Lab 7 report

In this lab we created the https server (https://localhost:8443) and connected to it through the Google Chrome browser.
During this lab we created root certificate (Certification authority) and root CA key.
Then, based on root certificate(which we've added to keychain) we created domain key and sertificate. We put the configs into files server.csr.cnf (for request) and v3.ext.
We used SHA256 for hashing, RSA2048, TLS 1.3
Commands that we've used for creating certificates:

createdn root key

```
openssl genrsa -des3 -out rootCA.key 2048
```

created root cert

```
openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out
rootCA.pem
```

created domain key and request

```
openssl req -new -sha256 -nodes -out server.csr -newkey rsa:2048
-keyout server.key -config <( cat server.csr.cnf )
```

*server.csr.cnf is a config file stored in repo

created domain cert

```
openssl x509 -req -in server.csr -CA rootCA.pem -CAkey rootCA.key
-CAcreateserial -out server.crt -days 500 -sha256 -extfile v3.ext
```

*v3.ext is a config file stored in repo