Date-19 /8/2023

Roll No. - 13

Expt. No. - 9

K.M.S.P. Mandal’s

Sant Rawool Maharaj Mavidyalaya, Kudal

**Department of Computer Science**

Signature

Analyze email headers and content to trace the origin of suspicious emails.

Title - \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

An email header, also known as the email's "message header" or "internet header," is a block of metadata that is prepended to the actual email message. It contains technical information about the email and its transmission. When you view an email header, you can see details about how the message traveled from the sender to the recipient.

**Key information found in an email header includes:**

1. Return-Path: The email address to which bounced or undeliverable messages are sent.

2. Received: A series of entries indicating the mail servers through which the email passed, including timestamps and IP addresses. This helps trace the route of the email.

3. From: The email address of the sender.

4. To: The email address of the recipient.

5. Subject: The subject line of the email.

6. Date: The date and time when the email was sent.

7. MIME- Version: Indicates the MIME (Multipurpose Internet Mail Extensions) version used for formatting the message.

8. Content-Type: Describes the type and format of the content within the email (e.g., text/plain for plain text or text/html for HTML).

9. Message-ID: A unique identifier for the email message.

10. User-Agent: Information about the email client or software used by the sender.

11. X-Mailer: Similar to User-Agent, it provides information about the email client.

12. References and In-Reply-To: Used for threading emails in a conversation.

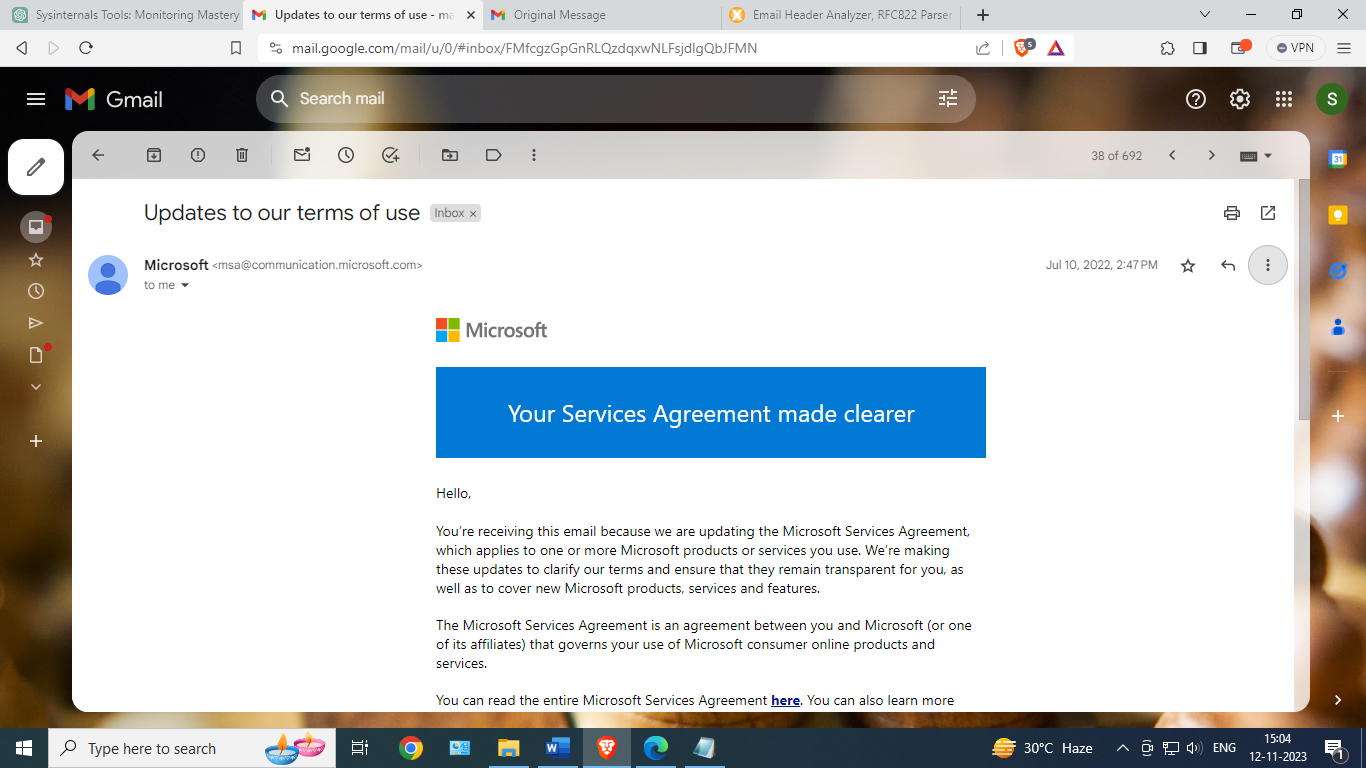
Email headers are often hidden by default in most email clients, as they contain technical details that are not relevant to most users. However, they can be useful in troubleshooting email issues, verifying the authenticity of emails, and investigating potential spam or phishing attempts. Advanced users, IT professionals, and cybersecurity experts may examine email headers to gather more information about the email's origin and path.

### Cybersecurity First Principles

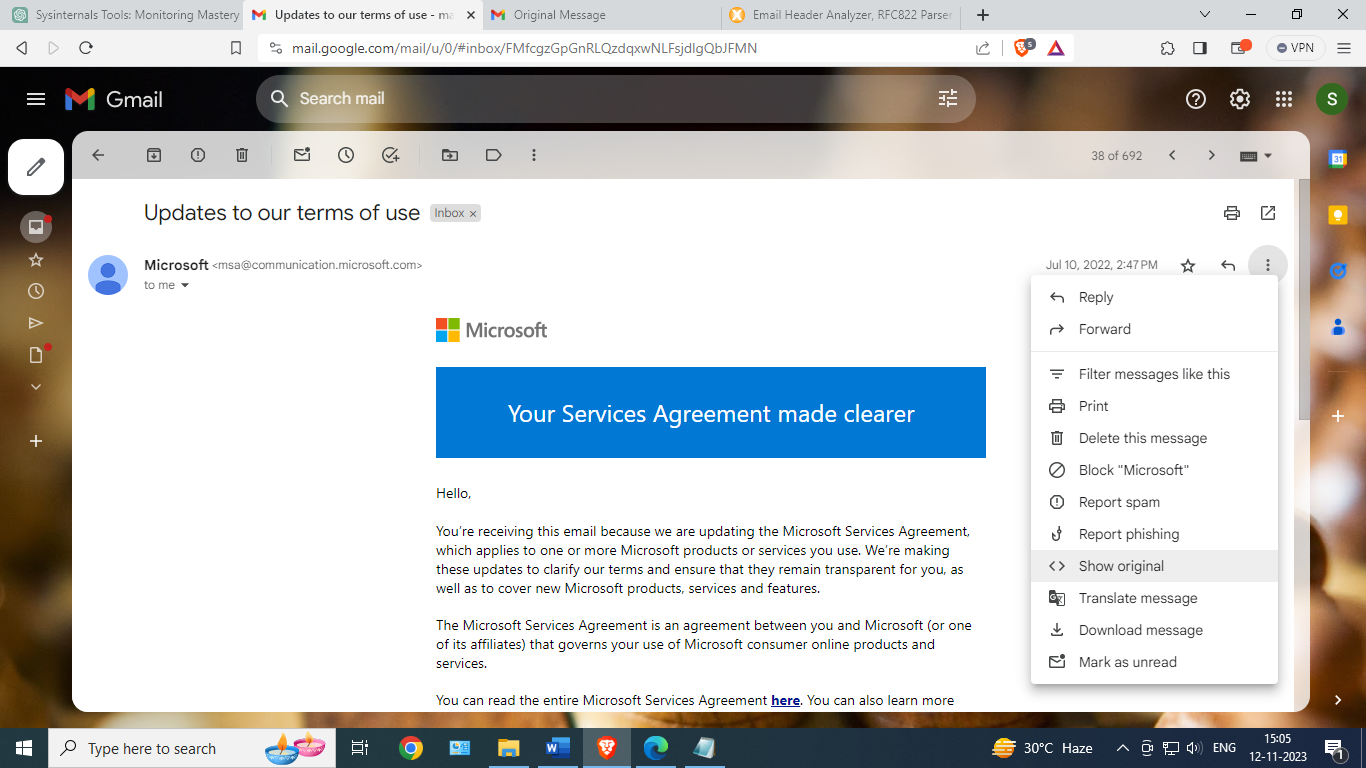
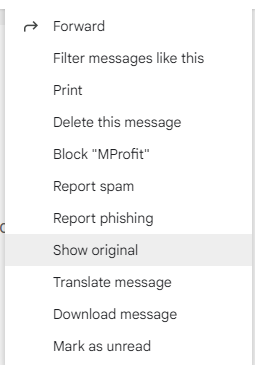
* **Layering**: Cyber security uses multiple layers of defense or protecting information. If one layer is defeated the next layer should catch it. This lesson emphasizes the human element, that is we as humans have to catch problems (like phishing) that make it past the email-level and browser-level filtering mechanisms.

