# Task 2: Analyse a Phishing Email Sample.

**( Its real suspicious mail I got)**

**1. Email Sample Details**

Subject: Interview Process – LIVE CODING Round

Sender: HR AIVOA <admin@aivoa.net> via mail3.zcsn.zcinsend.net

Reply-To: admin@aivoa.net

To: balaruban.2003@gmail.com

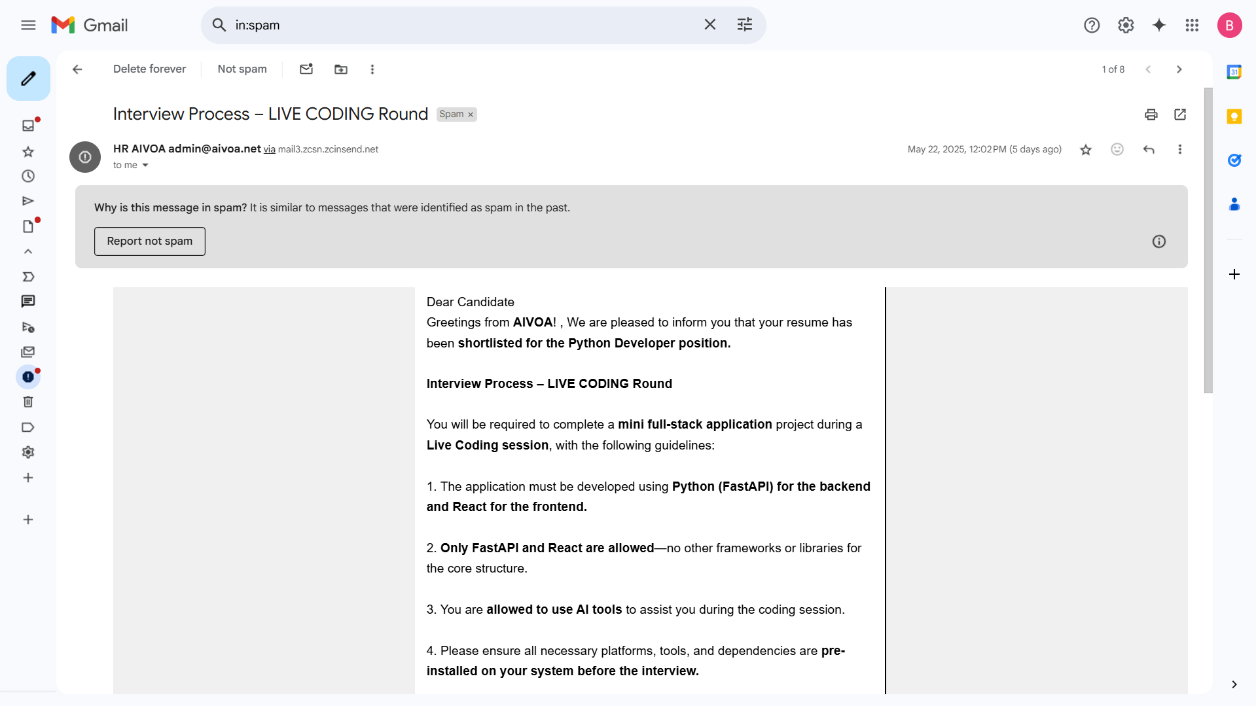
Date Received: May 22, 2025, 12:02 PM

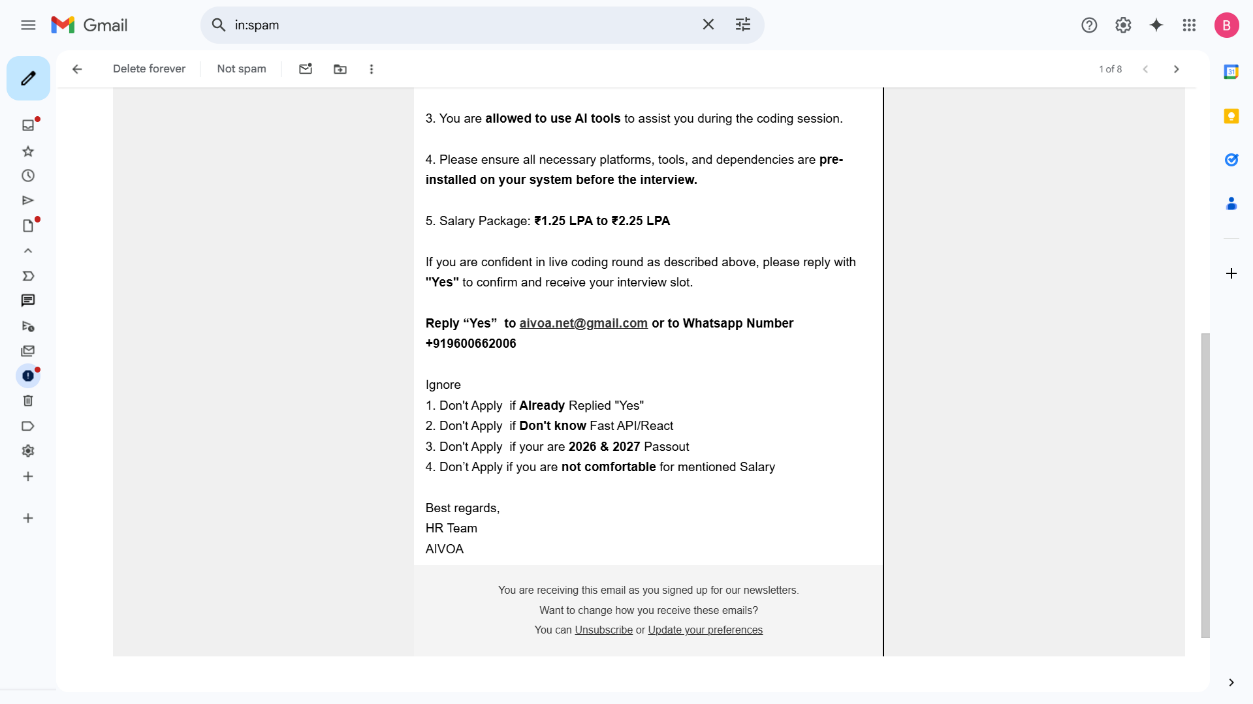
Email Client Used: (Let me know if it was Gmail, Outlook, etc.)

Mailed-By: mail3.zcsn.zcinsend.net

Signed-By: mail3.zcsn.zcinsend.net

Encryption: Standard TLS





**2. Sender Email Spoofing Analysis:**

|  |  |  |
| --- | --- | --- |
| **Aspect** | **Observation** | **Verdict** |
| **Display Name** | "HR AIVOA" — This can be easily faked. | Spoofing Possible |
| **Actual Email** | admin@aivoa.net — Not a well-known or verifiable domain. | Suspicious |
| **Mailing Server** | Sent **via** mail3.zcsn.zcinsend.net — third-party mailing service. | Not Matching |
| **Reply-To Address** | admin@aivoa.net — Same as sender, but not from a trusted domain. | Can Be Spoofed |

