

Network and System Security ET2595

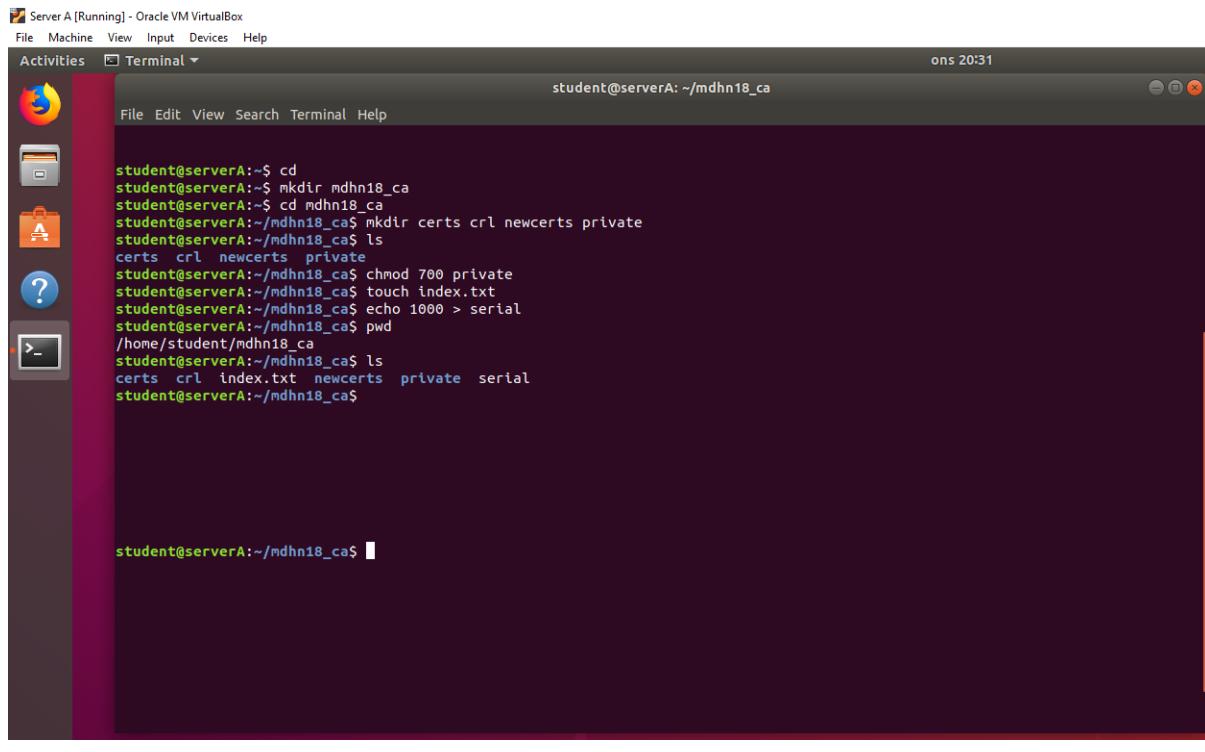
Lab 2 Report

Name: Md Rabiul Ahamed Bin Hanif

P. no. [REDACTED]

Email: mdhn18@student.bth.se

Environments create:



```
student@serverA:~$ cd
student@serverA:~$ mkdir mdhn18_ca
student@serverA:~$ cd mdhn18_ca
student@serverA:~/mdhn18_ca$ mkdir certs crl newcerts private
student@serverA:~/mdhn18_ca$ ls
certs crl newcerts private
student@serverA:~/mdhn18_ca$ chmod 700 private
student@serverA:~/mdhn18_ca$ touch index.txt
student@serverA:~/mdhn18_ca$ echo 1000 > serial
student@serverA:~/mdhn18_ca$ pwd
/home/student/mdhn18_ca
student@serverA:~/mdhn18_ca$ ls
certs crl index.txt newcerts private serial
student@serverA:~/mdhn18_ca$
```



```
student@serverA:~$ cp /etc/ssl/openssl.cnf /home/student/mdhn18_ca
student@serverA:~$
```

- openssl.cnf file was changed according to the instruction. All screen short are given below.

```

# We can add new OIDs in here for use by 'ca', 'req' and 'ts'.
# Add a simple OID like this:
# testoid1=1.2.3.4
# or use config file substitution like this:
# testoid2=$(testoid1).5.6

# Policies used by the TSA examples.
tsa_policy1 = 1.2.3.4.1
tsa_policy2 = 1.2.3.4.5.6
tsa_policy3 = 1.2.3.4.5.7

#####
[ ca ]
default_ca = CA_default      # The default ca section

#####
[ CA_default ]

dir      = /home/student/mdhn18_ca    # Where everything is kept
certs   = $dir/certs        # Where the issued certs are kept
crl_dir = $dir/crl          # Where the issued crl are kept
database = $dir/index.txt   # database index file.
unique_subject = no          # Set to 'no' to allow creation of
                             # several certs with same subject.
new_certs_dir = $dir/newcerts # default place for new certs.

certificate = $dir/certs/root.cert.pem # The CA certificate
serial    = $dir/serial        # The current serial number
crlnumber = $dir/crlnumber    # the current crl number
crl      = $dir/crl.pem       # The current CRL
private_key = $dir/private/root.key.pem # The private key
RANDFILE  = $dir/private/.rand # private random number file

# x509_extensions = usr_cert      # The extensions to add to the cert

# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt = ca_default         # Subject Name options
cert_opt = ca_default          # Certificate field options

# Extension copying options: use with caution.
# copy_extensions = copy

```

Task 1: [v3_ca]

```

[ v3_ca ]

# Extensions for a typical CA

# PKIX recommendation.

subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer
basicConstraints = critical,CA:true

# Key usage: this is typical for a CA certificate. However since it will
# prevent it being used as an test self-signed certificate it is best
# left out by default.
keyUsage = critical, digitalSignature, cRLSign, keyCertSign

# Some might want this also
# nsCertType = sslCA, emailCA

# Include email address in subject alt name: another PKIX recommendation
# subjectAltName=DNS:$copy
# Copy issuer details
# issuerAltName=$copy

```

subjectKeyIdentifier = hash

Identifies certificates which contain a specific public key.

authorityKeyIdentifier = keyid:always,issuer

Identifies the public key corresponding to the private key which was used to sign a certificate. For the **keyid** option, if it is present an attempt is made to copy the subject key identifier from the parent certificate.

For the **issuer** option, it copies the issuer and serial number from the issuer certificate. This is applicable when the **keyid** option fails or is not included unless the "always" flag will always include the value.

basicConstraints = CA:true

This is a multi valued extension which indicates whether a certificate is a CA certificate. The first (mandatory) name is CA followed by TRUE or FALSE. If CA is TRUE then an optional "pathlen" is used followed by an non-negative integer value can be included.

`keyUsage = critical, digitalSignature, cRLSign, keyCertSign`

Key usage is a multi valued extension consisting of a list of names of the permitted key usages. The digitalSignature bit is used when the subject public key is used for verifying digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), such as those used in an entity authentication service, a data origin authentication service, and/or an integrity service.

The cRLSign bit is used when the subject public key is used for verifying signatures on certificate revocation lists (for example, CRLs, delta CRLs, or ARLs).

The keyCertSign bit is used when the subject public key is used for verifying signatures on public key certificates.

Task 2: [[v3_intermediate_ca]]

```
[ v3_intermediate_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true, pathlen:0
keyUsage = critical, digitalSignature, cRLSign, keyCertSign
```

`subjectKeyIdentifier=hash`

Identifies certificates which contain a specific public key.

`authorityKeyIdentifier = keyid:always,issuer`

Identifies the public key corresponding to the private key which was used to sign a certificate.

For the **keyid** option, if it is present an attempt is made to copy the subject key identifier from the parent certificate.

For the **issuer** option, it copies the issuer and serial number from the issuer certificate. This is applicable when the keyid option fails or is not included unless the "always" flag will always include the value.

`basicConstraints = critical, CA:true, pathlen:0`

Indicates whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.

If CA is TRUE then an optional pathlen name followed by an non-negative integer value can be included.

The pathlen parameter indicates the maximum number of CAs that can appear below this one in a chain. So, a CA with a pathlen of zero can only be used to sign end user certificates and not further CAs.

`keyUsage = critical, digitalSignature, cRLSign, keyCertSign`

Key usage is a multi valued extension consisting of a list of names of the permitted key usages. The digitalSignature bit is used when the subject public key is used for verifying digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), such as those used in an entity authentication service, a data origin authentication service, and/or an integrity service.

The cRLSign bit is used when the subject public key is used for verifying signatures on certificate revocation lists (for example, CRLs, delta CRLs, or ARLs).

The keyCertSign bit is used when the subject public key is used for verifying signatures on public key certificates.

Difference between [v3_ca] and [v3_intermediate_ca] is the values of basicConstraints. The values are **CA:true** and **critical, CA:true, pathlen:0** respectively.

Task 3: [usr_cert]

```
[ usr_cert ]
?
# These extensions are added when 'ca' signs a request.

# This goes against PKIX guidelines but some CAs do it and some software
# requires this to avoid interpreting an end user certificate as a CA.

basicConstraints=CA:FALSE

# Here are some examples of the usage of nsCertType. If it is omitted
# the certificate can be used for anything *except* object signing.

# This is OK for an SSL server.
# nsCertType          = server

# For an object signing certificate this would be used.
# nsCertType = objsign

# For normal client use this is typical
# nsCertType = client, email

# and for everything including object signing:
# nsCertType = client, email, objsign

# This is typical in keyUsage for a client certificate.
keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = clientAuth, emailProtection

# This will be displayed in Netscape's comment listbox.
nsComment          = "OpenSSL Generated Certificate"

# PKIX recommendations harmless if included in all certificates.
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer
```

subjectKeyIdentifier=hash

Identifies certificates which contain a specific public key.

authorityKeyIdentifier = keyid,issuer

Identifies the public key corresponding to the private key which was used to sign a certificate. For the **keyid** option, if it is present an attempt is made to copy the subject key identifier from the parent certificate.

For the **issuer** option, it copies the issuer and serial number from the issuer certificate. This will only be done if the keyid option fails or is not included unless the "always" flag will always include the value.

basicConstraints=CA:FALSE

An end user certificate must either set CA to FALSE or exclude the extension entirely. Some software may require the inclusion of basic Constraints with CA to be set to FALSE for end entity certificates.

nsComment = "OpenSSL Generated Certificate"

This message will be displayed in Netscape's comment listbox.

keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment

The **nonRepudiation** bit is used when the subject public key is used to verify digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), used to provide a non-repudiation service that protects against the signing entity falsely denying some action.

The **digitalSignature** bit is used when the subject public key is used for verifying digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), such as those used in an entity authentication service, a data origin authentication service, and/or an integrity service.

The **keyEncipherment** bit is used when the subject public key is used for enciphering private or secret keys, i.e., for key transport.

extendedKeyUsage = clientAuth, emailProtection

This extension consists of a list of usages indicating purposes of which the certificate public key could be used for.

The value **clientAuth** represents SSL/TLS Web Client Authentication.

The value **emailProtection** represents E-mail Protection (S/MIME).

Task 4: [server_cert]

```
[ server_cert ]
basicConstraints = CA:FALSE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer:always
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth
```

basicConstraints=CA:FALSE

An end user certificate must either set CA to FALSE or exclude the extension entirely. Some software may require the inclusion of basic Constraints with CA to be set to FALSE for end entity certificates.

subjectKeyIdentifier=hash

Identifies certificates which contain a specific public key.

authorityKeyIdentifier = keyid,issuer:always

Identifies the public key corresponding to the private key which was used to sign a certificate. For the **keyid** option, if it is present an attempt is made to copy the subject key identifier from the parent certificate.

For the issuer option, it copies the issuer and serial number from the issuer certificate. This will only be done if the keyid option fails or is not included unless the "always" flag will always include the value.

keyUsage = critical, digitalSignature, keyEncipherment

The digitalSignature bit is used when the subject public key is used for verifying digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), such as those used in an entity authentication service, a data origin authentication service, and/or an integrity service. The keyEncipherment bit is asserted when the subject public key is used for enciphering private or secret keys, i.e., for key transport.

extendedKeyUsage = serverAuth

This extension consists of a list of usages indicating purposes of which the certificate public key could be used for.

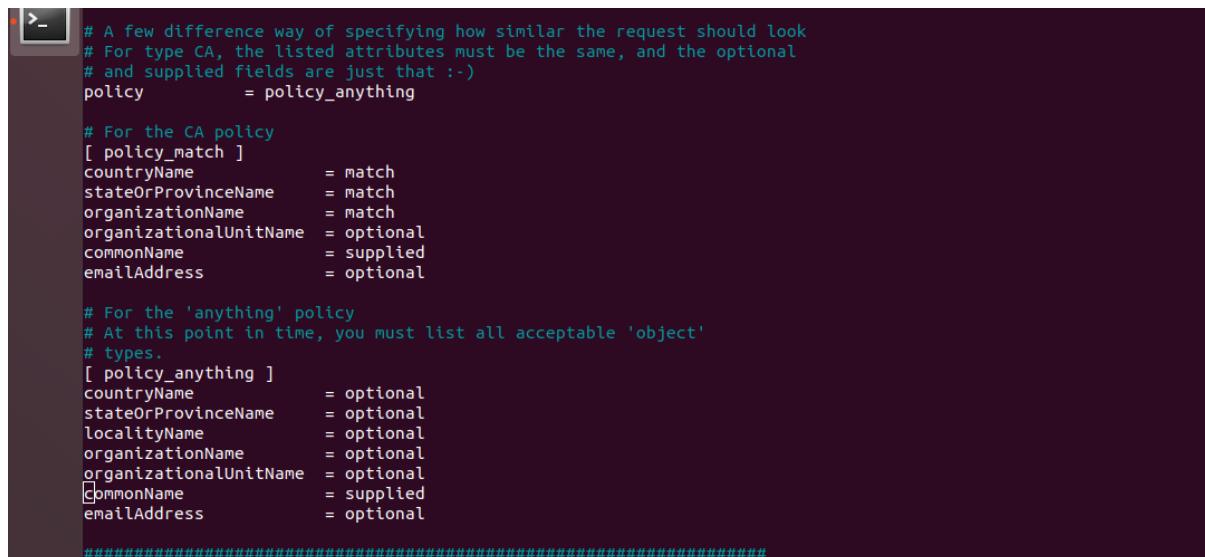
The value **serverAuth** represents SSL/TLS Web Server Authentication

Task 5: Policies

- Before checking the policy, I create ca1 directory which is shown I below screen short.



```
student@serverA:~/mdhn18_ca$ mkdir ca1
student@serverA:~/mdhn18_ca$ cd ca1
student@serverA:~/mdhn18_ca/ca1$ ls
certs crl newcerts private csr
student@serverA:~/mdhn18_ca/ca1$ ls
certs crl csr newcerts private
student@serverA:~/mdhn18_ca/ca1$ chmod 700 private
student@serverA:~/mdhn18_ca/ca1$ touch index.txt echo 2000 > serial
student@serverA:~/mdhn18_ca/ca1$ echo 2000 > crlnumber
student@serverA:~/mdhn18_ca/ca1$ cp ./openssl.cnf .
student@serverA:~/mdhn18_ca/ca1$
```



```
# A few difference way of specifying how similar the request should look
# For type CA, the listed attributes must be the same, and the optional
# and supplied fields are just that :-)
policy      = policyAnything

# For the CA policy
[policyMatch]
countryName      = match
stateOrProvinceName = match
organizationName   = match
organizationalUnitName = optional
commonName        = supplied
emailAddress       = optional

# For the 'anything' policy
# At this point in time, you must list all acceptable 'object'
# types.
[policyAnything]
countryName      = optional
stateOrProvinceName = optional
localityName     = optional
organizationName   = optional
organizationalUnitName = optional
commonName        = supplied
emailAddress       = optional
```

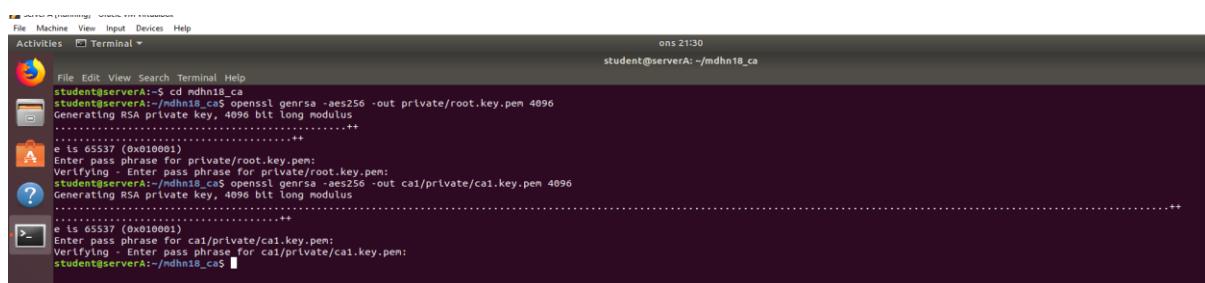
If the value of an attribute is "match", then it should be matched with the CA's DN. All fields listed as "supplied" must be present. If a field is listed as "optional", then it is allowed and not even required to be there.

In **policy_match** section, the values of countryName, stateOrProvinceName, organizationName must be present as the CA for all certificates it signs and commonName will be supplied by the issuer.

In **policy_anything** section, only commonName needs to be supplied and all the other values are optional.

Task 6: Options for the root certificate

- create the private RSA key for *root* and *ca1*, respectively.



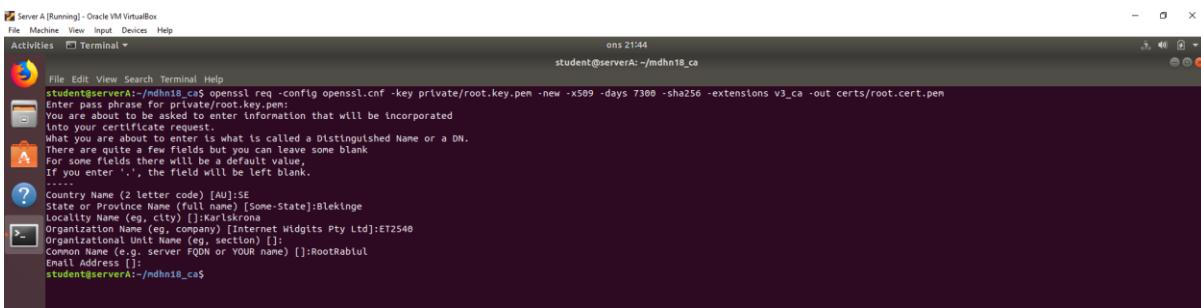
```
student@serverA:~/mdhn18_ca$ cd mdhn18_ca
student@serverA:~/mdhn18_ca$ openssl genrsa -aes256 -out private/root.key.pem 4096
Generating RSA private key, 4096 bit long modulus
.....+
e Ls 65537 (0x010001)
Enter pass phrase for private/root.key.pem:
Verifying - Enter pass phrase for private/root.key.pem:
student@serverA:~/mdhn18_ca$ openssl genrsa -aes256 -out ca1/private/ca1.key.pem 4096
Generating RSA private key, 4096 bit long modulus
.....+
e Ls 65537 (0x010001)
Enter pass phrase for ca1/private/ca1.key.pem:
Verifying - Enter pass phrase for ca1/private/ca1.key.pem:
student@serverA:~/mdhn18_ca$
```

- To obtain the public key (e.g., for root.ca.pem) using OpenSSH you can use the following command.
- For additional protection, the filesystem access rights to private keys should be restricted to the owner.



```
Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal 21:38
student@serverA: ~/mdhn18_ca
student@serverA:~$ cd mdhn18_ca
student@serverA:~/mdhn18_ca$ openssl rsa -in private/root.key.pem -pubout -out root.pub.pem
writing RSA key
student@serverA:~/mdhn18_ca$ chmod 400 private/root.key.pem
student@serverA:~/mdhn18_ca$ chmod 400 ca1.key.pem
student@serverA:~/mdhn18_ca$
```

- To generate the self-signed certificate entering the following command.



```
Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal 21:44
student@serverA: ~/mdhn18_ca
student@serverA:~/mdhn18_ca$ openssl req -config openssl.cnf -key private/root.key.pem -new -x509 -days 7300 -sha256 -extensions v3_ca -out certs/root.cert.pem
Enter pass phrase for private/root.key.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are about to be 6 fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [AU]:SE
State or Province Name (full name) [Some-State]:Blekinge
Locality Name (eg, city) []:Karlskrona
Organization Name (eg, company) [Internet Widgets Pty Ltd]:ET2540
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:RootRabilul
Email Address []:
student@serverA:~/mdhn18_ca$
```

Command

openssl req -config openssl.cnf -key private/root.key.pem -new -x509 -days 7300 -sha256 -extensions v3_ca -out certs/root.cert.pem

Description

-config filename

this allows an alternative configuration file to be specified, this overrides the compile time filename or any specified in the OPENSSL_CONF environment variable.

-key filename

This specifies the file to read the private key from. It also accepts PKCS#8 format private keys for PEM format files.

-new

this option generates a new certificate request. It will prompt the user for the relevant field values. The actual fields prompted for and their maximum and minimum sizes are specified in the configuration file and any requested extensions. If the -key option is not used it will generate a new RSA private key using information specified in the configuration file.

-x509

this option outputs a self signed certificate instead of a certificate request. This is typically used to generate a test certificate or a self signed root CA. The extensions added to the certificate (if any) are specified in the configuration file. Unless specified using the set_serial option, a large random number will be used for the serial number.

-days n

when the -x509 option is being used this specifies the number of days to certify the certificate for. The default is 30 days.

-extensions section

this option specifies alternative sections to include certificate extensions (if the -x509 option is present) or certificate request extensions. This allows several different sections to be used in the same configuration file to specify requests for a variety of purposes.

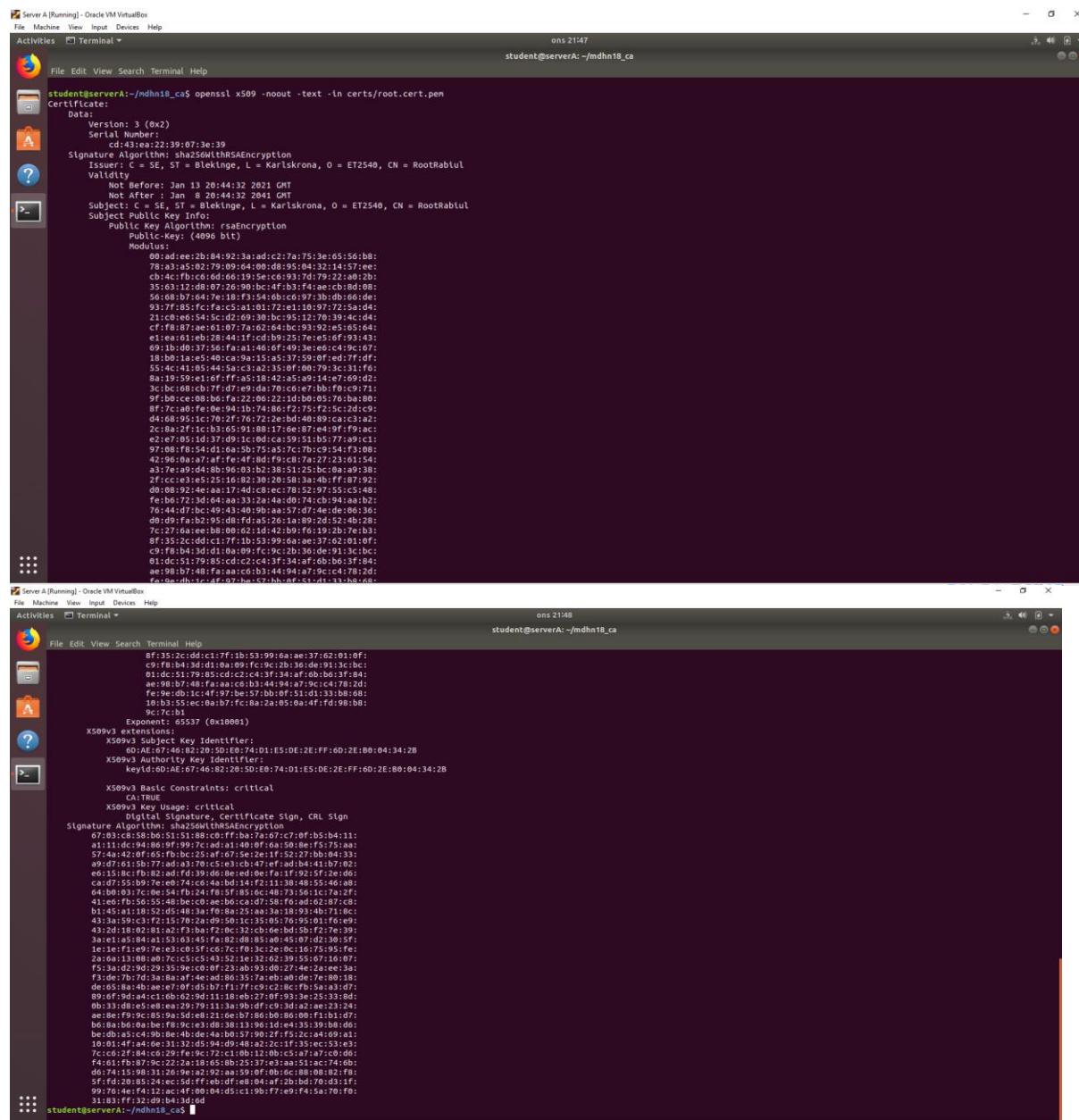
-out filename

This specifies the output filename to write to or standard output by default.

