Date-19 /8/2023

Roll No. - 25

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 - \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

Email is an indispensable communication tool. We use it every day. Unfortunately, many attacks also originate in emails. Wouldn’t it be great if everyone had some mad email ninja skills! Don’t worry, at the end of this session, you should feel pretty good about your email analysis skills.

A vigilant, trained and aware human user is a critical layer of defense against threats, both internal and external. Even if malicious URLs and emails get past spam filters and anti-virus software, a human user can catch it. Such a defensive strategy is common in secure system designs. It also demonstrates a cyber security first principle called Layering.

When reading emails, the first item that grabs our attention is the sender’s name, email, and subject. But, it may come as a surprise that spoofing these in an email is a pretty easy thing! It is also effective at fooling unsuspecting email users.

## Email Headers

Email Headers hold a lot of information. Much of this information is never displayed to the user. The email reader only sees a select few pieces of information like the subject, date, and the sender’s email and info. The surprising part is that the information that is actually displayed to a user can be easily forged!

[Phishing](https://www.consumer.ftc.gov/articles/0003-phishing) emails often appear to be from someone you know. They ask for urgent and critical actions like sending money, sharing bank information and passwords. Double-check the real source of the email. Follow-up with a call to confirm the emergency.

* **When in doubt, throw it out:** Links in emails, social media posts, and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it.
* **Think before you act:** Be wary of communications that implore you to act immediately, offer something that sounds too good to be true or ask for personal information.

## Role of Email in Investigation

Emails play a very important role in business communications and have emerged as one of the most important applications on internet. They are a convenient mode for sending messages as well as documents, not only from computers but also from other electronic gadgets such as mobile phones and tablets.

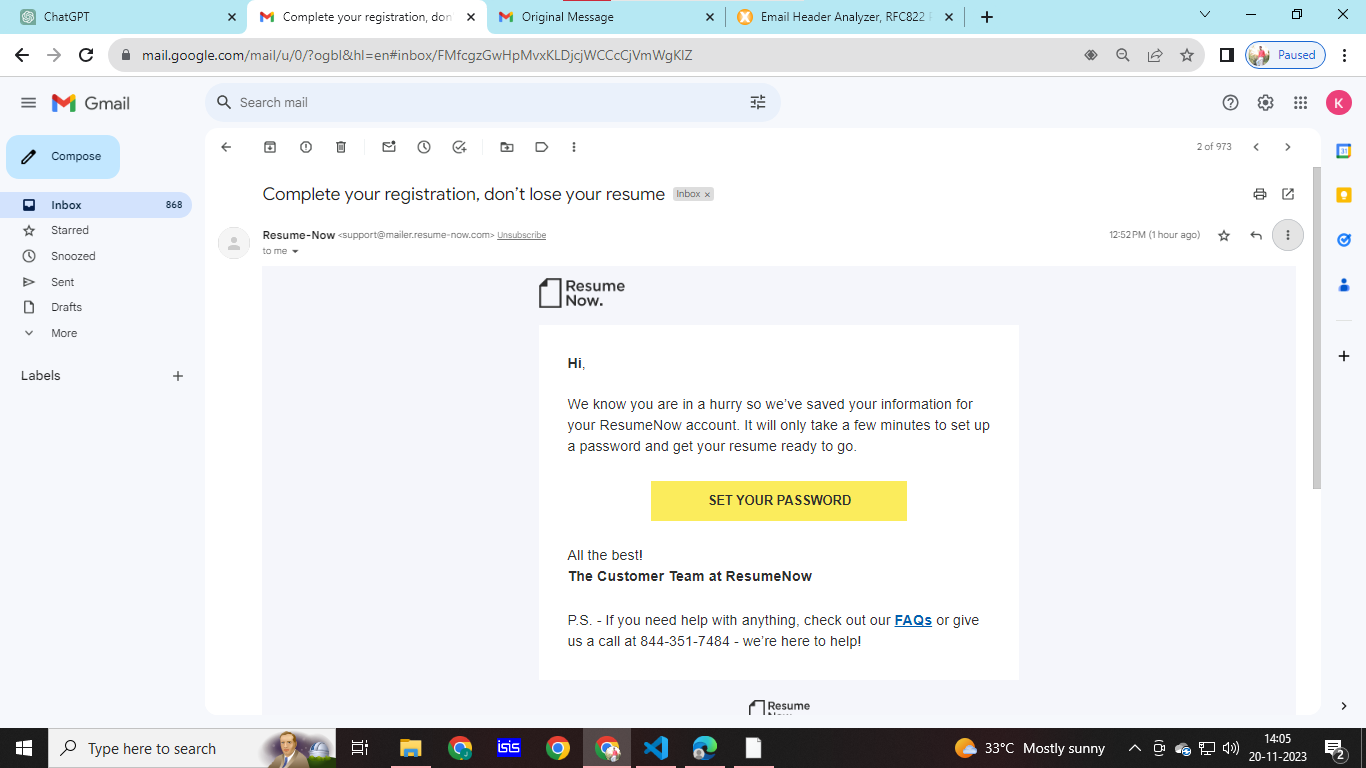
The negative side of emails is that criminals may leak important information about their company. Hence, the role of emails in digital forensics has been increased in recent years. In digital forensics, emails are considered as crucial evidences and Email Header Analysis has become important to collect evidence during forensic process.

