**TASK 2:**

**Objective:** Identify phishing characteristics in a suspicious email sample.

**Tools:** Email client or saved email file (text), free online header analyzer.

**Deliverables**: A report listing phishing indicators found

**HOW I DID THE TASK:**

**STEP 1:**

First I downloaded a sample phising email from a github repo.

**STEP 2:**

Now i researched in internet on what is phising email and how to do header spoofing.

**STEP 3:**

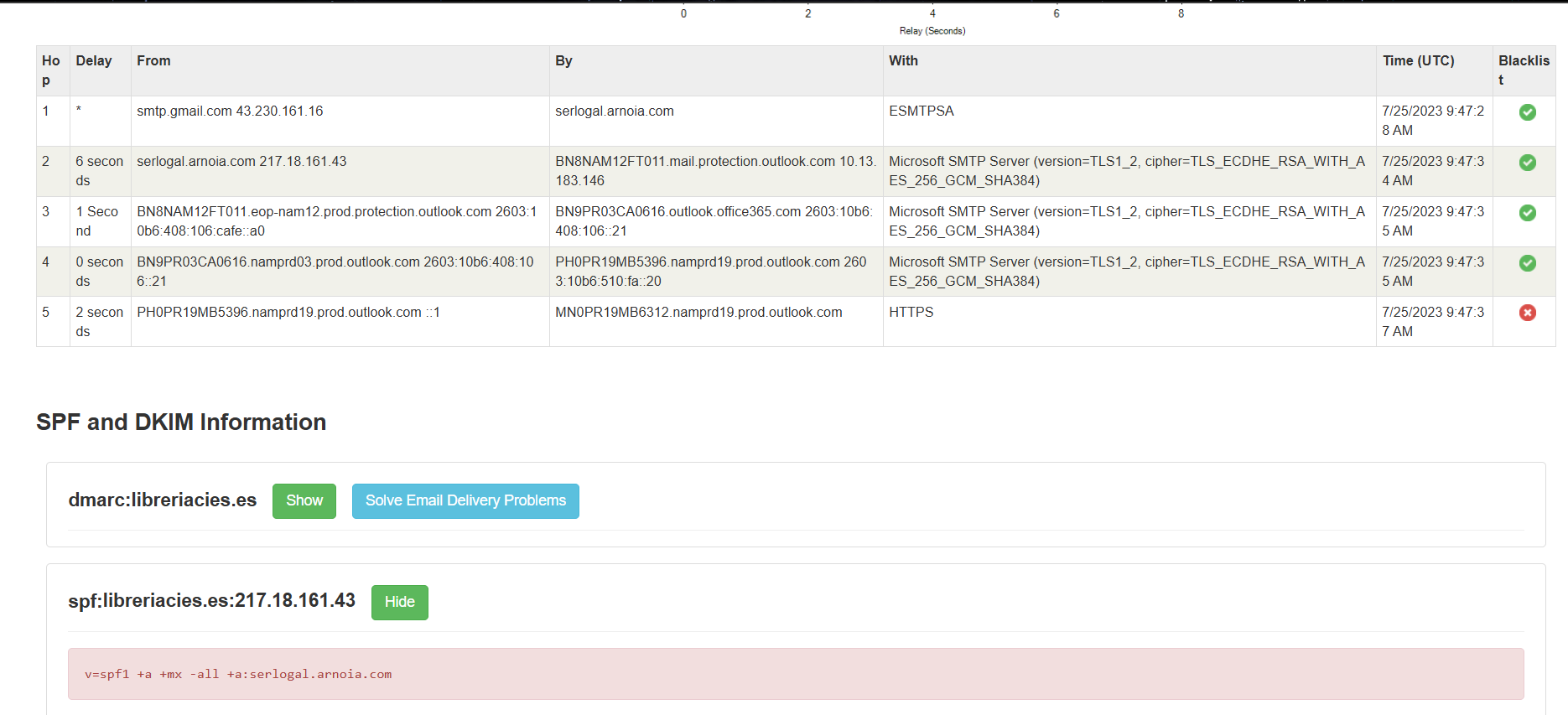
I used <https://mxtoolbox.com> website for spoofing.

