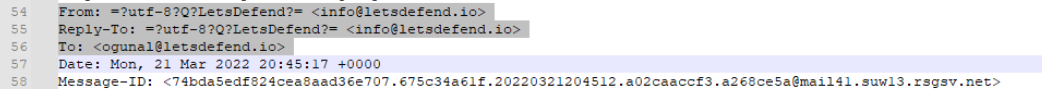
In this lab, I will be analysing a suspicious email.

Accessing the Email header:

Starting, I download the message and open it in a notebook application (notepad2).



Analysing the email header

If I reply to this email, will it return to the original sender? Not always, if the From and Return-path/Reply-to values are different any reply will be sent to a different email address. In this email example, the emails are different and could raise a red flag needing further investigation as most legitimate businesses try to keep reply-to and from fields the same. This email was sent from [mrs.dara@jcom.home.ne.jp](mailto:mrs.dara@jcom.home.ne.jp) and if I reply to the email it will instead go to mrs.dara@daum.net.



Using the received SPF field I found what the ip address the email was sent from, while it did pass the Sender Policy Framework verifying that it came from a legitimate sender, that doesn’t prove it’s safe only that it's authorised by the domain SPF record. In this case, it was authorized by google mail servers.