**Analyzer email header**

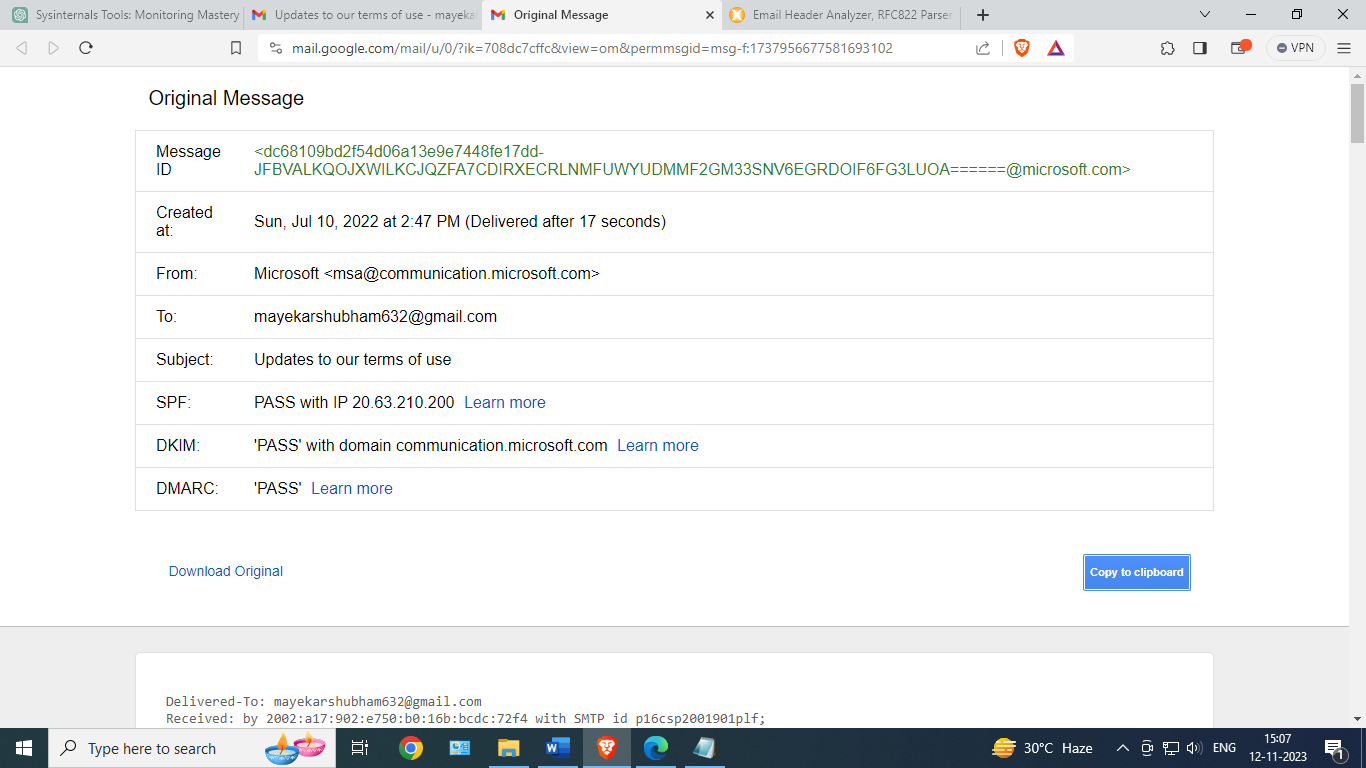
Open mail



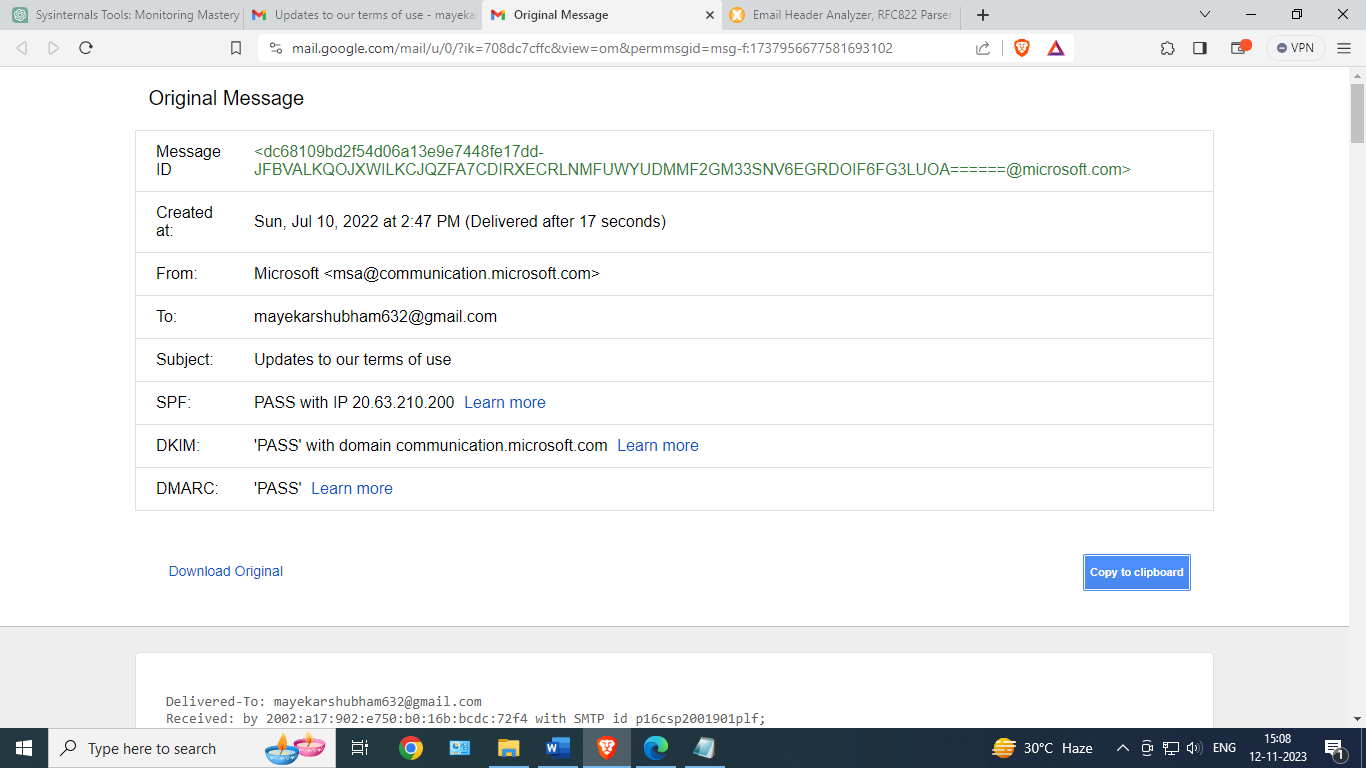
Click on more option and choose show original