Task 7: Verify the root certificate

Command:

openssl x509 -noout -text -in certs/root.cert.pem



```
student@serverA:~/mdhn18_ca$ openssl x509 -noout -text -in certs/root.cert.pem
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
    cd:43:ee:22:39:07:3e:99
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = RootRabil
Validity:
    Not Before: Jan 13 20:44:32 2021 GMT
    Not After : Jan 8 20:44:32 2041 GMT
Subject: C = SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = RootRabil
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        Public-Key: (4096 bit)
            Modulus:
                00:ad:ee:2b:84:92:3a:ad:c2:7a:75:3e:65:56:b8:
                78:a3:a5:02:79:09:64:00:08:95:04:32:14:57:ee:
                c0:3d:50:1f:3c:4f:b3:f4:aec:cb:8d:08:
                35:63:12:08:07:26:90:bc:4f:b3:f4:aec:cb:8d:08:
                56:06:b7:64:7e:10:f1:51:0b:c0:97:3b:0b:66:de:
                93:7f:85:f5:cfa:c5:a1:01:72:e1:10:97:72:5a:d4:
                21:c0:ed:54:1c:d2:d9:3b:dc:95:12:76:19:4c:d4:
                cf:18:05:1c:37:2d:03:4b:4a:30:94:01:4b:4a:54:
                e1:k8:61:6b:28:44:1f:cd:b9:25:7e:ee:f9:93:43:
                69:1b:d0:37:56:fa:1a:0d:0f:49:3e:ee:c4:9c:07:
                18:b6:1a:e5:40:ca:9a:11:5a:37:59:0f:fe:d7:df:
                55:4c:41:05:44:5a:c1:a1:23:0f:00:79:c1:31:f6:
                5d:41:1c:05:41:1a:11:11:11:11:11:11:11:11:11:
                3c:bc:0d:cb:7f:1d:0e:da:70:c6:67:bb:0d:c9:73:
                9f:bc:ce:08:bb:6b:fa:22:d6:22:1d:b6:b0:05:76:ba:80:
                8f:7c:a0:fe:fe:0e:94:1b:74:86:f2:75:f2:c1:2d:c9:
                d4:16:95:1c:70:2f:76:72:2e:bd:40:89:ca:c3:a2:
                2c:18:a2:2f:c1:0c:91:18:01:0e:0e:0e:0e:0f:0f:0f:0c:
                5c:15:01:37:09:09:09:09:09:09:09:09:09:09:09:09:
                57:08:ff:54:d1:6a:5b:75:a5:7c:7b:c9:54:f3:08:
                42:96:0a:aa:7a:fe:fe:f7:8d:79:c8:7a:27:23:01:54:
                a3:7e:a9:d4:8b:96:03:bd:23:38:51:25:bc:0a:9:38:
                2f:cc:ce:0e:53:16:82:00:20:58:01:4b:0f:f7:92:
                0d:09:0a:0e:0e:0e:0e:0e:0e:0e:0e:0e:0e:0e:0e:0e:
                fe:9e:72:3d:64:aa:31:7a:4a:00:74:cb:94:aa:b2:
                76:44:0d:7b:c4:99:43:40:99:aa:57:d7:4e:de:06:36:
                d0:d9:fa:b2:95:d8:fd:a5:26:1a:89:24:52:4b:28:
                7c:27:0a:ee:bb:00:02:id:42:b9:fo:19:1b:7e:b3:
                8f:7f:02:2e:00:00:00:00:00:00:00:00:00:00:00:00:
                c9:f8:54:1d:01:0a:00:ff:c1:9c:2b:36:0d:9e:93:cbc:
                01:dc:51:79:85:cd:c2:c4:3f:34:af:0b:0b:63:3f:84:
                ae:9b:7b:74:0b:aa:cc:0b:14:94:07:9c:c4:78:2d:
                fa:0e:dh:1c:4e:0f:07:ba:57:bb:ef:51:41:33:0b:68:
                student@serverA:~/mdhn18_ca$ 
```

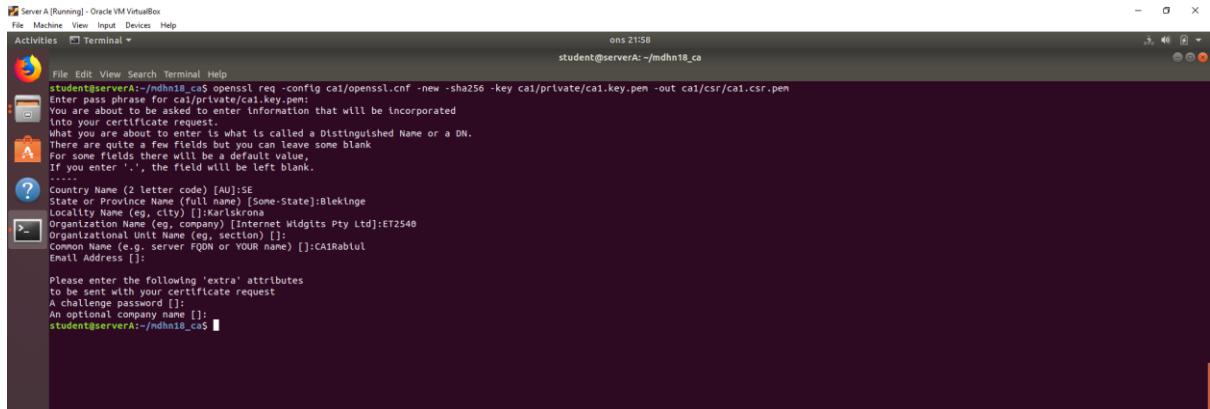


```
student@serverA:~/mdhn18_ca$ openssl x509 -noout -text -in certs/root.cert.pem
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
    8f:35:2c:dd:c1:57:f5:1b:53:99:6a:ee:37:62:01:b7:
    61:3d:51:79:85:cd:c2:c4:3f:34:a1:79:c1:c4:78:2d:
    ae:9b:7b:48:fa:a1:a6:c6:b3:44:94:a7:9c:c1:7b:2d:
    fe:9e:db:1c:4f:f7:97:be:57:bb:0f:51:d0:33:bb:68:
    01:dc:51:79:85:cd:c2:c4:3f:34:af:0b:0b:63:3f:84:
    9c:7c:cb: Exponent: 65537 (0x10000)
X509v3 extensions:
    X509v3 Key Identifier:
        60:A6:d7:46:82:20:50:E0:74:01:E5:DE:2E:FF:6D:2E:B0:04:34:28
    X509v3 Authority Key Identifier:
        keyid:60:A6:d7:46:82:20:50:E0:74:01:E5:DE:2E:FF:6D:2E:B0:04:34:28
    X509v3 Basic Constraints: critical
        CA:TRUE
    X509v3 Key Usage: critical
        digitalSignature, certificateSign, cRLSign
Signature Algorithm: sha256WithRSAEncryption
67:03:08:5b:6b:51:51:88:c0:ff:ba:7a:67:c7:0f:b5:bd:11:
a1:11:1d:c9:94:86:9f:99:7c:ada:14:0f:0a:50:8e:f5:75:8a:
57:42:0e:1c:7a:31:0b:1f:0b:31:0b:0b:0b:0b:0b:0b:0b:0b:
a5:d7:41:5b:77:09:70:c5:ee:c9:bf:ad:41:41:b7:02:
ed:15:8c:fb:82:ad:f3:39:d6:8e:ed:ee:a1:f9:92:5f:2e:66:
ca:d7:55:09:7e:eb:74:0e:4a:bd:14:f2:11:38:48:55:46:08:
60:90:0b:0b:0b:0b:0b:0b:0b:0b:0b:0b:0b:0b:0b:0b:0b:0b:
41:3e:0b:56:55:48:0c:0b:0c:0b:c4:d7:58:76:ad:62:87:2d:
b1:45:a1:10:52:d5:4b:3a:t0:8a:25:a3:a3:10:93:4b:71:bc:
43:3a:59:c3:f2:15:79:2a:d9:50:1c:35:05:76:95:01:f6:ee:9:
43:20:0c:0c:0c:0c:0c:0c:0c:0c:0c:0c:0c:0c:0c:0c:0c:0c:0c:
34:01:45:04:01:53:01:45:78:01:45:0d:0d:0d:0d:0d:0d:0d:0d:
1e:1e:f1:09:7e:c5:c5:f5:c6:7c:f0:3c:2e:0c:16:75:95:fe:
2a:6a:13:08:0a:07:c5:c5:43:52:1e:32:02:39:55:07:16:07:
f5:3a:0d:29:0d:29:35:9e:0c:0f:23:ab:93:0d:27:4e:2a:ee:3a:
f1:0d:0d:0d:0d:0d:0d:0d:0d:0d:0d:0d:0d:0d:0d:0d:0d:0d:
de:65:8a:4b:ae:07:0f:0d:55:07:f1:77:c9:c2:2a:7b:5a:a1:d7:
89:0f:9d:04:c1:0b:02:9d:11:18:eb:27:0f:93:3e:25:33:bd:
0b:33:0b:0c:0e:29:79:13:3a:0d:0f:c0:03:02:01:0a:01:24:
a3:03:0c:0c:05:05:21:33:3a:0d:0f:c0:03:02:01:0a:01:24:
b6:b1:b6:0a:be:f8:9c:ee:3d:03:19:9b:1d:e4:35:39:bd:06:
be:bd:a5:c4:9b:8e:40:de:4a:b6:57:9b:2f:f5:2c:a4:69:a1:
10:01:24:f1:0e:31:32:id:94:09:48:a2:2c:1f:35:ee:c5:3e:3:
7c:0c:0c:0c:0c:0c:0c:0c:0c:0c:0c:0c:0c:0c:0c:0c:0c:0c:
f4:61:f5:87:9c:22:2a:18:05:8b:25:37:e3:a1:a1:51:ac:74:0b:
de:74:15:98:31:26:9e:ea:29:92:aa:59:0f:0b:0c:88:08:02:f8:
5f:f2:20:0c:24:ec:5d:fe:eb:df:eb:04:a1:f2:2b:bd:70:d3:1f:
93:11:f4:0a:0d:0e:00:00:04:ds:c1:9b:f7:e9:f4:a5:70:f0:
31:b1:ff:32:d9:b1:3d:0d: 
```

student@serverA:~/mdhn18_ca\$

Task 8: Verify the CSR

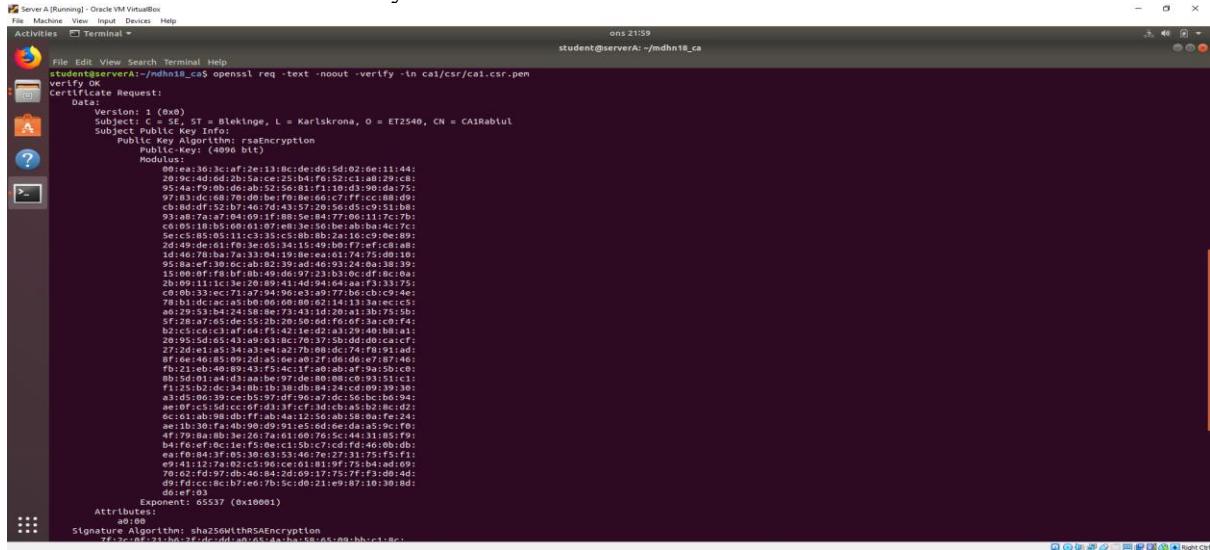
- Following command below to create the CSR



```
student@serverA:/mdhn18_ca$ openssl req -config ca1/openssl.cnf -new -sha256 -key ca1/private/ca1.key.pem -out ca1/csr/ca1.csr.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
if you enter '.', the field will be left blank.
Country Name (2 letter code) [AU]:SE
State or Province Name (full name) [Some-State]:Blekinge
Locality Name (eg, city) [Karlskrona]:Karlskrona
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ET2540
Organization Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:CA1Rabtl
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
student@serverA:/mdhn18_ca$
```

- command below to verify the CSR



```
student@serverA:/mdhn18_ca$ openssl req -text -noout -verify -in ca1/csr/ca1.csr.pem
verify OK
Certificate Request:
Data:
Version: 1 (0x0)
Subject: C = SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = CA1Rabtl
SubjectKeyId: 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
Public Key Algorithm: rsaEncryption
        Public-Key: (4096 bit)
          Modulus:
            00:ea:30:c1:a5:2e:13:8c:de:d6:5d:02:6e:31:44:
            20:9c:4d:dd:2b:5a:ce:25:ba:4f:6:52:c1:a1:29:c8:
            95:48:f9:03:00:ab:52:50:11:00:00:00:00:00:00:00:00:
            cb:8d:df:52:07:46:7d:43:57:20:56:ds:c0:s1:b8:
            93:a8:7a:z7:84:69:1f:88:59:84:77:06:11:7c:7b:
            c0:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
            5e:c5:85:05:11:c3:35:c5:8b:8b:2a:10:c0:ee:89:
            2d:49:der:01:70:3e:05:34:15:49:be:f7:ef:c8:a8:
            15:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
            95:8a:ef:30:0c:ab:82:39:ad:46:93:24:b0:38:39:
            15:00:0f:f8:bf:0b:49:de:97:23:b3:0c:df:f1:c0:0a:
            23:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
            c0:0b:33:ec:c1:71:a7:94:96:e3:a9:77:be:c0:c9:4e:
            78:b1:dc:ae:a5:b0:00:69:00:62:14:13:30:01:c5:
            09:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
            5f:28:a7:05:de:55:2b:29:50:0d:f6:cf:3a:c0:c0:f4:
            b2:c5:c0:c1:c1:a4:f4:2f:42:11:00:00:00:00:00:00:
            20:79:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
            27:2d:e1:a5:54:a3:e4:02:7b:00:dc:74:f0:91:ad:
            ff:6e:46:08:09:2d:a2:6e:a0:2f:dc:de:ef:78:7:46:
            49:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
            b0:5d:01:a4:4d:aa:97:de:80:00:c0:93:51:c1:
            f1:25:b2:dc:34:8b:1b:38:db:84:24:c0:09:39:30:
            31:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
            ae:0f:c1:5d:cc:0f:fd:13:fc:f1:ad:cba:5b:2c:d2:
            6c:61:ab:98:0d:bf:ff:ab:44:12:56:ab:58:00:fe:24:
            4f:79:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
            b4:f6:ef:0c:c1:f5:0e:c1:5b:c7:c0:fd:40:0b:db:
            ea:f0:84:39:05:15:63:53:46:7e:27:31:75:5f:f1:
            09:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
            70:02:fd:97:b4:84:2d:09:17:75:77:f3:d0:4d:
            d9:fd:cc:0b:7e:7b:5c:0d:02:21:e9:87:10:30:8d:
            00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
            Exponent: 65537 (0x10001)
Attributes:
    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
Signature Algorithm: sha256WithRSAEncryption
    7f+7c-0f-23-bc-7f-dc-dd-ab-65-d-a-ba-k8-as-m9-bh-c1-8c-
```

```

Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
File Edit View Search Terminal Help
student@serverA: ~/mdhn18_ca

File Edit View Search Terminal Help
0ns 22:00
student@serverA: ~/mdhn18_ca

8f:6e:46:85:99:2d:a5:6e:a0:2f:d6:d6:7:87:46:
fb:21:eb:40:89:43:f5:4c:1f:a0:ab:a7:9a:5b:c0
Bb:6d:01:a0:3d:aa:be:97:de:80:08:cb:03:51:c1
f1:52:9c:6a:2d:40:94:0d:61:0d:3d:3b:03:39:
a3:d5:06:39:ce:b5:97:df:96:a7:dc:56:bc:b6:94:
ae:0f:c5:5d:c5:0f:d3:3f:c7:d3:cb:a5:b2:8c:d2:
6c:61:ab:98:0d:bf:ab:4a:12:56:ab:58:0a:fe:24:
ae:1b:30:a1:4b:90:d9:1a:55:0e:61:0a:59:c7:f0:
4f:70:01:00:38:1c:09:32:8d:0e:77:13:60:6a:59:11:f7:
b4:f8:ef:8c:1e:f5:0e:c1:5b:c7:75:fd:4d:0b:0b:db:
ea:f0:84:3f:05:30:63:53:46:7e:27:31:75:5f:f1:
e9:41:12:7:a0:02:c5:96:ce:61:81:9f:75:b4:d:69:
70:02:fd:97:0b:46:84:24:09:17:75:7f:f3:00:4d:
70:93:0f:0c:07:e6:7b:5c:0d:0:21:e9:87:10:30:8d:
d1:e7:03:
Exponent: 05537 (0x10001)
Attributes:
a0:00
Signature algorithm: sha256WithRSAEncryption
7f:3c:0f:21:bd:2f:dc:dd:a0:65:4a:ba:58:65:09:bb:c1:8c:
Bb:6d:b7:35:28:a6:ca:8a:18:60:a2:44:11:06:3d:f5:08:c0:
29:5e:da:ff:41:91:70:14:dc:dd:2e:6:48:ad:5a:cf:1d:83:36:
c7:25:3f:ad:25:0e:bf:6c:08:ad:40:7e:2a:05:47:21:30:4c:
32:20:3d:0d:0b:01:00:00:00:00:00:00:00:00:00:00:00:11:
dc:29:1a:67:cf:c7:49:67:f4:22:08:c3:25:bc:09:71:8d:8e:
bf:a9:37:f2:88:78:be:b4:93:0d:0b:bc:be:1b:a4:11:31:24:
64:50:b5:96:d7:ed:6:08:22:28:c7:76:1f:c3:2b:64:ed:8:1:a:f3:
1f:3e:0a:5a:ac:87:02:e0:35:a9:c6:c7:9a:8c:0d:06:b7:b2:
ec:52:20:01:00:00:00:00:00:00:00:00:00:00:00:00:00:50:
49:01:00:00:00:1c:09:32:8d:0e:77:13:60:6a:59:11:f7:
f5:c9:27:5f:88:a9:03:57:ca:0d:ca:4f:9d:76:b3:f3:46:d3:
aa:fc:ca:a0:01:bf:a3:c1:f4:49:0a:3b:d0:12:1b:10:1b:d9:be:
9d:be:d6:cf:04:a3:0b:2:30:46:43:1:7:e4:92:ef:74:58:f4:
1b:09:0f:0c:31:33:0a:00:00:00:00:00:00:00:00:00:00:00:00:
bf:9b:12:1a:04:06:0d:cd:11:00:00:00:00:00:00:00:00:00:
a8:78:bc:3d:01:07:67:85:cc:2:c2:bf:f6:ed:ed:fe:b5:d7:
17:4c:70:99:cd:57:0a:ad:f4:00:0b:2:6d:a8:0f:cdd2:d2:78:
5c:0d:8b:b6:87:2e:b3:6f:81:33:69:2e:2e:7c:a8:ab:07:bb:
e7:20:fa:01:00:00:00:00:00:00:00:00:00:00:00:00:00:00:45:
f1:0d:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:45:
4a:7e:cd:00:46:fa:57:b5:df:18:6d:bf:09:14:0d:03:01:e8:
82:65:c1:ea:73:f3:00:98:a1:28:d6:6f:59:3d:c3:d5:a3:c9:
48:a6:c1:78:98:31:f4:c5:14:60:59:bc:2a:41:ed:39:73:b5:
8e:52:ec:ed:a1:4b:0b:32:0a:16:00:00:00:00:00:00:00:00:37:
78:53:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:97:44:
u8:74:ee:00:cf:a5:4e:b9:73:42:0c:c1:c8:c3:46:4d:41:9:24:3a:
f8:b9:73:8d:a0:33:3d:07:7e:1b:9e:8a:f5:78:1f:86:ab:97:
83:c1:d1:81:83:ae:11:38:70:
student@serverA:~/mdhn18_ca$ 

```

Task 9: Options for intermediate CA certificate

- Create the certificate for CA1 using the CSR and the root CA is signing the certificate it is important to use *root's* OpenSSL configuration file.

```

Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
File Edit View Search Terminal Help
0ns 22:05
student@serverA: ~/mdhn18_ca

File Edit View Search Terminal Help
student@serverA:~/mdhn18_ca$ openssl ca -config openssl.cnf -extensions v3_intermediate_ca -days 3650 -notext -md sha256 -in ca1/csr/ca1.csr.pem -out ca1/certs/ca1.cert.pem
Using configuration from /openssl.cnf
Enter pass phrase for /home/student/mdhn18_ca/private/root.key.pem:
Can't open '/home/student/mdhn18_ca/index.txt.attr' for reading, No such file or directory
13966560471488:error:2081002:system library:fopen:'/home/student/mdhn18_ca/index.txt.attr','r'
13966560471488:error:0E00008B:BIO routines:IO_new_file:no such file:../crypto/bio/bss_file.c:8:
No certificate found
The request matches the signature
Signature ok
Certificate details:
    Serial Number: 4096 (0x1000)
    Validity
        Not Before: Jan 13 21:05:46 2021 GMT
        Not After : Jan 11 21:05:46 2031 GMT
    Subject:
        countryName           = SE
        stateOrProvinceName   = Stockholm
        organizationName      = SFI49
        commonName             = CA1Rabitul
    X509v3 extensions:
        X509v3 Subject Key Identifier:
            A2:32:FA:60:A6:41:01:17:E3:90:91:79:92:5B:71:A4:6E:86:59:97
        X509v3 Authority Key Identifier:
            keyId:00:A6:07:46:B2:20:50:E0:74:D1:E5:DE:2E:FF:6D:2E:80:04:34:28
        X509v3 Basic Constraints: critical
            CA:TRUE, pathlen:0
        X509v3 Extended Key Usage:
            Digital Signature, Certificate Sign, CRL Sign
Certificate is to be certified until Jan 11 21:05:46 2031 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]
Write out database with 1 new entries
Data Base Updated
student@serverA:~/mdhn18_ca$ 

```

Command

```
openssl ca -config openssl.cnf -extensions v3_intermediate_ca -days 3650 -notext -md sha256 -in ca1/csr/ca1.csr.pem -out ca1/certs/ca1.cert.pem
```

Description

-config openssl.cnf

specifies the configuration file to use.

-extensions v3_intermediate_ca

the section of the configuration file containing certificate extensions to be added when a certificate is issued (defaults to x509_extensions unless the -extfile option is used). If no extension section is present then, a V1 certificate is created. If the extension section is present (even if it is empty), then a V3 certificate is created.

-days 3650

the number of days to certify the certificate for.

-notext

don't output the text form of a certificate to the output file.

-md sha256

the message digest to use. Possible values include md5, sha1 and mdc2. This option also applies to CRLs.

-in ca1/csr/ca1.csr.pem

an input filename containing a single certificate request to be signed by the CA.

-out ca1/certs/ca1.cert.pem

the output file to output certificates to. The default is standard output. The certificate details will also be printed out to this file in PEM format (except that -spkac outputs DER format).

