Certainly! Here's the **process to analyze a phishing email**, without using a specific example:

**Phishing Email Analysis Process**

**1. Collect the Email**

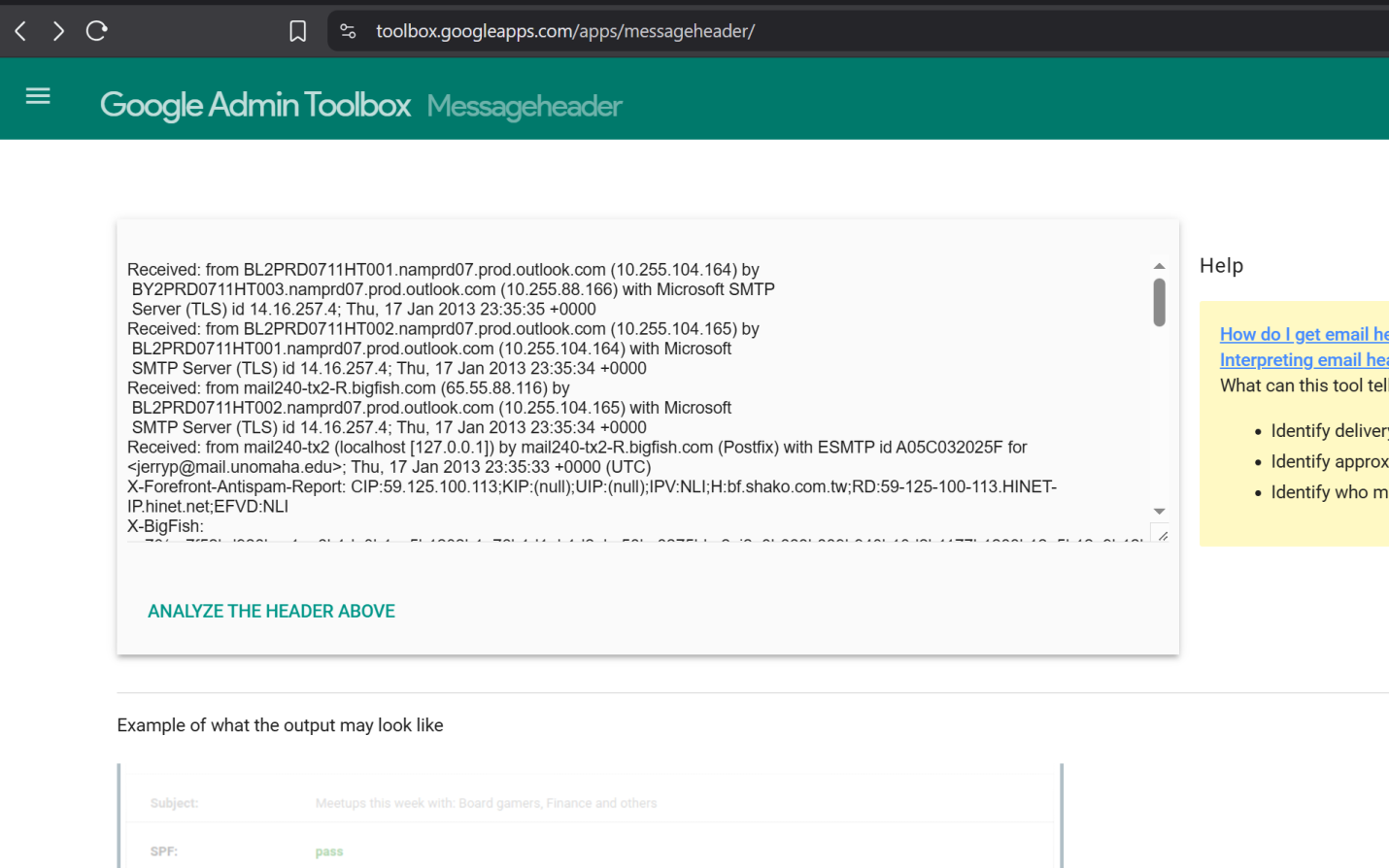
* Obtain the suspicious email either from your inbox, a spam folder, or from a phishing dataset.
* Using this mail header for analysis - https://mlhale.github.io/nebraska-gencyber-modules/phishing/email-headers/email-header1.txt

