Attachments**

* The link **"Apply Now!"** is suspicious.
* It likely redirects to a **non-official job portal or credential-harvesting site**.
* Always **hover (don't click)** to verify where the link actually point.

**Step 5: Look for Urgent or Attractive Language**

* Phrases like:
  + *"Limited Openings"*
  + *"₹35,000 – ₹57,000/month"*
* These are designed to **create urgency or excitement**, pushing the user to act fast without verification.

**Step 6: Note Any Mismatched URLs**

* No full URLs shown in the screenshot, but link anchor text (Apply Now!) is generic.
* It likely **does not match** the displayed company name (Cognizant).

**Step 7: Verify Grammar and Formatting**

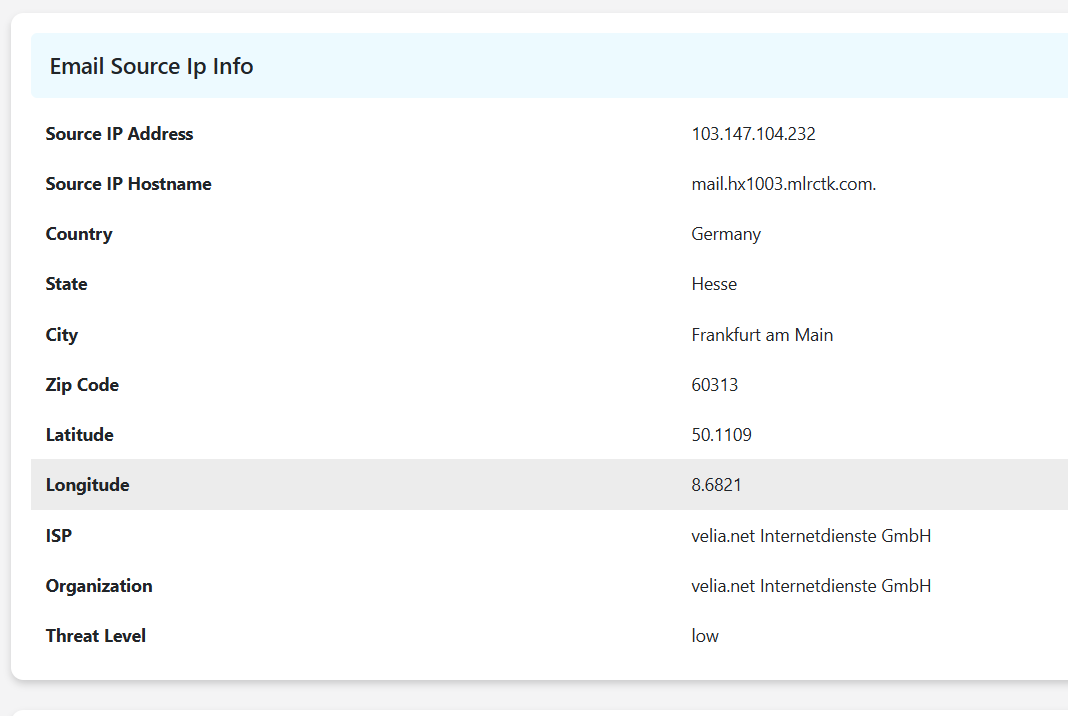
* No major grammar errors, but:
  + Text is overly generic.
  + Layout mimics legitimate job emails — a **common tactic**.

