CYBERSECURITY ASSIGNMENT

**Report on Email Spoofing Detection**

Name:Polkampalli Pragna

Roll No:160123737080

Class: IT-2

Project Title: Email Spoofing Detection (Tool Explored: MxToolbox)

Date: 01/09/2025

# Project Overview

The objective of this project was to explore techniques for detecting and flagging spoofed emails — messages where the sender information is forged to appear as if it originated from a trusted source. Email spoofing is widely used in phishing and Business Email Compromise (BEC) scams, often leading to credential theft, malware infections, or financial fraud. This project simulates how real-world organizations detect spoofed emails by analyzing email headers and enforcing authentication protocols (SPF, DKIM, DMARC).

# Technologies & Tools Used

- Programming Language: Not required (used pre-existing tool)  
- Tool Explored: MxToolbox (free online email header analyzer)  
- Protocols: SPF, DKIM, DMARC  
- Version Control: Git & GitHub (for documentation if required)

# System Architecture

1. Email Received → Spoofed email with forged 'From' address.  
2. Header Extraction → Collect metadata (From, Reply-To, Return-Path, Received).  
3. Authentication Check → Verify SPF, DKIM, DMARC results.  
4. Analysis Tool → Run header through MxToolbox Analyzer.  
5. Flagging → If authentication fails or headers mismatch, mark as spoofed.

# Security Features

- SPF Validation: Ensures sender’s IP is authorized.  
- DKIM Verification: Confirms the email hasn’t been tampered with.  
- DMARC Alignment: Checks if the sender domain matches SPF/DKIM.  
- Header Analysis: Detects mismatched From vs Return-Path.  
- Visual Reports: MxToolbox highlights pass/fail checks clearly.

# Folder Structure

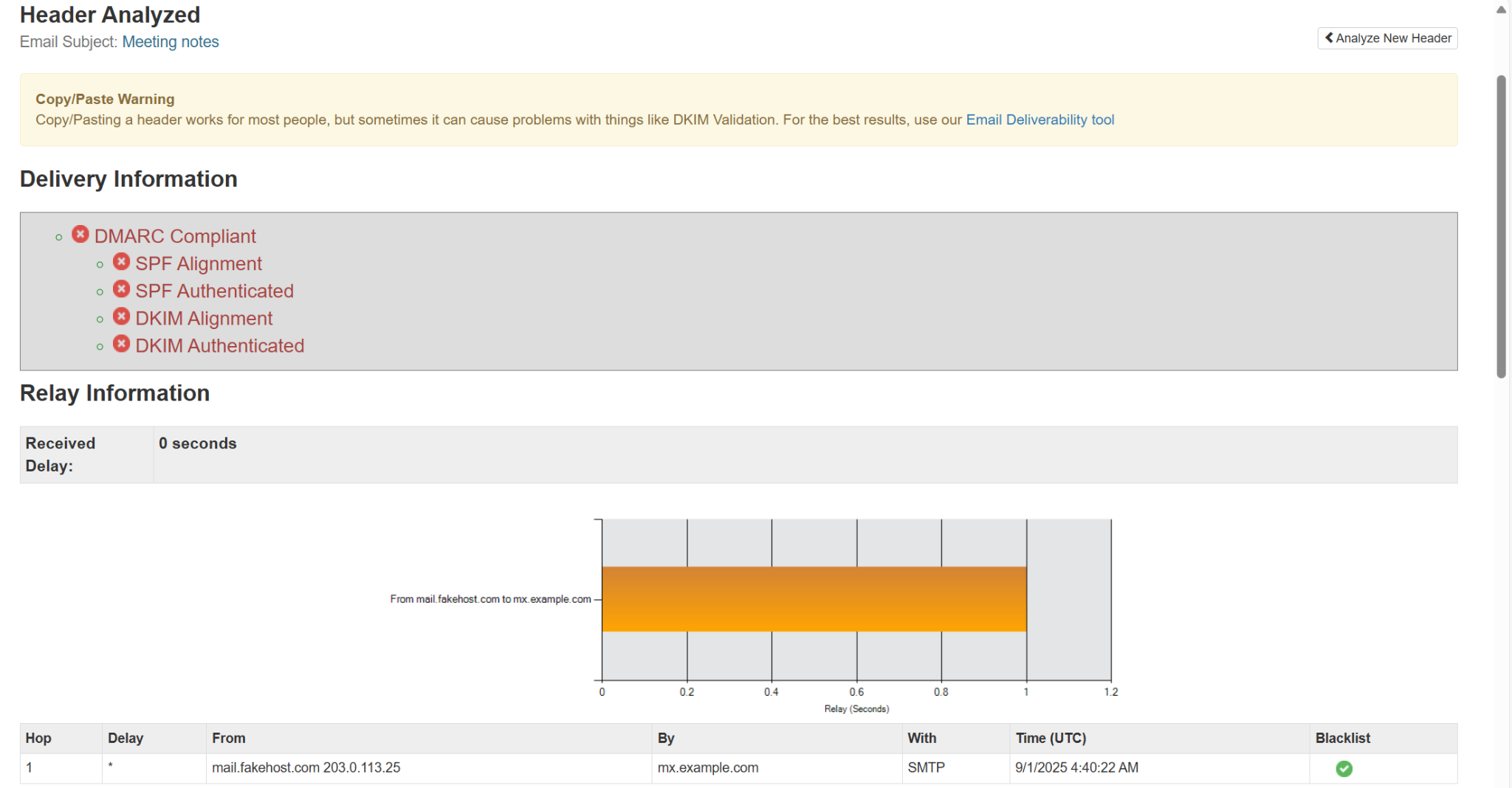
EmailSpoofingDetection/  
├── docs/  
│ └── report.docx # Project documentation  
├── samples/  
│ ├── spoofed\_email\_header.txt # Example spoofed header  
│ └── genuine\_email\_header.txt # Example genuine header  
└── screenshots/  
 └── spoof\_vs\_genuine.png # Result of spoofed vs genuine detection