Task 10: Verify the certificate for CA1

- Verify the certificate for CA1, first command prints the cert and the second verifies the CA1's certificate authenticity against the root certificate.

```
student@serverA:~/mdhn18_ca5 openssl x509 -noout -text -in ca1/certs/ca1.cert.pem
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 4096 (0x1000)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = RootRabilul
Validity
    Not Before: Jan 13 21:05:46 2021 GMT
    Not After : Jan 11 21:05:46 2031 GMT
Subject: C = SE, ST = Blekinge, O = ET2540, CN = CA1Rabilul
Subject Key Identifier:
Public Key Algorithm: rsaEncryption
Public-Key: (4096 bit)
Modulus:
00:ea:3b:5c:ef:2e:1b:8c:d6:d6:5d:9f:6e:11:45:
a9:29:4d:cd:2b:5b:c2:25:b4:f6:52:c2:39:4a:75:
55:4a:f9:b6:ab:52:5a:b1:f1:10:d1:90:a8:75:
97:83:dc:68:70:d0:bef0:66:7f:ff:cc:98:09:
cb:8d:df:52:7:46:7d:43:5:7:20:56:5d:c9:51:b3:
93:a8:7a:a7:7:9:49:1f:88:5e:84:77:0e:11:7c:7b:
e9:2d:9d:7e:20:47:61:85:33:45:1f:8f:89:4a:4d:
5e:c5:85:b5:11:c3:35:5:5:0:b2:2a:16:c9:0e:89:
2d:49:de:61:f0:3e:65:13:41:5:49:bf:ff:fc:c8:a8:
1d:46:78:be:a7:33:04:19:88:e0:61:74:75:08:10:
95:8a:ef:30:0:c:ab:82:39:ad:46:93:24:0:a3:39:
15:08:0f:78:5f:8b:60:40:77:05:77:3d:5f:8c:0a:
28:03:48:9b:13:1f:44:94:64:5f:75:55:
c0:0b:33:ec:c7:1:7:94:96:3:a9:77:bc:0:b1:c9:4e:
78:b1:dc:ac:5:b6:06:66:0:62:14:13:3:a:c:c5:
a6:29:53:b1:2:4:58:8e:73:4:3:1d:20:a1:3:b7:5:b5:
37:0:3:7:2:1:1:7:1:3:5:1:2:1:1:1:1:1:1:1:1:
b1:C5:0:1:c:af:64:F5:2:1:1:e:42:43:29:40:08:11:
20:95:5d:65:43:a9:e3:0:c7:70:37:5b:dd:d0:c:a:c:f:
27:2:d:el:a3:4:a3:ed:a2:7:b:88:dc:74:fb:8:91:ad:
bf:6e:40:85:09:2d:a5:6e:0:2:fd:de:ei:7:87:46:
fb:21:eb:a:0:89:43:f5:4:c:1:f:8:ab:a7:9:a5:b0:c8:
0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:
f1:25:b2:d:c3:94:8b:1b:38:b8:84:24:cd:0:9:39:30:
a3:d5:06:39:c:b5:97:df:96:a7:dc:56:bc:b6:94:
ae:0:f:c5:5d:cc:0:f:d3:37:c:f:d3:cb:a5:b2:8:c:2:
dc:6:1:ab:8:0:bb:ff:ab:4:2:2:1:5:8:b:1:1:1:1:
a5:8:1:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:
4:f7:79:8a:b:b3:e:26:74:a6:1:60:76:5c:44:3:1:85:f9:
b4:f6:f6:b:c1:f5:0:ec:1:5:b:c7:c:d:f:d4:0:0:db:
ea:9:84:3:f:0:5:30:0:3:53:46:7:e:7:27:31:75:f5:f1:
e9:41:12:7:a:0:2:c5:96:c:e:0:1:81:9:f7:5b:4:d:69:
70:0:2:1:0:9:f:0:0:4:6:2:0:0:9:1:7:75:1:3:80:1:q:
d9:f:cc:8:c:b7:ee:7b:5c:6:0:21:e:9:87:1:0:30:6d:
```

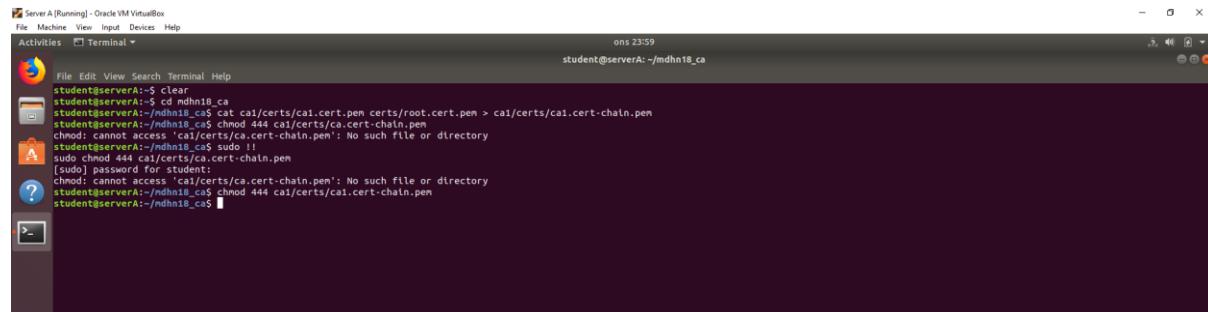
```
student@serverA:~/mdhn18_ca5 openssl x509 -noout -text -in ca1/certs/ca1.cert.pem
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 4096 (0x1000)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = RootRabilul
Validity
    Not Before: Jan 13 21:05:46 2021 GMT
    Not After : Jan 11 21:05:46 2031 GMT
Subject: C = SE, ST = Blekinge, O = ET2540, CN = CA1Rabilul
Subject Key Identifier:
Public Key Algorithm: rsaEncryption
Public-Key: (4096 bit)
Modulus:
00:ea:3b:5c:ef:2e:1b:8c:d6:d6:5d:9f:6e:11:45:
a9:29:4d:cd:2b:5b:c2:25:b4:f6:52:c2:39:4a:75:
55:4a:f9:b6:ab:52:5a:b1:f1:10:d1:90:a8:75:
97:83:dc:68:70:d0:bef0:66:7f:ff:cc:98:09:
cb:8d:df:52:7:46:7d:43:5:7:20:56:5d:c9:51:b3:
93:a8:7a:a7:7:9:49:1f:88:5e:84:77:0e:11:7c:7b:
e9:2d:9d:7e:20:47:61:85:33:45:1f:8f:89:4a:4d:
5e:c5:85:b5:11:c3:35:5:5:0:b2:2a:16:c9:0e:89:
2d:49:de:61:f0:3e:65:13:41:5:49:bf:ff:fc:c8:a8:
1d:46:78:be:a7:33:04:19:88:e0:61:74:75:08:10:
95:8a:ef:30:0:c:ab:82:39:ad:46:93:24:0:a3:39:
15:08:0f:78:5f:8b:60:40:77:05:77:3d:5f:8c:0a:
28:03:48:9b:13:1f:44:94:64:5f:75:55:
c0:0b:33:ec:c7:1:7:94:96:3:a9:77:bc:0:b1:c9:4e:
78:b1:dc:ac:5:b6:06:66:0:62:14:13:3:a:c:c5:
a6:29:53:b1:2:4:58:8e:73:4:3:1d:20:a1:3:b7:5:b5:
37:0:3:7:2:1:1:7:1:3:5:1:2:1:1:1:1:1:1:1:
b1:C5:0:1:c:af:64:F5:2:1:1:e:42:43:29:40:08:11:
20:95:5d:65:43:a9:e3:0:c7:70:37:5b:dd:d0:c:a:c:f:
27:2:d:el:a3:4:a3:ed:a2:7:b:88:dc:74:fb:8:91:ad:
bf:6e:40:85:09:2d:a5:6e:0:2:fd:de:ei:7:87:46:
fb:21:eb:a:0:89:43:f5:4:c:1:f:8:ab:a7:9:a5:b0:c8:
0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:
f1:25:b2:d:c3:94:8b:1b:38:b8:84:24:cd:0:9:39:30:
a3:d5:06:39:c:b5:97:df:96:a7:dc:56:bc:b6:94:
ae:0:f:c5:5d:cc:0:f:d3:37:c:f:d3:cb:a5:b2:8:c:2:
dc:6:1:ab:8:0:bb:ff:ab:4:2:2:1:5:8:b:1:1:1:1:
a5:8:1:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:
4:f7:79:8a:b:b3:e:26:74:a6:1:60:76:5c:44:3:1:85:f9:
b4:f6:f6:b:c1:f5:0:ec:1:5:b:c7:c:d:f:d4:0:0:db:
ea:9:84:3:f:0:5:30:0:3:53:46:7:e:7:27:31:75:f5:f1:
e9:41:12:7:a:0:2:c5:96:c:e:0:1:81:9:f7:5b:4:d:69:
70:0:2:1:0:9:f:0:0:4:6:2:0:0:9:1:7:75:1:3:80:1:q:
d9:f:cc:8:c:b7:ee:7b:5c:6:0:21:e:9:87:1:0:30:6d:
```

```
student@serverA:~/mdhn18_ca5 openssl verify -CAfile certs/root.cert.pem ca1/certs/ca1.cert.pem
ca1/certs/ca1.cert.pem: OK
student@serverA:~/mdhn18_ca5
```

Task 11: Create server certificate

Create a certificate chain.

Ensure the certificate chain is accessible to all users on Server A



```
student@serverA:~/mdhn18_ca$ clear
student@serverA:~/mdhn18_ca$ cd mdhn18/ca1
student@serverA:~/mdhn18/ca1$ cat ca1.cert.pem root.cert.pem > ca1/certs/ca1.cert-chain.pem
student@serverA:~/mdhn18/ca1$ chmod 444 ca1/certs/ca1.cert-chain.pem
chmod: cannot access 'ca1/certs/ca1.cert-chain.pem': No such file or directory
student@serverA:~/mdhn18/ca1$ sudo !!
sudo chmod 444 ca1/certs/ca1.cert-chain.pem
[sudo] password for student:
[sudo] password for student: access 'ca1/certs/ca1.cert-chain.pem': No such file or directory
student@serverA:~/mdhn18/ca1$ chmod 444 ca1/certs/ca1.cert-chain.pem
student@serverA:~/mdhn18/ca1$
```

Content of the CSR

To solve this task, I follow those steps. All screen shorts are the evidence to show, did this task successfully.

Steps

1. Create an RSA private key for the server.

```
openssl genrsa -out ca1/private/ca1server.key.pem 2048
```

2. Generate a CSR using the RSA private key from the previous step.

```
openssl req -config ca1/openssl.cnf -new -key ca1/private/ca1server.key.pem -out
ca1/csr/ca1server.csr.pem
```

3. Content of the CSR

```
openssl req -noout -text -in ca1/csr/ca1server.csr.pem
```

4. Use CA1's private key to sign the CSR and create a certificate for the server.

```
openssl ca -config ca1/openssl.cnf -extensions server_cert -days 3650 -notext -in
ca1/csr/ca1server.csr.pem -out ca1/certs/ca1server.cert.pem
```

5. Content of the signed certificate.

```
openssl x509 -noout -text -in ca1/certs/ca1server.cert.pem
```

6. Verify the server certificate against certificate chain.

```
openssl verify -CAfile ca1/certs/ca1.cert-chain.pem ca1/certs/ca1server.cert.pem
```

```

Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal tor 00:17
student@serverA: ~/mdhn18_ca$ openssl genrsa -out ca1/private/caiserver.key.pem 2048
Generating RSA private key, 2048 bit long modulus
....+
e is 65537 (0x10001)
student@serverA:~/mdhn18_ca$ openssl req -config ca1/openssl.cnf -new -key ca1/private/caiserver.key.pem -out ca1/csr/caiserver.csr.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [AU]:SE
State or Province Name (full name) [Some-State]:Blekinge
Locality Name (eg, city) [Karlskrona]:Karlskrona
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ET2540
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:localhost
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
student@serverA:~/mdhn18_ca$ openssl req -nouout -text -in ca1/csr/caiserver.csr.pem
Certificate Request:
Data:
Version: 1 (0x0)
Subject: C = SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = localhost
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:d0:02:d9:9e:3e:91:d6:5a:17:cd:0e:d7:5f:6d:
d2:90:eb:51:97:14:e8:9a:a7:c8:8a:8e:31:14:3e:5e:
e3:0f:4e:34:60:33:fb:d2:a1:f8:a8:ee:84:3e:ba:
be:f3:db:a4:60:c7:74:24:27:06:c3:46:0e:0a:81:b3:2e:
84:6a:27:5f:ad:f6:26:47:7f:66:9d:dc:11:81:de:f4:
02:86:53:dc:c0:b4:1a:b1:df:f3:2a:41:81:1d:6a:
70:9f:fb:0b:40:5c:56:f7:d5:04:2c:0e:35:54:62:
3d:5b:9c:02:f7:73:c1:8b:dd:fc:9d:86:06:d9:03:18:
73:4c:92:f7:35:c1:8b:dd:fc:9d:86:06:d9:03:18:
0e:2b:9b:99:01:3c:25:33:cc:33:47:70:17:ff:bf:
0f:2b:0f:45:a1:b6:9d:de:95:35:50:b3:ee:89:12:
f0:3d:d9:1c:33:52:65:ds:30:98:6f:51:ee:43:2a:3:
07:48:7f:ca:8a:7d:0b:9f:1c:4b:ea:ea:4f:81:ba:
....+
student@serverA:~/mdhn18_ca$ 

```

```

Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal tor 00:17
student@serverA: ~/mdhn18_ca$ openssl req -nouout -text -in ca1/csr/caiserver.csr.pem
Certificate Request:
Data:
Version: 1 (0x0)
Subject: C = SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = localhost
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:d0:02:d9:9e:3e:91:d6:5a:17:cd:0e:d7:5f:6d:
d2:90:eb:51:97:14:e8:9a:a7:c8:8a:8e:31:14:3e:5e:
e3:0f:4e:34:60:33:fb:d2:a1:f8:a8:ee:84:3e:ba:
be:f3:db:a4:60:c7:74:24:27:06:c3:46:0e:0a:81:b3:2e:
84:6a:27:5f:ad:f6:26:47:7f:66:9d:dc:11:81:de:f4:
02:86:53:dc:c0:b4:1a:b1:df:f3:2a:41:81:1d:6a:
70:9f:fb:0b:40:5c:56:f7:d5:04:2c:0e:35:54:62:
3d:5b:9c:02:f7:73:c1:8b:dd:fc:9d:86:06:d9:03:18:
73:4c:92:f7:35:c1:8b:dd:fc:9d:86:06:d9:03:18:
0e:2b:9b:99:01:3c:25:33:cc:33:47:70:17:ff:bf:
0f:2b:0f:45:a1:b6:9d:de:95:35:50:b3:ee:89:12:
f0:3d:d9:1c:33:52:65:ds:30:98:6f:51:ee:43:2a:3:
07:48:7f:ca:8a:7d:0b:9f:1c:4b:ea:ea:4f:81:ba:
....+
student@serverA:~/mdhn18_ca$ 

```

```
Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal tor 00:17
student@serverA: ~/mdhn18_ca5
student@serverA:~/mdhn18_ca5$ openssl req -nouot -text -in ca1/csr/caiserver.csr.pem
Certificate Request
  Data:
    Version: 1 (0x0)
    Subject: C = SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = localhost
    Subject Public Key Info:
      Public-Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
        Modulus:
          00:d0:02:d9:9e:3e:91:d6:5d:17:cd:0e:d7:5f:6d:
          d2:90:eb:51:97:14:e8:9a:a7:c0:8a:8e:31:14:3e:
          53:0c:0a:7a:81:1d:94:62:41:32:c2:64:ab:
        Exponent:
          01:00:01:00:00:00:00:00:00:00:00:00:00:00:00:00:
        Attributes:
          a0:00
      Signature Algorithm: sha256WithRSAEncryption
        30:46:02:3f:9e:0b:05:01:00:00:00:00:00:00:00:00:
        99:98:00:17:17:74:05:73:1b:c6:78:00:b1:b3:a7:9e:86:
        b5:37:0f:fe:76:b2:a5:47:5a:71:4b:3b:7f:1b:81:66:08:55:
        63:ea:a4:f4:9f:8c:c3:31:52:ed:eb:a2:a5:b2:c9:98:37:fb:c0:1d:
        f4:ba:60:39:ea:14:04:d6:8a:c7:77:cb:4a:dc:7d:76:8c:51:
        01:00:9b:79:c9:13:da:01:81:fd:73:00:00:00:00:00:00:00:00:
        b3:32:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
        00:id:76:40:33:bb:2:a6:3c:b3:3a:72:61:9e:dd:ee:08:c0:8f:
        a0:98:25:dc:14:63:a4:f4:45:1c:8a:25:f8:22:59:09:46:45:f3:
        13:88:02:18:7c:57:05:7f:e5:3d:bc:18:9c:5:cd:f0:2a:52:
        09:f2:41:05:01:00:00:00:00:00:00:00:00:00:00:00:00:00:
        5c:31:00:00:00:c9:02:60:c0:8a:51:00:00:00:00:00:00:00:00:
        ca:ff:e9:04:db:9b:0e:93:fd:9e:89:00:fd:24:2a:c1:f1:3b:
        9a:03:13:54:64:50:65:8f:58:f4:e8:f2:75:be:ad:ce:0f:c9:
        9b:5:ee:4d
      Exponent: 65537 (0x10001)
student@serverA:~/mdhn18_ca5$
```

```
Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal tor 00:53
student@serverA: ~/mdhn18_ca5
student@serverA:~/mdhn18_ca5$ openssl ca -config ca1/openssl.cnf -extensions server_cert -days 3650 -notext -in ca1/csr/caiserver.csr.pem -out ca1/certs/caiserver.cert.pem
Using configuration from /home/student/mdhn18_ca/ca1/openssl.cnf
Enter pass phrase for /home/student/mdhn18_ca/ca1/private/ca1.key.pem:
Can't open '/home/student/mdhn18_ca/ca1/index.txt.attr' for reading, No such file or directory
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 8192 (0x2000)
    Validity
        Not Before: Jan 13 23:52:44 2021 GRT
        Not After : Jan 11 23:52:44 2031 GRT
    Subject:
        countryName           = SE
        stateOrProvinceName  = Blekinge
        localityName         = Karlskrona
        organizationName     = ET2540
        commonName            = localhost
X509v3 extensions:
    X509v3 Basic Constraints:
        CA:FALSE
    X509v3 Subject Key Identifier:
        E2:C4:45:B5:D9:3B:53:7D:1F:C0:A4:9A:AB:AB:A0:15:6F:97:C8:62
    X509v3 Authority Key Identifier:
        keyid:A2:32:FA:00:04:41:01:17:E3:98:91:79:92:71:A4:66:80:59:97
        Dir:/etc/ssl/certs/localhost/C=SE/L=Karlskrona/O=ET2540/CN=RootRahul
        serial:10:00
    X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
    X509v3 Extended Key Usage:
        TLS Web Server Authentication
Certificate is certified until Jan 11 23:52:44 2031 GRT (3650 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated
student@serverA:~/mdhn18_ca5$
```

```

student@serverA:~/mdhn18_ca$ openssl x509 -noout -text < ca1/certs/caiserver.cert.pem
-----  

Certificate:  

    Version: 3 (0x1)  

    Serial Number: 8192 (0x2000)  

    Signature Algorithm: sha256WithRSAEncryption  

        Issuer: C = SE, ST = Blekinge, O = ET2540, CN = CAIRabil  

        Valid From: Mon Jan 13 23:52:44 2021 GMT  

        Valid Until: Mon Jan 11 23:52:44 2031 GMT  

    Subject: C = SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = localhost  

    Subject Public Key Info:  

        Public Key Algorithm: rsaEncryption  

            Modulus:  

                00:d0:02:0d:91:9c:3c:91:de:5d:1f:cd:0c:6d:f2:f0:  

                d2:4b:01:0b:4e:27:72:c9:b8:e6:31:23:45:  

                e3:1f:4e:34:00:33:fb:d2:a1:f0:8e:0b:3e:be:  

                c9:0e:37:79:08:97:f3:a2:72:5f:41:37:c2:04:ab:  

                94:6a:27:5f:ad:f6:2d:47:7f:66:9d:dc:1b:de:f6:  

                92:86:53:dc:0:b4:1a:b1:df:3f:2a:41:81:13:6a:  

                78:4c:42:1b:13:1a:0e:45:56:f7:05:04:2c:9e:35:54:02:  

                73:4c:42:f7:35:c1:bb:dd:fc:9d:8c:0e:ad:03:18:  

                9c:60:03:45:1a:0b:9d:de:05:35:50:b3:e9:09:12:  

                8f:0b:0f:45:1a:0b:9d:de:05:35:50:b3:e9:09:12:  

                f0:3d:d9:1c:13:52:65:05:30:98:6f:51:e4:32:a3:  

                f0:3d:9f:45:1a:0b:9d:de:05:35:50:b3:e9:09:12:  

                b0:c7:79:9c:67:e2:c5:1a:0b:9d:de:05:35:50:b3:e9:  

                0f:8a:99:bd:41:88:33:3b:71:13:c1:60:94:40:ab:61:  

                ca:31  

            Exponent: 05537 (0x10001)  

X509v3 extensions:  

    X509v3 Basic Constraints:  

        CA:FALSE  

    X509v3 Subject Key Identifier:  

        E2:C4:45:85:D9:3B:53:70:1F:C0:A4:9A:AB:AB:15:6F:97:C8:62  

    X509v3 Authority Key Identifier:  

        KeyId:A2:32:F4:69:60:41:01:17:E3:98:91:79:92:58:71:A4:6E:B6:59:97  

        DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=RootRabil  

    serial:10:00  

X509v3 Key Usage: critical  

    Digital Signature, Key Encipherment  

X509v3 Extended Key Usage:  

    TLS Web Server Authentication  

Signature Algorithm: sha256WithRSAEncryption

```

```

student@serverA:~/mdhn18_ca$ openssl x509 -noout -text < ca1/certs/ca1.cert-chain.pem
-----  

Certificate:  

    Version: 3 (0x1)  

    Serial Number: 5537 (0x10001)  

    Signature Algorithm: sha256WithRSAEncryption  

        Issuer: C = SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = RootRabil  

        Valid From: Mon Jan 13 23:52:44 2021 GMT  

        Valid Until: Mon Jan 11 23:52:44 2031 GMT  

    Subject: C = SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = localhost  

    Subject Public Key Info:  

        Public Key Algorithm: rsaEncryption  

            Modulus:  

                04:4e:18:5e:a1:9e:82:68:ab:57:5c:ed:8e:75:57:af:  

                0b:4b:ed:65:ec:75:3b:14:5b:56:bd:7d:32:ff:dd:5b:67:8b:  

                4e:22:8c:49:7d:4b:1b:96:3a:44:1f:0b:45:3a:0e:01:  

                51:86:0b:db:8b:75:f1:49:8e:0e:0b:5d:fd:0e:31:66:7e:32:  

                78:9e:3b:8f:f9:ob:5e:3f:be:ff:fd:de:63:b2:bd:79:66:9a:  

                3b:3d:09:43:1a:44:0b:4a:4d:41:40:4d:44:41:42:43:  

                20:52:77:72:d4:1a:14:cd:bb:aa:20:0b:56:3b:35:bd:96:03:d7:  

                0d:02:8e:c2:4d:e5:c5:34:02:f6:20:74:d9:ba:ae:ec:b1:df:  

                5d:5f:9c:1e:1b:4d:15:5c:10:1b:1a:1b:1c:1d:1e:1f:  

                0f:rc:11:e2:f5:11:5c:dc:cb:aa:27:7a:aa:0f:4b:5d:17:02:b4:  

                fd:08:4e:1e:cb:9e:5c:3c:34:f2:d9:5c:16:fc:eb:1b:95:86:a9:  

                5c:2c:2d:3f:3e:3f:3d:3e:3f:3d:3e:3f:3d:3e:3f:3d:  

                ff:43:ab:76:3e:eb:03:50:b7:dd:ee:3f:83:ca:ad:05:00:e0:  

                e0:52:91:21:41:80:11:ff:99:5d:23:49:80:e1:d2:46:10:75:64:  

                ad:id:ce:2e:07:da:43:1f:2b:7a:52:0d:55:1a:6e:19:0e:16:  

                e2:22:30:11:1f:1a:0b:11:1f:1a:0b:11:1f:1a:0b:11:1f:  

                1d:dc:3e:1c:79:17:cd:9e:78:90:0d:66:22:92:1a:rc:07:22:28:55:  

                99:2c:74:5d:62:79:30:c1:ed:93:od:19:25:18:40:1d:68:22:  

                01:1b:3e:1c:79:17:cd:9e:78:90:0d:66:22:92:1a:rc:07:22:28:55:  

                bd:30:c5:44:ad:df:70:05:30:6a:51:25:30:ac:91:bf:df:07:64:  

                29:0d:2c:5e:c9:71:8a:e4:91:14:f2:f8:79:07:ca:13:70:1d:  

                9c:2c:2d:3f:3e:3f:3d:3e:3f:3d:3e:3f:3d:3e:3f:3d:  

                12:0e:01:11:6b:77:ed:05:19:27:17:20:21:23:46:4e:02:bf:2c:1c:  

                bd:06:8e:0c:01:dc:ea:b0:9c:ad:91:f7:01:50:23:bb:41:1d:87:96:  

                70:32:11:1f:1a:0b:11:1f:1a:0b:11:1f:1a:0b:11:1f:  

                9b:77:9a:5b:f0:b5:99:06:ea:40:66:6c:e0:c3:27:d7:1c:  

                0c:cc:1a:2d:1b:1a:1b:1a:1b:1a:1b:1a:1b:1a:1b:1a:  

                21:98:fb:c9:c1:7a:ad:01:1f:1a:0b:11:1f:1a:0b:11:  

                1d:dc:3e:1c:79:17:cd:9e:78:90:0d:66:22:92:1a:rc:07:22:28:55:  

                student@serverA:~/mdhn18_ca$ openssl verify -CAfile ca1/certs/ca1.cert-chain.pem ca1/certs/caiserver.cert.pem  

ca1/certs/caiserver.cert.pem: OK  

student@serverA:~/mdhn18_ca$ 

```

Task 12: Show your certificate in Firefox

Before that task start, I need.

Configure Apache web server to use the server certificate.