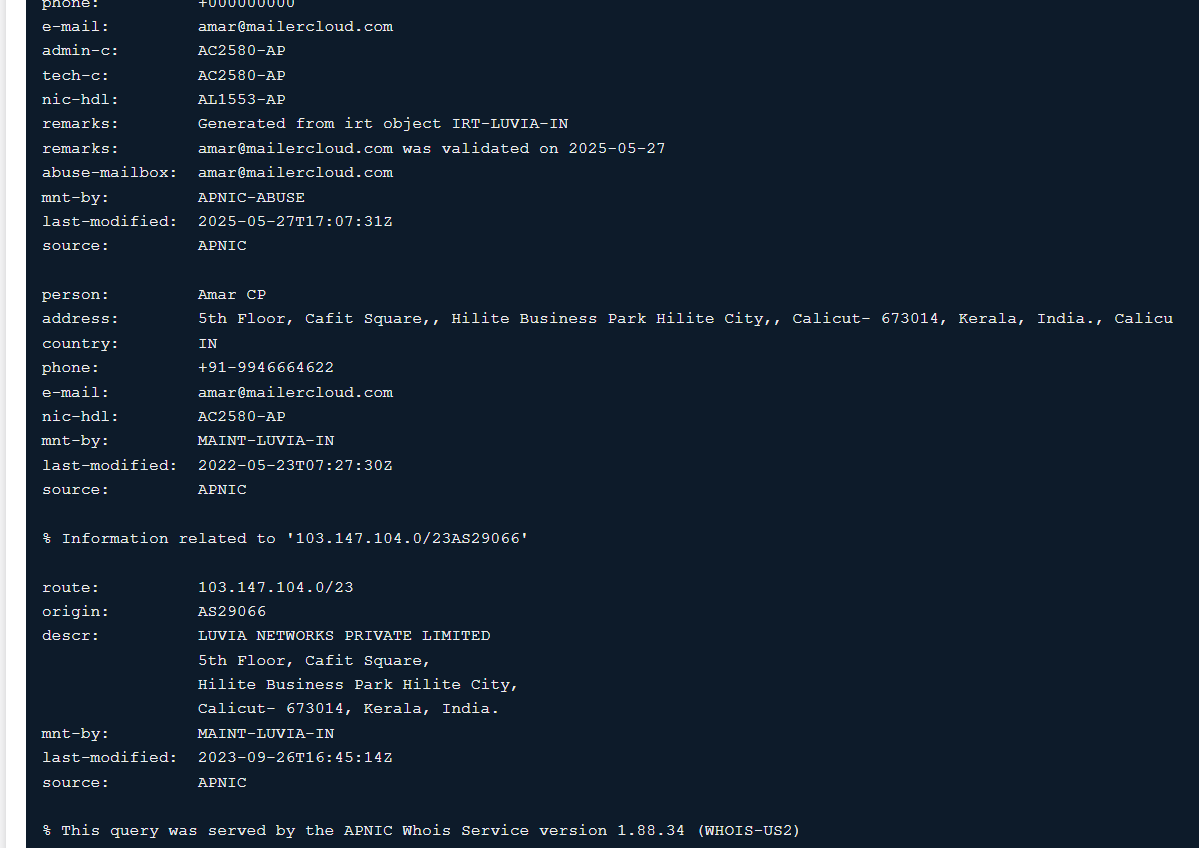
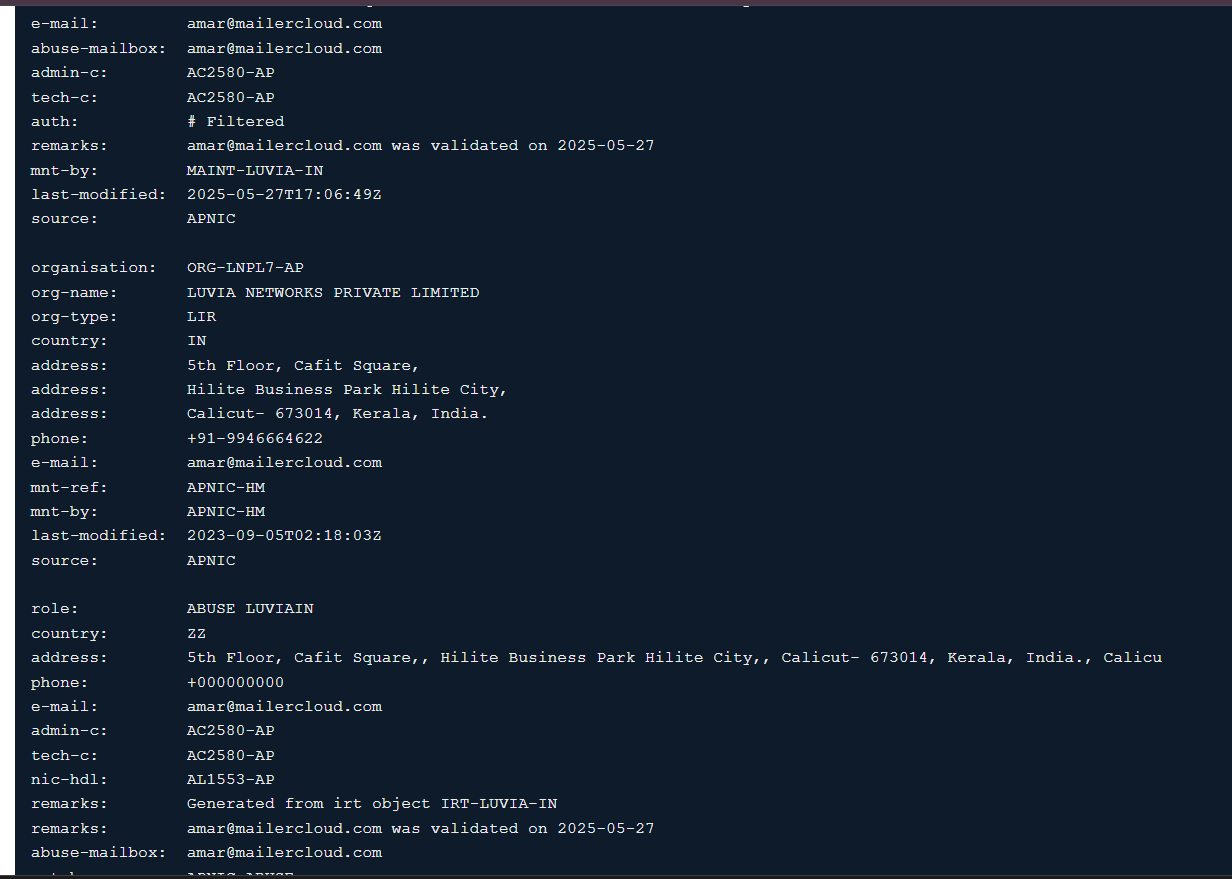
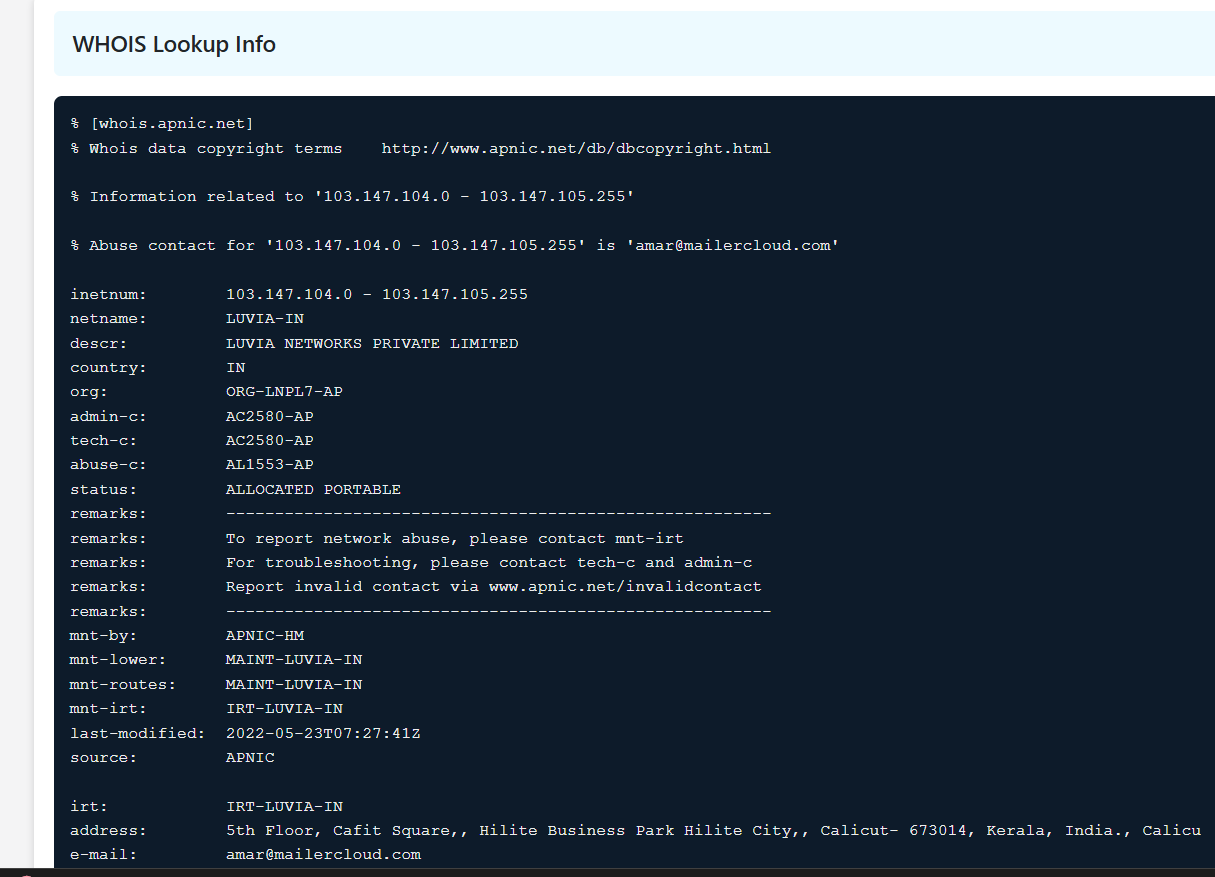
**Step 8: Summarize Traits Found**