# Screenshots

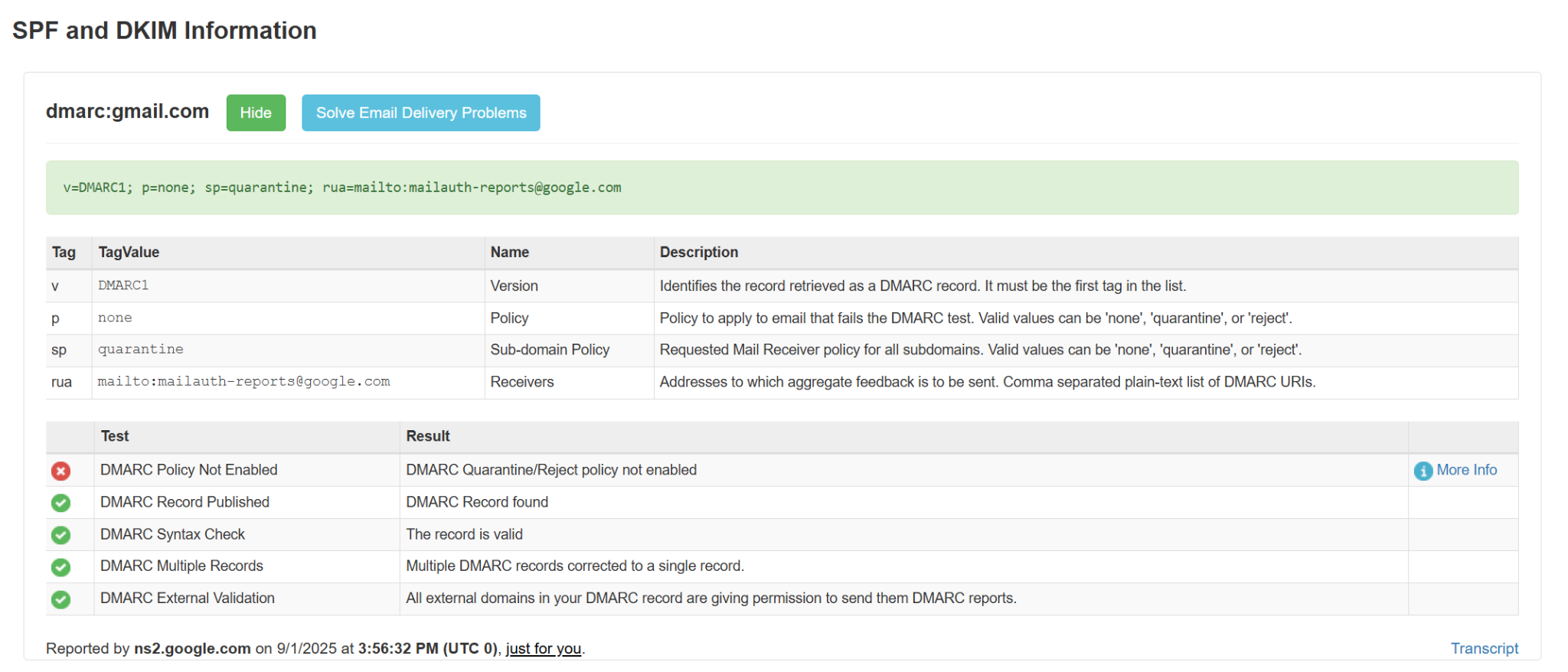
1. Tool explored: MxToolbox - Spoofed Header Analysis



