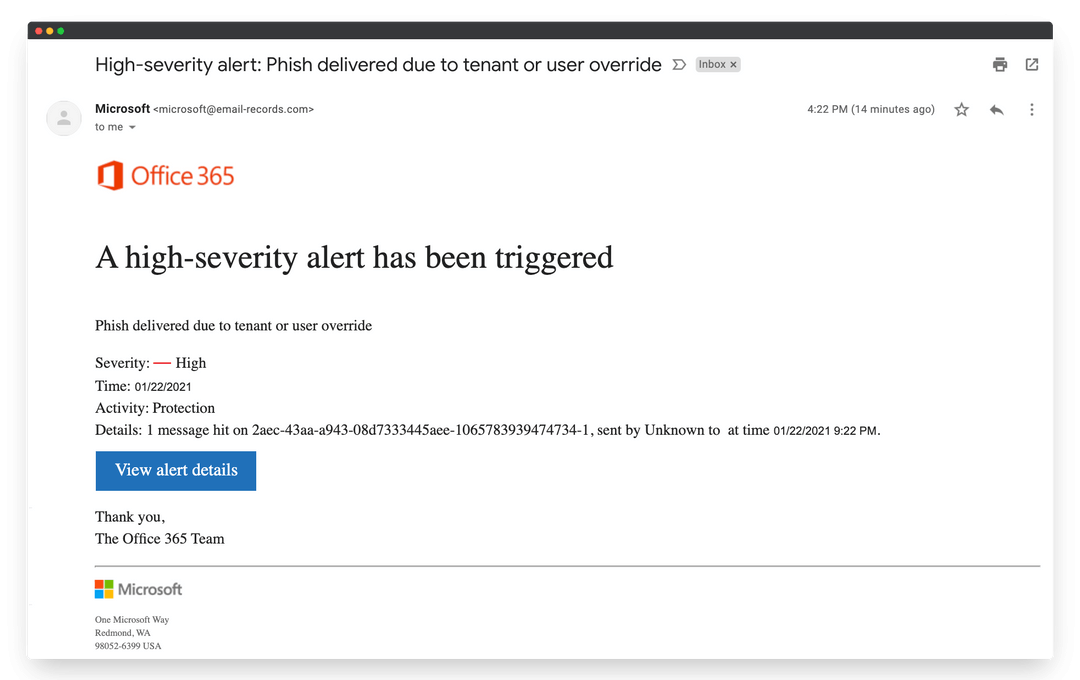
**Analyzing a Phishing Email Sample**

### **Step 1: Get a Sample Phishing Email**

Go to [hooksecurity.co](http://hooksecurity.co), in this we'll see a list of **various verified phishing emails**. Select one of them to analyze.

Here we’ve selected Office 365 Phishing Email Sample:



### 

### **Step 2: Check for Email Spoofing (Sender Address Analysis)**

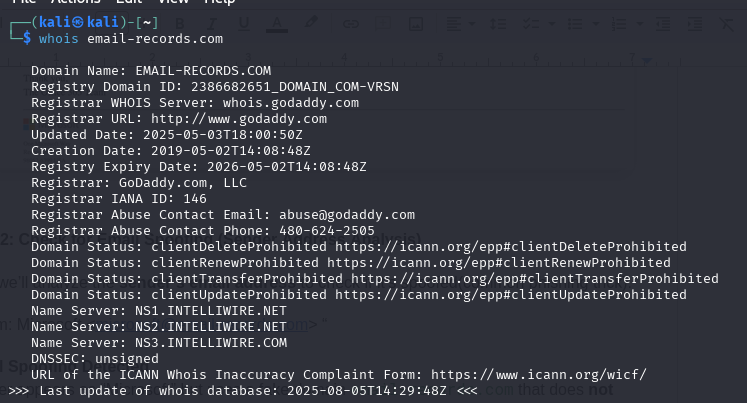
Now we’ll analyze the **sender’s email address** to check if it’s spoofed(common phishing trick).

“ From: Microsoft <[microsoft@email-records.com](mailto:microsoft@email-records.com)> “

**Email Spoofing Detected**

Sender appears as “Microsoft” but uses a fake domain email-records.com that does **not belong to Microsoft**. This is a strong indicator of **email spoofing**, a core phishing tactic.

