# Kaushal Kotkar

**BE-15**

# Roll no: 54

**Experiment No. 1**

**Aim:** a) Perform Email Header Analysis for extracting valuable information like sender IP address, email servers, and routing information.

1. Conduct email address enumeration by attempting to verify the existence of email addresses within a target domain. Use tools like the Harvester or thehunter.io to search for email addresses associated with a specific domain. This can help identify valid email addresses within an organization
2. Analyze the metadata of an email, including date and time stamps, email clients used, or the originating IP address, email's origin, potential geographic location of the sender, or possible email routing

**Lab outcome:** Conduct advanced searches to gather intelligence and apply advanced OSINT search techniques and tools.

# Theory:

Email header analysis is a process of examining the header section of an email to extract valuable information about the email's origin, path, and routing details. This information can be useful for various purposes, such as identifying the source of spam or phishing emails, tracing the origin of suspicious emails, and understanding the email delivery path.

The email header is a crucial part of an email message and contains essential metadata about the message's journey from the sender to the recipient. It consists of various fields, each providing specific details about the email's origin, routing, and delivery. Some of the key fields that can be analyzed for extracting valuable information are:

From: This field contains the email address of the sender. It is essential to verify the sender's address to identify possible spoofing or phishing attempts.

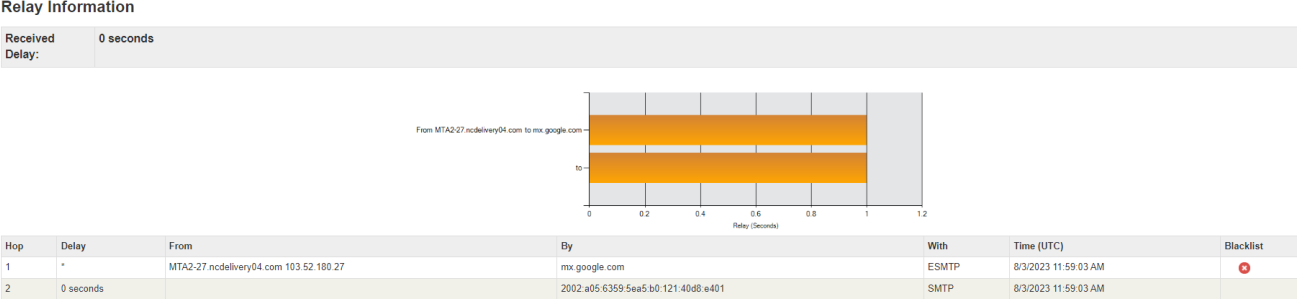
Received: This field appears multiple times in the email header, and each occurrence indicates a hop in the email delivery path. The received field typically includes the IP address of the email server that handled the message, along with the timestamp. By analyzing these entries, it's possible to trace the email's route and identify any suspicious or unauthorized servers in the path.

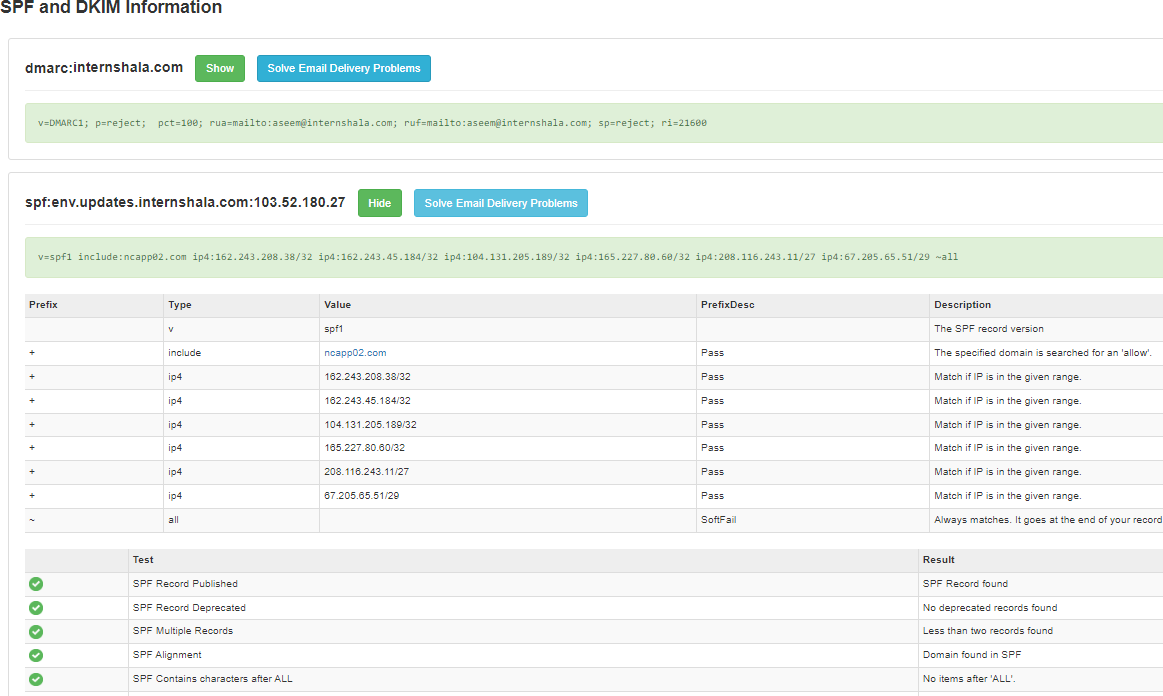
Return-Path: This field indicates the email address to which delivery errors and bounce-backs will be sent. It is used by mail servers to handle undeliverable emails.