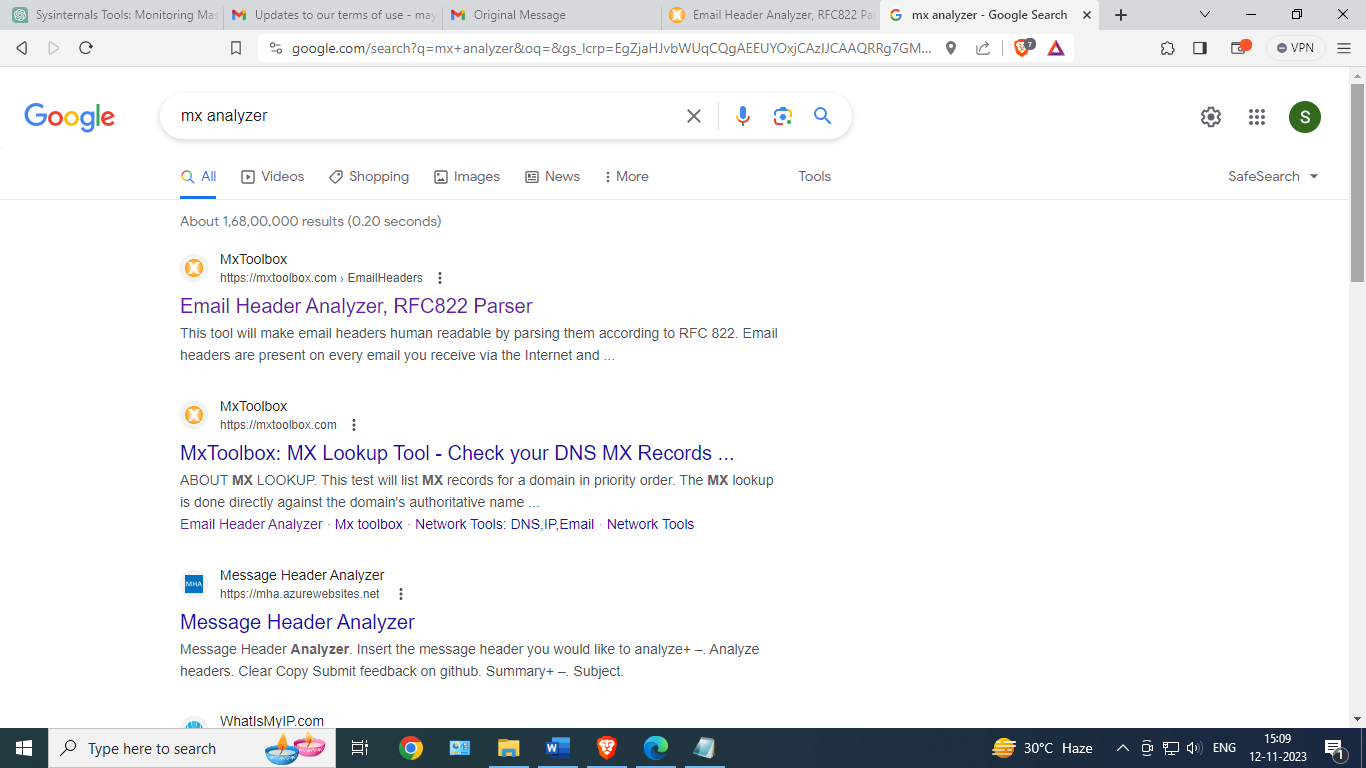
Original message

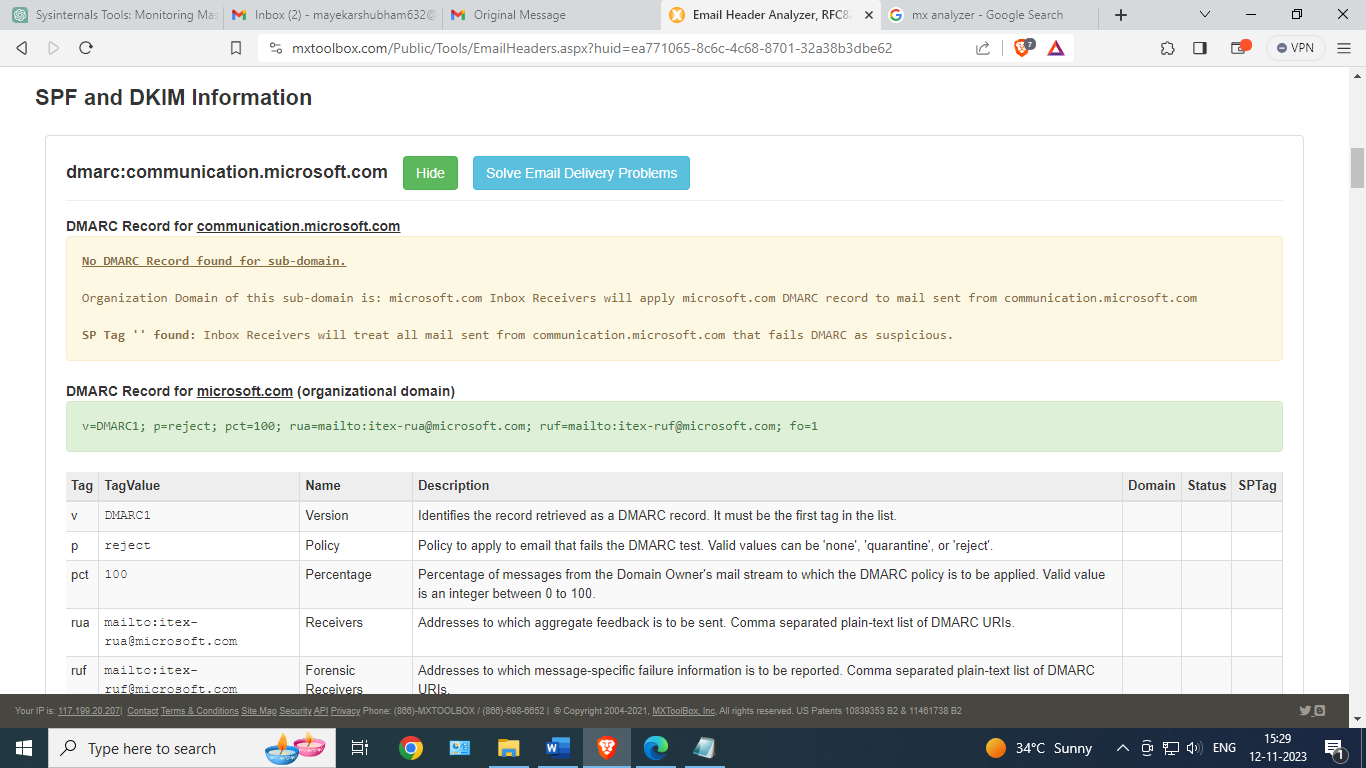


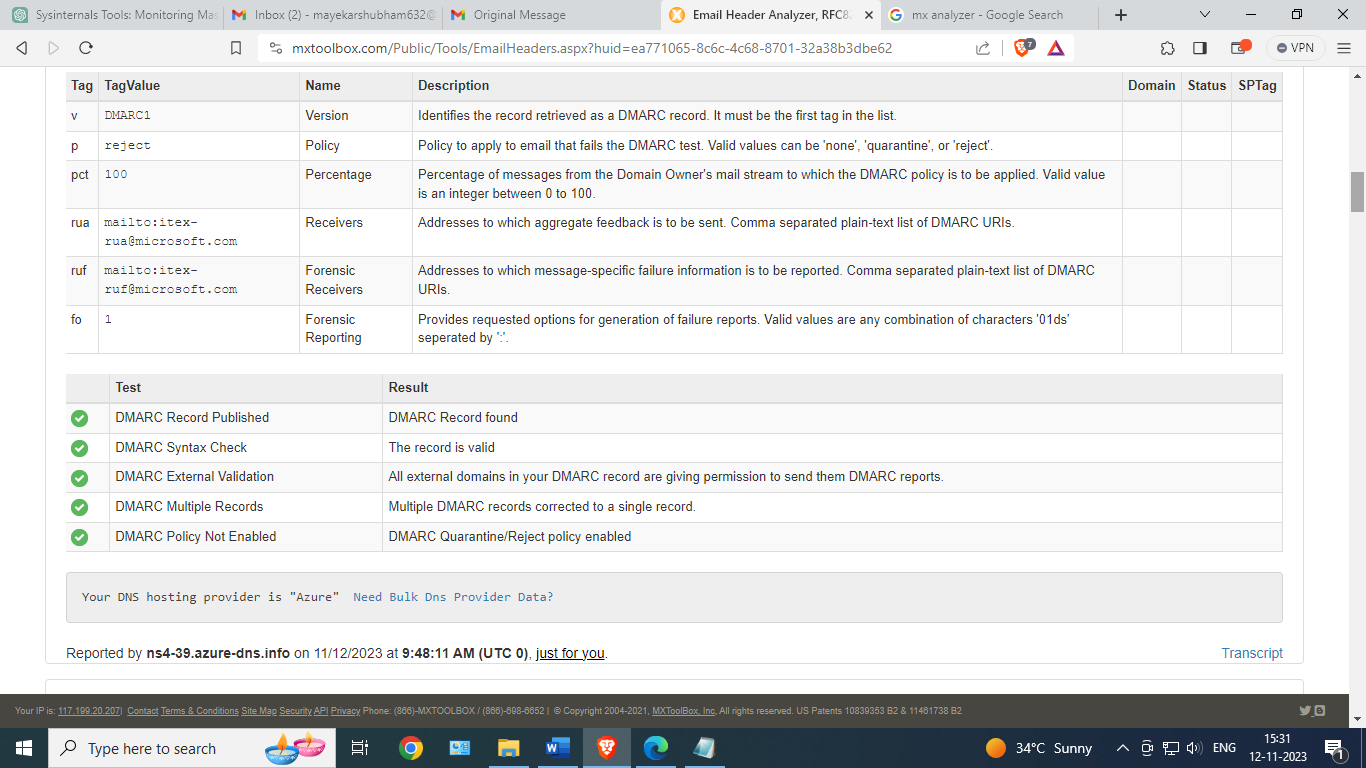
Click on Copy clipboard

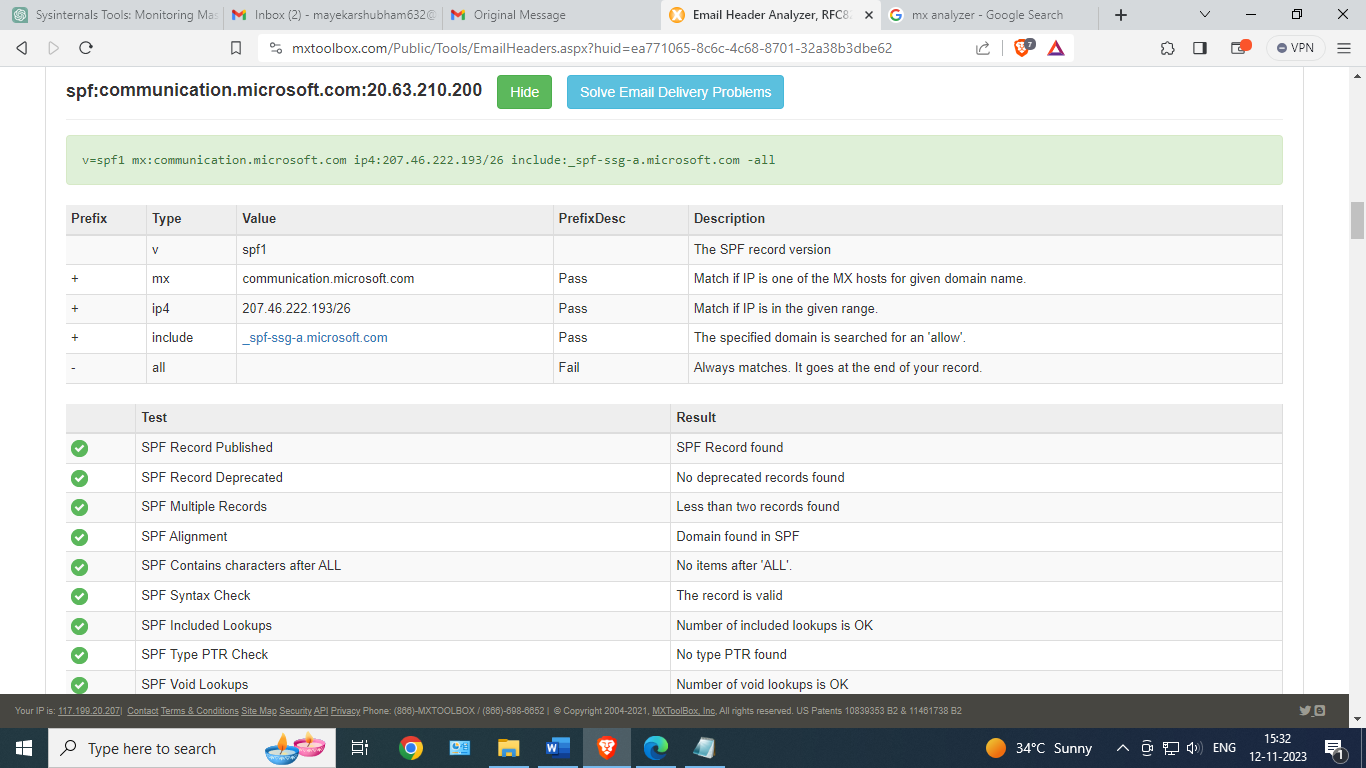