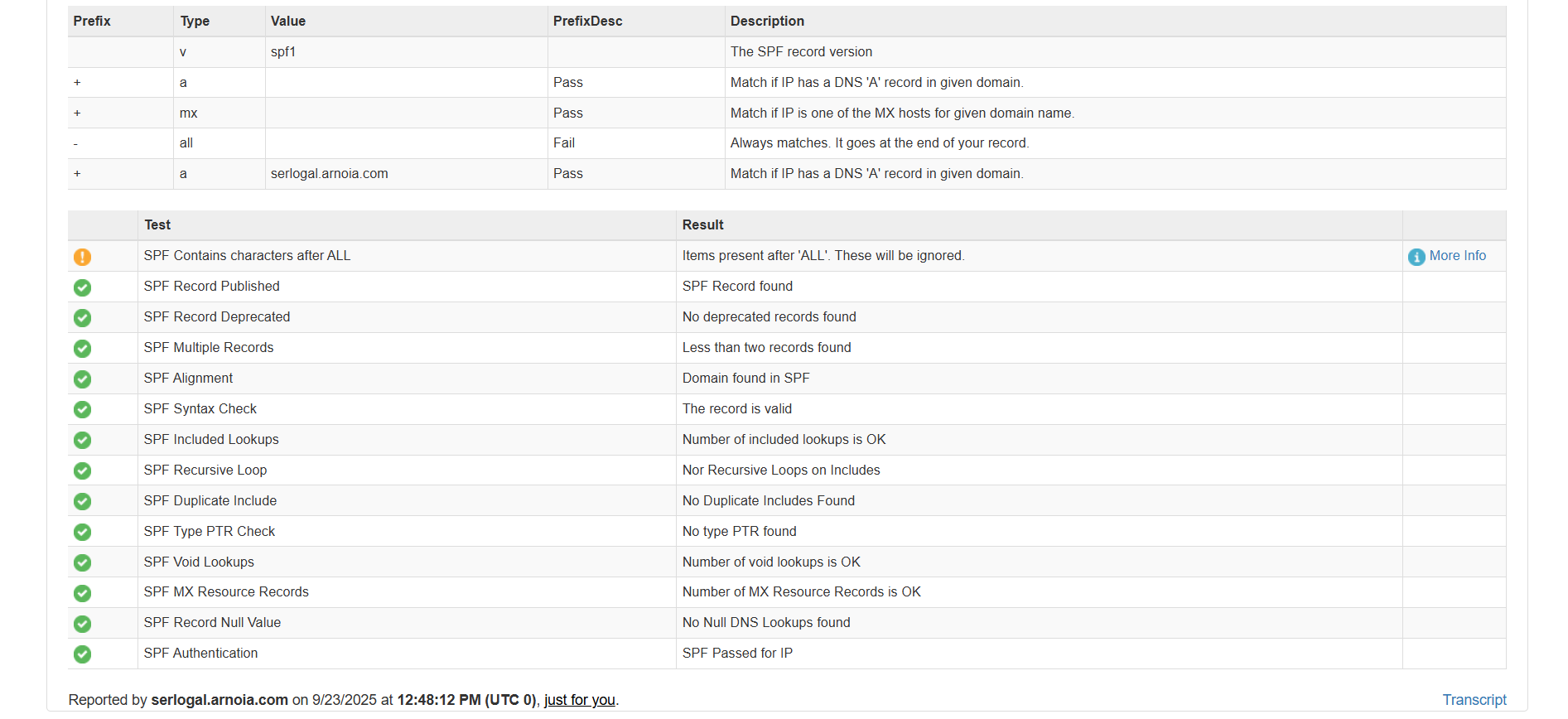
**STEP 4:**

I copied the header of the phising email and pasted in this website to get my result.

**RESULT: (IN SCREENSHOT)**

****

****

****

****

**What is SPF and DKIM Information?**

Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) are email authentication standards that help prevent email spoofing and phishing. Both work by adding a layer of verification to emails, but they do it in different ways.

**INFO**: I HAVE ATTACHED THE SAMPLE PHISHING EMAIL FILE IN THE GITHUB REPO FOLDER.