Received-SPF: Sender Policy Framework (SPF) is an email authentication method that helps prevent email spoofing. This field indicates whether the email passed SPF authentication and can provide insights into the email's legitimacy.

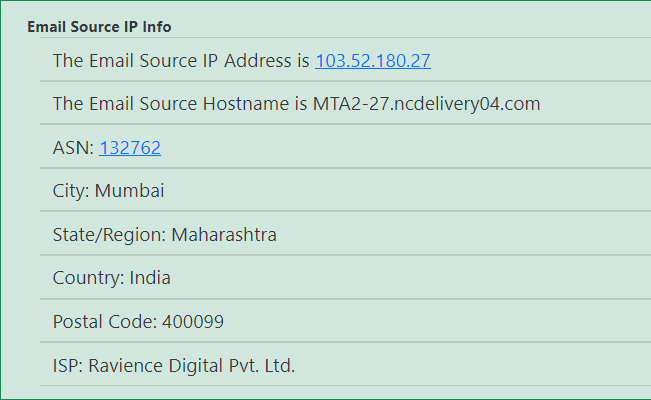
# Output:

**MXtoolbox:** MXtoolbox provides email-related diagnostic tools, including the ability to analyze email headers. It can extract information like sender IP addresses, sender domains, and mail server details from email headers.

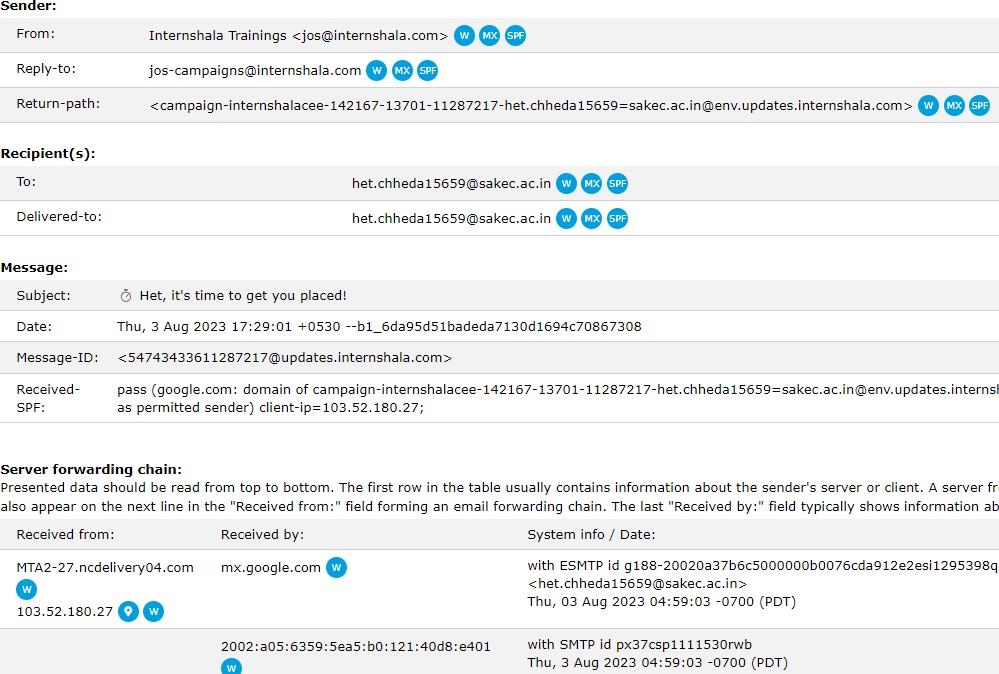




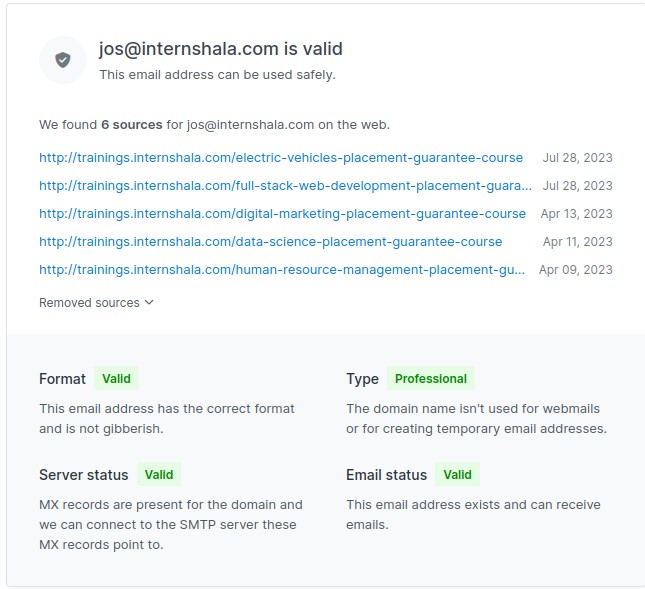
**WhatIsMyIP:** This tool allows you to identify the sender's IP address from the email header. It helps you determine the geographical location and other information associated with the IP.



**Wintelguy:** Wintelguy offers a range of networking tools, including email header analysis. It can reveal sender IP addresses and provide details about the route the email took.



**Hunter.io:** Hunter.io is a tool designed for email-related tasks, including email verification and discovery. It may provide additional context to the analysis by identifying the domain’s characteristics.



**Conclusion:** Through email header analysis using tools like mxtoolbox, WhatIsMyIP, and wintelguy, & hunter.io we successfully extracted valuable information from the headers, including sender IP addresses, email server details, and routing information.