### Cybersecurity First Principles

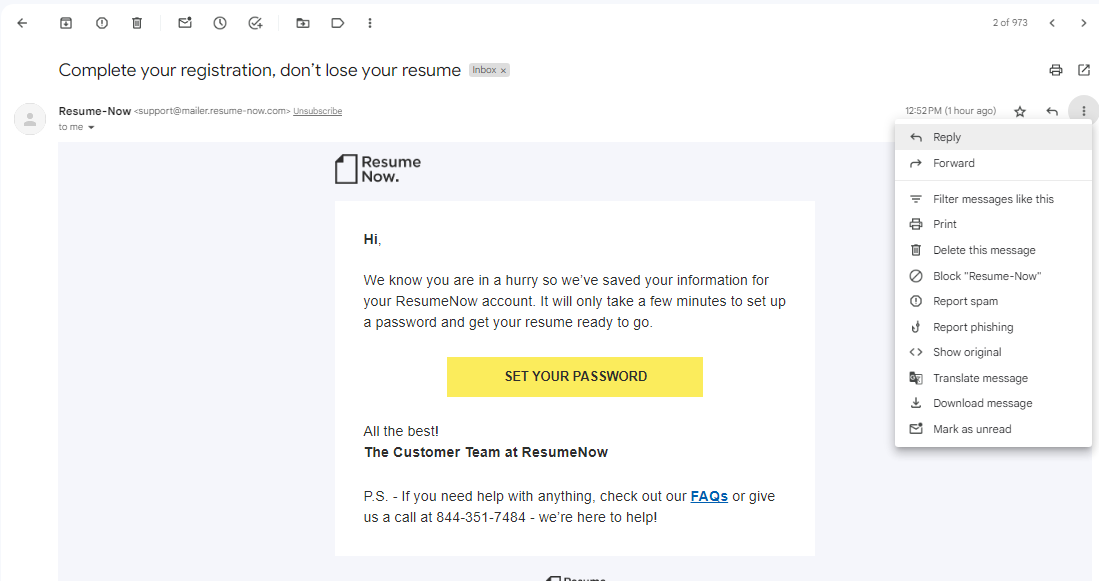
* **Layering**: Cyber security uses multiple layers of defense or protecting information. If one layer is defeated the next layer should catch it. This lesson emphasizes the human element, that is we as humans have to catch problems (like phishing) that make it past the email-level and browser-level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