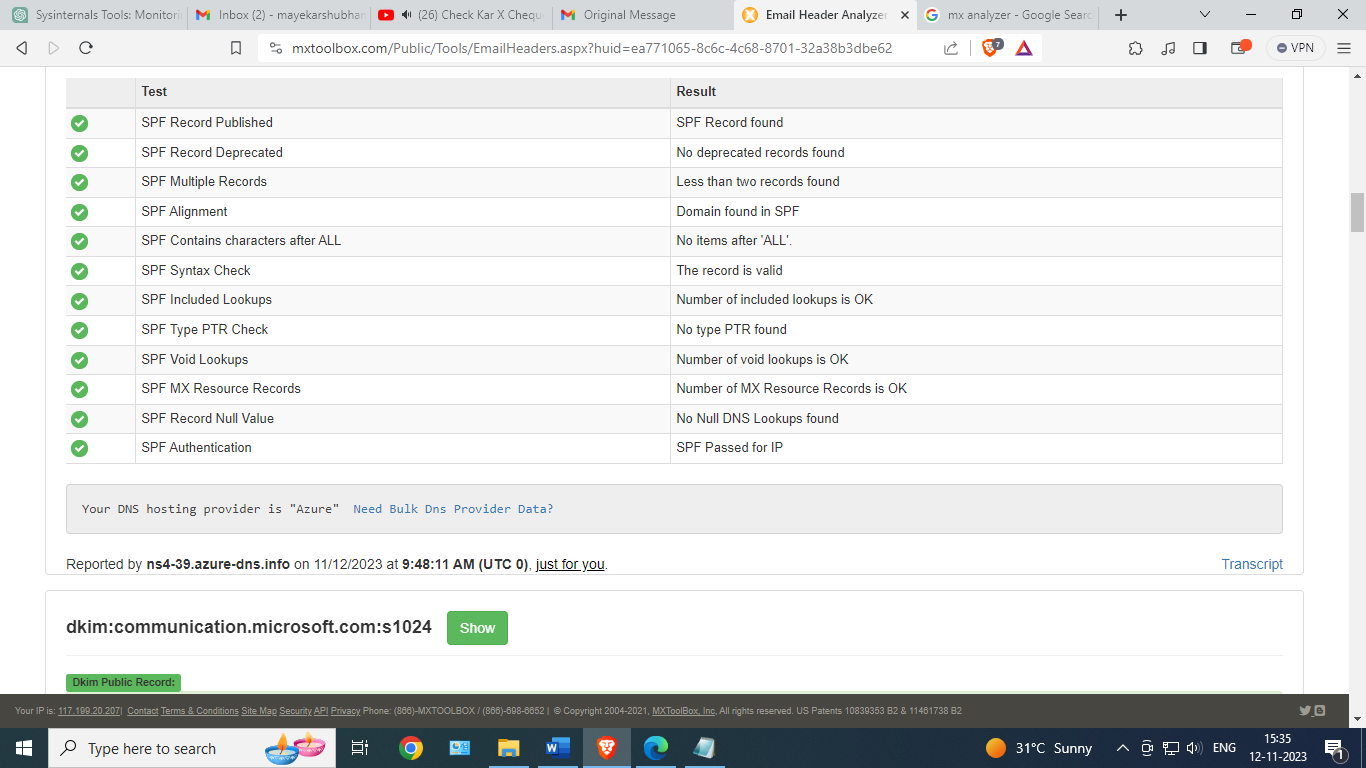
Open mx analyzer

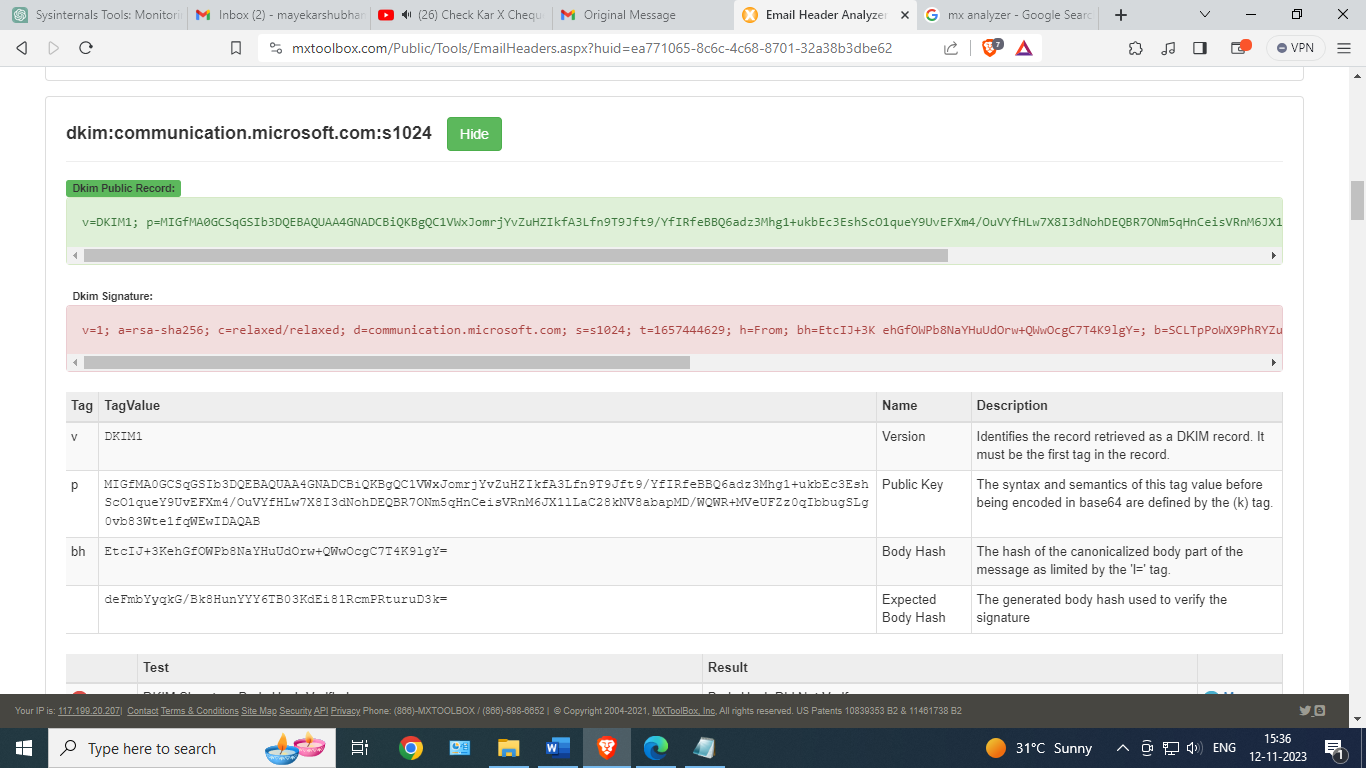


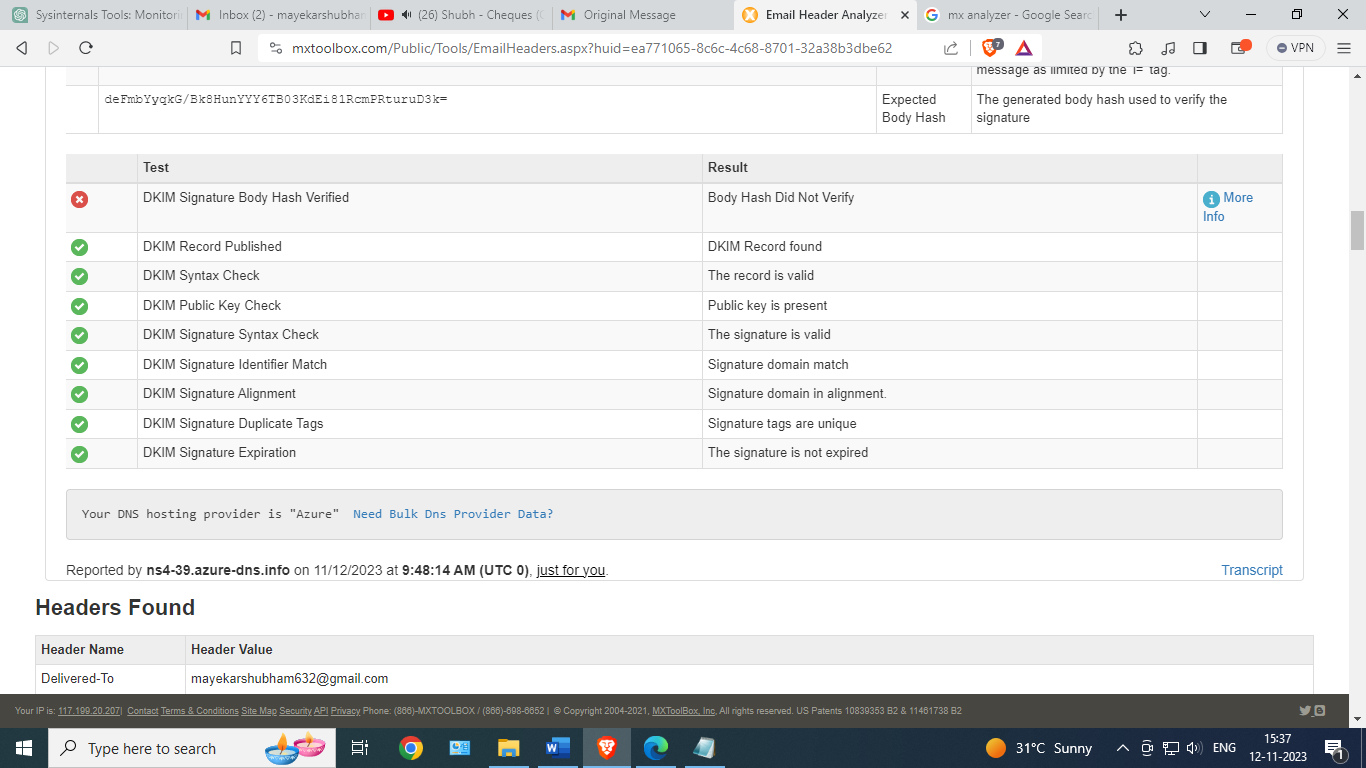




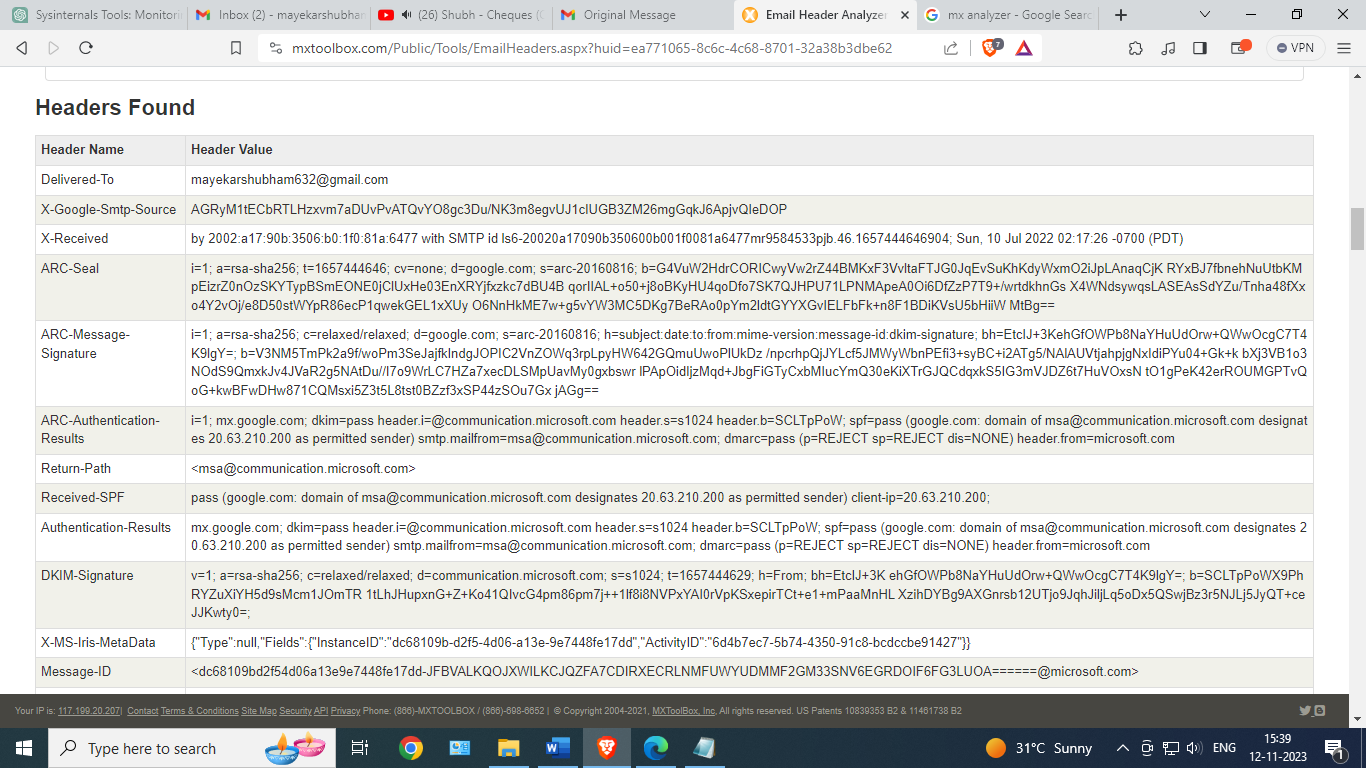








