Ex. No 4: Analyze email headers and detect email spoofing using MHA (Mail Header Analyzer)

AIM:

To analyze email headers using the Mail Header Analyzer (MHA) tool and identify signs of email spoofing or phishing attempts.

DESCRIPTION / THEORY:

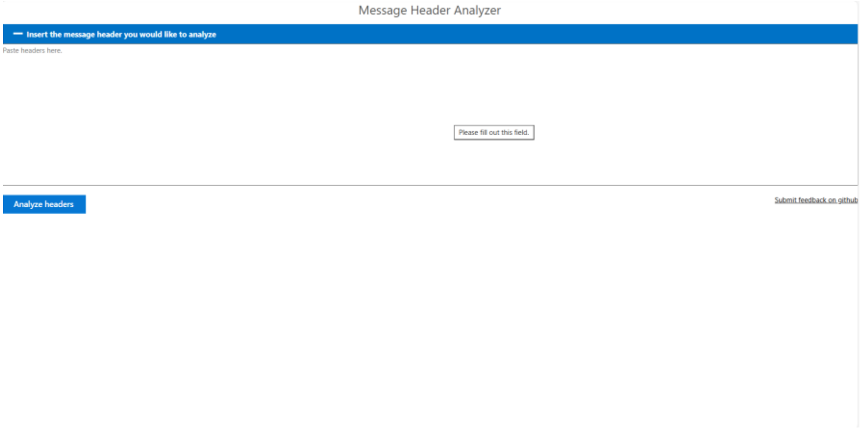
Email spoofing is a technique used by attackers to forge the sender's email address, making it appear as if the message came from a trusted source. Spoofed emails are commonly used in **phishing attacks**, **social engineering**, and **spam campaigns**.

An **email header** contains metadata about the message such as:

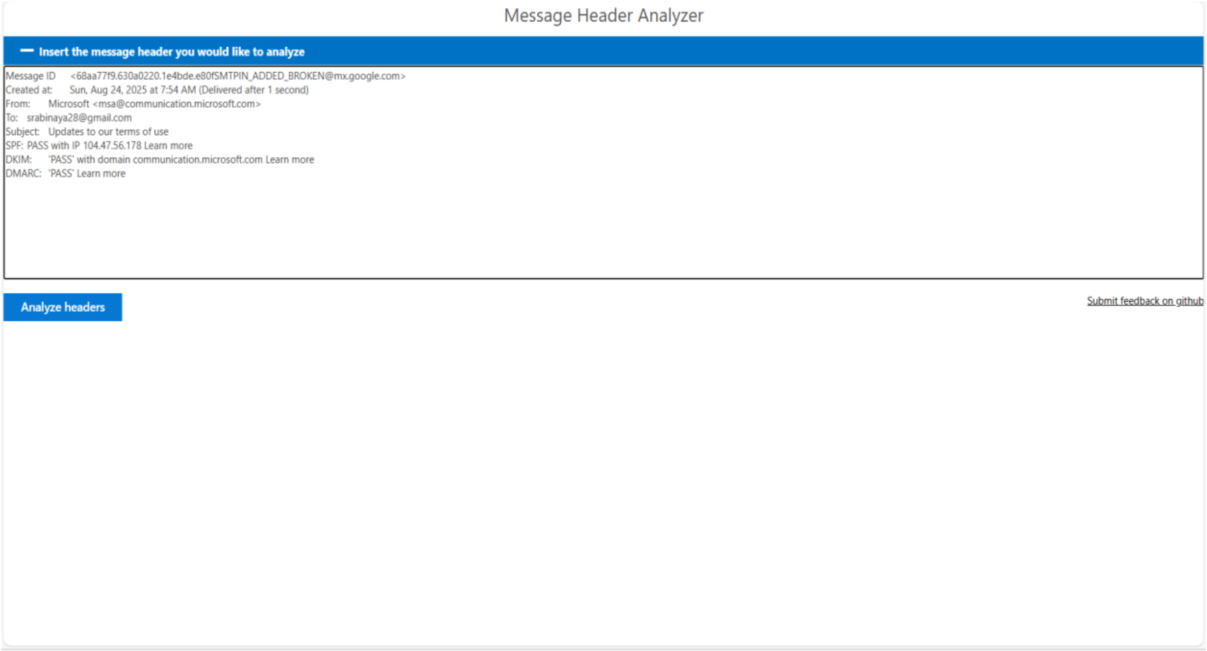
- Sender and receiver information
- Message-ID
- Mail server path (Received fields)
- SPF, DKIM, and DMARC authentication results
- Timestamps and originating IP addresses

The **Mail Header Analyzer (MHA)** tool is used to decode and visualize these header fields. It helps investigators trace the **real source** of the email, detect **forged addresses**, and verify **mail server authenticity**.

PROCEDURE:


Message Header Analyzer
Insert the message header you would like to analyze
Paste headers here.
Analyze headers
Submit feedback on github

Please fill out this field.