**Analyzer email header**

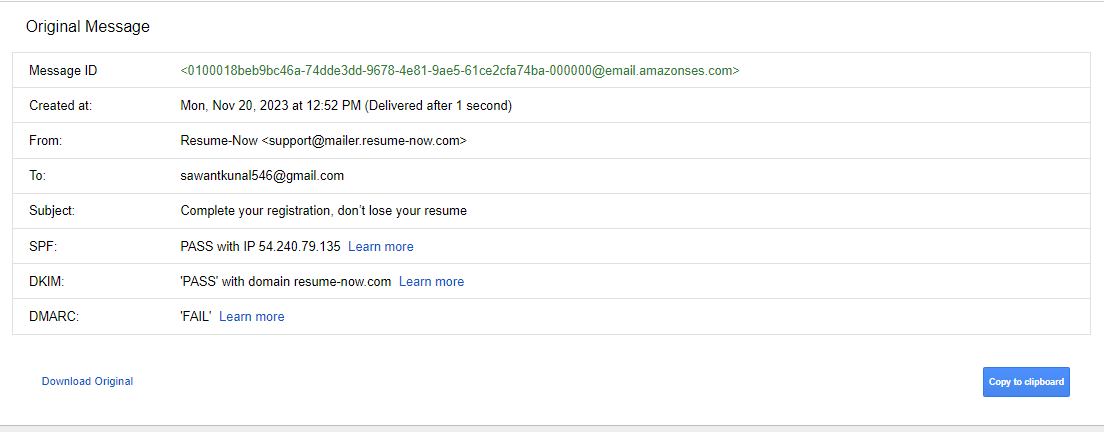
Open mail

****

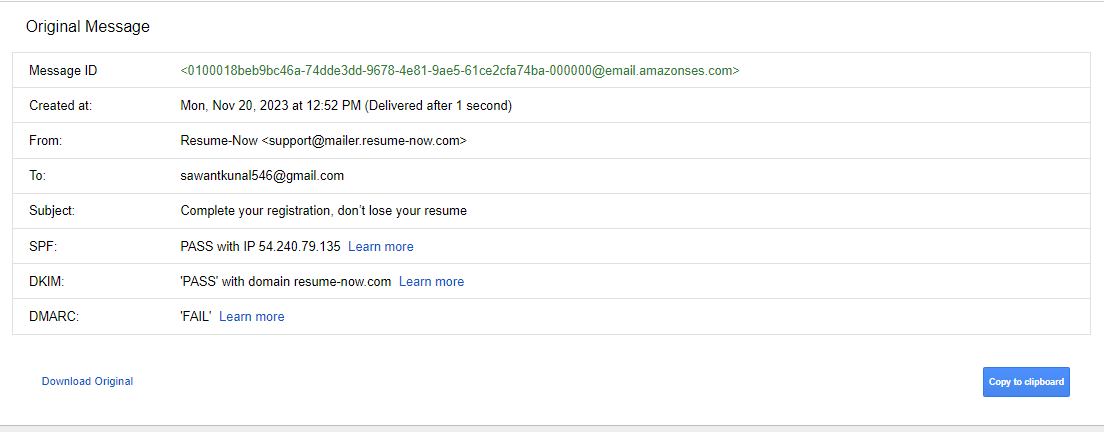
Click on more option and choose show original



