**What do we get when a mail arrives on server?**

Step #1: After composing a message and hitting send, your email client – whether it’s Outlook Express or Gmail – connects to your domain’s SMTP server. This server can be named many things; a standard example would be smtp.example.com.

Step #2: Your email client communicates with the SMTP server, giving it your email address, the recipient’s email address, the message body and any attachments.

Step #3: The SMTP server processes the recipient’s email address – especially its domain. If the domain name is the same as the sender’s, the message is routed directly over to the domain’s POP3 or IMAP server – no routing between servers is needed. If the domain is different, though, the SMTP server will have to communicate with the other domain’s server.

Step #4: In order to find the recipient’s server, the sender’s SMTP server has to communicate with the DNS, or Domain Name Server. The DNS takes the recipient’s email domain name and translates it into an IP address. The sender’s SMTP server cannot route an email properly with a domain name alone; an IP address is a unique number that is assigned to every computer that is connected to the Internet. By knowing this information, an outgoing mail server can perform its work more efficiently.

Step #5: Now that the SMTP server has the recipient’s IP address, it can connect to its SMTP server. This isn’t usually done directly, though; instead, the message is routed along a series of unrelated SMTP servers until it arrives at its destination.

Step #6: The recipient’s SMTP server scans the incoming message. If it recognizes the domain and the user name, it forwards the message along to the domain’s POP3 or IMAP server. From there, it is placed in a sendmail queue until the recipient’s email client allows it to be downloaded. At that point, the message can be read by the recipient.

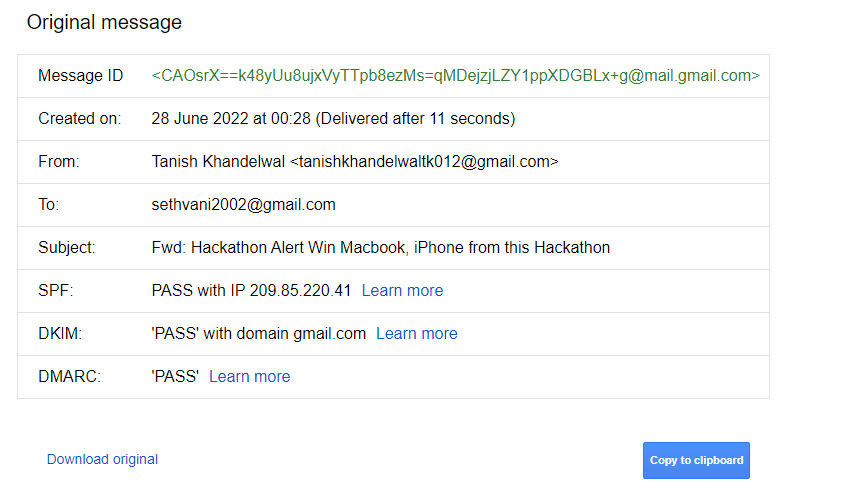
**When an email arrives at the inbox is it still on the server?**

Think of your email inbox as a digital version of your actual postal mailbox. The mail has to sit somewhere before it gets delivered to you. The server that stores this mail and then sends it to your inbox is called an incoming mail server. It may also be referred to as a POP, POP3, or IMAP server

**What useful features does the email carry with it – FEATURE ENGINEERING**

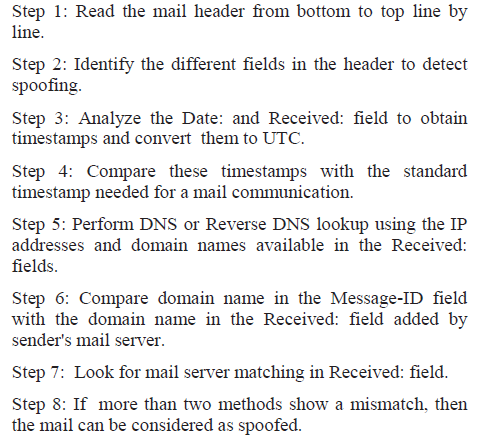
1. **How to read email headers?**

Open the email 🡪 next to reply button, click on more 🡪 show original



1. **Various features that an email brings with it - TBD**

**How to detect spoofed mails using date and time**

****

Reference: Detection of spoofed mail (Research Paper)

**Our approach: what all stages email passes through when it arrives at the server.**

1. SPF, DKIM, DMARC checkers – Header info (anomaly pdf)
2. IP address validity checker
3. Blacklist words in the subject line and body

(https://www.kaggle.com/code/rtatman/get-body-text-of-e-mails)

(<https://www.kaggle.com/datasets/rtatman/fraudulent-email-corpus>)

1. Date and time to check the spoofed email
2. Database and logs of the email at the server.

STEPS:

Connect the server to an email 🡪 setup an attack on the email 🡪 email arrives on the server 🡪 retrieve the info that email carries 🡪 check for SPF, DKIM, DMARC 🡪 IP checker 🡪 Subject and body check for content relevance (i.e is the content provided in the body of the email matches with the subject with which the email came)

IMP:

Our system is prepared in such a way that it blocks the spoofed email. We also want that after a certain interval of time the set of the discarded emails is being checked. The discarded emails will be checked regularly for upcoming improvements by spoofers to bypass current system and system will be updated accordingly to prevent such measures.