In this article, I will discuss

the basic scheme of sending an email.

The basic scheme of sending an email using STMP protocol is illustrated as following figure.

Diagram

Description automatically generated

Sender uses SMTP protocol sends message from MUA to MSA in sender’s email server.

The message was sent to MTA from MSA using SMTP protocol.

The message was sent to MTA in receiver’s email server from MTA in sender’s email server.

The message was sent to MDA from MTA.

The message was sent to message store.

Then the receiver can use POP3 or IMAP to receive message.

Term:

(2.1)MUA

MUA=Mail User Agent

MUA allows us to edit, browse etc emails before sending.

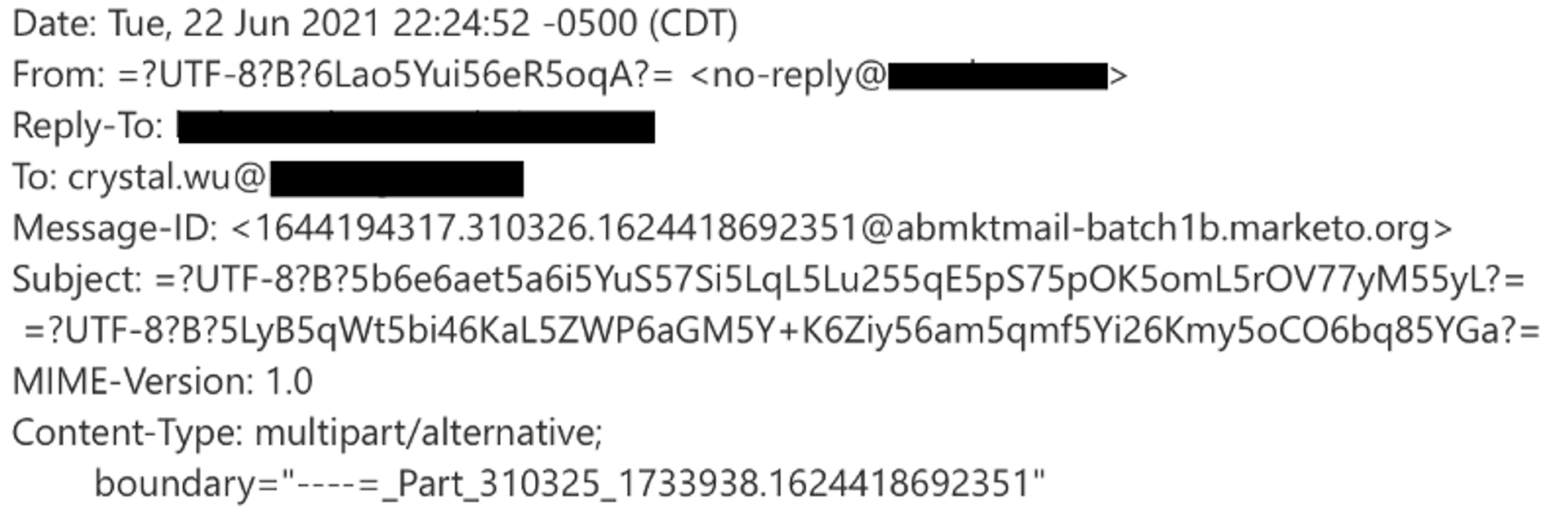
At startup of sending message from sender.

MUA will insert necessary headers at front of body.

(including header.From, header.To, header.Reply-To, header.BCC , header.CC )

If you open the email after email sent successfully, you will see the header of the email.

The figure illustrates a part of the header of the email.



(2.2)MSA

MSA=Mail Submission Agent

It checks and verifies the message sent from MTA.

It verifies the format of message is vaild, or invalid and the header is missing or not.

(2.3)MTA

MTA=Mail Transfer Agent

It is sometimes called mail relay, mail exchanger ,and MX host.

It routines the messages.

It uses DNS to find out the IP which corresponds to MX.

It sends the message to receiver’s email server using

(2.4)MDA:

MDA=Mail Delivery Agent

LDA=Local Delivery Agent

MDA is called LDA.

First, MDA inserts a SMTP trace and assigns the attribute the return-path as the value of the attribute smtp.MailFrom .

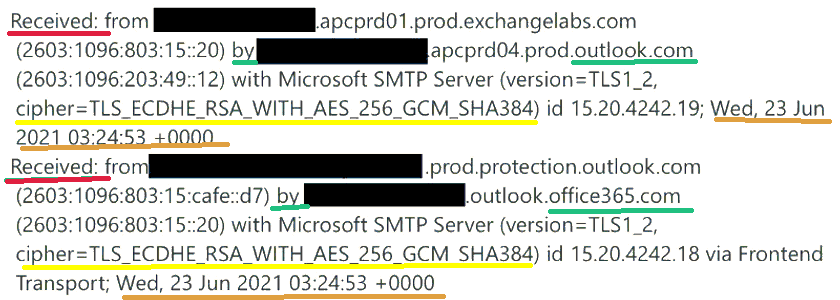
After that, it will classify all messages in receiver’s email server according its attribute smtp.RcptTo, then it puts each one’s message store.

(2.5)MS:

MS=message store

Where you can place message sent from the other’s.

The figure gives you some information about the email.



The red underline illustrates the receiver’s information (including what product it is used).

The green underline illustrates the sender’s information (including what product it is used).

The yellow underline illustrates the ciphertext when sending message.

The orange underline illustrate the date and time the message was sent.

[ref]

https://tech-blog.cymetrics.io/posts/crystal/email-sec-theory/