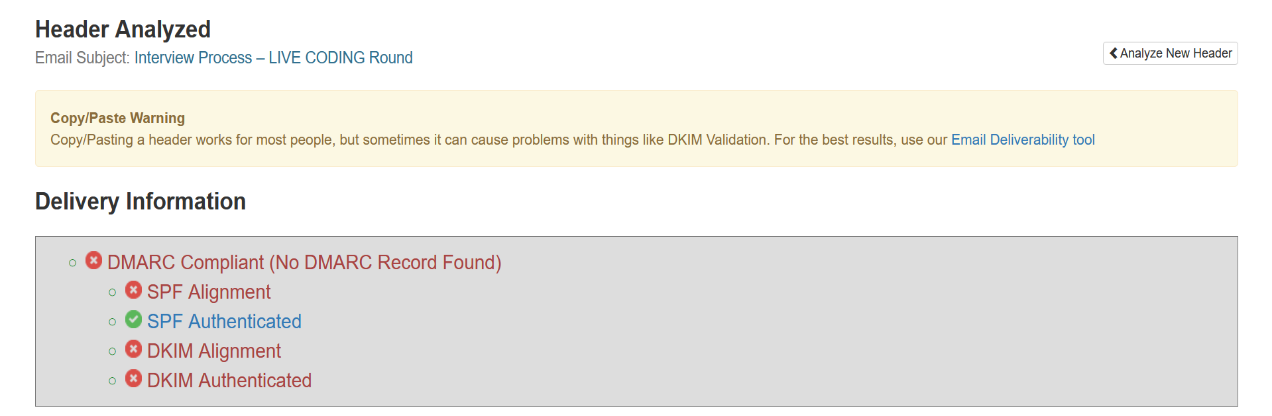
**3. Header Analysis**

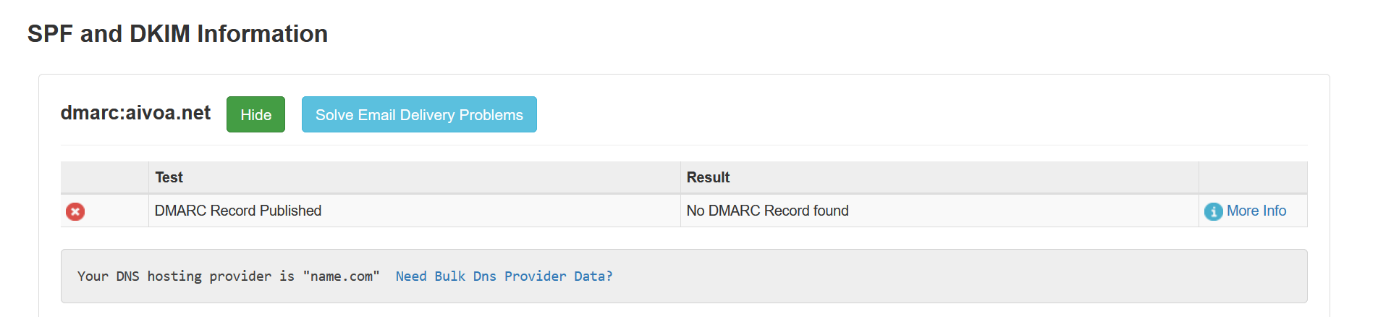
* DMARC: No DMARC record found – indicates poor email domain security; possible spoofing.
* SPF (Sender Policy Framework):
  + SPF Authenticated: Pass – the sender IP is allowed to send on behalf of the domain.
  + SPF Alignment: Failed – suggests that the sending domain doesn't match the "From" domain.
* DKIM (DomainKeys Identified Mail):
  + DKIM Authentication: Failed – the email signature is invalid or missing.
  + DKIM Alignment: Failed – misalignment between sending domain and DKIM domain

