Exercise 3

Step 1

Write a Python3 script able to connect to an **https** website. The script has to print on `stdout` the `data` field received as `response` by the server.

Hint: use the `http.client` Python3 module

Analyze the data exchanged between your python3 client and the webserver using Wireshark. Which protocols are visible on Wireshark?

Step 2

Write a Python3 TLS socket client able to connect to a TLS encrypted website. The script should be able to:

1. Connect to the specified website
2. Verify its certificate
3. Print some debug information such as:
    a. Type of the secure socket created
    b. Min and max supported TLS version
    c. Other SSL/TLS options enabled for the connection
    d. Current protocol
    e. Verify flags for certificates
    f. Verification mode

Hint: you can use the following Python3 modules

- `socket`
- `ssl`
- `certifi`

Step 3

Write a Python3 TLS socket server and socket client able to use TLS certificates for secure connections. Use the certificate you obtained from Letsencrypt in order to establish a secured communication.

N.B.: You have to study how these modules work by yourself!