- Copy the certificate to the location, shown in a screen short.

```

student@serverA:~/mdhn18_ca$ sudo su
[sudo] password for student:
root@serverA:/home/student/mdhn18_ca# cp /home/student/mdhn18_ca/ca1/private/caiserver.key.pem /etc/ssl/private
root@serverA:/home/student/mdhn18_ca# cp /home/student/mdhn18_ca/ca1/certs/caiserver.cert.pem /etc/ssl/certs
root@serverA:/home/student/mdhn18_ca# cp /home/student/mdhn18_ca/ca1/certs/ca1.cert-chain.pem /etc/apache2
root@serverA:/home/student/mdhn18_ca# sudo gedit /etc/apache2/sites-enabled/default-ssl.conf
** (gedit:2723): WARNING **: 01:12:19.510: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:2723): WARNING **: 01:12:19.510: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:2723): WARNING **: 01:12:23.712: Set document metadata failed: Setting attribute metadata::gedit-position not supported
root@serverA:/home/student/mdhn18_ca# sudo service apache2 restart
root@serverA:/home/student/mdhn18_ca#

```

- Edit the file /etc/apache2/sites-enabled/default-ssl.conf

```
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

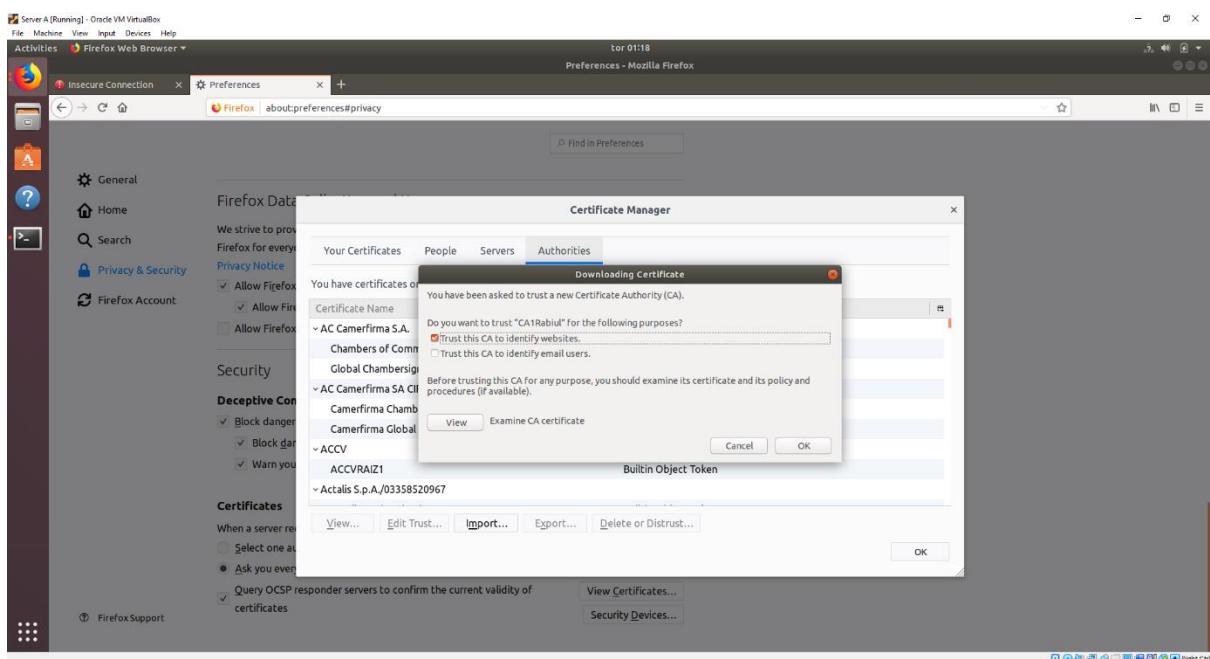
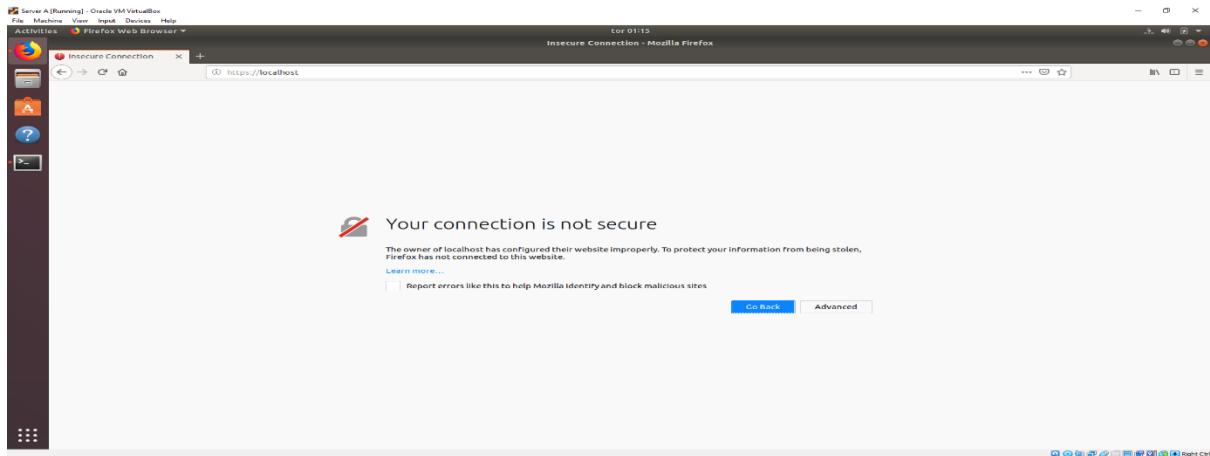
# SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on

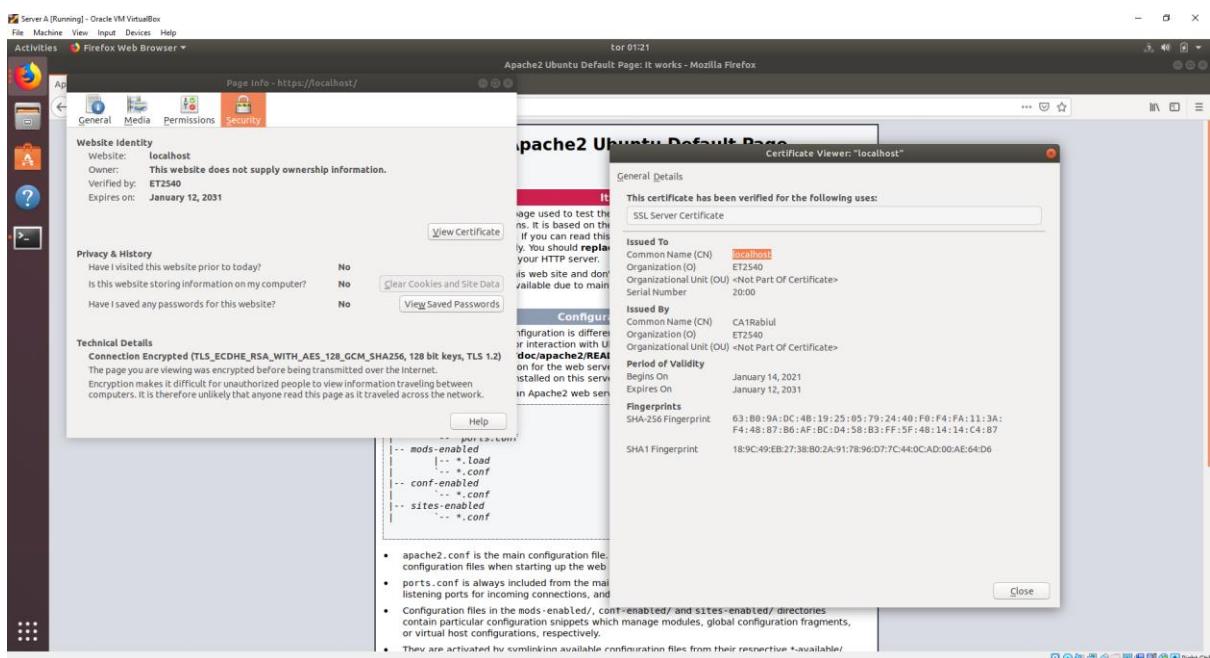
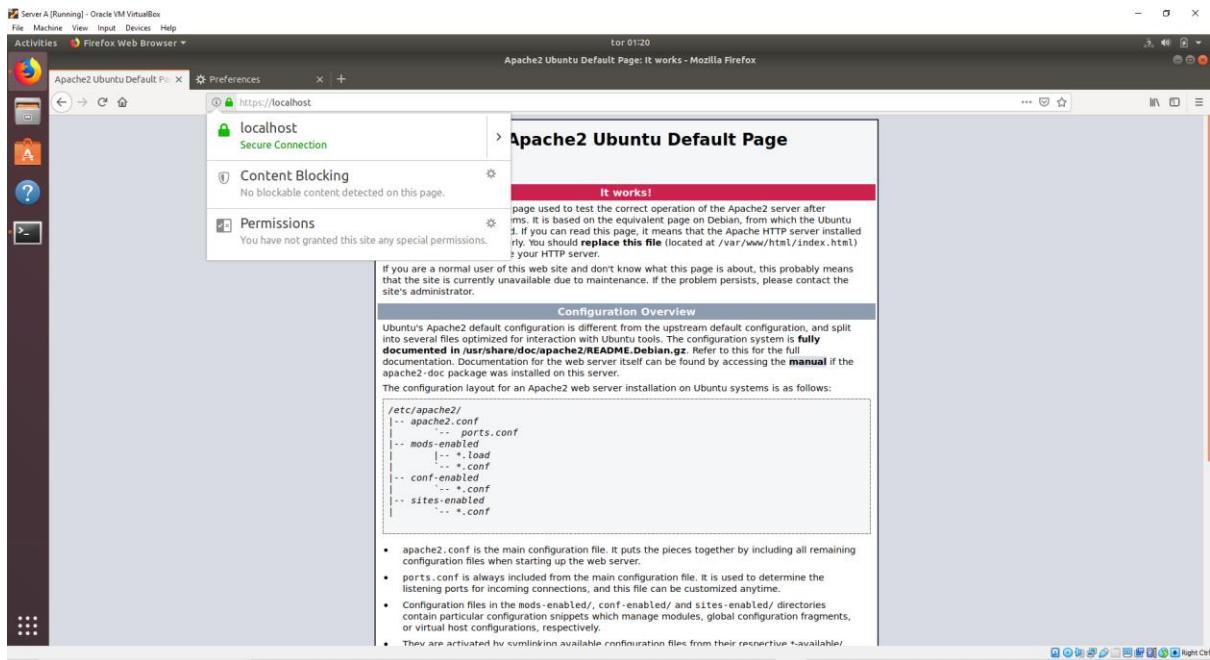
# A self-signed (snakeoil) certificate can be created by installing
# the ssl-cert package. See
# /usr/share/doc/apache2/ssl-cert/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, only the
# SSLCertificateFile directive is needed.
SSLCertificateFile /etc/ssl/certs/calserver.cert.pem
SSLCertificateKeyFile /etc/ssl/private/calserver.key.pem

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively the
# referenced file can be the same as SSLCertificateFile
# and the certificate file will be directly appended to the server
# certificate for convenience.
SSLCertificateChainFile /etc/apache2/cal.cert-chain.pem

# Certificate Authority (CA):
```

Add certificate chain to Firefox web browser.





Task 13: Create a CRL for CA1

Before that I edit the CA1 OpenSSL configuration file and add the following parameter to the serv_cert section:

crlDistributionPoints = URI:https://localhost/ca1.crl.pem

- Following command to create a CRL for CA1
`openssl ca -config ca1/openssl.cnf -gencrl -out ca1/crl/ca1.crl.pem`

- Dump the contents of the CRL using the following command and include the contents in the report:

```
openssl crl -in ca1/crl/ca1.crl.pem -noout -text
```

```
student@serverA:/mdhn18_ca$ openssl crl -in ca1/crl/ca1.crl.pem -noout -text
-----  
Certificate Revocation List (CRL)  
Version: 1 (0x1)  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: /C=SE/ST=blekinge/O=ET2540/CN=CA1habitul  
Last Update: Jan 14 00:31:05 2021 GMT  
Next Update: Jan 13 00:31:05 2021 GMT  
CRL extensions:  
X509v3 CRL Number:  
8193  
No Revoked Certificates:  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: /C=SE/ST=blekinge/O=ET2540/CN=CA1habitul  
Last Update: Jan 14 00:31:05 2021 GMT  
Next Update: Jan 13 00:31:05 2021 GMT  
CRL extensions:  
X509v3 CRL Number:  
8193  
-----  
student@serverA:/mdhn18_ca$
```

Task 14: Revoke a certificate

I follow those steps to complete this task, and all screen short provide as proof.

Steps

- Create an RSA private key for the server.

```
openssl genrsa -out ca1/private/dragos.ilie@bth.se.key.pem 2048
```

- Generate a CSR using the RSA private key from the previous step.

```
openssl req -config ca1/openssl.cnf -new -key ca1/private/dragos.ilie@bth.se.key.pem -out ca1/csr/dragos.ilie@bth.se.csr.pem
```

- Content of the CSR.

```
openssl req -noout -text -in ca1/csr/dragos.ilie@bth.se.csr.pem
```

- Use CA1's private key to sign the CSR and create a certificate for the server.

```
openssl ca -config ca1/openssl.cnf -extensions usr_cert -days 3650 -notext -in ca1/csr/dragos.ilie@bth.se.csr.pem -out ca1/certs/dragos.ilie@bth.se.cert.pem
```

- Content of the signed certificate.

```
openssl x509 -noout -text -in ca1/certs/dragos.ilie@bth.se.cert.pem
```

- Verify the server certificate against certificate chain.

```
openssl verify -CAfile ca1/certs/ca1.cert-chain.pem ca1/certs/dragos.ilie@bth.se.cert.pem
```

```
Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal tor 01:46
student@serverA: ~/mdhn18_ca
student@serverA:~/mdhn18_ca$ openssl genrsa -out ca1/private/dragos.llie@bth.se.key.pem 2048
Generating RSA private key, 2048 bit long modulus
.....+++
e is 65537 (0x10000)
A
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
if you enter '.', the field will be left blank.
<...
Country Name (2 letter code) [AU]:SE
State or Province Name (full name) [Some-State]:Blekinge
Locality Name (eg, city) [Karlskrona]:Karlskrona
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ET2540
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:dragos.llie@bth.se
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
student@serverA:~/mdhn18_ca$ openssl req -newout -text -in ca1/csr/dragos.llie@bth.se.csr.pem
Certificate Request:
Data:
Version: 1 (0x0)
Subject: C = SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = dragos.llie@bth.se
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:d5:d1:00:b7:0a:b1:d9:71:ea:b3:74:72:e2:a7:
07:20:c2:c5:57:9b:f3:3b:8f:12:c4:53:d1:48:65:
45:0c:6d:40:35:70:49:2d:75:5b:11:49:
29:1c:dc:f7:be:f0:60:9f:07:9b:49:0e:rd:41:bc:2a:
cc:bf:99:64:9b:05:0c:1aa:52:52:63:0e:6e:25:15:
76:99:34:90:0f:0a:50:b1:76:87:e5:44:21:55:4b:
93:db:32:ee:0d:4d:08:66:a3:a8:9d:f8:bf:0d:0e:4:53:
9d:c9:9d:0d:0a:0f:0a:0f:0a:0f:0a:0f:0a:0f:0a:0f:
af:0d:0a:0d:0d:01:93:f7:77:61:bd:f1:50:af:fd:
e1:b8:8c:8c:c7:59:6b:ice:43:c1:c1:26:1e:h5:95:
b6:1e:4a:f4:88:03:c6:a7:bb:95:38:c3:dc:b6:3b:
eb:d6:a5:b6:54:a5:F7:41:2d:iae:0d:10:34:c9:e8:
d1:28:f5:ce:4e:35:2f:7a:8d:2b:b3:c2:78:be:25:
d1:05:22:be:7e:10:55:ee:78:1c:24:2d:78:0b:16:4a:
bd:77:9f:46:0d:e1:33:ice:87:f5:dc:8c:56:11:fc:
b1:87:c1:dc:97:df:a8:4b:a2:ea:8d:9c:ab:fd:85:
za:bd
Exponent: 65537 (0x10000)
Attributes:
    a0:00
Signature Algorithm: sha256WithRSAEncryption
0f:2f:8f:f4:51:b1:e0:ac:ad:16:c:f3:38:51:35:bd:b3:0a:8b:
88:85:1:ea:ed:08:84:ef:5e:05:1c:01:01:01:01:01:01:01:01:
44:01:01:01:01:01:01:01:01:01:01:01:01:01:01:01:01:01:01:
22:f0:57:d1:94:75:28:8d:74:9f:73:ec:c5:59:e7:bb:fc:7e:74:
51:a6:2d:c2:07:de:a7:ed:e4:bd:30:a9:05:ff:53:3b:6d:
25:e2:56:8d:80:c5:78:83:b2:72:d1:13:cfa:74:45:a5:70:b7:
be:3e:81:20:19:08:33:b2:01:03:c1:c7:c0:16:17:
b9:01:01:01:01:01:01:01:01:01:01:01:01:01:01:01:01:01:
fb:15:ee:ce:eb:40:eb:41:26:11:f1:86:2c:79:dd:12:5b:25:e:
e3:ac:22:91:c9:03:24:a2:da:96:f4:aa:87:a8:11:09:2:97:
7f:c9:91:c8:cd:0f:f:fd:46:39:0d:75:87:24:5:f:dd:1e:1:07:67:
f5:7a:3c:3c:77:04:b3:77:5b:4c:3d:c3:2e:83:2b:ff:01:7f:
4e:03:3d:0d:0d:2:b1:f1:53:9b:05:0b:fc:73:67:0b:19:28:79:
30:ca:cd:30:59:00:24:51:aa:3c:09:a7:2e:82:0f:79:3e:c8:
ec:7a:41:d5
student@serverA:~/mdhn18_ca$ openssl ca -config ca1openssl.cnf -extensions usr_cert -days 3650 -notext -in ca1/csr/dragos.llie@bth.se.csr.pem -out ca1/certs/dragos.llie@bth.se.cert.pem
Using configuration from ca1openssl.cnf
Enter pass phrase for /home/student/mdhn18_ca/ca1/private/ca1.key.pem:
aborted!
unable to load CA private key
140312339108288:error:PEM routines:PEM_do_header:bad password read:../crypto/pem/pem_lib.c:418:
student@serverA:~/mdhn18_ca$ openssl ca -config ca1openssl.cnf -extensions usr_cert -days 3650 -notext -in ca1/csr/dragos.llie@bth.se.csr.pem -out ca1/certs/dragos.llie@bth.se.cert.pem
Using configuration from ca1openssl.cnf
Enter pass phrase for /home/student/mdhn18_ca/ca1/private/ca1.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 8193 (0x2001)
    Validity
        Not Before: Jan 14 00:43:56 2021 GMT
        Not After : Jan 12 00:43:56 2031 GMT
    Subject:
        countryName      = SE
        stateOrProvinceName = Blekinge
        localityName     = Karlskrona
        organizationName = ET2540
        commonName       = dragos.llie@bth.se
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA=TRUE
```

```
Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal tor 01:46
student@serverA: ~/mdhn18_ca
student@serverA:~/mdhn18_ca$ openssl ca -config ca1openssl.cnf -extensions usr_cert -days 3650 -notext -in ca1/csr/dragos.llie@bth.se.csr.pem -out ca1/certs/dragos.llie@bth.se.cert.pem
Using configuration from ca1openssl.cnf
Enter pass phrase for /home/student/mdhn18_ca/ca1/private/ca1.key.pem:
aborted!
```

```

Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal ▾
student@serverA: ~/mdhn18_ca
student@serverA: ~/mdhn18_ca$ openssl x509 -noout -text -in ca1/certs/dragos.ilie@bth.se.cert.pem
Certificate:
    X509v3 Basic Constraints:
        CA:FALSE
    X509v3 Key Usage: critical
        Digital Signature, Non Repudiation, Key Encipherment
    X509v3 Extended Key Usage:
        TLS Web Client Authentication, E-mail Protection
    Netscape Comment:
        OpenSSL Generated Certificate
    X509v3 Subject Key Identifier:
        D1:19:0A:F0:A1:01:F1:15:21:AD:9B:8B:AB:F5:6F:2F:15:0F:35:87
    X509v3 Authority Key Identifier:
        keyid:D2:32:FA:60:A6:41:01:17:E3:9B:91:79:92:5B:71:A4:6E:B6:59:97
        Certificate is to be certified until Jan 12 00:43:56 2031 GMT (3650 days)
Sign the certificate? [y/n]y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Database successfully updated
student@serverA: ~/mdhn18_ca$ openssl x509 -noout -text -in ca1/certs/dragos.ilie@bth.se.cert.pem
Certificate:
    Version: 3 (0x2)
    Serial Number: 1193 (0x2001)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C = SE, ST = Blekinge, O = ET2540, CN = Ca1Rabiu1
    Validity
        Not Before: Jan 14 00:43:56 2021 GMT
        Not After : Jan 13 2031 04:35:56 2031 GMT
    Subject: C = SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = dragos.ilie@bth.se
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
        [REDACTED]
        Exponent: 65537 (0x100001)
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        X509v3 Key Usage: critical
            Digital Signature, Non Repudiation, Key Encipherment
        X509v3 Extended Key Usage:
            TLS Web Client Authentication, E-mail Protection
        Netscape Comment:
            OpenSSL Generated certificate
        X509v3 Subject Key Identifier:
            D1:19:0A:F0:A1:01:F1:15:21:AD:9B:8B:AB:F5:6F:2F:15:0F:35:87
        X509v3 Authority Key Identifier:
            keyid:D2:32:FA:60:A6:41:01:17:E3:9B:91:79:92:5B:71:A4:6E:B6:59:97
        Signature Algorithm: sha256WithRSAEncryption

```

```

Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal ▾
student@serverA: ~/mdhn18_ca
student@serverA: ~/mdhn18_ca$ 2>> /dev/null
student@serverA: ~/mdhn18_ca$ openssl x509 -noout -text -in ca1/certs/dragos.ilie@bth.se.cert.pem
Certificate:
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        X509v3 Key Usage: critical
            Digital Signature, Non Repudiation, Key Encipherment
        X509v3 Extended Key Usage:
            TLS Web Client Authentication, E-mail Protection
        Netscape Comment:
            OpenSSL Generated certificate
        X509v3 Subject Key Identifier:
            D1:19:0A:F0:A1:01:F1:15:21:AD:9B:8B:AB:F5:6F:2F:15:0F:35:87
        X509v3 Authority Key Identifier:
            keyid:D2:32:FA:60:A6:41:01:17:E3:9B:91:79:92:5B:71:A4:6E:B6:59:97
        Signature Algorithm: sha256WithRSAEncryption
student@serverA: ~/mdhn18_ca$ openssl verify -CAfile ca1/certs/ca1.cert-chain.pem ca1/certs/dragos.ilie@bth.se.cert.pem
ca1/certs/dragos.ilie@bth.se.cert.pem: OK
student@serverA: ~/mdhn18_ca$ 

```

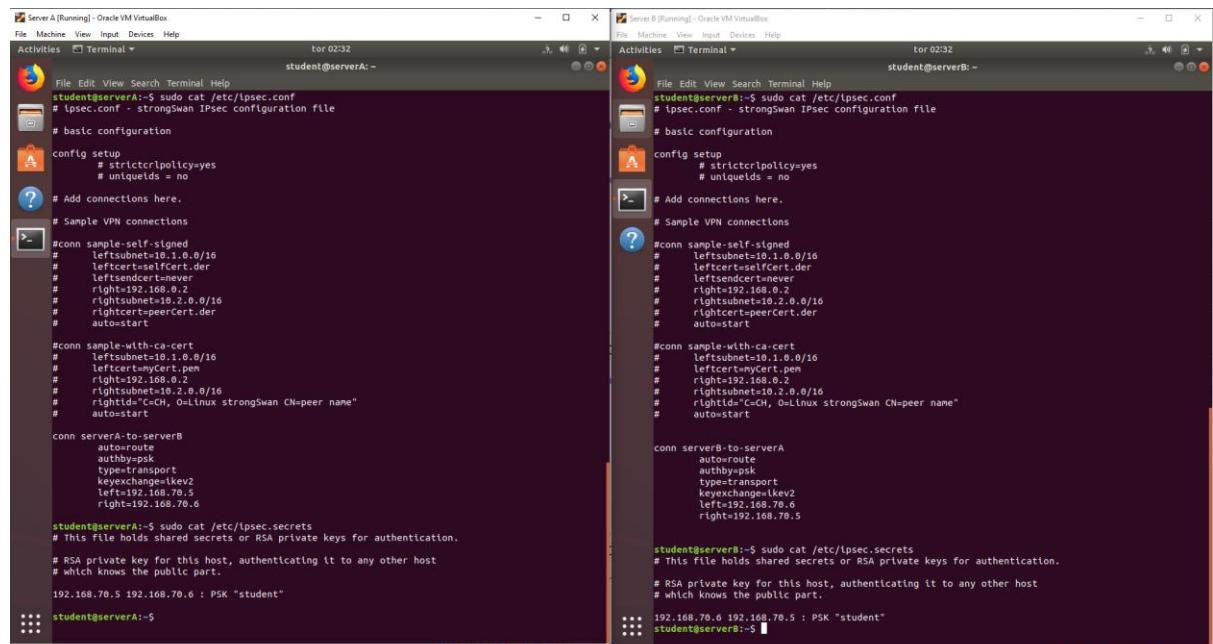
- Now, revoke the newly created certificate by entering the following command:
`openssl ca -config ca1/openssl.cnf -revoke ca1/certs/dragos.ilie@bth.se.cert.pem`

- Content of the file ca1/index.txt file

```
Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal tor 02:13
student@serverA:~/mdhn18_ca$ openssl ca -config ca1/openssl.cnf -revoke ca1/certs/dragos.ilie@bth.se.cert.pem
Using configuration from ca1/openssl.cnf
Enter pass phrase for /home/student/mdhn18_ca/ca1/private/ca1.key.pem:
Revoking Certificate 2001.
Data Base Updated.
student@serverA:~/mdhn18_ca$ cat ca1/index.txt
3 31011235244Z 2000 unknown /C=SE/S+Beckinge/L=Karlskrona/O=ET2540/CN=localhost
R 31011204356Z 21011401040Z 2001 unknown /C=SE/S+Beckinge/L=Karlskrona/O=ET2540/CN=dragos.ilie@bth.se
student@serverA:~/mdhn18_ca$ openssl ca -config ca1/openssl.cnf -genrsa -out ca1/crl/ca1.crl.pem
Using configuration from ca1/openssl.cnf
student@serverA:~/mdhn18_ca$ openssl crl -in ca1/crl/ca1.crl.pem -noout -text
Certificate Revocation List (CRL):
Version 2 (0x1)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=SE,O=ET2540,CN=dragos.ilie@bth.se
Last Update: Jan 14 01:12:27 2021 GMT
Next Update: Feb 13 01:12:27 2021 GMT
CRL extensions:
X509V3 CRL Number:
    1
Revoked Certificates:
Serial Number: 2001
    Revocation Date: Jan 14 01:04:02 2021 GMT
Signature Algorithm: sha256WithRSAEncryption
    es:31011235244Z:f1:0e:01:1d:17:2d:9d:b8:f2:d9:61:e6:90:81:
    65:00:b1:74:54:e1:12:4f:bc:05:f6:ff:2e:96:94:82:4d:c7:
    72:f0:33:d0:19:03:f2:0f:49:05:09:ff:4a:58:0f:2d:46:35:
    05:f6:91:3b:4f:7f:f3:ff:0a:3c:0c:ds:87:31:db:37:75:b2:
    5b:9d:1b:70:5e:4c:03:6c:53:0c:49:1d:1a:0e:2e:0c:9e:31:
    21:86:96:35:1b:80:86:87:87:bc:f1:7f:ff:0a:5f:15:6c:77:b3:
    33:c2:c4:4a:59:f9:07:ad:0f:16:42:2b:1d:fd:00:53:f3:37:4e:
    43:77:6a:d6:9c:f1:f1:10:92:2e:2b:1d:fd:00:53:f3:37:4e:
    21:a0:08:04:e4:f5:7a:7c:d2:d0:70:ad:f9:bb:5e:2:be:de:
    a9:d5:01:61:57:01:31:00:00:00:00:00:00:00:00:00:00:00:
    C4:43:43:91:31:00:c4:26:31:57:09:44:49:49:39:39:
    79:f0:15:02:cc:ca:7:37:74:cc:79:02:01:81:b1:d9:dc:f9:bc:d9:
    1e:dd:ff:63:0e:8a:bf:27:1a:0e:bb:92:4d:ds:29:9a:2e:18:
    2:f5:53:1b:05:c4:b4:60:fe:76:95:92:cb:2e:ba:02:e1:dc:
    c5:36:bd:03:85:53:97:cd:32:35:10:92:01:00:00:00:00:00:
    5f:26:bd:03:85:53:97:cd:32:35:10:92:01:00:00:00:00:00:
    69:24:0c:57:b5:71:1b:24:45:52:4b:ca:58:76:f9:32:41:2d:88:
    57:4f:7e:66:0b:37:f1:f1:81:42:5e:ab:82:75:c4:4b:1f:f3:0e:
    e6:et:7:c5:f5:cc:5e:12:c:fb:9b:14:4f:c0:0e:b6:5d:18:d7:f0:
    32:ab:62:be:d0:c1:c0:c7:73:4a:31:30:41:30:41:30:41:30:
    0f:9e:64:06:31:2a:4e:3a:19:9b:01:c9:31:a1:1c:03:cc:
    b2:48:cce:16:2a:15:4e:3a:19:9b:01:c9:31:a1:1c:03:cc:
    98:44:61:e5:25:b3:66:5b:06:3b:a8:66:6d:74:3:b0:5e:2e:54:
    d8:b7:f8:35:8c:46:5e:3c:ff:ca:4:ch:79:85:ah:06:f0:9a:ah
```