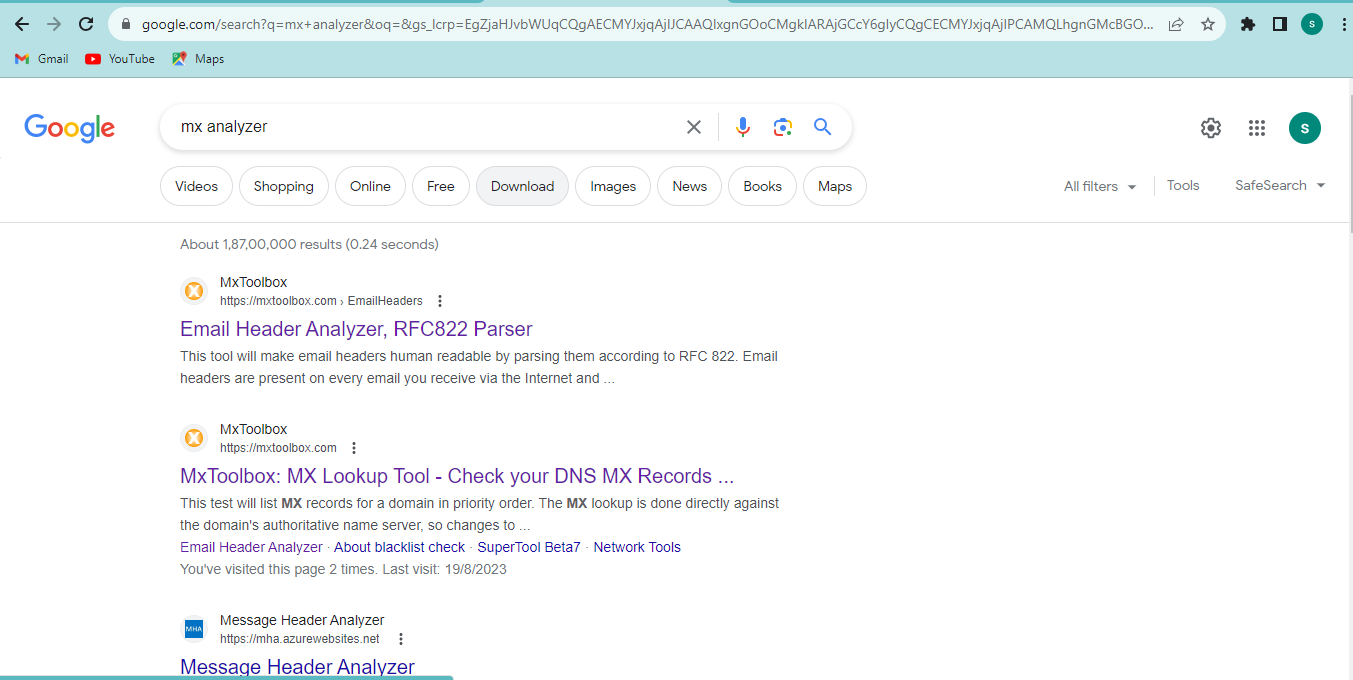
Original message

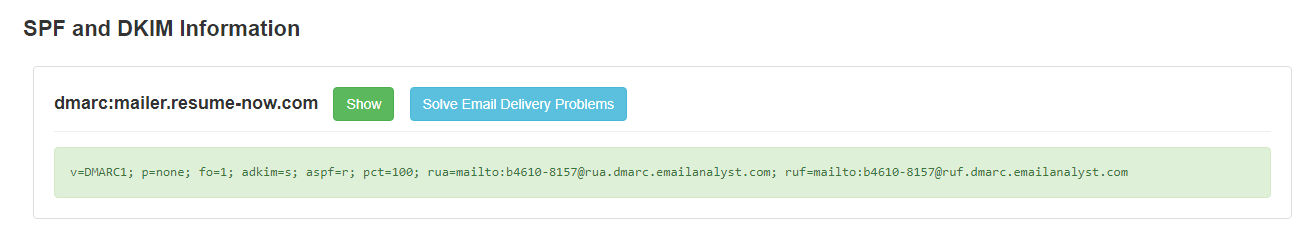


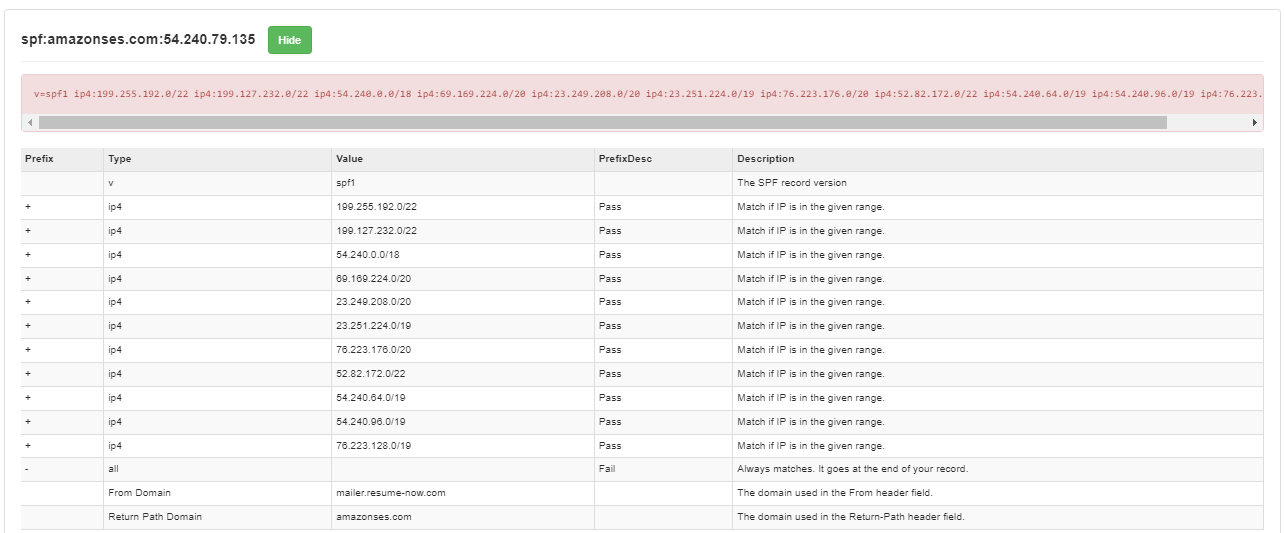