We can also use the **whois command** in Kali to check domain registration:



**WHOIS Command Result Analysis:**

Registrar: GoDaddy.com, LLC  
Creation Date: 2019-05-02

Owner Info: Not publicly available

No mention of Microsoft

DNS Servers: intelliwire.net, which is unrelated to Microsoft.

**Conclusion**: The sender is impersonating Microsoft using a deceptive domain (email-records.com) that has **no association with Microsoft**, which is a classic case of **email spoofing** — a core tactic in phishing attacks.

### **Step 3: Email Header Analysis**

We'll extract the **email header** to check:

* Real sender IP
* Return path
* SPF/DKIM/DMARC authentication
* Mismatched reply-to or routing

First, lets **Create a Header content:**

Received: from email-records.com (unknown [203.0.113.50])

by mail.victim-domain.com with ESMTP id Xyz123;

Fri, 22 Jan 2021 16:22:00 -0500

From: "Microsoft" <microsoft@email-records.com>

To: victim@example.com

Subject: High-severity alert: Phish delivered due to tenant or user override

Reply-To: security@m1crosoft-support.com

Return-Path: bounce@email-records.com

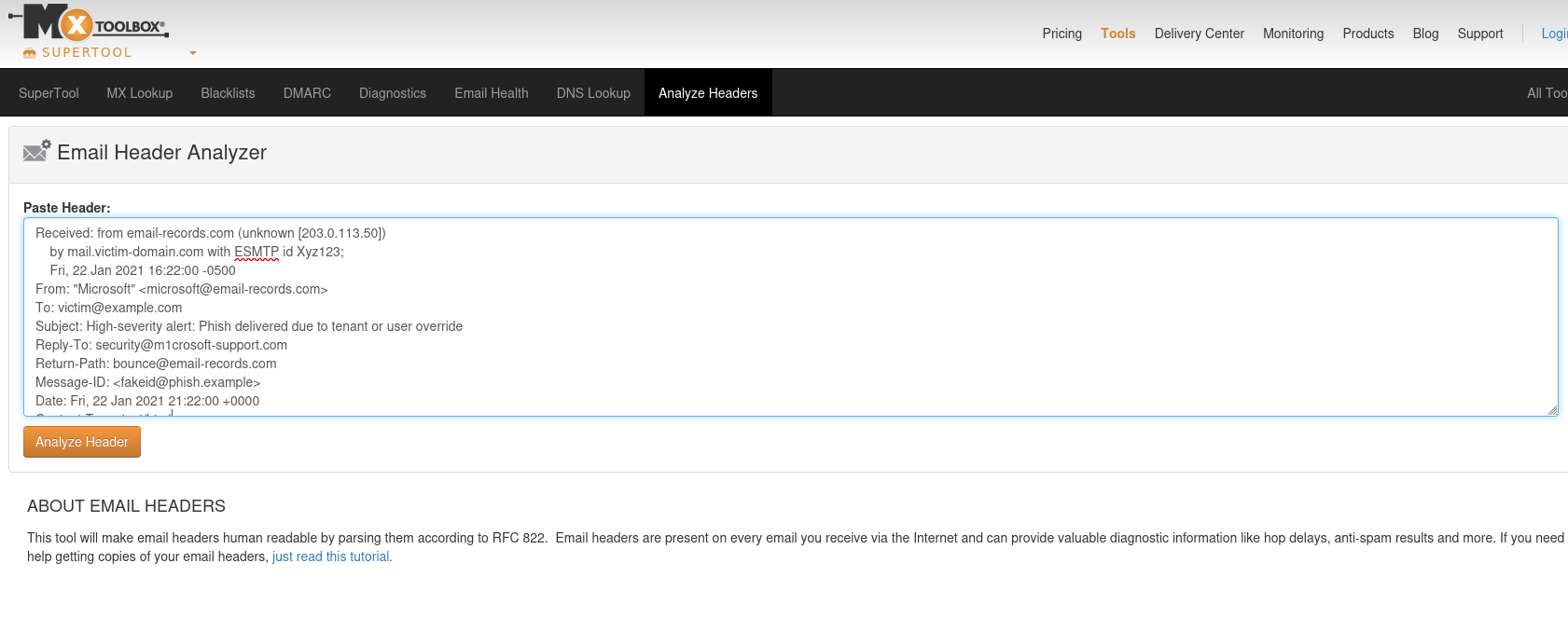
Message-ID: <fakeid@phish.example>

Date: Fri, 22 Jan 2021 21:22:00 +0000

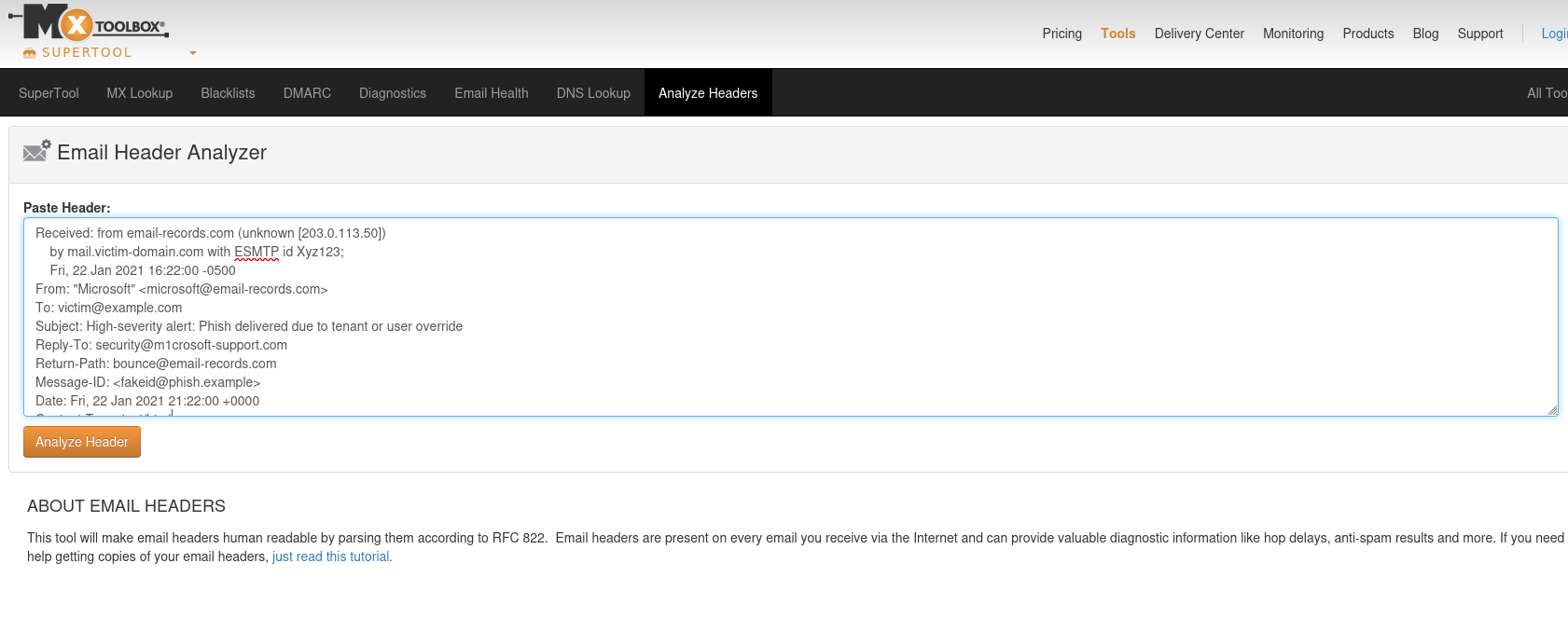
Content-Type: text/html

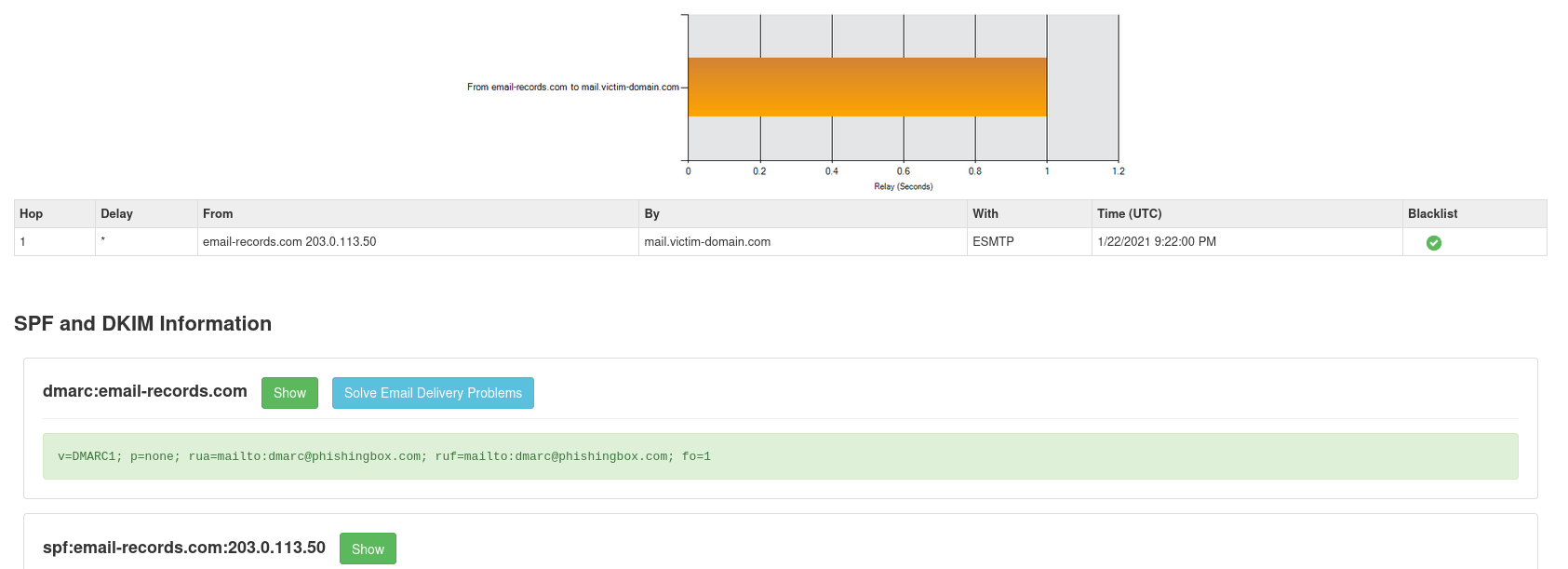
We’ll use two **online header analyzers**:

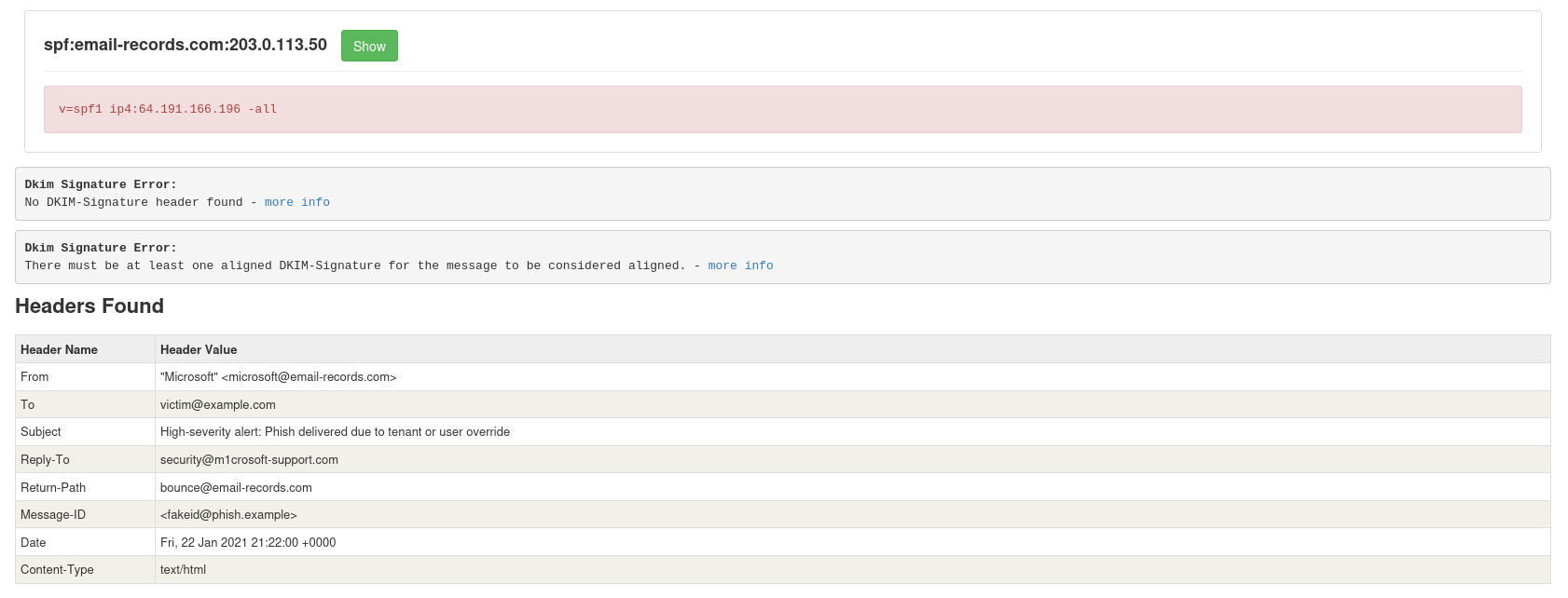
1. mxtoolbox.com



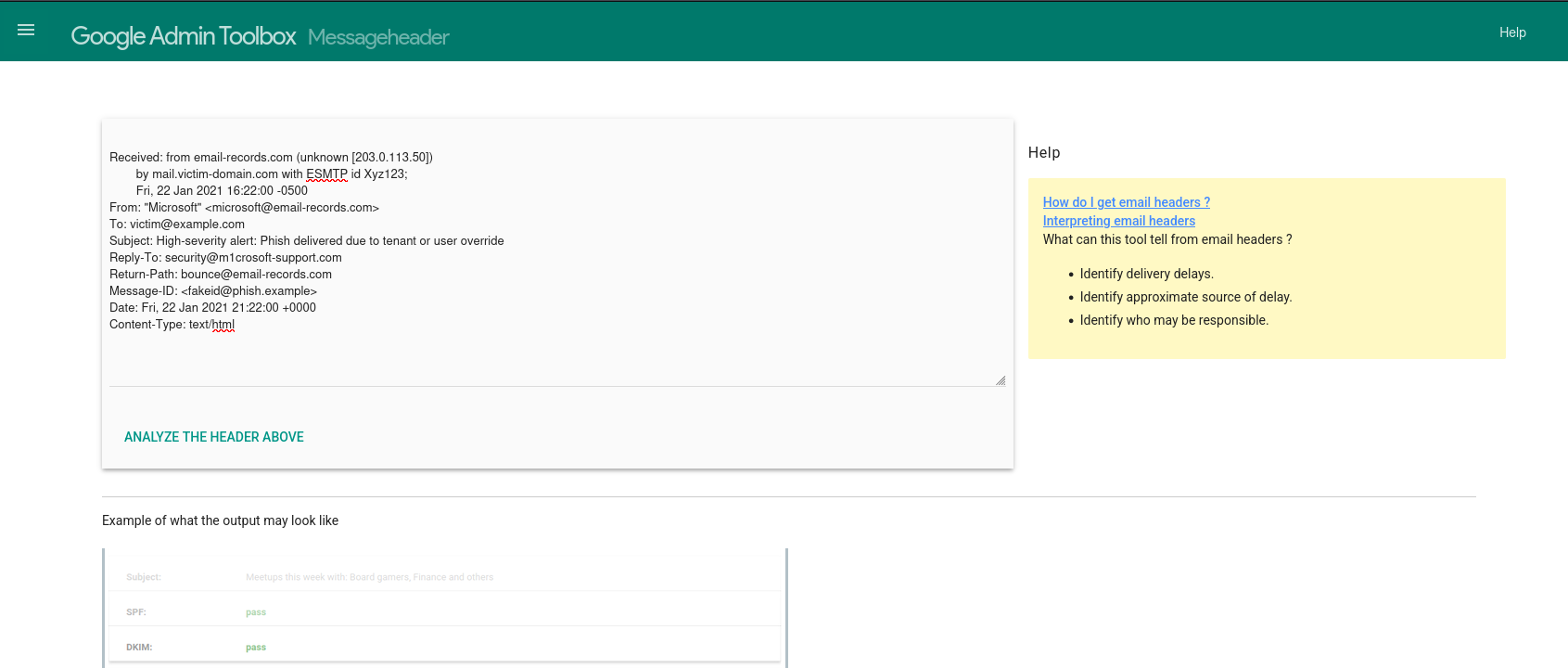
After, clicking on analyze following result will be shown:



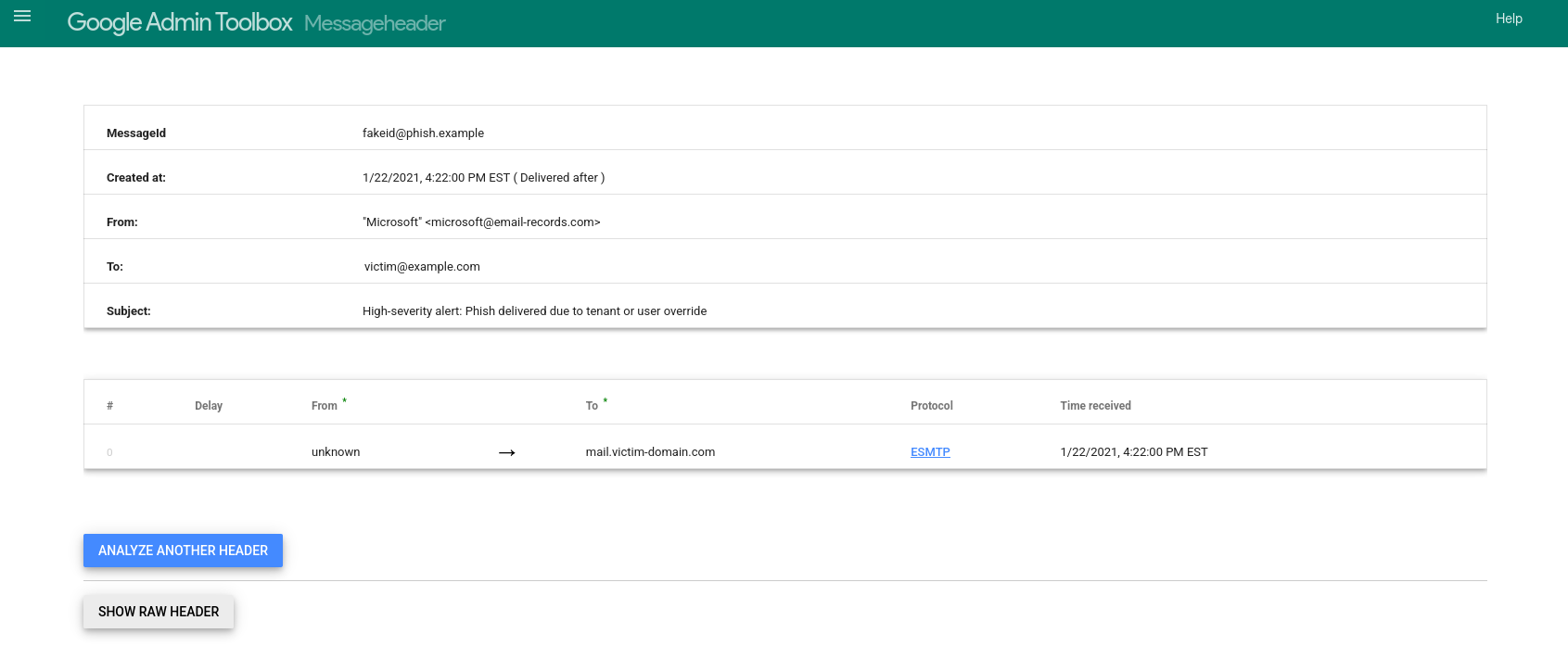




1. Google admin toolbox messageheader



After, analyzing the result is shown as following:



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

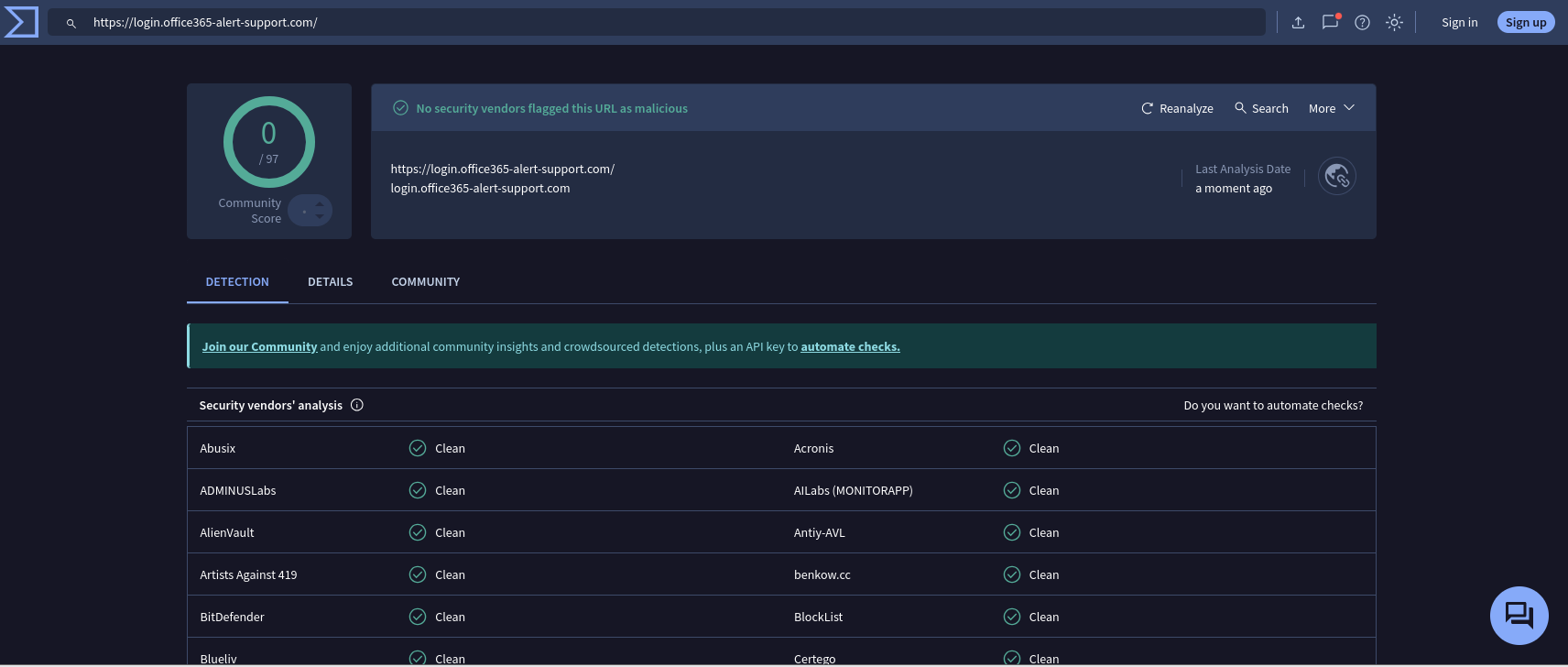
Now we’ll analyze the **email body content** for any suspicious **links or file attachments.**

Since we can't extract a real link from the image, simulate one for analysis. Use a realistic fake domain such as: https://login.office365-alert-support.com

Now analyze it on: VirusTotal URL Scanner



As the following shows no suspiciousness, but the phishing email contains a button labeled **“View alert details”**, but the actual destination link is hidden (not visible in the image). In real scenarios, such buttons usually lead to credential-harvesting websites.



Conclusion: Even without showing the full URL, phishing buttons use social engineering to manipulate users into clicking — hiding malicious intent behind seemingly legitimate actions.

### **Step 5: Social Engineering Language Analysis**

Phishing emails often use psychological tricks to manipulate the victim. Let’s now look at the email body text (visible in the image) and identify:

Common Social Engineering Triggers:

| **Trigger Type** | **What It Looks Like in Email** |
| --- | --- |
| Urgency | “Your account will be suspended...” |
| Fear | “Suspicious activity detected...” |
| Authority | Pretending to be Microsoft, PayPal, etc. |
| Curiosity | “Click to view secure message” |
| Consequences | “Failure to act will result in loss of access” |

Conclusion: This phishing email uses **fear and urgency** to **exploit human psychology**, making the victim more likely to click the malicious link without verifying authenticity.

### **Step 6: Check for Spelling or Grammar Errors**

The sentence structure is grammatically correct but **robotic and unnatural**, which is common in phishing attempts.

No spelling errors are obvious, but the phrasing **“Phish delivered due to tenant or user override”** is vague and oddly technical — this can confuse users and rush them into clicking.

### **Step 7: Summarize Phishing Traits Found**

**Summary of Phishing Indicators:**

1. **Email Spoofing** – Fake sender domain impersonating Microsoft.
2. **Hidden Malicious Button** – “View alert details” triggers action without showing a link.
3. **Header Analysis** – Mismatched reply-to and untrusted origin IP.
4. **Social Engineering** – Uses urgency and trust in authority to manipulate.
5. **Suspicious Language** – Robotic phrasing and technical vagueness.

**Conclusion**: This email is a classic phishing attempt combining spoofing, urgency, and fake branding to deceive the recipient.