Task 15: Host-to-host transport mode VPN with PSK authentication

- For this task need to install by this command:
`sudo apt-get install strongswan`
- The main configuration files for strongSwan are `/etc/ipsec.conf` and `/etc/ipsec.secrets`.



```
Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal tor 02:32
student@serverA:~$ sudo cat /etc/ipsec.conf
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
    # strictcrlpolicy=yes
    # uniqueids = no

# Add connections here.

# Sample VPN connections

#conn sample-self-signed
#    leftsubnet=10.1.0.0/16
#    leftcert=serverA.cert.der
#    leftsendcert=never
#    right=192.168.0.2
#    rightsubnet=10.2.0.0/16
#    rightcert=peerCert.der
#    auto=start

#conn sample-with-ca-cert
#    leftsubnet=10.1.0.0/16
#    leftcert=serverA.cert.pem
#    right=192.168.0.2
#    rightsubnet=10.2.0.0/16
#    rightid="C=CH, O=Linux strongSwan CN=peer name"
#    auto=start

conn serverA-to-serverB
    auto=route
    authby=psk
    type=transport
    keyexchange=ikev2
    left=192.168.70.5
    right=192.168.70.6

student@serverA:~$ sudo cat /etc/ipsec.secrets
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

192.168.70.5 192.168.70.6 : PSK "student"

student@serverA:~$
```

```
Server B [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal tor 02:32
student@serverB:~$ sudo cat /etc/ipsec.conf
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
    # strictcrlpolicy=yes
    # uniqueids = no

# Add connections here.

# Sample VPN connections

#conn sample-self-signed
#    leftsubnet=10.0.0/16
#    leftcert=serverB.cert.der
#    leftsendcert=never
#    right=192.168.0.2
#    rightsubnet=10.2.0.0/16
#    rightcert=peerCert.der
#    auto=start

#conn sample-with-ca-cert
#    leftsubnet=10.0.0/16
#    leftcert=serverB.cert.pem
#    right=192.168.0.2
#    rightsubnet=10.2.0.0/16
#    rightid="C=CH, O=Linux strongSwan CN=peer name"
#    auto=start

conn serverB-to-serverA
    auto=route
    authby=psk
    type=transport
    keyexchange=ikev2
    left=192.168.70.6
    right=192.168.70.5

student@serverB:~$ sudo cat /etc/ipsec.secrets
# This file holds shared secrets or RSA private keys for authentication.

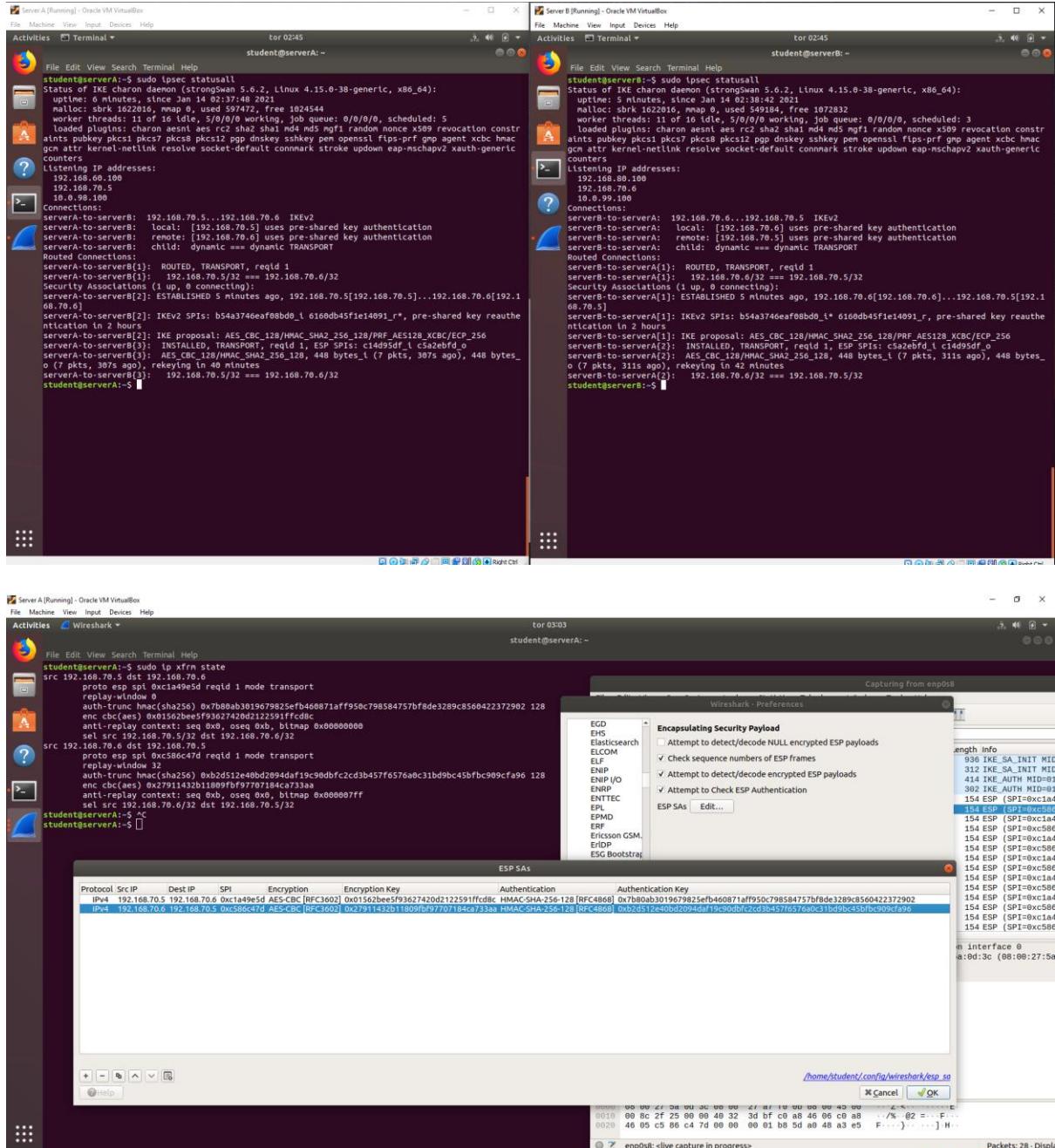
# RSA private key for this host, authenticating it to any other host
# which knows the public part.

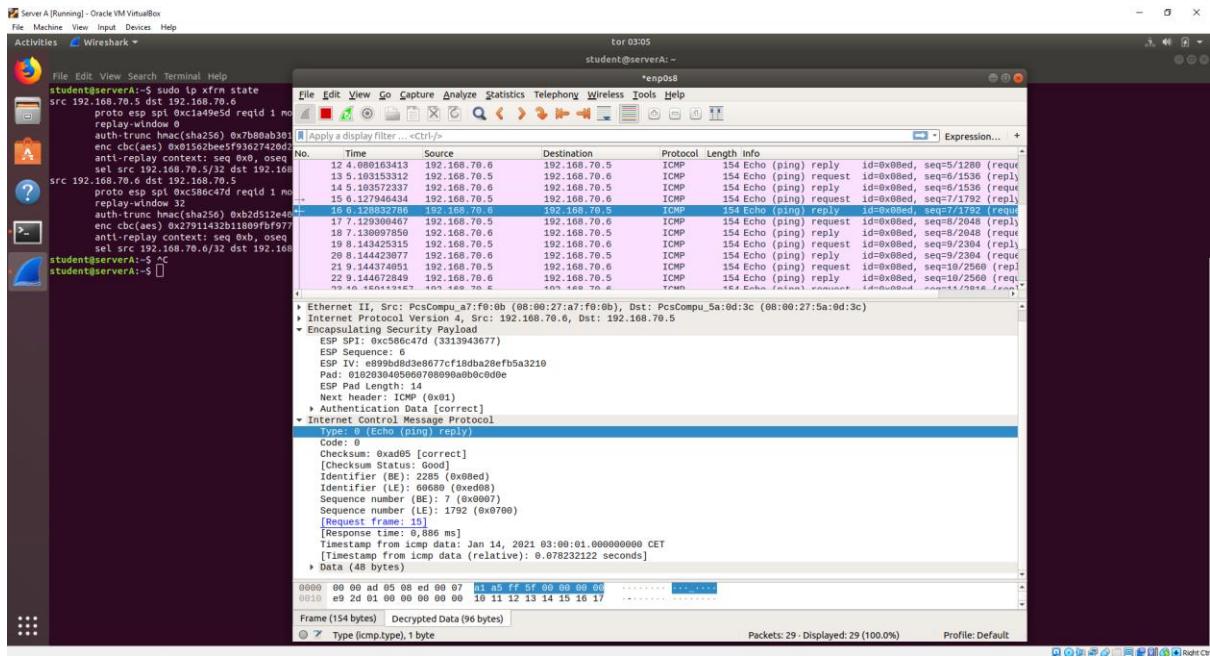
192.168.70.6 192.168.70.5 : PSK "student"

student@serverB:~$
```

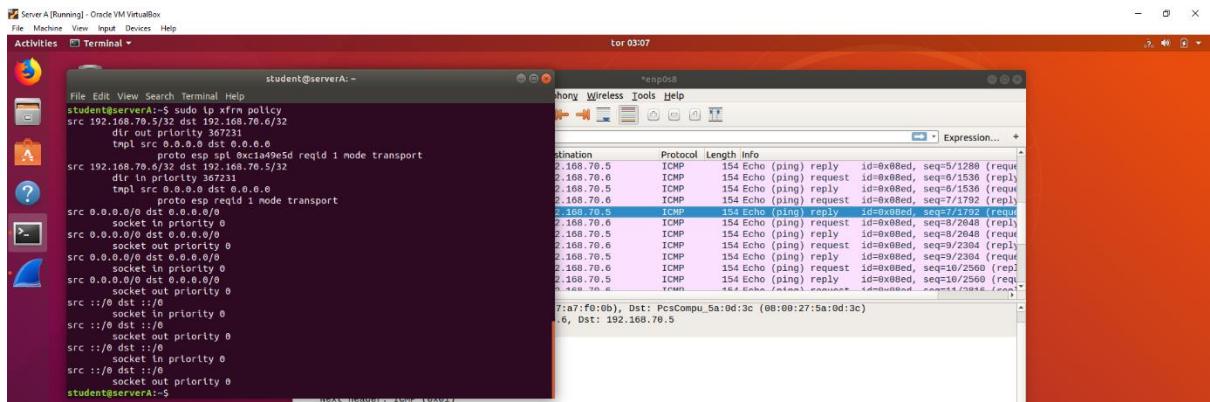

Task 16: Decrypt traffic with Wireshark

- For this task, decrypt traffic with wireshark shown below screen shorts.





Task 17: List the entries in the SPD



Description in

It specifies the incoming SAs from ipsec.

tmpl

It defines how ipsec should encapsulate matching packets.

esp

It shows that the type of protocol was esp.

reqid

It links the Security Policy Database (SPD) and the Security Association Database (SAD).

transport

It shows that the mode of transport was transport.

Task 18: Host-to-host transport mode VPN with cert authentication

- Before Host-to-host transport mode VPN with certificate authentication we need to create key for serverA and serverB.
- All screen short are shown those process step by step.
- Lastly verified all the certificates.

```
student@serverA:~$ cd /mdhn18_ca/
student@serverA:~/mdhn18_ca$ openssl genrsa -out ca1/private/192.168.70.5.key.pem 2048
Generating RSA private key, 2048 bit long modulus
.....+
e is 65537 (0x100001)
student@serverA:~/mdhn18_ca$ openssl req -config ca1/openssl.cnf -new -key ca1/private/192.168.70.5.key.pem -out ca1/csr/192.168.70.5.csr.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [AU]:SE
State or Province Name (full name) [Some-State]:Blekinge
Locality Name (eg, city) []:Karlskrona
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ET2540
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:192.168.70.5
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
X509 extensions []:
student@serverA:~/mdhn18_ca$ openssl req -noout -text -in ca1/csr/192.168.70.5.csr.pem
Certificate Request:
Data:
Version: 3 (0x80)
Subject: O = SE, ST = Blekinge, L = Karlskrona, C = ET2540, CN = 192.168.70.5
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
            Modulus:
                00:c6:0a:3a:a6:44:13:ec:33:33:cc:0a:4e:1b:33:
                50:75:90:1a:76:e8:24:7b:26:ce:6c:f8:13:5b:52:
                38:6c:03:58:04:54:71:fd:c8:90:00:80:0c:46:6a:
                39:9b:fb:ef:08:3e:eb:20:39:4b:el:4f:df:7:d9:
                3c:29:e9:eb:cc:03:73:73:1b:1d:32:71:2d:23:c1:2f:
                40:9b:3d:4c:1a:12:12:12:12:12:12:12:12:12:12:4c:
                8f:87:be:57:fd:40:hf:9f:76:97:3d:58:a1:95:c8:
                cd:d4:33:ee:c4:79:d1:9c:35:f9:01:77:02:b8:ec:
                ab:61:d2:2d:f3:57:54:5d:90:cd:aa:3f:r:fb:2b:2b:
                7d:53:6e:0:cc:44:a8:ed:18:3d:42:8b:5b:9a:fd:
                cc:3a:7e:07:5:73:32:3b:4c:ab:89:06:ea:ed:59:
                b2:31:96:fb:0b:04:4c:5c:91:39:7d:fe:22:9d:25:2c:
                b4:f0:12:95:ab:14:9f:5e:fa:54:ba:26:80:1e:0:60:
                b1:95:70:db:b5:ff:cf:31:0c:43:d8:95:10:cb:e5:5b:
                f9:93
            Exponent: 65537 (0x100001)
Attributes:
    a0:00
Signature Algorithm: sha256WithRSAEncryption
7a:82:12:0a:a2:4e:d0:f8:1c:19:2a:5f:88:0f:9e:1b:b7:8c:
50:49:12:12:12:12:12:12:12:12:12:12:12:12:12:12:12:12:
ad:ef:ef:bf:11:4a:0:2:f6:f5:bd:1d:1e:10:8d:94:c2:08:ba:de:
ca:5b:dd:6d:d9:10:3c:0a:40:b4:fd:4c:4ce:7d:59:ca:16:5a:de:
7e:9d:0c:c4:9c:f8:1:f:2d:ae:d2:04:53:85:87:10:21:fd:ba:
e3:9a:14:c7:74:70:cd:9d:1a:6e:0:4:1:1:1:1:1:1:1:1:1:1:1:1:
95:bf:11:31:09:ef:11:11:11:11:11:11:11:11:11:11:11:11:
b2:ae:1f:18:aa:a1:f1:a5:ed:bc:75:97:7f:cd:0d:01:9c:ac:1e:
78:de:c4:44:f6:27:3e:ee:d9:f8:15:25:61:0f:0e:01:0b:50:a6:
1d:47:50:b6:0b:0b:d5:85:c8:re:9f:3a:fs:f1:cb:bf:bf:ef:9:12:
3e:4:c9:9f:20:a3:e:cc:84:bd:cb:5e:02:5f:89:1e:0:44:14:
03:08:14:14:14:14:14:14:14:14:14:14:14:14:14:14:14:14:
97:59:dc:bf:00:31:16:53:44:39:17:3a:37:38:be:47:96:6d:
86:9e:eb:6d:0f:1b:09:71:84:ca:1e:11:15:bb:45:2b:cd:cc:02:
a2:9b:08:70
```

```
student@serverA:~/mdhn18_ca$ openssl ca -config ca1/openssl.cnf -extensions server_cert -days 3650 -notext -in ca1/csr/192.168.70.5.csr.pem -out ca1/certs/192.168.70.5.cert.pem
Using configuration from /home/student/openssl.cnf
Enter pass phrase for /home/student/openssl.cnf:
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 8194 (0x2002)
    Validity
        Not Before: Jan 14 02:22:08 2021 GMT
        Not After : Jan 12 02:22:08 2031 GMT
    Subject:
        countryName      = SE
        stateOrProvinceName = Blekinge
        localityName     = Karlskrona
        organizationName  = ET2540
        commonName        = 192.168.70.5
X509v3 extensions:
    X509v3 Basic Constraints:
        CA:FALSE
    X509v3 Subject Key Identifier:
        F1:C:E:7:C7:AD:4D:1C:52:08:D9:72:3D:80:25:F7:56:6B:80:85:E3:F3
    X509v3 Authority Key Identifier:
        KeYid:43:32:5a:4b:9b:6c:01:17:E3:09:01:70:03:50:71:14:6E:BA:49:07
```



```

Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal *
student@serverA: ~/mdhn18_ca

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
student@serverA:~/mdhn18_ca$ openssl req -nouot -text -in ca1/csr/192.168.70.6.pem
Certificate Request:
Data:
Version: 1 (0x0)
Subject: C = SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = 192.168.70.6
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:b1:0b:18:f2:b1:86:e0:c3:c3:f0:a4:0a:c0:c0:
e5:eb:ef:de:c4:b5:d0:08:21:e8:d6:9d:04:66:ba:
28:1e:0f:9c:5f:77:1b:0d:c1:b5:8c:5d:0f:ed:26:
ab:b6:5f:9f:c9:78:9e:88:f6:4e:ba:88:c1:03:26:
30:43:3a:cfc:f8:1d:84:6d:4b:05:c9:56:09:cb:ac:
33:17:73:72:1e:3d:ab:3f:c0:15:ea:33:cc:86:1a:
f7:eb:40:32:ba:1f:f6:5b:00:d0:a3:21:cb:be:e9:
f2:35:3b:0d:c1:c5:53:10:88:27:d6:82:a1:31:f9:90:
d9:46:51:97:53:39:0c:8c:50:9c:ab:bb:f4:c5:cd:86:
a2:26:29:a0:23:33:e9:b3:82:12:ae:2f:59:a2:2f:85:
64:5a:27:a1:3c:d7:24:9a:c7:64:96:e4:4b:7:12:
54:d0:3f:bd:04:42:c1:bd:ba:71:1a:b2:a3:7:84:7f:
f4:35:3b:0d:c1:c5:53:10:88:27:d6:82:a1:31:f9:90:
c9:83:3e:5d:0c:45:b9:63:71:04:86:55:98:25:20:
e7:bd:aa:32:32:32:04:58:f1:7e:94:17:f0:f0:1b:
fa:d3:0f:9e:c3:eb:19:91:2d:fa:0c:67:ee:2a:c9:
02:13
Exponent: 65537 (0x10001)
Attributes:
a0:00
Signature Algorithm: sha256WithRSAEncryption
03:0c:f0:65:dd:07:46:7b:6a:6e:08:08:0d:37:9b:08:ed:32:
03:0c:f0:65:dd:07:46:7b:6a:6e:08:08:0d:37:9b:08:ed:32:
dd:25:37:9e:9e:0d:21:c2:74:12:32:49:c2:de:be:75:7:49:
52:1e:0c:8c:30:14:43:3a:27:28:a6:c4:51:dd:cd:17:29:7e:
8f:4e:18:a1:f0:d5:dc:a1:b6:fd:a1:d2:25:2e:72:23:dc:c5:ab:
c9:b7:32:33:3a:1e:18:a7:77:17:25:2e:72:23:dc:c5:ab:
ab:35:45:0d:2a:ab:09:d2:ef:31:f7:f0:d4:b2:50:99:a6:52:
1b:1c:07:53:09:c5:10:e0:70:8f:c3:70:a2:41:ea:c1:d6:80:
1b:1c:07:53:09:c5:10:e0:70:8f:c3:70:a2:41:ea:c1:d6:80:
70:c3:62:69:9c:68:71:53:30:da:5b:8f:34:c7:40:06:51:b3:
#e:3a:6h:6a

student@serverA:~/mdhn18_ca
```

```

Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal *
student@serverA: ~/mdhn18_ca

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
student@serverA:~/mdhn18_ca$ openssl ca -config ca1/openssl.cnf -extensions server_cert -days 3650 -notext -in ca1/csr/192.168.70.6.pem -out ca1/certs/192.168.70.6.cert.pem
Using configuration from ca1/openssl.cnf
-----
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 8195 (0x2003)
    Validity
        Not Before: Jan 14 02:24:58 2021 GMT
        Not After : Jan 12 02:24:58 2031 GMT
    Subject:
        commonName   = SE
        stateOrProvinceName = Blekinge
        localityName  = Karlskrona
        organizationName = ET2540
        commonName   = 192.168.70.6
X509v3 extensions:
    X509v3 Subject Key Identifier:
        66:0B:5A:D1:C0:9C:9E:5A:C3:FD:98:E5:4F:EB:19:48:18:A2:B8
    X509v3 Authority Key Identifier:
        keyid:1a:32:FA:69:04:41:01:17:E3:98:91:79:92:71:A4:6E:86:59:97
        DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=RootRabilu
        serial:10:00
    X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
    X509v3 Extended Key Usage:
        TLS Web Server Authentication
    X509v3 CRL Distribution Points:
        Full Name:
            URL:https://localhost/ca1.crl.pem

Certificate is to be certified until Jan 12 02:24:58 2031 GMT (3650 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
-----
Data Base Updated
student@serverA:~/mdhn18_ca$ openssl x509 -nouot -text -in ca1/certs/192.168.70.6.cert.pem
-----
```

```

Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal *
student@serverA: ~/mdhn18_ca

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
student@serverA:~/mdhn18_ca$ openssl x509 -nouot -text -in ca1/certs/192.168.70.6.cert.pem
-----
```

Certificate:

```

Data:
Version: 3 (0x9)
Serial Number: 8195 (0x2003)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = CAIRabilu
Validity
    Not Before: Jan 14 02:24:58 2021 GMT
    Not After : Jan 12 02:24:58 2031 GMT
Subject:
    commonName   = SE
    stateOrProvinceName = Blekinge
    localityName  = Karlskrona
    organizationName = ET2540
    commonName   = 192.168.70.6
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
        Modulus:
00:b1:0b:18:f2:b1:86:e0:c3:c3:f0:a4:0a:c0:c0:
e5:eb:ef:de:c4:b5:d0:08:21:e8:d6:9d:04:66:ba:
28:1e:0f:9c:5f:77:1b:0d:c1:b5:8c:5d:0f:ed:26:
ab:b6:5f:9f:c9:78:9e:88:f6:4e:ba:88:c1:03:26:
30:43:3a:cfc:f8:1d:84:6d:4b:05:c9:56:09:cb:ac:
33:17:73:72:1e:3d:ab:3f:c0:15:ea:33:cc:86:1a:
f7:eb:40:32:ba:1f:f6:5b:00:d0:a3:21:cb:be:e9:
f2:35:3b:0d:c1:c5:53:10:88:27:d6:82:a1:31:f9:90:
c3:35:3b:0d:c1:c5:53:10:88:27:d6:82:a1:31:f9:90:
d9:46:51:97:53:39:0c:8c:50:9c:ab:bb:f4:c5:cd:86:
a2:26:29:a0:23:33:e9:b3:82:12:ae:2f:59:a2:2f:85:
64:5a:27:a1:3c:d7:24:9a:c7:64:96:e4:4b:7:12:
54:d0:3f:bd:04:42:c1:bd:ba:71:1a:b2:a3:7:84:7f:
f4:f9:27:77:00:3c:ad:08:5b:c9:c9:31:86:93:
c3:35:3b:0d:c1:c5:53:10:88:27:d6:82:a1:31:f9:90:
d9:46:51:97:53:39:0c:8c:50:9c:ab:bb:f4:c5:cd:86:
e7:bd:aa:32:32:32:04:58:f1:7e:94:17:f0:f0:1b:
fa:d3:0f:9e:c3:eb:19:91:2d:fa:0c:67:ee:2a:c9:
02:13
Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Subject Key Identifier:
        66:0B:5A:D1:C0:9C:9E:5A:C3:FD:98:E5:4F:EB:19:48:18:A2:B8
    X509v3 Authority Key Identifier:
        keyid:1a:32:FA:69:04:41:01:17:E3:98:91:79:92:71:A4:6E:86:59:97
        DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=RootRabilu
        serial:10:00

X509v3 Key Usage: critical
    Digital Signature, Key Encipherment
    TLS Web Server Authentication
X509v3 Extended Key Usage:
```

```

student@serverA:~$ openssl verify -CAfile ca/certs/ca1.cert-chain.pem ca/certs/192.168.70.6.cert.pem
ca/certs/192.168.70.6.cert.pem: OK
student@serverA:~$ mdhn18_ca

```

- Distribute the certificate exact location in serverA and serverB.

```

student@serverA:~$ sudo ls /etc/ipsecd/private/
192.168.70.5.key.pem
student@serverA:~$ sudo ls /etc/ipsecd/certs/
192.168.70.5.cert.pem
student@serverA:~$ sudo ls /etc/ipsecd/cacerts/
ca1.cert.pem root.cert.pem
student@serverA:~$ 
student@serverB:~$ sudo ls /etc/ipsecd/private/
192.168.70.6.key.pem
student@serverB:~$ sudo ls /etc/ipsecd/certs/
192.168.70.6.cert.pem
student@serverB:~$ sudo ls /etc/ipsecd/cacerts/
ca1.cert.pem root.cert.pem
student@serverB:~$ 

```

- Edit the ipsec.conf and ipsec.secrets as shown in below:

```

# Sample VPN connections
#conn sample-self-signed
# leftsubnet=10.1.0.0/16
# leftcert=SelfCert.der
# leftscert=never
# rightsubnet=10.2.0.0/16
# rightcert=PeerCert.der
# auto=start
#
#conn sample-with-ca-cert
# leftsubnet=10.1.0.0/16
# leftcert=MyCert.pem
# right=192.168.0.2
# rightsubnet=10.2.0.0/16
# rightid="C=CH, O=Linux strongSwan CN=peer name"
# auto=start
#
#conn %default
#   ikelifetime=60m
#   keylife=20m
#   rekeymargin=3m
#   keytries=3
#   nobike=no
#   keyexchange=ikev2
#
#conn serverA-to-serverB-transport
# left=192.168.70.5
# leftcert=192.168.70.5.cert.pem
# leftid="C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5"
# leftscert=never
# right=192.168.70.6
# rightid="C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
# type=transport
# authby=rsa
# auto=route
#

