Install Apache on windows with https

A. Install Apache for Windows
B. Configure Apache server
C. Configure https
D. Copy certificate

Install Apache for Windows

1. Go on download apache for windows and install the version that match with your OS architecture.
2. Unzip downloaded archive into custom folder
3. Rename apache folder into "Apache"

Configure Apache Server

1. Go on conf folder, and open file httpd.conf
   a. Modify "Define SVROOT" value with your apache path
   b. Modify "ServerAdmin" value with the email used for certificate generation
   c. Modify "ServerName" value with domain used for certificate generation
   d. Delete <Directory> </Directory> and all contents inside this parenthesis
   e. Remove # in front at "Include conf/extra/httpd-vhosts.conf" to allow using of virtual hosts
2. Create a folder with your "domain name" as name
   a. Create a simple index.html file
3. Create configuration of virtual host for our website
   a. Go on 'apache/conf/extras' and edit httpd-vhosts.conf file
   b. Add following configuration modified with your data

```
<VirtualHost _default_:80>
    DocumentRoot "${SRVROOT}/networksecuritydemacs"
    serverName networksecuritydemacs.tk
    <Directory "${SRVROOT}/networksecuritydemacs">
        AllowOverride None
        Options FollowSymLinks
        Require all granted
    </Directory>
</VirtualHost>
```

   c. Adapt "DocumentRoot" value replacing "networksecuritydemacs" with the name of folder previously created
   d. Adapt "serverName" value with your domain
   e. Adapt "<Directory" with same value used for DocumentRoot

4. Install apache as server
    a. Go on apache/bin folder
    b. Open shell with WIN+R and write cmd
    c. Execute following command: **httpd.exe -k install**
5. Restart apache service
    a. We can use following command: **httpd.exe -k restart**
    b. Or using ApacheServerMonitor GUI
6. Once apache service is running, we can test it opening a browser and going on http://127.0.0.1/
7. Edit File Hosts
    a. Open file "C:\Windows\System32\drivers\etc\hosts" with admin privileges
    b. Insert a line "127.0.0.1 <<YOUR_DOMAIN.TLD>>"
    c. Insert a line "127.0.0.1 www.<<YOUR_DOMAIN.TLD>>"
8. Test resolved name opening a browser and going on <<YOUR_DOMAIN.TLD>> and see if everything works.

Configure HTTPS

1. Configure Apache
    a. Open a terminal
    b. Go on "Apache\bin" in your terminal
    c. Set two environment variables useful for configuration

    Set OPENSS_CONF = <<YOUR_PATH_TO_APACHE_FOLDER>>\conf\openssl.cnf

    Set RANDFILE = <<YOUR_PATH_TO_APACHE_FOLDER>>\bin\.rnd

    d. Edit httpd.conf file and remove # in front at the following lines:
        i. Include conf/extra/httpd-ssl.conf
        ii. LoadModule ssl_module modules/mod_ssl.so
        iii. LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
2. Configure virtual host for ssl
    a. Go on "Apache\conf\extra"
    b. Edit httpd-ssl.conf
    c. Change the following field with your configuration
        i. DocumentRoot ---> with same folder used into http virtualhost configuration
        ii. ServerName   --->   <<yourdomain.tld>>
        iii. ServerAlias   --->   [www.<<yourdomain.tld](www.%3C%3Cyourdomain.tld)>>
        iv. SSLCertificateFile   ---> "${SRVROOT}/letsencrypt_certs/cert.pem"
        v. SSLCertificateKeyFile   ---> "${SRVROOT}/letsencrypt_certs/privkey.pem"
        vi. SSLCertificateChainFile ---> "${SRVROOT}/letsencrypt_certs/fullchain.pem"
    d. Add following <directory> to grant all privileges to the files

```
<Directory "${SRVROOT}/networksecuritydemacs">
  Require all granted
</Directory>
```
        i.
        ii. Replace networksecuritydemacs with name of your folder previously created

Copy Certificate

1. Open a bash
2. Obtain administrator privileges
3. Go on "/etc/letsencrypt/live/<<yourdomain>>" folder
4. Copy all certificates files into /apache/letsencrypt_certs
   a. cp *.pem /<path_to_your_apache_folder>/letsencrypt_certs
5. reload apache
6. go on https://<<your_domain.tld>>/ and see if it works!