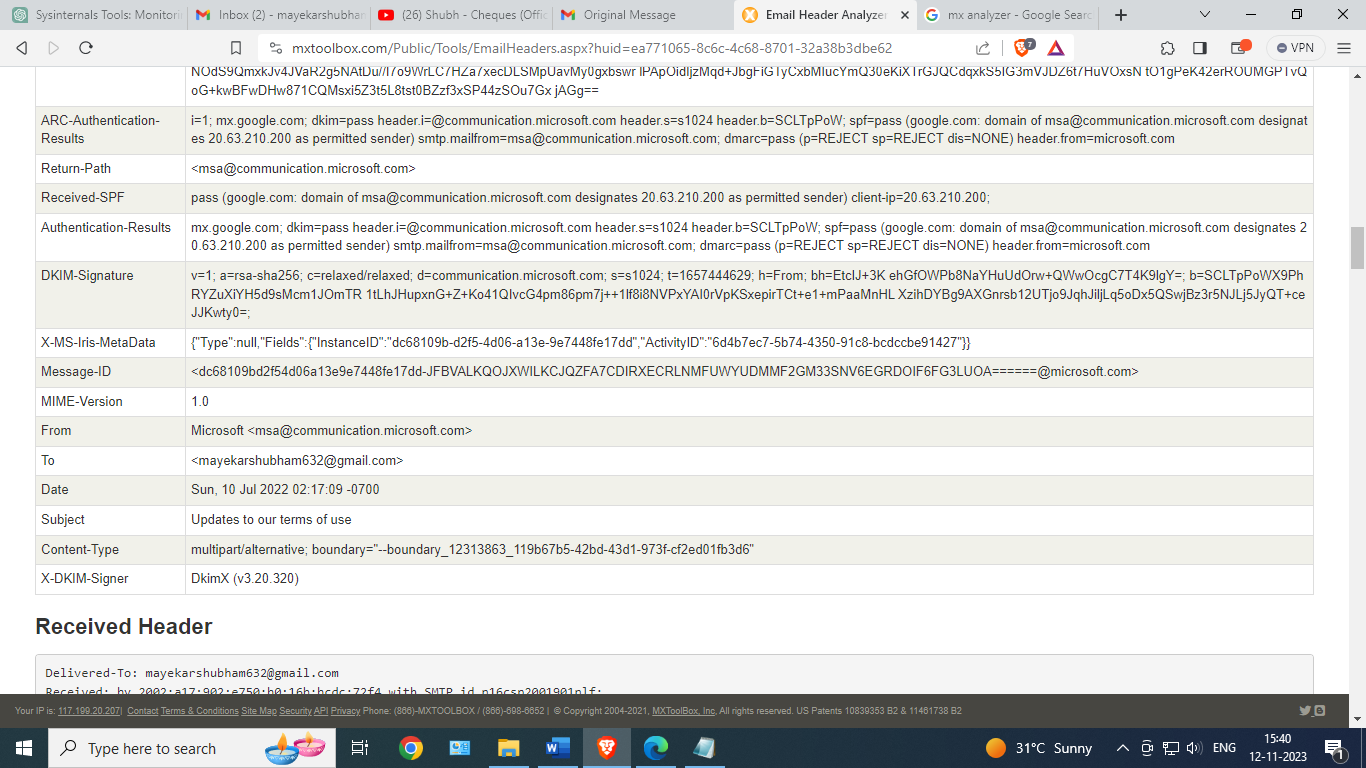
Headers found



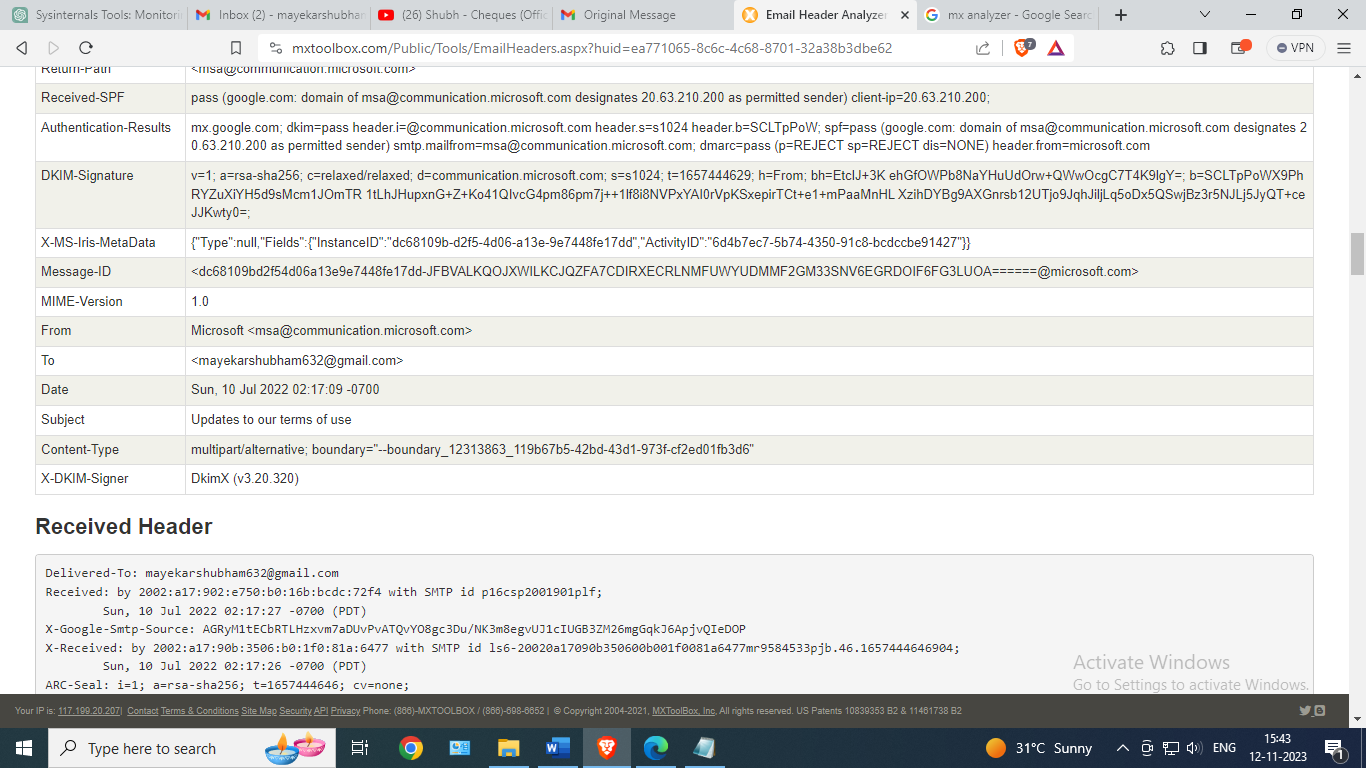
MIME- Version

15. MIME version

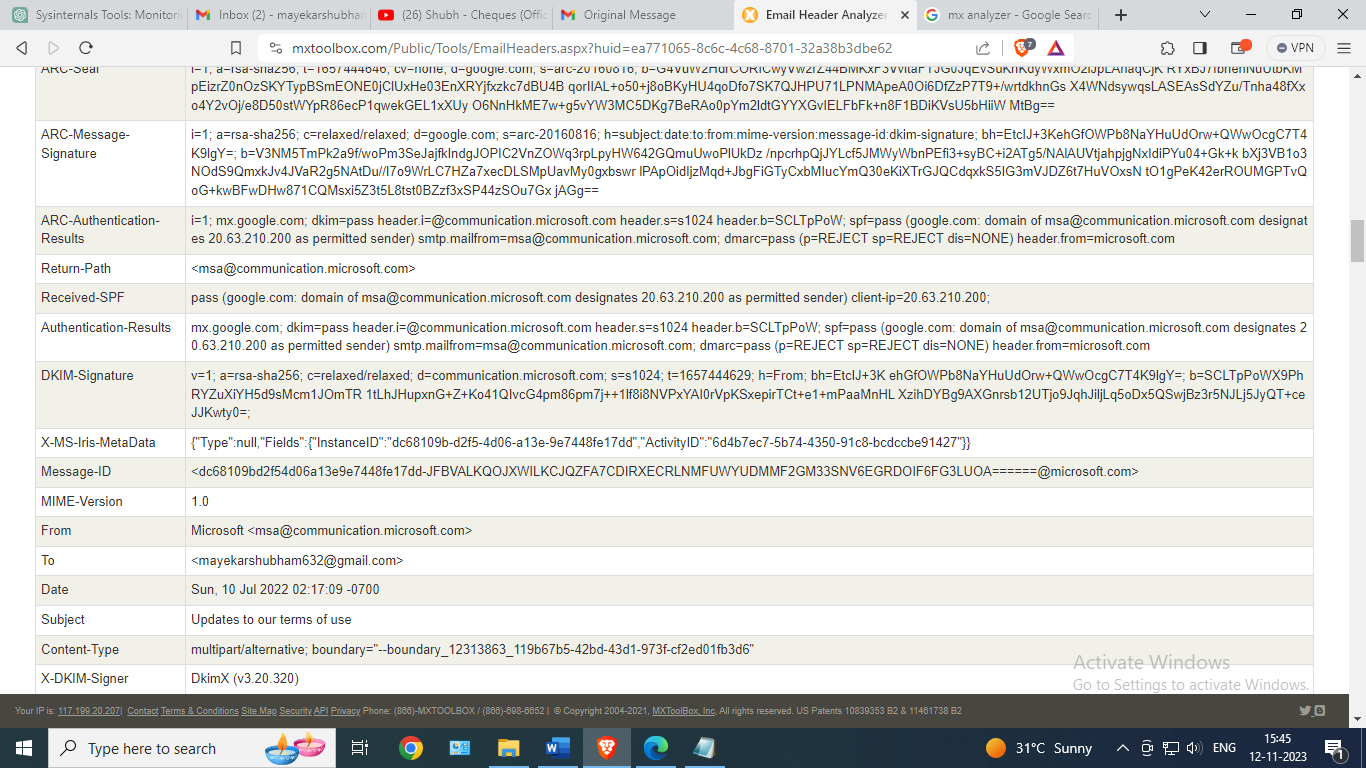