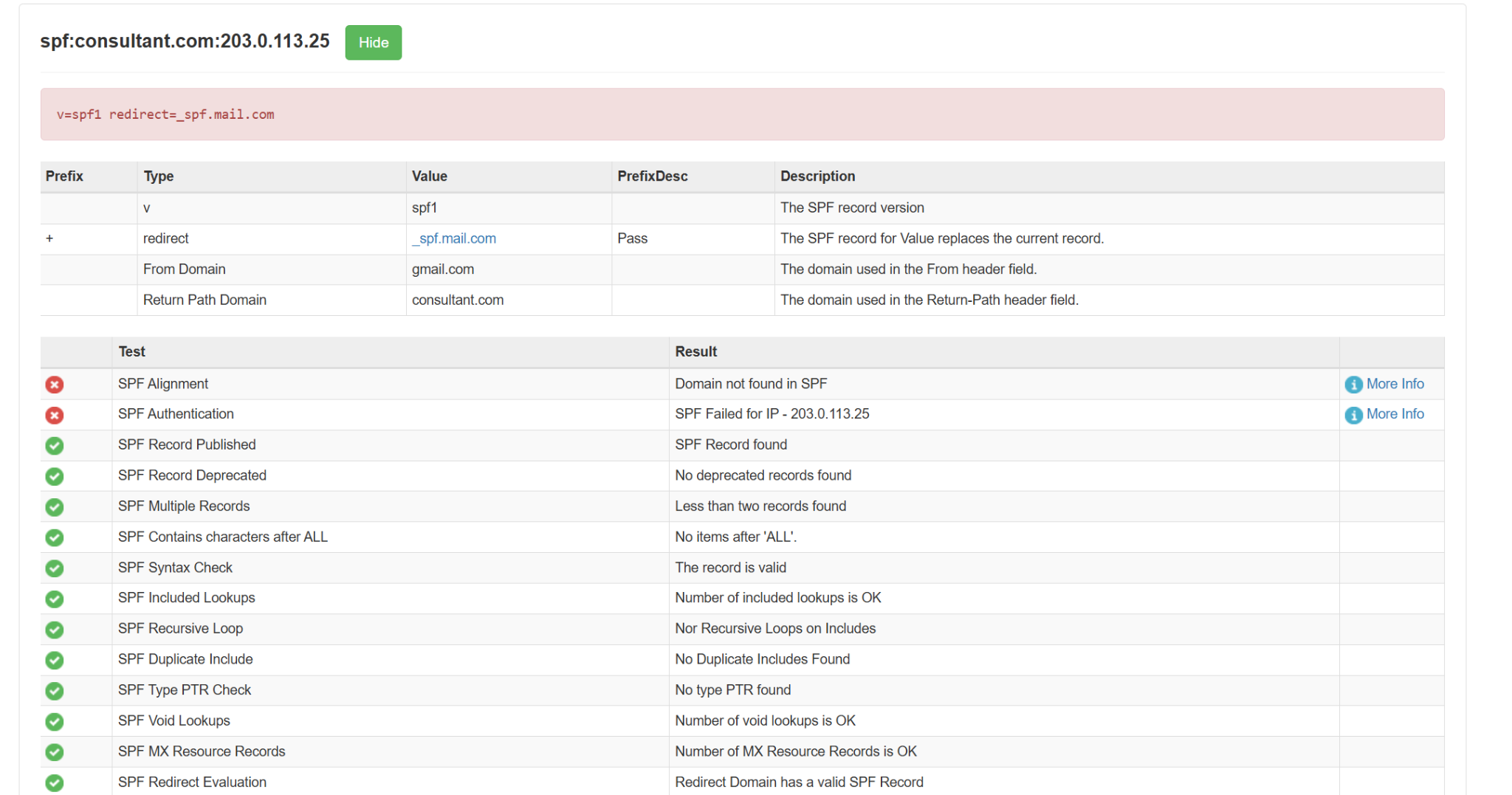
2. SPF & DKIM Test Results - Spoofed Email



