Step 3: Email Header Analysis

Tool Used: Google Header Analyzer (https://toolbox.googleapps.com/apps/messageheader/)

Sample Header Analyzed:

```
-----------------------------------------------
Delivered-To: youremail@example.com
Received: from mail.paypa1.com (fake IP: 192.168.1.55)
    by mx.google.com with ESMTPS id abc123xyz
    for <youremail@example.com>;
    Wed, 01 Aug 2025 12:34:56 -0700 (PDT)
From: "PayPal Security" <support@paypa1.com>
Reply-To: support@paypa1.com
Return-Path: scammer@malicious.com
Authentication-Results: spf=fail (google.com: domain of paypa1.com does not designate
192.168.1.55 as permitted sender)
-----------------------------------------------
```

Findings:

- From address: support@paypa1.com (Fake domain pretending to be PayPal)
- Return-Path: scammer@malicious.com (does not match the sender — spoofed)
- SPF: Failed — sender not authorized to send from this domain
- DKIM: Missing — indicates lack of authenticity
- Source IP: 192.168.1.55 — private IP, not valid for public email traffic

Conclusion:

The email fails key authentication checks (SPF, DKIM) and contains a spoofed Return-Path.

This indicates that the email is likely a phishing attempt created using a fake domain and spoofed sender.