Message ID

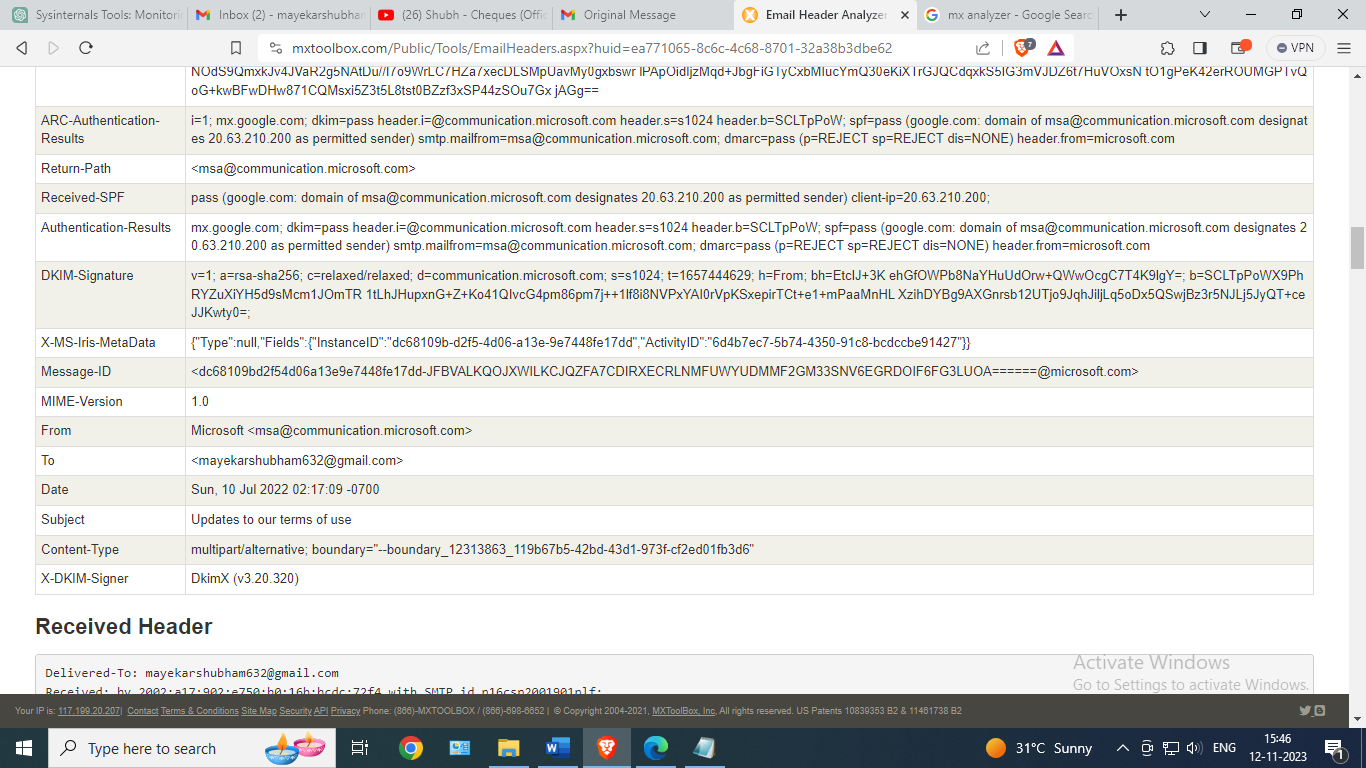


DKIM -Signature

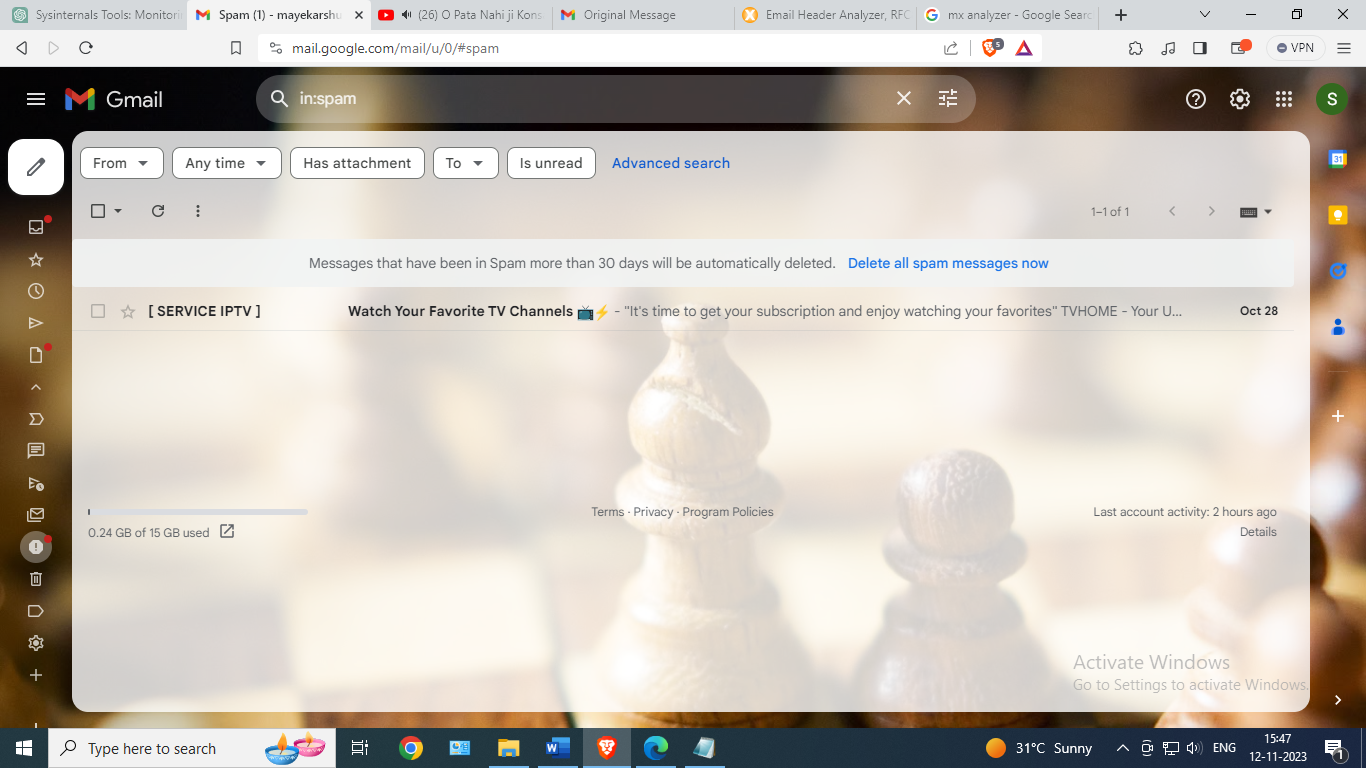


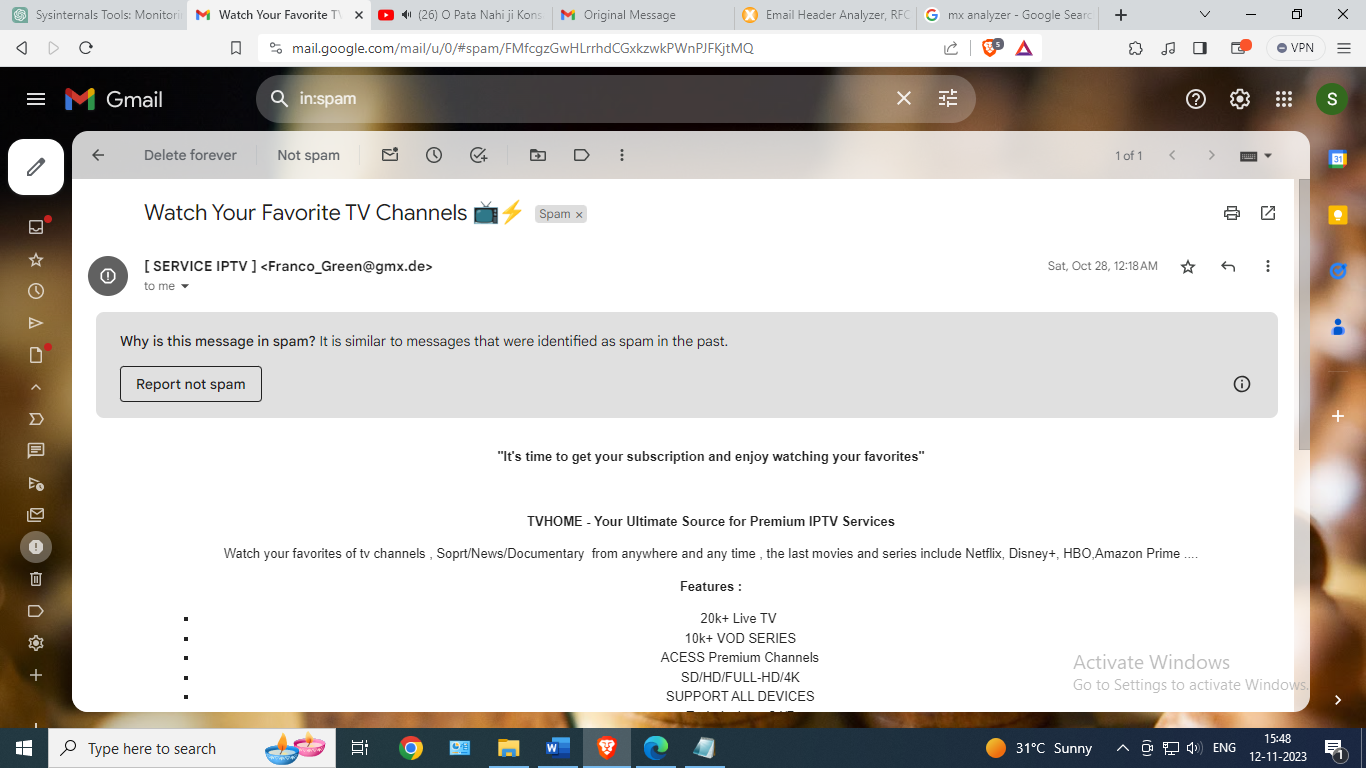
Return path



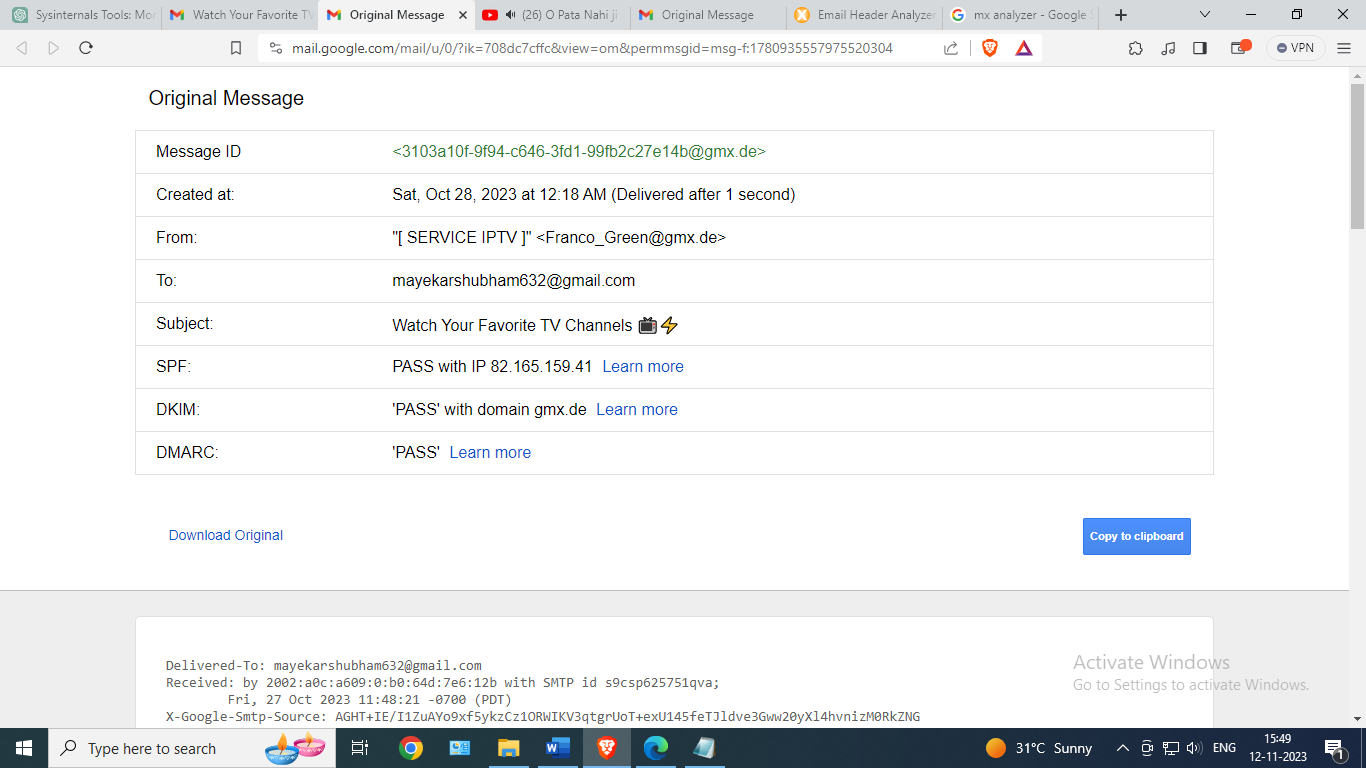