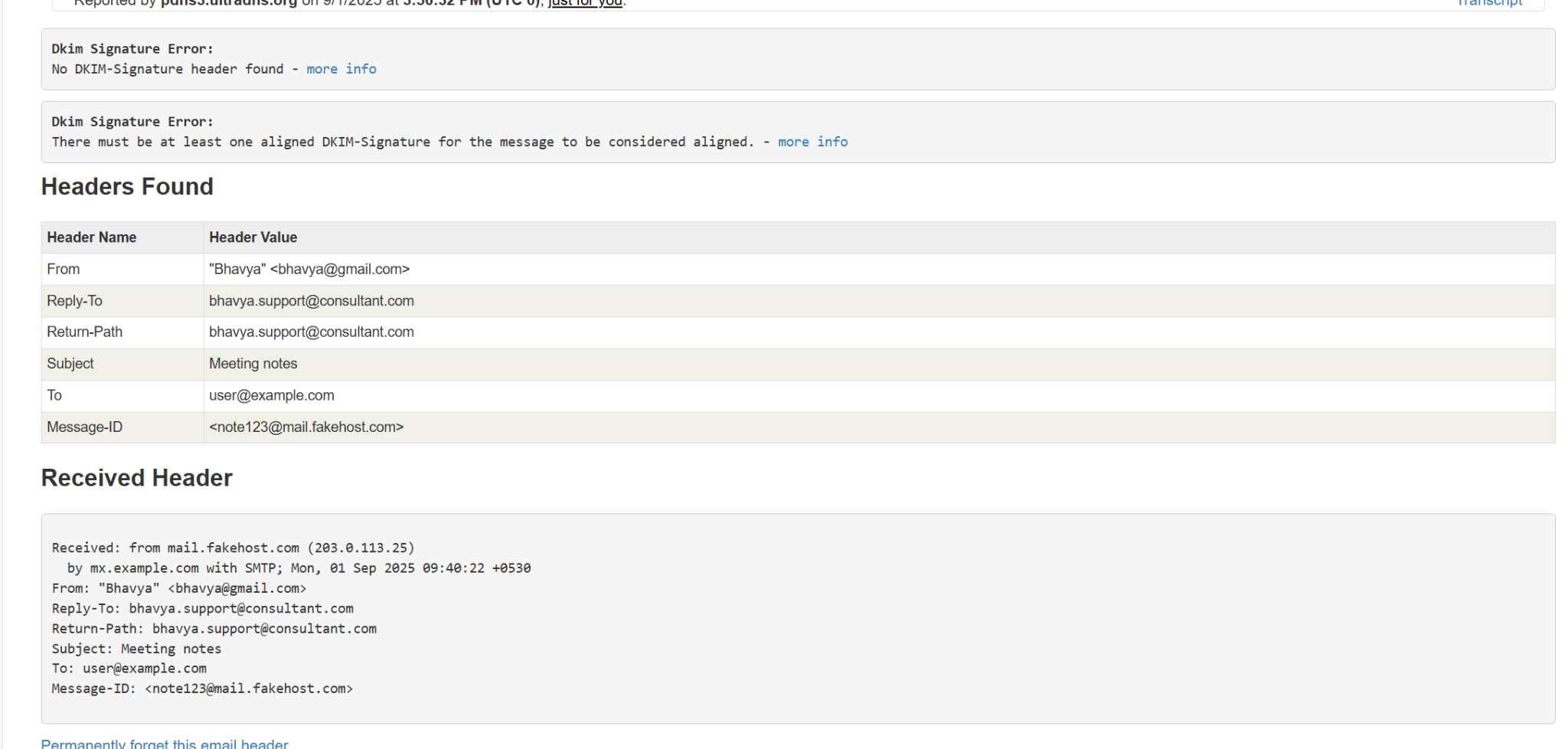
3. Genuine Gmail Email Header Analysis



4. Authentication Failures (Spoofed Email)



5. DMARC Information - Gmail (Legitimate Email)



# Deliverables

- Word report with full documentation.  
- Screenshots demonstrating spoofed and genuine email analysis.  
- Sample email headers used for testing.

# Learning Outcomes

- Practical understanding of email spoofing techniques.  
- Hands-on experience with MxToolbox email header analyzer.  
- Knowledge of email authentication protocols (SPF, DKIM, DMARC).  
- Awareness of phishing and BEC prevention strategies.

# Conclusion

This project demonstrates the importance of detecting spoofed emails in cybersecurity. By using free tools like MxToolbox and enforcing authentication protocols (SPF, DKIM, DMARC), organizations can effectively reduce the risk of phishing and identity deception. The project highlights the relevance of email header analysis and security awareness in protecting users against cyber threats.