```

```

# This file holds shared secrets or RSA private keys for authentication.
# RSA private key for this host, authenticating it to any other host
# which knows the public part.
6 192.168.70.5 192.168.70.6 : PSK "student"
7 : RSA 192.168.70.5.key.pem

```

- Here is ipsec listcacerts

```

student@serverA:~$ sudo ipsec rereadcacerts
student@serverA:~$ sudo ipsec listcacerts

List of X.509 CA Certificates

subject: "C=SE, ST=Blekinge, O=ET2540, CN=CAIRabul"
issuer: "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=RootRabul"
validity: not before Jan 13 22:05:46 2021, ok
not after Jan 11 22:05:46 2031, ok (expires in 3649 days)
serial: 10:8E:00:00:00:00:00:00:00:00:00:00:00:00:00:00
flags: CA CRLSign
pathlen: 0
authkeyid: 2d:32:ff:fa:80:41:01:e3:98:91:79:92:5b:71:a4:e6:b6:59:97
subkeyid: RSA_4096_bits
keyid: 44:c1:22:ff:c3:d0:ac:ea:bd:59:96:3f:4d:b2:25:f0:a1:36:c8:c6
subkey: a2:32:fa:00:a6:41:01:17:e3:98:91:79:92:5b:71:a4:e6:b6:59:97

subject: "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=RootRabul"
issuer: "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=RootRabul"
validity: not before Jan 13 21:44:32 2021, ok
not after Jan 08 21:44:32 2041, ok (expires in 7299 days)
serial: cd:43:ee:22:39:07:3e:39
flags: CA CRLSign self-signed
authkeyid: dd:ae:67:46:82:20:5d:e0:74:d1:e5:de:2e:ff:6d:2e:b0:04:34:2b
subkeyid: dd:ae:67:46:82:20:5d:e0:74:d1:e5:de:2e:ff:6d:2e:b0:04:34:2b
pubkey: RSA_4096_bits
keyid: d3:d4:a5:b7:a7:57:1a:cf:76:30:92:92:8c:ed:9d:9e:7c:f2:73:1e:54
subkey: dd:ae:67:46:82:20:5d:e0:74:d1:e5:de:2e:ff:6d:2e:b0:04:34:2b
student@serverA:~$ sudo ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.6.2 IPsec [starter]...
student@serverA:~$ 
```



```

student@serverB:~$ sudo ipsec rereadcacerts
student@serverB:~$ sudo ipsec listcacerts

List of X.509 CA Certificates

subject: "C=SE, ST=Blekinge, O=ET2540, CN=CAIRabul"
issuer: "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=RootRabul"
validity: not before Jan 13 22:05:46 2021, ok
not after Jan 11 22:05:46 2031, ok (expires in 3649 days)
serial: 10:8E:00:00:00:00:00:00:00:00:00:00:00:00:00:00
flags: CA CRLSign
pathlen: 0
authkeyid: a2:32:fa:60:a6:41:01:17:e3:98:91:79:92:5b:71:a4:e6:b6:59:97
subkeyid: RSA_4096_bits
keyid: 44:c1:22:ff:c3:d0:ac:ea:bd:59:96:3f:4d:b2:25:f0:a1:36:c8:c6
subkey: a2:32:fa:00:a6:41:01:17:e3:98:91:79:92:5b:71:a4:e6:b6:59:97

subject: "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=RootRabul"
issuer: "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=RootRabul"
validity: not before Jan 08 21:44:32 2041, ok (expires in 7299 days)
serial: cd:43:ee:22:39:07:3e:39
flags: CA CRLSign self-signed
authkeyid: dd:ae:67:46:82:20:5d:e0:74:d1:e5:de:2e:ff:6d:2e:b0:04:34:2b
subkeyid: dd:ae:67:46:82:20:5d:e0:74:d1:e5:de:2e:ff:6d:2e:b0:04:34:2b
pubkey: RSA_4096_bits
keyid: d3:d4:a5:b7:a7:57:1a:cf:76:30:92:92:8c:ed:9d:9e:7c:f2:73:1e:54
subkey: dd:ae:67:46:82:20:5d:e0:74:d1:e5:de:2e:ff:6d:2e:b0:04:34:2b
student@serverB:~$ sudo ipsec restart
Stopping strongSwan IPsec...
Starting StrongSwan 5.6.2 IPsec [starter]...
student@serverB:~$ 
```

- Host-to-host transport mode VPN with cert authentication successfully established.

```

student@serverA:~$ sudo ipsec up serverA-to-serverB-transport
Untangling IPsec security associations
generating SA_SA_INIT request 0 [ SA KE NO(NATD_S_IP) (NATD_O_IP) (FRAG_SUP) (HASH_ALG) (NCREDIR_SUP) ]
sending packet: From 192.168.70.5[500] to 192.168.70.6[500] (194 bytes)
parsed IKE_SA_INIT response 0 [ SA KE NO(NATD_S_IP) (NATD_O_IP) CERTREQ NFRAG_SUP (NOHASH_ALG) (NCREDIR_SUP) ]
received cert request for "C=SE, ST=Blekinge, O=ET2540, CN=CAIRabul"
parsed cert response 0 [ SA KE NO(NATD_S_IP) (NATD_O_IP) CERTREQ NFRAG_SUP (NOHASH_ALG) (NCREDIR_SUP) ]
sending cert request for "C=SE, ST=Blekinge, O=ET2540, CN=RootRabul"
sending cert request for "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5" (myself) with RSA_EMSA_PKCS1_SHA2_256 success
ul
authentication of "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5" (myself) with RSA_EMSA_PKCS1_SHA2_256 success
ul
sending end entity cert "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5"
generating IKE_SA_INIT request 1 [ IDI CERT_NINIT_CONTACT CERTREQ IDP AUTH_NOUSE_TRANSF SA TSL Tsr (NCREDIR_AUTH) (NEAP_ONLY) N (MSG_ID_SYN_SUP) ]
parsed IKE_SA_INIT response 1 [ IDI CERT_NINIT_CONTACT CERTREQ IDP AUTH_NOUSE_TRANSF SA TSL Tsr (NCREDIR_AUTH) (NEAP_ONLY) N (MSG_ID_SYN_SUP) ]
generating IKE_AUTH request 1 [ EF(1/2) ]
generating IKE_AUTH request 1 [ EF(2/2) ]
sending packet: From 192.168.70.5[500] to 192.168.70.6[500] (122 bytes)
received packet: From 192.168.70.6[500] to 192.168.70.5[500] (122 bytes)
parsed IKE_AUTH response 1 [ EF(1/2) ]
parsed IKE_AUTH response 1 [ EF(2/2) ]
received Fragment #1 of 2, waiting for complete IKE message
received packet: From 192.168.70.6[500] to 192.168.70.5[500] (724 bytes)
received Fragment #2 of 2, reassembling fragmented IKE message
parsed IKE_AUTH response 1 [ IDR CERT AUTH NOUSE_TRANSF ] SA TSL Tsr (NCREDIR_AUTH) (NEAP_ONLY) N (MSG_ID_SYN_SUP)
parsed IKE_AUTH response 1 [ IDR CERT AUTH NOUSE_TRANSF ] SA TSL Tsr (NCREDIR_AUTH) (NEAP_ONLY) N (MSG_ID_SYN_SUP)
using certificate "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=RootRabul"
using trusted intermediate ca certificate "C=SE, ST=Blekinge, O=ET2540, CN=CAIRabul"
choosing certificate "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5"
Fetching crl from https://localhost/ca1.crl.pem
unable to fetch from https://localhost/ca1.crl.pem, no capable fetcher found
certificate status is not available
using trusted ca certificate "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=RootRabul"
choose certificate "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=CAIRabul"
certificate status is not available
reached self-signed root ca with a path length of 1
parsed certificate "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=RootRabul", RSA_EMSA_PKCS1_SHA2_256 successful
IKE_SA server-to-server-transport[1] established between 192.168.70.5[500] (C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5), 192.168.70.6[500] (C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6)
maximum IKE_SA lifetime 3500s
CHILD_SA serverA-to-serverB-transport[2] established with SPIs c469cb1_l c57e71db_o and TS 192.168.70.5/32 == 192.168.70.6/32
connection 'serverA-to-serverB-transport' established successfully
student@serverA:~$ 
```



```

student@serverB:~$ sudo ipsec up serverB-to-serverA-transport
establishing CHILD_SA serverB-to-serverA-transport[3]
generating SA_SA_INIT request 0 [ SA KE NO(NATD_S_IP) (NATD_O_IP) (FRAG_SUP) (HASH_ALG) (NCREDIR_SUP) ]
sending packet: From 192.168.70.5[500] to 192.168.70.6[500] (272 bytes)
received packet: From 192.168.70.6[500] to 192.168.70.5[500] (208 bytes)
parsed CREATE_CHILD_SA response 0 [ N(USE_TRANSF) SA No TSL Tsr ]
CHILD_SA serverB-to-serverA-transport[3] established with SPIs cf4c5077_l c2aa1d53_o and TS 192.168.70.6/32 == 192.168.70.5/32
connection 'serverB-to-serverA-transport' established successfully
student@serverB:~$ 
```

Server A [Running] - Oracle VM VirtualBox

```
student@serverA:~$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.6.2, Linux 4.15.0-38-generic, x86_64):
  uptime: 3 minutes, since Jan 14 04:01:33 2021
  malloc: sbrk 1622016, mmap 0, used 625712, free 996384
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon aesni aes rc2 sha2 sha3 md4 md5 md5gri random nonce x509 revocation constraints pubkey pkcs1 pkcs8 pkcs12 ppp dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac gcm actr kernel-netlink resolve socket-default connmark stroke updown eap-mschapv2 xauth-generic counters
  Listening IP addresses:
    192.168.66.100
    192.168.70.5
    192.168.70.6
    192.168.70.7
    192.168.70.8
    192.168.70.9
    192.168.70.10
    10.0.99.100
  Connections:
    serverA-to-serverB-transport: 192.168.70.5...192.168.70.6 IKEv2
    serverA-to-serverB-transport: local: [{<S>, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5} uses public key authentication
    serverA-to-serverB-transport: cert: [{<S>, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6}]
    serverA-to-serverB-transport: remote: [{<S>, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.7}]
    serverA-to-serverB-transport: child: dynamic == dynamic TRANSPORT
  Routed Connections:
    serverA-to-serverB-transport[1]: ROUTED, TRANSPORT, reqid 1
    serverA-to-serverB-transport[1]: 192.168.70.5/32 === 192.168.70.6/32
  Security Associations (1 up, 0 connecting):
    serverA-to-serverB-transport[1]: ESTABLISHED 2 minutes ago, 192.168.70.5({<S>, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5})...192.168.70.6({<S>, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6})
    serverA-to-serverB-transport[1]: IKEv2 SPIs: 3ad4fb28aabb47e_l* 819e989e83f01895_r, public key reauthentication in 49 minutes
    serverA-to-serverB-transport[1]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_AES128_XCBC/ECP_256
    serverA-to-serverB-transport[2]: INSTALLED, TRANSPORT, reqid 1, ESP SPIs: c469cb2_l c57e71db_o
    serverA-to-serverB-transport[2]: AES_CBC_128/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 12 minutes
    serverA-to-serverB-transport[2]: 192.168.70.5/32 === 192.168.70.6/32
    serverA-to-serverB-transport[3]: INSTALLED, TRANSPORT, reqid 1, ESP SPIs: c2aa1d53_l cf4c5077_o
    serverA-to-serverB-transport[3]: AES_CBC_128/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 13 minutes
    serverA-to-serverB-transport[3]: 192.168.70.5/32 === 192.168.70.6/32
student@serverA:~$
```

Server B [Running] - Oracle VM VirtualBox

```
student@serverB:~$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.6.2, Linux 4.15.0-38-generic, x86_64):
  uptime: 3 minutes, since Jan 14 04:02:19 2021
  malloc: sbrk 1622016, mmap 0, used 626224, free 995792
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 2
  loaded plugins: charon aesni aes rc2 sha2 sha3 md4 md5 md5gri random nonce x509 revocation constraints pubkey pkcs1 pkcs8 pkcs12 ppp dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac gcm actr kernel-netlink resolve socket-default connmark stroke updown eap-mschapv2 xauth-generic counters
  Listening IP addresses:
    192.168.66.100
    192.168.70.6
    192.168.70.7
    192.168.70.8
    192.168.70.9
    192.168.70.10
    10.0.99.100
  Connections:
    serverB-to-serverA-transport: 192.168.70.6...192.168.70.5 IKEv2
    serverB-to-serverA-transport: local: [{<S>, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6} uses public key authentication
    serverB-to-serverA-transport: cert: [{<S>, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5}]
    serverB-to-serverA-transport: remote: [{<S>, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.7}]
    serverB-to-serverA-transport: child: dynamic == dynamic TRANSPORT
  Routed Connections:
    serverB-to-serverA-transport[1]: ROUTED, TRANSPORT, reqid 1
    serverB-to-serverA-transport[1]: 192.168.70.6/32 === 192.168.70.5/32
  Security Associations (0 up, 1 connecting):
    serverB-to-serverA-transport[1]: ESTABLISHED 2 minutes ago, 192.168.70.6({<S>, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6})...192.168.70.5({<S>, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5})
    serverB-to-serverA-transport[1]: IKEv2 SPIs: 3ad4fb28aabb47e_l* 819e989e83f01895_r, public key reauthentication in 52 minutes
    serverB-to-serverA-transport[1]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_AES128_XCBC/ECP_256
    serverB-to-serverA-transport[2]: INSTALLED, TRANSPORT, reqid 1, ESP SPIs: c57e71db_l c469cb2_o
    serverB-to-serverA-transport[2]: AES_CBC_128/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 12 minutes
    serverB-to-serverA-transport[2]: 192.168.70.6/32 === 192.168.70.5/32
    serverB-to-serverA-transport[3]: INSTALLED, TRANSPORT, reqid 1, ESP SPIs: cf4c5077_l c2aa1d53_o
    serverB-to-serverA-transport[3]: AES_CBC_128/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 13 minutes
    serverB-to-serverA-transport[3]: 192.168.70.6/32 === 192.168.70.5/32
student@serverB:~$
```

Server A [Running] - Oracle VM VirtualBox

```
student@serverA:~$ sudo ip xfrm state
src 192.168.70.5 dst 192.168.70.6
  proto esp spl 0xfc7f077 regid 1 mode transport
  replay-window 8
  auth-trunc hmac(hash256) 0x232ff7fc4a2195bdd5235f2a8769eb1da6e551c343a25873d115d59df862f7
  a 128
    enc cbc(aes) 0x0383a82a796bb792bea8aced6796478
    anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
    sel src 192.168.70.5/32 dst 192.168.70.6/32
  src 192.168.70.6 dst 192.168.70.5
  proto esp spl 0xfc2aa0d53 regid 1 mode transport
  replay-window 32
  auth-trunc hmac(hash256) 0x4b6649774a0719a2b29e0cc2d9ac25489bbfb3cdffb656e1f6f7af5
  a 128
    enc cbc(aes) 0xcb1bfedcd9de57a707fd6d25a8c52cc
    anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
    sel src 192.168.70.6/32 dst 192.168.70.5/32
  src 192.168.70.5 dst 192.168.70.6
  proto esp spl 0xfc57e71db regid 1 mode transport
  replay-window 32
  auth-trunc hmac(hash256) 0x09969ec0ce9a51c1ddb797ca07416fce1115f29e1fda1c97c8d90bc12afc0
  a 128
    enc cbc(aes) 0x04dc105db0d0647fe7c25945ae8971a
    anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
    sel src 192.168.70.6/32 dst 192.168.70.5/32
  src 192.168.70.6 dst 192.168.70.5
  proto esp spl 0xfc4956cb2 regid 1 mode transport
  replay-window 32
  auth-trunc hmac(hash256) 0x73dce79ba5809d12b69ac457cf904eb5d0bfb844fd15b109ec283117c45ea
  a 128
    enc cbc(aes) 0x03aeef243d9c07ef28d0588da9924725
    anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
    sel src 192.168.70.5/32 dst 192.168.70.6/32
  src 192.168.70.5 dst 192.168.70.6
  proto esp spl 0xfc57e71db regid 1 mode transport
  replay-window 32
  auth-trunc hmac(hash256) 0x09969ec0ce9a51c1ddb797ca07416fce1115f29e1fda1c97c8d90bc12afc0
  a 128
    enc cbc(aes) 0x04dc105db0d0647fe7c25945ae8971a
    anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
    sel src 192.168.70.5/32 dst 192.168.70.6/32
student@serverA:~$
```

Server B [Running] - Oracle VM VirtualBox

```
student@serverB:~$ sudo ip xfrm state
src 192.168.70.6 dst 192.168.70.5/32
  dir out priority 367231
  tmpl src 0.0.0.0 dst 0.0.0.0
    proto esp spl 0xc2aa1d53 regid 1 mode transport
  src 192.168.70.5/32 dst 192.168.70.6/32
  dir in priority 367231
  tmpl src 0.0.0.0 dst 0.0.0.0
    proto esp reqid 1 mode transport
  src 0.0.0.0/0 dst 0.0.0.0/0
    socket in priority 0
  src 0.0.0.0/0 dst 0.0.0.0/0
    socket out priority 0
  src 0.0.0.0/0 dst 0.0.0.0/0
    socket in priority 0
  src 0.0.0.0/0 dst 0.0.0.0/0
    socket out priority 0
  src ::/0 dst ::/0
    socket in priority 0
  src ::/0 dst ::/0
    socket out priority 0
  src ::/0 dst ::/0
    socket in priority 0
  src ::/0 dst ::/0
    socket out priority 0
student@serverB:~$
```

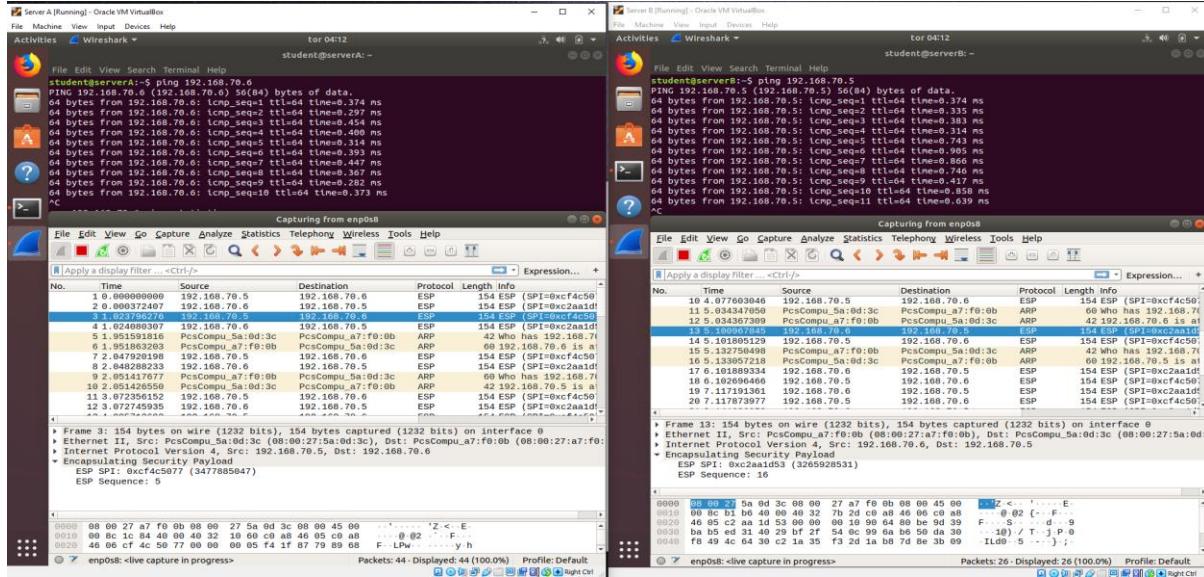
Server A [Running] - Oracle VM VirtualBox

```
student@serverA:~$ sudo ip xfrm policy
src 192.168.70.5 dst 192.168.70.6/32
  dir out priority 367231
  tmpl src 0.0.0.0 dst 0.0.0.0
    proto esp spl 0xc2aa1d53 regid 1 mode transport
  src 192.168.70.6/32 dst 192.168.70.5/32
  dir in priority 367231
  tmpl src 0.0.0.0 dst 0.0.0.0
    proto esp reqid 1 mode transport
  src 0.0.0.0/0 dst 0.0.0.0/0
    socket in priority 0
  src 0.0.0.0/0 dst 0.0.0.0/0
    socket out priority 0
  src 0.0.0.0/0 dst 0.0.0.0/0
    socket in priority 0
  src ::/0 dst ::/0
    socket out priority 0
  src ::/0 dst ::/0
    socket in priority 0
  src ::/0 dst ::/0
    socket out priority 0
  src ::/0 dst ::/0
    socket in priority 0
  src ::/0 dst ::/0
    socket out priority 0
student@serverA:~$
```

Server B [Running] - Oracle VM VirtualBox

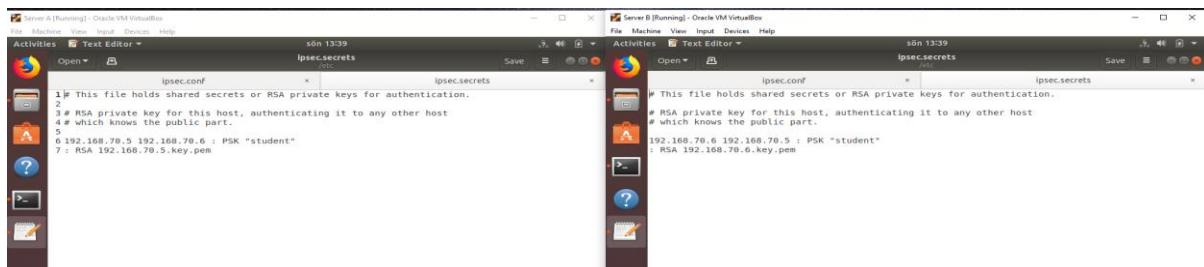
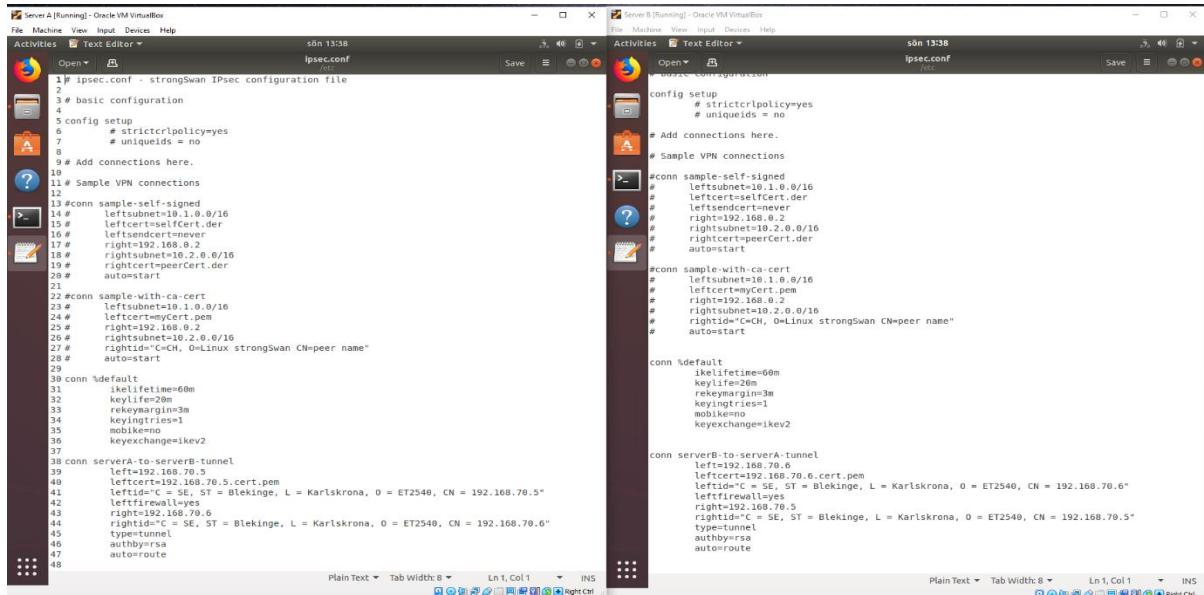
```
student@serverB:~$ sudo ip xfrm policy
src 192.168.70.6 dst 192.168.70.5/32
  dir out priority 367231
  tmpl src 0.0.0.0 dst 0.0.0.0
    proto esp spl 0xc2aa1d53 regid 1 mode transport
  src 192.168.70.5/32 dst 192.168.70.6/32
  dir in priority 367231
  tmpl src 0.0.0.0 dst 0.0.0.0
    proto esp reqid 1 mode transport
  src 0.0.0.0/0 dst 0.0.0.0/0
    socket in priority 0
  src 0.0.0.0/0 dst 0.0.0.0/0
    socket out priority 0
  src 0.0.0.0/0 dst 0.0.0.0/0
    socket in priority 0
  src ::/0 dst ::/0
    socket out priority 0
  src ::/0 dst ::/0
    socket in priority 0
  src ::/0 dst ::/0
    socket out priority 0
  src ::/0 dst ::/0
    socket in priority 0
  src ::/0 dst ::/0
    socket out priority 0
student@serverB:~$
```

- Successfully ping serverA to server and server to serverA with wireshark traffic.



Task 19: Tunnel mode VPN with cert authentication between Server A and Server B

- For this task I edit again ipsec.conf and ipsec.secrets.