Click on Copy clipboard

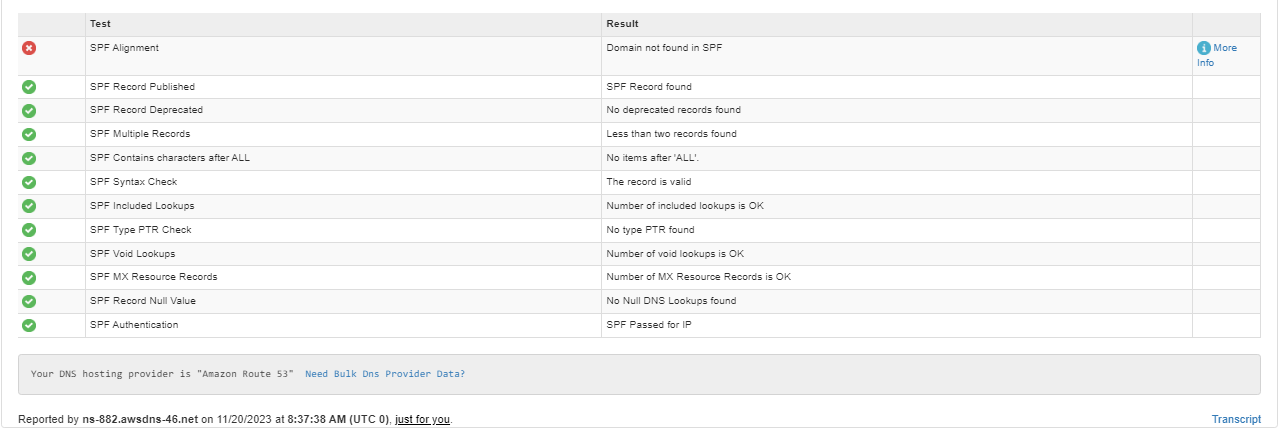


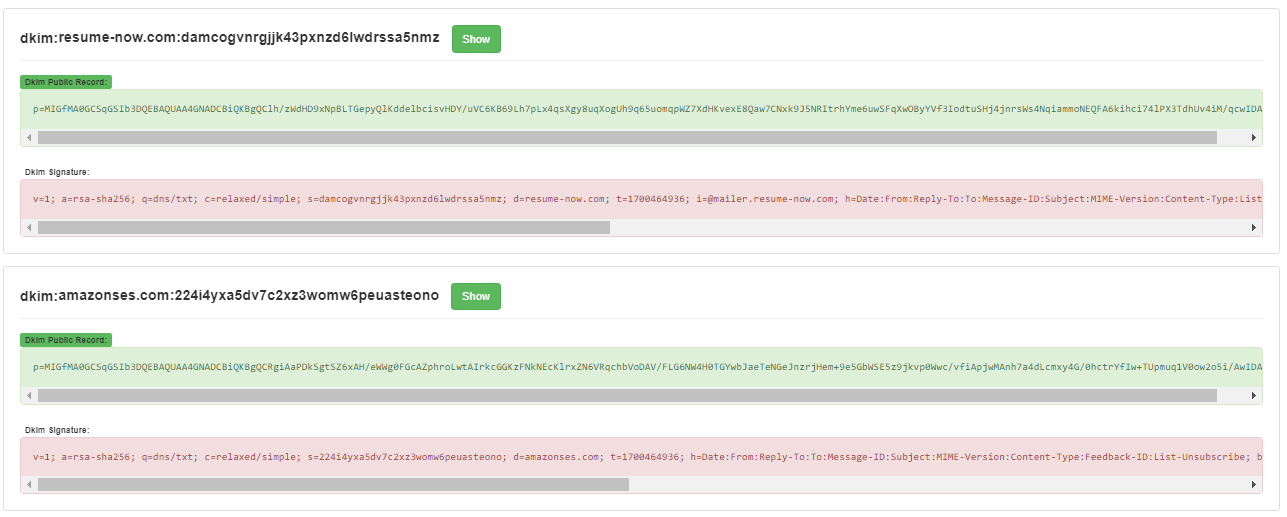
Open mx analyzer



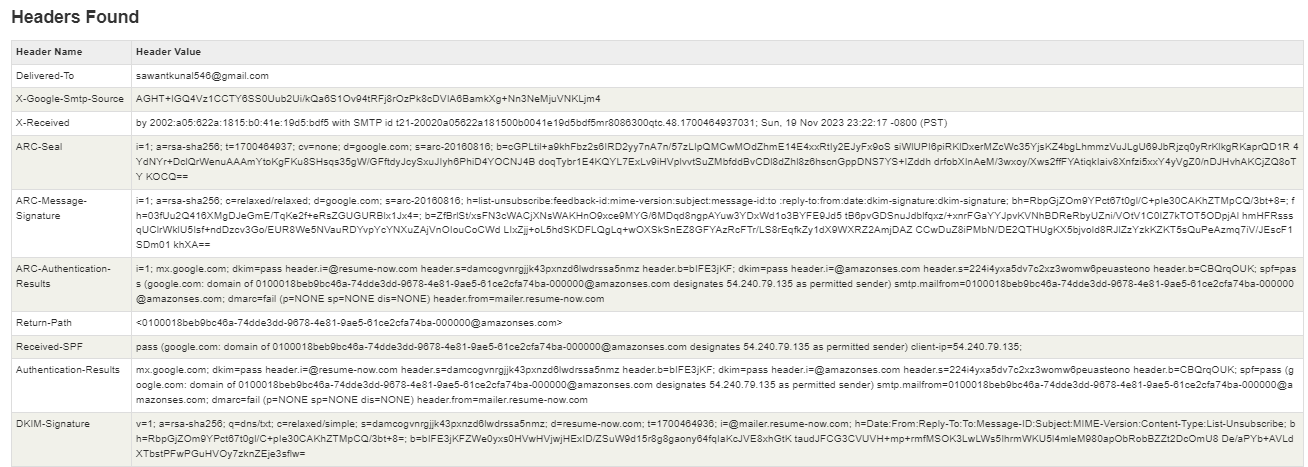








Headers found



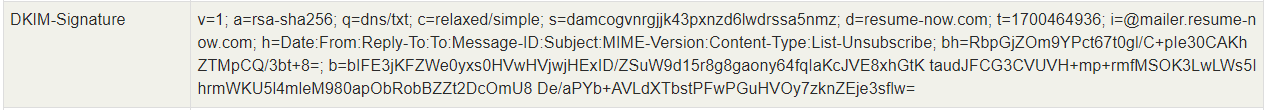
MIME- Version



Message ID



DKIM -Signature



Return path