2) Spam Mail header analyzer

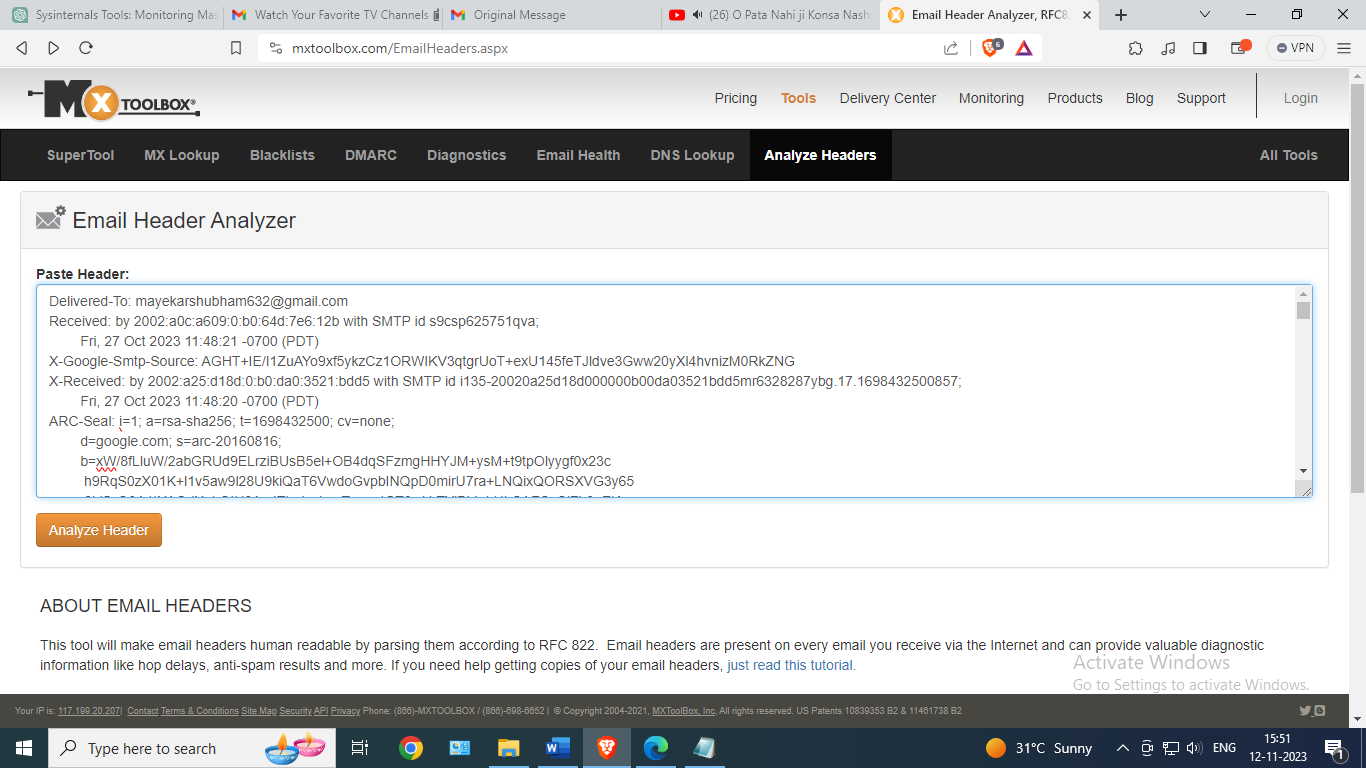


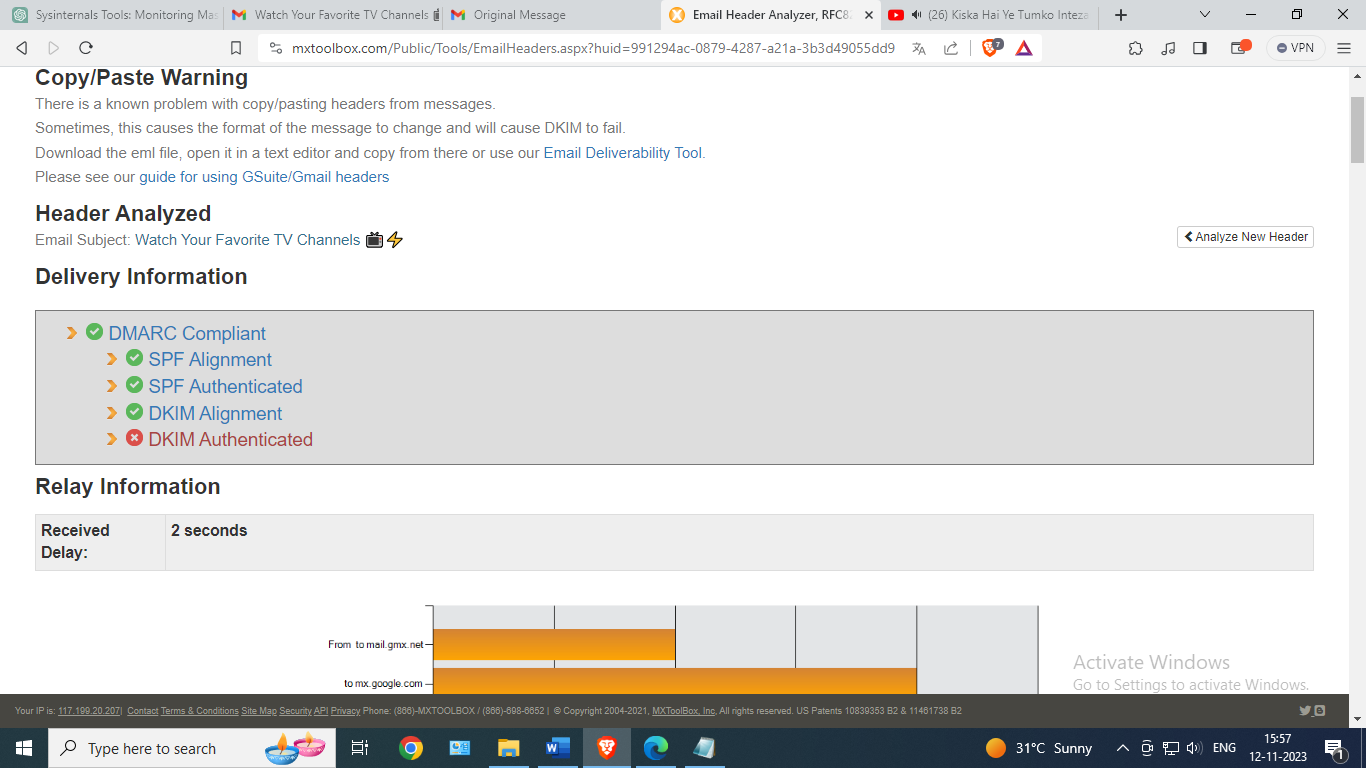


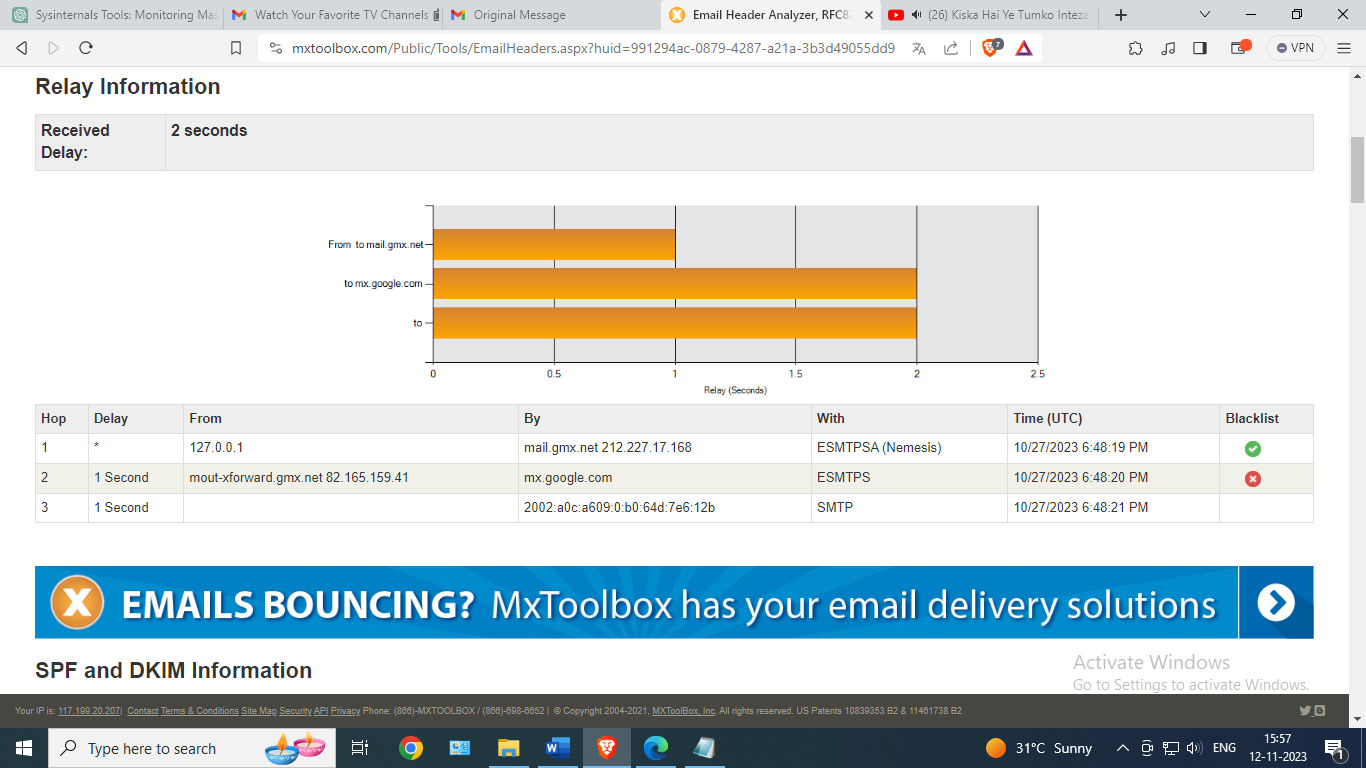
Original Message