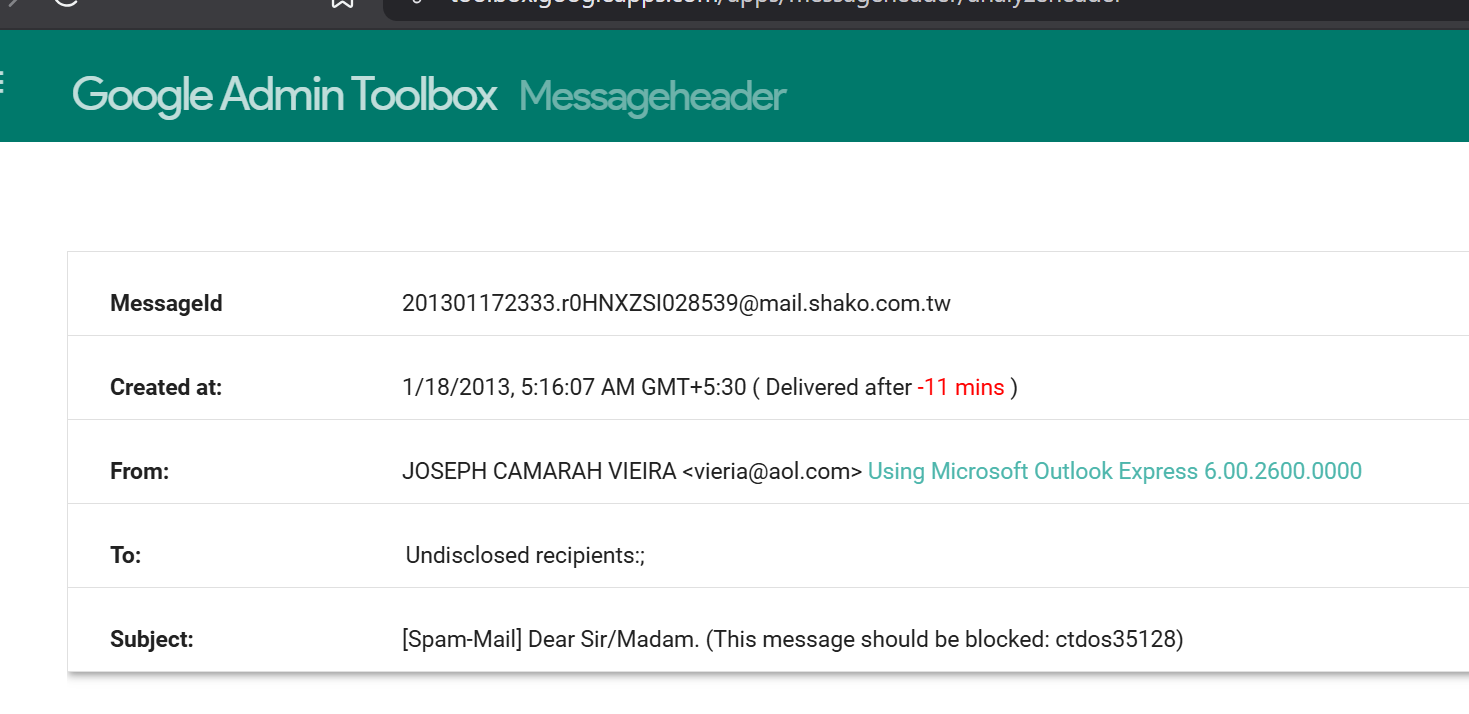
**2. Check the Sender’s Email Address**

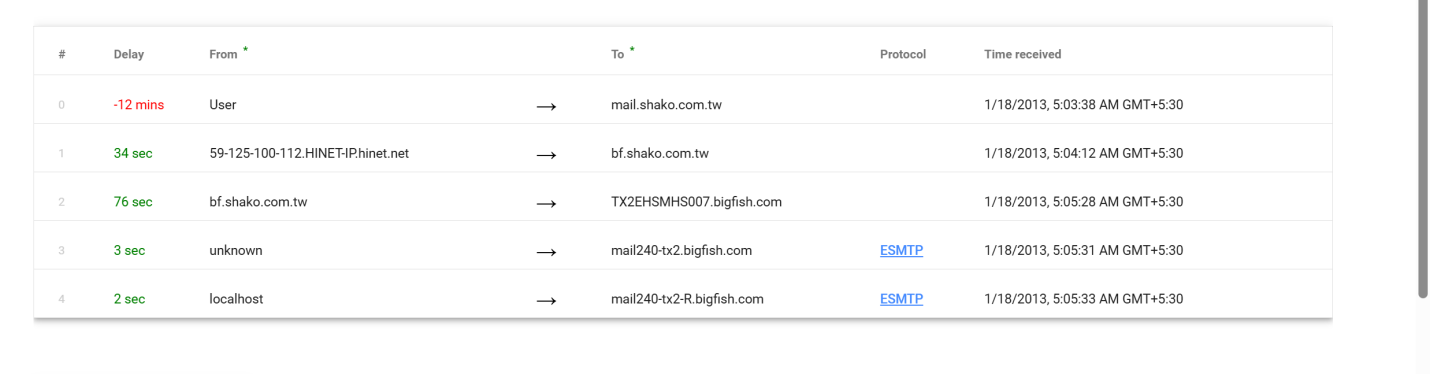
* Inspect the **"From" field** to see if the sender's email address matches the claimed organization.
* Look for **misspelled domains** or addresses that appear suspicious or generic.

**3. Analyze Email Headers**

* Open full email headers (most email clients allow this).
* Use a **free online email header analyzer** (e.g., MXToolbox or Google’s tool).
* Look for:
  + **SPF**, **DKIM**, **DMARC** validation results.
  + **IP origin** — Check if it matches the sender’s legitimate location.
  + **Return-path** or **Reply-To** addresses that differ from the sender’s.







**4. Inspect Hyperlinks**

* Hover over any links in the email (do not click).
* Compare the **displayed URL** with the **actual destination**.
* Look for **typos**, **non-official domains**, or use of **URL shorteners**.

**5. Check for Attachments**

* Review any attached files.
* Phishing emails may contain:
  + PDF forms
  + Word documents with macros
  + Executable files
* Do **not open** attachments unless in a secure analysis environment.

**6. Look for Urgency or Threatening Language**

* Identify phrases that create pressure:
  + Urgent payment needed
  + Account will be suspended
  + Legal or security warnings
* These are social engineering tactics to provoke fast action.

**7. Check for Personalization and Grammar**

* Look for:
  + Generic greetings ("Dear customer")
  + Spelling or grammatical mistakes
  + Awkward tone or formatting
* Legitimate companies usually use proper branding and personalization.

**8. Summarize Findings**

* Make a list of phishing indicators found:
  + Sender spoofing?
  + Authentication failures?
  + Fake links or domains?
  + Urgent tone?
  + Attachments?
  + Grammar issues?
* Assess the **overall risk** and **recommend action** (report, block, delete).