Introduction

A user with the email address sandino347@proton.me has received an email from an unknown sender info@cssexam.ch. The origin and technical background of this email should now be investigated.

Download the ZIP file from the resource section and check its integrity by calculating and comparing the MD5 checksum.

```
MD5 (c7-email.zip) = 8d6caa6ced0d8ec791be01d2f03fd57c
```

Extract the EML file from the ZIP file. Hint: EML files are emails as readable text files that contain all meta information in addition to the content. Goal and tasks

Investigate and analyze the given email by completing the following 4 tasks. Record your results and findings in a written report.

Task 1

Sketch a simple flow chart diagram showing all MTAs that have transferred the email from source to destination. Extract information solely from the given email. Label all MTAs with the FQDN and the IP (if retrievable) and connect them with arrows, indicating the protocol used.

Task 2

Obviously, the email was originally addressed to bkchagent@quickline.ch. Explain the reason why the email has arrived in the mailbox of sandino347@proton.me and provide a technical justification for your statement.

Task 3

Obviously, emails of the domain cssexam.ch are sent from an MTA outside of Switzerland. Investigate the reasons by gathering additional information, report the technical background and provide evidence for your findings.

Task 4

Analyze the aspect of encryption in the given email communication and formulate a brief assessment including justification for each of the following 3 aspects

- End-to-end encryption between sender and receiver
- Encryption at transit between the MTAs and along the entire route
- Encryption at rest on each of the MTAs along the entire route

Submission

Submit a written report as PDF document, containing your results and findings as well as all details on how you retrieved the information.