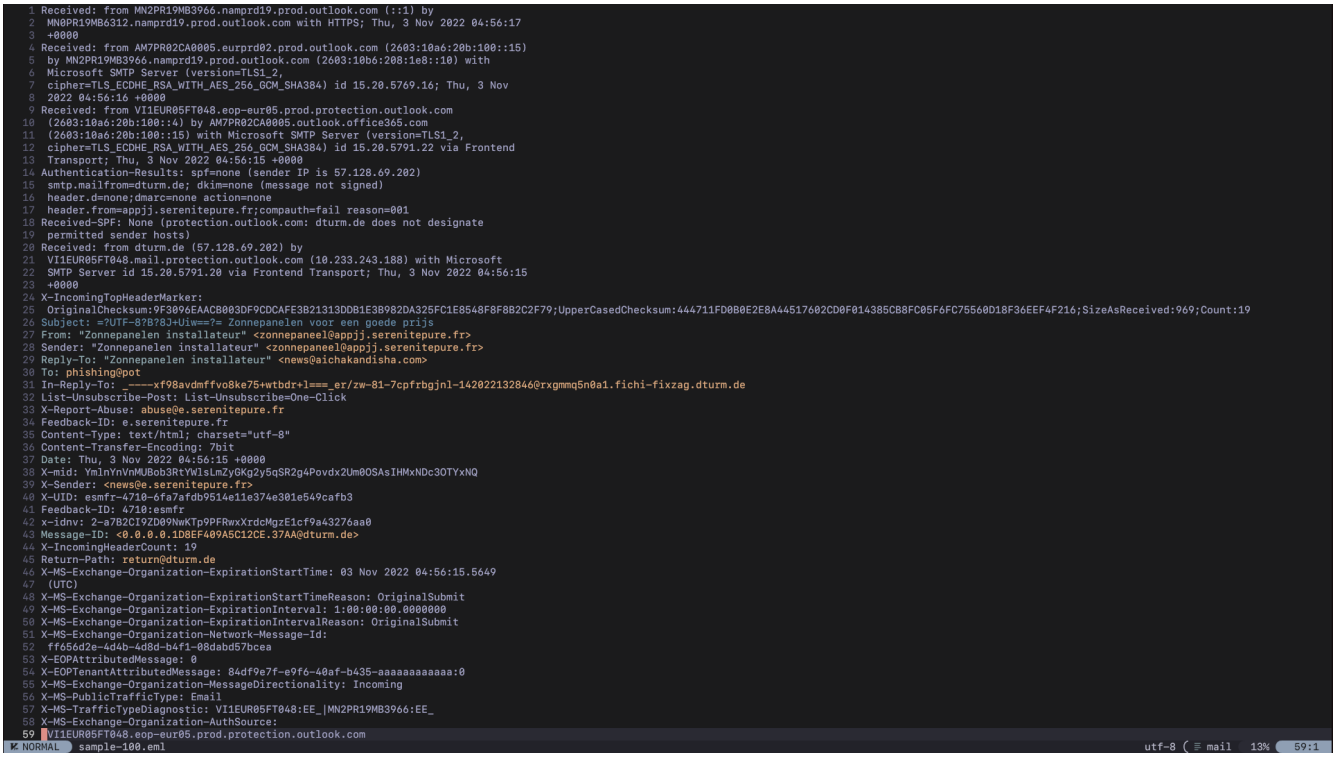
Task - 2

Identifying phishing mails

Step 1: Download an email from your mail vendor, preferrably in .eml format, for analysing the headers in the mail.

Step 2: Read through the contents, and understand what the mail is about, so that you get an idea whether the content is actually credible.



Here is what I analysed from this eml file (Refer to the attached .eml file for a better reference):

- Inconsistent use of emails through out the mail, the sender and the reply to mail is not the same.
- No authentication protocols is enformed, (SPF,DKIM,DMARC,compauth) all of them failed, and the email vendor has flagged this, and put them into it’s spam folder.
- The sender IP is not associated with the organisation name specified but is associated with a RIPE Network Coordination.
- The url is just http instead of a https, organisations are very much insisted to use HTTPS on hosting their websites. The domain name is nowhere near to the sender.

- And the dutch used in this file, when translated, gives us a content which grabs the reader's attention using emotions, but uses incorrect language grammer, including the incorrect spellings.

Go through the given analysis, this will give us a clear red flag on why this email is not to be trusted and the link given has so many redirections.

- Hareekshith AS