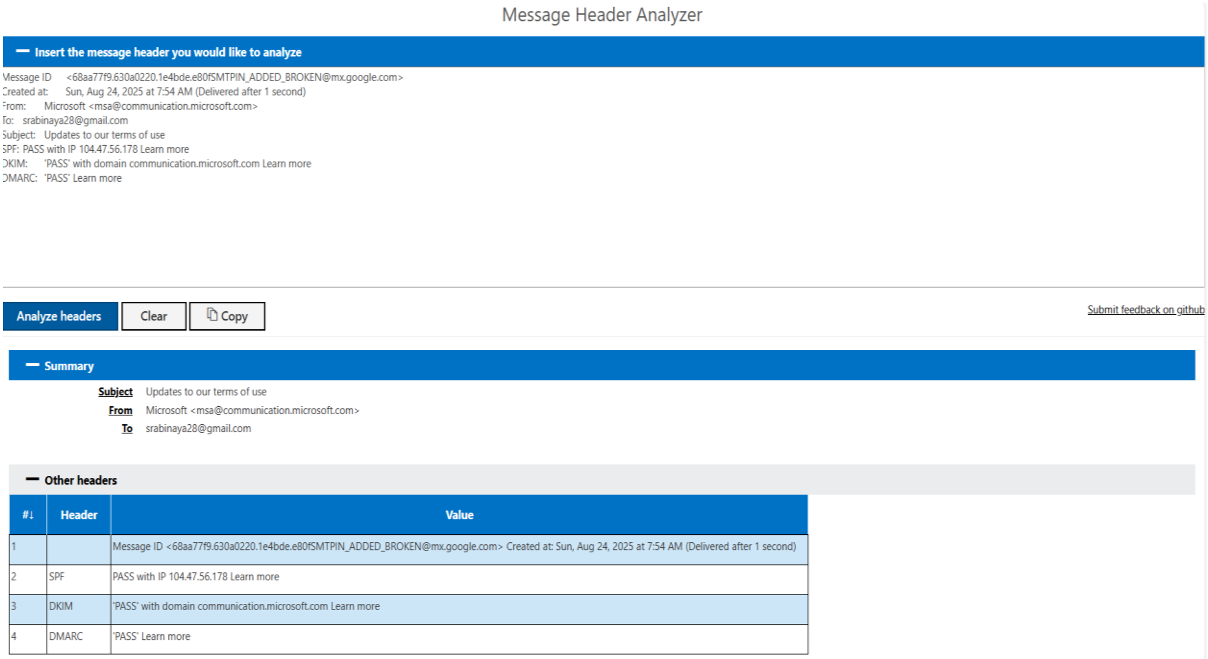
Message Header Analyzer

— Insert the message header you would like to analyze

```
Message ID    <68aa77f9.630a0220.1e4bde.e80fSMTPIN_ADDED_BROKEN@mx.google.com>
Created at:    Sun, Aug 24, 2025 at 7:54 AM (Delivered after 1 second)
From:    Microsoft <msa@communication.microsoft.com>
To:  srabinaya28@gmail.com
Subject:  Updates to our terms of use
SPF: PASS with IP 104.47.56.178 Learn more
DKIM:    'PASS' with domain communication.microsoft.com Learn more
DMARC:  'PASS' Learn more
```

Analyze headers
Submit feedback on github

OUTPUT:



Message Header Analyzer

— Insert the message header you would like to analyze

```
Message ID    <68aa77f9.630a0220.1e4bde.e80fSMTPIN_ADDED_BROKEN@mx.google.com>
Created at:    Sun, Aug 24, 2025 at 7:54 AM (Delivered after 1 second)
From:    Microsoft <msa@communication.microsoft.com>
To:  srabinaya28@gmail.com
Subject:  Updates to our terms of use
SPF: PASS with IP 104.47.56.178 Learn more
DKIM:    'PASS' with domain communication.microsoft.com Learn more
DMARC:  'PASS' Learn more
```

Analyze headers
Clear
Copy
Submit feedback on github
— Summary

Subject Updates to our terms of use
From Microsoft <msa@communication.microsoft.com>
To srabinaya28@gmail.com

#↓	Header	Value
1		Message ID <68aa77f9.630a0220.1e4bde.e80fSMTPIN_ADDED_BROKEN@mx.google.com> Created at: Sun, Aug 24, 2025 at 7:54 AM (Delivered after 1 second)
2	SPF	PASS with IP 104.47.56.178 Learn more
3	DKIM	'PASS' with domain communication.microsoft.com Learn more
4	DMARC	'PASS' Learn more

RESULT:

The **Mail Header Analyzer (MHA)** tool was successfully used to analyze email headers. The experiment identified sender domain mismatches and failed SPF/DKIM checks, confirming the presence of **email spoofing** in the analyzed message.