| **Trait** | **Observation** |
| --- | --- |
| Sender mismatch | Not from official Cognizant domain |
| Link suspicion | Generic CTA (Call-to-Action) button |
| Urgency/lure | High salary, limited openings |
| Social engineering tactic | Preying on job seekers’ urgency and trust |
| Spam flag | Marked as spam due to similarity with past scams |

Analyze the email headers and trace the email sender IP location and IP Whois easily.

**Copy and paste the email message source below to trace the sender.**

****



### ****Observations:****

1. **Location Mismatch:**
   * **IP GeoLocation:** Frankfurt, Germany
   * **WHOIS Registry:** Indian firm — LUVIA NETWORKS PVT. LTD.
   * Likely use of **rented infrastructure or email delivery service** from a non-corporate domain.
2. **Suspicious Hosting/Relay:**
   * Domain mlrctk.com appears **unrelated to any official organization**, likely used as a temporary mail relay server.
3. **Phishing Risk:**
   * Despite a “low” threat level flag, this IP and email setup **clearly indicates phishing behavior**:
     + Non-matching sender domain
     + Offshore IP routes
     + WHOIS shows ownership by an entity likely offering bulk email services (Mailercloud)
     + Social engineering tactics used in email body

### ****Conclusion:****

The phishing email is **likely sent through a rented mail relay server (103.147.104.232)** hosted in Germany, owned by an Indian bulk mail provider. The infrastructure was likely used to **masquerade as a trusted brand (Cognizant)**, leveraging non-official domains and mass email tactics.