- Tunnel mode VPN with cert authentication between Server A and Server B established successfully.

```

student@serverA:~$ sudo ipsec up serverA-to-serverB-tunnel
introducing IKE_SA serverA-to-serverB[1] to 192.168.70.6
generating CERT_AUTH_SA request 0 [ SA No TSLr ]
sending packet: from 192.168.70.5[500] to 192.168.70.6[500] (256 bytes)
received packet: from 192.168.70.6[500] to 192.168.70.5[500] (208 bytes)
parsed CERT_AUTH_SA response 0 [ SA No TSLr ]
IKE_SA serverA-to-serverB[1] established with SPIs ca4b6004_1 cb06f8df_o and TS 192.168.70.6/32
connection 'serverA-to-serverB-tunnel' established successfully
student@serverA:~$ 

student@serverB:~$ sudo ipsec up serverB-to-serverA-tunnel
establishing CHILD_SA serverB-to-serverA-tunnel[3]
generating CREATE_CHILD_SA request 0 [ SA No TSLr ]
sending packet: from 192.168.70.5[500] to 192.168.70.6[500] (256 bytes)
received packet: from 192.168.70.6[500] to 192.168.70.5[500] (208 bytes)
parsed CREATE_CHILD_SA response 0 [ SA No TSLr ]
CHILD_SA serverB-to-serverA-tunnel[3] established with SPIs ca4b6004_1 cb06f8df_o and TS 192.168.70.5/32
connection 'serverB-to-serverA-tunnel' established successfully
student@serverB:~$ 

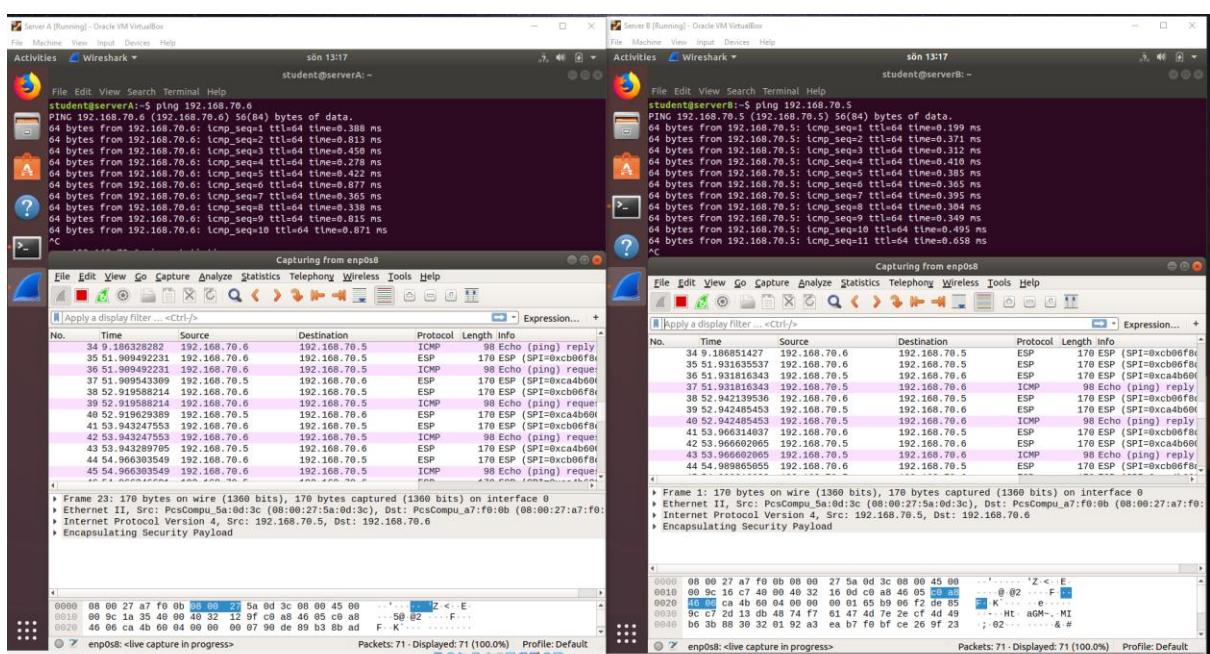
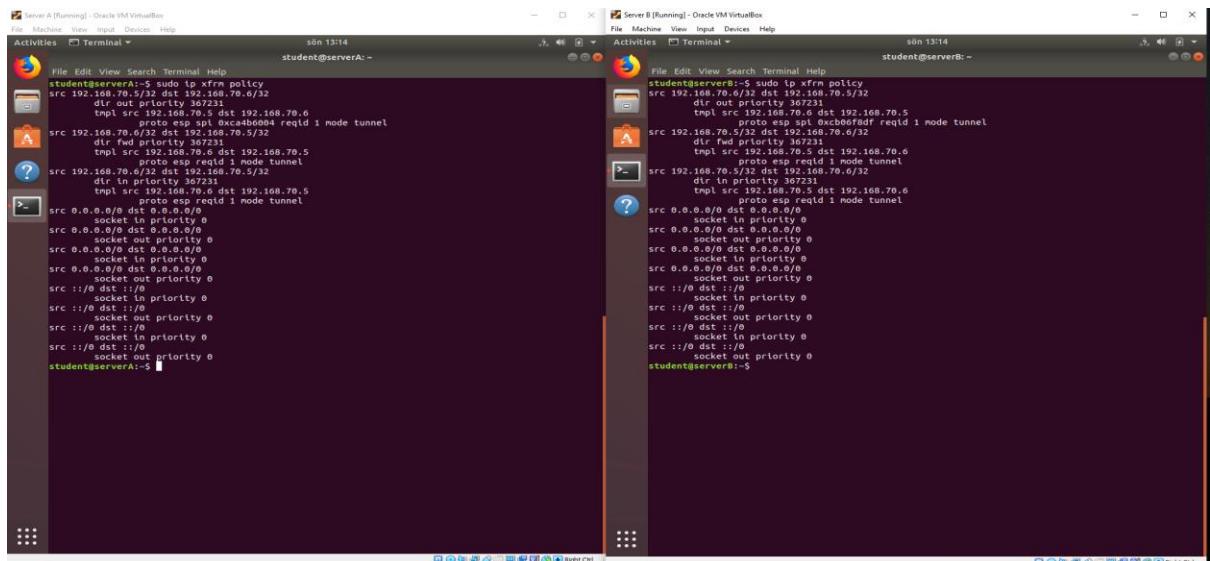
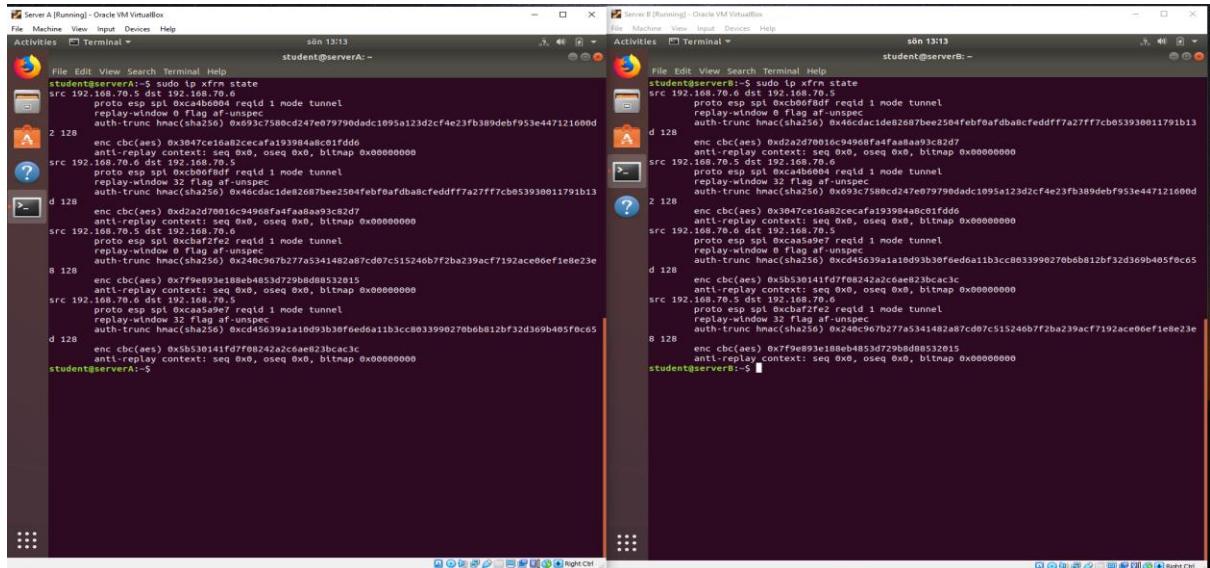
```

```

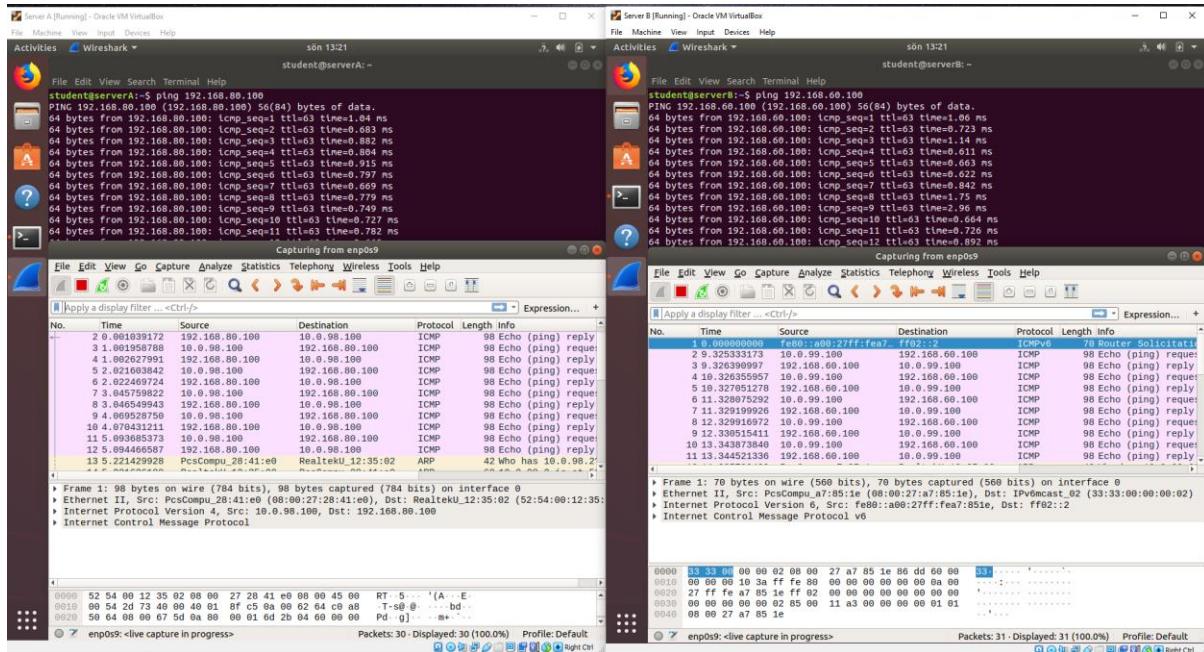
student@serverA:~$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.6.2, Linux 4.15.0-38-generic, x86_64):
    uptime: 7 minutes, since Jan 17 13:02:48 2021
    pid: 89184, uptime: 7 minutes
    worker threads: 11 of 16 idle, 5/0/0 working, job queue: 0/0/0, scheduled: 3
    loaded plugins: charon aesint aes rc2 sha2 sha1 md4 md5 md5f1 random nonce x509 revocation constraints pubkey pkcs7 pkcs8 pkcs12 ppp dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac gcm actr kernel-netlink resolve socket-default connmark stroke updown eap-mschapv2 xauth-generic counters:
    Listening IP addresses:
        192.168.68.100
        192.168.70.5
        10.0.99.100
    Connections:
    serverA-to-serverB-tunnel: 192.168.70.5...192.168.70.6 IKEV2
    serverA-to-serverB-tunnel: local: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5]
    uses public key authentication
    serverA-to-serverB-tunnel: cert: "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5"
    serverA-to-serverB-tunnel: remote: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6]
    serverA-to-serverB-tunnel: uses public key authentication
    serverA-to-serverB-tunnel: child: dynamic === dynamic TUNNEL
    Routed connections:
    serverA-to-serverB-tunnel(): ROUTED, TUNNEL, reqid 1
    serverA-to-serverB-tunnel(): 192.168.70.5/32 === 192.168.70.6/32
    serverA-to-serverB-tunnel(): 0 connected
    serverA-to-serverB-tunnel(): ESTABLISHED 6 minutes ago, 192.168.70.5[C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5]...192.168.70.6[C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6]
    serverA-to-serverB-tunnel(): IKEV2 SPIs: 32421880903c0238_*^ aa0794c4780e7Sea_r, public key reauthentication in 7 minutes
    serverA-to-serverB-tunnel(): IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_AES128_XCBC/ECP_256
    serverA-to-serverB-tunnel(): INSTALLED, TUNNEL, reqid 1, ESP SPIs: caa59e7_l cbaf2fe2_o
    serverA-to-serverB-tunnel(): AES_CBC_128/HMAC_SHA2_256_128, 0 bytes_o, 0 bytes_o, rekeying in 9 minutes
    serverA-to-serverB-tunnel(): 192.168.70.5/32 == 192.168.70.6/32
    serverA-to-serverB-tunnel(): INSTALLED, TUNNEL, reqid 1, ESP SPIs: cb06f8df_i ca4b6004_o
    serverA-to-serverB-tunnel(): AES_CBC_128/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 8 minutes
    serverA-to-serverB-tunnel(): 192.168.70.5/32 == 192.168.70.6/32
student@serverA:~$ 

student@serverB:~$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.6.2, Linux 4.15.0-38-generic, x86_64):
    uptime: 7 minutes, since Jan 17 13:02:48 2021
    pid: 892736, uptime: 7 minutes
    worker threads: 11 of 16 idle, 5/0/0 working, job queue: 0/0/0, scheduled: 2
    loaded plugins: charon aesiint aes rc2 sha2 sha1 md4 md5 md5f1 random nonce x509 revocation constraints pubkey pkcs7 pkcs8 pkcs12 ppp dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac gcm actr kernel-netlink resolve socket-default connmark stroke updown eap-mschapv2 xauth-generic
    counters:
    Listening IP addresses:
        192.168.88.100
        192.168.70.6
        10.0.99.100
    Connections:
    serverB-to-serverA-tunnel: 192.168.70.6...192.168.70.5 IKEV2
    serverB-to-serverA-tunnel: local: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6]
    uses public key authentication
    serverB-to-serverA-tunnel: cert: "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
    serverB-to-serverA-tunnel: remote: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5]
    serverB-to-serverA-tunnel: uses public key authentication
    serverB-to-serverA-tunnel: child: dynamic === dynamic TUNNEL
    Routed connections:
    serverB-to-serverA-tunnel(): ROUTED, TUNNEL, reqid 1
    serverB-to-serverA-tunnel(): 192.168.70.6/32 == 192.168.70.5/32
    security associations (1 up, 0 connecting):
    serverB-to-serverA-tunnel(): ESTABLISHED 6 minutes ago, 192.168.70.6[C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6]...192.168.70.5[C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5]
    serverB-to-serverA-tunnel(): IKEV2 SPIs: 32421880903c0238_*^ aa0794c4780e7Sea_r, public key reauthentication in 40 minutes
    serverB-to-serverA-tunnel(): 0 connected
    serverB-to-serverA-tunnel(): IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_AES128_XCBC/ECP_256
    serverB-to-serverA-tunnel(): INSTALLED, TUNNEL, reqid 1, ESP SPIs: cbaf2fe2_l caa59e7_o
    serverB-to-serverA-tunnel(): AES_CBC_128/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 7 minutes
    serverB-to-serverA-tunnel(): 192.168.70.6/32 == 192.168.70.5/32
    serverB-to-serverA-tunnel(): INSTALLED, TUNNEL, reqid 1, ESP SPIs: ca4b6004_l cb06f8df_o
    serverB-to-serverA-tunnel(): AES_CBC_128/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 7 minutes
    serverB-to-serverA-tunnel(): 192.168.70.6/32 == 192.168.70.5/32
student@serverB:~$ 

```



- Tested by pinging the private addresses of Server A (192.168.60.100) and Server B (192.168.80.100), respectively.



Task 20: Tunnel mode VPN with IP forwarding for client A and client B

- For this task I edit ipsec.conf.

```

# /etc/ipsec.conf
# Sample VPN connections
conn sample-self-signed
  leftsubnet=10.1.0.0/16
  leftcert=selfcert.der
  rightcert=never
  right=192.168.0.2
  rightsubnet=10.2.0.0/16
  rightcert=peerCert.der
  auto=start

conn sample-with-ca-cert
  leftsubnet=10.1.0.0/16
  leftcert=myCert.pem
  right=192.168.0.2
  rightsubnet=10.2.0.0/16
  rightid="<CH, 0>Linux strongSwan CN=peer name"
  auto=start

conn default
  ikelifetime=60m
  keylife=20m
  rekeymargin=3m
  keyingtries=1
  mobike=no
  keyexchange=ikev2

conn serverA-to-serverB-tunnel
  left=192.168.70.5
  leftcert=192.168.70.5.cert.pem
  leftid="<SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = 192.168.70.5"
  leftsubnet=192.168.60.0/24
  leftfirewall=yes
  right=192.168.70.6
  rightid="<SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = 192.168.70.6"
  rightsubnet=192.168.80.0/24
  type=tunnel
  authby=rsa
  auto=route

conn serverB-to-serverA-tunnel
  left=192.168.70.6
  leftcert=192.168.70.6.cert.pem
  leftid="<SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = 192.168.70.6"
  leftsubnet=192.168.60.0/24
  leftfirewall=yes
  right=192.168.70.5
  rightid="<SE, ST = Blekinge, L = Karlskrona, O = ET2540, CN = 192.168.70.5"
  rightsubnet=192.168.80.0/24
  type=tunnel
  authby=rsa
  auto=route

```

- Main part of this task added firewall rules under the section “# Firewall rules for task 20”

```

Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Text Editor tor 01:20
fw_lab2.sh
Save
24 #IPPT -t nat -j
25 # Delete any user-defined chains in NAT table
26 SIPT -t nat -X
27 # Flush all chains in MANGLE table
28 SIPT -t mangle -F
29 # Delete any user-defined chains in MANGLE table
30 SIPT -t mangle -X
31 # Flush all chains in RAW table
32 SIPT -t raw -F
33 # Delete any user-defined chains in RAW table
34 SIPT -t mangle -X
35
36 # Default policy is to send to a dropping chain
37 SIPT -t filter -P INPUT ACCEPT
38 SIPT -t filter -P OUTPUT ACCEPT
39 SIPT -t filter -P FORWARD ACCEPT
40
41
42
43 # Create logging chains
44 SIPT -t filter -N input_log
45 SIPT -t filter -N output_log
46 SIPT -t filter -N forward_log
47
48 # Set some logging targets for DROPPED packets
49 SIPT -t filter -A input_log -j LOG --log-level notice --log-prefix "input drop: "
50 SIPT -t filter -A output_log -j LOG --log-level notice --log-prefix "output drop: "
51 SIPT -t filter -A forward_log -j LOG --log-level notice --log-prefix "forward drop: "
52 echo "Added Logging"
53
54 # Return from the logging chain to the built-in chain
55 SIPT -t filter -A input_log -j RETURN
56 SIPT -t filter -A output_log -j RETURN
57 SIPT -t filter -A forward_log -j RETURN
58
59
60 # Firewall rules for task 20
61 SIPT -A INPUT -s 192.168.70.5 -d 192.168.70.6 -j ACCEPT
62 SIPT -A OUTPUT -s 192.168.70.6 -d 192.168.70.5 -j ACCEPT
63 SIPT -t filter -A FORWARD -l $HIF -j ACCEPT
64 SIPT -t filter -A FORWARD -l $INIF -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
65
66
67
68 # These rules must be inserted at the end of the built-in
69 # chain to log packets that will be dropped by the default
sh Tab Width: 8 Ln 60, Col 16 INS

```



```

Server B [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Text Editor tor 01:20
fw_lab2.sh
Save
24 #IPPT -t nat -j
25 # Delete any user-defined chains in NAT table
26 SIPT -t nat -X
27 # Flush all chains in MANGLE table
28 SIPT -t mangle -F
29 # Delete any user-defined chains in MANGLE table
30 SIPT -t mangle -X
31 # Flush all chains in RAW table
32 SIPT -t raw -F
33 # Delete any user-defined chains in RAW table
34 SIPT -t mangle -X
35
36 # Default policy is to send to a dropping chain
37 SIPT -t filter -P INPUT ACCEPT
38 SIPT -t filter -P OUTPUT ACCEPT
39 SIPT -t filter -P FORWARD ACCEPT
40
41
42
43 # Create logging chains
44 SIPT -t filter -N input_log
45 SIPT -t filter -N output_log
46 SIPT -t filter -N forward_log
47
48 # Set some logging targets for DROPPED packets
49 SIPT -t filter -A input_log -j LOG --log-level notice --log-prefix "input drop: "
50 SIPT -t filter -A output_log -j LOG --log-level notice --log-prefix "output drop: "
51 SIPT -t filter -A forward_log -j LOG --log-level notice --log-prefix "forward drop: "
52 echo "Added Logging"
53
54 # Return from the logging chain to the built-in chain
55 SIPT -t filter -A input_log -j RETURN
56 SIPT -t filter -A output_log -j RETURN
57 SIPT -t filter -A forward_log -j RETURN
58
59
60 # Firewall rules for task 20
61 SIPT -A INPUT -s 192.168.70.5 -d 192.168.70.6 -j ACCEPT
62 SIPT -A OUTPUT -s 192.168.70.6 -d 192.168.70.5 -j ACCEPT
63 SIPT -t filter -A FORWARD -l $HIF -j ACCEPT
64 SIPT -t filter -A FORWARD -l $INIF -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
65
66
67
68 # These rules must be inserted at the end of the built-in
69 # chain to log packets that will be dropped by the default
sh Tab Width: 8 Ln 60, Col 29 INS

```

```

Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal tor 01:25
student@serverA:~$ sudo ./fw_lab2.sh
Added Logging
student@serverA:~$ 

```



```

Server B [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal tor 01:25
student@serverB:~$ sudo ./fw_lab2.sh
Added Logging
student@serverB:~$ 

```

```

Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal tor 01:22
student@serverA:~$ 

```

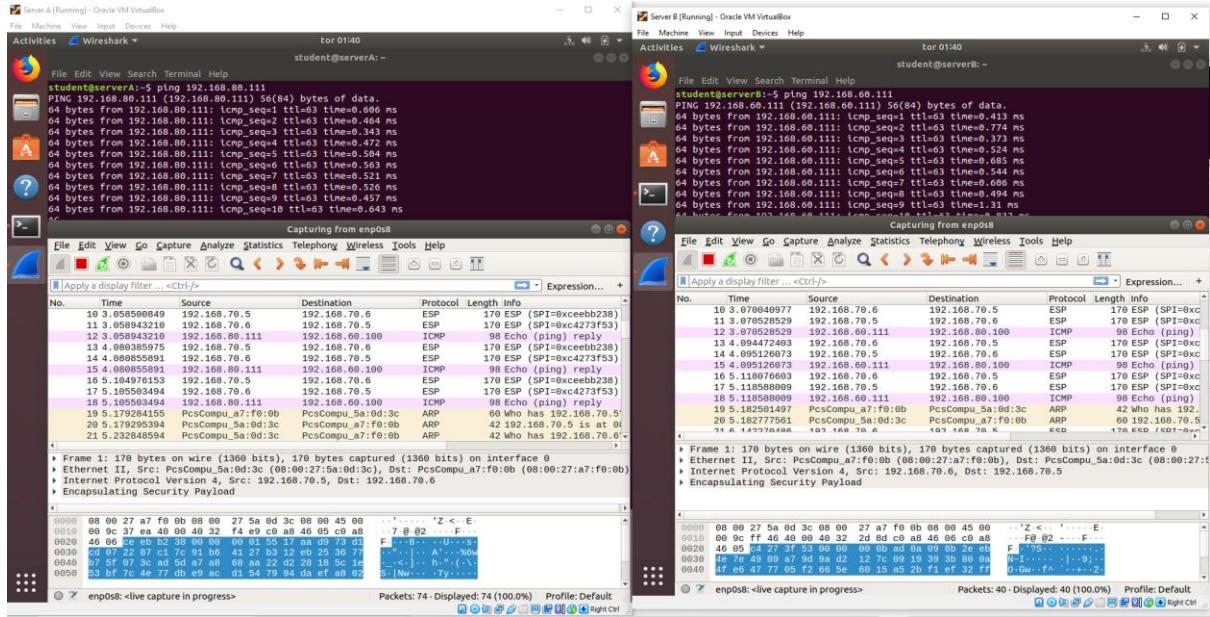


```

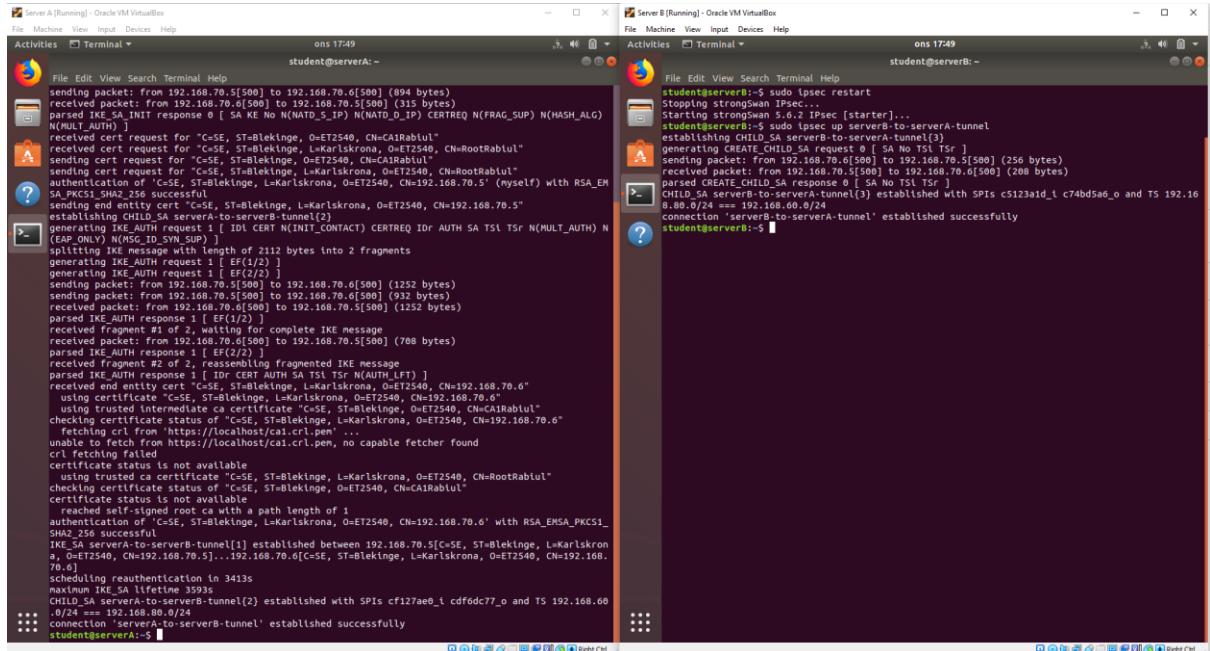
Server B [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal tor 01:22
student@serverB:~$ sudo ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.6.2 IPsec [starter]...
student@serverB:~$ sudo ipsec up serverA-to-serverB-tunnel
establishing CHILD_SA serverA-to-serverB-tunnel(3)
generating CREATE_CHILD_SA request 0 [ SA No TSL TsR ]
sending packet: from 192.168.70.5[500] to 192.168.70.5[500] (256 bytes)
received packet: from 192.168.70.5[500] to 192.168.70.5[500] (268 bytes)
parsed CREATE_CHILD_SA response 0 [ SA No TSL TsR ]
parsed SAck from 192.168.70.5[500] to 192.168.70.5[500]
connection 'serverA-to-serverB-tunnel' established successfully
student@serverB:~$ 

```

- As a evidence for this task ping from serverA to clientB and from serverB to clientA which is shown below screen short with wireshark traffic.