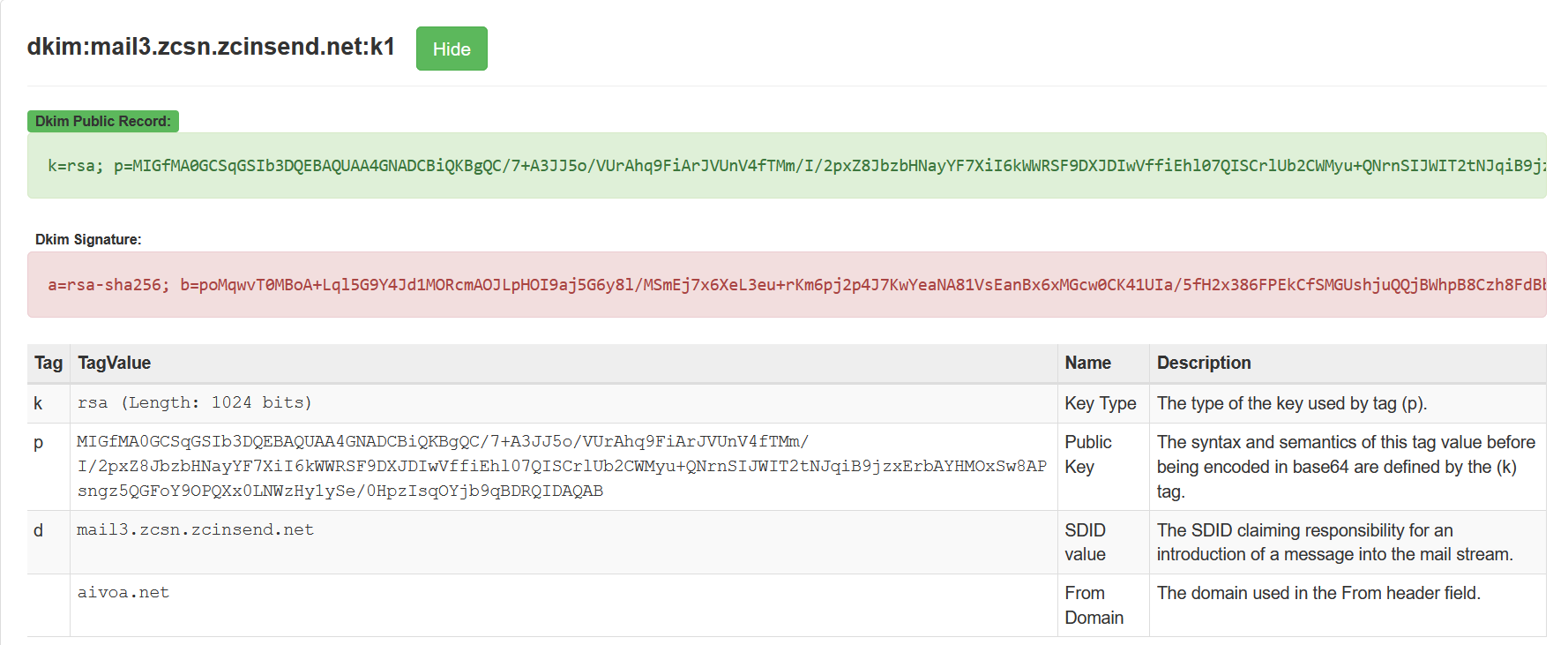
**4.SPF, DKIM, and DMARC Analysis:**

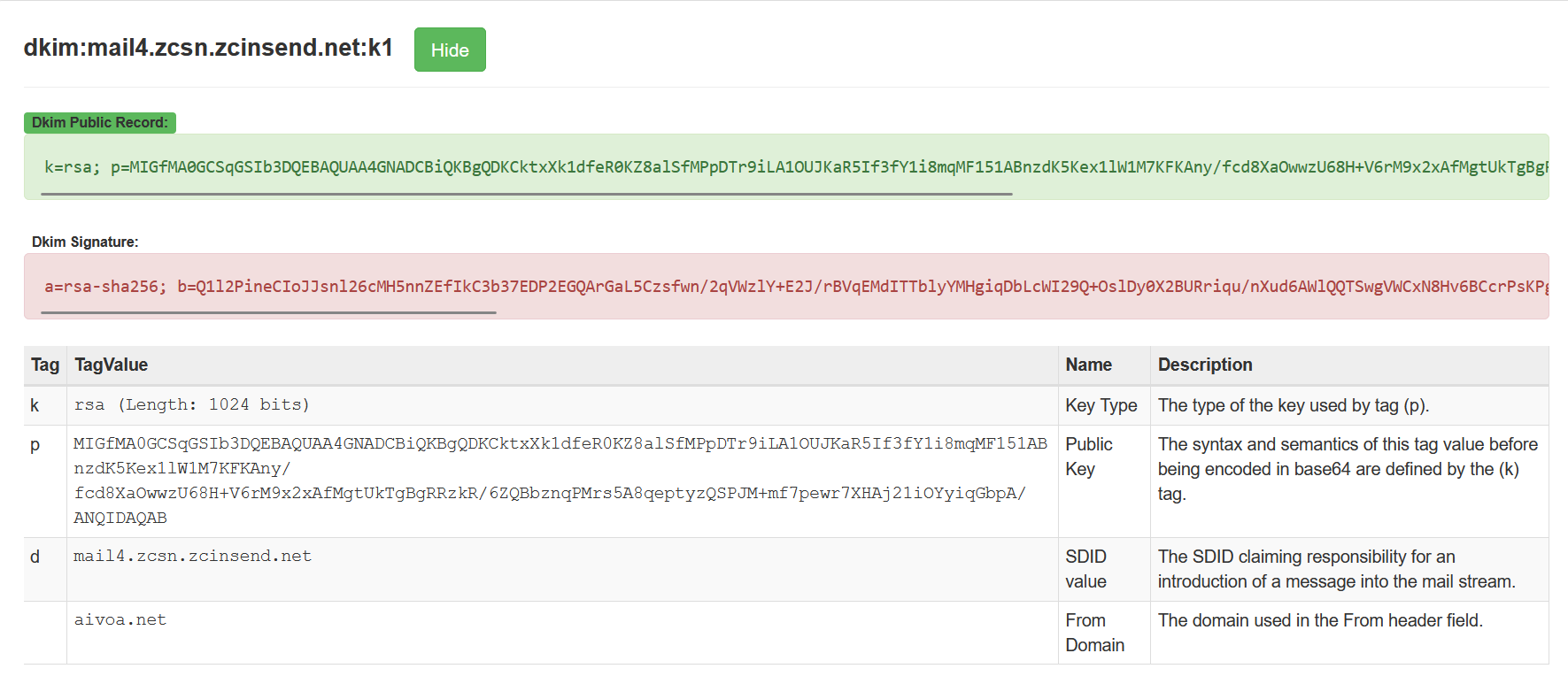
| Authentication Method | Result | Explanation & Risk |
| --- | --- | --- |
| SPF Record | Passed | The sending IP (103.103.198.46) is authorized to send for zcsend.in and zcsend.net. However, SPF alignment failed because the domain in the "From" header (aivoa.net) is not included in the SPF record. This suggests the email might not be legitimately from aivoa.net. |
| DKIM Signature | Failed (signature did not verify, alignment failed) | DKIM signatures exist for mail3.zcsn.zcinsend.net and mail4.zcsn.zcinsend.net, but neither aligns with the "From" domain (aivoa.net). Lack of alignment means DKIM cannot be trusted as proof that aivoa.net authorized this email. |
| DMARC Record | No DMARC record or policy enabled for aivoa.net | Without a DMARC policy to enforce alignment, spoofed emails can easily pass through SPF/DKIM checks, increasing phishing risk. |

**HEADER ANALYZED:**



**SPK AND DKIM INFORMATION:**





**5. Suspicious Links or Attachments:**

Upon analysing the email content, no hyperlinks were found embedded in the message body. This means there were no clickable links redirecting to external websites, which are commonly used in phishing attacks to steal credentials or install malware. Additionally, the email had no file attachments, such as PDFs or ZIP files, which are also typical vectors for delivering malicious payloads. While the absence of links or attachments reduces the technical threat level, it does not eliminate the possibility of a phishing attempt, especially when other indicators like spoofed sender address and failed authentication checks are present.

**5. Conclusion**

This email shows multiple signs of phishing.  
It uses:

* Poor authentication (SPF/DKIM/DMARC issues),
* Unverified sender addresses,
* Informal contact methods,
* Social engineering language,
* And odd job offers details.

( I use ChatGPT for that report creation)