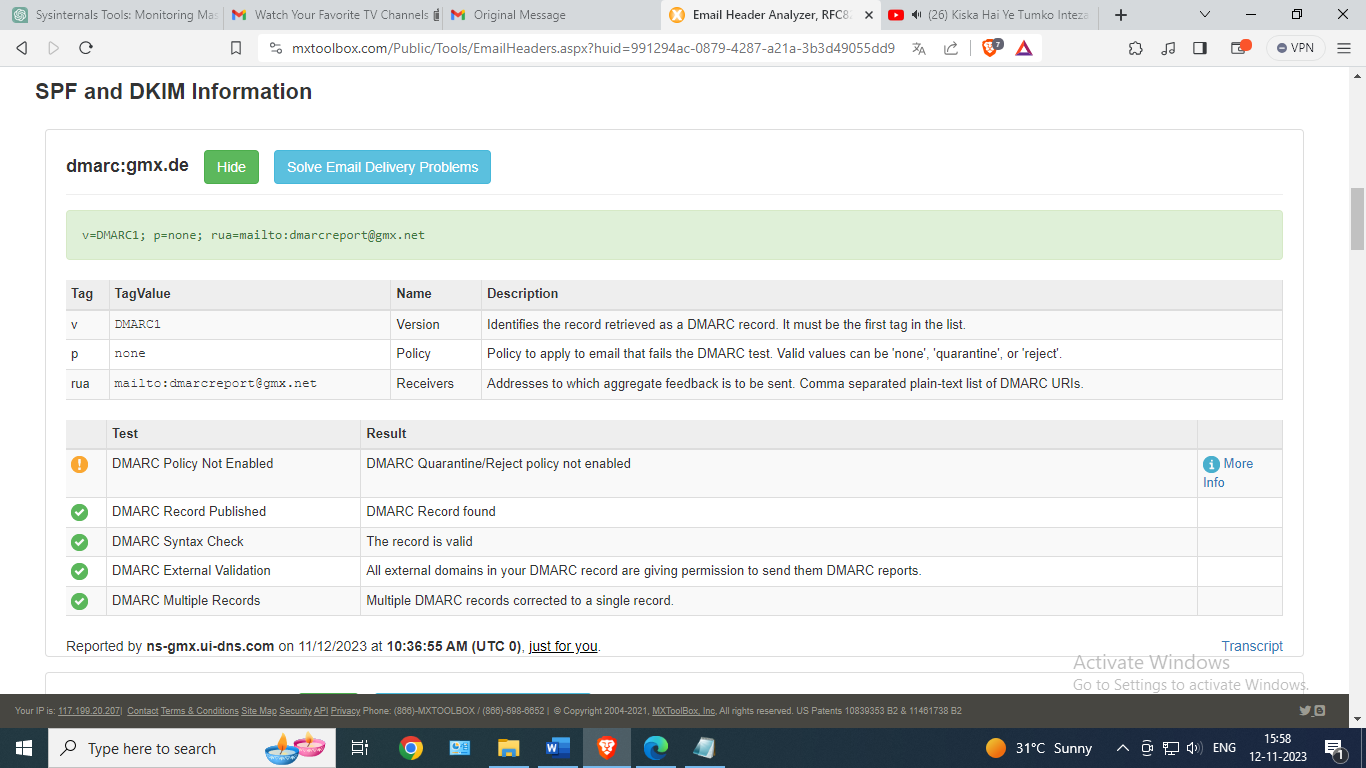


Header Analyzer

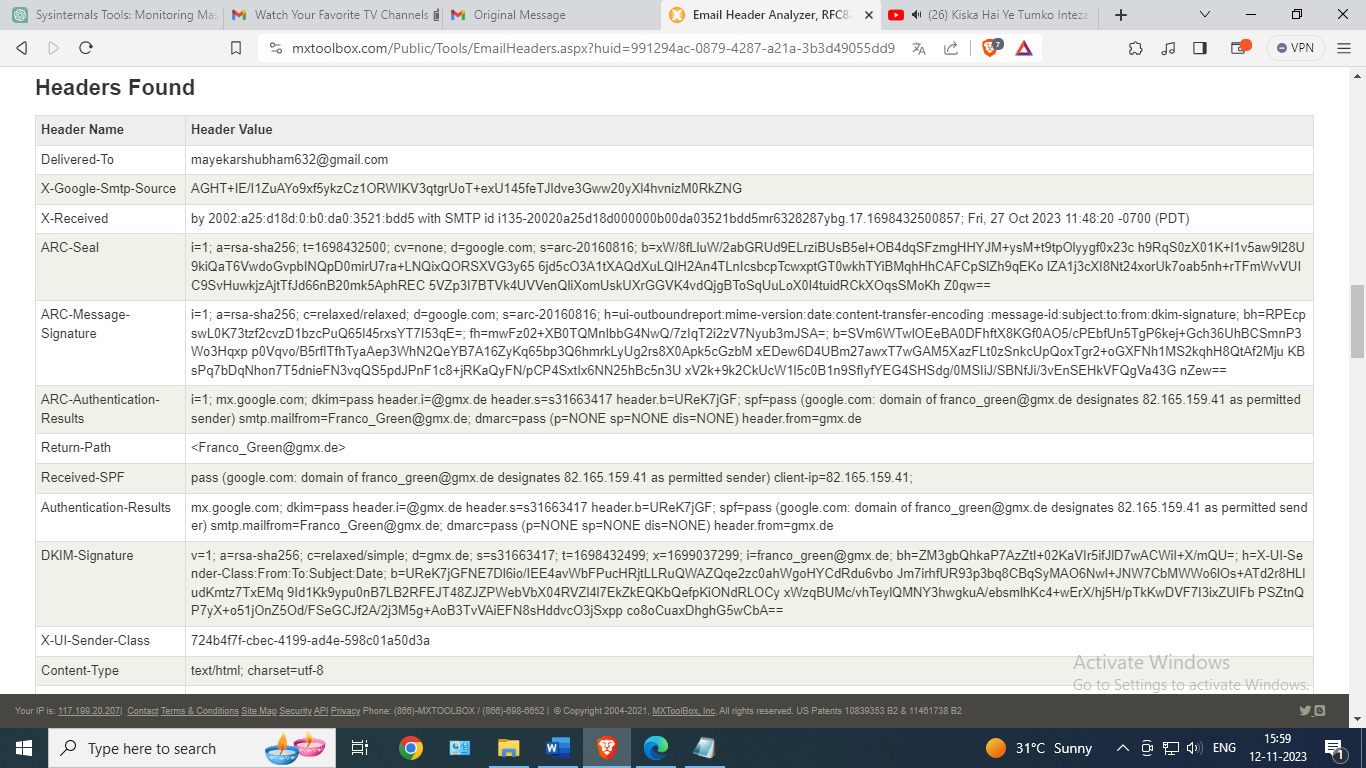


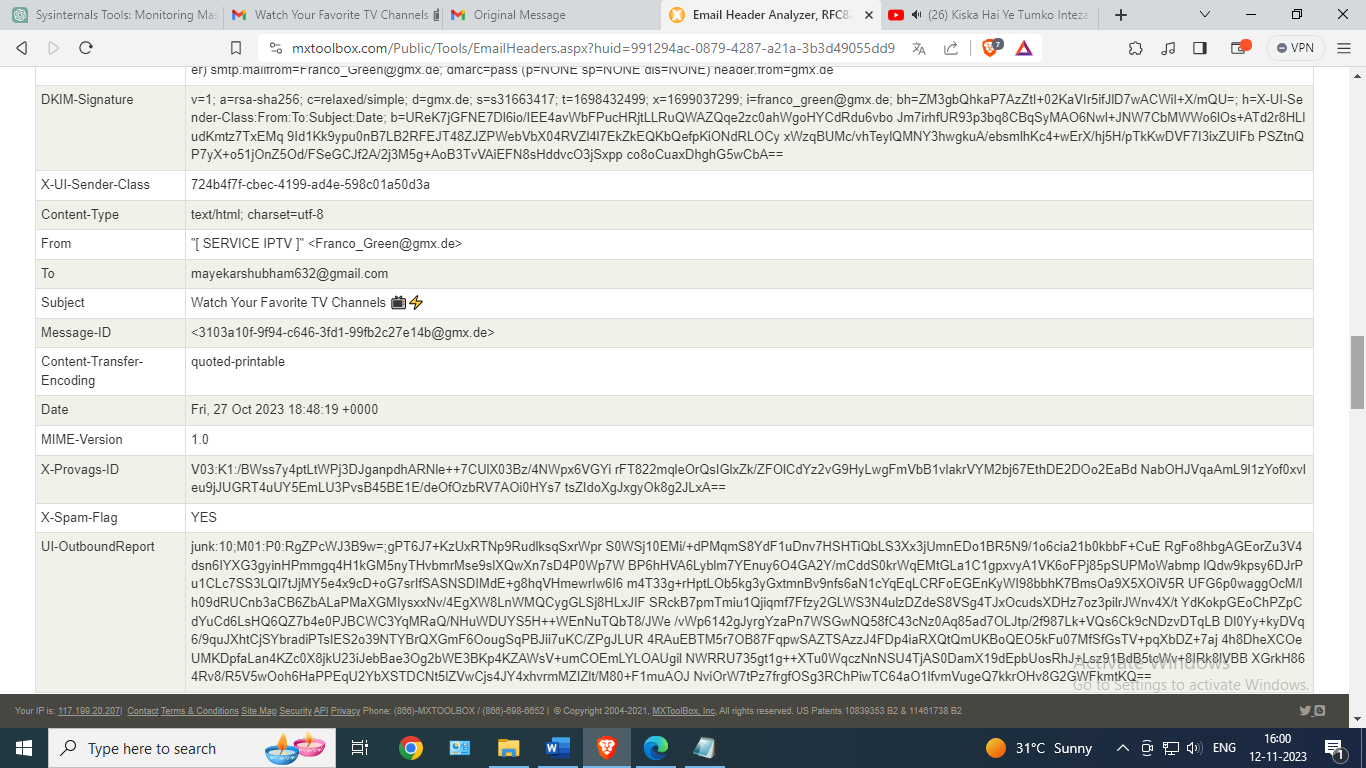






Headers Found





3) Email Header analyzer