Task 21: Site A to Site B VPN with default DROP firewall rules



- I did not make any changes to ipsec.conf files. I just restarted strongSwan and enabled tunnel mode. Then I set the default firewall policies to DROP for both Server A and Server B. After that, I added the firewall rules for Server A and Server B mentioned in the screenshot below:

```

33 # Delete any user-defined chains in KMR table
34 #IPT -t nftangle -X
35
36 # Default firewall policy to DROP
37 #IPT -t filter -P INPUT DROP
38 #IPT -t filter -P OUTPUT DROP
39 #IPT -t filter -P FORWARD DROP
40
41
42 # Create logging chains
43 #IPT -t filter -N input_log
44 #IPT -t filter -N output_log
45 #IPT -t filter -N forward_log
46
47 # Set some logging targets for DROPPED packets
48 #IPT -t filter -A input_log -j LOG --log-level notice --log-prefix "input drop: "
49 #IPT -t filter -A output_log -j LOG --log-level notice --log-prefix "output drop: "
50 #IPT -t filter -A forward_log -j LOG --log-level notice --log-prefix "forward drop: "
51 echo "Added logging"
52
53 # Return from the logging chain to the built-in chain
54 #IPT -t filter -A input_log -j RETURN
55 #IPT -t filter -A output_log -j RETURN
56 #IPT -t filter -A forward_log -j RETURN
57
58 #Firewall rules for task 20
59 #IPT -A INPUT -s 192.168.70.5 -d 192.168.70.6 -j ACCEPT
60 #IPT -A OUTPUT -s 192.168.70.6 -d 192.168.70.5 -j ACCEPT
61 #IPT -t filter -A FORWARD -l SHIF -j ACCEPT
62 #IPT -t filter -A FORWARD -l SNIF -n conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
63
64 #task 21
65 #IPT -A FORWARD -s 192.168.80.0/24 -d 192.168.60.0/24 -j ACCEPT
66 #IPT -A FORWARD -s 192.168.60.0/24 -d 192.168.80.0/24 -j ACCEPT
67 #IPT -t filter -A FORWARD -l SHIF -j ACCEPT
68 #IPT -t filter -A FORWARD -l SNIF -n conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
69
70 #IPT -A INPUT -s 192.168.60.111 -d 192.168.70.5 -j ACCEPT
71 #IPT -A OUTPUT -s 192.168.70.5 -d 192.168.60.111 -j ACCEPT
72 #IPT -A INPUT -s 192.168.70.6 -d 192.168.70.5 -j ACCEPT
73 #IPT -A OUTPUT -s 192.168.70.5 -d 192.168.70.6 -j ACCEPT
74
75 #IPT -t nat -A POSTROUTING -j SNAT -o SNIF --to SNIP
76 # These rules must be inserted at the end of the built-in
77 # chain to log packets that will be dropped by the default
78 # DROP policy
79 #IPT -t filter -A INPUT -j input_log
80 #IPT -t filter -A OUTPUT -j output_log
81 #IPT -t filter -A FORWARD -j forward_log

```

- Then I ran the firewall scripts and enabled forwarding.

```

File Edit View Search Terminal Help
student@serverA:~$ sudo ./fw_lab2.sh
Added logging
student@serverA:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
student@serverA:~$ sudo sysctl -p
student@serverA:~$ 

File Edit View Search Terminal Help
student@serverB:~$ sudo ./fw_lab2.sh
Added logging
student@serverB:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
student@serverB:~$ sudo sysctl -p
student@serverB:~$ 

```

- The following is the iptables state after running the firewall script from server A and serverB.

```

File Edit View Search Terminal Help
student@serverA:~$ sudo iptables -L
Chain INPUT (policy DROP)
target prot opt source destination
ACCEPT all -- clientA vpnA
ACCEPT all -- vpnB vpnA
ACCEPT all -- vpnB vpnA

Chain FORWARD (policy DROP)
target prot opt source destination
ACCEPT all -- 192.168.80.0/24 192.168.80.0/24
ACCEPT all -- 192.168.60.0/24 192.168.60.0/24
ACCEPT all -- anywhere anywhere ctstate RELATED,ESTABLISHED
ACCEPT all -- anywhere anywhere ctstate RELATED,ESTABLISHED

Chain OUTPUT (policy DROP)
target prot opt source destination
ACCEPT all -- vpnA clientA
ACCEPT all -- vpnA vpnB
ACCEPT all -- vpnB vpnA

Chain forward_log (@ references)
target prot opt source destination
LOG all -- anywhere anywhere LOG level notice prefix "forward drop"
p: = RETURN all -- anywhere anywhere

Chain input_log (@ references)
target prot opt source destination
LOG all -- anywhere anywhere LOG level notice prefix "input drop"
p: = RETURN all -- anywhere anywhere

Chain output_log (@ references)
target prot opt source destination
LOG all -- anywhere anywhere LOG level notice prefix "output drop"
p: = RETURN all -- anywhere anywhere
student@serverA:~$ 

File Edit View Search Terminal Help
student@serverB:~$ sudo iptables -L
Chain INPUT (policy DROP)
target prot opt source destination
ACCEPT all -- clientB vpnB
ACCEPT all -- vpnA vpnB
ACCEPT all -- vpnB vpnA

Chain FORWARD (policy DROP)
target prot opt source destination
ACCEPT all -- 192.168.80.0/24 192.168.80.0/24
ACCEPT all -- 192.168.60.0/24 192.168.60.0/24
ACCEPT all -- anywhere anywhere ctstate RELATED,ESTABLISHED
ACCEPT all -- anywhere anywhere ctstate RELATED,ESTABLISHED

Chain OUTPUT (policy DROP)
target prot opt source destination
ACCEPT all -- vpnB clientB
ACCEPT all -- vpnB vpnA
ACCEPT all -- vpnA vpnB

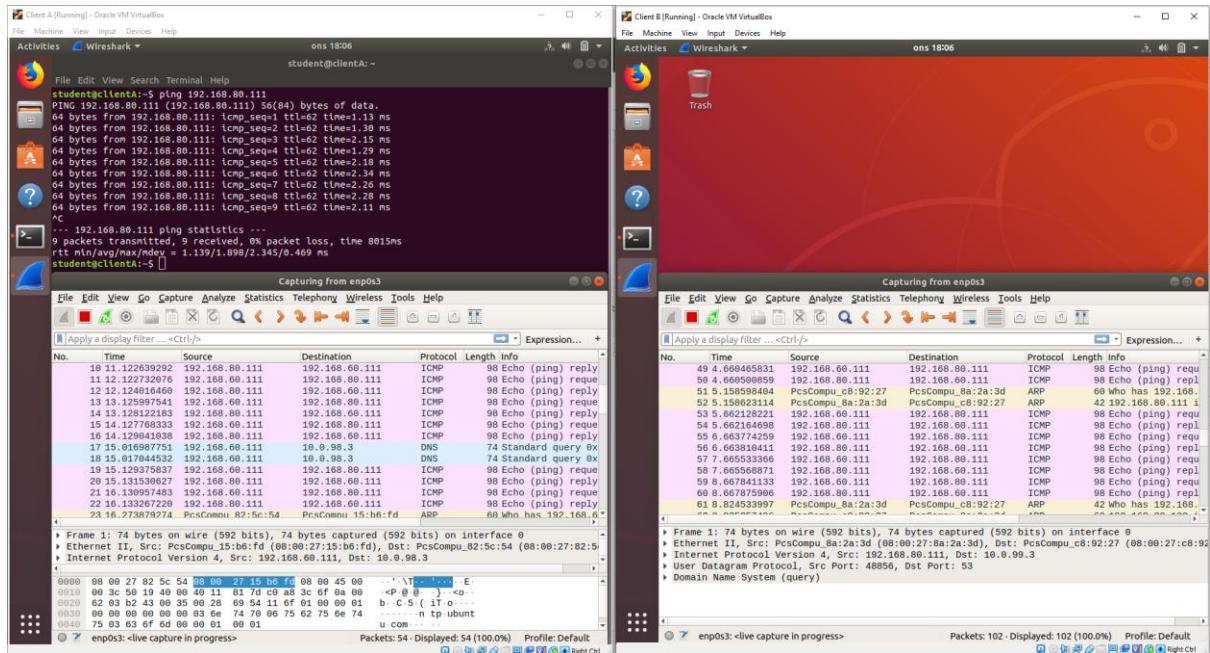
Chain forward_log (@ references)
target prot opt source destination
LOG all -- anywhere anywhere LOG level notice prefix "forward drop"
p: = RETURN all -- anywhere anywhere

Chain input_log (@ references)
target prot opt source destination
LOG all -- anywhere anywhere LOG level notice prefix "input drop"
p: = RETURN all -- anywhere anywhere

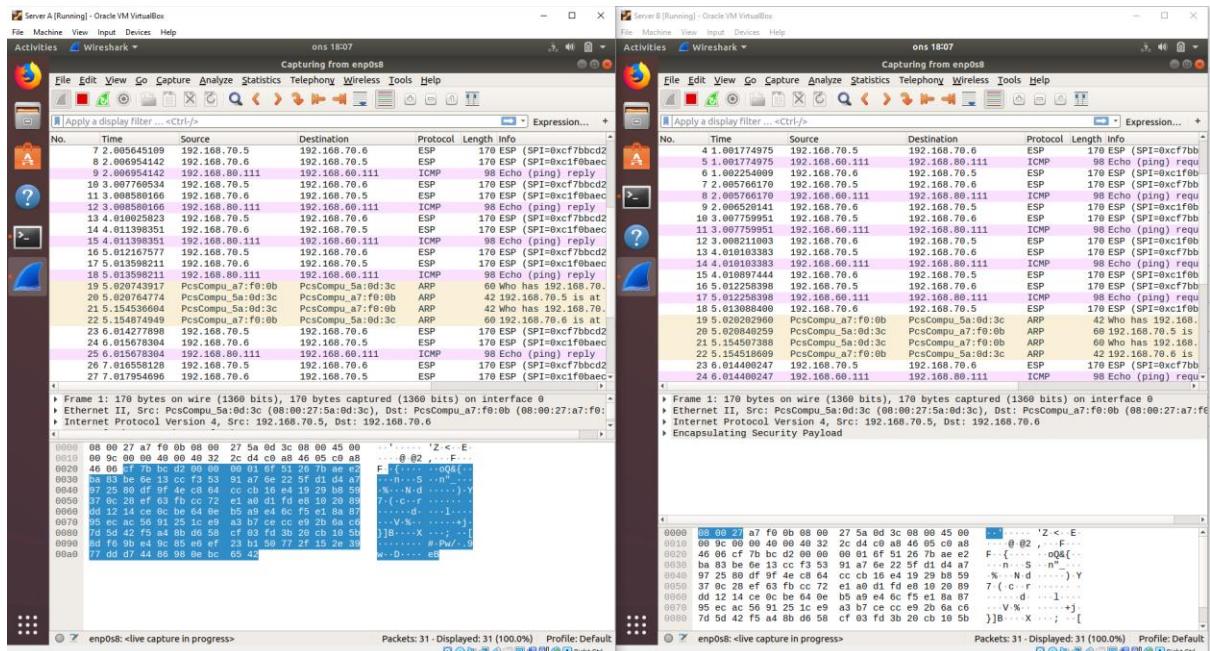
Chain output_log (@ references)
target prot opt source destination
LOG all -- anywhere anywhere LOG level notice prefix "output drop"
p: = RETURN all -- anywhere anywhere
student@serverB:~$ 

```

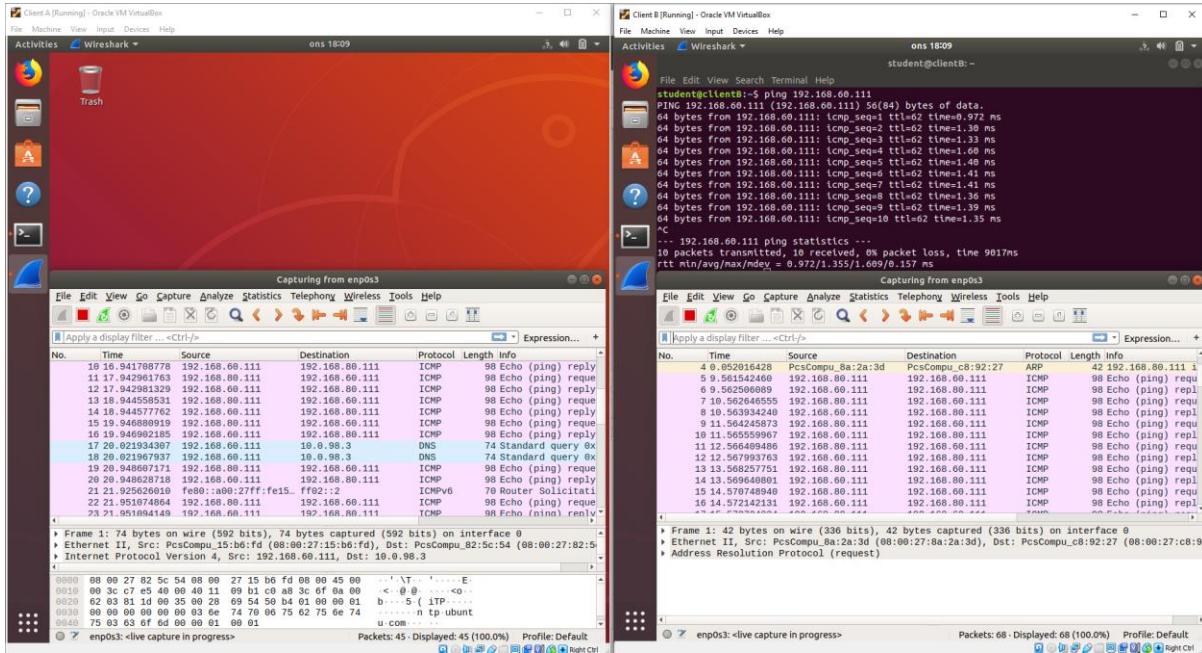
- Then I ping from Client A to Client B and it was working.



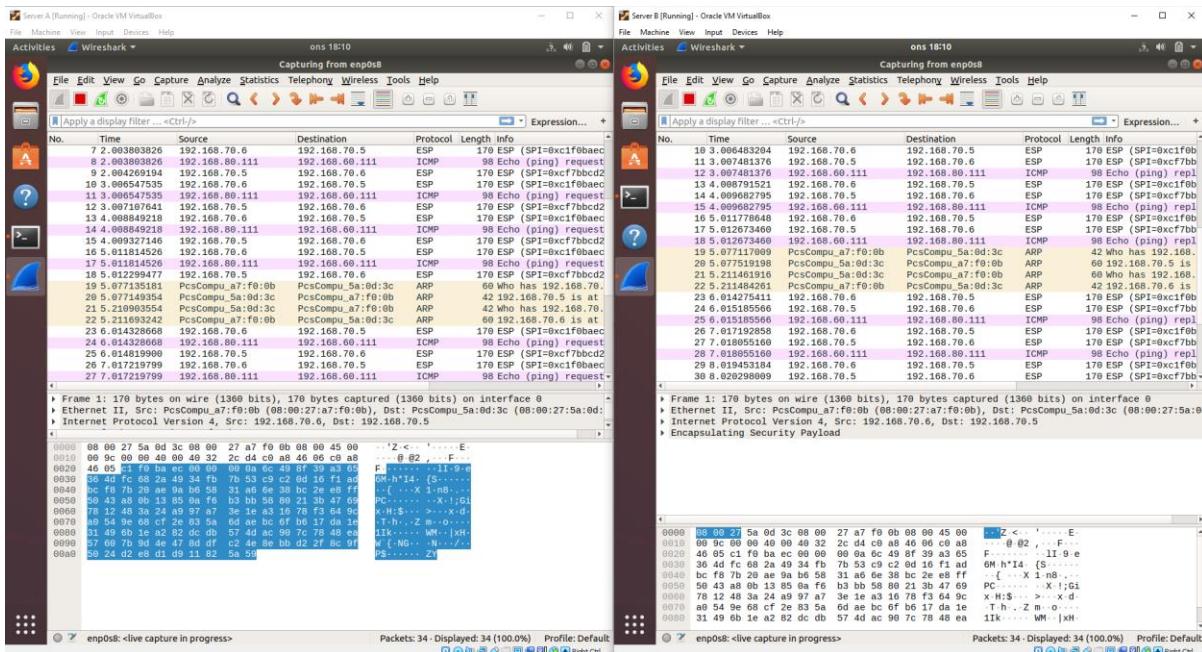
- At the same time, I observed the traffic in Server A and Server B. I found the traffic is going on over enp0s8 interface and it was clear that the traffic was going over the IPsec tunnel.



- Next, I ping from Client B to Client A and it was working.



- At the same time, I again observed the traffic in Server A and Server B. I found the traffic is going on over enp0s8 interface and it was clear that the traffic was going over the IPsec tunnel.



- Then I ping to Google from both Client A and Client B. It worked in both cases. Client A's traffic was forwarded by Server A to the NAT and this is how it accessed the internet. Same goes for Client B's to Server B.

```

Client A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal on 18:13 student@clientA:~ 
student@clientA:~$ ping 192.168.80.111
PING 192.168.80.111 (192.168.80.111) 56(84) bytes of data.
64 bytes from 192.168.80.111: icmp_seq=1 ttl=62 time=1.13 ms
64 bytes from 192.168.80.111: icmp_seq=2 ttl=62 time=1.13 ms
64 bytes from 192.168.80.111: icmp_seq=3 ttl=62 time=1.13 ms
64 bytes from 192.168.80.111: icmp_seq=4 ttl=62 time=1.13 ms
64 bytes from 192.168.80.111: icmp_seq=5 ttl=62 time=1.29 ms
64 bytes from 192.168.80.111: icmp_seq=6 ttl=62 time=2.18 ms
64 bytes from 192.168.80.111: icmp_seq=7 ttl=62 time=2.18 ms
64 bytes from 192.168.80.111: icmp_seq=8 ttl=62 time=2.34 ms
64 bytes from 192.168.80.111: icmp_seq=9 ttl=62 time=2.26 ms
64 bytes from 192.168.80.111: icmp_seq=10 ttl=62 time=2.26 ms
64 bytes from 192.168.80.111: icmp_seq=11 ttl=62 time=2.11 ms
^C
... 192.168.80.111 ping statistics ...
14 packets transmitted, 14 received, 0% packet loss, time 8015ms
rtt min/avg/max/mdev = 1.097/1.108/2.345/0.469 ms
student@clientA:~$ ping google.com
PING google.com (172.217.20.44) 56(84) bytes of data.
64 bytes from arn11s01-in-f14.1e100.net (172.217.20.46): icmp_seq=1 ttl=112 time=50.2 ms
64 bytes from arn11s01-in-f14.1e100.net (172.217.20.46): icmp_seq=2 ttl=112 time=349 ms
64 bytes from arn11s01-in-f14.1e100.net (172.217.20.46): icmp_seq=3 ttl=112 time=37.7 ms
64 bytes from arn11s01-in-f14.1e100.net (172.217.20.46): icmp_seq=4 ttl=112 time=42.0 ms
64 bytes from arn11s01-in-f14.1e100.net (172.217.20.46): icmp_seq=5 ttl=112 time=516 ms
64 bytes from arn11s01-in-f14.1e100.net (172.217.20.46): icmp_seq=6 ttl=112 time=137 ms
64 bytes from arn11s01-in-f14.1e100.net (172.217.20.46): icmp_seq=7 ttl=112 time=45.2 ms
64 bytes from arn11s01-in-f14.1e100.net (172.217.20.46): icmp_seq=8 ttl=112 time=45.2 ms
64 bytes from arn11s01-in-f14.1e100.net (172.217.20.46): icmp_seq=9 ttl=112 time=48.5 ms
64 bytes from arn11s01-in-f14.1e100.net (172.217.20.46): icmp_seq=10 ttl=112 time=49.1 ms
64 bytes from arn11s01-in-f14.1e100.net (172.217.20.46): icmp_seq=11 ttl=112 time=133 ms
64 bytes from arn11s01-in-f14.1e100.net (172.217.20.46): icmp_seq=12 ttl=112 time=48.6 ms
64 bytes from arn11s01-in-f14.1e100.net (172.217.20.46): icmp_seq=13 ttl=112 time=204 ms
64 bytes from arn11s01-in-f14.1e100.net (172.217.20.46): icmp_seq=14 ttl=112 time=41.7 ms
^C
... google.com ping statistics ...
14 packets transmitted, 14 received, 0% packet loss, time 13012ms
rtt min/avg/max/mdev = 41.707/173.259/672.391/192.903 ms
student@clientA:~$ 

Client B [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal on 18:13 student@clientB:~ 
student@clientB:~$ ping 192.168.80.111
PING 192.168.80.111 (192.168.80.111) 56(84) bytes of data.
64 bytes from 192.168.80.111: icmp_seq=1 ttl=62 time=0.972 ms
64 bytes from 192.168.80.111: icmp_seq=2 ttl=62 time=1.30 ms
64 bytes from 192.168.80.111: icmp_seq=3 ttl=62 time=1.46 ms
64 bytes from 192.168.80.111: icmp_seq=4 ttl=62 time=1.58 ms
64 bytes from 192.168.80.111: icmp_seq=5 ttl=62 time=1.40 ms
64 bytes from 192.168.80.111: icmp_seq=6 ttl=62 time=1.41 ms
64 bytes from 192.168.80.111: icmp_seq=7 ttl=62 time=1.41 ms
64 bytes from 192.168.80.111: icmp_seq=8 ttl=62 time=1.36 ms
64 bytes from 192.168.80.111: icmp_seq=9 ttl=62 time=1.39 ms
64 bytes from 192.168.80.111: icmp_seq=10 ttl=62 time=1.33 ms
^C
... 192.168.80.111 ping statistics ...
10 packets transmitted, 10 received, 0% packet loss, time 9017ms
rtt min/avg/max/mdev = 0.972/1.355/1.609/0.157 ms
student@clientB:~$ 
student@clientB:~$ ping google.com
PING google.com (172.217.20.44) 56(84) bytes of data.
64 bytes from par10s09-in-f46.1e100.net (172.217.20.46): icmp_seq=1 ttl=112 time=39.7 ms
64 bytes from par10s09-in-f46.1e100.net (172.217.20.46): icmp_seq=2 ttl=112 time=243 ms
64 bytes from par10s09-in-f46.1e100.net (172.217.20.46): icmp_seq=3 ttl=112 time=38.6 ms
64 bytes from par10s09-in-f46.1e100.net (172.217.20.46): icmp_seq=4 ttl=112 time=97.0 ms
64 bytes from par10s09-in-f46.1e100.net (172.217.20.46): icmp_seq=5 ttl=112 time=458 ms
64 bytes from par10s09-in-f46.1e100.net (172.217.20.46): icmp_seq=6 ttl=112 time=511 ms
64 bytes from par10s09-in-f46.1e100.net (172.217.20.46): icmp_seq=7 ttl=112 time=48.5 ms
64 bytes from par10s09-in-f46.1e100.net (172.217.20.46): icmp_seq=8 ttl=112 time=596 ms
64 bytes from par10s09-in-f46.1e100.net (172.217.20.46): icmp_seq=9 ttl=112 time=49.2 ms
64 bytes from par10s09-in-f46.1e100.net (172.217.20.46): icmp_seq=10 ttl=112 time=56.8 ms
64 bytes from par10s09-in-f46.1e100.net (172.217.20.46): icmp_seq=11 ttl=112 time=948 ms
64 bytes from par10s09-in-f46.1e100.net (172.217.20.46): icmp_seq=12 ttl=112 time=48.4 ms
^C
... google.com ping statistics ...
12 packets transmitted, 12 received, 0% packet loss, time 14567ms
rtt min/avg/max/mdev = 38.697/222.875/948.580/280.936 ms
student@clientB:~$ 

```

Reference:

- Lab 1.2: Certificates and VPN instructions
- https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.13/gtps7/cfgcert.html
- <http://rcardon.free.fr/websign/download/api-x509ext/be/cardon/asn1/x509/extensions/KeyUsage.html>
- <https://www.phildev.net/ssl/opensslconf.html>
- https://www.ibm.com/support/knowledgecenter/sl/SSKTMJ_9.0.1/admin/conf_keyusageextensions_andextendedkeyusage_r.html
- http://javadoc.iaik.tugraz.at/iaik_jce/old/iaik/x509/extensions/ExtendedKeyUsage.html
- <https://security.stackexchange.com/questions/84816/what-exactly-is-meant-by-serverauthandclientauth>
- <https://jamielinux.com/docs/openssl-certificate-authority/create-the-root-pair.html>
- <https://www.phildev.net/ssl/opensslconf.html>
- <https://linux.die.net/man/1/openssl>
- <https://www.openssl.org/docs/manmaster/man1/smime.html>
- <http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html>
- https://www.gypthecat.com/ipsec-vpn-host-to-host-on-ubuntu-14-04-with-strongswan?fbclid=IwAR1ZUnRqyNBr6ggXWzGOzH%20UL_k5LWZyKSxqhHKGcW0eZN4zSL4INdCvK00